# Competency Based Learning Material (CBLM)

# IT Support Service

## Level-4

## Module: Maintaining Network Security

**Code: CBLM-ICT-ITSS-05-L4-V1**

**National Skills Development Authority**
**Prime Minister's Office**
**Government of the People's Republic of Bangladesh**

## Copyright

National Skills Development Authority
Prime Minister's Office
Level: 10-11, Biniyog Bhaban,
E-6 / B, Agargaon, Sher-E-Bangla Nagar Dhaka-1207, Bangladesh.
Email: ec@nsda.gov.bd
Website: www.nsda.gov.bd.
National Skills Portal: http:\\skillsportal.gov.bd

This Competency-Based Learning Materials (CBLM) on "Maintaining Network Security" under the IT Support Service, Level-4" qualification is developed based on the national competency standard approved by the National Skills Development Authority (NSDA)

This document is to be used as a key reference point by the competency-based learning materials developers, teachers/trainers/assessors as a base on which to build instructional activities.



It serves as the document for providing training consistent with the requirements of the industry to meet the qualification of individuals who graduated through the established standard via competency-based assessment for a relevant job.

This document has been developed by NSDA with the assistance of a related specialist/trainer /related employee

Public and private institutions may use the information contained in this CBLM for activities benefitting Bangladesh.

Approved by _____ th Authority meeting held on .....

# How to use this Competency-Based Learning Material (CBLM)

The module, Maintaining Network Security contains training materials and activities for you to complete. These activities may be completed as part of structured classroom activities or you may be required to work at your own pace. These activities will ask you to complete associated learning and practice activities to gain the knowledge and skills you need to achieve the learning outcomes.

1. Review the **Learning Activity** page to understand the sequence of learning activities you will undergo. This page will serve as your road map towards the achievement of competence.

2. Read the **Information Sheets.** This will give you an understanding of the jobs or tasks you are going to learn how to do. Once you have finished reading the **Information Sheets** complete the questions in the **Self-Check.**

3. **Self-checks** are found after each **Information Sheet**. **Self-checks** are designed to help you know how you are progressing. If you are unable to answer the questions in the **Self-Check** you will need to re-read the relevant **Information Sheet**. Once you have completed all the questions check your answers by reading the relevant **Answer Keys** found at the end of this module.

4. Next move on to the **Job Sheets. Job Sheets** provide detailed information about *how to do the job* you are being trained in. Some **Job Sheets** will also have a series of **Activity Sheets**. These sheets have been designed to introduce you to the job step by step. This is where you will apply the new knowledge you gained by reading the Information Sheets. This is your opportunity to practice the job. You may need to practice the job or activity several times before you become competent.

5. **Specification sheets**, specifying the details of the job to be performed will be provided where appropriate.

6. A review of competency is provided on the last page to help remind you if all the required assessment criteria have been met. This record is for your information and guidance and is not an official record of competency.

When working through this Module always be aware of your safety and the safety of others in the training room. Should you require assistance or clarification please consult your trainer or facilitator.

When you have satisfactorily completed all the Jobs and/or Activities outlined in this module, an assessment event will be scheduled to assess if you have achieved competency in the specified learning outcomes. You will then be ready to move on to the next Unit of Competency or Module

# Table of Contents

# Module Content

| | |
|---|---|
| **Unit of Competency** | **Maintain Network Security** |
| **Unit Code** | **OU-ICT-ITSS-05-L4-V1** |
| **Module Title** | **Maintaining Network Security** |
| Module Descriptor | This module covers the knowledge, skills, and attitudes required to maintain network security.<br>It includes the task of interpreting network security, configuring firewall services monitoring the threat, and documenting and reporting the threat |
| Nominal Hours | 40 Hours |
| **Learning** Outcome | After completing the practice of the module, the trainees will be able to perform the following jobs:<br>1. Interpret network security<br>2. Configure firewall services<br>3. Monitor the threat<br>4. Document and report the threat |

**Assessment Criteria**

1. Network security is defined
2. Types of network security is defined
3. Network security control is interpreted
4. Common network security Vulnerabilities are interpreted
5. Network attack architecture is interpreted
6. Search engine privacy is interpreted
7. Browser security and tracking prevention are interpreted
8. Network security best practices are interpreted
9. Security is ensured using a network administration tool
10. Filter rules are configured as per requirement
11. Mangle/Packet Filtering is configured as per the requirement
12. Security services are configured as per requirement
13. Access Control List (ACL) is configured as per requirement
14. A possible security threat is identified.
15. Possible cause of infection is determined
16. Identified security threat is monitored to find out its characteristics with network monitoring tools.
17. The capability of the security threat is determined from the analysis.
18. Network device hardening is interpreted
19. Network attack prevention is interpreted
20. Report is prepared using the monitoring system
21. The report is documented and submitted to the authority

**Learning Outcome-**1: **Interpret Network Security**

| | |
|---|---|
| Assessment Criteria | 1. Network security is defined<br>2. Types of network security is defined<br>3. Network security control is interpreted<br>4. Common network security Vulnerabilities are interpreted<br>5. Network attack architecture is interpreted<br>6. Search engine privacy is interpreted<br>7. Browser security and tracking prevention are interpreted<br>8. Network security best practices are interpreted |
| Conditions and Resources | 1. Actual workplace or training environment<br>2. CBLM<br>3. Handouts<br>4. Laptop/ Desktop<br>5. Multimedia Projector<br>6. Paper, Pen, Pencil, and Eraser<br>7. Internet Facilities<br>8. Whiteboard and Marker |
| Contents | 1. Network security<br>2. Type of network security -<br>▪ Physical<br>▪ Technical<br>▪ Administrative<br>▪ Authentication and access control<br>▪ Wireless access point control<br>3. Common network security Vulnerabilities<br>▪ Improperly installed hardware or software<br>▪ Operating systems or firmware that have not been updated<br>▪ Misused hardware or software<br>▪ Poor or a complete lack of physical security<br>▪ Insecure password<br>▪ Design flaws in a device's operating system in the network<br>4. Network security best practices<br>5. Network attack architecture<br>▪ Human exploits<br>▪ Social engineering<br>▪ Denial of service<br>▪ Wireless attack<br>▪ Man in the middle attack<br>▪ Password Attack<br>▪ Wireless attack |

| | |
|---|---|
| | 6. Search engine privacy<br>7. Browser security and tracking |
| Activities/job/Task | 1. Conduct interviews with key stakeholders (department heads, IT staff, users) to understand their current and future network needs.<br>2. Review existing documentation like network diagrams, policies, and service level agreements (SLAs) to understand the current network infrastructure and its limitations.<br>3. Analyze the existing network topology (star, mesh, etc.) to assess its scalability and suitability for expansion |
| Training Methods | 1. Blended<br>2. Discussion<br>3. Presentation<br>4. Demonstration<br>5. Guided Practice<br>6. Individual Practice<br>7. Project Work<br>8. Problem Solving<br>9. Brainstorming |
| Assessment Methods | Assessment methods may include but are not limited to<br>1. Written Test<br>2. Demonstration<br>3. Oral Questioning<br>4. Portfolio |

## Learning Experience-1: Interpret Network Security

To achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

| Learning Activities | Recourses/Special Instructions |
|---|---|
| 1. Students will ask the instructor about "Interpret network security." | 1. Instructor will provide the learning materials "Interpret network security." |
| 2. Read the Information sheet and complete the Self-check & Check answer sheets on "Interpret network security." | 2. Read Information sheet:<br>a. Network security<br>b. Type of network security<br>c. Common network security Vulnerabilities<br>d. Network security best practices<br>e. Network attack architecture<br>f. Search engine privacy<br>g. Browser security and tracking<br>3. Answer Self-check 1: Interpret network security.<br>4. Check your answer with Answer key 1: Interpret network security |
| 3. Read the Job/Task Sheet and Specification Sheet and perform the job/Task | 5. Job/Task Sheet and Specification Sheet |

# Information Sheet-1: Interpret Network Security.

**Learning Objective:**

After completion of this information sheet, the learners will be able to explain, define, and interpret the following contents:

1.1 Network security.
1.2 Type of network security -
- Physical
- Technical
- Administrative
- Authentication and access control
- Wireless access point control

1.3 Common network security Vulnerabilities
- Improperly installed hardware or software
- Operating systems or firmware that have not been updated.
- Misused hardware or software
- Poor or a complete lack of physical security
- Insecure password
- Design flaws in a device's operating system in the network.

1.4 Network security best practices.
1.5 Network attack architecture.
- Human exploits
- Social engineering
- Denial of service
- Wireless attack
- Man in the middle attack.
- Password Attack
- Wireless attack

1.6 Search engine privacy.
1.7 Browser security and tracking

## 1.1 Network security

Network Security protects your network and data from breaches, intrusions, and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.

Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, and wireless), firewalls, VPN encryption, and more.

**Aspects of Network Security**

The following are the desirable properties to achieve secure communication:

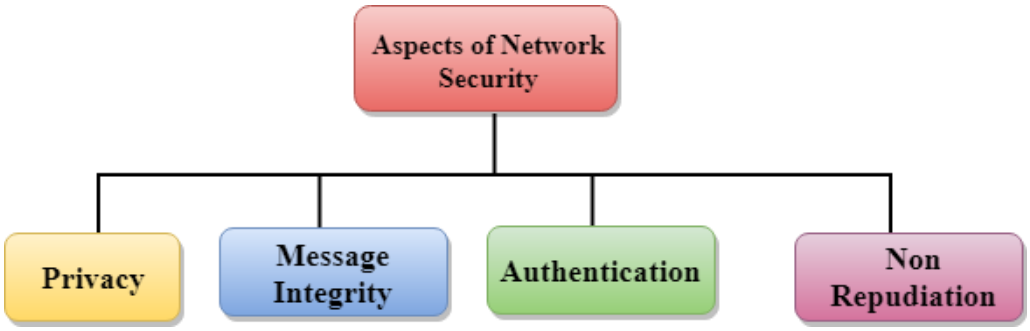



Figure 1: Network Security

- **Privacy:** Privacy means both the sender and the receiver expect confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
- **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accidentally, in transit. As there are more and more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.
- **End-point authentication:** Authentication means that the receiver knows the sender. identity, i.e., no imposter has sent the message.
- **Non-Repudiation:** Non-Repudiation means that the receiver must prove that the received message has come from a specific sender. The sender must not deny sending a message that he or she sent. The burden of proving the identity comes to the receiver. For example, if a customer requests to transfer money from one account to another, the bank must have proof that the customer has requested the transaction.

## 1.2 Type of network security

### Physical Network Security

Physical network security refers to the measures and mechanisms put in place to protect the physical infrastructure of a network from unauthorized access, damage, or interference. It involves safeguarding the hardware, cables, equipment, and other physical components that make up a network.

Here are some common elements of physical network security:

- **Secured Access Points:** This involves controlling physical access to network devices such as routers, switches, and servers. Access should be restricted to authorized

personnel only, typically through measures like keycards, biometric scanners, or security guards.

- Perimeter Security: This includes fencing, gates, locks, and other physical barriers to prevent unauthorized individuals from gaining physical access to network facilities.
- Surveillance Systems: Video cameras and other monitoring devices can be used to keep an eye on critical areas and detect any unauthorized access or suspicious activity.
- Environmental Controls: Ensuring that network equipment is housed in environments with appropriate temperature, humidity, and ventilation levels to prevent damage or malfunction.
- Cable Security: Protecting network cables from tampering, theft, or damage. This can involve using cable locks, conduits, or secure enclosures.
- Equipment Protection: Safeguarding network devices and servers from physical damage, theft, or tampering. This may involve locking server rooms or cabinets, using equipment enclosures, or employing security seals.
- Disaster Preparedness: Implementing measures to protect network infrastructure from natural disasters, such as earthquakes, floods, or fires.

**Technical Network Security**

Technical network security refers to the use of technology and software-based solutions to protect a network from unauthorized access, data breaches, and other cyber threats. Unlike physical network security, which focuses on safeguarding the physical components of a network, technical network security involves implementing various technological measures to secure the digital aspects of a network. Here are some common technical network security measures:

- **Firewalls**: Firewalls are essential network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between a trusted internal network and untrusted external networks, such as the Internet.
- **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** IDS and IPS solutions monitor network traffic for suspicious activity or potential security breaches. IDS systems detect and alert administrators to potential threats, while IPS systems can take automated action to block or prevent malicious traffic.
- **Virtual Private Networks (VPNs):** VPNs provide secure remote access to a network by encrypting the communication between the user's device and the network. They are commonly used to establish secure connections over public networks, such as the Internet.
- **Access Control Lists (ACLs):** ACLs are used to control which users or devices are allowed to access specific resources on a network. They can be implemented on routers, switches, and other network devices to enforce security policies.
- **Encryption:** Encryption is the process of encoding data in such a way that only authorized parties can access it. It is used to protect sensitive information as it travels across a network, preventing unauthorized interception or eavesdropping.

- **Authentication Mechanisms:** Authentication mechanisms, such as passwords, biometrics, and two-factor authentication (2FA), are used to verify the identity of users and devices before granting them access to the network.
- **Vulnerability Management:** Vulnerability management involves identifying, prioritizing, and mitigating security vulnerabilities in network devices and software to reduce the risk of exploitation by attackers.
- **Security Information and Event Management (SIEM):** SIEM solutions collect, analyze, and correlate security event data from various sources across the network to provide comprehensive visibility into potential security incidents and threats.
- **Endpoint Security:** Endpoint security solutions protect individual devices, such as computers, smartphones, and tablets, from malware, phishing attacks, and other threats that may originate from network connections.

**Administrative Network Security**

Administrative network security involves the policies, procedures, and practices implemented by an organization to manage and govern the security of its network infrastructure. While technical and physical security measures focus on the technological and physical aspects of security, administrative security focuses on the human and procedural aspects. Here are some key components of administrative network security:

- Security Policies and Standards: Establishing comprehensive security policies and standards that outline the organization's security objectives, expectations, and requirements. These policies should cover areas such as access control, data protection, incident response, and acceptable use of resources.
- Risk Management: Conducting risk assessments to identify potential security risks and vulnerabilities within the network infrastructure. Risk management processes help prioritize security efforts and allocate resources effectively to mitigate identified risks.
- Security Awareness Training: Providing security awareness training and education to employees to help them recognize and respond to security threats effectively. Training programs should cover topics such as phishing awareness, password hygiene, and social engineering tactics.
- Access Control and User Management: Implementing access control mechanisms to restrict access to network resources based on the principle of least privilege. This involves managing user accounts, permissions, and privileges to ensure that only authorized individuals have access to sensitive information and systems.
- Change Management: Implementing change management processes to control and track changes made to the network infrastructure. Changes to configurations, software updates, and patches should be carefully planned, documented, and tested to minimize the risk of introducing security vulnerabilities.
- Incident Response and Reporting: Establishing incident response procedures to detect, investigate, and respond to security incidents in a timely and effective manner. This includes defining roles and responsibilities, establishing communication channels, and documenting incident response procedures.

- Compliance and Regulatory Requirements: Ensuring compliance with relevant laws, regulations, and industry standards related to network security. This may include regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), or industry-specific standards like the Payment Card Industry Data Security Standard (PCI DSS).
- Security Audits and Assessments: Conduct regular security audits and assessments to evaluate the effectiveness of existing security controls and identify areas for improvement. External audits may also be conducted by third-party organizations to validate compliance with regulatory requirements and industry standards.
- Security Governance: Establishing a security governance framework to provide oversight and accountability for security-related decisions and activities. This includes defining roles and responsibilities, establishing reporting structures, and ensuring alignment with business objectives.

**Authentication and access control**

Authentication and access control are fundamental components of network security that work together to ensure that only authorized users and devices can access resources within a network. Here's an overview of each:

- **Authentication:** Authentication is the process of verifying the identity of a user or device attempting to access a network or a specific resource within a network. It ensures that only legitimate users are granted access to authorized services or data. Authentication typically involves the following methods:
  - **Passwords**: The most common form of authentication, where users provide a unique combination of characters known only to them.
  - **Biometrics**: Using physical characteristics such as fingerprints, iris scans, or facial recognition to authenticate users.
  - **Two-factor authentication (2FA) and Multi-Factor Authentication (MFA):** Adding a layer of security by requiring users to provide two or more forms of authentication, such as a password and a one-time code sent to their mobile device.
  - **Certificates:** Using digital certificates issued by a trusted Certificate Authority (CA) to verify the identity of users or devices.
  - **Token-based authentication:** Utilizing physical or virtual tokens, such as smart cards or security tokens, to generate one-time passwords for authentication.

- **Access Control:**

Access control refers to the process of restricting or granting access to resources based on the identity and permissions of users or devices. It ensures that users only have access to the resources they are authorized to use and prevents unauthorized access to sensitive information. Access control mechanisms include:

- **Role-Based Access Control (RBAC):** Assigning permissions to users based on their roles within the organization. Users are granted access rights based on their job responsibilities.
- **Discretionary Access Control (DAC**): Allowing resource owners to determine who has access to their resources and what level of access is granted.
- **Mandatory Access Control (MAC):** Implementing a centralized policy that determines access permissions based on security labels assigned to users and resources.
- **Attribute-Based Access Control (ABAC):** Granting access based on various attributes such as user roles, location, time of access, and other contextual factors.
- **Access Control Lists (ACLs):** Lists of permissions attached to resources that specify which users or groups are granted or denied access to those resources.

**Wireless access point control**

Wireless Access Point (WAP) control refers to the management and security measures implemented to regulate and secure access to wireless networks provided by access points. Here are some key aspects of WAP control:

**Access Point Placement and Configuration:**

- Proper placement of access points to ensure adequate coverage while minimizing signal leakage outside the intended area.
- Configuration of access point settings such as SSID (Service Set Identifier), encryption methods (e.g., WPA2-PSK, WPA3), and transmission power to optimize performance and security.

**Authentication and Encryption:**

- Implementation of strong authentication methods such as WPA2-Enterprise or WPA3-Enterprise, which use a RADIUS server for centralized authentication.
- Encryption of wireless communications using protocols like WPA2-AES or WPA3-SAE to protect data transmitted over the wireless network from eavesdropping and unauthorized access.

**Network Segmentation:**

- Segmentation of wireless networks into separate VLANs (Virtual Local Area Networks) to isolate different types of traffic (e.g., guest network, employee network) and restrict access between them.
- Use of VLAN tagging and trunking to ensure that traffic from different VLANs remains separate and secure.

**Rogue Access Point Detection:**

- Implementation of tools and techniques to detect and mitigate unauthorized access points (rogue APs) that may be deployed within the network without proper authorization.
- Regular scanning and monitoring of the wireless environment to identify rogue APs and take appropriate action to remove them.

**Access Control Policies:**

- Enforcement of access control policies to regulate which devices and users are allowed to connect to the wireless network.
- Use of MAC address filtering, which allows only devices with approved MAC addresses to connect to the network.
- Integration with identity management systems and directory services to enforce user-based access policies.

**Intrusion Detection and Prevention:**

- Deployment of intrusion detection and prevention systems (IDPS) to monitor wireless network traffic for signs of malicious activity or security breaches.
- Automatic or manual blocking of suspicious devices or traffic to prevent unauthorized access or attacks.

**Firmware Updates and Patch Management:**

- Regular updates and patch management for access point firmware to address known vulnerabilities and ensure that devices are running the latest security patches.
- Implementation of a patch management process to systematically update access point firmware without disrupting network operations.

By implementing robust WAP control measures, organizations can ensure the security, reliability, and performance of their wireless networks, protecting sensitive information and resources from unauthorized access and cyber threats.

## 1.3 Common network security Vulnerabilities

What Is A Network Vulnerability?

A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach. Nonphysical network vulnerabilities typically involve software or data. For example, an operating system (OS) might be vulnerable to network attacks if it's not updated with the latest security patches. If left unpatched a virus could infect the OS, the host that it's located on, and potentially the entire network.

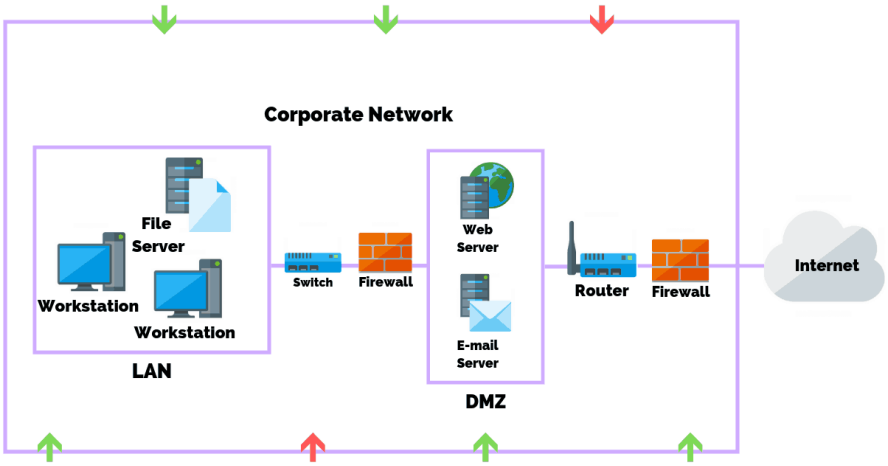



**Figure 2: Common network security Vulnerabilities**

Physical network vulnerabilities involve the physical protection of an asset such as locking a server in a rack closet or securing an entry point with a turnstile.

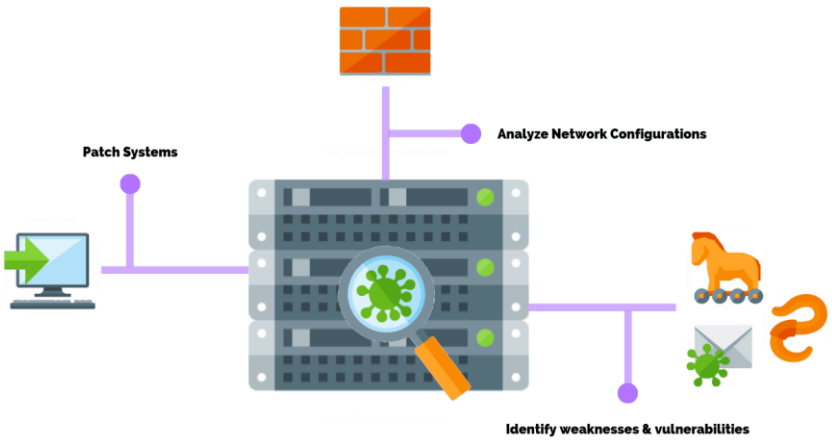
Servers have some of the strongest physical security controls in place as they contain valuable data and trade secrets or perform a revenue-generating function like a web server hosting an eCommerce site. Often stored in off-site data centers or secure rooms, servers should be protected with personalized access cards and biometric scanners. Before investing in security controls, a vulnerability risk assessment is performed to quantify the cost and acceptable loss of the equipment and its function. As with all things in cyber security, it's a balancing act of resources vs functionality that makes for the most practical solutions.

**Different Types of Network Vulnerabilities:**

Network vulnerabilities come in many forms, but the most common types are:

- Malware, short for malicious software, such as Trojans, viruses, and worms that are installed on a user's machine or a host server.
- Social engineering attacks that fool users into giving up personal information such as a username or password.
- Outdated or unpatched software that exposes the systems running the application and potentially the entire network.

- Misconfigured firewalls / operating systems that allow or have default policies enabled.




Your network security team must address these factors when assessing the overall security posture of your systems.

**Improperly installed hardware or software**

Improperly installed hardware or software can introduce various network security vulnerabilities, potentially leading to unauthorized access, data breaches, and service disruptions. Here are some common network security vulnerabilities associated with improperly installed hardware or software:

- Default Configurations: Many hardware devices and software applications come with default configurations that are often insecure. Failure to change default passwords, enable security features, or adjust default settings can leave the network vulnerable to attacks.

- Unpatched Software: Failing to apply patches and updates to software applications and operating systems can leave them vulnerable to known security vulnerabilities. Attackers often exploit unpatched software to gain unauthorized access to networks and compromise systems.

- Insecure Protocols and Services: Improperly configured network protocols and services can create security vulnerabilities. For example, enabling outdated and insecure protocols such as Telnet or FTP without encryption exposes sensitive data to interception and unauthorized access.

- Lack of Access Controls: Inadequate access controls, such as weak authentication mechanisms or overly permissive permissions, can result in unauthorized users gaining access to network resources. This may include granting excessive privileges to users or failing to enforce proper authentication requirements.

**Operating systems or firmware that have not been updated.**

Operating systems or firmware that have not been updated pose significant network security vulnerabilities, as they often contain known security flaws that can be exploited by attackers. Here are some common network security vulnerabilities associated with outdated operating systems or firmware:

- Unpatched Vulnerabilities: Operating systems and firmware contain vulnerabilities that are discovered over time. Software vendors release patches and updates to fix these vulnerabilities and improve security. Failure to apply these patches leaves systems vulnerable to exploitation by attackers who can exploit known weaknesses to gain unauthorized access or compromise systems.

- Malware Infections: Outdated operating systems and firmware are more susceptible to malware infections. Malicious software, such as viruses, worms, and ransomware, often targets known vulnerabilities in operating systems and firmware to infect devices and spread across networks. Once infected, malware can steal sensitive data, disrupt network operations, or provide attackers with unauthorized access to network resources.

- Data Breaches: Vulnerable operating systems and firmware increase the risk of data breaches. Attackers can exploit unpatched vulnerabilities to gain unauthorized access to sensitive information stored on network devices, such as servers, workstations, and storage systems. Data breaches can result in financial losses, reputational damage, and legal liabilities for organizations.

- Denial of Service (DoS) Attacks: Outdated operating systems and firmware are more susceptible to denial of service (DoS) attacks. Attackers can exploit vulnerabilities to launch DoS attacks against network devices, such as routers, switches, and servers, causing them to become unresponsive or crash. DoS attacks can disrupt network services, degrade performance, and impact business operations.

**Misused hardware or software**

Misused hardware or software can introduce various network security vulnerabilities, potentially leading to unauthorized access, data breaches, and service disruptions. Here are some common network security vulnerabilities associated with misused hardware or software:

- Weak Passwords: Failure to use strong, unique passwords for hardware devices, software applications, and user accounts can make them susceptible to brute-force attacks and unauthorized access. Users may also misuse passwords by sharing them or using easily guessable passwords, further increasing the risk of compromise.

- Improper Access Controls: Misconfiguration of access controls, such as file permissions, user privileges, and network policies, can lead to unauthorized access to sensitive data and resources. Users may be granted excessive permissions or privileges, allowing them to access or modify data beyond their role or responsibility.

- Unnecessary Services and Ports: Running unnecessary services or opening unnecessary ports on hardware devices and software applications increases the attack surface and provides potential entry points for attackers. Misused hardware or software may have default services enabled or unused ports left open, exposing them to exploitation.

- Lack of Encryption: Failure to encrypt sensitive data in transit and at rest can result in data exposure and unauthorized access. Misused hardware or software may transmit or store sensitive information without encryption, making it vulnerable to interception or theft by attackers.

- Failure to Update or Patch: Neglecting to update hardware firmware, operating systems, and software applications with the latest security patches and updates leaves them vulnerable to known vulnerabilities and exploits. Misused hardware or software may be left unpatched, exposing them to security risks and exploitation.

- Misconfigured Firewalls and Security Devices: Misconfiguring firewalls, intrusion detection/prevention systems, and other security devices can weaken network defenses and allow unauthorized traffic to pass through. Misused hardware or software may have overly permissive firewall rules or inadequate security settings, compromising network security.

- Social Engineering Attacks: Users may be manipulated or deceived into disclosing sensitive information or performing actions that compromise network security. Social engineering attacks, such as phishing, pretexting, and impersonation, exploit human vulnerabilities to gain unauthorized access to hardware or software systems.

- Physical Security Breaches: Failure to secure hardware devices physically can result in theft, tampering, or unauthorized access. Misused hardware may be left unattended in insecure locations, allowing physical attackers to gain access to sensitive information or compromise the integrity of systems.

**Poor or a complete lack of physical security**

Poor or a complete lack of physical security can result in various network security vulnerabilities, potentially leading to unauthorized access, data breaches, and service disruptions. Here are some common network security vulnerabilities associated with poor physical security:

- Unauthorized Access to Hardware Devices: Lack of physical security measures, such as locks, access control systems, and surveillance cameras, can result in unauthorized individuals gaining physical access to hardware devices, such as servers, routers, and switches. Attackers may exploit this access to tamper with hardware components, install malicious software, or steal sensitive data.

- Theft of Hardware Devices: Unsecured hardware devices are susceptible to theft, which can result in loss of sensitive information, disruption of network services, and financial losses for organizations. Stolen hardware devices may contain valuable data or provide access to critical network infrastructure, allowing attackers to compromise network security.

- Tampering with Network Infrastructure: Attackers may physically tamper with network infrastructure, such as cables, connectors, and network switches, to intercept or manipulate network traffic. This can result in data interception, man-in-the-middle attacks, or disruption of network communications.

- Physical Damage to Hardware: Lack of physical security measures can expose hardware devices to damage from environmental factors, such as water, heat, dust, or power surges. Physical damage to hardware devices can lead to hardware failures, data loss, and service outages, impacting business operations.

- Installation of Rogue Hardware Devices: Without proper physical security controls, attackers may install rogue hardware devices, such as unauthorized access points or network taps, within the network infrastructure. Rogue hardware devices can be used to intercept network traffic, bypass security controls, or launch attacks against network resources.

- Social Engineering Attacks: Attackers may exploit physical security weaknesses to gain unauthorized access to secure areas or manipulate employees into providing access to hardware devices or sensitive information. Social engineering techniques, such as tailgating, impersonation, or phishing, can be used to deceive employees and bypass physical security measures.

- Compromise of Physical Security Credentials: Inadequate protection of physical security credentials, such as keys, access cards, or PINs, can result in their theft, loss, or unauthorized duplication. Compromised physical security credentials can be used by attackers to gain unauthorized access to secure areas or sensitive information.
- Securing hardware devices in locked cabinets, server rooms, or data centers.
- Implementing access control systems, surveillance cameras, and alarm systems to monitor and control access to secure areas.
- Restricting access to sensitive hardware devices and network infrastructure to authorized personnel only.

- Requiring users to create complex passwords that are at least eight characters long and include a mix of uppercase and lowercase letters, numbers, and special characters.
- Enforcing password expiration and rotation policies to ensure that passwords are regularly updated and not reused across multiple accounts.
- Implementing multi-factor authentication (MFA) or two-factor authentication (2FA) to add an extra layer of security beyond passwords.
- Educating users about the importance of password security and providing training on how to create and manage strong passwords.
- Implementing password management tools and solutions to securely store and manage passwords, such as password managers or identity and access management (IAM) systems.

By implementing these security measures, organizations can reduce the risk of unauthorized access and data breaches resulting from insecure passwords.

**Design flaws in a device's operating system in the network**

Design flaws in a device's operating system can introduce various network security vulnerabilities, potentially leading to unauthorized access, data breaches, and service disruptions. Here are some common design flaws in a device's operating system that can impact network security:

- Lack of Secure Defaults: Operating systems that lack secure default configurations may have unnecessary services enabled, weak authentication settings, or default passwords that are easily guessable. Attackers can exploit these insecure defaults to gain unauthorized access to the device or compromise network security.

- Vulnerabilities in Network Protocols: Design flaws in network protocols implemented by the operating system can introduce vulnerabilities that attackers can exploit to intercept, manipulate, or disrupt network communications. For example, insecure implementations of protocols like TCP/IP, DNS, or DHCP may be susceptible to spoofing, injection, or denial-of-service attacks.

- Insecure Authentication Mechanisms: Operating systems that use insecure authentication mechanisms, such as plaintext passwords or weak encryption algorithms, can compromise the security of user credentials and authentication processes. Attackers may intercept or crack insecurely transmitted or stored authentication credentials to gain unauthorized access to the device or network resources.

- Privilege Escalation Vulnerabilities: Design flaws that allow unauthorized users to escalate their privileges or gain administrative access to the operating system can

lead to unauthorized access to sensitive data and resources. Privilege escalation vulnerabilities may allow attackers to bypass access controls, execute arbitrary code, or modify system configurations.

- Buffer Overflow and Memory Corruption: Operating systems with design flaws related to buffer overflow or memory corruption vulnerabilities are susceptible to exploitation by attackers to execute arbitrary code or crash the system. Attackers may exploit these vulnerabilities to gain remote code execution or escalate their privileges on the device.

- Inadequate Input Validation: Design flaws that result in inadequate input validation mechanisms can expose the operating system to various types of attacks, including injection attacks (e.g., SQL injection, command injection) and cross-site scripting (XSS) attacks. Attackers may exploit input validation vulnerabilities to manipulate or execute malicious commands on the device.

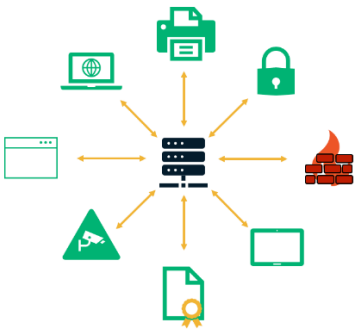
- Insufficient Logging and Monitoring: Operating systems that lack robust logging and monitoring capabilities may fail to detect and respond to security incidents effectively. Design flaws that result in insufficient logging or monitoring may prevent administrators from identifying and mitigating security threats promptly, allowing attackers to persist undetected on the device or network.

To mitigate the vulnerabilities associated with design flaws in a device's operating system, manufacturers and developers should follow security best practices, such as:

- Implementing secure default configurations and minimizing the attack surface of the operating system.
- Regularly patching and updating the operating system to address known vulnerabilities and security issues.
- Conducting thorough security reviews and audits of the operating system design and implementation to identify and remediate potential security flaws.
- Implementing robust authentication mechanisms, access controls, and encryption to protect sensitive data and resources.
- Implementing secure coding practices and performing rigorous testing, including fuzz testing and code review, to identify and mitigate potential vulnerabilities.
- Providing security training and education to system administrators and users to raise awareness of security risks and best practices for securing the operating system and network.

## 1.4 Network security best practices.

**Baseline network protocols and monitor usage.**

| | | |
|---|---|---|
| Establish the baseline usage of different protocols on your wired and wireless networks. To create an accurate baseline, data should be gathered from a variety of sources including routers, switches, firewalls, wireless access points, network sniffers, and dedicated data collectors. Then monitor for deviations from these baselines, which can be indicative of data tunneling, malicious software transmitting data to unauthorized destinations, and other threats. |  | |

**Use honeypots and honeynets.**
A honeypot is a decoy system designed to look like a real network asset, and a honeynet is a network of honeypots that simulate a larger, more complex network environment. They are designed to lure adversaries into interacting with them, both to divert malicious actors from true assets and to enable security teams to study attack techniques and gather other intelligence for effective threat management.

**Use intrusion detection and prevention systems.**
It is vital to monitor and log activity across the network and analyze it to spot unusual logins, suspicious computer events, and other anomalies. An intrusion detection system (IDS) monitors network data flows for potentially malicious activity and alerts administrators about anomalies. An intrusion prevention system (IPS) also monitors network traffic for threats; however, in addition to alerting administrators, it can automatically take action to block or mitigate threats.

These tools can be a valuable part of your network security strategy. For example, by comparing current activity to an established baseline, they could spot a spike in network activity that could indicate a ransomware or SQL injection attack. They can also use attack signatures — characteristic features common to a specific attack or pattern of attacks — to spot attacks that don't generate activity that violates your organization's baseline.

**Automate response to attacks when appropriate.**
Many modern security tools can be configured to respond automatically to known threats. For example, these systems can:

- **Block IP address** — An IPS or firewall can block the IP address from which the attack originated. This option is very effective against phishing and denial-of-service attacks. However, some attackers spoof the source IP address during attacks, so the wrong address will be blocked.

- **Terminate connections** — Routers and firewalls can be configured to disrupt the connections that an intruder maintains with the compromised system by targeting RESET TCP packets at the attacker.
- **Acquire additional information** — Tools can also collect valuable information that helps determine the point of initial access, which accounts were compromised, how the intruders moved across the network, and what data was compromised.

## 1.5 Network attack architecture

The term "Network attack architecture" isn't commonly used in the field of cybersecurity. However, if we were to interpret it, we could consider it as the structure or framework that encompasses various components, methods, and stages involved in launching network-based attacks. Let's break it down:

- Components: These are the individual elements or parts involved in executing a network attack. This could include things like attacker-controlled servers, malicious software, compromised devices, and network infrastructure.

- Methods: These are the techniques and tactics used by attackers to exploit vulnerabilities, gain unauthorized access, or disrupt network operations. Methods can vary widely and may include phishing, malware injection, denial-of-service (DoS) attacks, and exploitation of software vulnerabilities.

- Stages: Network attacks often involve multiple stages or phases, each serving a specific purpose in the attack lifecycle. These stages may include reconnaissance (gathering information about the target), weaponization (developing or obtaining attack tools), delivery (sending the attack payload to the target), exploitation (taking advantage of vulnerabilities), installation (establishing persistence), command and control (maintaining control over compromised systems), and actions on objectives (achieving the attacker's goals).

Understanding the network attack architecture can help security professionals and organizations develop effective defense strategies and countermeasures to detect, prevent, and respond to network-based attacks. This may involve implementing security controls such as firewalls, intrusion detection/prevention systems (IDS/IPS), endpoint security solutions, and security awareness training for employees. Additionally, conducting regular security assessments, vulnerability scans, and incident response exercises can help identify and mitigate vulnerabilities in network infrastructure and systems before they are exploited by attackers.

**Human exploits**

In the context of network attack architecture, human exploits refer to the use of social engineering techniques to manipulate individuals within an organization to facilitate or enable cyberattacks. Human exploits are often an integral part of the attack lifecycle, complementing technical exploits to gain unauthorized access to networks, systems, or sensitive information. Here's how human exploits fit into the network attack architecture:

- **Reconnaissance Phase:** Social Engineering Reconnaissance: Attackers gather information about the target organization's employees, organizational structure, and communication channels to identify potential targets for social engineering attacks. This may involve researching employees' roles and responsibilities, identifying key decision-makers, and mapping out communication patterns.

- **Weaponization Phase**: Crafting Social Engineering Messages: Attackers create convincing social engineering messages, such as phishing emails or phone scripts, designed to manipulate recipients into taking specific actions, such as clicking on malicious links, downloading malware-infected attachments, or disclosing sensitive information.

- **Delivery Phase**: Phishing and Social Engineering Campaigns: Attackers deliver social engineering messages through various channels, including email, phone calls, instant messaging, or social media, to trick targeted individuals into falling for their scams. This phase relies heavily on human psychology and manipulation tactics to deceive recipients.

- **Exploitation Phase:** Successful Social Engineering Attacks: If recipients fall for the social engineering tactics, attackers exploit their trust, curiosity, or ignorance to gain unauthorized access to network resources, systems, or sensitive information. This may involve obtaining login credentials, compromising user accounts, or bypassing security controls through deception.

- **Installation Phase:** Establishing Persistence: Once attackers gain initial access to the network through social engineering attacks, they may install backdoors, remote access trojans (RATs), or other malware to maintain persistent access and control over compromised systems. This allows attackers to continue their malicious activities undetected.

- **Command and Control (C2) Phase**: Communicating with Compromised Systems: Attackers use social engineering techniques to communicate with compromised systems, issue commands, and exfiltrate data. This may involve sending instructions to compromised employees via email, phone calls, or other communication channels to carry out specific tasks or provide additional access.

- **Actions on Objectives Phase**: Data Theft or Disruption: Attackers achieve their objectives, such as stealing sensitive information, disrupting network operations, or causing financial damage, by leveraging the access obtained through social engineering attacks. This may involve exfiltrating data, altering configurations, or spreading malware to other systems.

**Social engineering**

Incorporating human exploits into the network attack architecture allows attackers to exploit the weakest link in the security chain: human beings. To mitigate the risk of human exploits, organizations should prioritize security awareness training for employees, establish clear policies and procedures for handling sensitive information, and implement technical controls to detect and prevent social engineering attacks. Additionally, organizations should encourage a culture of skepticism and vigilance among employees to recognize and report suspicious activities or requests.

Social engineering plays a crucial role in the network attack architecture, leveraging human psychology and manipulation tactics to deceive individuals within an organization and facilitate cyberattacks. Here's how social engineering fits into the network attack architecture:

- Reconnaissance Phase: Gathering Information: Attackers research the target organization to gather information about employees, organizational structure, communication channels, and security practices. This information helps attackers tailor social engineering attacks to specific individuals and departments.

- Weaponization Phase: Crafting Social Engineering Messages: Attackers create convincing social engineering messages, such as phishing emails, phone scripts, or fake websites, designed to trick recipients into taking specific actions. Messages may impersonate trusted entities, use urgent language, or offer enticing incentives to manipulate victims.

- Delivery Phase: Sending Social Engineering Messages: Attackers deliver social engineering messages through various channels, including email, phone calls, instant messaging, or social media. The goal is to deceive targeted individuals into falling for the scam and revealing sensitive information, clicking on malicious links, or downloading malware-infected attachments.

- Exploitation Phase: Successful Social Engineering Attacks: If recipients fall for the social engineering tactics, attackers exploit their trust, curiosity, or ignorance to gain unauthorized access to network resources, systems, or sensitive information. This may involve obtaining login credentials, compromising user accounts, or bypassing security controls through deception.

- Installation Phase: Establishing Persistence: Once attackers gain initial access to the network through social engineering attacks, they may install backdoors, remote access trojans (RATs), or other malware to maintain persistent access and control over compromised systems. This allows attackers to continue their malicious activities undetected.

- Command and Control (C2) Phase: Communicating with Compromised Systems: Attackers use social engineering techniques to communicate with compromised systems, issue commands, and exfiltrate data. This may involve sending instructions to compromised employees via email, phone calls, or other communication channels to carry out specific tasks or provide additional access.

- Actions on Objectives Phase: Data Theft or Disruption: Attackers achieve their objectives, such as stealing sensitive information, disrupting network operations, or causing financial damage, by leveraging the access obtained through social engineering attacks. This may involve exfiltrating data, altering configurations, or spreading malware to other systems.

Social engineering attacks are particularly effective because they exploit the human element, which is often the weakest link in the security chain. To mitigate the risk of social engineering attacks, organizations should prioritize security awareness training for employees, establish clear policies and procedures for handling sensitive information, and implement technical controls to detect and prevent social engineering attacks. Additionally, organizations should encourage a culture of skepticism and vigilance among employees to recognize and report suspicious activities or requests.

**Password Attack**

A password attack is a type of cyberattack that aims to compromise user passwords in toin unauthorized access to accounts, systems, or data. Password attacks exploit weaknesses in password security mechanisms to guess, crack, or steal passwords. Here are some common types of password attacks:


- Brute Force Attack: In a brute force attack, an attacker systematically tries all possible combinations of characters until the correct password is found. This method can be time-consuming and resource-intensive but is effective against weak or short passwords.

- Dictionary Attack: In a dictionary attack, an attacker uses a predefined list of commonly used passwords, words from dictionaries, or variations of known passwords to guess the correct password. This method is more efficient than brute force and targets common human tendencies in password selection.

- Rainbow Table Attack: A rainbow table attack involves the use of precomputed tables containing hashed passwords and their corresponding plaintext equivalents. Attackers compare password hashes obtained from stolen password databases or intercepted network traffic against entries in the rainbow table to find matching passwords.

- Credential Stuffing: Credential stuffing involves using usernames and passwords obtained from data breaches or leaks to gain unauthorized access to user accounts on other websites or services. Attackers automate the login process using botnets or specialized tools to test stolen credentials on multiple sites.

- Phishing: Phishing attacks attempt to trick users into revealing their passwords by impersonating legitimate websites or services. Attackers send deceptive emails, messages, or websites that mimic trusted entities and prompt users to enter their login credentials, which are then captured by the attacker.

- Keylogging: Keylogging attacks involve installing malicious software or hardware on a victim's device to capture keystrokes, including passwords, as they are entered. Attackers can remotely monitor and record user activity, including login credentials, without the victim's knowledge.

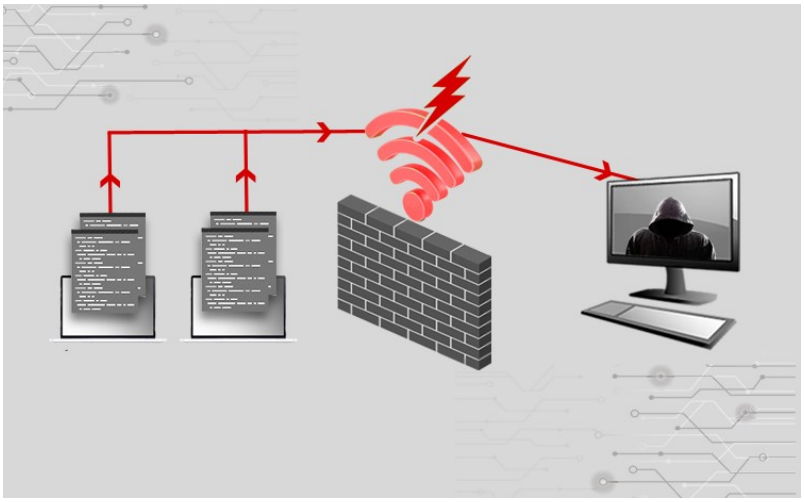
- Shoulder Surfing: Shoulder surfing attacks involve observing or recording a user's login credentials, including passwords, by watching them enter information on a computer, mobile device, or ATM keypad in public places.

To defend against password attacks, organizations, and individuals can implement the following security best practices:

- Use strong, unique passwords for each account, consisting of a mix of letters, numbers, and special characters.
- Enable multi-factor authentication (MFA) to add layer of security beyond passwords.
- Implement account lockout policies and rate limiting to prevent brute force and dictionary attacks.
- Regularly update passwords and avoid reusing passwords across multiple accounts.
- Educate users about password security best practices and how to recognize and avoid phishing attacks.
- Monitor network traffic and user activity for signs of unauthorized access or suspicious behavior.

**Wireless Attack**

A wireless attack is a type of cyberattack that targets wireless networks, devices, or protocols to gain unauthorized access, intercept communications, or disrupt network operations. Wireless attacks exploit vulnerabilities in wireless technologies, such as Wi-Fi, Bluetooth, or RFID, to compromise the security and privacy of wireless networks and connected devices. Here are some common types of wireless attacks:



- Wi-Fi Eavesdropping: Wi-Fi eavesdropping attacks involve intercepting and monitoring wireless communications between devices and access points. Attackers use tools like packet sniffers to capture data packets transmitted over Wi-Fi networks, including sensitive information such as passwords, usernames, or financial data.

- Man-in-the-Middle (MitM) Attack: In a MitM attack, an attacker intercepts and alters communication between two parties without their knowledge. In the context of wireless networks, attackers position themselves between a client device and an access point to intercept and manipulate data packets, steal credentials, or inject malicious code.

- Evil Twin Attack: An evil twin attack involves setting up a rogue access point with the same SSID (network name) as a legitimate Wi-Fi network to trick users into connecting to it. Once connected, attackers can capture sensitive information, perform MitM attacks, or distribute malware to connected devices.

- Wireless Deauthentication Attack: A de-authentication attack involves sending forged de-authentication packets to legitimate clients or access points, causing them to disconnect from the wireless network. Attackers can use de-authentication attacks to disrupt network connectivity, launch denial-of-service (DoS) attacks, or force clients to connect to malicious access points.

- Wireless Jamming Attack: A jamming attack involves transmitting interference signals on the same frequency as a wireless network, disrupting or blocking communication between devices and access points. Attackers use jamming devices to overwhelm wireless channels, causing network congestion or rendering the network unusable.

- Bluetooth Sniffing: Bluetooth sniffing attacks involve intercepting and capturing Bluetooth communications between devices, such as smartphones,

- Use strong encryption protocols, such as WPA3 for Wi-Fi networks, to protect wireless communications.
- Enable network segmentation and access controls to restrict access to sensitive resources and devices.
- Implement intrusion detection/prevention systems (IDS/IPS) to detect and respond to suspicious activity on wireless networks.
- Regularly update firmware and software to patch known vulnerabilities in wireless devices and protocols.
- Use Bluetooth pairing mechanisms and encryption to secure Bluetooth connections between devices.
- Conduct regular security audits and penetration tests to identify and remediate vulnerabilities in wireless networks and devices.
- Educate users about wireless security best practices and how to recognize and avoid common wireless attacks, such as connecting to unknown or unsecured networks.

## 1.6 Search engine privacy

Search engine privacy is a subset of internet privacy that deals with user data being collected by search engines. Both types of privacy fall under the umbrella of information privacy. Privacy concerns regarding search engines can take many forms, such as the ability for search engines to log individual search queries, browsing history, IP addresses, and cookies of users, and conducting user profiling in general. The collection of personally identifiable information (PII) of users by search engines is referred to as tracking.


This is controversial because search engines often claim to collect a user's data to better tailor results to that specific user and to provide the user with a better search experience. However, search engines can also abuse and compromise their users' privacy by selling their data to advertisers for profit. In the absence of regulations, users must decide what is more important to their search engine experience: relevance and speed of results or their privacy and choose a search engine accordingly.

The legal framework in the United States for protecting user privacy is not very solid. The most popular search engines collect personal information, but other search engines that are focused on privacy have cropped up recently. There have been several well-publicized breaches of search engine user privacy that occurred with companies like AOL and Yahoo.

## 1.7 Browser Security and Tracking

Browser security refers to the measures and features implemented by web browsers to protect users from various online threats, including malware, phishing, and data breaches. Additionally, browser security encompasses privacy features designed to protect user's sensitive information and prevent unauthorized tracking by third-party entities. Here's an overview of browser security and tracking:

- Malware Protection: Modern web browsers include built-in security features, such as malware detection and blocking, to protect users from malicious websites and downloads. Browsers may use various techniques, such as heuristics, reputation-based filtering, and real-time scanning, to identify and block malware threats.

- Phishing Protection: Browsers often incorporate anti-phishing mechanisms to warn users about potentially fraudulent websites designed to steal sensitive information, such as login credentials or financial data. Phishing protection may involve checking website reputations, analyzing page content, and displaying warning messages to users.

- HTTPS Encryption: Browsers encourage the use of HTTPS (Hypertext Transfer Protocol Secure) to encrypt data transmitted between users and websites, preventing eavesdropping and tampering by attackers. Browsers may display security indicators, such as padlock icons or HTTPS warnings, to indicate the security status of website connections.

- Content Security Policies (CSP): CSP is a security feature that allows website owners to specify which content sources are allowed to be loaded and executed on their web pages. Browsers enforce CSP rules to mitigate risks associated with cross-site scripting (XSS) attacks and other code injection vulnerabilities.

- Cross-Origin Resource Sharing (CORS): CORS is a security mechanism that controls access to resources on a web page from different domains. Browsers enforce CORS policies to prevent unauthorized access to sensitive data and resources, reducing the risk of cross-site request forgery (CSRF) attacks.

## Self-Check -1: Interpret Network Security

### Questionnaire

1. What is a denial of service (DoS) attack?
   Answer:

2. What is phishing?
   Answer:

3. What is an evil twin attack?
   Answer:

4. What is the purpose of multi-factor authentication (MFA)?
   Answer:

5. What is a brute force attack?
   Answer:

6. What is the role of reconnaissance in a network attack?
   Answer:

7. What is the purpose of HTTPS encryption?
   Answer:

8. What is a dictionary attack?
   Answer:

9. What is the difference between phishing and spear phishing?
   Answer:

10. What is the objective of a man-in-the-middle (MITM) attack?
    Answer:

11. What is the purpose of content security policies (CSP)?
    Answer:

12. What is the significance of regular password updates?
    Answer:

13. How does an evil twin attack work?
    Answer:

## Answer Key-1: Interpret Network Security

1. What is a denial of service (DoS) attack?
   Answer: A DoS attack is a cyberattack that aims to disrupt the availability of services or resources, rendering them inaccessible to legitimate users.

2. What is phishing?
   Answer: Phishing is a type of social engineering attack where attackers use deceptive emails, messages, or websites to trick individuals into revealing sensitive information or performing actions.

3. What is an evil twin attack?
   Answer: An evil twin attack involves setting up a rogue access point with the same SSID as a legitimate Wi-Fi network to trick users into connecting to it and stealing their information.

4. What is the purpose of multi-factor authentication (MFA)?
   Answer: MFA adds an extra layer of security beyond passwords by requiring users to provide additional verification factors, such as a code sent to their phone, to access their accounts.

5. What is a brute force attack?
   Answer: A brute force attack is a method of guessing passwords by systematically trying all possible combinations until the correct one is found.

6. What is the role of reconnaissance in a network attack?
   Answer: Reconnaissance involves gathering information about the target network, such as IP addresses and system configurations, to identify potential vulnerabilities and entry points.

7. What is the purpose of HTTPS encryption?
   Answer: HTTPS encryption protects data transmitted between users and websites by encrypting it, preventing eavesdropping and tampering by attackers.

8. What is a dictionary attack?
   Answer: A dictionary attack is a method of guessing passwords by using a predefined list of commonly used passwords or words from dictionaries.

9. What is the difference between phishing and spear phishing?
   Answer: Phishing is a generic attack targeting a wide range of individuals, while spear phishing is a targeted attack aimed at specific individuals or organizations.

10. What is the objective of a man-in-the-middle (MitM) attack?

Answer: The objective of a MitM attack is to intercept and manipulate communication between two parties without their concern.

11. What is the purpose of content security policies (CSP)?
    Answer: CSP allows website owners to specify which content sources are allowed to be loaded and executed on their web pages, mitigating risks associated with code injection vulnerabilities.

12. What is the significance of regular password updates?
    Answer: Regular password updates help mitigate the risk of password-based attacks by reducing the window of opportunity for attackers to guess or crack passwords.

13. How does an evil twin attack work?
    Answer: In an evil twin attack, an attacker sets up a rogue wireless access point with the same SSID as a legitimate network to trick users into connecting to it and disclosing sensitive information.

## Learning Outcome-2: Configure Firewall Services

| | |
|---|---|
| Assessment Criteria | 1. Security is ensured using network administration tool<br>2. Filter rules is configured as per requirement<br>3. Mangle/Packet Filtering is configured as per requirement<br>4. Security services is configured as per requirement<br>5. Access Control List (ACL) is configured as per requirement |
| Conditions and Resources | 1. Actual workplace or training environment<br>2. CBLM<br>3. Handouts<br>4. Laptop/ Desktop<br>5. Multimedia Projector<br>6. Paper, Pen, Pencil, and Eraser<br>7. Internet Facilities<br>8. Whiteboard and Marker |
| Contents | 1. Network administration tool for ensuring secured network<br>2. Security services configuration<br>▪ SSH<br>▪ Layer 7 protocol<br>▪ IPsec<br>3. Filtering rules<br>4. Mangle / packet filtering<br>5. Access control list (ACL)<br>6. Practice Firewall operation using PFSENSE |
| Activities/job/Task | 1. Configure firewall services using following activity:<br>▪ Ensure Security using network administration tool<br>▪ Configure Filter rules as per requirement<br>▪ Configure Mangle/Packet Filtering as per requirement<br>▪ Configure Security services as per requirement<br>▪ Configure Access Control List (ACL) as per requirement |
| Training Methods | 1. Blended<br>2. Discussion<br>3. Presentation<br>4. Demonstration<br>5. Guided Practice<br>6. Individual Practice<br>7. Project Work<br>8. Problem Solving<br>9. Brainstorming |
| Assessment Methods | Assessment methods may include but not limited to<br>1. Written Test<br>2. Demonstration<br>3. Oral Questioning<br>4. Portfolio |

## Learning Experience-2: Configure firewall services

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

| Learning Activities | Recourses/Special Instructions |
|---|---|
| 4. Students will ask the instructor about "Configure firewall services." | A. The instructor will provide the learning materials for "Configure firewall services." |
| 5. Read the Information sheet and complete the self-check & Check answer sheets on "Configure firewall services." | 1. Read Information sheet:<br>a. Network administration tool for ensuring secured network<br>b. Security services configuration<br>c. Filtering rules<br>d. Mangle / packet filtering<br>e. Access control list (ACL)<br>f. Practice Firewall operation using PFSENSE<br>2. Answer Self-check 1: Configure firewall services.<br>3. Check your answer with Answer key 1: Configure firewall services |
| 6. Read the Job/Task Sheet and Specification Sheet and perform job/Task | 6. Job/Task Sheet and Specification Sheet<br>**Job Sheet 2.1:** Configure Firewall Services<br>**Specification Sheet 2.1:** Configure Firewall Services |

# Information Sheet-2: Configure firewall services

**Learning Objective:**

After completion of this information sheet, the learners will be able to explain, define, and interpret the following contents:

1.1 Network administration tool for ensuring a secure network.
1.2 Security Services Configuration
- SSH
- Layer 7 protocol
- IPsec

1.3 Filtering rules
1.4 Mangle/packet filtering.
1.5 Access Control List (ACL)
1.6 Practice Firewall operation using PFSENSE.

## 2.1 Network administration tool.

A network management tool is software or hardware designed to monitor, analyze, and control a computer network. It helps administrators oversee network performance, troubleshoot issues, and optimize resource usage.

**Benefit of Network Management Tool**

Network management tools provide several benefits, including:

- Improved Efficiency: Streamlined network monitoring and management processes enhance operational efficiency and reduce downtime.
- Enhanced Security: Effective monitoring and security features help identify and mitigate potential security threats, safeguarding sensitive data and systems.
- Optimized Performance: Monitoring tools track network performance metrics, allowing administrators to identify bottlenecks and optimize resource allocation for better performance.
- Cost Reduction: Proactive network management reduces the likelihood of costly network failures and downtime, saving money in the long-run.
- Centralized Control: Network management tools offer centralized control and visibility, simplifying administration tasks and ensuring consistent network policies across all devices.
- Scalability: Scalable solutions can accommodate growing network infrastructure, adapting to changing business needs without sacrificing performance or security.
- Compliance and Reporting: Tools provide reporting and auditing capabilities, facilitating compliance with industry regulations and internal policies.

Overall, network management tools contribute to a stable, secure, and efficient network environment, supporting business objectives and user productivity.

**Network administration tool for ensuring secured network:**

One essential tool for network administration and security is a Unified Threat Management (UTM) appliance or software. These systems integrate multiple security features into one platform, providing comprehensive protection against various threats. Here are some key features a UTM should offer:

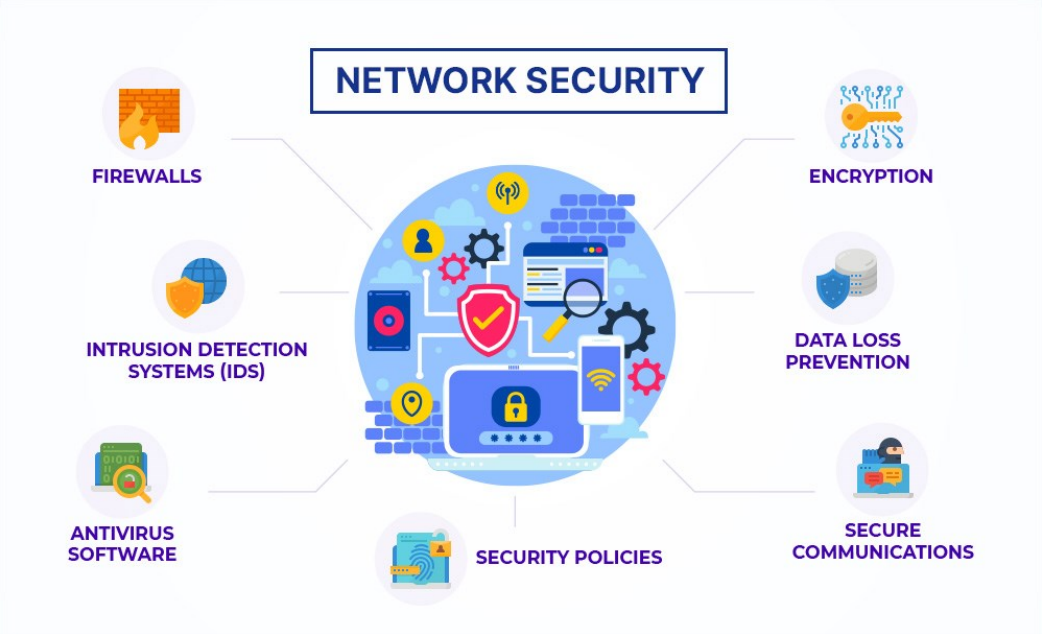


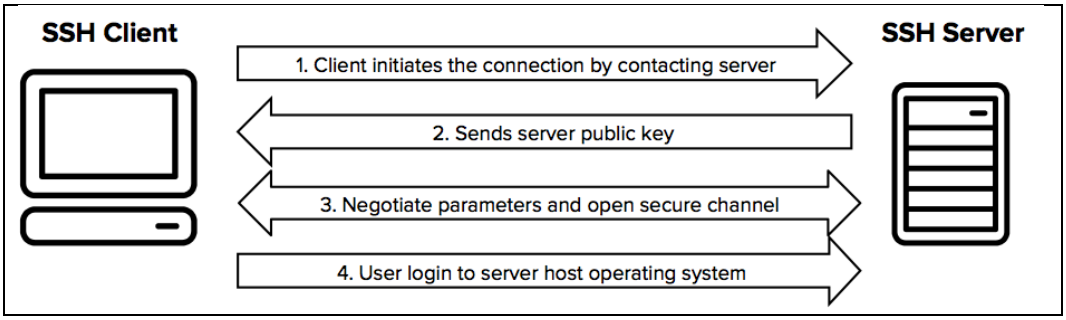

**Figure 3: Network Security**

- Firewall: Provides a barrier between your internal network and the outside world, controlling incoming and outgoing traffic based on predetermined security rules.
- Intrusion Detection and Prevention System (IDPS): Monitors network traffic for suspicious activity or known attack patterns and takes action to prevent unauthorized access or data breaches.
- Virtual Private Network (VPN): Allows secure remote access to the network for authorized users, ensuring data confidentiality and integrity over public networks.
- Antivirus/Anti-malware: Scans incoming and outgoing traffic for known viruses, malware, and other malicious software, preventing them from infecting the network.
- Web Filtering: Controls access to websites based on predefined categories or URLs, helping to block malicious or inappropriate content and reduce the risk of malware infections.
- Email Security: Filters incoming and outgoing emails for spam, phishing attempts, and malware attachments, protecting against email-based threats.
- Data Loss Prevention (DLP): Monitors and controls sensitive data transfers to prevent unauthorized access or accidental disclosure of confidential information.
- Network Segmentation: Divides the network into separate segments or VLANs to contain security breaches and limit the spread of malware or unauthorized access.

## 2.2 Security Service Configuration:

Security services configuration involves setting up and managing various security measures such as firewalls, intrusion detection/prevention systems, VPNs, antivirus, and data encryption to protect networks from unauthorized access, malware, and data breaches.

- **SSH**: SSH (Secure Shell) is a network protocol used for secure communication between a client and a server. It provides encrypted communication over an unsecured network and enables users to securely log into remote systems and execute commands. SSH is commonly used for remote administration, file transfers, and tunneling network connections.
  SSH, or Secure Shell, is a fundamental component of security services configuration. It's used to securely access and manage remote systems, making it a critical tool for configuring and maintaining various security measures.




- Secure Access: SSH allows administrators to securely access remote systems for configuration and management purposes. This secure access ensures that sensitive configuration settings are not exposed to unauthorized parties.
- Remote Administration: With SSH, administrators can remotely administer security services such as firewalls, intrusion detection/prevention systems, and VPN servers. They can configure settings, monitor logs, and troubleshoot issues without the need for physical access to the devices.

- Encryption: SSH encrypts communication between the client and server, ensuring that sensitive configuration data, such as passwords and cryptographic keys, are protected from interception and eavesdropping.
- Authentication: SSH provides robust authentication mechanisms, including password-based authentication and public-key cryptography. This ensures that only authorized users can access and configure security services.
- Secure File Transfer: SSH includes protocols like SCP (Secure Copy Protocol) and SFTP (SSH File Transfer Protocol), which enable secure file transfer between systems. This allows administrators to transfer configuration files, software updates, and security patches securely.
- Tunneling: SSH tunneling allows administrators to securely access internal network resources from remote locations. This capability is useful for configuring and managing security services deployed in private networks.

Overall, SSH plays a vital role in the configuration and management of security services by providing secure remote access, encryption, authentication, and file transfer capabilities. It's a foundational tool for maintaining the security and integrity of network infrastructure.

**Layer 7 protocol**

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies.

The modern Internet is not based on OSI but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate and helps isolate and troubleshoot networking problems.

OSI Model Explained: The OSI 7 Layers:

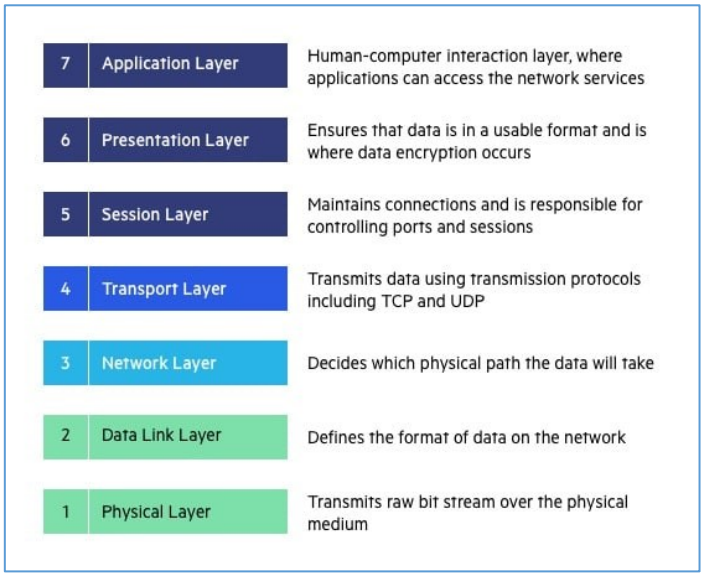



**Figure 4: Network Layer**

Layer 7, the Application layer, encompasses protocols and services directly interacting with end-users and applications. In security services configuration, Layer 7 protocols are essential for implementing granular security policies and controlling access to specific applications and services.

Here's how Layer 7 protocols contribute to security services configuration:

- Deep Packet Inspection (DPI): Layer 7 protocols enable DPI, allowing security devices to inspect the content of application-layer data packets. This level of inspection allows fine-grained control over network traffic based on application-specific attributes.
- Application Control: Security appliances and firewalls use Layer 7 protocols to identify and control access to individual applications and services. By inspecting application-layer data, administrators can enforce policies based on specific applications, such as allowing or blocking access to social media, file-sharing, or gaming sites.

- Content Filtering: Layer 7 protocols facilitate content filtering by allowing security devices to analyze the content of web pages, emails, and other application data. This enables the enforcement of policies related to content categories, such as blocking access to inappropriate or malicious websites or filtering out spam emails.
- Intrusion Detection and Prevention: Layer 7 protocols provide the context necessary for detecting and preventing application-layer attacks. Security devices can analyze application-specific traffic patterns and behavior to identify signs of malicious activity or unauthorized access attempts.
- Quality of Service (QoS): Layer 7 protocols enable QoS mechanisms to prioritize or throttle traffic based on application requirements. Administrators can allocate bandwidth resources according to the criticality of different applications, ensuring optimal performance and availability.
- User Authentication and Authorization: Layer 7 protocols support user authentication and access control mechanisms at the application layer. This allows security devices to enforce policies based on user identities, roles, or groups, ensuring that only authorized users can access specific applications or services.

Overall, Layer 7 protocols play a crucial role in security services configuration by enabling deep visibility, control, and protection of application-layer traffic. They empower administrators to implement granular security policies tailored to the unique requirements of individual applications and users.

**IPsec**

IPsec (Internet Protocol Security) is a suite of protocols used to secure Internet protocol (IP) communications by encrypting and authenticating IP packets. In security services configuration, IPsec is commonly employed to establish secure VPN (Virtual Private Network) connections between network devices, ensuring confidentiality, integrity, and authenticity of data transmitted over untrusted networks.

- Encryption: IPsec provides encryption mechanisms to protect the confidentiality of data transmitted over the network. By encrypting IP packets, it prevents eavesdropping and unauthorized access to sensitive information.
- Authentication: IPsec ensures the authenticity of data by providing authentication mechanisms. It uses cryptographic techniques such as digital signatures or pre-shared keys to verify the identity of communicating parties and protect against spoofing attacks.
- Integrity: IPsec verifies the integrity of data to prevent tampering and unauthorized modification during transmission. It employs cryptographic hash functions to generate message digests, allowing recipients to verify that the data has not been altered en route.
- VPN Establishment: IPsec is commonly used to establish secure VPN tunnels between network devices, such as routers, firewalls, or VPN gateways. These

Overall, IPsec plays a critical role in security services configuration by providing robust encryption, authentication, and integrity protection for IP-based networks, particularly in the context of VPN deployments. It enables organizations to establish secure communication channels and protect sensitive data transmitted over insecure networks.

## 2.3 Filtering rules

Filtering rules in firewall services are the set of instructions or policies implemented to control the flow of network traffic based on defined criteria such as source and destination IP addresses, port numbers, protocols, and other packet attributes. These rules are configured within the firewall to permit, deny, or restrict specific types of traffic, thereby enhancing network security and controlling access to resources.

| | Source IP | Dest. IP | Source Port | Dest. Port | Action |
|---|---|---|---|---|---|
| 1 | 192.168.21.0 | -- | -- | -- | deny |
| 2 | -- | -- | -- | 23 | deny |
| 3 | -- | 192.168.21.3 | -- | -- | deny |
| 4 | -- | 192.168.21.0 | -- | >1023 | Allow |

- Traffic Classification: Filtering rules are used to classify incoming and outgoing network traffic based on various criteria, including source and destination IP addresses, port numbers, protocols (TCP, UDP, ICMP), and application-layer information (such as HTTP headers).
- Action Definition: Each filtering rule specifies an action to be taken on matching traffic, such as allowing, denying, or logging the packets. For example, a rule may permit incoming traffic on port 80 (HTTP) to access web servers while blocking traffic on other ports.
- Ordering: Filtering rules are typically organized in sequential order within the firewall's rule set. When a packet enters the firewall, it is compared against the filtering rules sequentially until a matching rule is found. The order of rules is crucial as the first matching rule is applied, and subsequent rules may not be evaluated.

- Stateful Inspection: Modern firewalls often employ stateful inspection, which tracks the state of active connections and dynamically adjusts filtering rules accordingly. This enables the firewall to allow return traffic related to established connections without the need for explicit rules.
- Default Policy: Firewalls may have default policies to handle traffic that does not match any explicitly defined rules. For instance, a firewall may have a default deny policy, blocking all traffic unless explicitly permitted by filtering rules.

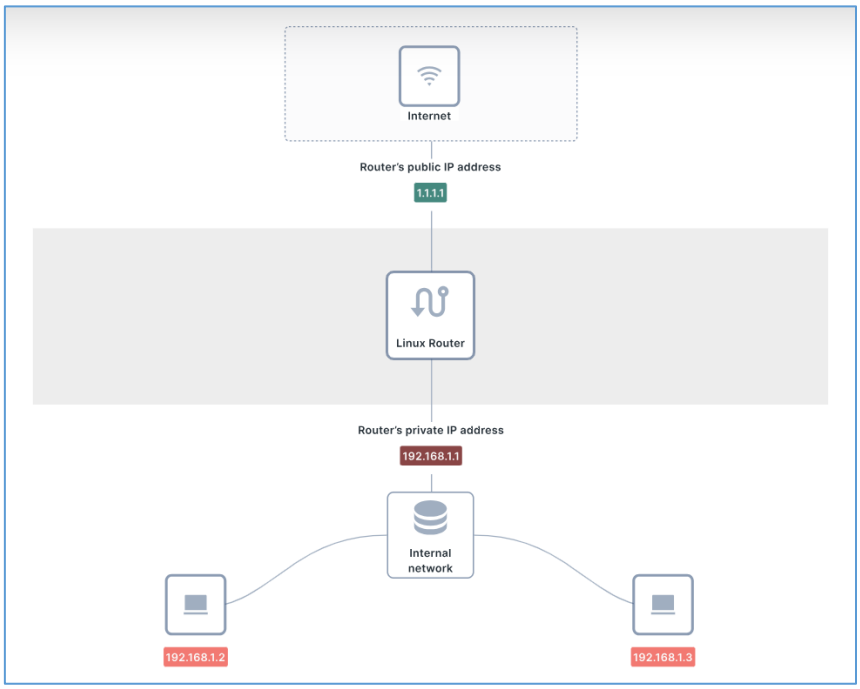
- Logging and Monitoring: Filtering rules can be configured to log matching traffic, allowing administrators to monitor network activity, analyze security incidents, and troubleshoot connectivity issues.
- Granular Control: Firewall administrators can configure filtering rules with granular precision to enforce security policies tailored to the organization's requirements. This includes controlling access to specific services, restricting traffic between network segments, and mitigating known threats.

## 2.4 Mangle/packet filtering

"Mangle" and "packet filtering" are terms often associated with firewall and networking configurations, particularly in systems like iptables, which is a firewall management tool for Linux. Let's break down what each term means:

- **Mangle**: In the context of firewall configuration, "mangle" typically refers to a specific table within the iptables firewall framework. The mangle table is responsible for modifying certain characteristics of packets as they traverse the firewall. These modifications might include altering packet headers, marking packets for special treatment, or changing the Type of Service (TOS) field in the IP header.

- **Packet Filtering:** Packet filtering is the process of examining packets as they pass through a firewall or network device and making decisions about whether to allow or deny them based on predefined criteria. These criteria typically include attributes such as source and destination IP addresses, port numbers, protocols, and packet states.



Packet filtering rules define what types of traffic are permitted or denied based on the specified criteria. For example, a packet filtering rule might allow inbound traffic on port 80 (HTTP) to reach a web server while blocking all other inbound traffic.
packet filtering is a fundamental aspect of firewall configuration and is essential for enforcing network security policies, controlling access to network resources, and protecting against unauthorized access and malicious activity.

In summary, "mangle" refers to a specific table within the iptables firewall framework used for modifying packet characteristics, while "packet filtering" is the process of examining and making decisions about packets based on predefined criteria to enforce network security policies. Both concepts are crucial components of firewall configuration and network security management.

## Self-Check-2: Configure Firewall Services

### Questionnaire

1. What is a firewall?
   Answer:

2. What are iptables?
   Answer:

3. What is the purpose of the mangle table in iptables?
   Answer:

4. What are the packet-filtering rules used for firewall?
   Answer:

5. What criteria are typically used in packet filtering rules?
   Answer:

6. What is Quality of Service (QoS) management?
   Answer:

7. How do iptables handle packet filtering?
   Answer:

8. What is stateful inspection?
   Answer:

9. What is the default policy in firewall configuration?
   Answer:

10. What is the purpose of packet marking in firewall configuration?
    Answer:

11. What are some common actions in firewall rules?
    Answer:

12. What is IPsec?
    Answer:

13. What is the primary purpose of IPsec?
    Answer:

14. What are some components of IPsec?

Answer:

15. How does IPsec contribute to VPNs?
Answer:

16. What is the role of encryption in IPsec?
Answer:

17. What is authentication in the context of IPsec?
Answer:

18. What is NAT (Network Address Translation)?
Answer:

19. What is Deep Packet Inspection (DPI)?
Answer:

## Answer Key-2: Configure Firewall Services

1. What is a firewall?
   Answer: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

2. What is iptables?
   Answer: Iptables is a firewall management tool for Linux systems. It allows administrators to configure rules for packet filtering and network address translation (NAT).

3. What is the purpose of the mangle table in iptables?
   Answer: The mangle table in iptables is used for modifying characteristics of packets as they traverse the firewall, such as packet headers and markings.

4. What are packet filtering rules used for firewall?
   Answer: Packet filtering rules are used to examine packets as they pass through a firewall and make decisions about whether to allow or deny them based on predefined criteria.

5. What criteria are typically used in packet filtering rules?
   Answer: Criteria such as source and destination IP addresses, port numbers, protocols, and packet states are commonly used in packet filtering rules.

6. What is Quality of Service (QoS) management?
   Answer: Quality of Service (QoS) management involves prioritizing certain types of network traffic to ensure a consistent level of service for critical applications.

7. How do iptables handle packet filtering?
   Answer: Iptables examines incoming and outgoing packets against a set of rules, applying actions (such as accept, drop, or reject) based on the criteria defined in the rules.

8. What is stateful inspection?
   Answer: Stateful inspection is a firewall technology that tracks the state of active connections and makes decisions based on the context of the traffic, allowing return traffic related to established connections without the need for explicit rules.

9. What is the default policy in firewall configuration?
   Answer: A default policy is a rule or set of rules that specify how to handle traffic that doesn't match any explicitly defined rules. For example, a default deny policy blocks all traffic unless explicitly permitted.

10. What is the purpose of packet marking in firewall configuration?

Answer: Packet marking is used to label packets with special identifiers, allowing for special treatment or routing decisions based on the markings.

11. What are some common actions in firewall rules?
Answer: Common actions in firewall rules include accepting, dropping, or rejecting packets, as well as logging matching traffic for monitoring and analysis purposes.

12. What is IPsec?
Answer: IPsec (Internet Protocol Security) is a suite of protocols used to secure IP communications by encrypting and authenticating IP packets.

13. What is the primary purpose of IPsec?
Answer: The primary purpose of IPsec is to provide confidentiality, integrity, and authenticity for IP communications, particularly over untrusted networks like the internet.

14. What are some components of IPsec?
Answer: Components of IPsec include encryption mechanisms, authentication methods, key management protocols (such as IKE), and security associations (SA).

15. How does IPsec contribute to VPNs?
Answer: IPsec is commonly used to establish secure VPN (Virtual Private Network) connections between network devices, ensuring encrypted and authenticated communication over public networks.

16. What is the role of encryption in IPsec?
Answer: Encryption in IPsec protects the confidentiality of data by encoding it in such a way that only authorized parties can decrypt and read it.

17. What is authentication in the context of IPsec?
Answer: Authentication in IPsec verifies the identities of communicating parties and ensures that data has not been altered or tampered with during transmission.

18. What is NAT (Network Address Translation)?
Answer: NAT is a technique used to modify network address information in IP packet headers while they are in transit across a routing device, typically to allow multiple devices on a private network to share a single public IP address.

19. What is Deep Packet Inspection (DPI)?
Answer: Deep Packet Inspection is a method of analyzing the contents of data packets as they pass through a network, allowing for more granular inspection and control based on the actual content of the packets.

# Job Sheet-2.1: Configure Firewall Services

**Task Overview:**

Configure and verify firewall services to ensure the security and proper functioning of network traffic according to organizational policies.

**Objectives:**

1. Secure network boundaries.
2. Control inbound and outbound traffic.
3. Implement organizational security policies.
4. Ensure minimal disruption to network services.

**Prerequisites:**

1. Access to firewall management interface.
2. Knowledge of network topology and policies.
3. Necessary administrative permissions.
4. Backup of current firewall configuration.
5. Updated documentation of network requirements and security policies.

**Steps to Configure Firewall Services:**

1. Preparation:

Review network topology and security policies.
Ensure all necessary permissions and access are granted.
Backup the current firewall configuration.

2. Access Firewall Management Interface:

Connect to the firewall management interface using the required software or web browser.
Authenticate using administrative credentials.

3. Configure Inbound Rules:

Navigate to the firewall rules section.
and apply the changes.

4. Configure Outbound Rules:

Navigate to the firewall rules section.
Add or update outbound rules according to security policies.
Specify the allowed IP addresses, ports, and protocols.
Save and apply the changes.

5. Configure Network Address Translation (NAT):

Navigate to the NAT settings.
Configure NAT rules as per network requirements.
Save and apply the changes.

6. Enable Logging and Monitoring:
Navigate to the logging and monitoring settings.
Enable logging for firewall rules and traffic.
Set up alerts and notifications for critical events.
Save and apply the changes.

7. Test Configuration:
Test the new configuration by simulating traffic.
Verify that the rules are correctly applied and traffic is as expected.
Check logs and monitoring tools for any anomalies.

8. Documentation and Reporting:
Document all changes made to the firewall configuration.
Update network diagrams and security policy documentation.
Prepare a report summarizing the changes and test results.

9. Review and Approval:
Review the configuration changes with relevant stakeholders.
Obtain necessary approvals for the changes.
Schedule a follow-up to review the impact of the changes.

**Troubleshooting Tips:**

- If connectivity issues arise, verify rule configurations and ensure there are no conflicts.
- Check logs for any denied traffic that should be allowed.
- Revert to the previous configuration using the backup if necessary.

**Completion Checklist:**

- [ ] Backup current firewall configuration.
- [ ] Configure inbound rules.
- [ ] Configure outbound rules.
- [ ] Configure NAT settings.
- [ ] Enable logging and monitoring.
- [ ] Test the configuration.
- [ ] Document changes.
- [ ] Obtain approvals.

## Specification Sheet-2.1: Configure Firewall Services

**Necessary Personal Protective Equipment (PPE)**

| Sl. No | Name of PPE | Unit | Quantity |
|---|---|---|---|
| 1 | Antistatic Wrist Strap | Pair | 01 |
| 2 | Safety Glasses | Pair | 01 |
| 3 | Gloves | Pair | 01 |
| 4 | Dust Mask | Pair | 01 |
| 5 | Knee Pads | Pair | 01 |
| 6 | Proper Footwear | Pair | 01 |
| 7 | Work Apron | Pair | 01 |

**Necessary tools and equipment**

| Sl. No | Name of Tools & Equipment | Specification | Unit | Quantity |
|---|---|---|---|---|
| 1 | Firewall management software. | | | |
| 2 | Network diagrams. | | | |
| 3 | Security policy documentation. | | | |
| 4 | Backup storage for current configuration. | | | |
| 5 | Laptop/PC with network access. | | No. | |
| 6 | | | Set | |

## Learning Outcome-3: Monitor The Threat

| | |
|---|---|
| Assessment Criteria | 1. Possible security threat is identified.<br>2. Possible cause of infection is determined.<br>3. Identified security threat is monitored to find out its characteristics with network monitoring tools.<br>4. Capability of the security threat is determined from the analysis. |
| Conditions and Resources | 1. Actual workplace or training environment<br>2. CBLM<br>3. Handouts<br>4. Laptop/ Desktop<br>5. Multimedia Projector<br>6. Paper, Pen, Pencil, and Eraser<br>7. Internet Facilities<br>8. Whiteboard and Marker |
| Contents | 1. Common security threat<br>2. Possible cause of infection<br>3. Common types of spam<br>4. Use of security threat monitoring tools.<br>▪ Wireshark<br>▪ Wincap<br>▪ NST<br>▪ Netminer<br>▪ Cable testers<br>5. Installing procedure of anti-malware software<br>6. Capability of common security threat |
| Activities/job/Task | 1. Monitor the threat using following activity:<br>▪ Identify Possible security threat.<br>▪ Determine Possible cause of infection<br>▪ Monitor Identified security threat to find out its characteristics with network monitoring tools.<br>▪ Determine Capability of the security threat from the analysis. |
| Training Methods | 1. Blended<br>2. Discussion<br>3. Presentation<br>4. Demonstration<br>5. Guided Practice<br>6. Individual Practice<br>7. Project Work<br>8. Problem Solving<br>9. Brainstorming |
| Assessment Methods | Assessment methods may include but not limited to<br>1. Written Test |

| | |
|---|---|
| | 2. Demonstration<br>3. Oral Questioning<br>4. Portfolio |

## Learning Experience-3: Monitor the threat

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

| Learning Activities | Recourses/Special Instructions |
|---|---|
| 1. Students will ask the instructor about "Monitor the threat." | 1. The instructor will provide the learning materials "Monitor the threat." |
| 2. Read the Information sheet and complete the Self-check & Check answer sheets on "Monitor the threat." | 1. Read Information sheet:<br>a. Common security threat<br>b. Possible cause of infection<br>c. Common types of spam<br>d. Use of security threat monitoring tools.<br>e. Installing procedure of anti-malware software<br>f. Capability of common security threat<br>2. Answer Self-check 1: Configure firewall services.<br>3. Check your answer with Answer key 1: Configure firewall services |
| 3. Read the Job/Task Sheet and Specification Sheet and perform job/Task | 1. Job/Task Sheet and Specification Sheet<br>**Job Sheet 3.1:** Monitor the threat<br>**Specification Sheet 3.1:** Monitor the threat |

# Information Sheet-3: Monitor The Threat

**Learning Objective:**

After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

3.1 Common security threat
3.2 Possible cause of infection
3.3 Common types of spam
3.4 Use of security threat monitoring tools.
- Wireshark
- Wincap
- NST
- Netminer
- Cable testers

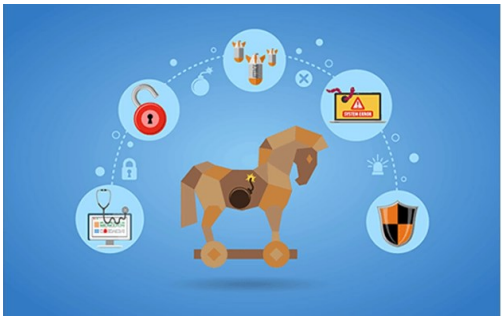
3.5 Installing procedure of anti-malware software
3.6 Capability of common security threat

## 3.1 Common Security

A common security threat in today's digital landscape is malware, which encompasses various types of malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or data. Here are some common forms of malware:

A. **Viruses:** Viruses are malicious programs that attach themselves to legitimate files or programs and replicate themselves to spread across systems. They can be transmitted through infected files, email attachments or compromised websites. Once activated, viruses can execute various harmful actions, such as deleting files, corrupting data, or even rendering the system inoperable. Their ability to self-replicate makes them particularly dangerous as they can quickly spread throughout a network.

B. **Trojans:**



Named after the legendary Trojan horse, Trojans are deceptive programs that masquerade as legitimate software or files to trick users into installing them. Once installed, Trojans often create backdoors or remote access points for hackers to gain unauthorized access to the system. They can also steal sensitive information, such as login credentials or financial data, and facilitate other types of malware infections.

Trojans commonly spread through email attachments, malicious websites, or software downloads from untrusted sources.

C. **Ransomware:**


Ransomware is a type of malware that encrypts the victim's files or locks them out of their system, demanding a ransom payment in exchange for decryption keys or restoring access. It typically spreads through malicious email attachments, compromised websites, or exploit kits.

Ransomware attacks can have devastating consequences for individuals and organizations, causing data loss, financial damages, and reputational harm. Some ransomware variants also threaten to publish stolen data unless the ransom is paid, adding an additional layer of extortion.

D. **Spyware:** Spyware is designed to stealthily monitor and collect information about a user's activities, such as browsing habits, keystrokes, and personal data, without their consent. It often operates covertly in the background, making it difficult for users to detect. Spyware can be used for various malicious purposes, including identity theft, espionage, and targeted advertising. It commonly infiltrates systems through bundled software installations, malicious websites, or infected email attachments.

E. **Adware**: Adware is software that displays unwanted advertisements, usually in the form of pop-ups or banners, to generate revenue for the developer. While not inherently malicious, adware can degrade system performance, consume network bandwidth, and disrupt the user experience. In some cases, adware may also collect and transmit user data to third parties without consent, raising privacy concerns. Adware often piggybacks on free software downloads or deceptive advertisements, tricking users into unwittingly installing it on their systems.

F. **Worms:** Worms are self-replicating malware that spread independently across networks by exploiting vulnerabilities in operating systems or software. Unlike viruses, worms do not require user interaction to spread and can propagate rapidly, infecting large numbers of

## 3.2 Possible cause of infection

In a network environment, there are several possible causes of infection by various types of malwares. Here are some common vectors through which malware can infiltrate and infect systems:

A. **Phishing Emails:** Phishing emails are one of the most prevalent methods used by attackers to distribute malware. These emails typically appear legitimate and may impersonate trusted entities, such as banks, government agencies, or well-known companies. They often contain malicious attachments or links that, when clicked or opened, execute malware on the recipient's system. Employees who inadvertently open such emails and interact with their contents can unknowingly trigger a malware infection.

B. **Malicious Websites:** Visiting compromised or malicious websites can expose users to drive-by downloads, where malware is automatically downloaded and executed without user intervention. Attackers may compromise legitimate websites by injecting malicious code or exploiting vulnerabilities in web servers or content management systems. Users who visit these sites with unpatched browsers or outdated software are at risk of having malware silently installed on their systems.

C. **Software Vulnerabilities**: Exploiting vulnerabilities in software applications, operating systems, or firmware is another common method used by attackers to deliver malware. Vulnerabilities are weaknesses or flaws in software code that can be exploited to gain unauthorized access or execute arbitrary code on a system. Attackers often use exploit kits or exploit publicly disclosed vulnerabilities for which patches are not yet available. Organizations that fail to promptly apply security patches or updates to their systems are susceptible to exploitation and subsequent malware infections.

D. **Removable Medi Answer:** USB drives, external hard drives, and other removable media can serve as vectors for malware transmission. Attackers may infect removable media with malware and strategically place them in public areas or targeted locations where they are likely to be picked up and used by unsuspecting individuals. Once connected to a computer, the infected media can automatically execute malware or prompt users to open malicious files, leading to an infection.

E. **Social Engineering:** Social engineering tactics exploit human psychology to manipulate individuals into divulging sensitive information or performing actions that compromise security. Attackers

may impersonate trusted entities, such as IT support personnel or coworkers, to deceive users into installing malware or disclosing login credentials. Social engineering techniques, such as pretexting, baiting, or tailgating, can be used in combination with other malware delivery methods to increase the likelihood of successful infections.

F. **Malicious File Downloads:** Downloading files from untrusted or compromised sources, such as file-sharing networks, pirated software repositories, or suspicious websites, can result in malware infections. Attackers may disguise malware as legitimate software, media files, or documents to entice users into downloading and executing them. Users who bypass security warnings or ignore file authenticity checks are at risk of inadvertently installing malware on their systems.

## 3.3 Common types of spam

### Computer spam

What comes to mind when you think of spam? Miracle pills from Internet pharmacies, requests for money from "princes" of other countries, or perhaps the food, Spam. This article is all about spam with a lowercase "s." While many people enjoy the food Spam, no one wants to be tricked into losing money or downloading malware because of the other kind of spam.

Spam is annoying, but it's also a threat. While many of us might think we're savvy enough to recognize any form of it, spammers regularly update their methods and messages to trick potential victims. The reality is that we're all constantly under attack from cybercriminals and the proof is in your inbox.

Also, Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

**What does spam stand for?**

| | |
|---|---|
| Spam is not an acronym for a computer threat, although some have been proposed (stupid pointless annoying malware, for instance). The inspiration for using the term "spam" to describe mass unwanted messages is a Monty Python skit in which the actors declare that everyone must eat the food Spam, whether they want it or not. Similarly, everyone with an email address must unfortunately be bothered by spam messages, whether we like it or not. |  |

**Types of spam**

Spammers use many forms of communication to bulk-send their unwanted messages. Some of these are marketing messages peddling unsolicited goods. Other types of spam messages can spread malware, trick you into divulging personal information, or scare you into thinking you need to pay to get out of trouble.

Email spam filters catch many of these types of messages, and phone carriers often warn you of a "spam risk" from unknown callers. Whether via email, text, phone, or social media, some spam messages do get through, and you want to be able to recognize them and avoid these threats. Below are several types of spam to look out for.

**a. Phishing emails**

Phishing emails are a type of spam cybercriminals send to many people, hoping to "hook" a few people. Phishing emails trick victims into giving up sensitive information like website logins or credit card information.

Adam Kujawa, Director of Malwarebytes Labs, says of phishing emails: "Phishing is the simplest kind of cyberattack and, at the same time, the most dangerous and effective. That is because it attacks the most vulnerable and powerful computer on the planet: the human mind."

**b. Email spoofing**

Spoofed emails mimic, or spoof, an email from a legitimate sender, and ask you to take some sort of action. Well-executed spoofs will contain familiar branding and content, often from a large well-known company such as PayPal or Apple. Common email spoofing spam messages include:

- A request for payment of an outstanding invoice
- A request to reset your password or verify your account
- Verification of purchases you didn't make
- Request for updated billing information
- Tech support scams

c. **Email Spam:** Email spam is perhaps the most well-known type of spam. It includes unsolicited emails sent to a large number of recipients without their consent. These emails often promote products or services, contain misleading advertisements, or attempt to trick recipients into disclosing personal information or downloading malware. Email spam can also include phishing attempts, where attackers impersonate legitimate entities to deceive users into providing sensitive information such as login credentials or financial details.

d. **SMS Spam:** SMS spam involves the sending of unsolicited text messages to mobile devices. Similar to email spam, SMS spam often promotes products or services, offers fake prizes or discounts, or attempts to trick recipients into divulging personal

information. SMS spam can be particularly intrusive and annoying, as it directly targets users' mobile phones, interrupting their daily activities.

e. **Social Media Spam**: Social media platforms are increasingly targeted by spammers seeking to exploit their large user bases. Social media spam can take various forms, including fake accounts, automated bots, spam comments or messages, and deceptive advertisements. Spammers may use social media spam to spread malware, phishing links, or fraudulent schemes, as well as to artificially inflate follower counts or engagement metrics.

f. **Forum and Blog Spam**: Spammers often target online forums, discussion boards, and blogs to post unsolicited or irrelevant content, known as forum or blog spam. This content may include advertisements, links to malicious websites, or irrelevant comments designed to manipulate search engine rankings. Forum and blog owners typically employ spam filters and moderation tools to combat spam and maintain the quality of their platforms.

g. **Instant Messaging Spam**: Instant messaging platforms, such as WhatsApp, Telegram, or Messenger, are also susceptible to spamming. Instant messaging spam may involve unsolicited messages sent to individual users or group chats, often containing advertisements, phishing links, or malware attachments. Spammers may use automated bots to distribute spam messages on a large scale, targeting users with unwanted content.

h. **Comment Spam:** Comment spam refers to unsolicited or irrelevant comments posted on websites, blogs, or social media posts. Comment spammers often use automated tools to post large volumes of comments containing links to unrelated websites, advertisements, or malicious content. Comment spam can degrade the user experience, clutter discussion threads, and undermine the credibility of the platform.

**i. Current event scams**

Hot topics in the news can be used in spam messages to get your attention. In 2020 when the world was facing the Covid-19 pandemic and there was an increase in work-from-home jobs, some scammers sent spam messages promising remote jobs that paid in Bitcoin. During the same year, another popular spam topic was related to offering financial relief for small businesses, but the scammers ultimately asked for bank account details. News headlines can be catchy, but beware of them in regards to potential spam messages.

**j. Advance-fee scams**

This type of spam is likely familiar to anyone who has been using email since the 90s or 2000s. Sometimes called "Nigerian prince" emails as that was the purported message sender for many years, this type of spam promises a financial reward if you first provide a cash advance. The sender typically indicates that this cash advance is some sort of processing fee or earnest money to unlock the larger sum, but once you pay, they disappear. To make it more personal, a similar type of scam involves the sender pretending to be a family member that is in trouble and needs money, but if you pay, unfortunately the outcome is the same.

**k. Malspam**

Short for "malware spam" or "malicious spam," malspam is a spam message that delivers malware to your device. Unsuspecting readers who click on a link or open an email attachment end up with some type of malware including ransomware, Trojans, bots, info-stealers, cryptominers, spyware, and keyloggers. A common delivery method is to include malicious scripts in an attachment of a familiar type like a Word document, PDF file, or PowerPoint presentation. Once the attachment is opened, the scripts run and retrieve the malware payload.

**Spam calls and spam texts.**

Have you ever received a robocall? That's called spam. A text message from an unknown sender urging you to click an unknown link? That's referred to as text message spam or "smishing," a combination of SMS and phishing.

## 3.4 Use of security threat monitoring tools.

Security threat monitoring tools are essential for maintaining the integrity, confidentiality, and availability of an organization's IT infrastructure. These tools help identify, analyze, and respond to potential security threats and vulnerabilities in real-time. Here are some common types of security threat monitoring tools and their uses:

**Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):**

IDS: Monitors network traffic for suspicious activity and alerts administrators. It is a passive system that does not take action on its own.

IPS: Similar to IDS, but it can also take actions to block or prevent detected threats.

**Security Information and Event Management (SIEM) Systems:**

Collects and analyzes data from various sources within an organization to provide a comprehensive view of the security posture.

Correlates events and logs to identify patterns indicative of potential security incidents.

**Endpoint Detection and Response (EDR) Tools:**

Provides continuous monitoring and response capabilities for endpoint devices like computers and mobile devices.

Detects and investigates suspicious activities and responds to security incidents.

**Network Traffic Analysis (NTA) Tools:**
Monitors network traffic to identify unusual patterns or anomalies that may indicate a security threat.
Helps in detecting malware, ransomware, and other malicious activities within the network.

**Vulnerability Management Tools:**
Scans systems and networks to identify vulnerabilities that could be exploited by attackers.
Prioritizes vulnerabilities based on risk and helps in patch management.

**User and Entity Behavior Analytics (UEBA):**
Analyzes the behavior of users and entities (e.g., devices) to identify deviations from normal patterns.
Helps in detecting insider threats, compromised accounts, and advanced persistent threats (APTs).

**Threat Intelligence Platforms (TIP):**
Aggregates and analyzes threat data from various sources to provide actionable intelligence.
Helps organizations stay informed about emerging threats and adjust their defenses accordingly.

**Firewall and Unified Threat Management (UTM) Systems:**
Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules.
UTM systems combine multiple security features, such as firewalls, antivirus, and content filtering, into a single platform.

**Deception Technology**
Deploys decoys and traps to detect and mislead attackers.
Provides early warning of potential attacks and gathers information about attack techniques.

## Wireshark

Wireshark is a powerful, open-source network protocol analyzer widely used for network troubleshooting, analysis, software and protocol development, and education. It allows users to capture and interactively browse the traffic running on a computer network. Here are some key aspects of Wireshark:

**Features of Wireshark**
**Packet Capture:**
Wireshark can capture live network data from a variety of network media, including Ethernet, Wi-Fi, Bluetooth, and more.
It can capture packets in real-time and display them in a detailed and organized manner.

**Deep Inspection:**
Wireshark performs deep inspection of hundreds of protocols, with more being added continuously.

It can analyze and decode the details of various network protocols, providing insights into the structure and content of network traffic.

**Filtering and Search:**
Users can apply powerful display filters to focus on specific traffic or events of interest.
Wireshark supports complex filter expressions to narrow down captured data to relevant packets.

**Visualization:**
Wireshark offers various visualization tools such as packet details, packet bytes, protocol hierarchy, and flow graphs.
These visual tools help in understanding traffic patterns and identifying anomalies.

**Exporting and Reporting:**
Captured data can be saved in various file formats (e.g., pcap, pcapng) for later analysis.
Wireshark provides options to generate reports and export data for further processing.

**Cross-Platform:**
Wireshark is available for multiple operating systems, including Windows, macOS, and Linux.

## How to Use Wireshark

**Installation**
Download and install Wireshark from the official website (https://www.wireshark.org/).
Ensure appropriate permissions to capture network traffic on your system (e.g., running Wireshark as an administrator on Windows).

**Capturing Traffic**
Select the network interface to capture traffic from (e.g., Ethernet, Wi-Fi).
Start the capture session to begin collecting network packets.

**Analyzing Packets**
Use display filters to narrow down the packets of interest (e.g., `http`, `tcp.port == 80`).
Inspect packet details to understand the communication between devices.

**4. Saving and Exporting Dat Answer**
Save captured packets to a file for later analysis or sharing.
Export specific data or generate reports based on the analysis.

**Applying Advanced Features**
Use built-in tools like IO graphs, protocol hierarchy statistics, and expert information to gain deeper insights.
Leverage dissectors and plugins for specialized analysis.

## Wincap

WinPcap is a network packet capture library for Windows that provides the low-level network access needed for packet capture and network analysis. It allows applications to capture and transmit network packets bypassing the protocol stack, and has been used by many network tools including Wireshark. Here are the key aspects of WinPcap:

**Features of WinPcap:**

**Packet Capture:**

Captures raw packets from the network, both incoming and outgoing, allowing for detailed traffic analysis.

Supports packet filtering to capture only specific types of traffic.

**Packet Injection:**

Allows applications to inject custom packets into the network, useful for network testing and protocol development.

**High-Performance:**

Designed for efficiency, allowing for high-speed packet capture and analysis.

**Kernel-Level Packet Filtering:**

Implements a kernel-level filter to reduce the amount of data copied to user space, improving performance and reducing CPU usage.

**Support for Multiple Protocols:**

Supports a wide range of network protocols, making it versatile for various types of network analysis.

**Installation and Usage:**

**Download and Install:**

WinPcap can be downloaded from its official website or other trusted sources.

Installation typically involves running an installer and following the on-screen instructions.

**Integration with Applications:**

Many network tools, such as Wireshark, integrate WinPcap to capture and analyze network traffic.

Developers can use the WinPcap API to build custom network analysis applications.

**Starting a Capture Session:**

Choose the network interface to capture packets from.

Apply filters to capture specific types of traffic if needed.

Start the capture session to begin collecting network packets.

**NST**

NST (Network Security Toolkit) is a Linux-based live bootable ISO that provides a comprehensive suite of open-source network security tools. It is designed for network administrators and security professionals to perform network security assessments, monitoring, and diagnostics. Here are the key features and uses of NST:

**Key Features of NST:**

**Live Environment:**

- NST can be run directly from a bootable CD, DVD, or USB drive without installation, providing a portable and secure environment for network analysis.

**Web-based Interface:**

- NST provides a web-based graphical user interface (GUI) called the NST WUI, which simplifies access to its various tools and utilities.

**Extensive Toolset:**

- Includes a wide array of network security tools for tasks such as packet capture, traffic analysis, vulnerability assessment, network mapping, and intrusion detection.
- Notable tools include Wireshark, Nmap, Snort, Nessus, and many others.

**Packet Capture and Analysis:**

- Capable of capturing network traffic for in-depth analysis using tools like Wireshark and Tcpdump.
- Provides real-time traffic monitoring and analysis.

**Network Scanning and Mapping:**

- Includes tools like Nmap for network scanning and discovery.
- Can create detailed network maps and diagrams to visualize network topologies.

**Vulnerability Assessment:**

- Features tools for scanning networks and systems for vulnerabilities and security weaknesses.
- Integrates with Nessus for comprehensive vulnerability scanning.

**Intrusion Detection:**

- Supports intrusion detection systems (IDS) like Snort for monitoring network traffic and detecting malicious activity.
- Provides alerting and logging capabilities for detected threats.

**Wireless Networking:**

- Includes tools for wireless network analysis, including Aircrack-ng for wireless security testing and monitoring.

**System Monitoring:**

- Offers tools for monitoring system performance and resource usage.
- Includes utilities for process management, disk usage analysis, and system health monitoring.

**NetMiner**

NetMiner is a software tool designed for network analysis and visualization. It is used to analyze and visualize complex networks and relationships within data. NetMiner is widely used in various fields, including social network analysis, data mining, and network research. Here are the key aspects and features of NetMiner:

**Key Features of NetMiner:**

**Data Import and Management:**

- Supports various data formats for import, including CSV, Excel, and databases.
- Allows for the integration and management of multiple datasets.

**Network Visualization:**

- Provides advanced visualization techniques to display networks and their properties.
- Supports various layouts and customization options for effective visual representation.

**Network Analysis:**

- Offers a comprehensive set of tools for analyzing network structure and properties.
- Includes measures for centrality, clustering, path analysis, and community detection.

**Data Mining and Machine Learning:**

- Integrates data mining and machine learning algorithms to discover patterns and relationships within the network.
- Supports classification, clustering, and predictive modeling.

**Dynamic Network Analysis:**

- Allows for the analysis of dynamic networks, capturing changes over time.
- Supports the visualization and analysis of temporal patterns and trends.

**Geospatial Network Analysis:**

- Incorporates geospatial data to analyze and visualize networks in a geographical context.
- Supports mapping and spatial analysis of network data.

**Statistical Analysis:**

- Provides statistical tools to test hypotheses and validate network models.
- Supports various statistical tests and modeling techniques.

**Interactive Exploration:**

- Enables interactive exploration of network data, allowing users to drill down into specific nodes and edges.
- Supports filtering and manipulation of network elements.

**Use Cases for NetMiner:**

Social Network Analysis:

- Analyzes relationships and interactions within social networks.
- Identifies influential individuals, community structures, and information flow.

Organizational Network Analysis:
- Examines communication patterns and collaboration within organizations.
- Helps in identifying key players and improving organizational efficiency.

Marketing and Customer Analysis:
- Analyzes customer relationships and

**Cable Testers**

Cable testers are essential tools used to diagnose and troubleshoot issues with various types of cables, ensuring they are functioning correctly and efficiently. These devices are widely used in networking, telecommunications, and electrical installations to verify the integrity and performance of cables. Here are the key aspects of cable testers:

**Key Features of Cable Testers:**

Cable Continuity Testing:
- Verifies that all wires within a cable are correctly connected end-to-end.
- Detects broken wires, shorts, and miswiring.

**Wiremap Testing:**
- Checks the wiring configuration of twisted-pair cables (e.g., Ethernet cables) to ensure correct pin-to-pin connections.
- Identifies crossed wires, split pairs, and other wiring faults.

**Signal Quality Testing:**
- Measures the quality of the signal passing through the cable.
- Evaluates parameters such as signal loss (attenuation), crosstalk, and return loss.

**Length Measurement:**
- Determines the length of the cable.
- Helps identify where a break or fault might be located along the cable.

**PoE (Power over Ethernet) Testing:**
- Verifies the presence and type of PoE on Ethernet cables.
- Ensures that PoE devices are receiving the correct power levels.

**Cable Certification:**
- Provides detailed reports and certification for installed cabling systems.
- Ensures compliance with industry standards and specifications.

**Types of Cable Testers**

**Basic Continuity Testers:**
- Simple devices that check for continuity in the cable.
- Often used for basic troubleshooting and verification.

**Advanced Network Cable Testers:**
- More sophisticated devices that test various parameters of network cables (e.g., Cat5e, Cat6, Cat7).
- Can perform wiremap testing, signal quality testing, and length measurement.

**Optical Fiber Testers:**
- Designed specifically for testing optical fiber cables.
- Includes tools like optical time-domain reflectometers (OTDR) and optical power meters to measure signal loss and identify faults in fiber optic cables.

**Multifunction Cable Testers:**
- Combine multiple testing functions in one device.
- Suitable for testing various types of cables, including Ethernet, coaxial, and telephone cables.

**Use Cases for Cable Testers:**
1. Network Installation and Maintenance:
- Ensure that network cables are correctly installed and functioning.
- Diagnose and repair issues in existing network infrastructure.

**Telecommunications:**
- Verify the integrity of telephone lines and coaxial cables.
- Ensure that communication systems are working properly.

**Electrical Installations:**
- Test and verify the connections in electrical wiring.
- Ensure the safety and reliability of electrical systems.

**Audio/Visual Systems:**
Check the integrity of cables used in audio/visual installations.
Ensure that audio and video signals are transmitted without loss or interference.

## 3.5 Installing procedure of anti-malware software

Installing anti-malware software is a crucial step in protecting your computer from malicious software such as viruses, trojans, spyware, and ransomware. Here's a step-by-step guide to help you install anti-malware software:

**Step-by-Step Installation Procedure for Anti-Malware Software:**

**Choose Anti-Malware Software:**

- Research and select reputable anti-malware software. Some popular options include
- Malwarebytes, Norton, Kaspersky, Bitdefender, and McAfee.

**Download the Software:**

- Go to the official website of the chosen anti-malware software.
- Locate the download link, which is usually found on the product page or under a "Downloads" or "Get Started" section.
- Click the download link to save the installer file to your computer.

**Prepare for Installation:**

- Close all unnecessary applications and save your work.
- Ensure your internet connection is stable, as the installation may require downloading additional files or updates.

**4. Run the Installer:**

- Locate the downloaded installer file, usually in your Downloads folder.
- Double-click the installer file to start the installation process.
- If prompted by User Account Control (UAC), click "Yes" to allow the installer to make changes to your computer.

**Follow the Installation Wizard:**

- The installation wizard will guide you through the setup process. Follow these steps:
- Language Selection: Choose your preferred language and click "Next."
- License Agreement: Read the End User License Agreement (EULA). If you agree to the terms, select "I agree" or "Accept" and click "Next."
- Installation Type: Choose between a default or custom installation. Default is usually recommended for most users. Click "Next."
- Installation Location: Select the destination folder for the software. The default location is typically fine. Click "Next."

**Install the Software:**

- Click the "Install" button to begin the installation process.
- Wait for the installation to complete. This may take a few minutes.

**Complete the Installation:**

- Once the installation is complete, you may be prompted to restart your computer. Save your work and restart if necessary.

## Self-Check-3: Monitor The Threat

### Questionnaire

**1 What is Wireshark used for?**
Answer:

**2 What is the purpose of Nmap?**
Answer:

**3 What does NST stand for in network security?**
Answer:

**4 What is the primary function of Cable Testers?**
Answer:

**5 What is a common type of malware?**
Answer:

**6 What is phishing?**
Answer:

**7 What is the purpose of a firewall?**
Answer:

**8 What does SQL Injection exploit?**
Answer:

**9 What is a DDoS attack?**
Answer:

**10 What is XSS in web security?**
Answer:

**11 What does 'APT' stand for in cybersecurity?**
Answer:

**12 What is the function of an anti-malware software?**
Answer:

**13 What is a zero-day exploit?**
Answer:

**14 What is spam?**
Answer:

**15 What is smishing?**
Answer:

**16 What is an example of a social engineering attack?**
Answer:

## Answer Key-3: Monitor The Threat

**1 What is Wireshark used for?**
Answer: Wireshark is a network protocol analyzer used for capturing and analyzing network traffic in real-time.

**2 What is the purpose of Nmap?**
Answer: Nmap is used for network discovery and security auditing, including scanning for open ports and identifying network services.

**3 What does NST stand for in network security?**
Answer: NST stands for Network Security Toolkit, a live bootable Linux distribution with a suite of network security tools.

**4 What is the primary function of Cable Testers?**
Answer: Cable testers are used to diagnose and troubleshoot issues with cables, including checking continuity and signal quality.

**5 What is a common type of malware?**
Answer: Common types of malwares include viruses, ransomware, trojans, and spyware.

**6 What is phishing?**
Answer: Phishing is a type of attack where attackers deceive individuals into providing sensitive information by pretending to be a trustworthy entity.

**7 What is the purpose of a firewall?**
Answer: A firewall helps protect a network by controlling incoming and outgoing traffic based on security rules.

**8 What does SQL Injection exploit?**
Answer: SQL Injection exploits vulnerabilities in a web application's database queries to gain unauthorized access or manipulate data.

**9 What is a DDoS attack?**
Answer: A Distributed Denial of Service (DDoS) attack floods a target with traffic from multiple sources to make it unavailable.

**10 What is XSS in web security?**
Answer: Cross-Site Scripting (XSS) involves injecting malicious scripts into web pages to execute in a user's browser.

**11 What does 'APT' stand for in cybersecurity?**
Answer: APT stands for Advanced Persistent Threat, a prolonged and targeted cyberattack where an intruder remains undetected.

**12 What is the function of an anti-malware software?**
Answer: Anti-malware software detects, prevents, and removes malicious software from a computer system.

**13 What is a zero-day exploit?**

Answer: A zero-day exploit targets vulnerabilities that are unknown to the software vendor and have no patches available.

**14 What is spam?**

Answer: Spam refers to unsolicited or unwanted messages, often sent in bulk, for advertising or malicious purposes.

**15 What is smishing?**

Answer: Smishing is phishing via SMS, where attackers send fraudulent text messages to trick individuals into revealing personal information.

**16 What is an example of a social engineering attack?**

Answer: An example of a social engineering attack is pretexting, where an attacker creates a fabricated scenario to obtain sensitive information.

# Job Sheet-3.1: Monitor the threat

## Step 1: Identify Possible Security Threat

a. Use various tools and techniques to identify potential security threats, such as:
   - Network traffic analysis
   - System logs
   - Network-based intrusion detection systems (NIDS)
   - Host-based intrusion detection systems (HIDS)
   - Malware analysis

b. Look for unusual patterns or anomalies in network traffic, system logs, or system performance.

c. Identify potential threats such as:
   - Malware infections
   - Unauthorized access attempts
   - Denial-of-Service (DoS) attacks
   - Man-in-the-middle (MitM) attacks

## Step 2: Determine Possible Cause of Infection

a. Once a potential threat has been identified, determine the cause of the infection or attack.

b. Use tools such as:
   - Network protocol analyzers
   - Reverse engineering tools
   - Memory dump analysis tools

c. Analyze network traffic captures, system logs, and other data to identify the source of the threat.

d. Determine if the threat is:
   - A known malware variant
   - A zero-day exploit
   - A targeted attack

## Step 3: Monitor Identified Security Threat to Find Out Its Characteristics

a. Use network monitoring tools to gather more information about the security threat.

b. Tools may include:
   - Network packet sniffers (e.g., Wireshark)
   - Network traffic analysis software (e.g., Snort)
   - System monitoring software (e.g., Nagios)

c. Monitor the threat's behavior, such as:
   - Communication protocols used (e.g., TCP/IP, DNS)
   - Data being transmitted (e.g., malware payloads, login credentials)
   - Source and destination IP addresses
   - Ports and protocols used

d. Note any unusual or suspicious behavior, such as:
   - Unusual network traffic patterns
   - Unusual system logs or system events
   - Unusual system performance metrics

## Step 4: Determine Capability of the Security Threat

a. Based on the monitoring data collected, determine the capabilities of the security threat, such as:
   - What it can do (e.g., data exfiltration, system compromise)

- How it operates (e.g., remotely, locally)
- What resources it requires (e.g., specific software, hardware)

b. Consider the threat's potential impact on the organization, including:
    - Data confidentiality
    - Data integrity
    - System availability
    - Reputation damage

**Additional Steps**

a. Continuously monitor the security threat to track its behavior and detect any changes or updates.
b. Share findings with relevant stakeholders, such as security teams, IT teams, and management.
c. Develop a response plan to contain and remediate the security threat.
d. Implement measures to prevent similar threats in the future.
    - Network packet sniffers (e.g., Wireshark)
    - Network traffic analysis software (e.g., Snort)
    - System monitoring software (e.g., Nagios)

# Specification Sheet-3.1: Monitor the threat

**Necessary Personal Protective Equipment (PPE)**

| Sl. No | Name of PPE | Unit | Quantity |
|---|---|---|---|
| 1 | Antistatic Wrist Strap | Pair | 01 |
| 2 | Safety Glasses | Pair | 01 |
| 3 | Gloves | Pair | 01 |
| 4 | Dust Mask | Pair | 01 |
| 5 | Knee Pads | Pair | 01 |
| 6 | Proper Footwear | Pair | 01 |
| 7 | Work Apron | Pair | 01 |

**Necessary tools and equipment**

| Sl. No | Name of Tools & Equipment | Specification | Unit | Quantity |
|---|---|---|---|---|
| 1 | Firewall management software. | | | |
| 2 | Network diagrams. | | | |
| 3 | Security policy documentation. | | | |
| 4 | Backup storage for current configuration. | | | |
| 5 | Laptop/PC with network access. | | No. | |
| 6 | | | Set | |

## Learning Outcome-4: Configure Firewall Services

| | |
|---|---|
| Assessment Criteria | 1. Network device hardening is interpreted.<br>2. Network attack prevention is interpreted.<br>3. Report is prepared using monitoring system.<br>4. Report is documented and submitted to the authority |
| Conditions and Resources | 1. Actual workplace or training environment<br>2. CBLM<br>3. Handouts<br>4. Laptop/ Desktop<br>5. Multimedia Projector<br>6. Paper, Pen, Pencil, and Eraser<br>7. Internet Facilities<br>8. Whiteboard and Marker |
| Contents | 1. Network device hardening technique.<br>2. Network attack prevention technique.<br>3. Report preparation using monitoring system.<br>4. Documentation procedure for submitting report to the authority. |
| Activities/job/Task | 1. Document and report the threat using following activity:<br>▪ Interpret Network device hardening<br>▪ Interpret Network attack prevention<br>▪ Prepare Report using monitoring system<br>▪ Document and submit Report to the authority |
| Training Methods | 1. Blended<br>2. Discussion<br>3. Presentation<br>4. Demonstration<br>5. Guided Practice<br>6. Individual Practice<br>7. Project Work<br>8. Problem Solving<br>9. Brainstorming |
| Assessment Methods | Assessment methods may include but not limited to<br>1. Written Test<br>2. Demonstration<br>3. Oral Questioning<br>4. Portfolio |

## Learning Experience-4: Configure Firewall Services

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

| Learning Activities | Recourses/Special Instructions |
|---|---|
| 4. Students will ask the instructor about "Document and report the threat." | a. The instructor will provide the learning materials "Document and report the threat." |
| 5. Read the Information sheet and complete the Self-check & Check answer sheets on "Document and report the threat." | 1. Read Information sheet:<br>a. Network device hardening technique.<br>b. Network attack prevention technique.<br>c. Report preparation using monitoring system.<br>d. Documentation procedure for submitting report to the authority.<br>2. Answer Self-check 4: Document and report the threat.<br>3. Check your answer with Answer key 4: Document and report the threat |
| 6. Read the Job/Task Sheet and Specification Sheet and perform job/Task | 2. Job/Task Sheet and Specification Sheet<br>**Job Sheet 4.1:** Document and report the threat<br>**Specification Sheet 4.1:** Document and report the threat |

# Information Sheet-4: Document And Report The Threat

**Learning Objective:**

After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

4.1 Network device hardening technique.
4.2 Network attack prevention technique.
4.3 Report preparation using monitoring system.
4.4 Documentation procedure for submitting the report to the authority.

## 4.1 Network device hardening technique.

Network device hardening involves implementing various techniques to secure network devices like routers, switches, firewalls, and access points against unauthorized access and attacks. Here are some key techniques:

a. Change Default Credentials: Always change default usernames and passwords. Use strong, unique passwords and consider implementing multi-factor authentication.

b. Update Firmware and Software: Regularly update the device firmware and software to patch known vulnerabilities and improve security features.

c. Disable Unnecessary Services: Turn off any services or protocols that are not needed. This reduces the potential attack surface.

d. Use Access Control Lists (ACLs): Implement ACLs to control which devices can access the network device and specify what actions they can perform.

e. Implement Network Segmentation: Divide the network into segments to limit the impact of a potential breach and restrict access to critical systems.

f. Enable Logging and Monitoring: Turn on logging and monitor device activity for any suspicious behavior. Regularly review logs for signs of unauthorized access or other issues.

g. Configure Firewalls and Intrusion Detection Systems (IDS): Use firewalls to filter traffic and IDS to detect and respond to potential threats.

h. Secure Management Interfaces: Restrict access to management interfaces to trusted IP addresses and use encrypted management protocols like SSH instead of Telnet.

i. Implement Strong Encryption: Use strong encryption methods for data in transit and at rest to protect sensitive information.

j. Backup Configuration Files: Regularly back up device configuration files and store them securely to recover quickly in case of a failure or compromise.

k. Physical Security: Ensure that network devices are physically secured to prevent unauthorized access or tampering.

l. Regular Audits and Reviews: Conduct regular security audits and reviews to ensure that security policies are up to date and effective.

## 4.2 Network attack prevention technique.

Preventing network attacks involves implementing a range of strategies and techniques designed to detect, deter, and mitigate threats before they can compromise the network. Here are some key techniques for network attack prevention:

a. Firewalls: Deploy firewalls to monitor and filter incoming and outgoing network traffic based on predefined security rules. This helps to block unauthorized access and malicious traffic.

b. Intrusion Detection and Prevention Systems (IDPS): Use IDPS to detect and respond to suspicious activity in real time. Intrusion Prevention Systems (IPS) can actively block or mitigate threats.

c. Network Segmentation: Divide the network into segments or zones to contain and limit the impact of potential attacks. This helps to prevent lateral movement within the network.

d. Virtual Private Networks (VPNs): Implement VPNs to encrypt traffic and ensure secure remote access to the network, protecting data from interception.

e. Regular Software and Firmware Updates: Keep all network devices, software, and firmware up to date with the latest security patches to fix vulnerabilities that could be exploited by attackers.

f. Access Controls: Implement strong access control measures, including least privilege principles and multi-factor authentication (MFA), to ensure that only authorized users have access to network resources.

g. Security Information and Event Management (SIEM): Use SIEM systems to aggregate, analyze, and respond to security events and incidents across the network, improving threat detection and response.

## 4.3 Report preparation using monitoring system.

Preparing a report using a network monitoring system involves collecting, analyzing, and presenting data on network performance, security, and usage. Here's a step-by-step guide to help you prepare an effective report:

**Define the Report Objectives**

- Purpose: Determine what the report aims to achieve. This could be performance analysis, security incident review, or usage trends.
- Audience: Identify who will be reading the report (e.g., IT staff, management, executives) and tailor the content accordingly.

**Gather Data**

- Data Collection: Use your network monitoring system to collect relevant data, including traffic statistics, error rates, security events, and performance metrics.
- Time Frame: Specify the reporting period (e.g., daily, weekly, monthly) and ensure that data for this period is available.

**Analyze Data**

- Performance Metrics: Analyze network performance metrics such as bandwidth usage, latency, packet loss, and uptime.
- Security Events: Review security logs for any detected threats, anomalies, or incidents.
- Trend Analysis: Identify any trends or patterns in network usage and performance over time.
- Comparative Analysis: Compare current data with historical data or benchmarks to assess improvements or regressions.

**Generate Visualizations**

- Charts and Graphs: Create visual representations of data, such as line graphs for performance trends, bar charts for traffic volumes, and pie charts for resource utilization.
- Maps: Include network topology maps if relevant to illustrate the impact of issues or changes.

**Draft the Report**

- Executive Summary: Provide a high-level overview of key findings, trends, and recommendations. This section should be concise and focused on the most critical information.
- Detailed Analysis: Include detailed sections covering performance metrics, security events, and other relevant data. Use visualizations to support your analysis.
- Findings and Recommendations: Highlight significant findings and offer actionable recommendations for improving performance or addressing security issues.
- Appendices: Include additional data, raw logs, or supplementary information in appendices if needed.

**Review and Refine**

- Accuracy Check: Verify the accuracy of data and analysis. Ensure that visualizations correctly represent the data.
- Clarity: Ensure that the report is clear and easy to understand. Avoid technical jargon if the audience is non-technical.

## 4.4 Documentation procedure for submitting the report to the authority.

When submitting a report to an authority, it's important to follow a structured documentation procedure to ensure clarity, compliance, and proper handling. Here's a detailed procedure for submitting a report:

**Prepare the Report**

- Finalize Content: Ensure the report is complete, accurate, and free from errors. Review the findings, recommendations, and supporting data.
- Format and Style: Confirm that the report follows any specified formatting and style guidelines. This might include specific fonts, headings, and layout requirements.

**Review and Approval**

- Internal Review: Have the report reviewed by relevant internal stakeholders (e.g., team members, department heads) to gather feedback and make necessary revisions.
- Approval: Obtain formal approval from a designated authority or manager, if required. This may involve signing off on the report to confirm its accuracy and completeness.

**Prepare Submission Documentation**

- Cover Letter: Draft a cover letter to accompany the report. This letter should briefly summarize the purpose of the report, highlight key findings, and specify the intended recipient.
- Executive Summary: Ensure that the executive summary is included either within the report or as a separate document, providing a concise overview of the report's main points.

**Submit the Report**

- Determine Submission Method: Identify the preferred submission method for the authority. This could be through email, a physical copy, or an online submission system.
- Email: Attach the report and cover letter to an email. Include a clear subject line (e.g., "Submission of [Report Title] - [Date]") and a brief message in the email body.
- Physical Copy: If submitting a physical copy, print the report and cover letter. Ensure they are properly bound or organized, and deliver them to the designated recipient.
- Online Submission: If using an online portal, follow the submission guidelines provided. Upload the report and any accompanying documents as required.

**Confirmation and Tracking**

- Acknowledge Receipt: Request confirmation of receipt from the authority to ensure that the report has been received. This might be an automated confirmation for online submissions or a receipt acknowledgment for physical submissions.
- Track Submission: Maintain a record of the submission date, method, and any confirmation received. This will help in tracking the submission status and following up if necessary.

**Follow-Up**

- Review Status: Periodically check on the status of the report, especially if you have not received confirmation or feedback within the expected timeframe.
- Address Feedback: Be prepared to address any follow-up questions or requests for additional information from the authority.

## Self-Check-4: Document and Report The Threat

1. **What is the first step in hardening network devices?**
   ANSWER:

2. **Why is updating firmware important for network device security?**
   ANSWER:

3. **How can you reduce the attack surface on network devices?**
   ANSWER:

4. **What role do Access Control Lists (ACLs) play in network security?**
   ANSWER:

5. **Why is network segmentation useful?**
   ANSWER:

6. **What is the function of a firewall in network attack prevention?**
   ANSWER:

7. **What is the benefit of using Intrusion Detection and Prevention Systems (IDPS)?**
   ANSWER:

8. **Why should you implement VPNs?**
   ANSWER:

9. **How can regular software updates contribute to network security?**
   ANSWER:

10. **What is the importance of network monitoring?**
    ANSWER:

11. **What is the first step in preparing a network report?**
    ANSWER:

12. **What should you analyze in the network data?**
    ANSWER:

13. **How can you make your report more understandable?**
    ANSWER:

14. **What is an executive summary?**
    ANSWER:

15. **Why is it important to review the report before submission?**
    ANSWER:

## Answer Key-4: Document and Report the Threat

1. **What is the first step in hardening network devices?**
   **Answer**: Change default usernames and passwords to strong, unique ones.

2. **Why is updating firmware important for network device security?**
   **Answer**: It patches vulnerabilities and enhances security features.

3. **How can you reduce the attack surface on network devices?**
   **Answer**: By disabling unnecessary services and protocols.

4. **What role do Access Control Lists (ACLs) play in network security?**
   **Answer**: ACLs control which devices can access the network device and their actions.

5. **Why is network segmentation useful?**
   **Answer**: It limits the impact of a breach by isolating different network areas.

6. **What is the function of a firewall in network attack prevention?**
   **Answer**: It filters incoming and outgoing network traffic based on security rules.

7. **What is the benefit of using Intrusion Detection and Prevention Systems (IDPS)?**
   **Answer**: They detect and respond to suspicious activity in real-time.

8. **Why should you implement VPNs?**
   **Answer**: To encrypt traffic and secure remote access to the network.

9. **How can regular software updates contribute to network security?**
   **Answer**: They fix vulnerabilities and improve security features.

10. **What is the importance of network monitoring?**
    **Answer**: It helps identify unusual patterns or anomalies that could indicate a potential attack.

11. **What is the first step in preparing a network report?**
    **Answer**: Define the report's objectives and audience.

12. **What should you analyze in the network data?**
    **Answer**: Performance metrics, security events, trends, and comparative analysis.

13. **How can you make your report more understandable?**
    **Answer**: Use visualizations like charts and graphs to represent data.

14. **What is an executive summary?**
    Answer: A high-level overview of key findings and recommendations in the report.

15. **Why is it important to review the report before submission?**
    Answer: To ensure accuracy and clarity, and to gather feedback for improvements.

# Job Sheet-4.1: Document and report the threat

**Working Procedures**

**Step 1: Interpret Network Device Hardening**

- Analyze the network devices involved in the security threat, including:
  - Firewalls
  - Routers
  - Switches
  - Servers
- Identify any vulnerabilities or misconfigurations that may have contributed to the security threat.
- Document any changes made to the network devices to harden them against future threats, including:
  - Configuration changes
  - Firmware updates
  - Patching

**Step 2: Interpret Network Attack Prevention**

- Analyze the network attack prevention measures implemented to prevent the security threat, including:
  - Intrusion detection systems (IDS)
  - Intrusion prevention systems (IPS)
  - Firewall rules
  - Access control lists (ACLs)
- Identify any gaps or weaknesses in these measures that may have allowed the security threat to occur.
- Document any changes made to the attack prevention measures, including:
  - Configuration changes
  - Rule updates
  - Signature updates

**Step 3: Prepare Report using Monitoring System**

- Use monitoring system data to prepare a detailed report on the security threat, including:
  - Timeline of events
  - Network traffic captures
  - System logs
  - Malware analysis results
- Organize the report into sections, including:
  - Introduction
  - Threat description
  - Analysis of network device hardening and attack prevention measures
  - Recommendations for remediation and mitigation
- Include any relevant screenshots, diagrams, or charts to support the report.

**Step 4: Document and Submit Report to Authority**

- Document the report in a standard format, such as a Word document or PDF.
- Submit the report to the appropriate authority, such as:
  - Incident response team
  - Security team
  - Management
- Ensure that the report includes all relevant information and is easy to understand.

**Additional Steps**

- Follow up with the authority to ensure that the report is received and reviewed.
- Implement any recommendations for remediation and mitigation outlined in the report.
- Continuously monitor the network for further threats and update the report accordingly.

**Example Report Format**

a. Introduction
   - Brief overview of the security threat

b. Threat Description
   - Description of the security threat, including:
     - Type of threat (e.g., malware, DDoS)
     - Target systems or data
     - Impact of the threat

c. Analysis of Network Device Hardening
   - Summary of network device hardening measures implemented
   - Identification of vulnerabilities or misconfigurations that contributed to the security threat

d. Analysis of Network Attack Prevention
   - Summary of network attack prevention measures implemented
   - Identification of gaps or weaknesses in these measures that allowed the security threat to occur

e. Recommendations for Remediation and Mitigation
   - Specific steps to remediate and mitigate the security threat, including:
     - Configuration changes
     - Firmware updates
     - Patching
     - Access controls

## Specification Sheet-4.1: Document and report the threat

**Necessary Personal Protective Equipment (PPE)**

| Sl. No | Name of PPE | Unit | Quantity |
|---|---|---|---|
| 1 | Antistatic Wrist Strap | Pair | 01 |
| 2 | Safety Glasses | Pair | 01 |
| 3 | Gloves | Pair | 01 |
| 4 | Dust Mask | Pair | 01 |
| 5 | Knee Pads | Pair | 01 |
| 6 | Proper Footwear | Pair | 01 |
| 7 | Work Apron | Pair | 01 |

**Necessary tools and equipment**

| Sl. No | Name of Tools & Equipment | Specification | Unit | Quantity |
|---|---|---|---|---|
| 1 | Firewall management software. | | | |
| 2 | Network diagrams. | | | |
| 3 | Security policy documentation. | | | |
| 4 | Backup storage for current configuration. | | | |
| 5 | Laptop/PC with network access. | | No. | |
| 6 | | | Set | |

## Review of Competency

Below is yourself assessment rating for module ----------

| Assessment of performance Criteria | Yes | No |
|---|---|---|
| Network security is defined | | |
| Types of network security is defined | | |
| Network security control is interpreted | | |
| Common network security Vulnerabilities are interpreted | | |
| Network attack architecture is interpreted | | |
| Search engine privacy is interpreted | | |
| Browser security and tracking prevention are interpreted | | |
| Network security best practices are interpreted | | |
| Security is ensured using a network administration tool | | |
| Filter rules are configured as per requirement | | |
| Mangle/Packet Filtering is configured as per the requirement | | |
| Security services are configured as per requirement | | |
| Access Control List (ACL) is configured as per requirement | | |
| A possible security threat is identified. | | |
| Possible cause of infection is determined | | |
| Identified security threat is monitored to find out its characteristics with network monitoring tools. | | |
| The capability of the security threat is determined from the analysis. | | |
| Network device hardening is interpreted | | |
| Network attack prevention is interpreted | | |
| Report is prepared using the monitoring system | | |
| The report is documented and submitted to the authority | | |

I now feel ready to undertake my formal competency assessment.

Signed:

Date:

# Development of CBLM

The Competency based Learning Material (CBLM) of '**Maintaining Network Security' (Occupation: IT Support Service, Level-4)** for National Skills Certificate is developed by NSDA with the assistance of SIMEC System Ltd., ECF Consultancy & SIMEC Institute of Technology JV (Joint Venture Firm) in the month of July, 2024 under the contract number of package SD-9B dated 15th January 2024.

| SL No. | Name & Address | Designation | Contact Number |
|---|---|---|---|
| 1 | Mir Rashedul Islam | Writer | 01920576687 |
| 2 | Md. Abdul Hye Siddiqui | Editor | 01819-725610 |
| 3 | Md. Zuwel Parves | Co-Ordinator | 01737-278906 |
| 4 | Md. Saif Uddin | Reviewer | 01723-004419 |