N|DE
Network Defense Essentials

C|ND
Certified Network Defender

Module 01

Network Security Fundamentals -Attacks and Defense Strategies

Module Objectives Network Security Attacks

1. Understanding essential terminologies related to network security attacks
2. Examples of network level attack techniques
3. Examples of application level attack techniques
4. Examples of wireless network specific attack techniques
5. Attacker methodologies and frameworks

Module Objectives
Network Defenses

1. Understanding the Goals of Network Defense
2. Understanding Information Assurance (IA) Principles
3. Understanding the Benefits and Challenges of Network Defense
4. Overview of Different Types of Network Defense Approaches
5. Understanding the Different Types of Network Security Controls

Module Flow

Understand Fundamentals of Network Security

02 **Discuss Essential Network Security Protocols**

Essential terminologies related to Network Security

- Understanding the tactics and techniques adopted by attackers is key to successful cyber defense

Essential Terminologies

Definitions

Asset

An asset is anything that can be of interest to an attacker. It can be a tangible or Intangible resource in an organization, often with a monetary value, which an attacker targets, to gain control of it, compromise its security, etc. Examples of tangible assets of an organization include databases, the server that hosts the databases, and the network that provides connections to the server. The intangible assets include the organization's secrets, critical business processes, and its reputation.

Figure 1. 1: Examples of Assets

Definitions

Threat

A threat is a potential occurrence of an undesirable event that can eventually damage and disrupt the operational and functional activities of an organization.

Examples of Threats:

- An attacker can steal sensitive data of organization.
- An attacker can cause server to shut down.
- An attacker can trick employee to reveal sensitive information.
- An attacker can infect system with malware.

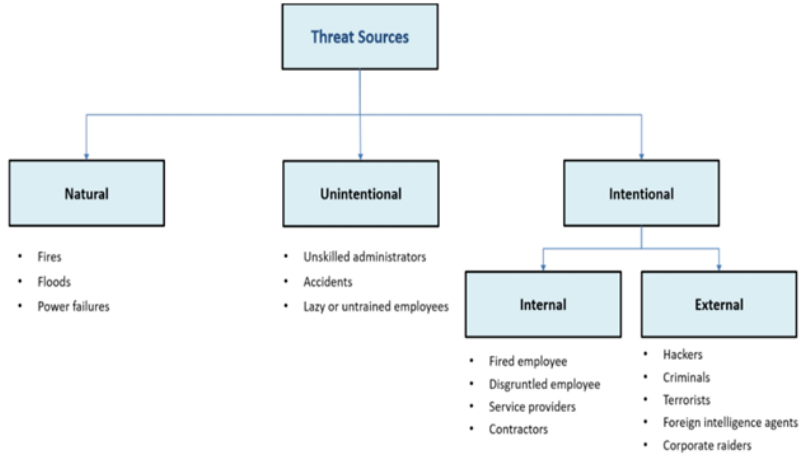


Figure 1.3: Threat Sources Classification

Types of Threat Actors

- **Hacktivists:** Individuals who use hacking as a means to promote a political or social agenda, rather than for monetary gains. They typically tend to deface or disable websites, and bring networks down via distributed denial of service (DDoS) attacks.
- **Cyber Terrorists/Criminals:** Individuals with a wide range of skills, like phishing and ransomware, motivated by religious beliefs, political beliefs, or monetary gains, to create threats of large-scale disruption of computer networks.
- **Suicide Hackers:** Individuals who aim to bring down the critical infrastructure for a "cause," and are not deterred by potential jail terms or other forms of punishment. They may sacrifice their lives for an attack.
- **State-Sponsored Hackers:** Individuals employed by the government to penetrate and obtain top-secret information, and to damage information systems of other governments. These hackers infiltrate large organizations to steal mission-critical

Types of Threat Actors

information.

- **Organized Hackers:** Professional hackers who attack a system for profits. They hack to obtain sensitive information such as social credit card information, security numbers, and monetary information.
- **Script Kiddies:** Unskilled individuals who compromise a system by running scripts, tools, and software developed by professional hackers. They attempt to emulate the attacks of skilled hackers.
- **Industrial Spies:** Individuals who attempt to attack companies for commercial purposes. These attackers are hired by business competitors or agencies to steal an organization's strategy, money records, and other sensitive data.
- **Insider Threat Actors:** Individuals such as disgruntled employees and terminated employees, who intentionally provide an organization's data to others for money or revenge. Undertrained staff may also unintentionally provide critical information when subject to social engineering attacks.

Vulnerability

Vulnerability refers to the existence of a weakness in the design or implementation of a system cthat can be exploited to compromise the security of the system. Frequently, it is a security loophole that enables an attacker to enter the system by bypassing user authentications.

Causes of Vulnerabilities:

- Hardware or Software Misconfiguration
- Insecure or poor design of network
- Inherent technology weaknesses
- End-user carelessness
- Intentional end-user acts

Vulnerabilities	Description
TCP/IP protocol vulnerabilities	HTTP, FTP, ICMP, SNMP, SMTP are inherently insecure
Operating System vulnerabilities	An OS can be vulnerable because: It is inherently insecure It is not patched with the latest updates
Network Device Vulnerabilities	Various network devices such as routers, firewall, and switches can be vulnerable due to: Lack of password protection Lack of authentication Insecure routing protocols Firewall vulnerabilities

Table 1.1: Technological Vulnerabilities

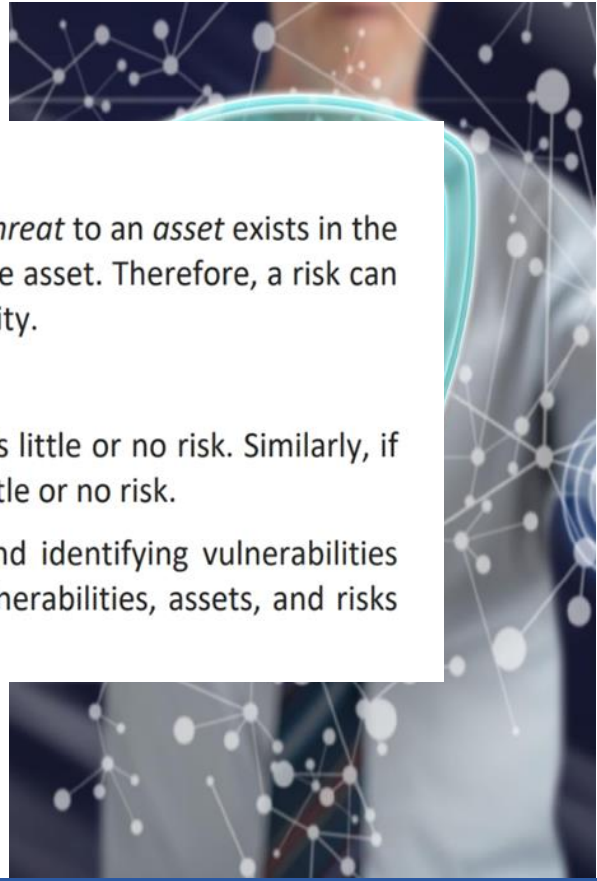
Vulnerabilities	Description
User account vulnerabilities	Originating from the insecure transmission of user account details such as usernames and passwords, over the network
System account vulnerabilities	Originating from setting of weak passwords for system accounts
Internet service misconfiguration	Misconfiguring internet services can pose serious security risks. For example, enabling JavaScript and misconfiguring IIS, Apache, FTP, and Terminal services, can create security vulnerabilities in the network
Default password and settings	Leaving the network devices/products with their default passwords and settings
Network device misconfiguration	Misconfiguring the network device

Table 1.2: Configuration Vulnerabilities

Vulnerabilities	Description
Unwritten Policy	Unwritten security policies are difficult to implement and enforce
Lack of Continuity	Lack of continuity in implementing and enforcing the security policy
Politics	Politics may cause challenges for implementation of a consistent security policy
Lack of awareness	Lack of awareness of the security policy

Table 1.3: Security Policy Vulnerabilities

Definitions



Risk

Risk refers to the potential loss or damage that can occur when a *threat* to an *asset* exists in the presence of a *vulnerability* that can be exploited to compromise the asset. Therefore, a risk can be thought of as the intersection of an asset, threat, and vulnerability.

Risk = Asset + Threat + Vulnerability

If threats exist, but vulnerabilities do not exist in a system, there is little or no risk. Similarly, if vulnerabilities exist in a system, but threats do not exist, there is little or no risk.

Understanding the level of risk to assets by assessing threats and identifying vulnerabilities accurately is fairly challenging. Clearly distinguishing between vulnerabilities, assets, and risks can facilitate the assessment of the extent of risk to assets.

Examples of Risks:

- Disruption of Business
- Loss of Productivity
- Loss of Privacy
- Theft of Information
- Legal Liability
- Damage to reputation and consumer confidence

Definitions

Attack

An attack is an action that is performed with the intent to breach an IT system's security by exploiting its vulnerabilities. An attack involves an attempt to obtain, edit, remove, destroy, implant, or reveal information without authorized access. It also refers to malicious software or commands that exploit vulnerabilities to cause unanticipated behavior in legitimate software or hardware. Therefore, an attack can be conceptualized as combination of a *motive*, with a *method* to perform the attack, which exploits one or more *vulnerabilities* in the system.

Attacks = Motive (Goal) + Method + Vulnerability

Examples of Motives:

- Disruption of Business Continuity
- Manipulating data
- Damaging reputation of the target
- Theft of Information

- Method (TTPs)
- Tactics
- Techniques
- Procedures

Examples of Network-level Attack Techniques

An attacker uses various network attack strategies to compromise network security. This section discusses some of the network attack techniques that an attacker follows to accomplish their objective. Specifically, this section depicts the workings of various network-level attacks, including reconnaissance attack, network sniffing, man-in-the-middle attack, password attack, privilege escalation, DNS poisoning, ARP poisoning, DHCP starvation attack, DHCP spoofing attack, MAC spoofing, denial-of-service (DoS), distributed denial-of-service (DDoS) attack, and malware attack.

Network Sniffing Attack

Sniffing involves capturing, decoding, inspecting, and interpreting the information inside a packet on a TCP/IP network. The purpose of sniffing is to steal information such as user IDs, passwords, network details, and credit card numbers. Sniffing is generally referred to as a "passive" type of attack, where the attacker can be silent/invisible on the network. This makes it difficult to detect and a dangerous type of attack. The TCP/IP packet contains vital information required for two network interfaces to communicate with each other. It contains fields such as source and destination IP addresses ports, sequence numbers, and the protocol type.

Figure 1.4: Network Sniffing Attack

Man-in-the-Middle Attack

A man-in-the-middle (MiTM) attack is a form of a session hijacking attack, in which attackers intrude into an existing connection between two systems to intercept the messages being exchanged, and inject fraudulent information. It is an eavesdropping attack in which the communication between two parties is monitored or modified by a third unauthorized party. Specifically, it involves eavesdropping on a connection, intruding into the connection, intercepting messages, and modifying the data.

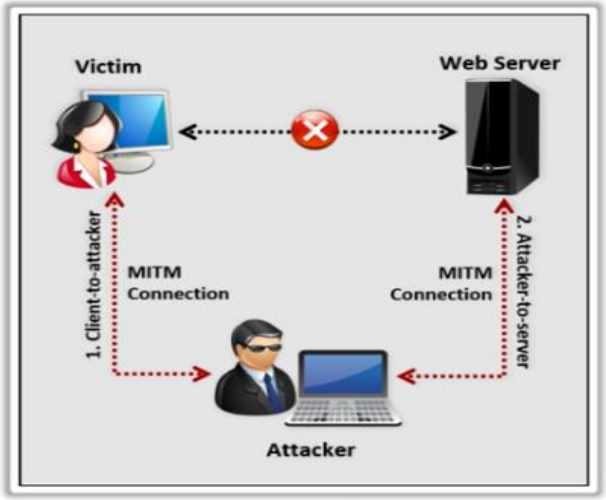


Figure 1.5: MiTM Attack

Distributed Denial-of-Service Attack (DDoS)

A distributed denial-of-service (DDoS) attack is a large-scale, coordinated attack on the availability of services on a target's system or network resources. It is launched indirectly through many compromised computers on the Internet.

The services under attack are those of the "primary target," while the compromised systems used to launch the attack are often called the "secondary target." The use of secondary targets in performing a DDoS attack enables the attacker to wage a larger scale and a more disruptive attack, while making it more difficult to track.

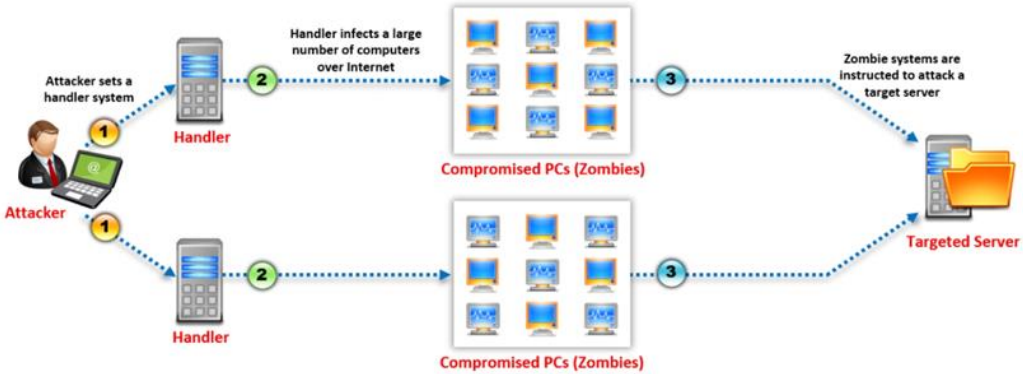


Figure 1.12: DDoS Attack

Application-level DoS Attack

Attackers exhaust available server resources by sending hundreds of resource-intensive requests such as retrieving large image files or requesting dynamic pages that require expensive search operations on the backend of database servers. Application-level DoS attacks emulate the same request syntax and network-level traffic characteristics as that of the legitimate clients, which makes it undetectable by existing DoS protection measures.

This type of attack targets CPU, memory, sockets, disk bandwidth, batabase bandwidth, worker processes, etc. Web applications can be vulnerable to DoS attacks due to various factors, such as application environment bottlenecks, implementation flaws, and poor data validation.

The following are some examples of application-level DoS.

- **User Registration DoS**

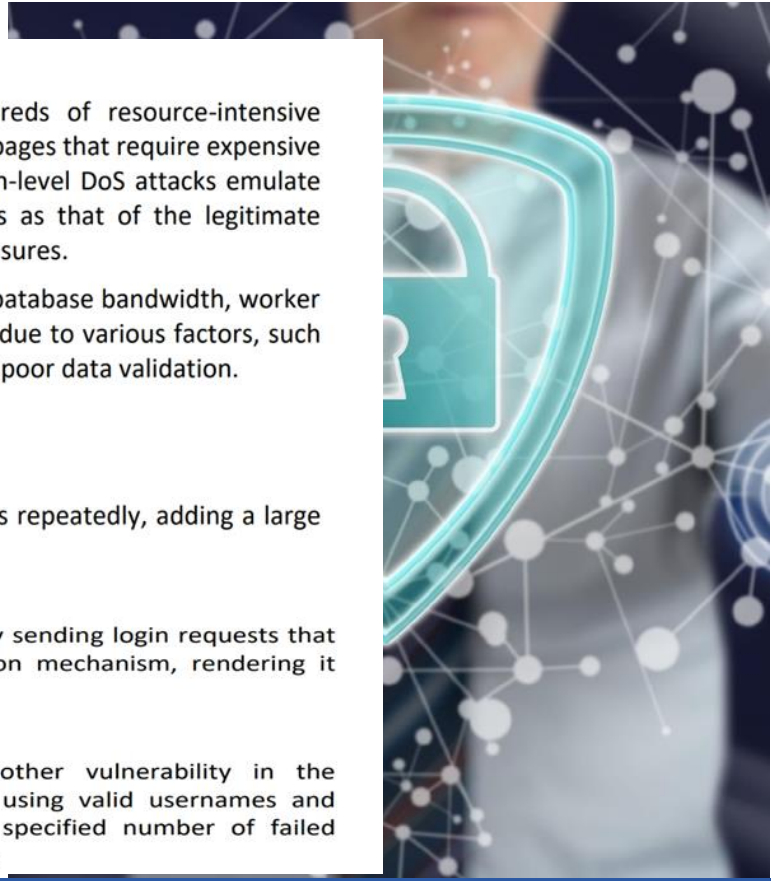
  The attacker creates a program to submit registration forms repeatedly, adding a large number of spurious users to the application.

- **Login Attacks**

  The attacker may overload the login process by continually sending login requests that require the presentation tier to access the authentication mechanism, rendering it unavailable or unreasonably slow to respond.

- **Account Lock Out Attacks**

  The attacker may enumerate usernames through another vulnerability in the application, and then attempt to authenticate the site using valid usernames and incorrect passwords, which locks the accounts after a specified number of failed attempts. At this point, legitimate users cannot use the site.



Session Hijacking Attack

Session hijacking refers to an attack where an attacker seizes a valid TCP communication session between two computers. Though any session in a system can be hijacked, session hijacking occurs primarily with browser sessions and web applications. The source of the attack is the session cookie, and therefore it is also called cookie hijacking or cookie side-jacking. Specifically, the attacker breaks into a system by stealing the session ID. The server then assumes it to be a legitimate session, enabling the attacker to extract system data and sniff the traffic from the established TCP sessions to conduct malicious activities such as identity theft, information theft, and fraud.

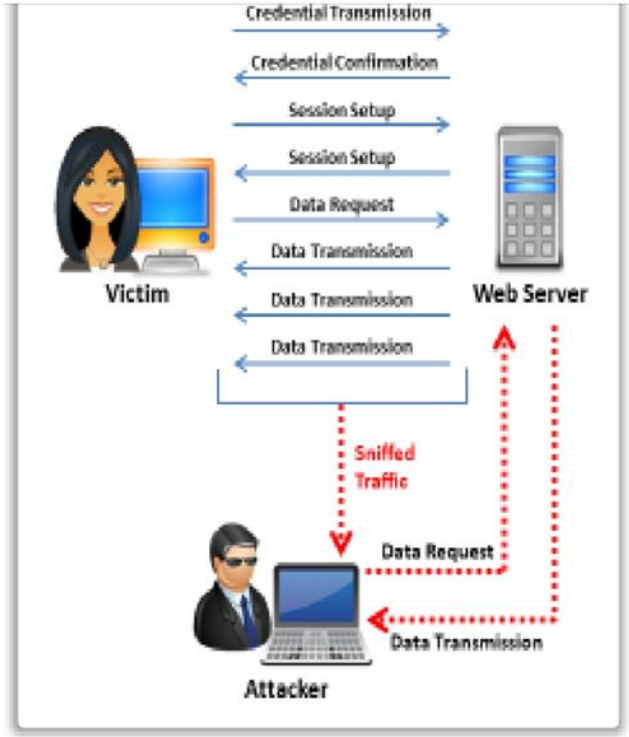


Figure 1.27: Session Hijacking Attack

Service Hijacking using Network Sniffing

Network sniffing involves interception and monitoring of network traffic transmitted between two cloud nodes. Unencrypted sensitive data (such as login credentials) during transmission across a network are at a higher risk of being sniffed.

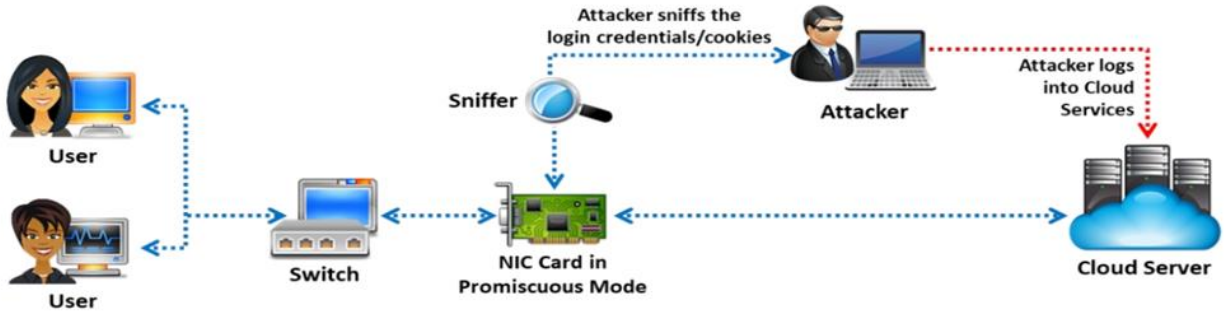


Figure 1.37 : Example of Service Hijacking using Network Sniffing

The above diagram illustrates an example of service hijacking using network sniffing. As shown in the diagram, when the user enters login credentials to access cloud services, the attacker sniffs these login credentials and cookies during their transmission across a network using packet sniffers such as Wireshark and Capsa Portable Network Analyzer. The attacker then logs into cloud services via the stolen credentials.

Examples of Wireless Network Specific Attack Techniques

Wardriving

In a wardriving attack, wireless LANs are detected either by sending probe requests over a connection or by listening to web beacons. An attacker who discovers a penetration point can launch further attacks on the LAN. Some of the tools that the attacker may use to conduct wardriving attacks are KisMAC, NetStumbler, and WaveStumber.

Honeypot Access Point Attack

In this attack, attackers spoof the SSID of a legitimate AP to deploy a fake "honeypot" AP that impersonates the legitimate AP. The fake AP is placed in the proximity of the legitimate AP with high power (gain) antennas. Once the user's device is connected to the fake AP, attackers can gather sensitive information about both the client and the network and can use this information to launch further attacks, like MiTM attacks and wireless denial of service (DOS) attacks.

Rogue Access Point Attack

In order to create a backdoor into a trusted network, an attacker may install an insecure AP or a fake AP inside a firewall. The attacker may use either a software or hardware AP to perform this attack. A wireless access point is termed as a rogue access point when it is installed on a trusted network without authorization. This can be performed by either an insider or outsider attacker for malicious intentions.

Attacker Hacking Methodologies and Frameworks

- CEH – Hacking Methodology
- Lockheed Martin's Cyber Kill Chain Methodology
- MITRE Attack Framework

Figure 1.43: MITRE Attack Framework

Figure 1.42: Cyber Kill Chain Methodology

Importance of Network Security

- A completely secure and robust network can be designed with proper **implementation** and **configuration** of network security elements

Elements of Network Security

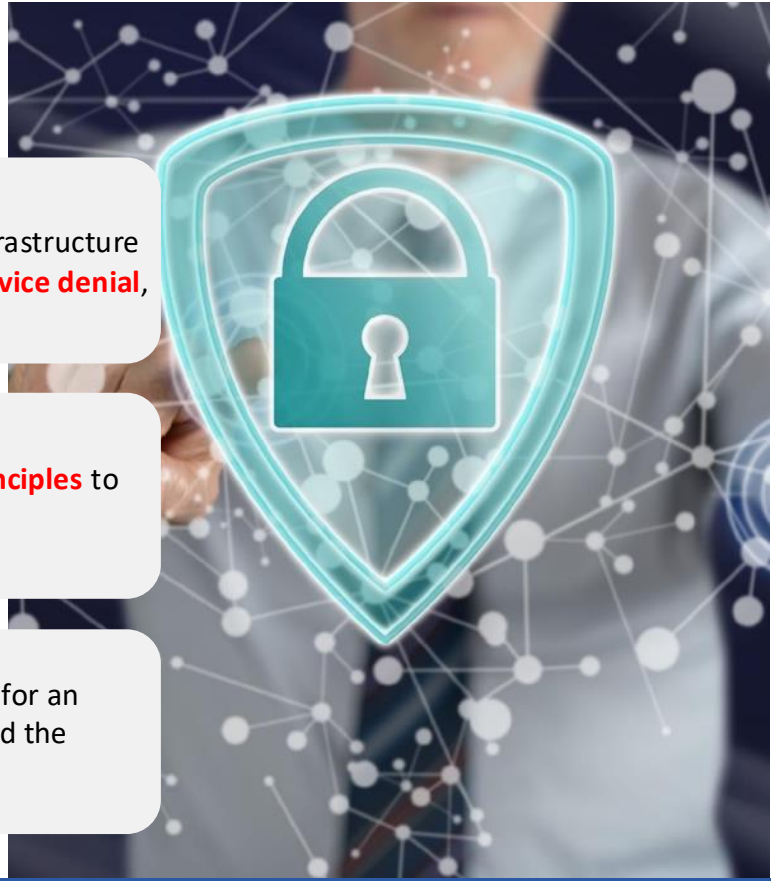
- Network Security Controls
- Network Security Protocols
- Network Security Devices

Goal of Network Defense

The ultimate goal of network defense is to protect an organization's information, systems, and network infrastructure from **unauthorized access**, **misuse**, **modification**, **service denial**, or any **degradation** and **disruptions**

Organizations rely on **information assurance (IA) principles** to attain defense-in-depth security

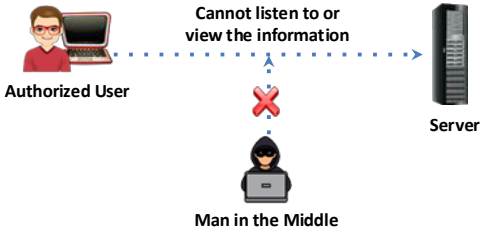
Information Assurance (IA) principles act as **enablers** for an organization's security activities to protect and defend the organizational network from security attacks



Information Assurance (IA) Principles

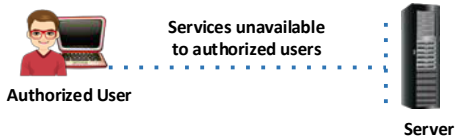
Confidentiality

- Ensures information is not **disclosed** to unauthorized parties



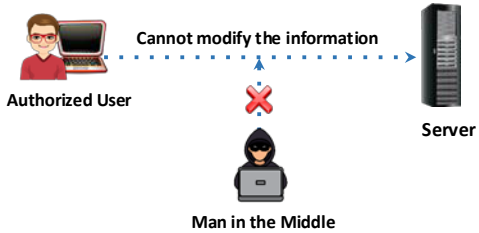
Availability

- Ensures information is **available** to authorized parties without any disruption



Integrity

- Ensures information is not **modified** or **tampered** with by unauthorized parties



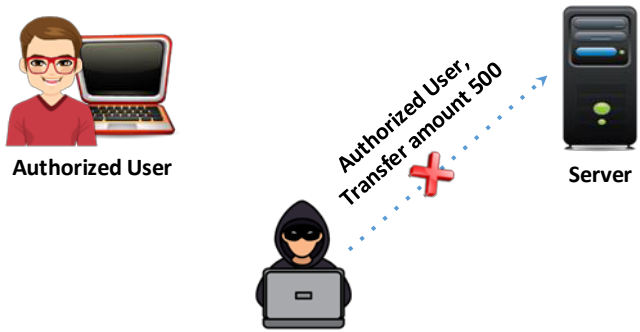
Information Assurance (IA) Principles (Cont'd)

Non-repudiation

- Ensures that a party in a communication cannot deny **sending** the message

Authentication

- Ensures the **identity** of an individual is verified by the system or service



Network Defense Benefits

- **Protect** information assets
- **Comply** with government and industry specific regulations
- **Ensure** secure communication with clients and suppliers
- **Reduce** the risk of being attacked
- **Gain** competitive edge over competitor by providing more secure services

Network Defense Challenges

Distributed Computing Environments

- With the advancement in **modern technology** and to meet business requirements, networks are becoming **vast** and **complex**, potentially leading to serious **security vulnerabilities**. Attackers exploit exposed security vulnerabilities to compromise network security

Emerging Threats

- Potential threats to the network evolve each day. Network security attacks are becoming technically more **sophisticated** and **better organized**

Lack of Network Security Skills

- Organizations are failing to defend themselves against rapidly increasing network attacks due to the **lack of network security skills**

Types of Network Defense Approaches

Preventive Approaches

Consist of methods or techniques that are used to avoid threats or attacks on the target network

Retrospective Approaches

Consist of methods or techniques that examine the causes for attacks, and contain, remediate, eradicate, and recover from damage caused by the attack on the target network

Reactive Approaches

Consist of methods or techniques that are used to detect attacks on the target network

Proactive Approaches

Consist of methods or techniques that are used to make informed decisions on potential attacks in the future on the target network

Network Security Controls: Administrative Security Controls

- The management implements administrative access controls to **ensure** the **safety** of the organization

Examples of Administrative Security Controls

01 | Regulatory framework Compliance

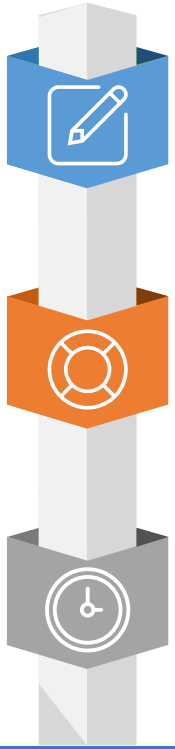
02 | Security policy

03 | Employee Monitoring and Supervising

04 | Information Classification

05 | Security Awareness and Training

Regulatory Frameworks Compliance



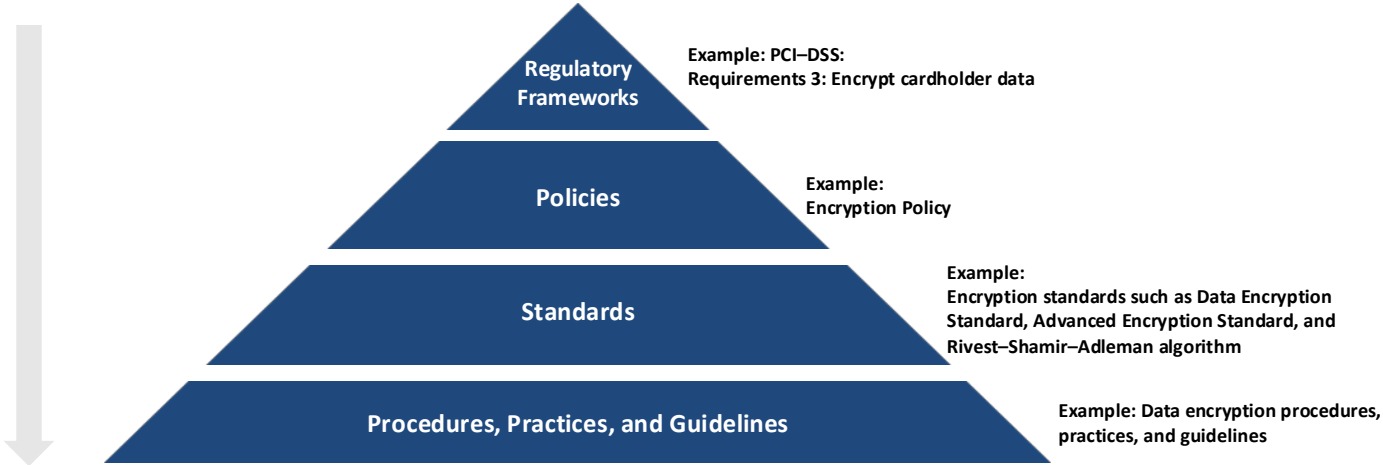
It is often required for the organizations to comply with some type of **security regulation**

Complying with regulatory frameworks is a **collaborative effort** between governments and private bodies to encourage voluntary/mandatory **improvements** to cybersecurity

IT security regulatory frameworks contain a set of **guidelines** and **best practices**

Regulatory Frameworks Compliance (Cont'd)

Role of Regulatory Frameworks Compliance in an Organization's Administrative Security



Identifying Which Regulatory Framework to Comply

- An organization needs to **assess** itself to determine which regulatory framework applies to it best
- For example, following table shows different regulations and which organization would be subject to the **scope** of the regulatory framework

Regulatory Framework	Organizations within Scope
Health Insurance Portability and Accountability Act (HIPAA)	Any company or office that deals with healthcare data, including, but not limited to, doctor's offices, insurance companies, business associates, and employers
Sarbanes Oxley Act	U.S. public company boards, management, and public accounting firms
Federal Information Security Management Act of 2002 (FISMA)	All federal agencies must develop a method of protecting information systems
Gramm Leach Bliley Act (GLBA)	Companies that offer financial products or services to individuals such as loans, financial or investment advice, or insurance
Payment Card Industry Data Security Standard (PCI-DSS)	Companies handling credit card information

ISO Information Security Standards

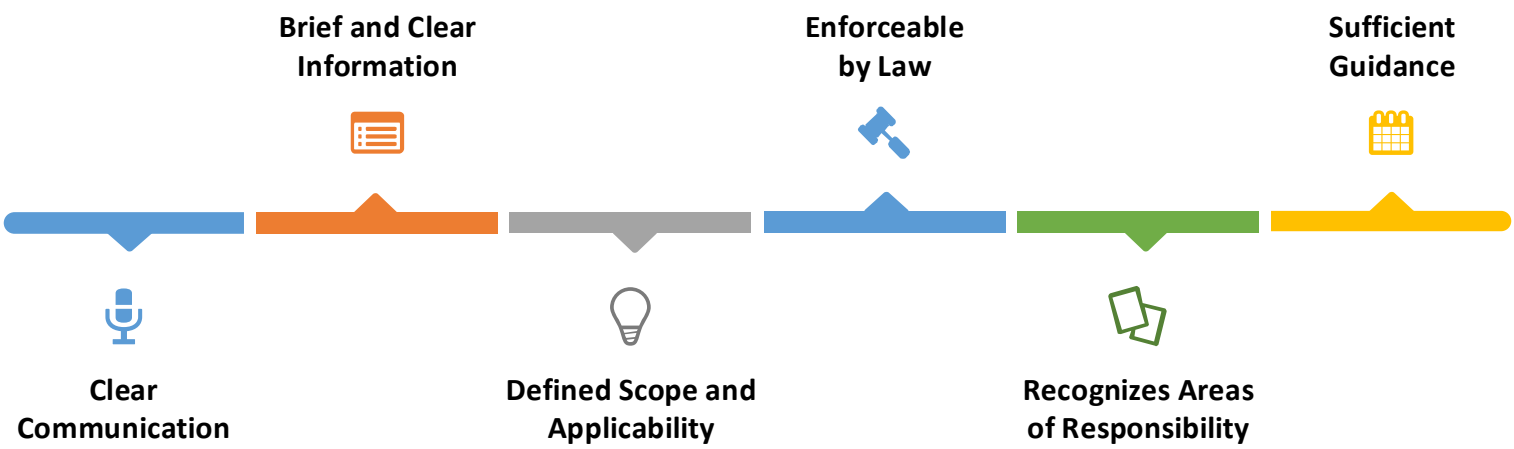
Sr. No.	Standards	Objective
1	ISO/IEC 27001	Formal ISMS specification
2	ISO/IEC 27002	Information security controls
3	ISO/IEC 27003	ISMS implementation guide
4	ISO/IEC 27004	Information security metrics
5	ISO/IEC 27005	Information security risk management
6	ISO/IEC 27006	ISMS certification guide
7	ISO/IEC 27007	Management system auditing
8	ISO/IEC TR 27008	Technical auditing
9	ISO/IEC 27010	For inter-organization communication
10	ISO/IEC 27011	Iso27k in telecoms
11	ISO/IEC 27013	ISMS & ITIL/service management
12	ISO/IEC 27014	Information security governance
13	ISO/IEC TR27015	Iso27k in financial services
14	ISO/IEC TR 27016	Information security economics
15	ISO/IEC 27017	Cloud security controls

Sr. No.	Standards	Objective
16	ISO/IEC 27018	Cloud privacy
17	ISO/IEC TR 27019	Process control in energy
18	ISO/IEC 27031	ICT business continuity
19	ISO/IEC 27032	Cybersecurity
20	ISO/IEC 27033-1 to -5	Network security
21	ISO/IEC 27034 -1 & -5	Application security
22	ISO/IEC 27035	Incident management
23	ISO/IEC 27036-1 -2 & -3	ICT supply chain
24	ISO/IEC 27037	Digital evidence [forensics]
25	ISO/IEC 27038	Document reduction
26	ISO/IEC 27039	Intrusion prevention
27	ISO/IEC 27040	Storage security
28	ISO/IEC 27041	Investigation assurance
29	ISO/IEC 27042	Analyzing digital evidence
30	ISO/IEC 27043	Incident investigation
31	ISO 27799 ISO27k	In healthcare

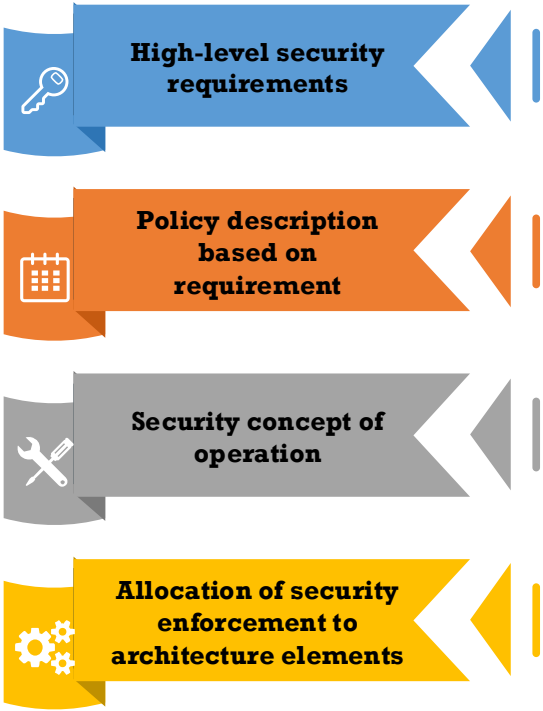
What is Security Policy?

- A security policy is a **well-documented** set of plans, processes, procedures, standards, and guidelines required to establish an ideal information security status of an organization
- Security policies are used to inform people on how to work in a safe and secure manner; they define and guide employee actions on how to deal with organization sensitive operation, data, or resources
- The security policy is an **integral** part of an information security management program for any organization

Key Elements of Security Policy



Contents of a Security Policy



- This features the **requirements** of a system when implementing security policies that include discipline security, safeguard security, procedural security, and assurance security
- Focuses on the security disciplines, **safeguards**, procedures, continuity of operations, and documentation
- Defines the **roles**, **responsibilities**, and **functions** of a security policy
- Provides a computer system **architecture allocation** to each system in the program

Types of Information Security Policies

Enterprise Information Security Policy (EISP)

- EISP drives an organization's scope and provides direction to their security policies

Examples of EISP:

- ✓ Application policy
- ✓ Network and network device security policy
- ✓ Back up and restore policy
- ✓ System security policy

Issue Specific Security Policy (ISSP)

- ISSP directs the audience on the usage of technology-based systems with the help of **guidelines**

Examples of ISSP:

- ✓ Remote access and wireless policies
- ✓ Incident response plan
- ✓ Password policies
- ✓ Policies for personal devices

System Specific Security Policy (SSSP)

- SSSP directs users while **configuring or maintaining** a system

Examples of SSSP:

- ✓ DMZ policy
- ✓ Encryption policy
- ✓ Policies for Intrusion detection and prevention
- ✓ Access control policy

Internet Access Policies

Promiscuous Policy

- ❑ **No restrictions** on Internet/remote access
- ❑ Nothing is blocked

Permissive Policy

- ❑ Known **dangerous services/ attacks** blocked
- ❑ Policy begins with no restrictions
- ❑ Known holes plugged; known dangers stopped

Paranoid Policy

- ❑ **Everything** is **forbidden**
- ❑ **No Internet connection**, or severely limited Internet usage
- ❑ Users find ways around overly severe restrictions

Prudent Policy

- ❑ Provides **maximum security** while allowing known, but necessary, dangers
- ❑ All services are blocked
- ❑ **Safe/necessary** services are enabled individually

Password Policy

Password policy provides guidelines for using strong passwords for an organization's resources

Design Considerations

01 Password length and formation

02 Complexity of password

03 Password blacklists

04 Password duration

05 Common password practice

Network Security Controls: Physical Security Controls

- This is a set of security measures taken to **prevent unauthorized access** to physical devices

Examples of Physical Access Controls

Locks

Fences

Badge system

Security guards

Mantrap doors

Biometric system

Lighting

Motion detectors

Closed-circuit TVs

Alarms

Employee Awareness and Training

- An organization need to provide **formal security awareness training** for its employees when they join and periodically thereafter, so employees
  - Know **how to defend** themselves and the organization against threats
  - **Follow security policies** and procedures for working with IT
  - Know **whom to contact** if they discover a security threat
  - Can identify the **nature of the data** based on data classification
  - Protect physical and **informational assets** of that organization

Different methods to train employees are:

Employee Awareness and Training: Security Policy

Security policy training teaches employees how to perform their duties and to comply with the security policy

Organizations should train new employees before granting them access to the network or provide limited access until the completion of their training

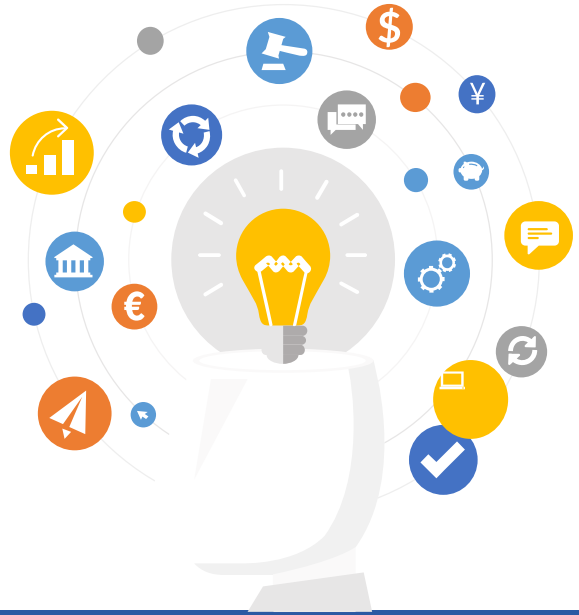
Advantages

- Effective implementation of a security policy
- Policies are followed and not just enforced
- Creates awareness on compliance issues
- Helps an organization enhance its network security

Employee Awareness and Training: Physical Security

Proper training should be given to **educate employees** on physical security

Training increases the knowledge and awareness about physical security

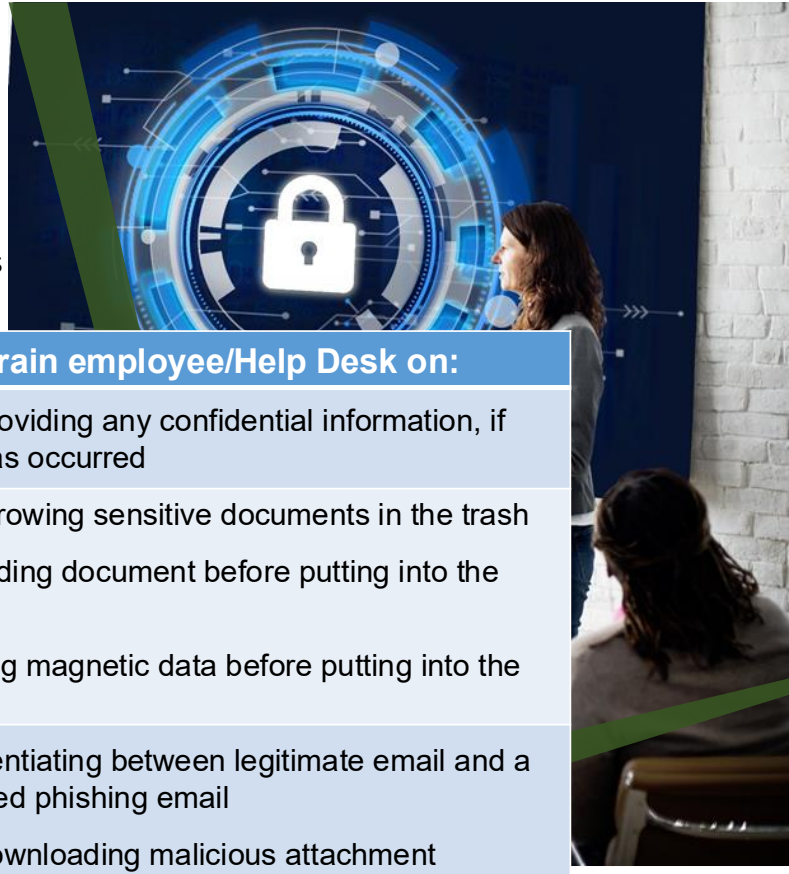


Training should educate employees about how to:

- Minimize breaches
- Identify the elements that are more prone to hardware theft
- Assess the risks handling sensitive data
- Ensure physical security at the workplace

Employee Awareness and Training: Social Engineering

Train employee on possible social engineering techniques and how to **combat** these techniques

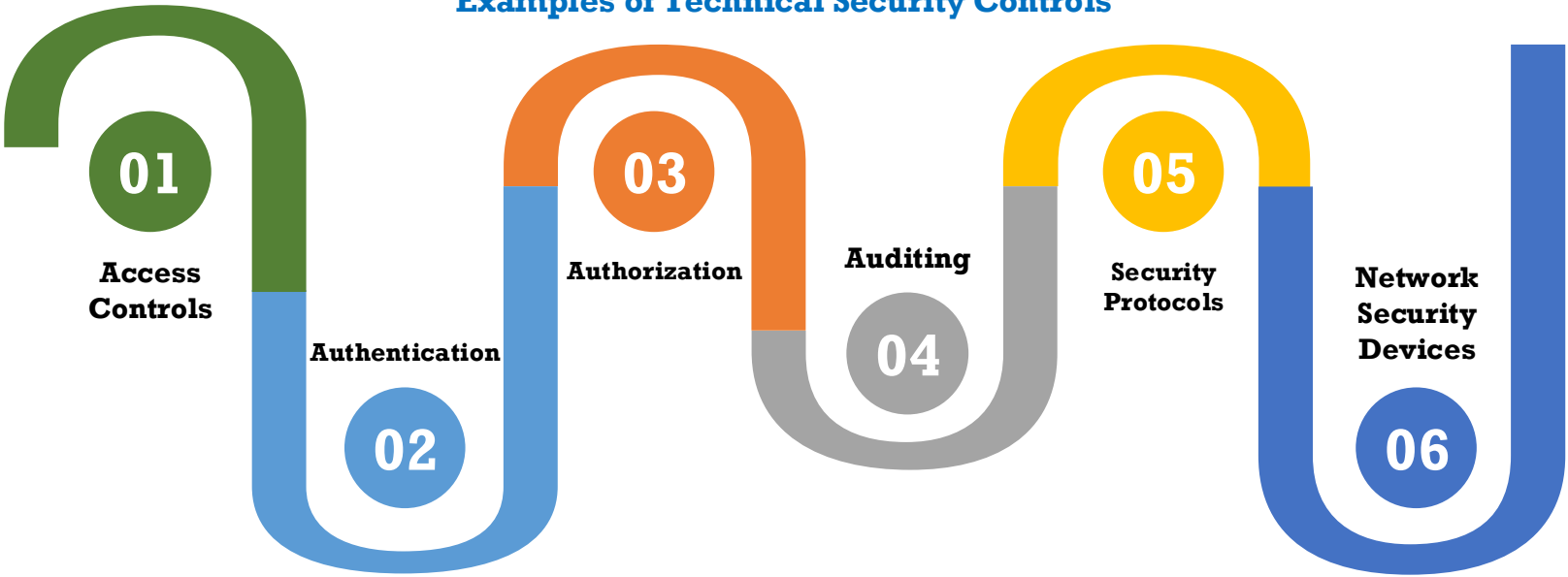


Areas of Risk	Attack Techniques	Train employee/Help Desk on:
Phone	Impersonation	• Not providing any confidential information, if this has occurred
Dumpsters	Dumpster Diving	• Not throwing sensitive documents in the trash • Shredding document before putting into the trash • Erasing magnetic data before putting into the trash
Email	Phishing, malicious attachment	• Differentiating between legitimate email and a targeted phishing email • Not downloading malicious attachment

Network Security Controls: Technical Security Controls

- This is a set of security measures taken to protect data and systems from unauthorized personnel

Examples of Technical Security Controls



Module Flow

Understand Fundamentals of Network Security

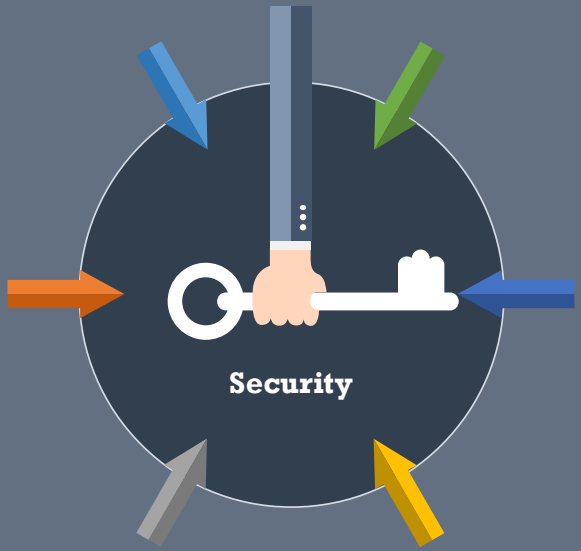
02 Discuss Essential Network Security Protocols

Network Security Protocols

- RADIUS
- TACACS +
- Kerberos
- PGP
- S/MIME

- Secure HTTP
- HTTPS
- TLS
- SSL
- IPsec

Module Summary



This module has discussed the essentials of network security, goal of network defense, and the information assurance (IA) principles

It has discussed benefits and challenges of network defense

It also discussed different types of network defense approaches and types of network security controls

Finally, this module ended with a discussion of various network security protocols

In the next module, we will discuss in detail on identification, authentication, and authorization concepts