RQF LEVEL 5

TRADE: NIT

MODULE CODE: NEWSS701

TEACHER'S GUIDE

Module name: BASIC SECURITY SERVICES ON COMPUTER NETWORK

Table of content

Acronyms

A/C: Air conditioning

AAA: Authentication, Authorization and accounting

BPA: business partner's agreement

CCTV: closed-circuit television

CIA: Confidentiality, integrity and availability

DDoS: distributed denial of service

DMZ: Demilitarized zone

DoS: Denial of service

FTP: file transfer protocol

FTPS: File Transfer Protocol over SSL

GPO: Group Policy Object

HTTP: hypertext transfer protocol

IAM: identity and access management

ICMP: Internet Control Message Protocol

ICT: Information communication and technology

IDS: Intrusion detection systems

IEEE: institute of electrical and electronic engineer

IP: Internet protocol

IPS: Intrusion prevention systems

ISO: International Organization for Standardization

IT: Information technology

LAN: Local area network

MAC: media access control

NAC: Network access control

NAT: Network address translation

NIC: network interface card

NIPS: Network Intrusion Prevention System

NIST: National Institute of Standards and Technology

NIT: networking and information technology

OSI: Open systems interconnection

P2P: peer to peer

PAT: Port address translation

PIN: personal identification number

PSK: Pre shared Key

RAT: remote access Trojan

RTB: Rwanda TVET Board

SCP: Secure Copy Protocol

SDN: Software-defined networking

SLA: Service-level agreement

SNMP: Simple Network Management Protocol

TCP: transmission control protocol

TFTP: Trivial File Transfer Protocol

UAP: User Account Control

UDP: user datagram protocol

UPS: Uninterrupted power supply

USB: Universal serial bus

UTM: Unified threat management

VLAN: Virtual local area network

WIPS: wireless intrusion prevention system

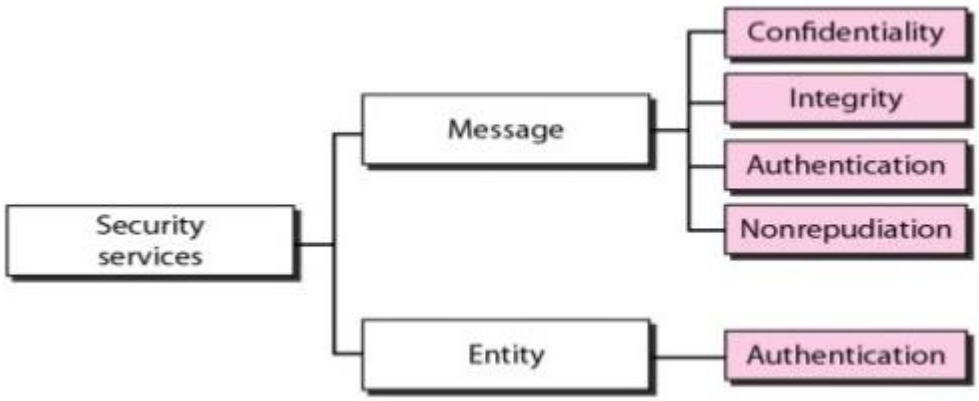
WPA: Wi-Fi Protected Access

Introduction

The term network security refers to the security services we typically expect in a network. These services are provided using cryptography. Cryptography is an art or science of transforming messages to make them secure and immune to attacks.

Network Security Services

Network Security Services means Confidentiality, Integrity, Authentication, Non-repudiation or Entity authentication. The first four services confidentiality, integrity, authenticity, and non-repudiation are related to the message exchange using a network while entity authentication service provides identification.



Network security encompasses all the steps taken to protect the integrity of a computer network and the data within it. Network security is important because it keeps sensitive data safe from cyber-attacks and ensures the network is usable and trustworthy. Successful network security strategies employ multiple security solutions to protect users and organizations from malware and cyber-attacks, like distributed denial of service.

Network security is critical because it prevents cybercriminals from gaining access to valuable data and sensitive information. When hackers get hold of such data, they can cause a variety of problems, including identity theft, stolen assets and reputational harm.

This module is intended to the learner pursuing TVET certificate V in Networking. At the end of this module the learner will be able to assess network security threats and vulnerabilities to identify risk, implement and test countermeasures for identified vulnerabilities, monitor and maintain network security, and will be able to work competitively in the ICT world under non directive supervision.

Module Code and Title: NEWSS701/BASIC SECURITY SERVICES ON COMPUTER NETWORK

Learning Units:

1. Assess network security threats and vulnerabilities to identify risks
2. Implement and test countermeasures for identified vulnerabilities and threats
3. Monitor and maintain network security

Learning Unit 1: Assess network security threats and vulnerabilities to identify risks

STRUCTURE OF LEARNING UNIT

Learning outcomes:

1.1. Adequate Assessment and report on current system security, according to required asset security level
1.2. Proper identification of system security threats and vulnerabilities
1.3. Proper mitigation of threats and vulnerability information to identify their impact on Business.
1.4. Right Suggestion of the best practice server and network hardening techniques and measures
1.5. Proper recommendations to management to address security deficiencies, according to current and future commercial and business requirements

Learning outcome 1.1 Adequate Assessment and report on current system security, according to required asset security level

 **Duration: 5 hrs**

 Learning outcome 1.1 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Explain Security fundamentals clearly
2. Define perfectly the Information security Cycle
3. Elaborate Clearly the Authentication Methods

 **Resources**

Equipment	Tools	Materials
Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual

 **Advance preparation:**

. Trainer should have all resources in place

. Trainer should have the skills about Network fundamentals

Indicative content 1.1.1: Security Fundamentals

The term information security is frequently used to describe the tasks of securing information that is in a digital format. The goal of information security is to ensure that protective measures are properly implemented to ward off attacks and prevent the total collapse of the system when a successful attack does occur.

Thus, information security is first protection. Second, information security is intended to protect information that provides value to people and organizations.

There are three protections that must be extended over information: confidentiality, integrity, and availability—or CIA:

- ✓ **Confidentiality:** It is important that only approved individuals are able to access important information.
- ✓ **Integrity:** Integrity ensures that the information is correct and no unauthorized person or malicious software has altered the data. In the example of the online purchase, an attacker who could change the amount of a purchase from $10,000.00 to $1.00 would violate the integrity of the information.
- ✓ **Availability**: Information has value if the authorized parties who are assured of its integrity can access the information. Availability ensures that data is accessible to authorized users.

In addition to CIA, another set of protections must be implemented to secure information. These are authentication, authorization, and accounting—or AAA:

- ✓ **Authentication:** Authentication ensures that the individual is who she claims to be (the authentic or genuine person) and not an imposter.
- ✓ **Authorization:** Authorization is providing permission or approval to specific technology resources. After a person has provided authentication she may have the authority to access the credit card number or enter a room that contains the web server, provided she has been given prior authorization.
- ✓ **Accounting:** Accounting provides tracking of events. This may include a record of who accessed the web server, from what location, and at what specific time.

A threat agent is a person or element that has the power to carry out a threat.

A risk is a situation that involves exposure to some type of danger.

Sometimes risk is illustrated by the calculation: Risk = Consequence × Vulnerability × Threat Likelihood.

There are different options available when dealing with risks:

- ✓ **Risk avoidance**. Risk avoidance involves identifying the risk but making the decision to not engage in the activity.
- ✓ **Acceptance.** Acceptance simply means that the risk is acknowledged but no steps are taken to address it.
- ✓ **Mitigation.** Risk mitigation is the attempt to address the risks by making risk less serious.
- ✓ **Deterrence.** If the apartment manager posted signs in the area that said "Trespassers will be punished to the full extent of the law" this would be an example of risk deterrence. Risk deterrence involves understanding something about the attacker and then informing him of the harm that may come his way if he attacks an asset.
- ✓ **Transference.** Ellie could transfer the risk to a third party. She can do this by purchasing insurance so that the insurance company absorbs the loss and pays if the scooter is stolen. This is known as risk transference.

Risk Likelihood Historical data is valuable in providing information on how likely it is that a risk will become a reality within a specific period of time. For example, when considering the risk of equipment failure, several quantitative tools can be used to predict the likelihood of the risk, including:

- ✓ ***Mean Time Between Failure (MTBF):*** MTBF calculates the average (mean) amount of time until a component fails, cannot be repaired, and must be replaced. It is a reliability term used to provide the amount of failures. Calculating the MTBF involves taking the total time measured divided by the total number of failures observed.
- ✓ ***Mean Time To Recovery (MTTR):*** MTTR is the average amount of time that it will take a device to recover from a failure that is not a terminal failure. Although MTTR is sometimes called Mean Time To Repair because in most systems this means replacing a failed hardware instead of repairing it, the Mean Time To Recovery is considered a more accurate term.
- ✓ ***Mean Time To Failure (MTTF):*** Mean Time To Failure (MTTF) is a basic measure of reliability for systems that cannot be repaired. It is the average amount of time expected until the first failure of a piece of equipment.
- ✓ ***Failure In Time (FIT):*** The Failure In Time calculation is another way of reporting MTBF. FIT can report the number of expected failures per one billion hours of operation for a device. This term is used particularly by the semiconductor industry. FIT can be stated as devices for 1 billion hours, 1 billion devices for 1000 hours each, or in other combinations.

Reducing Risk through Policies

What Is a Security Policy?

A security policy is a written document that states how an organization plans to protect the company's information technology assets. The policy outlines the protections that should be enacted to ensure that the organization's assets face minimal risks.

A security policy, along with the accompanying procedures, standards, and guidelines, is key to implementing information security in an organization.

Having a written security policy empowers an organization to take appropriate action to safeguard its data. An organization's information security policy can serve several functions:

- ✓ It can be an overall intention and direction, formally expressed by the organization's management. A security policy is a vehicle for communicating an organization's information security culture and acceptable information security behaviour.
- ✓ It details specific risks and how to address them, and so provides controls that executives can use to direct employee behaviour.
- ✓ It can help to create a security-aware organizational culture.
- ✓ It can help to ensure that employee behaviour is directed and monitored in compliance with security requirements.

Balancing Trust and Control

An effective security policy must carefully balance two key elements: trust and control. There are three approaches to trust:

- ✓ **Trust everyone all of the time**. This is the easiest model to enforce because there are no restrictions. This model, however, is impractical because it leaves systems vulnerable to attack.
- ✓ **Trust no one at any time**. This model is the most restrictive, but is also impractical. Few individuals would work for an organization that did not trust its employees.
- ✓ **Trust some people some of the time**. This approach exercises caution in the amount of trust given. Access is provided as needed, with technical controls to ensure the trust is not violated.

Who Are the Attackers?

The term hacker referred to a person who used advanced computer skills to attack computers. Different types of the attackers

- **Black hat hackers** were those attackers who violated computer security for personal gain (such as to steal credit card numbers) or to inflict malicious damage (corrupt a hard drive).
- **White hat hackers** were described as "ethical attackers": with an organization's permission they would attempt to probe a system for any weaknesses and then privately provide information back to that organization about any uncovered vulnerabilities.
- **Grey hat hackers** who would attempt to break into a computer system without the organization's permission (an illegal activity) but not for their own advantage; instead, they would publically disclose the vulnerability in order to shame the organization into taking action.

- **Information Security Life Cycle**

  Step one – Plan Involve senior management as well as stake holders and department managers. Information security is not just an IT issue, the whole organization needs to be on board in order to have a strong information security program. Form a committee and establish agreed on direction.

  Step two – Do Assign specific responsibility to individuals, determine timelines and desired results. Develop a "cookbook" that lays out policies, standards, procedures, and guidelines that can be followed to maintain a strong information security program. Just as parts of "recipes" may change over time, parts of your information security program may change as well.

  Step three – Check After solutions are implemented, review the audit findings to determine if the desired results are being achieved.

  Step four – Act These actions should be based on your audit results, with adjustments made as needed. Circle back to the Planning step and run through the process again until the threat is reduced to an acceptable level.

- **Information security controls**

  Control Types

- Technical controls use technology.
- Administrative controls use administrative or management methods.
- Physical controls refer to controls you can physically touch.
- Preventive controls attempt to prevent an incident from occurring.
- Detective controls attempt to detect incidents after they have occurred.
- Corrective controls attempt to reverse the impact of an incident.
- Deterrent controls attempt to discourage individuals from causing an incident.

- Compensating controls are alternative controls used when a primary control is not feasible

The first three control types in the list (technical, administrative, and physical) refer to how the security controls are implemented. The remaining control types refer to the goals of the security control.

a) Technical Controls

Technical controls use technology to reduce vulnerabilities. An administrator installs and configures a technical control, and the technical control then provides the protection automatically.

The following list provides a few examples: Encryption, Antivirus software, Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), Firewalls, Least privilege, etc.

b) Administrative Controls

Administrative controls use methods mandated by organizational policies or other guidelines.

For example, management may require personnel to periodically complete assessments and tests to reduce and manage risk. Many of these assessments provide an ongoing review of an organization's risk management capabilities. Some common administrative controls are:

• **Risk assessments**. Risk assessments help quantify and qualify risks within an organization so that the organization can focus on the serious risks.

• **Vulnerability assessments**. A vulnerability assessment attempts to discover current vulnerabilities or weaknesses. When necessary, an organization implements additional controls to reduce the risk from these vulnerabilities.

• **Penetration tests**. These go a step further than a vulnerability assessment by attempting to exploit vulnerabilities. For example, a vulnerability assessment might discover a server isn't kept up to date with current patches, making it vulnerable to some attacks. A penetration test would attempt to compromise the server by exploiting one or more of the unpatched vulnerabilities. People (not technology) implement these controls. Operational controls include the following families: **Awareness and training**, **Configuration and change management**, **Contingency planning**, **Media protection**, and **Physical and environmental protection**.

c) Physical Controls

Physical controls are any controls that you can physically touch. Some examples include lighting, signs, fences, security guards, and more.

Control Goals

Technical and administrative controls categorize the controls based on how they are implemented. Another way of classifying security controls is based on their goals in relationship to security incidents. Some common classifications are preventive, detective, corrective, deterrent, and compensating. The following sections describe them in more depth.

✓ **Preventive Controls**

Ideally, an organization won't have any security incidents and that is the primary goal of preventive controls—to prevent security incidents. Some examples include:

• **Hardening.** Hardening is the practice of making a system or application more secure than its default configuration.

• **Security awareness and training**. Ensuring that users are aware of security vulnerabilities and threats helps prevent incidents. When users understand how social engineers operate, they are less likely to be tricked.

• **Security guards**. Guards prevent and deter many attacks. For example, guards can prevent unauthorized access into secure areas of a building by first verifying user identities.

• **Change management**. Change management ensures that changes don't result in unintended outages. In other words, instead of administrators making changes on the fly, they submit the change to a change management process.

• **Account disablement policy.** An account disablement policy ensures that user accounts are disabled when an employee leaves. This prevents anyone, including employees, from continuing to use these accounts.

✓ **Detective Controls**

Although preventive controls attempt to prevent security incidents, some will still occur. Detective controls attempt to detect when vulnerabilities have been exploited, resulting in a security incident. An important point is that detective controls discover the event after it's occurred.

Some examples of detective controls are: Log monitoring, Trend analysis, Security audit, Video surveillance, Motion detection, etc.

✓ **Corrective Controls**

A corrective control would be any corrective action taken to correct any existing control that were faulty or wrongly installed.

✓ **Deterrent Controls**

Deterrent controls attempt to discourage a threat. Some deterrent controls attempt to discourage potential attackers from attacking, and others attempt to discourage employees from violating a security policy. You can often describe many deterrent controls as preventive controls. For example, imagine an organization hires a security guard to control access to a restricted area of a building. This guard will deter most people from trying to sneak in simply by discouraging them from even trying. The following list identifies some physical security controls used to deter threats:

• **Cable locks**. Securing laptops to furniture with a cable lock deters thieves from stealing the laptops. Thieves can't easily steal a laptop secured this way.

• **Hardware locks**. Other locks such as locked doors securing a wiring closet or a server room also deter attacks. Many server bay cabinets also include locking cabinet doors.

✓ **Compensating Controls**

Compensating controls are alternative controls used instead of a primary control. As an example, an organization might require employees to use smart cards when authenticating on a system.

Combining Control Types and Goals

It's important to realize that the control types (technical, administrative, and physical) and control goals (preventive, detective, corrective, deterrent, and compensating) are not mutually exclusive. In other words, you can describe most controls using more than one category.

Theoretical learning Activity

In pair group, Brainstorm about Authentication methods.

Points to Remember (Take home message)

- The term network security refers to the security services we typically expect in a network. These services are provided using cryptography.
- Network Security Services means Confidentiality, Integrity, Authentication, Non-repudiation or Entity authentication.
- A threat agent is a person or element that has the power to carry out a threat.
- A risk is a situation that involves exposure to some type of danger.
- A security policy is a written document that states how an organization plans to protect the company's information technology assets.
- Comparing Detection and Prevention Controls It's worth stressing the differences between detection and prevention controls. A detective control can't predict when an incident will occur and it can't prevent it. In contrast, prevention controls stop the incident from occurring at all.

Learning outcome 1.1 formative assessment

Written assessment

1. Your organization wants to reduce the amount of money it is losing due to thefts. Which of the following is the BEST example of an equipment theft deterrent?

A. Snapshots

B. **Cable locks**

C. Strong passwords

D. Persistent VDI

2. what is the Authentication Concepts?

Answer.

Authentication proves an identity with some type of credentials, such as a username and password. For example, identification occurs when users claim (or profess) their identity with identifiers such as usernames or email addresses. Users then prove their identity with authentication, such as with a password. In this context, a user's credentials refer to both a claimed identity and an authentication mechanism. The importance of authentication cannot be understated. You can't have any type of access control if you can't identify a user. In other words, if everyone is anonymous, then everyone has the same access to all resources.

3. list at least 3 authentication methods you know

Answer.

Types of the authentication:

• Something you know, such as a password or personal identification number (PIN)

• Something you have, such as a smart card or USB token

• Something you are, such as a fingerprint or other biometric identification

• Somewhere you are, such as your location using geolocation technologies

• Something you do, such as gestures on a touch screen

4. By using true (T) or false (f), Identify the types of Security countermeasures?

a. Preventative, (T)

b. Productive (F)

b. detective (T)

Learning outcome 1.2: Identify system security threats and vulnerabilities

 **Duration: 4 hrs**

 **Learning outcome 1.2 objectives:**

By the end of the learning outcome, the trainees will be able to:

1. list clearly all security threats
2. state clearly Security vulnerabilities
3. Differentiate clearly the security threats

 **Resources**

Equipment	Tools	Materials
Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual

 **Advance preparation:**

. Trainer should have all resources in place

. Trainer should have the skills about Network fundamentals

Indicative content 1.2.1: Security threats and vulnerabilities

Threats is a potential danger to information or a system

- An example: the ability to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network.

There may be weaknesses that greatly increase the likelihood of a threat manifesting

- Threats may include equipment failure, structured attacks, natural disasters, physical attacks, theft, viruses and many other potential events causing danger or damage A network vulnerability is a weakness in a system, technology, product or policy

Some Network security terms

- *Vulnerability* – a system, network or device weakness
- *Threat* – potential danger posed by a vulnerability
- *Threat Agent* – the entity that identifies a vulnerability and uses it to attack the victim
- *Risk* – likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact
- *Exposure* – potential to experience losses from a threat agent
- *Countermeasure* – put into place to mitigate the potential risk

✓ **Social Engineering**

Social engineering is the process by which intruders gain access to your facilities, your network, and even your employees by exploiting the generally trusting nature of people. A social engineering attack may come from someone posing as a vendor, or it could take the form of an email from a (supposedly) traveling executive who indicates that they have forgotten how to log on to the network or how to get into the building over the weekend. It's often difficult to determine whether the individual is legitimate or has bad intentions.

Occasionally, social engineering is also referred to as wetware. This term is used because it is a form of hacking that does not require software or hardware but rather the gray matter of the brain.

Types of Social Engineering Attacks

- **Shoulder surfing** is an attempt to gain unauthorized information through casual observation, such as looking over someone's shoulder, or monitoring screens with a camera. Screen filters can thwart shoulder surfing attempts.

Figure 1: Shoulder surfing example

- **A hoax** is a message, often circulated through email, that tells of impending doom from a virus or other security threat that simply doesn't exist.
- **Tailgating** is the practice of one person following closely behind another without showing credentials. Mantraps help prevent tailgating.

Figure 2: Tailgating example

- **Dumpster divers** search through trash looking for information. Shredding or burning documents reduces the risk of dumpster diving.
- **Watering hole attacks** discover sites that a targeted group visits and trusts. Attackers then modify these sites to download malware. When the targeted group visits the modified site, they are more likely to download and install infected files.
- **Spam** is unwanted or unsolicited email. Attackers often use spam in different types of attacks.

- **Phishing** is the practice of sending email to users with the purpose of tricking them into revealing sensitive information, installing malware, or clicking on a link.
- **Spear phishing**: Spear phishing is a unique form of phishing in which the message is made to look as if it came from someone you know and trust as opposed to an informal third party.
- **Whaling.** Whaling is nothing more than phishing or spear phishing, but for big users. Instead of sending out a To Whom It May Concern message to thousands of users, the whaler identifies one person from whom they can gain all of the data they want.
- **Vishing** When you combine phishing with Voice over IP (VoIP), it becomes known as vishing, an elevated form of social engineering. Although crank calls have been in existence since the invention of the telephone, the rise in VoIP now makes it possible for someone to call you from almost anywhere in the world without worrying about tracing, caller ID, and other landline-related features. They then pretend to be someone they are not in order to get data from you.

Social Engineering Attack Examples

Social engineering attacks are relatively low tech and are more akin to con jobs.

Here are a few examples.

Your help desk gets a call at 4 a.m. from someone purporting to be a vice president at your company.

She tells the help desk personnel that she is out of town to attend a meeting, that her computer just failed, and that she is sitting in a Kinko's trying to get a file from her desktop computer back at the office. She can't seem to remember her password and user ID. She tells the help desk representative that she needs access to the information right away or the company could lose millions of dollars. Your help desk rep believes the caller and gives the vice president her user ID and password over the phone instead of calling IT. You've been hit!

Another common approach is initiated by a phone call or email from someone claiming to be one of your software vendors, telling you that they have a critical fix that must be installed on your computer system. If this patch isn't installed right away, your system will crash and you'll lose all your data. For some reason, you've changed your maintenance account password, and they can't log on. Your systems operator gives the password to the person instead of calling IT. You've been hit again.

Theoretical learning Activity

In pair, discuss about how to test Social Engineering attack

Points to Remember (Take home message)

- Threats is a potential danger to information or a system
- Social engineering is the process by which intruders gain access to your facilities, your network, and even your employees by exploiting the generally trusting nature of people.
- *Vulnerability* – a system, network or device weakness
- *Threat* – potential danger posed by a vulnerability
- *Threat Agent* – the entity that identifies a vulnerability and uses it to attack the victim
- *Risk* – likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact
- *Exposure* – potential to experience losses from a threat agent
- *Countermeasure* – put into place to mitigate the potential risk
- Types of Social Engineering Attacks includes: Shoulder surfing, A hoax, Tailgating, Dumpster divers, spam, phishing, tec.

Learning outcome 1.2 formative assessment

Written assessment

1. As part of your training program, you're trying to educate users on the importance of security. You explain to them that not every attack depends on implementing advanced technological methods. Some attacks take advantage of human shortcomings to gain access that should otherwise be denied. What term do you use to describe attacks of this type?

A. Social engineering

B. IDS system

C. Perimeter security

D. Biometrics

Answer: A. Social engineering attacks take advantage of our inherent trust as human beings, as opposed to technology, to gain access to your environment.

2. Which of the following is another name for social engineering?

A. Social disguise

B. Social hacking

C. Wetware

D. Wetfire

3. Determining Malware Types

Malware includes several different types of malicious code, including viruses, worms, logic bombs, backdoors, Trojans, ransomware, rootkits, and more.

• **A virus** is malicious code that attaches itself to a host application. The code runs when the application is launched.

• **A worm** is self-replicating malware that travels throughout a network without user intervention.

• **A logic bomb** executes in response to an event, such as a day, time, or condition. Malicious insiders have planted logic bombs into existing systems, and these logic bombs have delivered their payload after the employee left the company.

• **Backdoors** provide another way of accessing a system. Malware often inserts backdoors into systems, giving attackers remote access to systems.

• **A Trojan** appears to be one thing, such as pirated software or free antivirus software, but is something malicious. A remote access Trojan (RAT) is a type of malware that allows attackers to take control of systems from remote locations.

• **Ransomware** is a type of malware that takes control of a user's system or data. Criminals attempt to extort payment as ransom combined to return control to the u s e r. Crypto-malware is ransomware that encrypts the user's data. Attackers demand payment to decrypt the data.

• **Spyware** is software installed on user systems without the user's knowledge or consent and it monitors the user's activities. It sometimes includes a keylogger that records user keystrokes.

• **A botnet** is a group of computers called zombies controlled through a command-and-control server. Attackers use malware to join computers to botnets. Bot herders launch attacks through botnets.

• **Rootkits take** root-level or kernel-level control of a system. They hide their processes to avoid detection. They can remove user privileges and modify system files.

Learning outcome 1.3: Mitigate threats and vulnerability

 **Duration: 5 hrs**

 **Learning outcome 1.3 objectives:**

By the end of the learning outcome, the trainees will be able to:

1. Explain clearly the general methods to mitigate common security threats to the network
2. List clearly the common security appliances and applications
3. Differentiate clearly the security threats
4. Explain clearly the security recommended practices

 **Resources**

Equipment	Tools	Materials
Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual

 **Advance preparation:**

. Trainer should have all resources in place

. Trainer should be remembering about Security threats to the network

. Trainer should be having a video/picture related to the session

Indicative content 1.3.1.: General methods to mitigate common security threats, Common security appliances and applications and security recommended practices to the network

Vulnerabilities

A feature or bug in a system or program which enables an attacker to bypass security measures.

- **General methods to mitigate common security threats to the network**

✓ **Strong authentication**: Strong authentication is any method of verifying the identity of a user or device that is intrinsically stringent enough to ensure the security of the system it protects by withstanding any attacks it is likely to encounter.

✓ **Desktop security**: Desktop security is not just a matter of protecting your own machine and the data on it.

✓ **LANs segmentation**: Network segmentation involves segregating the network into logical or functional units called zones.

Types of Network Segments

Network segments can be classified into the following categories:

✓ **Public networks** allow accessibility to everyone. The internet is a perfect example of a public network. There is a huge amount of trivial and unsecured data on public networks. Security controls on these networks are weak.

✓ **Semi-private networks** sit between public networks and private networks. From a security standpoint, a semi-private network may carry confidential information but under some regulations.

✓ **Private networks** are organizational networks that handle confidential and propriety data. Each organization can own one or more private networks. If the organization is spread over vast geographical distances, the private networks at each location may be interconnected through the internet or other public networks.

Demilitarized zone (DMZ) is a noncritical yet secure region at the periphery of a private network, separated from the public network by a firewall; it might also be separated from the private network by a second firewall. Organizations often use a DMZ as an area where they can place a public server for access by people they might not trust.

By isolating a server in a DMZ, you can hide or remove access to other areas of your network. You can still access the server using your network, but others aren't able to access further network resources.

Software-defined networking (SDN) is a relatively recent trend that can be useful both in placing security devices and in segmenting the network. Essentially, in an SDN, the entire network is virtualized, which enables relatively easy segmentation of the network. It also allows administrators to place virtualized security devices wherever they want.

- **Common security appliances and applications**

- **Firewall** — One of the first lines of defense in a network, a firewall isolates one network from another. Firewalls either can be standalone systems or included in other devices, such as routers or servers. You can find both hardware and software firewall solutions; some firewalls are available as appliances that serve as the primary device separating two networks.
- **Intrusion detection system (IDS**) — An IDS enhances cybersecurity by spotting a hacker or malicious software on a network so you can remove it promptly to prevent a breach or other problems, and use the data logged about the event to better defend against similar intrusion incidents in the future. Investing in an IDS that enables you respond to attacks. quickly can be far less costly than rectifying the damage from an attack and dealing with the subsequent legal issues.
- **Intrusion prevention system (IPS)** — An IPS is a network security solution that can not only detect intruders, but also prevent them from successfully launching any known attack. Intrusion prevention systems combine the abilities of firewalls and intrusion detection systems. However, implementing an IPS on an effective scale can be costly, so businesses should carefully assess their IT risks before making the investment. Moreover, some intrusion prevention systems are not as fast and robust as some firewalls and intrusion detection systems, so it might not be an appropriate solution when speed is an absolute requirement.
- **Network access control (NAC)** involves restricting the availability of network resources to endpoint devices that comply with your security policy. Some NAC solutions can automatically fix non-compliant nodes to ensure it is secure before access is allowed.
  NAC is most useful when the user environment is fairly static and can be rigidly controlled, such as enterprises and government agencies. It can be less practical in settings with a diverse set of users and devices that are frequently changing, which are common in the education and healthcare sectors.
- **Web filters** are solutions that by preventing users' browsers from loading certain pages from particular websites. There are different web filters designed for individual, family, institutional and enterprise use.

- **Proxy servers** act as negotiators for requests from client software seeking resources from other servers. A client connects to the proxy server, requesting some service (for example, a website); the proxy server evaluates the request and then allows or denies it. In organizations, proxy servers are usually used for traffic filtering and performance improvement.
- **Anti-DDoS devices** detect distributed denial of service (DDoS) attacks in their early stages, absorb the volume of traffic and identify the source of the attack.
- **Load balancers** are physical units that direct computers to individual servers in a network based on factors such as server processor utilization, number of connections to a server or overall server performance. Organizations use load balancers to minimize the chance that any particular server will be overwhelmed and to optimize the bandwidth available to each computer in the network.
- **Spam filters** detect unwanted email and prevent it from getting to a user's mailbox. Spam filters judge emails based on policies or patterns designed by an organization or vendor. More sophisticated filters use a heuristic approach that attempts to identify spam through suspicious word patterns or word frequency.

- **Security recommended practices**

  Network security is one of the most important ways that your business can protect itself against hackers. While it's just one tool in the cybersecurity toolbox, good network security is fundamental to keeping attackers out.

  While the exact processes to secure an internal network differ from company to company, some best practices apply to nearly every situation.

- Keep an Eye on Traffic: Monitoring and Logging
- Keep an Eye on Traffic: Monitoring and Logging
- Use Encryption, Even on Internal Sites
- Update Everything
- Segregate Device Types and Access Levels
- Control Privileged Users
- Automate Network Compliance

Theoretical learning Activity

In pair, Brainstorm the different types of network segment.

Points to Remember (Take home message)

- A feature or bug in a system or program which enables an attacker to bypass security measures.
- Strong authentication, Desktop security and LANs segmentation are the general methods to mitigate common security threats to the network
- Common security appliances: firewall, Intrusion detection system, Intrusion prevention system, Web filters, Proxy servers, Spam filters, etc.

Learning outcome 1.3 formative assessment

1. What is the application of:

a. Firewall: **a firewall isolates one network from another, Firewalls either can be standalone systems or included in other devices, such as routers or servers, you can find both hardware and software firewall solutions; some firewalls are available as appliances that serve as the primary device separating two networks.**

b. Proxy server: **act as negotiators for requests from client software seeking resources from other servers. A client connects to the proxy server, requesting some service (for example, a website); the proxy server evaluates the request and then allows or denies it. In organizations, proxy servers are usually used for traffic filtering and performance improvement.**

c. Spam filter: **detect unwanted email and prevent it from getting to a user's mailbox. Spam filters judge emails based on policies or patterns designed by an organization or vendor. More sophisticated filters use a heuristic approach that attempts to identify spam through suspicious word patterns or word frequency.**

2. State of types of network segment

Answer.

- Public networks
- Semi private networks
- Private networks

3. What is Demilitarized zone (DMZ)?

Answer.

DMZ or Demilitarized is a noncritical yet secure region at the periphery of a private network, separated from the public network by a firewall; it might also be separated from the private network by a second firewall. Organizations often use a DMZ as an area where they can place a public server for access by people they might not trust. By isolating a server in a DMZ, you can hide or remove access to other areas of your network. You can still access the server using your network, but others aren't able to access further network resources.

Learning outcome 1.4: Suggest the best practice server and network hardening techniques and measures

 **Duration: 5 hrs**

1. Install and configure the security controls when performing account management based on best practices
2. Mitigate clearly the issues associated with multiple accounts/roles and/or shared account
3. Manage account credentials clearly.

 **Resources**

Equipment	Tools	Materials
Server, Computer Firewall Router Switches	Simulation Internet	Books Trainer manual

 **Advance preparation:**

. Trainer should have all resources in place

. Trainer should be sure that the workplace is ready.

Indicative content 1.4.1: Installation and configuration of security controls when performing account management based on best practices.

- **Mitigate issues associated with users with multiple account/roles and/or shared accounts**

✓ Credential management

Group Policy

Windows domains use Group Policy to manage multiple users and computers in a domain. Group Policy allows an administrator to configure a setting once in a Group Policy Object (GPO) and apply this setting to many users and computers within the domain.

Active Directory Domain Services (AD DS) is a directory service Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Administrators implement domain Group Policy on domain controllers.

Password complexity

One method used to make passwords more secure is to require them to be complex and strong. A strong password is of sufficient length, doesn't include words found in a dictionary or any part of a user's name, and combines at least three of the four following character types:

• Uppercase characters (26 letters A–Z)

• Lowercase characters (26 letters a–z)

• Numbers (10 numbers 0–9)

• Special characters (32 printable characters, such as !, $, and *) A complex password uses multiple character types, such as Ab0@. However, a complex password isn't necessarily strong. It also needs to be sufficiently long.

Expiration

In addition to using strong passwords, users should change their passwords regularly, such as every 45 or 90 days.

Recovery

It's not uncommon for users to occasionally forget their password. In many organizations, help desk professionals or other administrators reset user passwords. Before resetting the password, it's important to verify the user's identity.

- **Password History and Password Reuse**

  Many users would prefer to use the same password forever simply because it's easier to remember.

  Even when technical password policies force users to change their passwords, many users simply change them back to the original password. Unfortunately, this significantly weakens password security. A password history system remembers past passwords and prevents users from reusing passwords. It's common for password policy settings to remember the last 24 passwords and prevent users from reusing these until they've used 24 new passwords.

- **Password length**

  In fact, the National Institute of Standards and Technology (NIST) states, Password length has been found to be a primary factor in characterizing password strength. To strengthen the security of your online information, ensure your passwords are a random mix of at least 14 to 16 characters.

- **Generic account prohibition**

  A generic account is a computer account that **is not uniquely owned by an individual use**r. It might be used by a number of individuals who share the same password. Ideally, user accounts should be uniquely owned so that account activities can be attributed to a specific person (with a reasonable level of assurance).

  Generic Account use is prohibited on all non-Public Computers and wherever Information Security and Assurance compensating controls cannot be implemented. Generic Account requests may be granted based on justification and appropriate need.

✓ **Group based privileges**

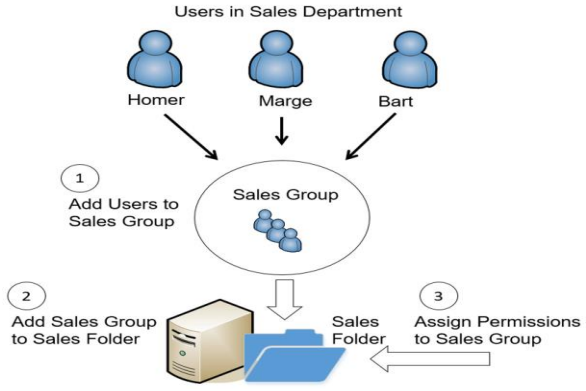


Figure 3. Group based privileges

The privileges assigned to a group may allow members of that group to access objects and perform operations that they are otherwise not allowed to do. In other words, privileges override the access rights settings.

If you select **User Manager** from the **Server Administration** tool, you will notice that the server configuration comes with some default groups: **All Users**, **Administrators**, **System Managers**, and **Security Administrators**. The default user named Administrator belongs to both the Administrators and the **Security Administrators** groups. By default, the **Administrators** group has all group privileges. Also by default, other groups have none of these privileges.

All members of a group have the same privileges on every project managed by this server configuration. The privileges apply to all levels equally: projects, views, folders, and items within folders. If users belong to more than one group, they have the maximum amount of privileges, regardless of which group provides them with those privileges.

✓ **User assigned privileges**

A privilege is the right of a user account to perform a particular system-related operation, such as shutting down the computer or changing the system time. You can use the Privilege Management feature to assign (enable) or deny (disable) privileges.

User privileges policies offer an alternative to using the default Elevate rule and can be customized to meet the needs of your organization.

Policies can range from making an individual user a member of a "Power User" group to removing user membership from the Administrators group.

When a User Privileges Policy is created, you can customize your policy using the following three tabs:

- **Group Membership** - Group Membership allows you to specify Windows user groups to be dropped or added when a policy is applied. You add a group action to the policy contents and then specify whether or not the selected group is to be applied to the newly created policy or whether their membership is to be dropped.

  When you assign membership to a user group, you will only add the group that you have selected, any nested groups will not be included. For example, if you assign group membership to Domain Administrators this will not automatically include the Local Administrator group and they will therefore need to be added separately.

- **Privileges** - A privilege is the right of a user account to perform a particular system-related operation, such as shutting down the computer or changing the system time. You can use the User Rights Management feature to enable, disable or remove privileges:

- No change - Leaves the privilege as it is with its original token.
- Enabled - Sets the flag in the token to enabled.
- Disabled - Sets the flag in the token to disabled.
- Remove - Removes the privilege from the token. You cannot undo this option.

- **Properties** - Add a description for the policy in the Properties tab. If required, you can force a custom admin token to use medium integrity, rather then defaulting to high integrity.

✓ **User access reviews**

User access reviews (sometimes referred to as "access certification" or "access recertification") are a periodic audit of existing access rights in your organization meant to remove unnecessary or outdated permissions, which are a risk to both cybersecurity and compliance.

✓ **Continuous monitoring**

Continuous monitoring is an approach where an organization constantly monitors its IT systems and networks to detect security threats, performance issues, or non-compliance problems in an automated manner. The goal is to identify potential problems and threats in real time to address them quickly.

However, not all businesses implement continuous monitoring or know how to implement it. Most companies use data to power their decision-making, but this is not necessarily continuous monitoring.

Continuous Monitoring Types

The scope of continuous monitoring involves three primary domains.

1. **The application layer of continuous monitoring measures application performance.** These applications can be custom-built by your business or third-party software. You will want to track metrics like transaction and errors per second, system uptime, and availability for application monitoring. Such tracking can help you quickly identify software bugs, performance bottlenecks, and overall user experience.

2. **Infrastructure monitoring is the next layer and covers the compute, storage, network, and other physical devices** found in traditional data centers or their virtual equivalents within cloud platforms. Monitoring this domain allows IT teams to troubleshoot performance issues, optimize usage, reduce cost, and forecast capacity needs.
3. **Network monitoring can help you understand the status of your firewalls, switches, routers, and other devices as the network evolves.** You'll capture the source and destination IP addresses, ports, and protocol metadata of your network traffic and use those to find bandwidth utilization, packet losses, delays, and potential malicious intrusion attempts.

 **Theoretical learning Activity**

In pair, Discuss the different of managing credentials.

 Practical learning Activity

Trainees in pair Create a User Privilege Management Policy

1. Select the **Library > User Privilege Policies node**.
2. Select **Add Policy** on the Privilege Management ribbon.
3. Select and right-click the new policy and select Rename.
4. Give the policy an intuitive name.
5. Do one or more of the following:

- Use the Group Membership tab to specify the credentials an application can run under, for example, what group and whether to add or drop membership for the group. Adding membership allows users to run an application as if they were a member of the group.
- Use the Privileges tab for granular control of the privileges the user will have over an application.
- Use the Properties tab to specify the integrity level. Applications with a low or medium integrity level cannot interoperate with applications that have a high integrity level. From Application Control 2020.3, a checkbox has been added to the Properties tab. It allows you to customize an admin token, assigning it a medium integrity level - instead of a high integrity level.

Assessment checklist

Checklist	Score	
	Yes	**No**
Indicator: User privilege mode policies		
✓ User privilege is added		
Indicator: Group membership		
✓ Group membership is created		
Indicator: Interpret the Group membership policy		
✓ Interpret how group membership works		
Indicator: Interpret the User privilege policy		
✓ Interpret user privilege policies		

Points to Remember (Take home message)

- when you want to manage the credentials, you have to deal with: Group Policy, Password complexity, Expiration, Recovery, Password History and Password Reuse, Password length and Generic account prohibition.
- A privilege is the right of a user account to perform a particular system-related operation, such as shutting down the computer or changing the system time.
- The privileges assigned to a group may allow members of that group to access objects and perform operations that they are otherwise not allowed to do.

Learning outcome 1.4 formative assessment

1. Define Group Membership

   Answer.

   Group Membership allows you to specify Windows user groups to be dropped or added when a policy is applied. You add a group action to the policy contents and then specify whether or not the selected group is to be applied to the newly created policy or whether their membership is to be dropped.

2. What is Continuous monitoring

   Answer.

   Continuous monitoring is an approach where an organization constantly monitors its IT systems and networks to detect security threats, performance issues, or non-compliance problems in an automated manner. The goal is to identify potential problems and threats in real time to address them quickly.

3. What is Password complexity

   Answer.

   One method used to make passwords more secure is to require them to be complex and strong.

   A strong password is of sufficient length, doesn't include words found in a dictionary or any part of a user's name, and combines at least three of the four following character types:

   • Uppercase characters (26 letters A–Z)

   • Lowercase characters (26 letters a–z)

   • Numbers (10 numbers 0–9)

   • Special characters (32 printable characters, such as!, $, and *) A complex password uses multiple character types, such as Ab0@. However, a complex password isn't necessarily strong. It also needs to be sufficiently long.

Learning outcome 1.5: make recommendations to management to address security deficiencies

 **Duration: 4 hrs**		
1. Install and configure the security controls when performing account management based on best practices 2. Mitigate clearly the issues associated with multiple accounts/roles and/or shared account 3. Manage account credentials clearly.		
 **Resources**		
Equipment	**Tools**	**Materials**
Server Computer Firewall	Simulation Internet	Books Trainer manual

Router Switches		
Advance preparation: . Trainer should have all resources in place		

Indicative content 1.5.1: Installation and configuration of security controls when performing account management based on best practices.

- **Mitigate issues associated with users with multiple account/roles and/or shared accounts**

✓ Credential management

Group Policy

Windows domains use Group Policy to manage multiple users and computers in a domain. Group Policy allows an administrator to configure a setting once in a Group Policy Object (GPO) and apply this setting to many users and computers within the domain.

Active Directory Domain Services (AD DS) is a directory service Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Administrators implement domain Group Policy on domain controllers.

Password complexity

One method used to make passwords more secure is to require them to be complex and strong.

A strong password is of sufficient length, doesn't include words found in a dictionary or any part of a user's name, and combines at least three of the four following character types:

• Uppercase characters (26 letters A–Z)

• Lowercase characters (26 letters a–z)

• Numbers (10 numbers 0–9)

• Special characters (32 printable characters, such as!, $, and *) A complex password uses multiple character types, such as Ab0@. However, a complex password isn't necessarily strong. It also needs to be sufficiently long.

- **Expiration**

  In addition to using strong passwords, users should change their passwords regularly, such as every 45 or 90 days.

- **Recovery**

  It's not uncommon for users to occasionally forget their password. In many organizations, help desk professionals or other administrators reset user passwords. Before resetting the password, it's important to verify the user's identity.

- **Password History and Password Reuse**

  Many users would prefer to use the same password forever simply because it's easier to remember. Even when technical password policies force users to change their passwords, many users simply change them back to the original password. Unfortunately, this significantly weakens password security. A password history system remembers past passwords and prevents users from reusing passwords. It's common for password policy settings to remember the last 24 passwords and prevent users from reusing these until they've used 24 new passwords.

- **Password length**

  In fact, the National Institute of Standards and Technology (NIST) states, Password length has been found to be a primary factor in characterizing password strength. To strengthen the security of your online information, ensure your passwords are a random mix of at least 14 to 16 characters.

- **Generic account prohibition**

  A generic account is a computer account that **is not uniquely owned by an individual use**r. It might be used by a number of individuals who share the same password. Ideally, user accounts should be uniquely owned so that account activities can be attributed to a specific person (with a reasonable level of assurance).

  Generic Account use is prohibited on all non-Public Computers and wherever Information Security and Assurance compensating controls cannot be implemented. Generic Account requests may be granted based on justification and appropriate need.

✓ **Group based privileges**

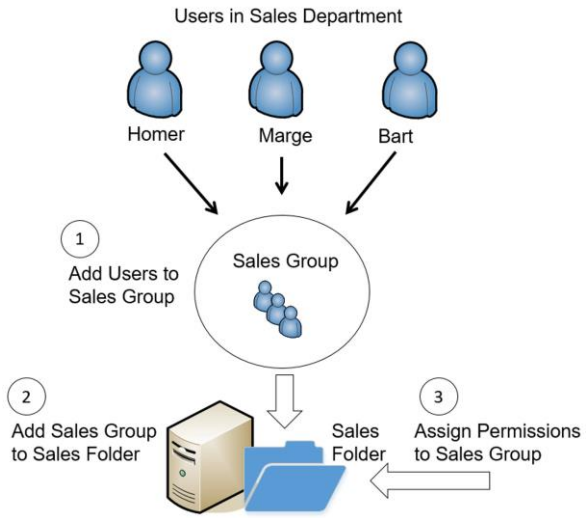


Figure 4. Group based privileges

The privileges assigned to a group may allow members of that group to access objects and perform operations that they are otherwise not allowed to do. In other words, privileges override the access rights settings.

If you select **User Manager** from the **Server Administration** tool, you will notice that the server configuration comes with some default groups: **All Users**, **Administrators**, **System Managers**, and **Security Administrators**. The default user named Administrator belongs to both the Administrators and the **Security Administrators** groups. By default, the **Administrators** group has all group privileges. Also by default, other groups have none of these privileges.

All members of a group have the same privileges on every project managed by this server configuration. The privileges apply to all levels equally: projects, views, folders, and items within folders. If users belong to more than one group, they have the maximum amount of privileges, regardless of which group provides them with those privileges.

✓ **User assigned privileges**

A privilege is the right of a user account to perform a particular system-related operation, such as shutting down the computer or changing the system time. You can use the Privilege Management feature to assign (enable) or deny (disable) privileges.

User privileges policies offer an alternative to using the default Elevate rule and can be customized to meet the needs of your organization.

Policies can range from making an individual user a member of a "Power User" group to removing user membership from the Administrators group.

When a User Privileges Policy is created, you can customize your policy using the following three tabs:

- **Group Membership** - Group Membership allows you to specify Windows user groups to be dropped or added when a policy is applied.

  You add a group action to the policy contents and then specify whether or not the selected group is to be applied to the newly created policy or whether their membership is to be dropped.

  When you assign membership to a user group, you will only add the group that you have selected, any nested groups will not be included. For example, if you assign group membership to Domain Administrators this will not automatically include the Local Administrator group and they will therefore need to be added separately.

- **Privileges** - A privilege is the right of a user account to perform a particular system-related operation, such as shutting down the computer or changing the system time. You can use the User Rights Management feature to enable, disable or remove privileges:

- No change - Leaves the privilege as it is with its original token.
- Enabled - Sets the flag in the token to enabled.
- Disabled - Sets the flag in the token to disabled.
- Remove - Removes the privilege from the token. You cannot undo this option.

- **Properties** - Add a description for the policy in the Properties tab. If required, you can force a custom admin token to use medium integrity, rather then defaulting to high integrity.

✓ **User access reviews**

User access reviews (sometimes referred to as “access certification” or “access recertification”) are a periodic audit of existing access rights in your organization meant to remove unnecessary or outdated permissions, which are a risk to both cybersecurity and compliance.

✓ Continuous monitoring

Continuous monitoring is an approach where an organization constantly monitors its IT systems and networks to detect security threats, performance issues, or non-compliance problems in an automated manner.

The goal is to identify potential problems and threats in real time to address them quickly.

However, not all businesses implement continuous monitoring or know how to implement it. Most companies use data to power their decision-making, but this is not necessarily continuous monitoring.

Continuous Monitoring Types

The scope of continuous monitoring involves three primary domains.

1. **The application layer of continuous monitoring measures application performance.** These applications can be custom-built by your business or third-party software. You will want to track metrics like transaction and errors per second, system uptime, and availability for application monitoring. Such tracking can help you quickly identify software bugs, performance bottlenecks, and overall user experience.
2. **Infrastructure monitoring is the next layer and covers the compute, storage, network, and other physical devices** found in traditional data centers or their virtual equivalents within cloud platforms. Monitoring this domain allows IT teams to troubleshoot performance issues, optimize usage, reduce cost, and forecast capacity needs.
3. **Network monitoring can help you understand the status of your firewalls, switches, routers, and other devices as the network evolves.**

You'll capture the source and destination IP addresses, ports, and protocol metadata of your network traffic and use those to find bandwidth utilization, packet losses, delays, and potential malicious intrusion attempts.

 **Theoretical learning Activity**

In pair, Discuss the different of managing credentials.

 Points to Remember (Take home message)

- One you want to manage the credentials, you have to deal with: Group Policy, Password complexity, Expiration, Recovery, Password History and Password Reuse, Password length and Generic account prohibition.
- A privilege is the right of a user account to perform a particular system-related operation, such as shutting down the computer or changing the system time.
- The privileges assigned to a group may allow members of that group to access objects and perform operations that they are otherwise not allowed to do.

Learning outcome 1.4 formative assessment

1. Define Group Membership

   Answer.

   Group Membership allows you to specify Windows user groups to be dropped or added when a policy is applied. You add a group action to the policy contents and then specify whether or not the selected group is to be applied to the newly created policy or whether their membership is to be dropped

2. What is Continuous monitoring

   Answer.

   Continuous monitoring is an approach where an organization constantly monitors its IT systems and networks to detect security threats, performance issues, or non-compliance problems in an automated manner. The goal is to identify potential problems and threats in real time to address them quickly.

3. What is Password complexity

   Answer.

   One method used to make passwords more secure is to require them to be complex and strong.

   A strong password is of sufficient length, doesn't include words found in a dictionary or any part of a user's name, and combines at least three of the four following character types:

   • Uppercase characters (26 letters A–Z)

   • Lowercase characters (26 letters a–z)

   • Numbers (10 numbers 0–9)

   • Special characters (32 printable characters, such as!, $, and *) A complex password uses multiple character types, such as Ab0@. However, a complex password isn't necessarily strong. It also needs to be sufficiently long.

Learning Unit 2: Implement and test countermeasures for identified vulnerabilities and threats

STRUCTURE OF LEARNING UNIT

Learning outcomes:

2.1. Establish required level of security
2.2. Apply best practice server and network hardening techniques and measures
2.3. Implement secure authentication and user account controls
2.4**.** Secure data integrity and transmission
2.5. Test and verify functionality and performance of security system

Learning outcome 2.1 Establish required level of security

Duration: 5 hrs
1. Explain physical security clearly 2. Integrate systems and data with third parties
Resources

Equipment	**Tools**	**Materials**
Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual

Advance preparation: . Trainer should have all resources in place . Trainer should have a related video to the session		

Indicative content 2.1.1: Implementation of compliance and operational security

- **Implementation of compliance and operational security**

<u>Compare and Contrast Physical Security and Environment Controls</u>

Physical security

Physical security is a prerequisite for overall security in the organizations. Hence, physical security controls should be implemented in the same manner as security controls are deployed for the IT infrastructure.

Physical security—A very important consideration for physical security is the use of physical access controls to manage and control entrance into an organization. A mantrap is a high-security barrier entrance device used to control entrance into a location. Besides, physical IDSs (intrusion detection systems), also known as burglar alarms, detect unauthorized activities and notify the security management.

Legal compliance

Legal compliance is the process by which a company adheres to the complex rules, policies and procedures that regulate business practices in a particular jurisdiction.

Compliance involves knowing and understanding the legislation that applies to the organization and demonstrating that the business and its entities are in compliance at all times.

Security awareness and training

Users must be aware of security to carry out their day-to-day tasks. Security training is essential for this purpose and should be part of all companies' security policies. The underlying techniques are used for awareness and training purposes.

User awareness—Each user must be aware of his/her company's security policy. The security management should play a crucial role in this regard. Security awareness can easily thwart social engineering attacks.

Security education—Security education is imparted to the users to guide them in how to perform their everyday tasks securely.

Compliance with laws, best practices, and standards—Compliance checking or compliance testing is a technique that ensures that all essential elements of security solutions are properly deployed. For an efficient security deployment, users must comply with laws, policies, guidelines, best practices, and standards.

Threat awareness—Threats are dynamic in nature and are being created every day. Users must do daily research about newly emerging threats, especially phishing attacks and viruses.

Social networking and peer-to-peer (P2P) services—Social networks and P2P (torrent) file sharing can be risky activities. Social networking is merely a waste of resources in the organization. Besides, the viruses can quickly be dispatched through P2P file sharing. Hence, P2P should be blocked altogether.

Integrate systems and data with third parties

Whenever systems and data are integrated with third parties, there is a huge risk of data loss, compromise, or leakage. Therefore, the security professionals must consider the security implications of integrating systems and data with third parties before implementation.

On-boarding/off-boarding—On-boarding is the process of hiring new employees. The identity and access management (IAM) is a system that holds members' records. The off-boarding process is the process of removing employers from IAM once they are terminated or retired.

Service-level agreement (SLA) and business partners agreement (BPA)—An SLA contract is an agreement between a customer and a supplier. On the other hand, a BPA contract is an agreement between two entities that determines their business relationship.

Memorandum of understanding (MOU)—An MOU is the nonbinding agreement between two parties outlining the details and terms of understanding, including the requirements and responsibilities of each party.

Theoretical learning Activity

In pair, Compare and Contrast Physical Security and Environment Controls.

Points to Remember (Take home message)

- Physical security is a prerequisite for overall security in the organization
- Legal compliance is the process by which a company adheres to the complex rules, …
- On-boarding/off-boarding—On-boarding is the process of hiring new employees.

Learning outcome 2.1 formative assessment

1. What is physical security

   Answer.

   Physical security is a prerequisite for overall security in the organizations.
2. Define User awareness.

   Answer.

   Each user must be aware of his/her company's security policy. The security management should play a crucial role in this regard.
3. How do you understand by Service-level agreement (SLA)?

   Answer.

   An SLA contract is an agreement between a customer and a supplier

Learning outcome 2.2 Apply best practice server and network hardening techniques and measures

Duration: 5 hrs

1. Configure security parameters on network devices and technology clearly
2. Implement network protocols and services
3. Apply the security in wireless network

Resources

Equipment	Tools	Materials
Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual

Advance preparation:

. Trainer should have all resources in place

. Trainer should b have knowledge about wireless network, security, network design element and components …

. Trainer should be sure that workplace is ready.

Indicative content 2.2.1: Implementation of network security

✓ **Standard Network Devices**

The security functions of standard network devices can be used to provide a degree of network security. These network devices can be classified based on their function in the OSI model. In 1978, the International Organization for Standardization (ISO) released a set of specifications that was intended to describe how dissimilar computers could be connected together on a network.

The key to the OSI reference model is layers. The model breaks networking steps down into a series of seven layers. Within each layer, different networking tasks are performed. In addition, each layer cooperates with the layers immediately above and below it.

The OSI model gives a visual representation of how a computer prepares data for transmission and how it receives data from the network, and illustrates how each layer provides specific services and shares with the layers above and below it.

Layer number	Layer name	Description	Function
7	Application	The top layer, application, provides the user interface to allow network services	Provides services for user applications
6	Presentation	The presentation layer is concerned with how the data is represented and formatted for the user.	Allow devices to establish and manage sessions
5	Session	This layer has the responsibility of permitting the two parties on the network to hold on going communication across the network.	Allows devices to establish and manage sessions
4	Transport	The transport layer is responsible for ensuring that error-free data is given to the user.	Provides connection establishment, management, and termination as well as acknowledgments and retransmissions.
3	Network	The network layer picks the route the packet is to take, and handles the addressing of the packets for delivery.	Makes logical addressing routing, fragmentation, and reassembly available.
2	Data link	The data link layer is responsible for dividing the data into frames. Some additional duties of the data link layer include error detection and correction(for example, if the data is not received properly, the data link layer would request that it be retransmitted).	Performs physical addressing, data framing, and error detection and handling
1	Physical	The job of this layer is to send the signal to the network or receive the signal from the network	Involved with encoding and signalling, and data transmission and reception.

Standard network devices can be classified by the OSI layer at which they function. These devices include switches, routers, load balancers, and proxies.

i. Switches

- Early local area networks (LANs) used a hub, which is a standard network device for connecting multiple network devices together so that they function as a single network segment.
- Hubs worked at the Physical Layer (Layer 1) of the OSI model. This means that they did not read any of the data passing through them and thus were ignorant of the source and destination of the frames.
- A hub would receive only incoming frames, regenerate the electrical signal, and then send all the frames received out to all other devices connected to the hub.
- Each device would then decide if the frame was intended for it (and retain it) or if it was intended for another device (and then ignore it).

Like a hub, a network switch is a device that connects network devices together. However, unlike a hub, a switch has a degree of "intelligence." Operating at the Data Link Layer (Layer 2), a switch can learn which device is connected to each of its ports, and then forward only frames intended for a specific device (unicast) or frames sent to all devices (broadcast).

Monitoring traffic on switches generally can be done in two ways. First, a managed switch on an Ethernet network that supports port mirroring allows the administrator to configure the switch to copy traffic that occurs on some or all ports to a designated monitoring port on the switch.

Port mirroring is illustrated in Figure, where the monitoring computer is connected to the mirror port and can view all network traffic (the monitoring computer can be a standalone device or a computer that runs protocol analyzer software). A second method for monitoring traffic is to install a network tap (test access point).

A network tap is a separate device that can be installed on the network. A network tap is illustrated in Figure below.

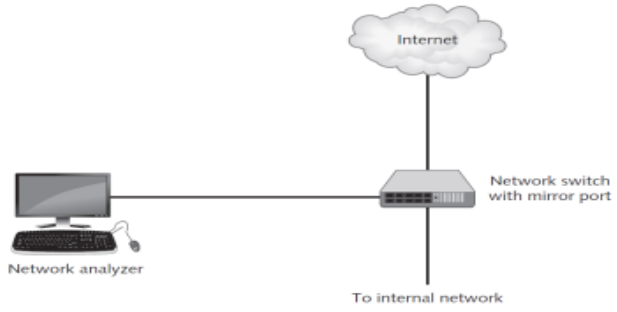


Figure 5. Port Mirroring

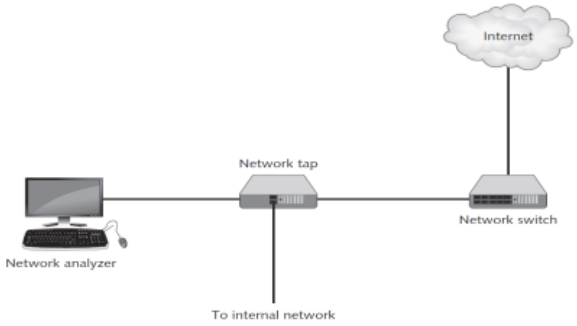


Figure 6. Network tap

A network tap is generally best for high-speed networks that have a large volume of traffic, while port mirroring is better for networks with light traffic.

Because a switch can still be used for capturing traffic, it is important that the necessary defenses be implemented to prevent unauthorized users from gathering this data. These attacks and defenses are summarized in Table below.

Type of attack	Description	Security defense
MAC flooding	An attacker can overflow the switch's address table with fake MAC addresses, forcing it to act like a hub, sending packets to all devices.	Use a switch that can close ports with too many MAC addresses.
MAC address impersonation	If two devices have the same MAC address, a switch may send frames to each device. An attacker can change the MAC address on her device to match the target device's MAC address.	Configure the switch so that only one port can be assigned per MAC address.
ARP poisoning	The attacker sends a forged ARP packet to the source device, substituting the attacker's computer MAC address.	Use an ARP detection appliance.
Port mirroring	An attacker connects his device to the switch's mirror port.	Secure the switch in a locked room.
Network tap	A network tap is connected to the network to intercept frames.	Keep network connections secure by restricting physical access.

Table 1. Protecting the Switch

Now, let's see the 6 key features offered by network switches.

1. Filtering: Here, switches prevent unauthorized users from viewing confidential information.

2. Port Mirroring or Mirroring: Here, switches enable a single port to be allocated as a mirror of other ports. In other words, the traffic to the target port is duplicated and sent to the mirroring port, and this can be used with packet analyzers for traffic monitoring.

3. Port Security: Switches utilize port security to ensure that only certain devices have access to the network, when plugged into the specified port. To do this, switches utilize the MAC addresses of devices. This is also termed as Physical Port Security.

4. Disabling Ports: Switches allow you to disable the unused physical ports on the switch. This prevents these ports from getting hijacked by a malicious person.

5. Creating Collision Domains: Switches enable you to create collision domains. This is important from a security perspective, because in segmented networks, data can collide. This was commonly observed with hubs. With a switch, each individual port creates a single collision domain that prevents actual collisions, since they are segmented into their own domain.

6. Virtual Local Area Networks or VLANs: Layer 3 managed switches can create VLANs, which is another form of network separation. These switches convert a separated network into multiple Virtual Local Area Networks, which divide data into their own networks over the switch. This data requires a router to pass information between VLANs. Also, VLANs provide network separation or segmentation through these switches

b) Router

Routers Operating at the Network Layer (Layer 3), a router is a network device that can forward packets across different computer networks.

When a router receives an incoming packet, it reads the destination address and then, using information in its routing table, sends the packet to the next network toward its destination. Routers also can perform a security function. The router can be configured to filter out specific types of network traffic. For example, a router can be set to disallow IP-directed broadcasts or incoming packets that have invalid addresses. Additionally, routers establish networks using logical addressing or IP addresses. In other words, routers note the IP addresses of the source and destination of data packets, and accordingly determine the best possible path. Because, the table stores local connections and destinations, a router knows the systems connected to it as well as the routing destination in case the destination is unknown.

c) Firewalls

In a network, a firewall is the main line of defense. Firewall exists as an appliance, which is installed as a main device separating two networks. Appliances are freestanding devices running in a self-contained way. They need less maintenance and support like a server-based component.

Firewalls help keeping networked computers safe and secure. This is achieved by examining data packets that reach the firewall, as well as checking whether the packet can pass through the firewall. Generally, you should set up firewall to block all traffic, which means no data packets can pass through. Then, you need to configure exceptions to the defined rule, so that the desired traffic can pass through the firewall. Let's take an example. If you want a Web server to be accessible through the Internet, deny all data packets except those from the TCP port 80, on which the server runs.

Packets can be filtered by a firewall in one of two ways. Stateless packet filtering looks at the incoming packet and permits or denies it based on the conditions that have been set by the administrator. Stateful packet filtering keeps a record of the state of a connection between an internal computer and an external device and then makes decisions based on the connection as well as the conditions.

d) A proxy server

Proxy server is a computer or an application program that intercepts user requests from the internal secure network and then processes that request on behalf of the user. When an internal client requests a service such as a file or a webpage from an external web server, it normally would connect directly with that remote server.

In a network using a proxy server, the client first connects to the proxy server, which checks its memory to see 40 if a previous request already has been fulfilled and whether a copy of that file or page is residing on the proxy server in its temporary storage area (cache). If it is not, the proxy server connects to the external web server using its own IP address (instead of the internal client's address) and requests the service. When the proxy server receives the requested item from the web server, the item is then forwarded to the client. Access to proxy servers is configured in a user's web browser.
An application-aware proxy is a special proxy server that "knows" the application protocols that it supports. For example, an FTP proxy server implements the protocol FTP.

Although proxy servers have some disadvantages, such as the added expense and the fact that caches may not always be current, they have several advantages:

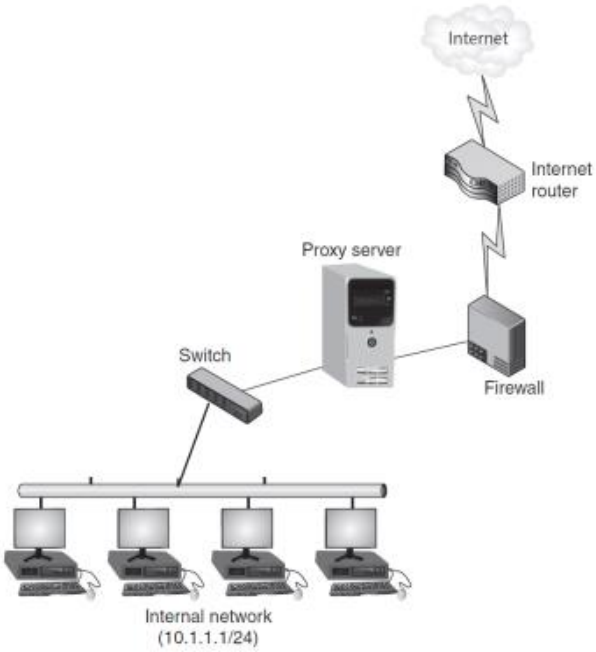


Figure 7. Proxy Server

- ✓ **Increased speed**. Because proxy servers can cache material, a request can be served from the cache instead of retrieving the webpage through the Internet.
- ✓ **Reduced costs**. A proxy server can reduce the amount of bandwidth usage because of the cache.
- ✓ **Improved management**. A proxy server can block specific webpages and/or entire websites. Some proxy servers can block entire categories of websites such as entertainment, pornography, or gaming sites.
- ✓ **Stronger security**. Acting as the intermediary, a proxy server can protect clients from malware by intercepting it before it reaches the client. In addition, a proxy server can hide the IP address of client systems inside the secure network.

Only the proxy server's IP address is used on the open Internet.

e) Load Balancer

Load balancing is a technology that can help to evenly distribute work across a network. Requests that are received can be allocated across multiple devices such as servers. To the user, this distribution is transparent and appears as if a single server is providing the resources. Load balancing technology provides these advantages:

- ✓ The probability of overloading a single server is reduced.
- ✓ Each networked computer can benefit from having optimized bandwidth.
- ✓ Network downtime can be reduced.

Load balancing can be performed either through software running on a computer or as a dedicated hardware device known as a load balancer. Load balancers are often grouped into two categories known as Layer 4 load balancers and Layer 7 load balancers. Layer 4 load balancers act upon data found in Network and Transport layer protocols such as Internet Protocol (IP), Transmission Control Protocol (TCP), File Transfer Protocol (FTP), and User Datagram Protocol (UDP). Layer 7 load balancers distribute requests based on data found in Application layer protocols such as HTTP. Although both Layer 4 and Layer 7 load balancers can distribute work based on a "round-robin" rotation to all devices equally or to those devices that have the least number of connections, Layer 7 load balancers also can use HTTP headers, cookies, or data within the application message itself to make a decision on distribution.

The use of a load balancer has security advantages. Because load balancers generally are located between routers and servers, they can detect and stop attacks directed at a server or application. A load balancer can be used to detect and prevent denial-of-service (DoS) and protocol attacks that could cripple a single server. Some load balancers can hide HTTP error pages or remove server identification headers from HTTP responses, denying attackers additional information about the internal network.

Network Security Hardware

Although standard networking devices can provide a degree of security, hardware devices that are specifically designed for security can give a much higher level of protection. These devices include network firewalls, spam filters, virtual private network concentrators, Internet content filters, web security gateways, intrusion detection and prevention systems, and Unified Threat Management appliances.

1. *Network Firewalls*

   Although a host-based application software firewall that runs as a program on one client is different from a hardware-based network firewall designed to protected an entire network, their functions are essentially the same: to inspect packets and either accept or deny entry
2. *Spam Filters*

   Beyond being annoying and disruptive, spam can pose a serious security risk. "Spammers" can distribute malware through their email messages as attachments and use spam for social engineering attacks. Due to the high volume of spam, most organizations use enterprise-wide spam filters to block spam before it ever reaches the client.
3. *Virtual Private Network (VPN) Concentrators*

   An unsecured public network should never be used for sensitive data transmissions. One solution could be to encrypt documents before transmitting them. However, there are drawbacks.

First, the user must consciously perform a separate action (such as encrypt a document) or use specific software (such as PGP) in order to transmit a secure document.

The time and effort required to do so, albeit small, may discourage users from protecting their documents. A second drawback is that these actions protect only documents that are transmitted; all other communications, such as accessing corporate databases, are not secure.

A more secure solution is to use a **virtual private network (VPN)**. **A virtual private network (VPN)** is a technology that enables authorized users to use an unsecured public network, such as the Internet, as if it were a secure private network. It does this by encrypting all data that is transmitted between the remote device and the network and not just specific documents or files. This ensures that any transmissions that are intercepted will be indecipherable. There are two common types of VPNs. A remote-access VPN or virtual private dial-up network (VPDN) is a user-to-LAN connection used by remote users. The second type is a site-to-site VPN, in which multiple sites can connect to other sites over the Internet.

4. **Internet Content Filters Internet content**

   Internet Content Filters Internet content filters monitor Internet traffic and block access to preselected websites and files. A requested webpage is displayed only if it complies with the specified filters. Unapproved websites can be restricted based on the Uniform Resource Locator or URL (URL filtering) or by searching for and matching keywords such as sex or hate (content inspection) as well as looking for malware (malware inspection).

5. **Web Security Gateways**

   Internet content filters monitor Internet traffic and block access to preselected websites and files. This makes them reactive security measures that only defend against known threats from known malicious sites. In contrast, a web security gateway can block malicious content in real time as it appears (without first knowing the URL of a dangerous site). Web security gateways enable a higher level of defense by examining the content through application-level filtering. For example, a web security gateway can block the following web-based traffic:

   - Adware and spyware
   - Cookies
   - Instant messengers
   - P2P (peer-to-peer) file sharing
   - Script exploits
   - TCP/IP malicious code attacks

6. **Protocol analyzers**

   In large organizations, a protocol analyzer can mean the difference between business as usual, and vital information walking out the door- and more importantly, being able to show evidence of how, when, and where the information started moving.

g) Unified Threat Management (UTM) Security Appliances

Because different types of network security hardware—firewalls, Internet content filters, web security gateways, etc.

Each provide a different defense, a network may require multiple devices for comprehensive protection. This can make it cumbersome to manage all of these devices.

An alternative is an integrated device that combines several security functions, called a Unified Threat Management (UTM) security product. Such multipurpose security appliances provide an array of security functions, such as:

- Antispam and antiphishing
- Antivirus and antispyware
- Bandwidth optimization
- Content filtering
- Encryption
- Firewall
- Instant messaging control
- Intrusion protection
- Web filtering

7. **NIDS and NIPS IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems)** both give information regarding what is going on in your network at a higher level than anti-virus and anti-malware can provide. This is critical in a situation where you may be dealing with custom malware that signature-based defenses have not dealt with before. If you can i subtle variations in user activity, or communications from servers that don't normally talk to each other- that very well could be the only warning you receive before your organization ends up on the 11 o'clock news. The large difference between the two is that IDS is purely passive listening, while IPS can perform some tasks on its own without user awareness. The two classes of IDS and IPS are based around looking at anom unusual activity compared to a baseline, or signature-based detection. Signature-based detection can be more accurate for what it sees, but that's as far as it goes.

- **Network design elements and components**

  Network design refers to planning a computer network infrastructure, and implementing security configuration parameters on network devices. Creating a network design requires a System Administrator to cover two key aspects:

  1. Thorough analysis to understand the components and protocols of the physical network, and

  2. Troubleshoot security issues related to wireless networking. Network technologies can also help to secure a network. Two such technologies are network address translation and network access control.

a) Network Address Translation (NAT)

Network address translation (NAT) is a technique that allows private IP addresses to be used on the public Internet. instead, they can be used by anyone on the private internal network. Private addresses function as regular IP addresses on an internal network; however, if a packet with a private address makes its way to the Internet, the routers drop that packet.

Class	Beginning address	Ending Address
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255

Table 2. Private IP address

NAT replaces a private IP address with a public IP address. As a packet leaves a network, NAT removes the private IP address from the sender's packet and replaces it with an alias IP public address. The NAT software maintains a table of the private IP addresses and alias public IP addresses. When a packet is returned to NAT, the process is reversed. A variation of NAT is port address translation (PAT). Instead of giving each outgoing packet a different IP address, each packet is given the same IP address but a different TCP port number. This allows a single public IP address to be used by several users.

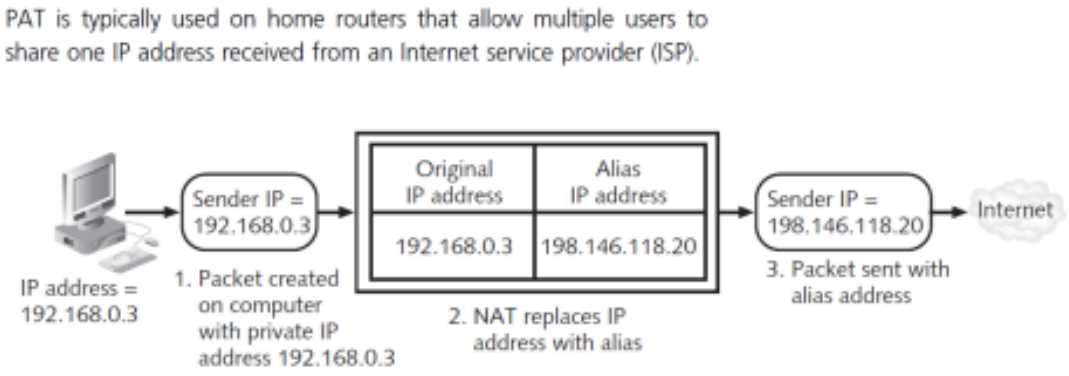


Figure 8. Network address translation

b) Network Access Control (NAC)

NAC examines the current state of a system or network device before it is allowed to connect to the network.

Any device that does not meet a specified set of criteria, such as having the most current antivirus signature or the software firewall properly enabled, is allowed to connect only to a "quarantine" network where the security deficiencies are corrected. After the problems are solved, the device is connected to the normal network. The goal of NAC is to prevent computers with suboptimal security from potentially infecting other computers through the network.

c) Demilitarized Zone (DMZ)

The DMZ is a place between the web and your internal network- where you can place outward pointing servers, but not have to open up your entire network. Imagine a bank that located its automated teller machine (ATM) in the middle of their vault. This would be an open invitation for disaster by inviting every outside user to enter the secure vault to access the ATM. Instead, the ATM and the vault should be separated so that the ATM is located in a public area that anyone can access, while the vault is restricted to trusted individuals.

In a similar fashion, locating public-facing servers such as web and email servers inside the secure network is also unwise. An attacker only has to break out of the security of the server to find herself inside the secure network.

In order to allow untrusted outside users, access to resources such as web servers, most networks employ a demilitarized zone (DMZ). The DMZ functions as a separate network that rests outside the secure network perimeter: untrusted outside users can access the DMZ but cannot enter the secure network.

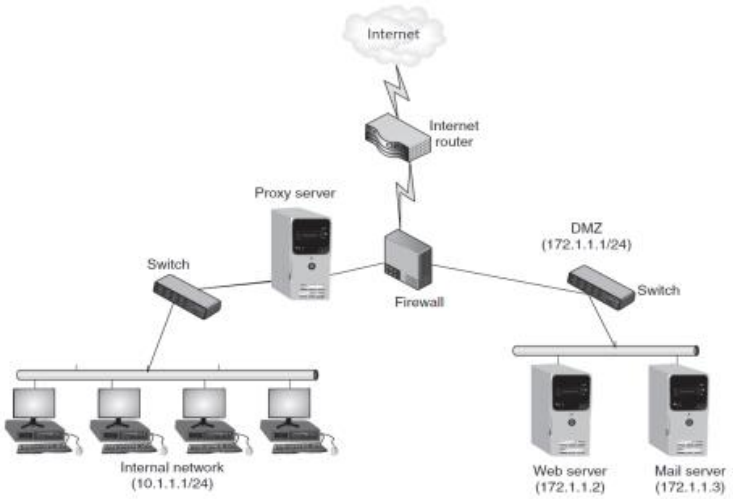


Figure 9. DMZ with One firewall

e) Subnetting

The TCP/IP protocol uses IP addresses, which are 32-bit (4-byte) addresses such as 192.146.118.20. IP addresses are actually two addresses: one part is a network address (such as 192.146.118) and one part is a host address (such as 20). This split between the network and host portions of the IP address originally was set on the boundaries between the bytes (called classful addressing).

Improved addressing techniques introduced in 1985 allowed an IP address to be split anywhere within its 32 bits.

This is known as subnetting or subnet addressing. Instead of just having networks and hosts, with subnetting, networks essentially can be divided into three parts: network, subnet, and host. Each network can contain several subnets, and each subnet connected through different routers can contain multiple hosts.

f) Virtual LANs (VLANs)

Networks are usually segmented by using switches to divide the network into a hierarchy. Core switches reside at the top of the hierarchy and carry traffic between switches, while workgroup switches are connected directly to the devices on the network.

g) Remote Access

Users who work away from the office have become commonplace today. These include telecommuters (who work occasionally or regularly from a home office), sales representatives who travel to meet distant customers, and workers who may be in another city at a conference or training.

Organizations typically provide avenues for these remote users to access corporate resources as if they were sitting at a desk in the office. It is important to maintain strong security for these remote communications because the transmissions are routed through networks or devices that the organization does not manage and secure.

h) Telephony

A term that most of the time it is used in the context of VoIP traffic and related technology, it can also sometimes be applied to anything that transmits voice.

i) Virtualization

The raw power that server systems are capable of now means that if you have physical boxes for every single separate process in a typical organization, not only would you have a lot of idle equipment most of the time, but an enormous extra expense for all of that added electricity and cooling. Virtualization allows that to be reduced by having fewer physical servers, but each one is capable of running many virtual machines- individual running instances of operating systems- at once

j) Cloud Computing

Taking the idea of virtualization a step further, Cloud Computing allows organizations with enormous amounts of processing power, storage space, and bandwidth to sell that to organizations that don't necessarily want the hassle of managing pieces of their infrastructure locally.

Indicative content 2.2.2: implementing networking protocols and services

Computer networks have protocols, or rules for communication. These protocols are essential for proper communication to take place between network devices. The most common protocol used today for both local area networks (LANs) and the Internet is Transmission Control Protocol/Internet Protocol (TCP/IP).

TCP/IP is not one single protocol; instead, it comprises several protocols that all function together (called a protocol suite). The two major protocols that make up its name, TCP and IP, are considered the most important protocols.
IP is the protocol that functions primarily at the Open Systems Interconnection (OSI) Network Layer (Layer 3) to provide addressing and routing.

TCP is the main Transport Layer (Layer 4) protocol that is responsible for establishing connections and the reliable data transport between devices.

TCP/IP uses its own four-layer architecture that includes Network Interface, Internet, Transport, and Application layers. This corresponds generally to the OSI reference model, as illustrated in Figure 8-1. The TCP/IP architecture gives a framework for the dozens of various protocols and several high-level applications that comprise the suite.

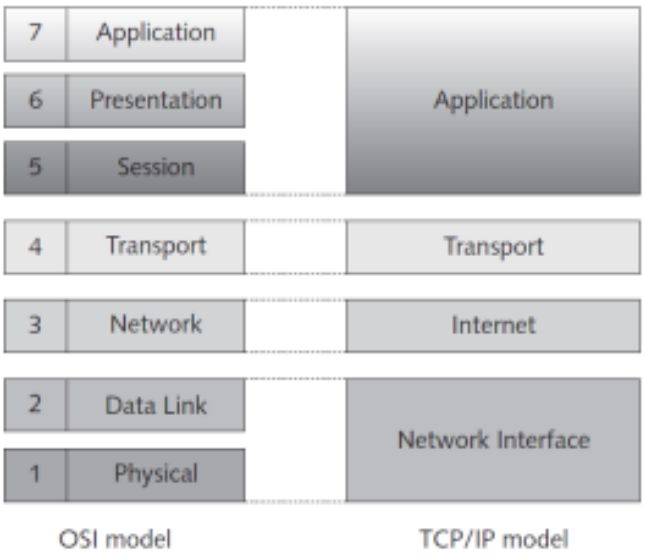


Figure 10. OSI model Vs TCP/IP Model

Several of the basic TCP/IP protocols that relate to security are Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), Domain Name System (DNS), file transfer and storage protocols, NetBIOS, and Telnet. In addition, a new and more secure version of IP is designed to replace the current version.

ii. Internet Control Message Protocol (ICMP)

Internet Control Message Protocol: a method to see if a remote device is responding.
The very popular ping command operates using ICMP packets to see if the targeted system is available. While Firewalls and even individual systems can choose to block ping, it is still a useful tool in the early stages of troubleshooting. ICMP operates on IP port 1.

- **Informational and query messages**. These messages are used for devices to exchange information and perform testing. They are generated either by an application or simply on a regular basis by devices to provide information to other devices.

- **Error messages.** ICMP error messages provide feedback to another device about an error that has occurred.

These messages can be sent as the result of basic errors (such as a requested service is not available or that a device cannot be reached) or more advanced 53 situations (such as a web security gateway does not have sufficient buffering capacity to forward a packet).

iii. Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is a popular protocol used to manage network equipment and is supported by most network equipment manufacturers. It allows network administrators to remotely monitor, manage, and configure devices on the network. SNMP functions by exchanging management.

information between networked devices. Depending on the version, SNMP can operate on ports 161 and 162 (SNMP v3), or ports 10161 and 10162 (Secure SNMP).

iv. Domain Name System (DNS)

The Domain Name System (DNS) is a TCP/IP protocol that resolves (maps) a symbolic name (www.cengage.com) with its corresponding IP address (69.32.133.11). The DNS database is organized as a hierarchy (tree). DNS normally uses UDP port 53.

v. File Transfer Protocols

Legacy method of transferring large files, this protocol operates over TCP port 21 (and sometimes 20) and broadcasts in the clear. The Internet was primarily a medium for transferring files from one device to another. Today transferring files is still considered an important task. Two TCP/IP protocols are used for transferring files. These are File Transfer Protocol (FTP) and Secure Copy Protocol (SCP).

- **SFTP**
  Modern method of transferring large files, this protocol operates over port 22 using an encrypted SSH tunnel to transfer files.
- **TFTP**

  Trivial File Transfer Protocol, this was primarily used for transferring files onto dedicated devices such as switches. Operating over UDP port 69, it has been superseded by SSH.

- **FTPS**
  File Transfer Protocol over SSL: an SSL variant of the popular FTP protocol. FTP is considered highly vulnerable without some form of protection, since it broadcasts its authentication and activity in clear text. Therefore, anyone listening on the wire can very easily use that data for their own purposes. FTPS operates over ports 989 and 990.

vi. **Secure Copy Protocol (SCP)**
Another protocol used for file transfers is Secure Copy Protocol (SCP). SCP is an enhanced version of Remote Copy Protocol (RCP).

SCP encrypts files and commands, yet has limitations. Secure Copy: a method of transferring files while staying within the protection of the SSH protocol. Traffic will remain within the created SSH connection on port 22.

vii. **IPSec**
Internet Protocol Security: one of the foundations of VPN tunneling. This allows data to be encrypted over an unsecured channel, such as the Web, and transmitted safely from end to end.

viii. **SSH**

Secure Shell: an encrypted method of remotely connecting to devices for administration and tunneling insecure protocols across the web. This operates over TCP port 22

ix. **TLS/SSL**

Transport Layer Security: the next generation of the Secure Socket Layer. Designed to prove that the computer on the other end of a connection is the one that it is supposed to be, TLS and SSL are commonly used to create encrypted connections from point to point. TLS and SSL protected traffic normally operates on ports that are different from their standard counterparts. For example: unprotected HTTP traffic operates on port 80, while protected HTTPS traffic operates on port 443.

1. **TCP/IP**
   Transmission Control Protocol and the Internet Protocol: the backbone of the modern network. TCP/IP is actually a suite of protocols, designed to work together to route traffic from source to destination.
2. **HTTPS**

   HyperText Transfer Protocol over SSL: an SSL variant of the incredibly popular HTTP protocol. HTTP is great for transmitting data that does not need to be protected, but if you are logging onto something like a banking website- you want to know for sure that nobody is going to be able to get your credentials and use them against you. HTTPS operates over port 443.

3. **IPv4**

   Legacy IP addresses in the 123.456.789.000 format with an estimated maximum number of public IP addresses of 4.3 billion. This sounds like a lot until you start to think about how many networked devices the average person has associated with themselves at any given time. l) IPv6 New-type IP scheme, presented in the 1111:2222:3333:4444:5555:6666:7777:AAAA format.

   Unlike IPv4, this addressing scheme is in Hexadecimal. Combined with the larger addressing style, this potentially can have up to 3.4 x 10^38 addresses.

   m) iSCSI

   Internet Small Computer System Interface, a protocol used for Storage Area Networks to fool servers into thinking they have very large local hard disks. iSCSI usually uses TCP ports 80 and 3260.

   n) FCoE

   Fiber Channel over Ethernet, allows the Fiber Channel Protocol to be used over standard network connections.

   o) TELNET

   Telnet is a program normally used for testing connections and remote administration. Operating by default on port 23, this has been primarily replaced by SSH.

   p) NetBIOS

   Network Basic Input Output System, it was a precursor to DNS. The primary way that users interact with it today is its naming convention, which must be 15 characters or less. NetBIOS operates on ports 137, 138 and 139.

q) RDP

(Remote Desktop Protocol) port 3389 Remote Desktop Protocol (RDP) is a Microsoft protocol designed to facilitate application data transfer security and encryption between client users, devices and a virtual network server

Storage Protocols The amount of data that is being stored has grown almost beyond imagination. Whereas at one time a single terabyte of storage was considered massive, today that is no longer the case Most organizations have turned to using a storage area network (SAN), which is a dedicated network storage facility that provides access to data storage over a high-speed network. SANs consolidate different storage facilities—disk arrays, tape libraries, and even "optical jukeboxes" that can load thousands of discs by robotic arms—so they are accessible to servers.

NetBIOS NetBIOS (Network Basic Input/Output System) is a transport protocol used by Microsoft Windows systems to allow applications on separate computers to communicate over a LAN. In modern networks NetBIOS normally runs over TCP/IP through the NetBIOS over TCP/IP (NBT) protocol.

This results in each computer in the network having both an IP address plus a NetBIOS name.

IPv6

The current version of the IP protocol is version 4 and is called IPv4. Developed in 1981, long before the Internet was universally popular, IPv4 has several weaknesses. One of the weaknesses is the number of available IP addresses. An IP address is 32 bits in length, providing about 4.3 billion possible IP address combinations. This no longer is sufficient for the number of devices that are being connected to the Internet. Another weakness is that of security. Due to its structure, IPv4 can be subject to several types of attacks.

Indicative content 2.2.3: Application of secure network administration principals

a) Rule-based management

A person or group is granted access to what they need to perform their tasks and nothing more. This is done to protect both the organization and the user. Administering a network can be a difficult task; administering a secure network can be even more challenging.

It is important that network security administration follow a rule-based management approach, which is the process of administration that relies on following procedural and technical rules, instead of creating security elements "on the fly." There are different types of rules. Procedural rules may be defined as the authoritative and prescribed direction for conduct. The procedural rules in turn, dictate technical rules. Technical rules may involve configuring a firewall or proxy server to conform to the procedural rules. It is the role of the network administrator to follow a rule-based management approach. This typically involves following rules that address device security, monitoring and analyzing logs, network design management, and port security.

b) Firewall rules

Firewalls have two types of rules: Explicit and Implicit. Explicit is laid out expressly to allow or deny access to a particular resource- for example, if you wanted to allow access to amazon.com to a particular ip range in your network. Implicit is a generic rule that is either inherited via other means, or are final 'catch-all' rules- for example, after all other rules are applied, you have a 'deny all' to block everything that doesn't need access.

c) Device Security

Because new devices are continually added to the network, securing devices is a never-ending task yet is key in maintaining a network's security.

Device security includes establishing a secure router configuration and implementing flood guards.

Secure Router Configuration

Default settings on a router are extremely dangerous- potentially allowing access from anywhere on the planet. Either locking down the router so that it can be accessed only locally or through a console port can be a great start.

Task	Explanation
Create a network design	Prior to any configuration, a network diagram that illustrates the router interfaces should be created. This diagram should reflect both the LAN and wide area network (WAN) interfaces.
Use a meaningful router name	Because the name of the router appears in the command line during router configuration, it helps ensure that commands are given to the correct router. For example, if the name *Internet_Router* is assigned to the device, the displayed command prompt would be *Internet_Router (config)#*.
Secure all ports	All ports to the router should be secured. This includes both physical ports (sometimes called the *console port* and *auxiliary port*) and inbound ports from remote locations (sometimes known as *VTY* for *virtual teletype*).
Set a strong administrator password	Most routers allow a user to access the command line in *user mode*, yet an administrator password is required to move to *privileged mode* for issuing configuration commands.
Make changes from the console	The configuration of the router should be performed from the console and not a remote location. This configuration can then be stored on a secure network drive as a backup and not on a laptop or USB flash drive.

Table 3.Basic secure router configuration.

Flood Guard

A basic defense against DDoS attacks, **flood guards** attempt to prevent traffic that could potentially overwhelm the network. Please note however that to be effective, this needs to be adjusted manually to meet the needs of your network- it doesn't come out of the box with automatic settings.

One defense against DoS and DDoS SYN flood attacks is to use a **flood guard**. A flood guard is a feature that controls a device's tolerance for unanswered service requests and helps to prevent a DoS attack. Flood guards are commonly found on firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

d) Monitoring and Analyzing Logs

A log is a record of events that occur. Security logs are particularly important because they can reveal the types of attacks that are being directed at the network and if any of the attacks were successful.

A security access log can provide details regarding requests for specific files on a system while an audit log is used to record which user performed an action and what that action was. System event logs document any unsuccessful events and the most significant successful 60 events (some system event logs can be tailored to specify the types of events that are recorded). The types of information that can be recorded might include the date and time of the event, a description of the event, its status, error codes, service name, and user or system that was responsible for launching the event.

- **Network Design Management**

In addition to device security and monitoring and analyzing logs, several network design management principles should be followed to ensure that security and the viability of the network are maintained. Network separation to prevent bridging, loop protection, and VLAN management are three principles that should be considered.

a) Network Separation

One of the important rules of network design is to separate secure parts of the network from unsecure parts.

That is, the part of the network that contains customer credit card information should not be accessible from the part of the network that manages heating and cooling systems. One way to provide network separation is to physically separate users by connecting them to different switches and routers. This prevents bridging and even prevents a reconfigured device from allowing that connection to occur.

b) Loop Protection

In Figure 11, Host Z, which is connected to Switch A, wants to send frames to Host X on Segment 2. Because Switch A does not know where Host X is located, it "floods" the network with the packet. The packet then travels down Segment 1 to Switch B and Segment 2 to Switch C. Switch B then adds Host Z to its lookup table that it maintains for Segment 1, and Switch C also adds it to its lookup table for Segment 3. Yet if Switch B or C has not yet learned the address for Host Z, they will both flood Segment 2 looking for Host X; that is, each switch will take the packet sent by the other switch and flood it back out again because they still do not know where Host X is located. Switch A then will receive the packet from each segment and flood it back out on the other segment. This switching loop causes a broadcast storm as the frames are broadcast, received, and rebroadcast by each switch. Broadcast storms can cripple a network in a matter of seconds to the point that no legitimate traffic can occur.

Broadcast storms can be prevented with loop protection, which uses the IEEE 802.1d standard spanning-tree algorithm (STA).

STA can determine that a switch has multiple ways to communicate with a host and then determine the best path while blocking out other paths.

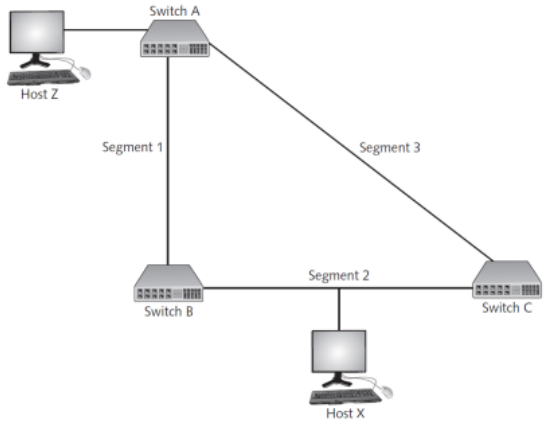


Figure 11. Broadcast storm

Although STA determines the best path, it also registers the other paths in the event that the primary path is unavailable.

c) VLAN Management

It is possible to segment a network by physical devices grouped into logical units through a virtual LAN (VLAN).

This allows scattered users to be logically grouped together even though they may be attached to different switches, thus reducing network traffic and providing a degree of security.

Some general principles for managing VLANs are:

- Configure empty switch ports to connect to an unused VLAN.
- Change any default VLAN names.
- Configure the ports on the switch that pass tagged VLAN packets to explicitly forward specific tags.
- Configure VLANs so that public devices, such as a web application server, are not on a private VLAN, forcing users to have access to that VLAN.

e) Port Security

Securing physical ports is an important step in network management. Ports can be secured through disabling unused interfaces, using MAC limiting and filtering, and through IEEE802.1x.

i. Disabling Unused Interfaces

Disabling unused interfaces is a security technique to turn off ports on a network device that are not required, such as a switch. This is an important security step that is often overlooked. A switch or router without port security allows attackers to connect to unused ports to access the network. It is important that all interfaces be secured before a router or switch is deployed. The network administrator should navigate to each unused interface and issue the appropriate shutdown command.

ii. MAC Limiting and Filtering In addition to disabling unused interfaces, another step in port security is MAC limiting and filtering. This will filter and limit the number of media access control (MAC) addresses allowed on a single port. A port can be set to a limit of only 1 and a specific MAC address can be assigned to that port. This enables only a single authorized host to connect through that port; attempts to access the interface by a host not listed will result in a security violation.

iii. IEEE 802.1x The IEEE 802.1x standard provides the highest degree of port security by implementing port-based authentication. This protocol authenticates users on a per switch port basis by permitting access to valid users but effectively disabling the port if authentication fails. This prevents an unauthenticated device from receiving any network traffic until its identity can be verified. It also strictly limits access to the device that provides the authentication to prevent attackers from reaching it.

Indicative content 2.2.4: Application of secure wireless network

As a result of the wireless security vulnerabilities in IEEE and Wi-Fi Alliance technologies, both organizations worked to create comprehensive security solutions. The results from the IEEE, known as 802.11i, served as the foundation for the Wi-Fi Alliance's Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA and WPA2 are the primary wireless security solutions today. In addition, there are other security steps that can be taken.

a) Wi-Fi Protected Access (WPA) As the IEEE worked on the 802.11i standard, the Wi-Fi Alliance grew impatient and decided that wireless security could no longer wait. In October 2003 it introduced its own Wi-Fi Protected Access (WPA).

b) Temporal Key Integrity Protocol (TKIP) Encryption The heart and soul of WPA is a newer encryption technology called Temporal Key Integrity Protocol (TKIP). TKIP functions as a "wrapper" around WEP by adding an additional layer of security but still preserving WEP's basic functionality.

TKIP's enhancements are in three basic areas: the required key length is increased from 64 bits to 128 bits (making it harder to break), the IV is increased from 24 bits to 48 bits (effectively eliminating collisions), and a unique "base key" is created for each wireless device using a master key derived in the authentication process along with the sender's unique MAC address (this key is used with the IV to create unique keys for each packet).

c) Preshared Key (PSK) Authentication

Authentication for WPA Personal is accomplished by using a preshared key (PSK). In cryptography, a PSK is a value that has been previously shared using a secure communication channel between two parties. In a WLAN, a PSK is slightly different. It is a secret value that is manually entered on both the AP and each wireless device, making it essentially identical to the "shared secret" used in WEP. Because this secret key is not widely known, it may be assumed that only approved devices have the key value. Devices that have the secret key are then automatically authenticated by the AP. Although using PSK has several weaknesses—the key must be kept secret, it can be difficult to manage multiple devices, the key itself may be weak, keys must be entered manually—the alternative requires a significant investment in hardware and software.

Authentication for enterprises should use the higher-level authentication process, but for home users, PSK is the option of choice.

WPA Vulnerabilities Although an improvement over WEP, WPA nevertheless has weaknesses. One of the design goals of WPA was to fit into the existing WEP engine without requiring extensive hardware upgrades or replacements.

d) Wi-Fi Protected Access 2 (WPA2)

In March 2001 the IEEE started work on addressing wireless security. This work was based on new wireless security mechanisms as opposed to transitional solutions such as WPA.

e) AES-CCMP Encryption

The WPA2 standard addresses encryption by using the Advanced Encryption Standard (AES) block cipher. AES performs three steps on every block (128 bits) of plaintext.

The encryption protocol used for WPA2 is the **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)** and specifies the use of CCM (a general-purpose cipher mode algorithm providing data privacy) with AES. The Cipher Block Chaining **Message Authentication Code (CBC-MAC)** component of CCMP provides data integrity and authentication.

IEEE 802.1x Authentication

Authentication for the WPA2 Enterprise model uses the IEEE 802.1x standard. This standard, originally developed for wired networks, provides a greater degree of security by implementing port-based authentication. IEEE 802.1x blocks all traffic on a port-byport basis until the client is authenticated using credentials stored on an authentication server. This prevents an unauthenticated device from receiving any network traffic until its identity can be verified. It also strictly limits access to the device that provides the authentication to prevent attackers from reaching it.

Additional Wireless Security Protections Other security steps can be taken to protect a wireless network. These include captive portal APs, rogue AP discovery tools, power level controls, antennas, and site surveys. Captive Portal APs A home user who installs a WLAN can simply launch a web browser to give immediate and unlimited access to the Internet.

Rogue AP Discovery Tools The problem of rogue APs is of increasing concern to organizations. Several methods can be used to detect a rogue AP by continuously monitoring the RF airspace.

The WLAN management system can instruct the switch to disable the port to which the rogue AP is connected, thus severing its connection to the wired network.

Power Level Controls Another security feature on some APs is the ability to adjust the level of power at which the WLAN transmits. On devices with that feature, the power can be adjusted so that less of the signal leaves the premises and reaches outsiders.

Antennas APs use antennas that radiate out a signal in all directions. Because these devices are generally positioned to provide the broadest area of coverage, APs should be located near the middle of the coverage area. Generally, the AP can be secured to the ceiling or high on a wall.

Site Surveys Ensuring that a wireless LAN can provide its intended functionality and meet its required design goals can best be achieved through a site survey. A site survey is an in-depth examination and analysis of a wireless LAN site.

Theoretical learning Activity

In pair, discuss about network design elements and components.

Points to Remember (Take home message)

- Standard network devices can be classified by the OSI layer at which they function. These devices include switches, routers, load balancers, and proxies.
- The key to the OSI reference model is layers
- Networks devices are: Switch, router, firewall, access point, hub, bridge…
- the 6 key features offered by network switches: **Filtering, Port Mirroring or Mirroring, Port Security, Disabling Ports, Creating Collision Domains, Virtual Local Area Networks or VLANs.**
- Proxy server is a computer or an application program that intercepts user requests from the internal secure network and then processes that request on behalf of the user.
- Computer networks have protocols, or rules for communication
- **Storage Protocols** The amount of data that is being stored has grown almost beyond imagination.
- A log is a record of events that occur.
- Broadcast storms can be prevented with loop protection, which uses the IEEE 802.1d standard spanning-tree algorithm (STA).
- Authentication for the WPA2 Enterprise model uses the IEEE 802.1x standard.

Learning outcome 2.2 formative assessment

1. Differentiate VLAN from subnetting

   Answer.

   There are differences between subnetting and VLANs. Subnets are subdivisions of IP address classes (Class A, B, or C) and allow a single Class A, B, or C network to be used instead of multiple networks.

   VLANs are devices that are connected logically rather than physically, either through the port they are connected to or by their media access control (MAC) address.
2. How do you understand by Network design?

   Answer.

   Network design refers to planning a computer network infrastructure, and implementing security configuration parameters on network devices.
3. What is Network Address Translation (NAT)

   Answer.

   Network address translation (NAT) is a technique that allows private IP addresses to be used on the public Internet.
4. Define **Cloud Computing**

   Answer.
5. How does a virtual LAN (VLAN) allow devices to be grouped?

   a. based on subnets

   b. logically

   c. directly to hubs

   d. only around core switches

   6. Which device is easiest for an attacker to take advantage of in order to capture and analyze packets?

   a. hub

   b. switch

   c. router

   d. load balancer

7. what is Domain Name System (DNS)

Answer.

The Domain Name System (DNS) is a TCP/IP protocol that resolves (maps) a symbolic name (www.cengage.com) with its corresponding IP address (69.32.133.11).

8. Explain **TLS/SSL?**

Answer.

Transport Layer Security: the next generation of the Secure Socket Layer. Designed to prove that the computer on the other end of a connection is the one that it is supposed to be, TLS and SSL are commonly used to create encrypted connections from point to point.

Learning outcome 2.3 Implement secure authentication and user account controls

Duration: 4 hrs

1. Understand User account control and Authentication clearly
2. Create an account and configure user account control

Resources

Equipment	Tools	Materials
Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual

Advance preparation:

. Trainer should have all resources in place

Indicative content 2.3.1: Creation of an account

✓ **Understand user account control and authentication**

What is User Account Control (UAC) in Windows?

User Account Control or UAC for short is a security feature of Windows which helps prevent unauthorized changes to the operating system. User Account Control makes sure certain changes are made only with approval from the administrator.

<u>There are four UAC settings that you can choose from:</u>

1. Always notify Select this setting if you:
   o Always want to be notified when programs try to install software or make changes to your computer
   o Make changes to Windows settings.

2. Notify me only when programs try to make changes to my computer Select this setting if you:
   o Want to be notified only when programs try to make changes to your computer.
   o Don't want to be notified when you make changes to Windows settings.
3. Notify me only when programs try to make changes to my computer (do not dim my desktop) Select this setting if you:
   o Want to be notified only when programs try to make changes to your computer without the desktop being dimmed.
   o Don't want to be notified when you make changes to Windows settings.
4. Never notify (Disable UAC)
   Select this setting if you:
   o Never want to be notified when programs try to install software or make changes to your computer.
   o Never want to be notified when you make changes to Windows settings

Theoretical learning Activity

1. In pair, Discuss about User account control (UAC) in Windows?

Points to Remember (Take home message)

- User Account Control or UAC for short is a security feature of Windows which helps prevent unauthorized changes to the operating system. User Account Control makes sure certain changes are made only with approval from the administrator.

Learning outcome 2.3 formative assessment

1. Define User account control (UAC) In windows

   Answer.

   User Account Control or UAC for short is a security feature of Windows which helps prevent unauthorized changes to the operating system.
2. List four UAC settings that you can choose from:

   Answer.

   - Always notify
   - Notify me only when programs try to make changes to my computer
   - Notify me only when programs try to make changes to my computer (do not dim my desktop)
   - Never notify

Learning Outcome 2.4: Secure data integrity and transmission

Duration: 4 hrs

1. Configure security parameters on network devices and technology clearly
2. Implement network protocols and services
3. Apply the security in wireless network

Resources

Equipment	Tools	Materials
Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual

Advance preparation:

. Trainer should have all resources in place

. Trainer should be having the knowledge about wireless network, security, network design element and components …

Indicative content 2.4.1: Implementation of network security

✓ **Standard Network Devices**

The security functions of standard network devices can be used to provide a degree of network security. These network devices can be classified based on their function in the OSI model.

In 1978, the International Organization for Standardization (ISO) released a set of specifications that was intended to describe how dissimilar computers could be connected together on a network.

The key to the OSI reference model is layers. The model breaks networking steps down into a series of seven layers. Within each layer, different networking tasks are performed. In addition, each layer cooperates with the layers immediately above and below it. The OSI model gives a visual representation of how a computer prepares data for transmission and how it receives data from the network, and illustrates how each layer provides specific services and shares with the layers above and below it.

Layer number	Layer name	Description	Function
7	Application	The top layer, application, provides the user interface to allow network services	Provides services for user applications
6	Presentation	The presentation layer is concerned with how the data is represented and formatted for the user.	Allow devices to establish and manage sessions
5	Session	This layer has the responsibility of permitting the two parties on the network to hold on going communication across the network.	Allows devices to establish and manage sessions
4	Transport	The transport layer is responsible for ensuring that error-free data is given to the user.	Provides connection establishment, management, and termination as well as acknowledgments and retransmissions.
3	Network	The network layer picks the route the packet is to take, and handles the addressing of the packets for delivery.	Makes logical addressing routing, fragmentation, and reassembly available.
2	Data link	The data link layer is responsible for dividing the data into frames. Some additional duties of the data link layer include error detection and correction(for example, if the data is not received properly, the data link layer would request that it be retransmitted).	Performs physical addressing, data framing, and error detection and handling
1	Physical	The job of this layer is to send the signal to the network or receive the signal from the network	Involved with encoding and signalling, and data transmission and reception.

Table 4. OSI 7 layers' reference model

Standard network devices can be classified by the OSI layer at which they function. These devices include switches, routers, load balancers, and proxies.

x. Switches

- Early local area networks (LANs) used a hub, which is a standard network device for connecting multiple network devices together so that they function as a single network segment.
- Hubs worked at the Physical Layer (Layer 1) of the OSI model. This means that they did not read any of the data passing through them and thus were ignorant of the source and destination of the frames.

Monitoring traffic on switches generally can be done in two ways. First, a managed switch on an Ethernet network that supports port mirroring allows the administrator to configure the switch to copy traffic that occurs on some or all ports to a designated monitoring port on the switch.

A network tap is a separate device that can be installed on the network. A network tap is illustrated in Figure below.

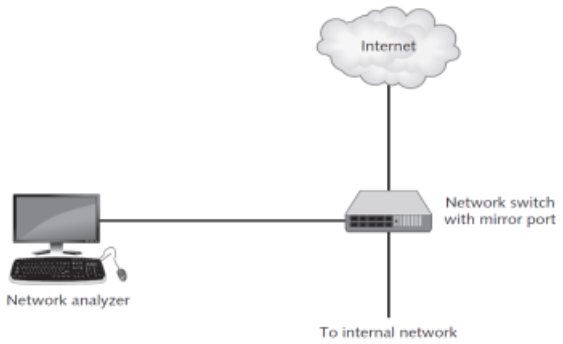


Figure 12. Port Mirroring

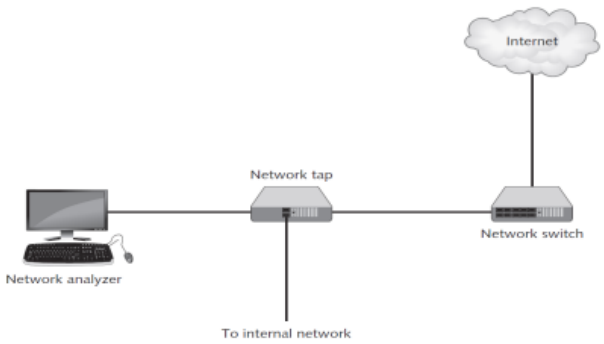


Figure 13. Network tap

A network tap is generally best for high-speed networks that have a large volume of traffic, while port mirroring is better for networks with light traffic.

Because a switch can still be used for capturing traffic, it is important that the necessary defenses be implemented to prevent unauthorized users from gathering this data. These attacks and defenses are summarized in Table below.

Type of attack	Description	Security defense
MAC flooding	An attacker can overflow the switch's address table with fake MAC addresses, forcing it to act like a hub, sending packets to all devices.	Use a switch that can close ports with too many MAC addresses.
MAC address impersonation	If two devices have the same MAC address, a switch may send frames to each device. An attacker can change the MAC address on her device to match the target device's MAC address.	Configure the switch so that only one port can be assigned per MAC address.
ARP poisoning	The attacker sends a forged ARP packet to the source device, substituting the attacker's computer MAC address.	Use an ARP detection appliance.
Port mirroring	An attacker connects his device to the switch's mirror port.	Secure the switch in a locked room.
Network tap	A network tap is connected to the network to intercept frames.	Keep network connections secure by restricting physical access.

Table 5. Protecting the Switch

These are six (6) key features offered by network switches: **Filtering, Port Mirroring or Mirroring, Port Security, Disabling Ports, Creating Collision Domains, Virtual Local Area Networks or VLANs**

b) Router

Routers Operating at the Network Layer (Layer 3), a router is a network device that can forward packets across different computer networks. When a router receives an incoming packet, it reads the destination address and then, using information in its routing table, sends the packet to the next network toward its destination. Routers also can perform a security function.

c) Firewalls

In a network, a firewall is the main line of defense. Firewall exists as an appliance, which is installed as a main device separating two networks.

k) A proxy server

Proxy server is a computer or an application program that intercepts user requests from the internal secure network and then processes that request on behalf of the user. Several advantages: **Increased speed**, **Reduced costs**, **Improved management**, **Stronger security, etc**.

e) Load Balancer

Load balancing is a technology that can help to evenly distribute work across a network. Requests that are received can be allocated across multiple devices such as servers. To the user, this distribution is transparent and appears as if a single server is providing the resources.

Network Security Hardware

Although standard networking devices can provide a degree of security, hardware devices that are specifically designed for security can give a much higher level of protection.

These devices include network firewalls, spam filters, virtual private network concentrators, Internet content filters, web security gateways, intrusion detection and prevention systems, and Unified Threat Management appliances.

1. *Network Firewalls*

   Although a host-based application software firewall that runs as a program on one client is different from a hardware-based network firewall designed to protected an entire network, their functions are essentially the same: to inspect packets and either accept or deny entry

2. *Spam Filters:* Beyond being annoying and disruptive, spam can pose a serious security risk.
3. *Virtual Private Network (VPN) Concentrators:* An unsecured public network should never be used for sensitive data transmissions.

g) Unified Threat Management (UTM) Security Appliances

Because different types of network security hardware—firewalls, Internet content filters, web security gateways, etc

- **Network design elements and components**

Network design refers to planning a computer network infrastructure, and implementing security configuration parameters on network devices. Creating a network design requires a System Administrator to cover two key aspects:

1. Thorough analysis to understand the components and protocols of the physical network, and

2. Troubleshoot security issues related to wireless networking. Network technologies can also help to secure a network.

Two such technologies are network address translation and network access control.

a) Network Address Translation (NAT)

Network address translation (NAT) is a technique that allows private IP addresses to be used on the public Internet.

b) Network Access Control (NAC)

NAC examines the current state of a system or network device before it is allowed to connect to the network.

c) Demilitarized Zone (DMZ)

The DMZ is a place between the web and your internal network- where you can place outward pointing servers, but not have to open up your entire network.

l) Subnetting

Subnetting is a process of breaking down big network into smaller networks.

m) Virtual LANs (VLANs)

Networks are usually segmented by using switches to divide the network into a hierarchy.

n) Remote Access

Users who work away from the office have become commonplace today. These include telecommuters (who work occasionally or regularly from a home office), sales representatives who travel to meet distant customers, and workers who may be in another city at a conference or training. Organizations typically provide avenues for these remote users to access corporate resources as if they were sitting at a desk in the office. It is important to maintain strong security for these remote communications because the transmissions are routed through networks or devices that the organization does not manage and secure.

o) Telephony

A term that most of the time it is used in the context of VoIP traffic and related technology, it can also sometimes be applied to anything that transmits voice.

p) Virtualization

The raw power that server systems are capable of now means that if you have physical boxes for every single separate process in a typical organization, not only would you have a lot of idle equipment most of the time, but an enormous extra expense for all of that added electricity and cooling.

q) Cloud Computing

Taking the idea of virtualization a step further, Cloud Computing allows organizations with enormous amounts of processing power, storage space, and bandwidth to sell that to organizations that don't necessarily want the hassle of managing pieces of their infrastructure locally.

Indicative content 2.4.2: implementing networking protocols and services

Computer networks have protocols, or rules for communication. These protocols are essential for proper communication to take place between network devices. The most common protocol used today for both local area networks (LANs) and the Internet is Transmission Control Protocol/Internet Protocol (TCP/IP).

TCP/IP is not one single protocol; instead, it comprises several protocols that all function together (called a protocol suite). The two major protocols that make up its name, TCP and IP, are considered the most important protocols. IP is the protocol that functions primarily at the Open Systems Interconnection (OSI) Network Layer (Layer 3) to provide addressing and routing. TCP is the main Transport Layer (Layer 4) protocol that is responsible for establishing connections and the reliable data transport between devices.

TCP/IP uses its own four-layer architecture that includes Network Interface, Internet, Transport, and Application layers. This corresponds generally to the OSI reference model, as illustrated in Figure 8-1. The TCP/IP architecture gives a framework for the dozens of various protocols and several high-level applications that comprise the suite.

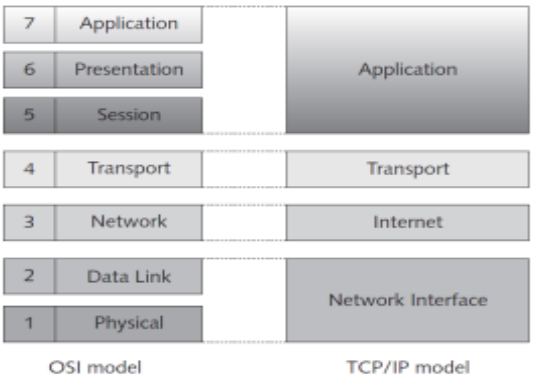


Figure 14. OSI model Vs TCP/IP Model

Several of the basic TCP/IP protocols that relate to security are Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), Domain Name System (DNS), file transfer and storage protocols, NetBIOS, and Telnet. In addition, a new and more secure version of IP is designed to replace the current version.

i. Internet Control Message Protocol (ICMP)

Internet Control Message Protocol: a method to see if a remote device is responding. The very popular ping command operates using ICMP packets to see if the targeted system is available. While Firewalls and even individual systems can choose to block ping, it is still a useful tool in the early stages of troubleshooting. ICMP operates on IP port 1.

- **Informational and query messages**. These messages are used for devices to exchange information and perform testing. They are generated either by an application or simply on a regular basis by devices to provide information to other devices.

- **Error messages.** ICMP error messages provide feedback to another device about an error that has occurred. These messages can be sent as the result of basic errors (such as a requested service is not available or that a device cannot be reached) or more advanced 53 situations (such as a web security gateway does not have sufficient buffering capacity to forward a packet).

ii. Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is a popular protocol used to manage network equipment and is supported by most network equipment manufacturers. It allows network administrators to remotely monitor, manage, and configure devices on the network. SNMP functions by exchanging management.

information between networked devices. Depending on the version, SNMP can operate on ports 161 and 162 (SNMP v3), or ports 10161 and 10162 (Secure SNMP).

iii. Domain Name System (DNS)

The Domain Name System (DNS) is a TCP/IP protocol that resolves (maps) a symbolic name (www.cengage.com) with its corresponding IP address (69.32.133.11). The DNS database is organized as a hierarchy (tree). DNS normally uses UDP port 53.

iv. File Transfer Protocols

Legacy method of transferring large files, this protocol operates over TCP port 21 (and sometimes 20) and broadcasts in the clear. The Internet was primarily a medium for transferring files from one device to another. Today transferring files is still considered an important task. Two TCP/IP protocols are used for transferring files. These are File Transfer Protocol (FTP) and Secure Copy Protocol (SCP).

- **SFTP**
  Modern method of transferring large files, this protocol operates over port 22 using an encrypted SSH tunnel to transfer files.
- **TFTP**

  Trivial File Transfer Protocol, this was primarily used for transferring files onto dedicated devices such as switches. Operating over UDP port 69, it has been superseded by SSH.

- **FTPS**
  File Transfer Protocol over SSL: an SSL variant of the popular FTP protocol. FTP is considered highly vulnerable without some form of protection, since it broadcasts its authentication and activity in clear text. Therefore, anyone listening on the wire can very easily use that data for their own purposes. FTPS operates over ports 989 and 990.

v. **Secure Copy Protocol (SCP)**
Another protocol used for file transfers is Secure Copy Protocol (SCP). SCP is an enhanced version of Remote Copy Protocol (RCP). SCP encrypts files and commands, yet has limitations.
Secure Copy: a method of transferring files while staying within the protection of the SSH protocol. Traffic will remain within the created SSH connection on port 22.

vi. **IPSec**
Internet Protocol Security: one of the foundations of VPN tunneling. This allows data to be encrypted over an unsecured channel, such as the Web, and transmitted safely from end to end

vii. **SSH**

Secure Shell: an encrypted method of remotely connecting to devices for administration and tunneling insecure protocols across the web. This operates over TCP port 22

viii. **TLS/SSL**

Transport Layer Security: the next generation of the Secure Socket Layer. Designed to prove that the computer on the other end of a connection is the one that it is supposed to be, TLS and SSL are commonly used to create encrypted connections from point to point.

TLS and SSL protected traffic normally operates on ports that are different from their standard counterparts. For example: unprotected HTTP traffic operates on port 80, while protected HTTPS traffic operates on port 443.

1. **TCP/IP**
Transmission Control Protocol and the Internet Protocol: the backbone of the modern network. TCP/IP is actually a suite of protocols, designed to work together to route traffic from source to destination.

2. HTTPS

   HyperText Transfer Protocol over SSL: an SSL variant of the incredibly popular HTTP protocol. HTTP is great for transmitting data that does not need to be protected, but if you are logging onto something like a banking website- you want to know for sure that nobody is going to be able to get your credentials and use them against you. HTTPS operates over port 443.

3. **IPv4**

   Legacy IP addresses in the 123.456.789.000 format with an estimated maximum number of public IP addresses of 4.3 billion. This sounds like a lot until you start to think about how many networked devices the average person has associated with themselves at any given time. l) IPv6 New-type IP scheme, presented in the 1111:2222:3333:4444:5555:6666:7777:AAAA format. Unlike IPv4, this addressing scheme is in Hexadecimal. Combined with the larger addressing style, this potentially can have up to 3.4 x 10^38 addresses.

m) iSCSI

Internet Small Computer System Interface, a protocol used for Storage Area Networks to fool servers into thinking they have very large local hard disks. iSCSI usually uses TCP ports 80 and 3260.

n) FCoE

Fiber Channel over Ethernet, allows the Fiber Channel Protocol to be used over standard network connections.

o) TELNET

Telnet is a program normally used for testing connections and remote administration. Operating by default on port 23, this has been primarily replaced by SSH.

p) NetBIOS

Network Basic Input Output System, it was a precursor to DNS. The primary way that users interact with it today is its naming convention, which must be 15 characters or less. NetBIOS operates on ports 137, 138 and 139.

q) RDP

(Remote Desktop Protocol) port 3389 Remote Desktop Protocol (RDP) is a Microsoft protocol designed to facilitate application data transfer security and encryption between client users, devices and a virtual network server

Storage Protocols The amount of data that is being stored has grown almost beyond imagination. Whereas at one time a single terabyte of storage was considered massive, today that is no longer the case Most organizations have turned to using a storage area network (SAN), which is a dedicated network storage facility that provides access to data storage over a high-speed network. SANs consolidate different storage facilities—disk arrays, tape libraries, and even "optical jukeboxes" that can load thousands of discs by robotic arms—so they are accessible to servers.

NetBIOS NetBIOS (Network Basic Input/Output System) is a transport protocol used by Microsoft Windows systems to allow applications on separate computers to communicate over a LAN. In modern networks NetBIOS normally runs over TCP/IP through the NetBIOS over TCP/IP (NBT) protocol. This results in each computer in the network having both an IP address plus a NetBIOS name.

IPv6

The current version of the IP protocol is version 4 and is called IPv4. Developed in 1981, long before the Internet was universally popular, IPv4 has several weaknesses. One of the weaknesses is the number of available IP addresses. An IP address is 32 bits in length, providing about 4.3 billion possible IP address combinations. This no longer is sufficient for the number of devices that are being connected to the Internet. Another weakness is that of security. Due to its structure, IPv4 can be subject to several types of attacks.

Indicative content 2.4.3: Application of secure network administration principals

a) Rule-based management

A person or group is granted access to what they need to perform their tasks and nothing more. This is done to protect both the organization and the user.
Administering a network can be a difficult task; administering a secure network can be even more challenging. It is important that network security administration follow a rule-based management approach, which is the process of administration that relies on following procedural and technical rules, instead of creating security elements "on the fly." There are different types of rules. Procedural rules may be defined as the authoritative and prescribed direction for conduct. The procedural rules in turn, dictate technical rules.

Technical rules may involve configuring a firewall or proxy server to conform to the procedural rules. It is the role of the network administrator to follow a rule-based management approach. This typically involves following rules that address device security, monitoring and analyzing logs, network design management, and port security.

b) Firewall rules

Firewalls have two types of rules: Explicit and Implicit. Explicit is laid out expressly to allow or deny access to a particular resource- for example, if you wanted to allow access to amazon.com to a particular ip range in your network. Implicit is a generic rule that is either inherited via other means, or are final 'catch-all' rules- for example, after all other rules are applied, you have a 'deny all' to block everything that doesn't need access.

c) Device Security

Because new devices are continually added to the network, securing devices is a never-ending task yet is key in maintaining a network's security. Device security includes establishing a secure router configuration and implementing flood guards.

Secure Router Configuration

Default settings on a router are extremely dangerous- potentially allowing access from anywhere on the planet. Either locking down the router so that it can be accessed only locally or through a console port can be a great start.

Task	Explanation
Create a network design	Prior to any configuration, a network diagram that illustrates the router interfaces should be created. This diagram should reflect both the LAN and wide area network (WAN) interfaces.
Use a meaningful router name	Because the name of the router appears in the command line during router configuration, it helps ensure that commands are given to the correct router. For example, if the name *Internet_Router* is assigned to the device, the displayed command prompt would be *Internet_Router (config)#*.
Secure all ports	All ports to the router should be secured. This includes both physical ports (sometimes called the *console port* and *auxiliary port*) and inbound ports from remote locations (sometimes known as *VTY* for *virtual teletype*).
Set a strong administrator password	Most routers allow a user to access the command line in *user mode*, yet an administrator password is required to move to *privileged mode* for issuing configuration commands.
Make changes from the console	The configuration of the router should be performed from the console and not a remote location. This configuration can then be stored on a secure network drive as a backup and not on a laptop or USB flash drive.

Table 6.Basic secure router configuration.

Flood Guard

A basic defense against DDoS attacks, **flood guards** attempt to prevent traffic that could potentially overwhelm the network.

Please note however that to be effective, this needs to be adjusted manually to meet the needs of your network- it doesn't come out of the box with automatic settings.

One defense against DoS and DDoS SYN flood attacks is to use a **flood guard**.

A flood guard is a feature that controls a device's tolerance for unanswered service requests and helps to prevent a DoS attack. Flood guards are commonly found on firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

d) Monitoring and Analyzing Logs

A log is a record of events that occur. Security logs are particularly important because they can reveal the types of attacks that are being directed at the network and if any of the attacks were successful. A security access log can provide details regarding requests for specific files on a system while an audit log is used to record which user performed an action and what that action was. System event logs document any unsuccessful events and the most significant successful 60 events (some system event logs can be tailored to specify the types of events that are recorded). The types of information that can be recorded might include the date and time of the event, a description of the event, its status, error codes, service name, and user or system that was responsible for launching the event.

- **Network Design Management**

In addition to device security and monitoring and analyzing logs, several network design management principles should be followed to ensure that security and the viability of the network are maintained. Network separation to prevent bridging, loop protection, and VLAN management are three principles that should be considered.

e) Network Separation

One of the important rules of network design is to separate secure parts of the network from unsecure parts. That is, the part of the network that contains customer credit card information should not be accessible from the part of the network that manages heating and cooling systems. One way to provide network separation is to physically separate users by connecting them to different switches and routers. This prevents bridging and even prevents a reconfigured device from allowing that connection to occur.

b) Loop Protection

In Figure 11, Host Z, which is connected to Switch A, wants to send frames to Host X on Segment 2. Because Switch A does not know where Host X is located, it "floods" the network with the packet. The packet then travels down Segment 1 to Switch B and Segment 2 to Switch C. Switch B then adds Host Z to its lookup table that it maintains for Segment 1, and Switch C also adds it to its lookup table for Segment 3. Yet if Switch B or C has not yet learned the address for Host Z, they will both flood Segment 2 looking for Host X; that is, each switch will take the packet sent by the other switch and flood it back out again because they still do not know where Host X is located.

Switch A then will receive the packet from each segment and flood it back out on the other segment. This switching loop causes a broadcast storm as the frames are broadcast, received, and rebroadcast by each switch. Broadcast storms can cripple a network in a matter of seconds to the point that no legitimate traffic can occur.

Broadcast storms can be prevented with loop protection, which uses the IEEE 802.1d standard spanning-tree algorithm (STA). STA can determine that a switch has multiple ways to communicate with a host and then determine the best path while blocking out other paths.

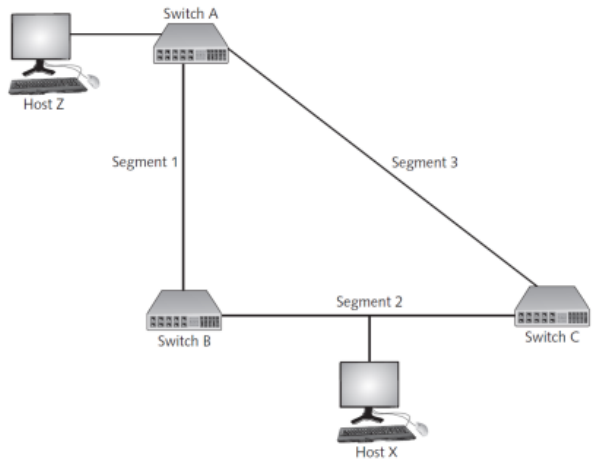


Figure 15. Broadcast storm

Although STA determines the best path, it also registers the other paths in the event that the primary path is unavailable.

c) VLAN Management

It is possible to segment a network by physical devices grouped into logical units through a virtual LAN (VLAN). This allows scattered users to be logically grouped together even though they may be attached to different switches, thus reducing network traffic and providing a degree of security. Some general principles for managing VLANs are:

- Configure empty switch ports to connect to an unused VLAN.
- Change any default VLAN names.
- Configure the ports on the switch that pass tagged VLAN packets to explicitly forward specific tags.
- Configure VLANs so that public devices, such as a web application server, are not on a private VLAN, forcing users to have access to that VLAN.

f) Port Security

Securing physical ports is an important step in network management. Ports can be secured through disabling unused interfaces, using MAC limiting and filtering, and through IEEE802.1x.

i. Disabling Unused Interfaces

Disabling unused interfaces is a security technique to turn off ports on a network device that are not required, such as a switch. This is an important security step that is often overlooked. A switch or router without port security allows attackers to connect to unused ports to access the network. It is important that all interfaces be secured before a router or switch is deployed. The network administrator should navigate to each unused interface and issue the appropriate shutdown command.

ii. MAC Limiting and Filtering In addition to disabling unused interfaces, another step in port security is MAC limiting and filtering. This will filter and limit the number of media access control (MAC) addresses allowed on a single port. A port can be set to a limit of only 1 and a specific MAC address can be assigned to that port. This enables only a single authorized host to connect through that port; attempts to access the interface by a host not listed will result in a security violation.

iii. IEEE 802.1x The IEEE 802.1x standard provides the highest degree of port security by implementing port-based authentication. This protocol authenticates users on a per switch port basis by permitting access to valid users but effectively disabling the port if authentication fails. This prevents an unauthenticated device from receiving any network traffic until its identity can be verified. It also strictly limits access to the device that provides the authentication to prevent attackers from reaching it.

Indicative content 2.4.4: Application of secure wireless network

As a result of the wireless security vulnerabilities in IEEE and Wi-Fi Alliance technologies, both organizations worked to create comprehensive security solutions. The results from the IEEE, known as 802.11i, served as the foundation for the Wi-Fi Alliance's Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA and WPA2 are the primary wireless security solutions today. In addition, there are other security steps that can be taken.

a) Wi-Fi Protected Access (WPA) As the IEEE worked on the 802.11i standard, the Wi-Fi Alliance grew impatient and decided that wireless security could no longer wait.

In October 2003 it introduced its own Wi-Fi Protected Access (WPA). One of the design goals of WPA was to fit into the existing WEP engine without requiring extensive hardware upgrades or replacements. There were two modes of WPA. WPA Personal was designed for individuals or small office/home office (SOHO) settings, which typically have 10 or fewer employees. A more robust WPA Enterprise was intended for larger enterprises, schools, and government agencies. WPA addresses both encryption and authentication.

b) Temporal Key Integrity Protocol (TKIP) Encryption The heart and soul of WPA is a newer encryption technology called Temporal Key Integrity Protocol (TKIP). TKIP functions as a "wrapper" around WEP by adding an additional layer of security but still preserving WEP's basic functionality.

TKIP's enhancements are in three basic areas: the required key length is increased from 64 bits to 128 bits (making it harder to break), the IV is increased from 24 bits to 48 bits (effectively eliminating collisions), and a unique "base key" is created for each wireless device using a master key derived in the authentication process along with the sender's unique MAC address (this key is used with the IV to create unique keys for each packet).

c) Preshared Key (PSK) Authentication

Authentication for WPA Personal is accomplished by using a preshared key (PSK). In cryptography, a PSK is a value that has been previously shared using a secure communication channel between two parties. In a WLAN, a PSK is slightly different. It is a secret value that is manually entered on both the AP and each wireless device, making it essentially identical to the "shared secret" used in WEP. Because this secret key is not widely known, it may be assumed that only approved devices have the key value. Devices that have the secret key are then automatically authenticated by the AP.

Although using PSK has several weaknesses—the key must be kept secret, it can be difficult to manage multiple devices, the key itself may be weak, keys must be entered manually—the alternative requires a significant investment in hardware and software. Authentication for enterprises should use the higher-level authentication process, but for home users, PSK is the option of choice.

WPA Vulnerabilities Although an improvement over WEP, WPA nevertheless has weaknesses. One of the design goals of WPA was to fit into the existing WEP engine without requiring extensive hardware upgrades or replacements. Because most existing WEP devices at the time WPA was released had very limited central processing unit (CPU) capabilities— with many APs operating at less than 40 MHz—a series of compromises had to be made.

d) Wi-Fi Protected Access 2 (WPA2)

In March 2001 the IEEE started work on addressing wireless security. This work was based on new wireless security mechanisms as opposed to transitional solutions such as WPA. After three years of effort, in June 2004 the IEEE 802.11i wireless security standard was ratified.

e) AES-CCMP Encryption

The WPA2 standard addresses encryption by using the Advanced Encryption Standard (AES) block cipher. AES performs three steps on every block (128 bits) of plaintext.
The encryption protocol used for WPA2 is the **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)** and specifies the use of CCM (a general-purpose cipher mode algorithm providing data privacy) with AES.

IEEE 802.1x Authentication
Authentication for the WPA2 Enterprise model uses the IEEE 802.1x standard. This standard, originally developed for wired networks, provides a greater degree of security by implementing port-based authentication. IEEE 802.1x blocks all traffic on a port-byport basis until the client is authenticated using credentials stored on an authentication server. This prevents an unauthenticated device from receiving any network traffic until its identity can be verified. It also strictly limits access to the device that provides the authentication to prevent attackers from reaching it.

It is important that the communication between the supplicant, authenticator, and authentication server in an IEEE 802.1x configuration be secure. A framework for transporting the authentication protocols is known as the Extensible Authentication Protocol (EAP). EAP was created as a more secure alternative than the weak Challenge-Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP). Despite its name, EAP is a framework for transporting authentication protocols instead of the authentication protocol itself.
EAP essentially defines the format of the messages and uses four types of packets: request, response, success, and failure. Request packets are issued by the authenticator and ask for a response packet from the supplicant. Any number of request–response exchanges may be used to complete the authentication. If the authentication is successful, a success packet is sent to the supplicant; if not, a failure packet is sent.

Additional Wireless Security Protections Other security steps can be taken to protect a wireless network. These include captive portal APs, rogue AP discovery tools, power level controls, antennas, and site surveys.

Captive Portal APs A home user who installs a WLAN can simply launch a web browser to give immediate and unlimited access to the Internet.

In a public area that is served by a WLAN, however, opening a web browser will rarely give immediate Internet access because the owner of the WLAN usually wants to advertise itself as providing this service, or wants the user to read and accept an Acceptable Use Policy (AUP) before using the WLAN. And sometimes a "general" authentication, such as a password given to all current hotel guests, must be entered before being given access to the network. This type of information, approval, or authentication can be supported through a captive portal AP. A captive portal AP uses a standard web browser to provide information, and gives the wireless user the opportunity to agree to a policy or present valid login credentials, providing a higher degree of security.

Rogue AP Discovery Tools The problem of rogue APs is of increasing concern to organizations. Several methods can be used to detect a rogue AP by continuously monitoring the RF airspace. This requires a special sensor called a wireless probe, a device that can monitor the airwaves for traffic. There are four types of wireless probes: Wireless device probe. A standard wireless device, such as a portable laptop computer, can be configured to act as a wireless probe. At regular intervals during the normal course of operation, the device can scan and record wireless signals within its range and report this information to a centralized database. This scanning is performed when the device is idle and not receiving any transmissions.

When a large number of mobile devices are used as wireless device probes, it can provide a high degree of accuracy in identifying rogue access points. Desktop probe.

Instead of using a mobile wireless device as a probe, a desktop probe utilizes a standard desktop PC. A universal serial bus (USB) wireless network interface card adapter is plugged into the desktop computer to monitor the RF frequency in the area for transmissions. Access point probe. Some AP vendors have included in their APs the functionality of detecting neighboring APs, friendly APs as well as rogue APs. However, this approach is not widely used. The range for a single AP to recognize other APs is limited because APs are typically located so that their signals overlap only in such a way as to provide roaming to wireless users. Dedicated probe. A dedicated probe is designed to exclusively monitor the RF frequency for transmissions. Unlike access point probes that serve as both an AP and a probe, dedicated probes monitor only the airwaves. Dedicated probes look very similar to standard access points.

Once a suspicious wireless signal is detected by a wireless probe, the information is sent to a centralized database where WLAN management system software compares it to a list of approved APs. Any device not on the list is considered a rogue AP. The WLAN management system can instruct the switch to disable the port to which the rogue AP is connected, thus severing its connection to the wired network.

Power Level Controls Another security feature on some APs is the ability to adjust the level of power at which the WLAN transmits. On devices with that feature, the power can be adjusted so that less of the signal leaves the premises and reaches outsiders.
Antennas APs use antennas that radiate out a signal in all directions. Because these devices are generally positioned to provide the broadest area of coverage, APs should be located near the middle of the coverage area. Generally the AP can be secured to the ceiling or high on a wall.

Site Surveys Ensuring that a wireless LAN can provide its intended functionality and meet its required design goals can best be achieved through a site survey.

 **Theoretical learning Activity**

In pair, discuss about network address translation (NAT)

 Points to Remember (Take home message)

- Standard network devices can be classified by the OSI layer at which they function. These devices include switches, routers, load balancers, and proxies.
- The key to the OSI reference model is layers
- Networks devices are: Switch, router, firewall, access point, hub, bridge…
- the 6 key features offered by network switches: **Filtering, Port Mirroring or Mirroring, Port Security, Disabling Ports, Creating Collision Domains, Virtual Local Area Networks or VLANs.**
- Proxy server is a computer or an application program that intercepts user requests from the internal secure network and then processes that request on behalf of the user.
- Computer networks have protocols, or rules for communication
- **Storage Protocols** The amount of data that is being stored has grown almost beyond imagination.
- A log is a record of events that occur.
- Broadcast storms can be prevented with loop protection, which uses the IEEE 802.1d standard spanning-tree algorithm (STA).
- Authentication for the WPA2 Enterprise model uses the IEEE 802.1x standard.

Learning outcome 2.4 formative assessment

1. Differentiate VLAN from subnetting

   Answer.

   There are differences between subnetting and VLANs. Subnets are subdivisions of IP address classes (Class A, B, or C) and allow a single Class A, B, or C network to be used instead of multiple networks. VLANs are devices that are connected logically rather than physically, either through the port they are connected to or by their media access control (MAC) address.
2. How do you understand by Network design?

   Answer.

   Network design refers to planning a computer network infrastructure, and implementing security configuration parameters on network devices.

3. What is Network Address Translation (NAT)

   Answer.

   Network address translation (NAT) is a technique that allows private IP addresses to be used on the public Internet.

4. Define **Cloud Computing**

   Answer.
5. How does a virtual LAN (VLAN) allow devices to be grouped?

   a. based on subnets

   b. logically

   c. directly to hubs

   d. only around core switches

   5. Which device is easiest for an attacker to take advantage of in order to capture and analyze packets?

   a. hub

   b. switch

   c. router

   d. load balancer

6. what is Domain Name System (DNS)

Answer.

The Domain Name System (DNS) is a TCP/IP protocol that resolves (maps) a symbolic name (www.cengage.com) with its corresponding IP address (69.32.133.11).

7. Explain TLS**/SSL?**

Answer.

Transport Layer Security: the next generation of the Secure Socket Layer. Designed to prove that the computer on the other end of a connection is the one that it is supposed to be, TLS and SSL are commonly used to create encrypted connections from point to point.

Learning Outcome 2.5: Test functionality and performance of security system implemented

 **Duration: 4 hrs**

1. Identify asset clearly
2. Identify threats clearly
3. Identify control clearly

 **Resources**

Equipment	Tools	Materials
Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual

 **Advance preparation:**

. Trainer should have all resources in place

Indicative content 2.5.1: Risk management identification and Risk analysis

- **Risk management identification**

✓ **Asset identification**

Asset identification: Asset identification determines the items that have a positive economic value, which may include data, hardware, personnel, physical assets, and software.

Along with the assets, the attributes of the assets need to be compiled and their relative value determined.

✓ **Threat identification**

Threat identification: After the assets have been inventoried and given a relative value, the next step is to determine the threats from threat agents. A threat agent is any person or thing with the power to carry out a threat against an asset. Control identification

✓ **Control identification**

As part of the engagement process, auditors obtain an understanding of controls and the control environment relevant to the audit, determine whether these controls prevent or mitigate assessed risks, and report on any deficiencies. The template helps you to easily record controls, associate them to identified risks, and indicate whether the identified risks have been addressed.

- **Risk Analysis**

✓ **Use Vulnerability Assessment Tools and Techniques**

Vulnerability assessment refers to identifying the loopholes, flaws, weaknesses, errors, perils, or areas of exposure, which can break security protection of a network, system, software, computer, and server.

In simple words, a vulnerability assessment helps you identify the configuration areas, which make your system susceptible to an attack or security breach. This assessment is done with the help of vulnerability scanners. For example, such a tool may check the patching status on the system to inform about missing patches. It may also report user accounts with no passwords, unused accounts, and too many administrative accounts.

Assessment Techniques

In this topic, you will learn the different assessment techniques, namely baseline reporting, code reviewing, determining attack surface, reviewing architecture, and reviewing designs

a) Namely baseline reporting

Baseline reporting records the system's baseline such as the system facts, and how it performs under normal working conditions, and then comparing it to the current performance data.

Let's consider a scenario wherein one of your network servers is slow since two days with a performance reporting of 90% CPU utilization. However, you have also ensured to use the system as per the norm. You now need to find out what is responsible for the slow performance of your system.

You can use the technique of baseline reporting in security incidents such as a malware attack or a denial of service, wherein the system is not performing up to the mark.

b) Code reviewing

The purpose of this review is to look at all the written codes for existing loopholes. The review should also assess the changes in code occurring at any point in time.

While examining the code, it is recommended to look for errors in logic or flaws in programming, which are often responsible for improper or no authentication, SQL injection, and crosssite request forgery.

For example, a critical security rule for validating any data sent to the application is not implemented. This allows a hacker to easily attack the system on which the application is running, such as a buffer overflow or a SQL injection attack.

c) Determining attack surface

This surface is a set of installed applications, protocols, and services available to users who are authenticated, and more prominently, even those who are not authenticated. That is, an attack surface faces the outside, and is subject to become an attack victim. Hence, smaller the surface, less likely it is to get attacked.

As a security professional, it is critical that you help reduce a system's attack surface by removing unwanted software and services, turn off unwanted functions, add authentication, and reduce privileges. This is known as Attack Surface Reduction or ASR

d) Reviewing architecture

You can also review the system's architecture for assessing the security of a network or a system. Through such an architectural approach, you use a control framework to look into the foundational infrastructure in terms of its resistance to forcible entry and dismissal.

This is likely to strengthen Crime Prevention through Environmental Design or CPTED, which motivates designers to boost security via building elements. Such an approach is compliant to security regulatory standards, such as International Organization for Standardization or ISO.

Cisco's SAFE is an example of an architectural approach. Another example of architectural security is the three-ring architecture of computer processors, which is responsible for executing applications.

e) Reviewing designs

Reviewing a design involves examining the ports and protocols in use, access control mechanisms, segmentation, and rules. It is critical to identify security concerns from the beginning so that you can claim a secure design status. After completing the security solution for a network or an application, you need to review the design to ensure what was required as solution is been implemented.

Tools used in Exploring the Vulnerabilities and Threats

Security assessment tools test a system for exploring known vulnerabilities and weaknesses through reports, You can use several tools to perform a vulnerability scan or discover and confirm the presence of a security threat, vulnerability, or a flaw. These include port scanners, banner grabbing tools, protocol analyzers, vulnerability scanners, and honeypots and honeynets.

Although the primary purpose of assessment tools is to help security personnel identify security weaknesses, these tools can likewise be used by attackers to uncover vulnerabilities to be exploited in an attack.

a) Port Scanners

Port scanner is a type of vulnerability scanner exclusively designed for scanning ports of different systems.

Just imagine a scenario wherein networking applications such as FTP and Web servers along with systems with Remote Desktop connection use different port numbers for connecting to their clients. As a network administrator, you have received few complaints regarding data hacking.

TCP/IP uses a numeric value as an identifier to the applications and services on these systems. This value is known as the port number. Each packet/datagram contains the source port and destination port, which identifies both the originating application/service on the local system and the corresponding application/service on the remote system.

Because port numbers are 16 bits in length, they can have a decimal value from 0 to 65535. TCP/IP divides port numbers into three categories:

- *Well-known port numbers* (0–1023). Reserved for the most universal applications
- *Registered port numbers* (1024–49151). Other applications that are not as widely used
- *Dynamic and private port numbers* (49152–65535). Available for use by any application A list of common protocols, the communication protocol that supports each (TCP and/or UDP), and the service port numbers is provided in table below.

Protocol name	Communication protocol	Port number
File transfer protocol (FTP) - data	TCP/UDP	20
File transfer protocol (FTP)- Command	TCP	21
Secure shell (SSH), secure shell file transfer protocol (SFTP), secure copy(SCP)	TCP, UDP	22
Simple mail transfer protocol (SMTP)	TCP	25
Domain name system	TCP/UDP	53
Hypertext transfer protocol (HTTP)	TCP	80
Post Office protocol Version 3 (POP3)	TCP	110
NetBIOS	TCP,UDP	139
Internet message protocol (IMAP)	TCP	143
Hypertext transfer protocol secure (HTTPS)	TCP	443
Microsoft terminal server	TCP, UDP	3389

Table 7. Common protocols, communication protocols, and ports

Because port numbers are associated with applications and services, if an attacker knows that a specific port is accessible, this could indicate what services are being used. For example, if port 20 is available, an attacker could assume that FTP is being used. With that knowledge he can target his attacks to that service. It is important to implement port security by disabling unused application/service ports to reduce the number of threat vectors.

When performing a vulnerability assessment, port scanner software can be used to search a system for port vulnerabilities.

b) Banner Grabbing Tools

A banner is a message that a service transmits when another program connects to it. For example, the banner for a Hypertext Transfer Protocol (HTTP) service will typically show the type of server software, its version number, when it was last modified,
and other similar information. When a program is used to intentionally gather this information, the process is called banner grabbing.

As the name suggests, a banner grabber looks at the header or banner information messages to know more about the systems.

It captures the welcome message or initial response from a network service. Usually, a banner shows the application's or host's identity along with other details such as the version and the operating system on which it is running Banner grabbing can be used as an assessment tool to perform an inventory on the services and systems operating on a server. This can be done by using a tool such as Telnet to create a connection with the host and then querying each port.

In short, banners have all the information required for breaching the security if used negatively, or overcoming security loopholes if used positively.

Can we now associate banner grabbing to port scanning? Well, after a port scan, you can perform a banner grab to find out which software is running on each open port. Here, banner grabbing connects to each port and gathers response from the server in the form of a ready message indicating the software version running on the system.

c) Protocol Analyzers

- ✓ A protocol analyzer is hardware or software that captures packets to decode and analyze their contents.
- ✓ Protocol analyzers help in detecting communication problems imposed by software and hardware problems.
- ✓ Further, they discover protocol anomalies due to malicious intent, malfunction, or improper configuration
- ✓ Protocol analyzers can fully decode application-layer network protocols such as HTTP or FTP.
- ✓ Security administrators often use protocol analyzers for tracking a communication problem or determining the source of an attack.

d) Honeypots and Honeynets

- ✓ **A honeypot** is a computer typically located in an area with limited security and loaded with software and data files that appear to be authentic, but are actually imitations of real data files. The honeypot is intentionally configured with security vulnerabilities so that it is open to attacks. It is intended to trick attackers into revealing their attack techniques.
- ✓ You can gain information about how the hacker's identity, the resource being attacked, and the attack mechanism or tool in use
- ✓ Honeypot system not only pulls the attackers away from a confidential network, but also allows administrators to obtain knowledge about the attack strategy.

When a honeypot system becomes larger, it is commonly known as Honeynet, Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security.

A honeynet typically contains one or more honeypots. A vulnerability scanner refers to an automated software application keeping a check on your network to detect known security holes.

- Such scanning involves finding out weaknesses and loopholes in applications, computers, and networks.

- A vulnerability scanner scans the system for reporting any known vulnerabilities

- Some of the most popular vulnerability scanners are Retina, Nessus, OpenVAS, and SAINT.

Indicative content 2.5.2: Vulnerability scanning and penetration testing tools and Mitigation and Deterrent Technique

Vulnerability assessment is a systematic and methodical evaluation of the exposure of assets to attackers, forces of nature, and any other entity that could cause potential harm. A vulnerability scanner can:

- Alert when new systems are added to the network
- Detect when an application is compromised or subverted
- Detect when an internal system begins to port scan other systems
- Detect which ports are served and which ports are browsed for each individual system
- Identify which applications and servers host or transmit sensitive data
- Maintain a log of all interactive network sessions
- Passively determine the type of operating system of each active system
- Track all client and server application vulnerabilities
- Track which systems communicate with other internal systems

Vulnerability Scanners is a generic term for a range of products that look for vulnerabilities in networks or systems.

There are two methods for performing a vulnerability scan. An **intrusive vulnerability** scan attempts to actually penetrate the system in order to perform a simulated attack, while a **non-intrusive vulnerability** scan uses only available information to hypothesize the status of the vulnerability.

Penetration Testing

Unlike a vulnerability scan, penetration testing (pentesting) is designed to actually exploit any weaknesses in systems that are vulnerable. Instead of using automated software, penetration testing relies upon the skill, knowledge, and cunning of the tester.

The tester herself is usually an independent contractor not associated with the organization. Such testers, known as "white hat hackers" or "ethical attackers," have the organization's permission to exploit vulnerabilities in a system and then privately provide information back to that organization. Testers are typically outside (instead of inside) the security perimeter and may even disrupt the operation of the network or devices (instead of passively probing for a known vulnerability).

The goals of a penetration test are to actively test all security controls and, when possible, bypass those controls, verify that a threat exists, and exploit any vulnerabilities. Whereas vulnerability scan software may uncover a vulnerability, it provides no indication regarding the risk to that specific organization. If a penetration tester uncovers a vulnerability, however, she will continue to exploit it to determine how dangerous it can be to the organization.

Three different techniques can be used by a penetration tester. Each technique varies in the amount of knowledge the tester has regarding the details of the systems that are being evaluated:

Black box. In a black box test, the tester has no prior knowledge of the network infrastructure that is being tested. The tester must determine the location and types of systems and devices before starting the actual tests. This technique most closely mimics an attack from outside the organization.

White box. The opposite of a black box test is a white box test, in which the tester has an in-depth knowledge of the network and systems being tested, including network diagrams, IP addresses, and even the source code of custom applications.

Grey box. Between a black box test and a white box test is a grey box test, in which some limited information has been provided to the tester.

Some examples of Vulnerability scanning and penetration testing tools are: Air crack 75, NMAP, OpenVAS, Wireshark, etc.

✓ **Wire shark**

Wireshark is one of the most popularly used network protocol analyzers. It is a cross-platform, open-source tool that allows users to microscopically view and troubleshoot their network

The key features of Wireshark include

- **Packet sniffing**: Wireshark uses a packet sniffing and capture API to capture data packets. On UNIX/Linux, it is called libpcap, which stands for Promiscuous Library Capture.
- **Voice over Internet Protocol (VoIP):** Wireshark can also capture voice over internet protocol data packets or calls made across the network, allowing the user access to the data.
- **Detailed comprehensive reports:** Wireshark provides the result of tests carried out on a network in a format that any operator can easily understand.
- **Operating system compatibility:** Wireshark can be used on operating systems such as Linux OS, macOS, Solaris, Windows OS, and other operating systems similar to UNIX.

Wireshark for Windows

Wireshark comes in two options for Windows: 32-bit and 64-bit. Pick the correct version for your OS; the current release is 3.0.3 as of this writing.

Wireshark for Mac

Wireshark is available on Mac as a Homebrew install.

To install Homebrew, you need to run this command at your Terminal prompt:

/usr/bin/ruby -e "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/master/install)"

Once you have the Homebrew system in place, you can access several open-source projects for your Mac. To install Wireshark, run this command from the Terminal:

brew install wireshark

Homebrew will download and install Wireshark and any dependencies needed to function correctly.

Wireshark for Linux

Installing Wireshark on Linux can be a little different depending on the Linux distribution. If you aren't running one of the following distros, please double-check the commands.

Ubuntu

From a Terminal prompt, run these commands:

- **sudo apt-get install wireshark**
- **sudo dpkg-reconfigure wireshark-common**
- **sudo adduser $USER wireshark**

Prevent Packet Sniffing attack?

In a packet sniffing attack, hackers capture network packets to intercept or steal data that may be unencrypted

There are several ways of preventing yourself from packet sniffing such as: VPN, Use Secure file transfer protocol (SFTP), Avoid clicking on suspicious links, Install an antivirus, Data encryption, Avoid unsecured network, etc.

How VPN prevent packet sniffer attack

A Virtual Private Network secures all the data sent from your computer over the internet by encrypting your connection and hiding your IP address. Using a robust VPN like AVG Secure VPN means that a sniffer spying on your traffic would just see scrambled info, while your data stays safe

- **Mitigation and Deterrent Technique**

Although there are a wide variety of attacks, standard techniques should be used in mitigating and deterring attacks. These techniques include creating a security posture, selecting and configuring controls, hardening, and reporting.

A. Creating a Security Posture

A security posture may be considered as an approach, philosophy, or strategy regarding security. A healthy security posture results from a sound and workable strategy toward managing risks. Several elements make up a security posture, including:

• **Initial baseline configuration**. A baseline is the standard security checklist against which systems are evaluated for a security posture.

A baseline outlines the major security considerations for a system and becomes the starting point for solid security. It is critical that a strong baseline be created when developing a security posture.

• **Continuous security monitoring**. Continual observation of systems and networks through vulnerability scanning and penetration testing can provide valuable information regarding the current state of preparedness. In particular, system logs—including event logs, audit logs, security logs, and access logs—should be closely monitored.

• **Remediation**. As vulnerabilities are exposed through monitoring, a plan must be in place to address the vulnerabilities before they are exploited by attackers.

B. Selecting Appropriate Controls

Selecting the appropriate controls to use is another key to mitigating and deterring attacks. Although many different controls can be used, there are common controls that are important to meet specific security goals. Table 15-9 summarizes some of these

Security goal	Common controls
Confidential	Encryption, steganography, access control
Integrity	Hashing, digital signatures, certificates, nonrepudiation tool
Availability	Redundancy, fault tolerance, patching
Safety	Fencing and lighting, locks, CCTV, escape plans and routes, safety drills

Table 8. Appropriate controls for different security goals

C. Configuring Controls

Another key to mitigating and deterring attacks is the proper configuration and testing of the controls. One category of controls is those that can either detect or prevent attacks. For example, a closed-circuit television (CCTV) camera's primary purpose in a remote hallway may be to detect if a criminal is attempting to break into an office. A security guard whose desk is positioned at the entrance of the hallway has the primary purpose of preventing the criminal from entering the hallway.

D. Hardening

The purpose of hardening is to eliminate as many security risks as possible and make the system more secure. A variety of techniques can be used to harden systems. Types of hardening techniques include:

- Protecting accounts with passwords
- Disabling any unnecessary accounts
- Disabling all unnecessary services
- Protecting management interfaces and applications

E. Reporting

It is important to provide information regarding the events that occur so that action can be taken. This reporting can take the form of alarms or alerts that sound a warning message of a specific situation that is occurring. For example, an alert could signal that someone is trying to guess a user's password by entering several different password attempts. The reporting also can involve providing information on trends that may indicate an even more serious impending situation. A trend report may indicate that multiple user accounts are experiencing multiple password attempts.

- **Port security**

  Port security is what can help secure the network by making sure to block foreign devices from forwarding packets. With the use of port security, users can restrict the number of MAC addresses that can be learned to a port, configure static MAC addresses, and impose penalties on unauthorized users that use the port.

  Disabling unused application/service ports to reduce the number of threat vectors.

- **Monitoring system logs**

  Log monitoring is a process by which developers and administrators continuously observe logs as they're recorded. With log monitoring software, teams can collect information and trigger alerts if something affects system performance and health.

Theoretical learning Activity

In pair, Explain all risk assessment techniques

Points to Remember (Take home message)

- Asset identification. Asset identification determines the items that have a positive economic value, which may include data, hardware, personnel, physical assets, and software.
- Threat identification. After the assets have been inventoried and given a relative value, the next step is to determine the threats from threat agents.
- Vulnerability assessment refers to identifying the loopholes, flaws, weaknesses, errors, perils, or areas of exposure, which can break security protection of a network, system, software, computer, and server.
- Assessment techniques include: Namely baseline reporting, code reviewing, determining attack surface, reviewing architecture and reviewing designs.
- **Vulnerability Scanners** is a generic term for a range of products that look for vulnerabilities in networks or systems.
- Three different techniques can be used by a penetration tester: grey box, black and white.

Learning outcome 2.5 formative assessment

1. List 4 examples of Vulnerability scanning and penetration testing tools:
   Answer.

b. Wireshark
c. Aircrack 75
d. NMAP
e. Openvas

2. Explain Three different techniques can be used by a penetration tester
   Answer.
   Black box. In a black box test, the tester has no prior knowledge of the network infrastructure that is being tested. The tester must determine the location and types of systems and devices before starting the actual tests. This technique most closely mimics an attack from outside the organization.
   White box. The opposite of a black box test is a white box test, in which the tester has an in-depth knowledge of the network and systems being tested, including network diagrams, IP addresses, and even the source code of custom applications.
   Grey box. Between a black box test and a white box test is a grey box test, in which some limited information has been provided to the tester.

3. Define these terms below:

a. Asset identification**: Asset identification determines the items that have a positive economic value, which may include data, hardware, personnel, physical assets, and software.**

b. Threat identification**: After the assets have been inventoried and given a relative value, the next step is to determine the threats from threat agents.**

c. Vulnerability assessment: **refers to identifying the loopholes, flaws, weaknesses, errors, perils, or areas of exposure, which can break security protection of a network, system, software, computer, and server.**

4. What a Protocol analyzer?

   Answer.

   A protocol analyzer is hardware or software that captures packets to decode and analyze their contents.

5. Enumerate at least 3 Risk assessment techniques.

   Answer.

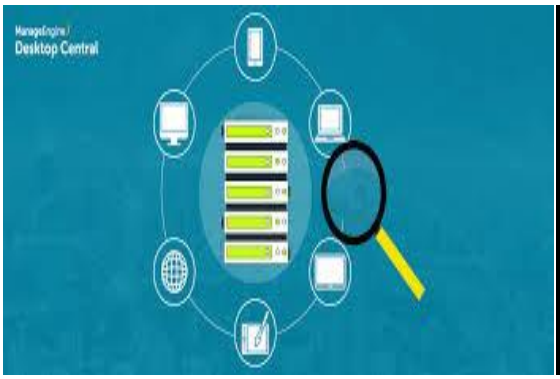
a. Namely baseline reporting,

b. Code reviewing,

c. Determining attack surface,

d. Reviewing architecture and reviewing designs.

Learning Unit 3: Monitor and maintain network security



STRUCTURE OF LEARNING UNIT

Learning outcomes:

3.1. Monitor current network security
3.2. Adjust security system.
3.3. Document on current system settings and file for future reference
3.4. Document on newly discovered security threats, vulnerabilities and risks

Learning outcome 3.1 Monitor current network security.

Duration: 4 hrs
Learning outcome 3.1 objectives: By the end of the learning outcome, the trainees will be able to: 1. Use network analysis tools clearly 2. Use intrusion detection and prevention systems clearly 3. Use network monitoring systems
Resources

Equipment	Tools	Materials

Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual
Advance preparation: . Trainer should have all resources in place		

Indicative content 3.1.1: Usage of network analysis tools, and usage of intrusion detection and prevention systems

- **Usage of network analysis tools**

  A protocol analyzer (also known as a sniffer, packet analyzer, network analyzer, or traffic analyzer) can capture data in transit for the purpose of analysis and review. Sniffers allow an attacker to inject themselves between a conversation between a digital source and destination in hopes of capturing useful data. Some data if unencrypted can be opened and viewed. Credentials can be sent in cleartext exposing your secured logins to risk. unless encrypted in a way that cannot be decrypted easily, any and all data sent to and from can be viewed and used for wrong doing.

IDS Hardware or software that captures packets to decode and analyze their contents.

- **Usage of intrusion detection and prevention systems**

  Intrusion Detection and Prevention An intrusion detection system (IDS) is a device that can detect an attack as it occurs. IDS systems can use different methodologies for monitoring for attacks. In addition, IDS can be installed on either local hosts or networks. An extension of IDS is an intrusion prevention system (IPS).

  Monitoring Methodologies *Monitoring* involves examining network traffic, activity, transactions, or behavior in order to detect security-related anomalies. There are four monitoring methodologies: *anomaly-based monitoring, signature-based monitoring, behaviorbased monitoring, and heuristic monitoring*.

- **Anomaly-based monitoring**

  Anomaly-based monitoring is designed for detecting statistical anomalies. First, a baseline of normal activities is compiled over time. (A baseline is a reference set of data against which operational data is compared.) Whenever there is a significant deviation from this baseline, an alarm is raised. An advantage of this approach is that it can detect the anomalies quickly without trying to first understand the underlying cause. However, normal behavior can change easily and even quickly, so anomaly-based monitoring is subject to false positives, or alarms that are raised when there is no actual abnormal behavior. In addition, anomaly based monitoring can impose heavy processing loads on the systems where they are being used. Finally, because anomaly-based monitoring takes time to create statistical baselines, it can fail to detect events before the baseline is completed.

- **Signature-based monitoring**

  Signature-based monitoring because it compares activities against a predefined signature. Signature-based monitoring requires access to an updated database of signatures along with a means to actively compare and match current behavior against a collection of signatures. One of the weaknesses of signature-based monitoring is that the signature databases must be constantly updated, and as the number of signatures grows, the behaviors must be compared against an increasingly large number of signatures.

- **Behavior-based monitoring**

  Behavior-based monitoring attempts to overcome the limitations of both anomaly-based monitoring and signature-based monitoring by being adaptive and proactive instead of reactive. Rather than using statistics or signatures as the standard by which comparisons are made, behavior-based monitoring uses the “normal” processes and actions as the standard. Behavior based monitoring continuously analyzes the behavior of processes and programs on a system and alerts the user if it detects any abnormal actions, at which point the user can decide whether to allow or block the activity. One of the advantages of behavior-based monitoring is that it is not necessary to update signature files or compile a baseline of statistical behavior before monitoring can take place. In addition, behavior-based monitoring can more quickly stop new attacks.

- **Heuristic monitoring**

  Heuristic monitoring, it attempts to answer the question, Will this do something harmful if it is allowed to execute? Heuristic (from the Greek word for find or discover) monitoring is similar to antivirus heuristic detection. However, instead of creating a virtual environment in which to test a threat, IDS heuristic monitoring uses an algorithm to determine if a threat exists.

- ✓ **Network intrusion detection system (NIDS)**

  A network-based intrusion detection system is designed to help organizations monitor their cloud, on-premise and hybrid environments for suspicious events that could indicate a compromise. This includes policy violations and port scanning, plus unknown source and destination traffic.

  NIDS security technologies are 'passive' rather than 'active' in nature. This means that they are designed solely to alert on suspicious activity, and for this reason are often deployed alongside intrusion prevention systems (IPS) which are 'active'.

  For organizations looking to further increase threat visibility, NIDS systems are commonly used in conjunction with host-based intrusion detection systems (HIDS) and SIEM solutions, which aggregate and analyze security events from multiple sources.

- ✓ **Wireless intrusion detection system (WIDS)**

  A wireless intrusion prevention system (WIPS) is a dedicated security device or integrated software application that monitors a wireless LAN network's radio spectrum for rogue access points and other wireless threats.

  A WIPS compares the MAC addresses of all wireless access points on a network against the known signatures of pre-authorized, known wireless access points and alerts an administrator when a discrepancy is found.

  In addition to providing a layer of security for wireless LANS, WIPS are also useful for monitoring network performance and discovering access points with configuration errors. In addition to intrusion detection, a WIPS also includes features that prevent against the threat automatically.

  The following types of threats can be prevented by a good WIPS:

a. Rogue access points – WIPS should understand the difference between rogue APs and external (neighbor's) APs
b. Mis-configured AP
c. Client mis-association
d. Unauthorized association
e. Man-in-the-middle attack
f. Ad hoc networks
g. MAC spoofing
h. Honeypot / evil twin attack
i. Denial-of-service attack

✓ **Network intrusion prevention system (NIPS)**

A network intrusion protection system (NIPS) is an umbrella term for a combination of hardware and software systems that protect computer networks from unauthorized access and malicious activity.

NIPS hardware may consist of a dedicated Network Intrusion Detection System (NIDS) device, an Intrusion Prevention System (IPS), or a combination of the two such as an Intrusion Prevention and Detection System (IPDS).

Note that while an NIDS can only detect intrusions, an IPS can pro-actively stop an attack by following established rules, such as changing firewall settings, blocking particular Internet protocol (IP) addresses or dropping certain packets entirely. The software components of an NIPS consists of various firewall, sniffer and antivirus tools in addition to dashboards and other data visualization tools.

A NIPS continually monitors an organization's computer networks for abnormal traffic patterns, generating event logs, alerting system administrators to significant events and stopping potential intrusions when possible. A NIPS is also useful for internal security auditing and providing documentation for compliance regulations. Spyware, viruses and attacks continue to grow and it is now recognized that a layered combination of security systems working together is necessary to protect computer networks from compromise. A NIPS in some form is vital for any computer network that can be accessed by unauthorized persons. Computers holding sensitive data always need protection; however, even seemingly insignificant networks can be hijacked for use in botnet attacks.

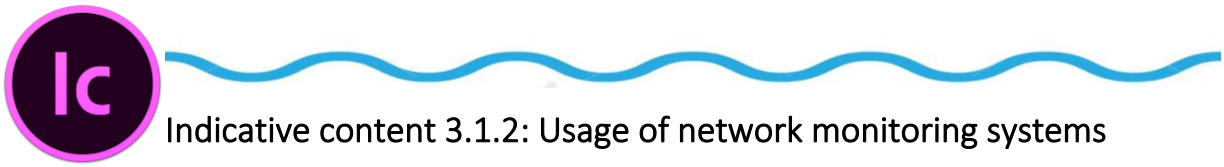
✓ **Wireless intrusion prevention system (WIPS)**

Purpose

A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures.

The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices.

A wireless intrusion detection system (WIDS) monitors the *radio spectrum* for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.



Indicative content 3.1.2: Usage of network monitoring systems

- ✓ **Behavior-based monitoring**

  Behavior Monitoring is the process of collecting and analyzing the network information to detect malicious activities. It is also referred to as network behavior analysis (NBA) or network behavior anomaly detection. Behavioral monitoring software analyses data from various sources and employs machine learning to spot trends that could indicate an attack is underway.

  In IT, behavioral monitoring checks and controls end-user, device, and network behavior patterns.

  The baseline is a model behavioral profile that the monitoring solution creates for individuals and devices. For each person, device, or app, a baseline would be set. This becomes easier to spot inconsistencies or anomalies once this baseline has been established.

  When done over a significant period, behavior monitoring allows companies to benchmark usual network behavior, which aids in the detection of anomalies. Any anomalies found can be submitted for further investigation. This method of information security is likely to play an increasingly crucial role in safeguarding computers at the network's edge as machine learning improves.

  Benefits of Behavior Monitoring?

  While some cyber security services are reactive, behavior monitoring is by definition active. Instead of responding to a threat or reducing its impact, you aim to eliminate it. This is why behavior-based security solutions are so effective against so-called zero-day exploits. It will indicate any action that mimics prior cyberattacks as a possible threat.

- ✓ **Signature-based monitoring**

  Signature-based detection is a process that is commonly used to address software threats on your computer. These threats may include malware, viruses, worms, Trojans, and many others.

  In signature-based detection, appropriate signatures for each file are created and compared with known signatures that have been stored and detected before. The process never stops until a match is found. When this happens, the file is considered a threat and automatically gets blocked. The antivirus programs you installed on your computer may be using signature-based detection to check for malware.

- ✓ **Anomaly-based monitoring**

  An anomaly-based intrusion detection system, is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.

  In order to positively identify attack traffic, the system must be taught to recognize normal system activity. The two phases of a majority of anomaly detection systems consist of the training phase (where a profile of normal behaviors is built) and testing phase (where current traffic is compared with the profile created in the training phase).

  Nomalies are detected in several ways, most often with artificial intelligence type techniques. Systems using artificial neural networks have been used to great effect.

  Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.

- ✓ **Heuristic monitoring**

  Heuristic analysis is a method of detecting viruses by examining code for suspicious properties. It was designed to spot unknown new viruses and modified versions of existing threats.

  Heuristic analysis is a method of detecting viruses by examining code for suspicious properties. It was designed to spot unknown new viruses and modified versions of existing threats.

Theoretical learning Activity

In pair, Brainstorming on possible motoring software

Points to Remember (Take home message)

- *A protocol analyzer (also known as a sniffer, packet analyzer, network analyzer, or traffic analyzer)* can capture data in transit for the purpose of analysis and review.
- IDS Hardware or software that captures packets to decode and analyze their contents.
- *Intrusion Detection and Prevention An intrusion detection system* (IDS) is a device that can detect an attack as it occurs.
- There are four monitoring methodologies: *anomaly-based monitoring, signature-based monitoring, behavior based monitoring, and heuristic monitoring*.
- *A wireless intrusion prevention system (WIPS)* is a dedicated security device or integrated software application that monitors a wireless LAN network's radio spectrum for rogue access points and other wireless threats.

Learning outcome 3.1 formative assessment

1. List at least 3 types of threats can be prevented by a good WIPS

   Answer.

   - Rogue access points
   - Mis-configured AP
   - Client mis-association
   - Unauthorized association
   - Man-in-the-middle attack
   - Ad hoc networks
   - MAC spoofing
   - Honeypot / evil twin attack

2. What is the primary purpose of Wireless intrusion detection (WIDS)

   Answer.

   The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices.

3. How do you understand by protocol analyzer.

   Answer.

   A protocol analyzer (also known as a sniffer, packet analyzer, network analyzer, or traffic analyzer) can capture data in transit for the purpose of analysis and review.

4. What is Network intrusion prevention system?

Answer.

Network Intrusion Prevention System (NIPS) is a type of network security software that detects malicious activity on a network, reports information about said activity, and takes steps to block or stop the activity from occurring automatically.

Learning outcome 3.2 Adjust security system

Duration: 4 hrs

Learning outcome 3.2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Check Virus definition clearly
2. manage power perfectly
3. Use network monitoring systems
4. Manage patches

Resources

Equipment	Tools	Materials
Server Computer Firewall Router Switches UPS	Simulation Internet Antivirus A/C	Books Trainer manual

Advance preparation:

. Trainer should have all resources in place

Indicative content 3.2.1: Patches management, Virus definition checking, Power management and temperature regulation

- **Patches management**

  Patch management is the practice of deploying firmware, driver, operating system (OS), and application updates to your computing endpoints.

  Patch management is critical to keeping systems updated, reducing attack surfaces, and ensuring employee productivity.

  Patch management is the process of applying updates to software, drivers, and firmware to protect against vulnerabilities. Effective patch management also helps ensure the best operating performance of systems, boosting productivity.

  Whether it's an employee laptop or userless PC-based device, such as a kiosk or digital signage, all systems need to be secured. The risks of ignoring patch management can include exposing your business to leaks and breaches, loss of productivity, and loss of reputation.

  Benefits: Why Is Patch Management Important?

  The ultimate goal of patch management is to protect your endpoints from hackers and keep your systems running in top-notch shape. But patch management also confers a number of other benefits:

  - Promote productivity within the organization.
  - Help lower the cost of device lifecycle management and repair
  - Help meet laws, regulations, and compliance standards.

✓ **OS features update**

An Operating System (OS) is an interface between a computer user and computer hardware. An operating system is a software which performs all the basic tasks like file management, memory management, process management, handling input and output, and controlling peripheral devices such as disk drives and printers.

Feature Updates use the same mechanism for monthly updates and will be delivered to Andrew domain-bound computers via Windows Update for Business. The main difference between Feature Updates and ordinary Windows updates will be duration and new Windows features.

Operating system updates contain new software that helps keep your computer current. Examples of updates include service packs, version upgrades, security updates, drivers, or other types of updates. Important and high-priority updates are critical to the security and reliability of your computer.

- **Virus definition checking**

✓ **Installation of anti-viruses**

Antivirus software is like fire extinguishers: You know you need one, but you hope you never have to use it. With all the emerging computer viruses, however, it's important to know how to buy, set up, install, and use antivirus software.

Install the antivirus program

1. If you purchased the antivirus program from a retail store, insert the CD or DVD into the computer's disc drive. The installation process should start automatically, with a window opening to help guide you through the install process.
2. if you downloaded the antivirus program on the Internet, find the downloaded file on your computer. If the downloaded file is a zip file, unzip the file to extract and access the installation files. Look for a file named setup.exe, install.exe, or something similar, then double-click that file. The installation process should start, with a window opening to help guide you through the install process.
3. When the install process is complete, close out of the install window.
4. If used, remove the CD or DVD from the computer's disc drive.
5. The antivirus program is now installed and ready to use. While it may not be required, we recommend restarting your computer so that any modified settings in the operating system can take effect correctly.

✓ **Updating anti-viruses**

Out of the box, antivirus programs are not up-to-date and are missing the latest virus and spyware definitions.

Without the latest definitions, the antivirus program will not know about the most recently created viruses and spyware, making your computer vulnerable to an infection.

After installing the antivirus program, we highly recommend you update it with the latest virus and spyware definitions. The updates allow the antivirus program to protect your computer from all viruses and spyware.

In many cases, the antivirus program automatically checks for and installs the latest updates. If prompted to do so, select Yes to update the antivirus program. If it does not prompt you to update immediately.

How to update an antivirus program.

Enable automatic updates for the antivirus program

1. By default, most antivirus programs enable the automatic update feature. We strongly recommend automatic updates be enabled to keep the antivirus program up-to-date at all times.
2. To check if automatic updates are enabled in your antivirus program, follow the general steps below.
3. Open the antivirus program.
4. Look for a Settings or Advanced Settings button or link in the antivirus program window. If you do not see either option, look for an option like Updates or something similar.
5. In the Settings or Updates window, look for an option like Automatically download and apply updates. It may also refer to virus definitions instead of updates.
6. For the automatic updates option, check the box for that option, if not already checked.
7. Click the Save or Apply button to save the settings change.

- **Power management**

✓ **Use of UPS (uninterruptible Power supply)**

An uninterruptible power supply (UPS) is used to protect critical loads from utility-supplied power problems, including spikes, brownouts, fluctuations and power outages, all using a dedicated battery.

A UPS performs the following functions:

- Absorb relatively small power surges.
- Smooth out noisy power sources.
- Continuously provides power to equipment during line sags.
- Automatically shuts down equipment during long power outages.
- Monitoring and logging of the status of the power supply.
- Display the voltage/current draw of the equipment.
- Restart equipment after a long power outage.
- Display the voltage currently on the power line.
- Provide alarms on certain error conditions.

- Provide short-circuit protection.

The three major types of UPS system configurations are online **double conversion, line-interactive and offline** (also called standby and battery backup). These UPS systems are defined by how power moves through the unit.

- **Temperature regulation**

✓ **Use of Air Conditioning (A/C)**

An *air conditioner cools* your home with a cold indoor coil called the evaporator. The condenser, a hot outdoor coil, releases the collected heat outside. The evaporator and condenser coils are serpentine tubing surrounded by aluminum fins. This tubing is usually made of copper.

An *air conditioner* is a system that is used to cool down a space by removing heat from the space and moving it to some outside area. The cool air can then be moved throughout a building through ventilation.

Air conditioning system can be for **heating, dehumidifying, cooling, and humidifying.**

 **Theoretical learning Activity**

In pair, Discussions on possible way of updating an Antivirus

 Points to Remember (Take home message)

- Patch management is critical to keeping systems updated, reducing attack surfaces, and ensuring employee productivity.
- An Operating System (OS) is an interface between a computer user and computer hardware.
- An uninterruptible power supply (UPS) is used to protect critical loads from utility-supplied power problems, including spikes, brownouts, fluctuations and power outages, all using a dedicated battery.
- An air conditioner cools your home with a cold indoor coil called the evaporator

Learning outcome 3.1 formative assessment

1. What are the four main purposes of air conditioning system?

Answer.
Air conditioning system can be for heating, dehumidifying, cooling, and humidifying.

2. What is a UPS system used for?

Answer.

Uninterruptible power supplies provide backup power, protecting equipment from damage in the event of grid power failure.
An uninterruptible power supply (UPS) is a type of device that powers equipment, nearly instantaneously, in the event of grid power failure, protecting the equipment from damage.

3. Define term Antivirus

Answer.
An antivirus product is a program designed to detect and remove viruses and other kinds of malicious software from your computer or laptop. Malicious software - known as malware - is code that can harm your computers and laptops, and the data on them.

4. Give 3 examples of Antivirus

Answer.
Avast One, Antivirus Business Edition, Bitdefender Total Security, Kaspersky, McAfee, Malwarebytes Premium Plus, Norton Antivirus 360, SecureMac, Trend Micro Antivirus+ Security, and Webroot SecureAnywhere are the top ten antivirus software in 2022

Learning outcome 3.3 Document on current system settings and file for future reference

Duration: 4 hrs

Learning outcome 3.3 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Produce a document on existing security threats and vulnerabilities clearly

2. File a produced documents on existing security threats and vulnerabilities

Resources

Equipment	Tools	Materials
Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual

Advance preparation:

. Trainer should have all resources in place

. Trainer should be make sure that workplace is ready

Indicative content 3.3.1: Produce a document on existing security threats and vulnerabilities

- ✓ **Preliminary development**

Preliminary plans are the initial design phase in preparing the construction bidding documents.

These documents are developed from the information contained in the budget package. Typically, the preliminary plans are developed in two distinct steps referred to as schematics and design development. The two-step process allows the department and architect/engineer to interact before the design is developed, helping to ensure a mutual understanding of the design objectives, limitations and budget.

1. **Schematic documents**: Schematic documents are the initial architectural and engineering plans prepared during the preliminary plan phase, depicting the designer's conceptual solution to project needs. The major difference compared with design documents is the amount of detail.

2. **Design documents**: These are the final documents which result from the preliminary plan phase, defined by Section 3.00 of the Budget Act as a site plan, architectural floor plans, elevations and a cost estimate. For each utility, site development, conversion, and remodeling project, the drawings must be sufficiently descriptive to convey accurately the location, scope, cost, and the nature of the improvement being proposed.

Preliminary means something that comes before something else.

✓ **Development**

- **Current system situation on existing security threats and vulnerabilities.**

- The main types of information security threats are: Malware attack. Social engineering attacks. Software supply chain attacks, Advanced persistent threats (APT), Distributed denial of service (DDoS), Man-in-the-middle attack (MitM) and Password attacks.

- **Conclusion and recommendations**

Today we use internet-connected devices in all aspects of our lives. We go online to search for information, shop, bank, do homework, play games, and stay in touch with family and friends through social networking. As a result, our devices contain a wealth of personal information about us. This may include banking and other financial records, and medical information—information that we want to protect. If your devices are not protected, identity thieves and other fraudsters may be able to get access and steal your personal information. Spammers could use your computer as a "zombie drone" to send spam that looks like it came from you. Malicious viruses or spyware could be deposited on your computer, slowing it down or destroying files.

By using safety measures and good practices to protect your devices, you can protect your privacy and your family. The following tips are offered to help you lower your risk while you're online.

These are the measure to take: Keep your device secure, keep up-to-date, Antivirus software, Antispyware software, Firewalls, Use strong protection, Choose strong passwords, Use stronger authentication, Protect your private information, Be careful what you click, Shop safely, Be careful what you share, Responding to data breaches, etc.

✓ **References**

Reference is the art of mentioning other writers' words, ideas, or information in the course of your own argument. Documentation is the technique of accurately identifying the precise source of others' words, ideas, and information.

Indicative content 3.3.2: File a produced document on existing security threats and vulnerabilities

Archiving is to store historical records or documents in an archive. in computer technology, to store electronic information that you no longer need to use regularly: This software helps firms archive and retrieve emails.

- ✓ **Manual archiving**

Manual archiving provides flexibility, and allows you to specify exactly which folders are included in the archive, and which archive Outlook Data File (.pst) is used. To manually archive Outlook items, do the following: Click the File tab. Click Cleanup Tools.
AutoArchive helps manage the space in your mailbox or on the e-mail server that you are using by automatically moving items to an archive location.

- ✓ **Online Archiving**

Online Archiving enables the user to access their archived email from any location, using the same methods they access their non-archived email. Online Archiving provides the user with a specialized archive mailbox that appears alongside the users' primary mailbox folders in Outlook or Outlook on the Web (OOTW).

The key reason to archive your documents is to avoid losing data. All documents are vulnerable to being destroyed or corrupted (if digital), either maliciously, by accident, or by a natural disaster, such as a flood or fire.

Theoretical learning Activity

In pair, brainstorm on possible components of a preliminary design

Points to Remember (Take home message)

- Preliminary means something that comes before something else.
- Archiving is to store historical records or documents in an archive.
- *The key reason to archive your documents is to avoid losing data.*

Learning outcome 3.3 formative assessment

1. What is archiving

   Answer.

   It is to store historical records or documents in an archive
2. What are not the types of files archive (Select multiple)?
   a. RAR Files.
   b. GIF
   c. Zip Files.
   d. 7Z Files.
   e. PNG
   f. TAR GZ Files.
   g. ISO Files.
3. Define Preliminary plan

   Answer.

   Preliminary plans are the initial design phase in preparing the construction bidding documents.

Learning outcome 3.3.4 Document newly discovered security threats, vulnerabilities and risks in a report.

Duration: 3 hrs

Learning outcome 3.4 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Produce a document on new security threats and vulnerabilities perfectly

2. Produce a document on suggested mitigation and deterrent techniques perfectly

Resources

Equipment	Tools	Materials

Server Computer Firewall Router Switches	Simulation Internet	Books Trainer manual
 **Advance preparation:** . Trainer should have all resources in place		

Indicative content 3.4.1: Produce a document on new security threats and vulnerabilities

✓ **Preliminary development**

Preliminary plans are the initial design phase in preparing the construction bidding documents. We have two (2) main kind of producing document: *Schematic and design documents.*

Preliminary means something that comes before something else.

✓ **Development**

Current system situation on existing security threats and vulnerabilities.

- The main types of information security threats are: Malware attack. Social engineering attacks. Software supply chain attacks, Advanced persistent threats (APT), Distributed denial of service (DDoS), Man-in-the-middle attack (MitM) and Password attacks.

Conclusion and recommendations

Today we use internet-connected devices in all aspects of our lives. We go online to search for information, shop, bank, do homework, play games, and stay in touch with family and friends through social networking.

By using safety measures and good practices to protect your devices, you can protect your privacy and your family. The following tips are offered to help you lower your risk while you're online.

- ✓ **References**

  Reference is the art of mentioning other writers' words, ideas, or information in the course of your own argument. Documentation is the technique of accurately identifying the precise source of others' words, ideas, and information.

  - **Produce a document on suggested mitigation and deterrent techniques.**

Produce a document is The process of delivering, or making available for review, documents in response to a request for documents, such as a request for production and a subpoena. A request for documents may call for the production of paper (hard copy) documents and electronically stored information (ESI).

There are four types of production forms: native, near-native, image (near-paper), and paper.

- ✓ **Preliminary development**
- ✓ **Development**
  - Current system situation on existing security threats and vulnerabilities
  - Conclusion and recommendations
- ✓ **References**

Reference is the art of mentioning other writers' words, ideas, or information in the course of your own argument.

 **Theoretical learning Activity**

Trainees in pair, brainstorm about **Schematic documents and design documents**

 Points to Remember (Take home message)

- Produce a document is The process of delivering, or making available for review, documents in response to a request for documents, such as a request for production and a subpoena.

Learning outcome 3.4 formative assessment

1. What is a technical report?

   Answer.

   A technical report is a formal report designed to convey technical information in a clear and easily accessible format. It is divided into sections which allow different readers to access different levels of information.

2. Define a reference

   Answer.

   It gives the readers details about the source so that they have a good understanding of what kind of source it is and could find the source themselves if necessary. The references are typically listed at the end of the lab report.

   The references are typically listed at the end of the lab report.

Summative Assessment

Integrated situation	Resources
Dragon Finance Company is an institution which is located in Kigali City, KICUKIRO District. It has a flat network environment with computers in different departments. One user in finance department is using an XP machine with access to internet. As there is no neither traffic in/out filtering or web filtering, that user likes much surfing websites with adult contents. One morning when he was busy working he received internet popup message telling him that his computer might be at risk with a proposal to install a quick malware scanner tool. As that user had administrative privileges on that computer he installed the tool and after 1 minutes he saw a warning message displayed on his screen that his computer data have been encrypted and to get them back he has to pay a ransom of 1000$. That user became very frightened and left his computer and goes to coffee	Internet Antivirus Firewall IDS Computer Vulnerabilities scanning tools Electricity UPS Router switcher

break and kept silent. After 15 minutes, every computer and server on the company network was showing the same message and all company data was encrypted. Please identify possible vulnerabilities and different types of threats in this situation. If you are called by this institution as an IT Support technician, what support can you provide to this institution to resume their business after this incident? The task should be accomplished in 3 hours and then the work report should be submitted to the General Director of the company.	

Assessment Criterion 1: Quality of Process

	Checklist	Score	
		Yes	**No**
	Indicator: Assess and report on current system security are done		
✓	Security fundamentals		
	Indicator: System security threats and vulnerabilities are identified		
✓	Security threats and vulnerabilities		
	Indicator: Threats and vulnerability are mitigated		
✓	General methods to mitigate common security threats to the network		
✓	Common security appliances and applications		
✓	Security recommended practices		
	Indicator: Suggest the best practice server and network hardening techniques and measures		
✓	Installation and configuration of security controls when performing account management based on best practices		
	Indicator: Recommendations to management to address security is made		
✓	Installation and configuration of security controls when performing account management, based on best practices		
	Indicator: Required level of security is established		
✓	Implementation of compliance and operational security		
	Indicator: Best practice server and network hardening techniques and measures are applied		
✓	Implementation of network security		

	Indicator: Implement secure authentication and user account controls Creation of an account		
✓	Risk management identification		
✓	Risk Analysis		
✓	Vulnerability scanning and penetration testing tools		
✓	Mitigation and Deterrent Technique		
	Indicator: Current network security is monitored		
✓	Usage of network analysis tools		
✓	Usage of intrusion detection and prevention systems		
✓	Usage of network monitoring systems		
	Indicator: Security system is adjusted		
✓	Patches management		
✓	Virus definition checking		
✓	Power management		
✓	Temperature regulation		
	Indicator: Current system settings and file for future reference is documented		
✓	Produce a document on new security threats and vulnerabilities		
✓	Produce a document on suggested mitigation and deterrent techniques		
	Observation		

Assessment Criterion 2: Quality of product

Checklist		Score	
		Yes	**No**
	Indicator: Necessary Software are used		
✓	OS features update		
✓	Installation of anti-virus		
✓	Updating anti-virus		
	Indicator: Network is secured		
✓	No popup messages		
	Indicator: authentication and user account controls are created		
✓	Privileges are set		
	Observation		

Assessment Criterion 3: Relevance

Checklist	Score	
	Yes	**No**
Indicator: Devices are well kept		
✓ Computer		
✓ Router		
✓ Switch		
Indicator: The time is respected		
✓ Time required(3h)		
Indicator: The report is Produced		
✓ Report format		
✓ Report content		
Observation		

References:

BOOKS

Joxean Koret, E. B. (2023). The Antivirus Hacker's Handbook. In E. B. Joxean Koret, *The Antivirus Hacker's Handbook.* 17 August 2015. Retrieved from The Antivirus Hacker's Handbook.

Morpus, N. (2023, April 19). Retrieved from Digital: https://digital.com/best-vpn-services/what-is-a-network-intrusion-prevention-system/

Wiley. (2023, April 20). Retrieved from O'REILLY: https://www.oreilly.com/library/view/the-antivirus-hackers/9781119028758/

WEBSITES

(2023, April 20). Retrieved from Bitwarded: https://bitwarden.com/blog/how-long-should-my-password-be/#:~:text=In%20fact%2C%20the%20National%20Institute,least%2014%20to%2016%20characters

(2023, April 20). Retrieved from FORDHAM UNIVERSITY: https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/generic-accounts-policy/#:~:text=Generic%20Account%20use%20is%20prohibited,on%20justification%20and%20appropriate%20need.

(2023, April 20). Retrieved from Restorepoint: https://www.restorepoint.com/topics/network-security-best-practices#

(2023, April 20). Retrieved from StarTeamServer Administration: https://www.microfocus.com/documentation/starteam/163/en/Help/SvrAdmin/STARTEAM-3AC54381-GROUPPRIVILIGES-REF.html

(2023, April 20). Retrieved from Ivanti: https://help.ivanti.com/ap/help/en_US/am/2020/Content/Application_Manager/User_Privileges.htm#:~:text=A%20privilege%20is%20the%20right,or%20deny%20(disable)%20privileges.

(2023, April 20). Retrieved from Tenfold: https://www.tenfold-security.com/en/user-access-review/#:~:text=OK%2C%20So%20What%20Is%20a,to%20both%20cybersecurity%20and%20compliance.

(2023, April 19). Retrieved from Growdstrike: https://www.crowdstrike.com/cybersecurity-101/observability/continuous-monitoring/#:~:text=Continuous%20monitoring%20is%20an%20approach,time%20to%20address%20them%20quickly.

(2023, April 19). Retrieved from Deligent: https://www.diligent.com/insights/legal-compliance/steps-evaluating-legal-compliance/#:~:text=Legal%20compliance%20is%20the%20process,practices%20in%20a%20particular%20jurisdiction.

(2023, April 19). Retrieved from CaseWare: https://documentation.caseware.com/latest/Audit/en/Content/User_Risk_Assessment_and_Identification/Controls/c_Control_Identification.htm#:~:text=As%20part%20of%20the%20engagement,and%20report%20on%20any%20deficiencies.

(2023, April 19). Retrieved from WhatIs.com: https://www.techtarget.com/whatis/definition/network-intrusion-protection-system-NIPS#:~:text=A%20network%20intrusion%20protection%20system,unauthorized%20access%20and%20malicious%20activity.

(2023, April 19). Retrieved from Techslang: https://www.techslang.com/definition/what-is-signature-based-detection/#:~:text=Signature%2Dbased%20detection%20is%20a,%2C%20Trojans%2C%20and%20many%20others.

(2023, April 19). Retrieved from Intel: https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/patch-management.html#:~:text=Patch%20management%20is%20the%20practice,surfaces%2C%20and%20ensuring%20employee%20productivity.

(2023, April 20). Retrieved from ENERGY SAVER: https://www.energy.gov/energysaver/air-conditioning#:~:text=An%20air%20conditioner%20cools%20your,is%20usually%20made%20of%20copper.

(2023, April 20). Retrieved from Computer Hope: https://www.computerhope.com/issues/ch001922.htm