Chapter 2
Basic Security Concepts

Er. Shiva Ram Dam

Assistant Professor

Gandaki University

Content:

2.1 Basic Security Concepts

- ❑ Basics of Information Security, Network Security, Firewall, PAM, ACLs
- ❑ Computer and Network threats (including but not limited to Malware, Trojans, Adware, D/DoS, Ransomware, Honeypot, Social Engineering)
- ❑ Security, Privacy and Trust

2.2 Introduction to Penetration Testing

- ❑ Basic Concepts of Information Gathering, Vulnerability Analysis, Forensics Tools, Sniffing, Spoofing, Password Attacks and Reverse Engineering

2.3 Threat, Vulnerability and Risk

2.4 Data Confidentiality (Privacy, Confidentiality, and Secrecy)

2.1 Basic Security Concepts

- ❑ **Basics of Information Security, Network Security, Firewall, PAM, ACLs**
- ❑ **Computer and Network threats (including but not limited to Malware, Trojans, Adware, D/DoS, Ransomware, Honeypot, Social Engineering)**
- ❑ **Security, Privacy and Trust**

2.1 Basics of Information Security

- Information security is the **practice of protecting information by mitigating information risks.**
- **Information Security (InfoSec)** refers to the **processes, policies, and tools** designed **to protect information from unauthorized access,** use, disclosure, disruption, modification, or destruction.
- This includes the protection of personal information, financial information, and sensitive or confidential information stored in both digital and physical forms.
- Effective information security requires a comprehensive and multi-disciplinary approach, involving people, processes, and technology.
- Information Security programs are **build around** 3 objectives, commonly known as CIA – **Confidentiality, Integrity, Availability**.

Three Principles of Information Security

1. **Confidentiality**
   - Ensures that sensitive information is accessible only to those authorized to have access.
   - Techniques: Encryption, access controls, authentication.
2. **Integrity**
   - Ensures that information is accurate and has not been tampered with.
   - Techniques: Checksums, hashing, digital signatures.
3. **Availability**
   - Ensures that authorized users have access to information and systems when needed.
   - Techniques: Redundancy, fault tolerance, DDoS protection.

Key Components of Information Security

1. **Authentication**
    - Verifying the identity of users before allowing access (e.g., passwords, biometrics).
2. **Authorization**
    - Granting permission to users based on their roles or credentials.
3. **Non-repudiation**
    - Ensures that a sender cannot deny sending a message (e.g., digital signatures).
4. **Accountability**
    - Keeping logs and audit trails to track user activity and ensure responsibility.

Assignment:

- Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access.

  Give examples of confidentiality, integrity, and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.

Use of Information security

- **Confidentiality:** Keeping sensitive information confidential and protected from unauthorized access.
- **Integrity:** Maintaining the accuracy and consistency of data, even in the presence of malicious attacks.
- **Availability:** Ensuring that authorized users have access to the information they need, when they need it.
- **Compliance:** Meeting regulatory and legal requirements, such as those related to data privacy and protection.
- **Risk management:** Identifying and mitigating potential security threats to prevent harm to the organization.
- **Disaster recovery:** Developing and implementing a plan to quickly recover from data loss or system failures.
- **Authentication:** Verifying the identity of users accessing information systems.
- **Encryption:** Protecting sensitive information from unauthorized access by encoding it into a secure format.
- **Network security:** Protecting computer networks from unauthorized access, theft, and other types of attacks.
- **Physical security:** Protecting information systems and the information they store from theft, damage, or destruction by securing the physical facilities that house these systems.

Example of security violations

- User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure.
- User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.

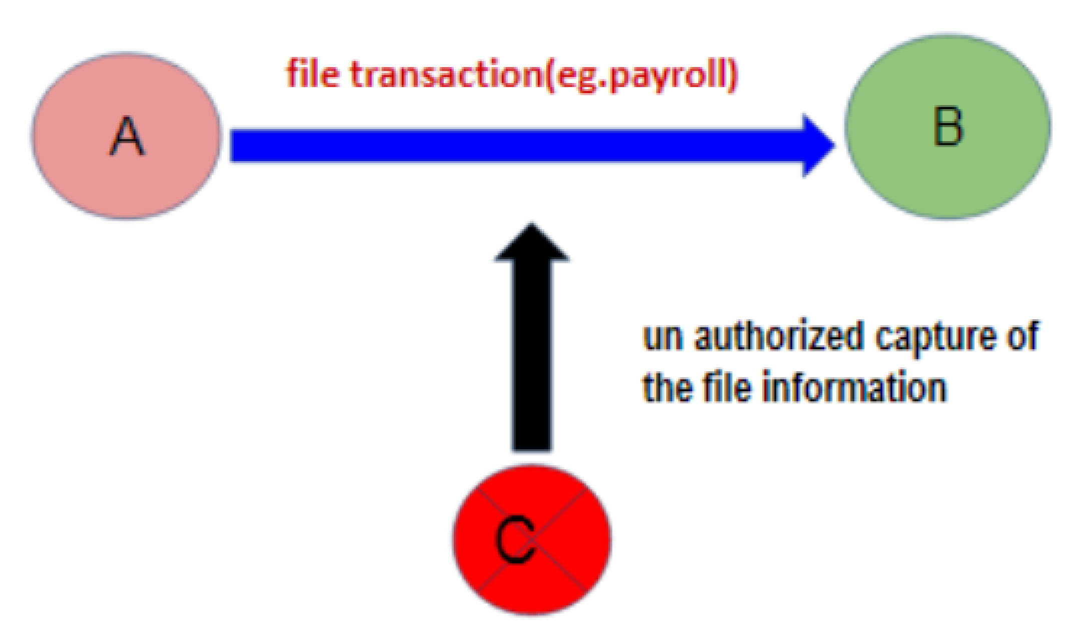

file transaction(eg.payroll)
A
B
un authorized capture of the file information
C

Fig 1.1 Example 1

- A network manager, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User **F intercepts the message, alters its contents to add or delete entries, and then forwards the message to** E, which accepts the message as coming from manager D and updates its authorization file accordingly.

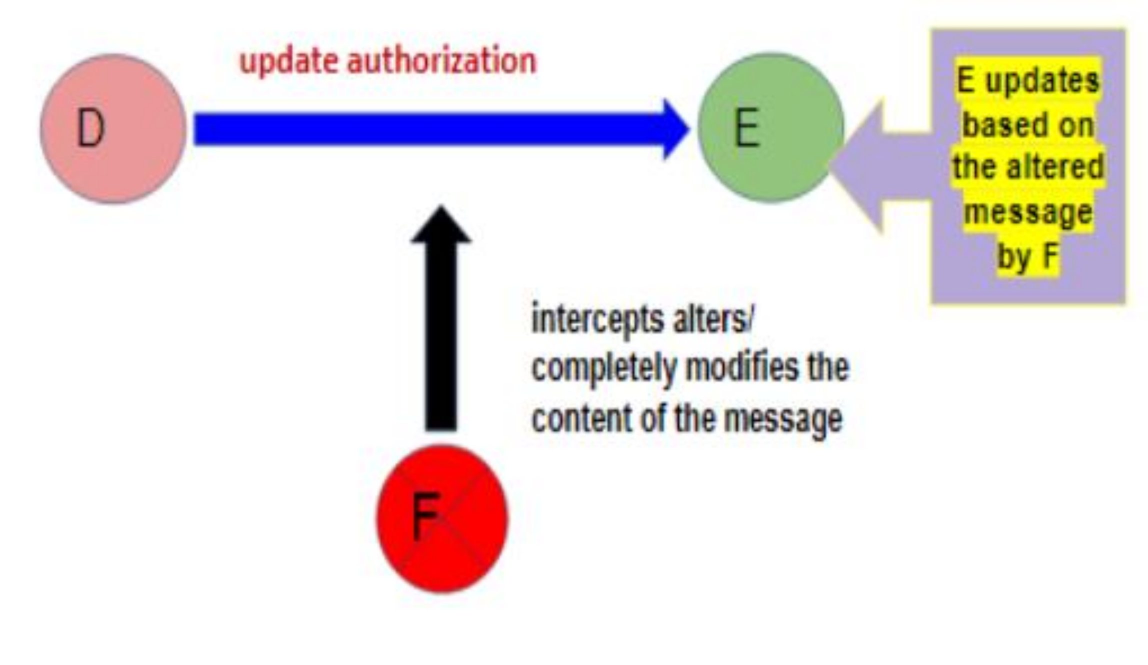

update authorization
D
E
E updates based on the altered message by F
intercepts alters/ completely modifies the content of the message
F

Fig 1.2 Example 2

- Rather than intercept a message, **user F constructs its own message with the desired entries and transmits that message to E** as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.

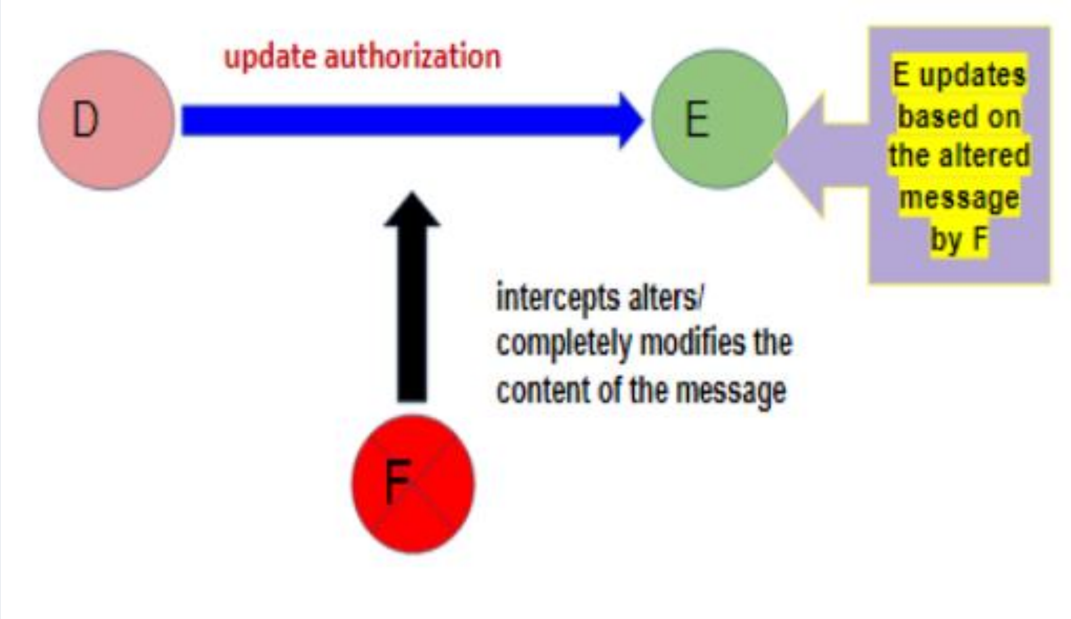

update authorization
D
E
E updates based on the altered message by F
intercepts alters/ completely modifies the content of the message
F

Fig 1.2 Example 2

Network Security

- Network security **protects networking infrastructure from data theft, unauthorized access, and manipulation**.
- Network Security **refers to the practices, policies, and technologies used to protect the integrity, confidentiality, and availability of data and resources** as they are transmitted and accessed across or within computer networks.
- It also includes network segmentation for security, which involves dividing your network into regions by using firewalls as borders.
- Network security technologies work within several layers to protect your network as a whole against any potential threats.
- Networking and security include three main areas: physical, technical, and administrative.

1. Physical Network Security

- Measures designed to prevent unauthorized physical access to network infrastructure.
- Physical network security controls are put in place **to stop unauthorized personnel from accessing components of the network.**
- **Purpose:** To prevent physical damage, theft, or tampering with network equipment such as switches, routers, servers, and cables.
- Example:
  - **Secured server rooms** with locks, biometrics, or access cards.
  - **Surveillance systems** (CCTV cameras).
  - **Fire suppression systems** to prevent equipment damage.
  - **Uninterruptible Power Supplies (UPS)** and generators to maintain uptime.
  - **Cable locks or secure racks** for routers, switches, and servers.

2. Technical Network Security

- Involves Software and hardware-based protections that secure data and systems within the network.
- Purpose: To protect data integrity, confidentiality, and availability during storage, processing, and transmission.
- Examples:
    - **Firewalls** (hardware/software)
    - **Intrusion Detection/Prevention Systems (IDS/IPS)**
    - **Encryption protocols** (e.g., SSL/TLS, IPSec)
    - **Antivirus and antimalware programs**
    - **Access controls** (passwords, biometrics, two-factor authentication)
    - **VPNs** for secure remote access
    - **Network segmentation** and VLANs

3. Administrative Network Security

- Administrative network security controls the level of access for each user within the network.
- Processes and policies are set to limit or allow access and control each user’s behavior on the network.
- This security will also control the amount and level of changes the IT staff can make to the infrastructure of the network.
- Policies, procedures, and standards that dictate how the network and information systems should be secured and managed.
- **Purpose:** To guide behavior, assign responsibilities, and ensure consistent enforcement of security practices.
- Examples:
  - **Security policies** (acceptable use, BYOD policies)
  - **User training and awareness programs**
  - **Incident response plans**
  - **Access control policies** (who can access what)
  - **Regular audits and risk assessments**
  - **Change management procedures**

Assignment:

- Why is Network security essential?

Common Threats to Network Security

- **Malware**: Includes viruses, worms, trojans, ransomware, spyware.
- **Phishing**: Fraudulent attempts to obtain sensitive information.
- **Denial of Service (DoS/DDoS)**: Overloading a system to make it unavailable.
- **Man-in-the-Middle (MitM) attacks**: Intercepting communication between two parties.
- **IP Spoofing**: Pretending to be a trusted IP address.
- **Sniffing**: Capturing unencrypted network traffic.
- **SQL Injection** and **Cross-Site Scripting (XSS)** via web applications

Core Components of Network Security

a) **Firewalls**
   - Filter incoming and outgoing network traffic based on predefined security rules.
   - Types: Packet-filtering, Next-gen firewalls.

b) **Intrusion Detection and Prevention Systems (IDS/IPS)**
   - **IDS**: Monitors and alerts about suspicious activities.
   - **IPS**: Takes actions to block or prevent such activities.

c) **Virtual Private Networks (VPNs)**
   - Encrypt data and create secure tunnels for remote access.

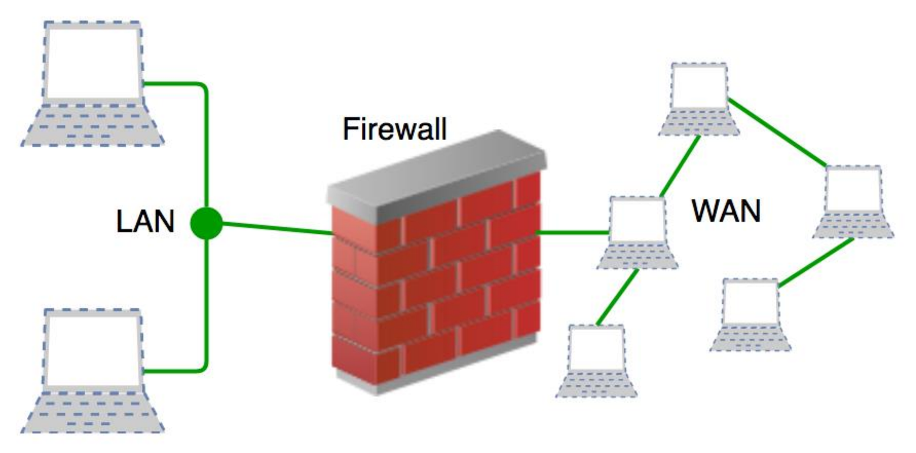
d) **Antivirus and Antimalware Software**
   - Detect and remove harmful software.

e) **Access Control**
   - Only authorized users and devices can access the network.
   - Implements user roles, permissions, and multi-factor authentication.

f) **Network Segmentation**
   - Divides a network into segments to limit access and contain breaches.

Firewall

- A firewall is **a network security device**, either hardware or software-based, which **monitors all incoming and outgoing traffic** and based on a defined set of security rules **accepts, rejects, or drops** that specific traffic.
  - ***Accept:*** *allow the traffic*
  - ***Reject:*** *block the traffic but reply with an "unreachable error"*
  - ***Drop :*** *block the traffic with no reply*
- A firewall is a type of network security device that **filters incoming and outgoing network traffic with security policies** that have previously been set up inside an organization.
- A firewall is essentially the wall that **separates a private internal network from the open Internet** at its very basic level.



What Firewalls Do?

- A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device.
- Firewalls, and especially Next Generation Firewalls, **focus on blocking malware and application-layer attacks**, along with an integrated intrusion prevention system (IPS)
- These Next Generation Firewalls can **react quickly and seamlessly to detect and react to outside attacks** across the whole network.
- They can **set policies to better defend your network** and carry out quick assessments to **detect invasive or suspicious activity**, like malware, and shut it down.

Network Layer Inspection

- Network layer or packet filters inspect packets at a relatively low level of the TCP/IP protocol stack, **not allowing packets to pass through the firewall** unless they match the established rule set where the source and destination of the rule set is based upon Internet Protocol (IP) addresses and ports.
- Firewalls also perform basic network level functions such as Network Address Translation (NAT) and Virtual Private Network (VPN).
  - NAT **hides or translates internal client or server IP addresses** that may be in a “private address range”, as defined in RFC 1918 to a public IP address.
  - A VPN **extends a private network across a public network** within a tunnel that is often encrypted where the contents of the packets are protected while traversing the Internet. This enables users to safely send and receive data across shared or public networks.

Firewall types

1. Hardware firewalls

- A hardware firewall is a system that works independently from the computer it is protecting as it filters information coming from the internet into the system.
- To protect your system, a **hardware firewall checks the data coming** in from the various parts of the internet and verifies that it is safe.
- Hardware firewalls that use packet filtering examine each data packet and check to see where it is coming from and its location.
- The data the firewall collects about each packet is then compared to a permissions list to see if it fits the profile of data that should be discarded.

2. Software Firewalls

- A software firewall is **a program used by a computer to inspect data that goes in and out** of the device.
- It can be customized by the user to meet their needs.
- Like hardware firewalls, software firewalls filter data by checking to see if it—or its behavior—fits the profile of malicious code.

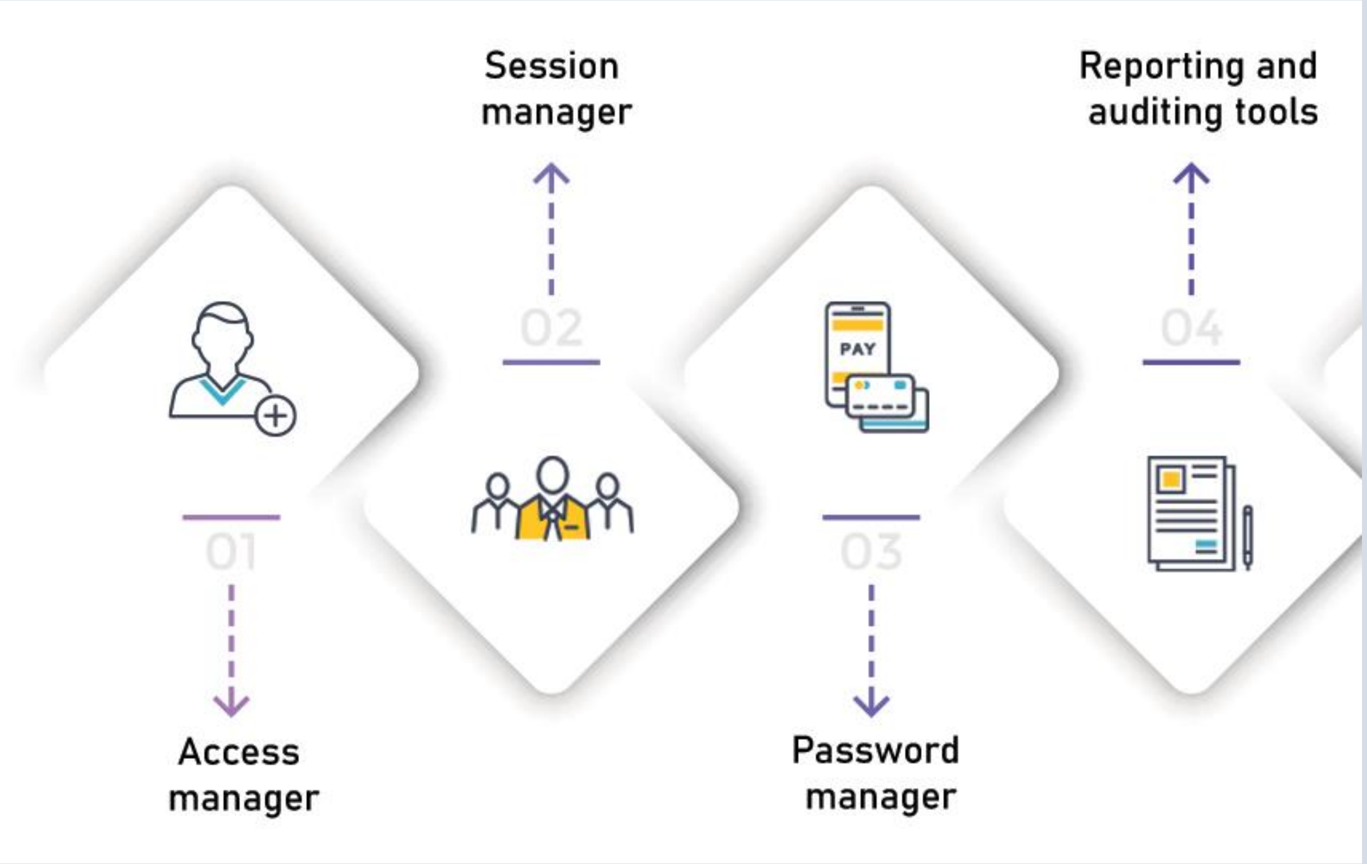
Privileged Access

- In an enterprise environment, “privileged access” is a term used to designate **special access or abilities above and beyond** that of a standard user.
- Privileged access refers to the special permission granted to certain users within a company, allowing them to execute high-level tasks that regular users can’t.
- **Privileged access** allows organizations to secure their infrastructure and applications, run business efficiently and maintain the confidentiality of sensitive data and critical infrastructure.
- Privileged access can be associated with human users as well as non-human users such as applications and machine identities.
- Examples privileged access used by humans;
    - **Super user account:** A powerful account used by IT system administrators that can be used to make configurations to a system or application, add or remove users or delete data.

Privileged Access Management (PAM)

- Privileged access management (PAM) is an identity security solution that focuses on ensuring that **only authorized individuals can perform critical tasks** such as:
  - Installing softwares
  - Making changes to system settings
  - Accessing sensitive data.

Key components of PAM



1. Access manager

- It **stores permissions, user roles, and privileged user information**. Policy managers use it to create access policies based on individual user identities or roles.

2. Session manager

- Session **manager monitors and controls all authenticated sessions** for users, apps, services, and systems.
- The session manager ensures real-time monitoring and sends out alerts in case of suspicious user behavior.
- In case of a verified attack, the manager must be able to terminate the session automatically.

3. Password manager

- All PAM solutions have a centralized, encrypted vault that **stores privileged credentials.**

4. Reporting and auditing tools

- Reporting tools are crucial for administrators to understand and evolve their existing security policies.
- These reports and the auditing system in the session manager, together, provide forensic information that can pin down how previous data breach attempts occurred and what mitigation techniques can prevent future attacks.

Reference video: https://www.youtube.com/watch?v=u-GxwreCzkk&list=PLN3wNGz9tgvKVzlNwb9zJoBRa3B-l2I9J

Access Control List (ACL)

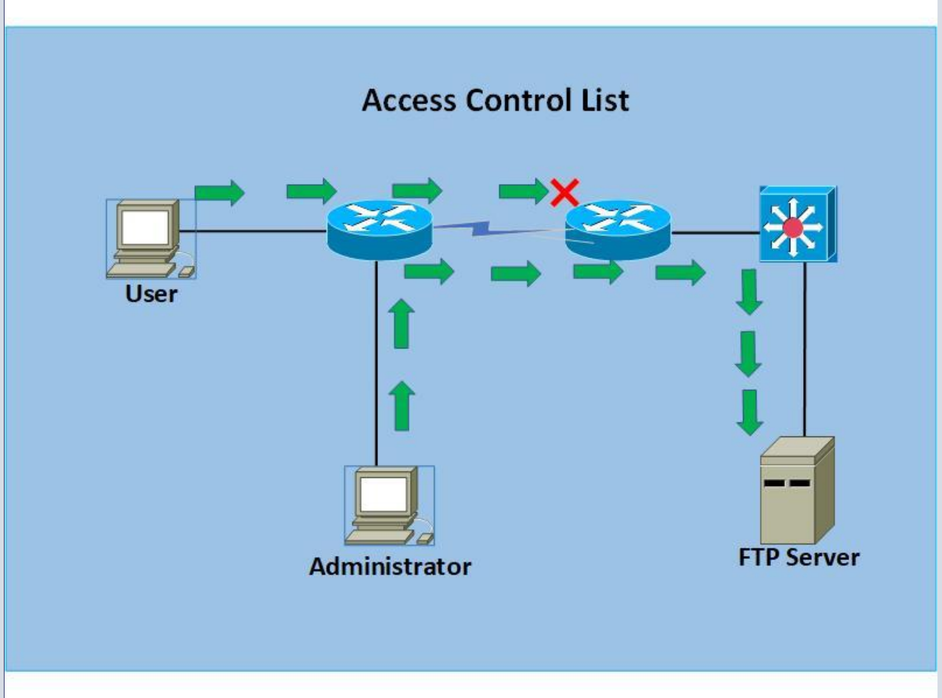
- An access control list (ACL) contains rules that grant or deny access to certain digital environments.
- Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.
- **Purpose**: To enhance security by restricting access to network resources based on IP addresses, protocols, ports, etc

Filesystem ACL vs Networking ACL

- **Filesystem ACLs:**
  - **filter access to files** and/or directories.
  - Filesystem ACLs tell operating systems which users can access the system, and what privileges the users are allowed.
- **Networking ACL**
  - **filter access to the network.**
  - Networking ACLs tell routers and switches which type of traffic can access the network, and which activity is allowed.

How ACL works?

- Networking **ACLs are installed in routers or switches,** where they **act as traffic filters**.
- Each networking **ACL contains predefined rules** (aka entries) that **control which packets or routing updates are allowed or denied access** to a network.
- Routers and switches with ACLs work like packet filters that **transfer or deny packets** based on filtering criteria.
- It decides this based on source and destination IP addresses, destination port and source port, and the official procedure of the packet.



Types of ACL

There are two main different types of Access-list namely:

1. **Standard ACL**
   - An access-list that is developed solely **using the source IP address.**
   - These access control lists allow or block the entire protocol suite.
   - They don’t differentiate between IP traffic such as UDP, TCP, and HTTPS.
   - They use numbers **1-99** or **1300-1999** so the router can recognize the address as the source IP address.
   - **Suitable for simple filtering** needs where only the source address matters
2. **Extended ACL**
   - An access-list that is widely used as it can differentiate IP traffic.
   - It **uses both source and destination IP addresses** and port numbers to make sense of IP traffic.
   - You can also specify which IP traffic should be allowed or denied. They use the numbers **100-199** and **2000-2699.**
   - **Suitable for complex filtering** needs where multiple attributes of traffic need to be considered.

Assignment:

- **Security, Privacy and Trust**

2.1.2 Computer and Network Threats

- Networks operate on the principles of communication and sharing.
- Unfortunately, these principles mean that network traffic and data can be more easily subject to access by people who have no authority to do so.
- Understanding the various types of computer and network threats is essential for developing effective cybersecurity strategies.
- These threats can compromise the integrity, confidentiality, and availability of information systems.

Malware

- **Malicious software designed to harm, exploit**, or otherwise compromise **a computer system**.
- Malware is a software that is designed to attack, control and damage a device's security and infrastructure systems.
- Once launched, malware will attach itself to a selected program or device.
- In order for malware to infect a device, it must be sourced. Some of the most common malware sources include: phishing, social engineering, pop-ups, drive-by downloads, shared networks,

Common Types of Malware

i. Viruses

ii. Worms

iii. Trojans

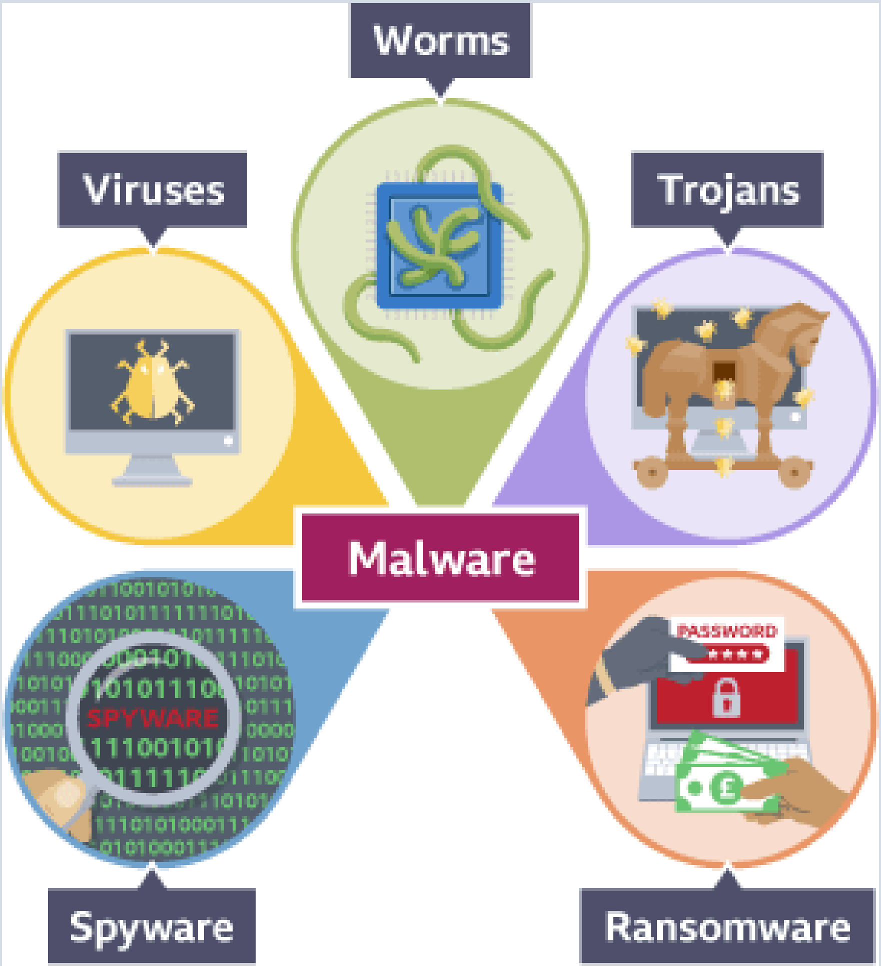
iv. Ransomware

v. Spyware

vi. Adware

vii. Rootkits

viii. Botnets



i) Viruses

- A virus is a type of malware that attaches itself to a legitimate program or file and spreads to other files and programs on the same system or across networks when the infected file is executed.
- **Characteristics**:
  - Requires user action to activate and spread (e.g., opening an infected file).
  - Can corrupt or modify files, causing system malfunction.
- **Examples**:
  - **File Infector Viruses**: Attach to executable files and spread when the files are run.
  - **Macro Viruses**: Infect macros in applications like Microsoft Word and Excel.
  - Others are like : Boot-sector viruses, polymorphic viruses, Multipartite viruses
- **Impact**:
  - Data corruption and loss.
  - System instability and crashes.
- **Mitigation**:
  - Install and regularly update antivirus software.
  - Avoid opening suspicious email attachments or downloading files from untrusted sources.

ii) Worms

- Worms are standalone malware that replicate and spread independently across networks without needing a host file.
- **Characteristics**:
  - Spread automatically through network connections.
  - Consume network bandwidth and system resources.
- **Examples**:
  - **ILOVEYOU Worm**: Spread via email and caused widespread damage.
  - **Code Red Worm**: Targeted web servers and caused denial of service attacks.
  - Category: Email worms, Internet worms, Network worms, Instant Messaging worms
- **Impact**:
  - Network congestion and slowdown.
  - Potential to carry and spread additional malware payloads.
- **Mitigation**:
  - Keep operating systems and software updated with security patches.
  - Use firewalls and intrusion detection/prevention systems.

iii) Trojans

- Trojans are deceptive malware that disguise themselves as legitimate software but perform malicious activities when executed.
- **Characteristics**:
  - Do not replicate themselves like viruses or worms.
  - Can create backdoors, allowing unauthorized remote access to the system.
- **Examples**:
  - **Remote Access Trojans (RATs)**: Allow attackers to control the infected system remotely.
  - **Banking Trojans**: Steal banking credentials and financial information.
- **Impact**:
  - Unauthorized access and control of the system.
  - Theft of sensitive information.
- **Mitigation**:
  - Be cautious of downloading and installing software from unknown sources.
  - Use security software that can detect and block Trojan behavior.

iv) Spyware

- Spyware is malware designed to secretly monitor and collect information about the user’s activities without their consent.
- **Characteristics**:
  - Runs in the background, often without the user’s knowledge.
  - Can collect data such as browsing habits, keystrokes, and personal information.
- **Examples**:
  - **Keyloggers**: Record every keystroke made on the keyboard to capture passwords and other sensitive data.
  - **Adware**: Displays unwanted advertisements and may track user behavior.
- **Impact**:
  - Privacy invasion.
  - Theft of personal and financial information.
- **Mitigation**:
  - Install anti-spyware software and regularly scan for spyware.
  - Be cautious of free software that may bundle spyware.

v) Ransomware

- Ransomware encrypts the victim's data and demands a ransom payment for the decryption key.
- **Characteristics**:
  - Prevents access to data by encrypting files or locking the system.
  - Often demands payment in cryptocurrency to avoid tracing.
- **Examples**:
  - **CryptoLocker**: Encrypted files and demanded a ransom for the decryption key.
  - **WannaCry**: Exploited a Windows vulnerability to spread rapidly and encrypt data.
- **Impact**:
  - Loss of access to important data.
  - Financial loss from ransom payments and recovery efforts.
- **Mitigation**:
  - Regularly back up data and store it offline.
  - Keep all systems and software updated with the latest security patches.
  - Educate users about the risks of phishing emails and suspicious links.

vi) Rootkit

- Rootkits are designed to gain root-level (administrator) access to a system while hiding their presence and activities from users and security software.
- **Characteristics**:
  - Can modify system files and processes to avoid detection.
  - Often used to maintain long-term control over an infected system.
- **Examples**:
  - **Kernel-Level Rootkits**: Operate at the kernel level, providing high-level control over the system.
  - **User-Mode Rootkits**: Operate at the user level and are easier to detect and remove than kernel-level rootkits.
- **Impact**:
  - Stealthy and persistent control over the system.
  - Can disable security software and facilitate other types of attacks.
- **Mitigation**:
  - Use advanced security tools capable of detecting rootkit behavior.
  - Regularly monitor system integrity and unusual behavior.
  - Ensure the use of secure and updated software.

vii) Adware

- Adware is software that displays unwanted advertisements on the user’s system, often bundled with free software.
- **Characteristics**:
  - Often comes bundled with free software downloads.
  - Displays intrusive ads, pop-ups, or redirects browser searches to advertising websites.
- **Examples**:
  - **Fireball**: A browser hijacker that turned infected systems into ad-clicking machines.
  - **Gator**: A well-known adware that displayed targeted ads based on user browsing habits.
- **Impact**:
  - Annoyance and disruption of user experience.
  - Potential privacy invasion by tracking user behavior.
  - Reduces system performance.
  - Can track user behavior and invade privacy.
- **Mitigation**:
  - Use reputable ad blockers and anti-adware tools.
  - Be cautious when downloading free software, and always opt for a custom installation to deselect unwanted adware.

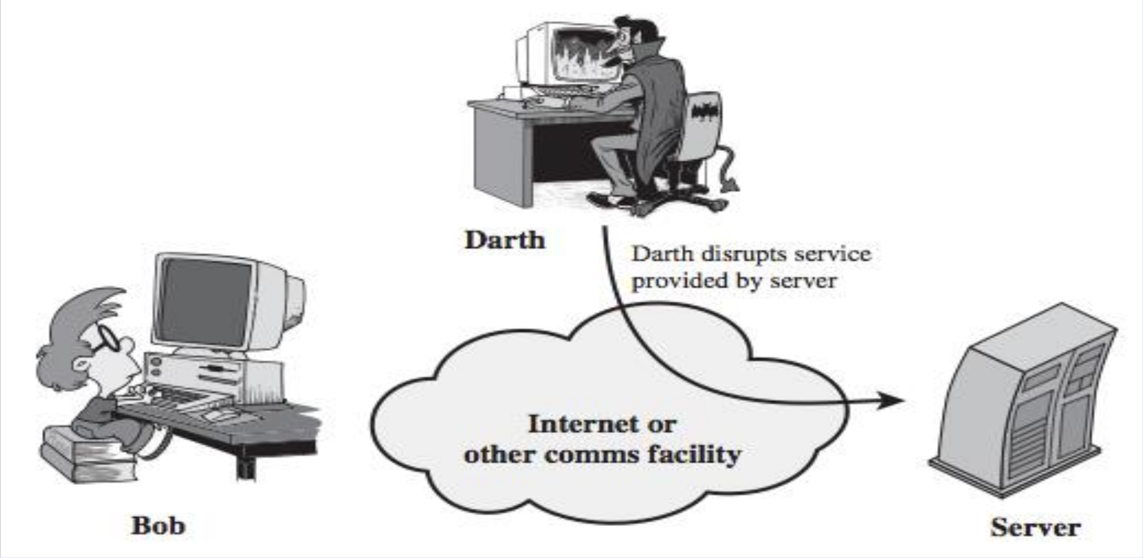
viii) Bots/Botnets

- type of malware that enables an attacker to take control of an infected computer without the user's knowledge. A botnet is a network of compromised computers (bots) that are controlled by a single attacker or a group of attackers.
- **Characteristics**:
  - Consists of thousands to millions of infected devices.
  - Controlled through command and control (C&C) servers.
  - Can be used to perform coordinated attacks or tasks.
- **Common Uses**:
  - **Distributed Denial of Service (DDoS) Attacks**: Overwhelming a target with traffic to make it unavailable.
  - **Mass Spam Campaigns**: Sending massive amounts of spam emails.
  - **Mining Cryptocurrencies**: Using the collective power of botnet devices to mine cryptocurrencies.
  - **Spreading Malware**: Distributing other types of malware to expand the botnet or infect more systems.
  - **Click Fraud**: Generating fraudulent ad clicks to generate revenue.
- **Mitigation:**
  - Detection and removal
  - Network security
  - User Awareness
  - Regular updates of OS

Distributed Denial of Service Attack (D/Dos)

- **An attempt to make a machine or network resource unavailable** to its intended users by overwhelming it with a flood of internet traffic.
- A distributed denial of service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually **by temporarily interrupting or suspending the services** of its hosting server.
- It **sends a flood of messages, malformed packets, or connection requests to the target system, forcing it to slow down** or entirely shut down, denying service to real systems and users. DDoS attacks can target a website, server, and other network resources.

- **Impacts**:
  - Service Disruption
  - Financial loses
  - Reputation Damage
- **Mitigation**:
  - Implement network firewalls and intrusion detection systems.
  - Use DDoS protection services.
  - Have an incident response plan in place.


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

Social Engineering

- Manipulation of individuals to divulge confidential information or perform actions that compromise security.
- **Techniques**:
  - **Phishing**: Fraudulent emails that appear legitimate to steal sensitive information.
  - **Pretexting**: Creating a fabricated scenario to obtain information.
  - **Baiting**: Offering something enticing to lure victims into a trap.
  - **Tailgating**: Gaining physical access to restricted areas by following authorized personnel.
- **Mitigation**:
  - Conduct regular security awareness training.
  - Implement strict access controls and verification processes.
  - Use multi-factor authentication.

Honeypot

- A honeypot is a security mechanism that **creates a virtual trap to lure attackers.**
- **Honeypot** is a network-attached system used as **a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers.
- Honeypots are a type of deception technology that allows you to understand attacker behavior patterns.
- Honeypots are mostly used by large companies and organizations involved in cybersecurity.
- It helps cybersecurity researchers to learn about the different type of attacks used by attackers.

2.2 Introduction to Penetration Testing

- ❑ **Basic Concepts of Information Gathering,**
- ❑ **Vulnerability Analysis,**
- ❑ **Forensics Tools,**
- ❑ **Sniffing,**
- ❑ **Spoofing,**
- ❑ **Password Attacks and**
- ❑ **Reverse Engineering**

2.2 Introduction to Penetration Testing

- Penetration testing (or pen testing) is a security exercise where a **cyber-security expert attempts to find and exploit vulnerabilities** in a computer system.
- The purpose of this simulated attack is **to identify any weak spots** in a system's defenses which attackers could take advantage of.
- Pen testing **involves ethical hackers** scaling planned attacks against a company's security infrastructure to hunt down security vulnerabilities that need to be patched up
- After completing a pen test, the **ethical hacker will share their findings** with the target company's security team.
- This **information can then be used to implement security upgrades** to plug up any vulnerabilities discovered during the test.

Purpose of Penetration testing:

1. **Identify Vulnerabilities**: Detect weaknesses in systems that could be exploited by attackers.
2. **Assess Impact**: Understand the potential impact of vulnerabilities if they were exploited.
3. **Improve Security**: Provide insights and recommendations to enhance the security posture of the organization.
4. **Compliance**: Ensure that the organization meets regulatory requirements and industry standards

Basic Concepts of Information Gathering

- Any product, website, or network these days is not secure from cyber-attacks.
- To prevent vulnerabilities and attacks, **organizations hire penetration testers to hack through their systems** and find out these vulnerabilities to fix them.
- The first stage an ethical hacker or attacker has to go through during a cyber attack is called **reconnaissance** or Information gathering.
- Reconnaissance in general is a military term that means gathering information about an enemy target.

Reconnaissance

- Reconnaissance, also known as information gathering, is the **first phase** of a penetration test or cyber attack, where **the attacker collects as much information as possible about the target, and plan the attack accordingly.**
- This can include information about the **target's physical characteristics**, **location**, and **activities**, as well as **information about the people** and **organizations** associated with the target.
- Reconnaissance can be **conducted in a variety of ways**, including through
  - physical surveillance,
  - online research, or
  - by using specialized tools and techniques,
- to identify vulnerabilities that can be exploited.

Methods of Reconnaissance:

1. Active Reconnaissance

- This **involves actively probing or interacting with the target system** to gather information.
- Some examples of active reconnaissance include **port scanning, vulnerability scanning**, and **social engineering.**
- Active reconnaissance can provide a wealth of information about the target, but it also carries a higher risk of detection and can potentially disrupt the target's operations.

2. Passive Reconnaissance

- This involves gathering information about the target **without actively interacting** with it.
- This is more like a **detective** gathering clues.
- Examples of passive reconnaissance include **observing network traffic, analyzing DNS records,** and **using search engines** to gather information about the target.
- Passive reconnaissance is less likely to be detected and can provide a lot of information about the target, but it may be less detailed than active reconnaissance.

Information Gathering Techniques

1. **Social Engineering:**
   - It is a form of passive reconnaissance
   - Social engineering is the **process of using psychological manipulation techniques to deceive people into providing sensitive information** or performing certain actions.
   - Social engineering techniques can include phishing, baiting, scareware, impersonation, dumpster diving, and shoulder surfing.
2. **Footprinting:**
   - This technique involves **gathering information about the target's network infrastructure and assets**, such as IP addresses, WHOIS records, DNS records, and other technical details.
3. **Network Scanning:**
   - It is an active reconnaissance method that involves sending packets to a range of IP addresses or ports on a target system and analyzing the responses and thus **identify active systems and open ports on a network.**
   - Network scanning can be done using a variety of tools, such as ping sweeps and port scanners.
   - The goal of network scanning is to create a map of the target network, including the IP addresses of active systems, open ports, and services.

4. Vulnerability Scanning:

- This technique involves using specialized tools **to scan a target's assets for known vulnerabilities**.

5. War Dialing:

- War dialing is a technique used in reconnaissance in cybersecurity that involves automatically dialing a range of phone numbers to identify active modems.
- It is an active reconnaissance method that is **used to identify potential targets** for a future attack.

6. Dumpster Diving:

- Dumpster diving is a technique used in cybersecurity that involves **looking through an organization's trash to gather information**.

7. Open-source Intelligence (OSINT):

- Open-Source Intelligence (OSINT) refers to the **process of collecting, analyzing, and disseminating publicly available information**.
- The information can be found on various sources such as the internet, social media, newspapers, publications, government reports, etc.

Vulnerability Analysis

- Vulnerability assessment is **the process of identifying, quantifying, and prioritizing vulnerabilities** in a system.
- It provides valuable insights into potential weaknesses that can be exploited by malicious actors and presents strategies to mitigate these risks.
- This process is not limited to IT systems; it also applies to physical locations, personnel, and procedural vulnerabilities.
- The **vulnerability assessment process typically involves the use of automated tools** to scan systems for known vulnerabilities.
- In a modern IT environment it is important to scan not only systems managed by the organization but also external systems such as cloud services and third party systems.

Importance of Vulnerability Assessment

1. **Identification of Security Weaknesses**
   - Security weaknesses could be **due to outdated software, misconfigurations, or lack of security controls**.
   - Identifying security weaknesses allows you to take preemptive action to fix them before they can be used against you.
2. **Prioritization of Threats**
   - Not all vulnerabilities carry the same level of risk. Some may pose a minor threat, while others **could lead to significant data breaches or system down times.**
   - It ensures that the most critical threats are dealt with first, thereby reducing the potential damage they could cause.
3. **Compliance with Regulations**
   - By **conducting a vulnerability assessment,** organizations demonstrate compliance, which can prevent fines and penalties and can build trust with customers and partners.
4. **Minimizing Internal and External Attack Surfaces**
   - Vulnerability assessment involves **identifying and minimizing all the possible points** in an organization's network—both internal and external—where unauthorized access can occur.

Some Common Vulnerabilities

1. **Software Bugs**:
   - Buffer overflows
   - Cross-site scripting (XSS)
   - SQL injection
2. **Configuration Issues**:
   - Default credentials
   - Unnecessary open ports
   - Weak encryption settings
3. **Outdated Software**:
   - Missing security patches
   - Unsupported software versions

- A **buffer overflow** occurs when more data is written to a buffer than it can hold. This can overwrite adjacent memory and potentially allow an attacker to execute arbitrary code or crash the system.
- **Cross-Site Scripting (XSS)** vulnerabilities occur when an application includes untrusted data in a web page without proper validation or escaping, allowing attackers to execute scripts in the context of another user's browser.
- **SQL injection** occurs when an attacker manipulates a SQL query by injecting arbitrary code through user input fields. This can result in unauthorized access to the database, data leakage, and modification or deletion of data.

Some Common Vulnerabilities

1. **Software Bugs**:
    - Buffer overflows
    - Cross-site scripting (XSS)
    - SQL injection
2. **Configuration Issues**:
    - Default credentials
    - Unnecessary open ports
    - Weak encryption settings
3. **Outdated Software**:
    - Missing security patches
    - Unsupported software versions

- **Default Credentials:** Many systems and applications come with default usernames and passwords, which are often well-known and easily exploitable if not changed.
- **Unnecessary Open Ports:** Open ports can expose services to the internet that may not be needed, increasing the attack surface and the potential for exploitation.
- **Weak Encryption Settings:** Weak or outdated encryption algorithms and settings can be broken by attackers, compromising the confidentiality and integrity of data.

Some Common Vulnerabilities

1. **Software Bugs**:
   - Buffer overflows
   - Cross-site scripting (XSS)
   - SQL injection
2. **Configuration Issues**:
   - Default credentials
   - Unnecessary open ports
   - Weak encryption settings
3. **Outdated Software**:
   - Missing security patches
   - Unsupported software versions

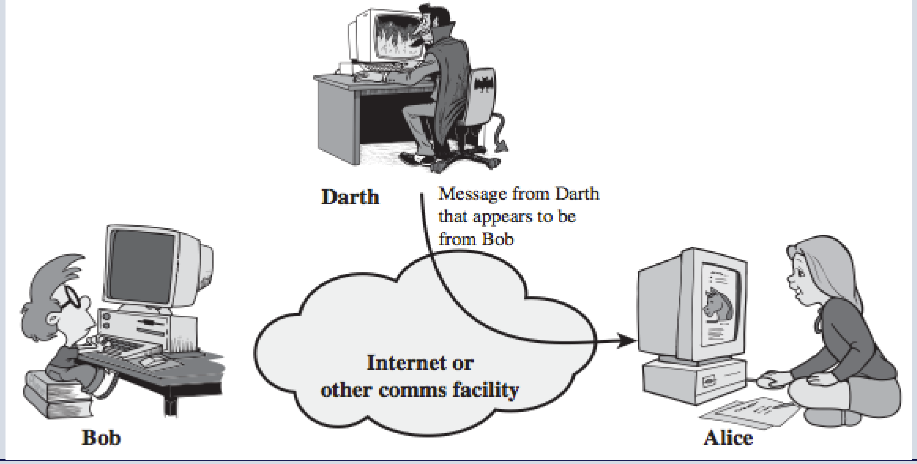
- **Missing Security Patches:** Software that is not regularly updated with security patches may contain known vulnerabilities that can be exploited by attackers.
- **Unsupported Software Versions:** Using software that is no longer supported by the vendor means no security updates or patches are available, leaving the system vulnerable.

Sniffing

- The **technique of capturing all data packets traveling through a network using a software application or hardware device** is known as network sniffing.
- Ethical hackers can use sniffing to gain tremendous insights into the workings of a network and the behavior of its users, which can be used to improve an organization's cybersecurity.
- However, when employed by malicious hackers, sniffing can be used to launch devastating attacks against unsuspecting targets.
- In its simplest form, sniffing is the **act of intercepting and monitoring traffic on a network.**

Spoofing (Masquerade)

- Spoofing is the **act of disguising a communication from an unknown source as being from a known**, trusted source.
- Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.
- Spoofing can be used to gain access to a target’s personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack.
- Types of Spoofing:
  - Email Spoofing
  - Called ID spoofing
  - Website Spoofing
  - IP spoofing
  - ARP Spoofing


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

1. Email Spoofing

- Email spoofing occurs when an **attacker uses an email message to trick a recipient into thinking it came from a known and/or trusted source**.
- These emails may include links to malicious websites or attachments infected with malware, or they may use social engineering to convince the recipient to freely disclose sensitive information.

2. Caller ID Spoofing

- With caller ID spoofing**, attackers can make it appear as if their phone calls are coming from a specific number**—either one that is known and/or trusted to the recipient, or one that indicates a specific geographic location.
- Attackers can then use social engineering—often posing as someone from a bank or customer support—to convince their targets to, over the phone, provide sensitive information such as passwords, account information, social security numbers, and more.

3. Website Spoofing

- Website spoofing refers to when **a website is designed to mimic an existing site known and/or trusted by the user.**
- Attackers use these sites to gain login and other personal information from users.

4. IP Spoofing

- Attackers may use IP (Internet Protocol) spoofing to **disguise a computer IP address, thereby hiding the identity of the sender** or impersonating another computer system.
- One purpose of IP address spoofing is to gain access to a networks that authenticate users based on IP addresses.

5. ARP Spoofing

- Address Resolution Protocol (ARP) is a protocol that resolves IP addresses to Media Access Control (MAC) addresses for transmitting data.
- ARP spoofing is used to link an attacker's MAC to a legitimate network IP address so the attacker can receive data meant for the owner associated with that IP address.
- ARP spoofing is commonly used to steal or modify data but can also be used in denial-of-service and man-in-the-middle attacks or in session hijacking.

6. DNS Server Spoofing

- DNS (Domain Name System) servers resolve URLs and email addresses to corresponding IP addresses.
- DNS spoofing allows attackers to divert traffic to a different IP address, leading victims to sites that spread malware.

Password Attacks

- A password attack is **any attempt to exploit a vulnerability** in user authorization within a digital system.
- Types of Password Attack:
  1. Phishing
  2. Man-in-the-Middle Attack
  3. Brute Force Attack
  4. Credential Stuffing
  5. Keylogging
  6. Rainbow Table Attack

1. Phishing

- Phishing involves a **hacker pretending to be a trusted party** and reaching out to their target requesting that they share personal login information.
- This often takes the **form of a password-reset request** or an account-confirmation email and can go as far as installing malicious code on the target's machine when the provided link is accessed.

2. Man-in-the-Middle Attack

- In a man-in-the-middle (MitM) attack, **a hacker positions himself between** a user and the system they are accessing.
- This form of wiretapping often **capitalizes on unsecured Wi-Fi connections** or unencrypted communications and allows the attacker to intercept or modify the data being communicated with the application.
- The hacker can **then capture, or even replace, login credentials**.

3. Brute Force Attack

- A brute force **attempts to gain access to restricted accounts and networks through trial and error,** trying a large number of username and password variations.

4. Credential Stuffing

- It seems like the first thing a **target would want to do after suffering an attack would be to change their login credentials.**
- Unfortunately, many victims continue to use the same (or similar) usernames and passwords — particularly if they aren’t aware that their information has been compromised.
- Credential stuffing is **a kind of password attack that uses leaked login information** captured during a previous attack in an attempt to gain further access.

5. Keylogging

- Keylogging is made **possible by malware infection.**
- A keylogger program is downloaded onto the target's device (generally by masquerading as a legitimate download), where it can then **record and share the user's keystrokes — including their usernames and passwords — with the attacker.**

6. Rainbow Table Attack

- One of the more complex kinds of password attacks, a rainbow table attack applies a similar approach as brute force attacks.
- The difference is that **these attacks attempt to decipher password encryptions rather than directly guess the passwords themselves**.
- Rainbow tables incorporate known solutions to common encryption algorithms, reaching into the system itself to expose the database of authorized login information.

Reverse Engineering

- When malware is discovered, the first thing that security researchers want to know is **how it works.**
- Reverse engineering is used in the realm of computer security to **investigate malware activities and develop solutions to combat it**.
- Applications in cybersecurity:
  1. Malware Analysis
  2. Vulnerability discovery
  3. Software cracking and piracy prevention
  4. Incident response
  5. Digital forensic

Threat, Vulnerability and Risk

- **Threat:** a potential cause of an incident that may result in harm to a system or organization
- **Vulnerability:** a weakness of an asset (resource) or a group of assets that can be exploited by one or more threats
- **Risk:** potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability
- Example:
  - In a system that allows weak passwords,
    - ○ **Vulnerability---**password is vulnerable for dictionary or exhaustive key attacks
    - ○ **Threat:** An intruder can exploit the password weakness to break into the system
    - ○ **Risk:** the resources within the system are prone for illegal access/modify/damage by the intruder.
- **Threat agent-**--entities that would knowingly seek to manifest a threat

Risk is the intersection of assets, threats and vulnerabilities

- A + T + V = R
- That is, Asset + Threat + Vulnerability = Risk
- Risk is a function of threats exploiting vulnerabilities to obtain, damage or destroy assets. Thus, threats (actual, conceptual, or inherent) may exist, but if there are no vulnerabilities then there is little/no risk

Asset: paper document

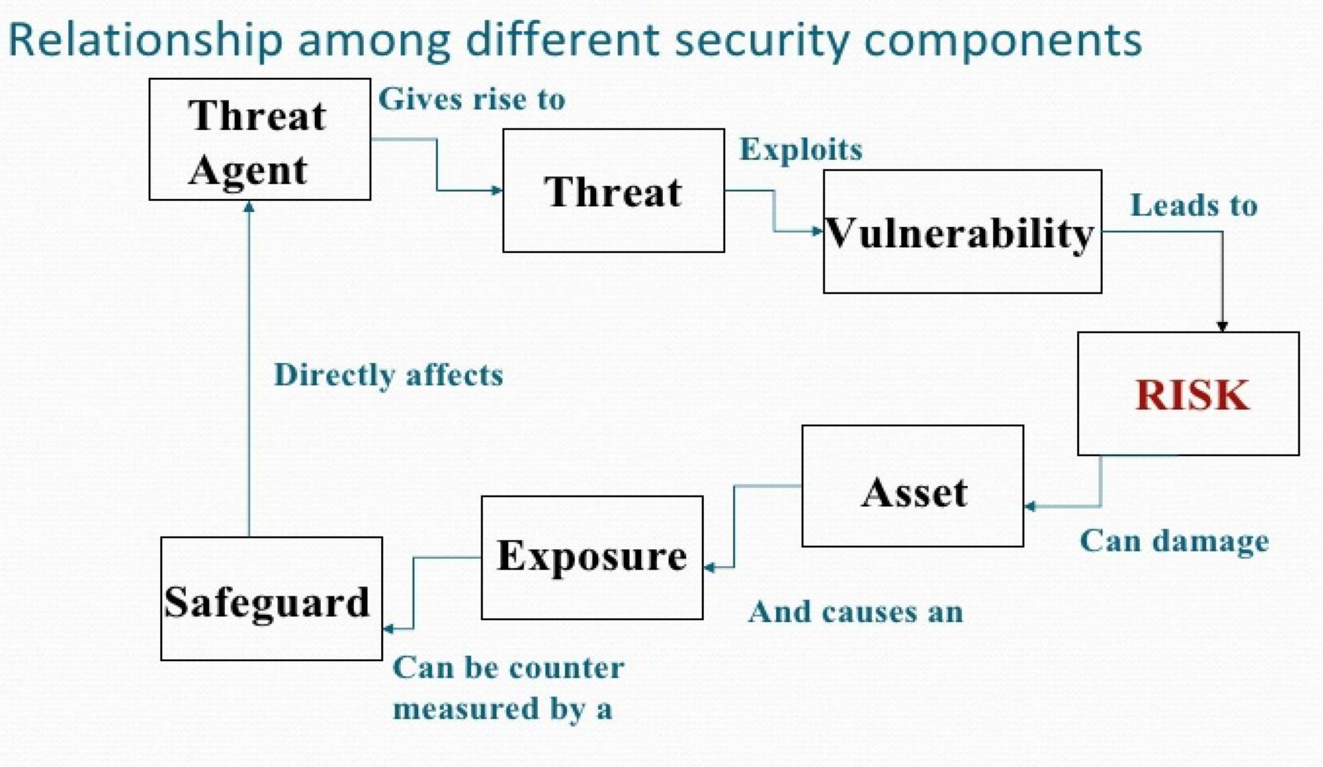
- **Threat:** fire; **vulnerability**: document is not stored in a fire-proof cabinet (risk related to the loss of availability of the information)
- **Threat**: fire; **vulnerability**: there is no backup of the document (potential loss of availability)
- **threat**: unauthorized access; **vulnerability**: document is not locked in a cabinet (potential loss of confidentiality)

Asset: digital document:

- **threat**: disk failure; **vulnerability**: there is no backup of the document (potential loss of availability)
- **threat**: virus; **vulnerability**: anti-virus program is not properly updated (potential loss of confidentiality, integrity and availability)
- **threat**: unauthorized access; **vulnerability**: access control scheme is not properly defined (potential loss of confidentiality, integrity and availability)
- **threat**: **unauthorized** access; **vulnerability**: the access was given to too many people (potential loss of confidentiality, integrity and availability)

Asset: system administrator:

- **threat**: unavailability of this person; **vulnerability**: there is no replacement for this position (potential loss of availability)
- **threat**: frequent errors; vulnerability: lack of training (potential loss of integrity and availability)



Relationship among different security components

2.3 Data Confidentiality (Privacy, Confidentiality, and Secrecy)

- Privacy, confidentiality, and secrecy are interrelated concepts in information security and data protection, but they have distinct meanings and applications.

Privacy:

- Privacy refers to an individual's right to control access to their personal information and to make decisions about how it is collected, used, and shared.
- **Example:** A social media user expects their personal messages to remain private and not be read by unauthorized parties or shared without their consent.
- Criminals can use personal data **to defraud or harass users.**
- Entities **may sell personal data to advertisers** or other outside parties **without user consent,** which can result in users receiving unwanted marketing or advertising.
- Data privacy is the **protection of personal data** from those who should not have access to it
- **data privacy governs how the data is collected, shared and used.**
- **Data privacy is the branch of data management that deals with handling personal data in compliance with data protection laws, regulations, and general privacy best practices**

Confidentiality:

- Confidentiality refers to the obligation to protect information from unauthorized access and disclosure. It ensures that data is only accessible to those who are authorized to view it.
- **Example:** A healthcare provider must keep patient medical records confidential and ensure that only authorized medical personnel can access them.
- **Key Aspects:**
  - **Access Control:** Implementing measures to restrict access to authorized users only.
  - **Encryption:** Using encryption to protect data in transit and at rest.
  - **Policies and Procedures:** Establishing protocols for handling and sharing confidential information.

Secrecy:

- Secrecy involves keeping information hidden from everyone except those explicitly authorized to know it.
- It is often used in contexts where information needs to be kept strictly limited to a few individuals.
- **Example:** A government agency may classify certain documents as top secret, limiting access to only those with the highest security clearance.
- **Key Aspects:**
    - **Strict Access:** Very limited and controlled access to the information.
    - **Non-Disclosure:** Ensuring that those who have access do not share the information.
    - **High Stakes:** Often involves information of critical importance, such as national security secrets or trade secrets.

Some Forensic Tools

Forensic Tools

1. **EnCase**: EnCase is a widely used commercial forensic tool that offers comprehensive capabilities for data acquisition, analysis, and reporting. It supports various file systems and can recover data from a wide range of storage devices.
2. **FTK (Forensic Toolkit)**: FTK is another popular commercial forensic tool that provides powerful features for digital evidence analysis, including keyword searching, timeline analysis, and email analysis. It also supports live analysis of running systems.
3. **Autopsy**: Autopsy is an open-source digital forensic tool that offers a graphical interface for analyzing disk images and file systems. It includes features such as keyword searching, timeline analysis, and support for various file formats.
4. **Sleuth Kit**: The Sleuth Kit is a collection of command-line tools for forensic analysis of disk images and file systems. It provides low-level access to disk data and supports various file systems, including NTFS, FAT, and ext.
5. **Volatility**: Volatility is an open-source memory forensics framework that allows investigators to extract and analyze volatile memory (RAM) from live systems. It provides capabilities for analyzing process memory, network connections, and malware artifacts.
6. **X-Ways Forensics**: X-Ways Forensics is a commercial forensic tool known for its speed and efficiency in analyzing disk images and file systems. It offers features such as file carving, registry analysis, and support for virtual machine disk images.
7. **Cellebrite UFED**: Cellebrite UFED is a mobile forensic tool used for extracting and analyzing data from mobile devices such as smartphones and tablets. It supports a wide range of device models and operating systems, including iOS and Android.
8. **Wireshark**: Wireshark is a popular open-source network protocol analyzer that is often used in digital investigations to capture and analyze network traffic. It allows investigators to reconstruct network sessions and identify suspicious activity.
9. **Oxygen Forensic Detective**: Oxygen Forensic Detective is a commercial forensic tool designed specifically for mobile device forensics. It supports data extraction from smartphones, tablets, drones, and other IoT devices.
10. **Paladin Toolbox**: Paladin Toolbox is a Linux-based forensic suite that includes a variety of open-source forensic tools pre-installed on a bootable USB drive. It is designed for live forensic analysis and supports both Windows and Linux systems.

Exercise:

1. Define Information security.
2. What do you mean by non-repudiation? Provide an example.
3. Mention the significance of information security.
4. What is security breach? Provide few examples.
5. Define network security. Why is it essential?
6. How is network security different from information security?
7. How firewall acts as a network security device?
8. What are NAT and VPN? How they provide network security?
9. Explain the types of firewall?
10. What is privileged access? Provide an example of privileged access mechanism in a bank.
11. What is Privileged access management (PAM)? Explain the key components of PAM.
12. What is Access control list (ACL)? Where is it used in the network?
13. How ACL acts as traffic filters in the network?
14. Differentiate between standard ACL and Extended ACL.

15. Explain the term: security, privacy and trust.
16. What are malwares? Why do people create malwares?
17. List any 8 malwares that you know.
18. Introduce viruses with their characteristics and examples.
19. What are the impacts of viruses? How can we mitigate computer viruses?
20. How worms are different to viruses? Provide the characteristics of worm. Also give examples.
21. What are Trojans? Write its characteristics and give examples.
22. What do spyware do? Where are they usually found to be working?
23. Ransomwares are evident nowadays. How do they harm our data? Explain with examples of it.
24. What are Rootkits? Explain with their characteristics, examples, impact and mitigation.
25. How adware annoys us? Provide examples of such, and explain it
26. What are Bots and Botnets?
27. Explain D/Dos in detail.

28. Social engineering is a hot topic in cybersecurity. How hackers use social engineering to steal confidential data from users? Explain the different techniques in brief.
29. How honeypot play a significant role in cyber security?
30. What do you mean by penetration testing? Is it essential? Give reasons.
31. What are the purposes of Pen-testing?
32. Explain the term: reconnaissance.
33. Differentiate between active reconnaissance and passive reconnaissance.
34. Mention the information gathering techniques for pen-test.
35. Explain the terms: war dialing and Dumpster diving.
36. How we need to perform vulnerability analysis? Write its importances.
37. Explain Cross-site scripting and SQL injection.
38. Explain sniffing and spoofing.
39. What is Masquerade?
40. Mention the types of spoofing (Masquerade).
41. Define password attack. Mention any six types of it.
42. Define reverse engineering.
43. Risk is the intersection of assets, threat and vulnerability. Justify.

End of Chapter