Security+ | Pritam Suryawanshi

Social Engineering:

Social engineering is the act of tracking people into giving up confidential information or doing things that compromise security. It relies on **manipulation human behavior** rather than hacking technology.

▼ Social Engineering Attacks :

1. Phishing: A scam where attackers pretend to be a trusted entity to trick people into revealing sensitive information like passwords and credit card numbers.
2. Spear Phishing: Phishing targeted at a specific group, organization, or demographic.
3. Whaling: A type of spear phishing targeting senior leaders of an organization.
4. Vishing: Where attackers **use phone calls** to trick people into revealing personal information.
5. Smishing (SMS Phishing): Sending fraudulent text messages to deceive recipients into providing sensitive information or clicking malicious links.

6. Spam: Unsolicited bulk messages sent to target audiences.
7. SPIM (Spam Over Instant Messaging): Attackers send unsolicited and often malicious messages through messaging services to promote scams.
8. Bluejacking: Spam over Bluetooth.
9. Credentials Harvesting: Specifically designed to steal account and authentication credentials.
10. Reconnaissance Attack: Using publicly available sources to collect information.
11. Watering Hole Attack: A technique where attackers inject malware through frequently used but insecure third-party applications or websites. When users in an organization regularly access a less secure site, it can become a vector for malware infection.
12. Typosquatting (URL Hijacking): When attackers create fake websites with addresses similar to popular websites, hoping users will mistype the web address and visit the fake site.
13. Dumpster Diving: A technique used to retrieve sensitive information by searching through an individual's or organization's trash, recycling, or other discarded materials. Attackers look for documents, hardware, or other items that may contain confidential data.
14. Shoulder Surfing: An attacker observes an authorized user—often by looking over their shoulder—to obtain sensitive information such as passwords, PINs, or other confidential data.
15. Tailgating: An unauthorized person follows an authorized person into a restricted area without their knowledge.
16. Piggybackingx: A security breach in which an unauthorized person gains access to a restricted area or system with the knowledge and consent of an authorized person, often by following closely behind them.

▼ Common Social Engineering Techniques:

1. Authority: Attackers pose as authority figures to gain compliance.
2. Intimidation: Attackers use threats and fear to pressure victims into compliance.

3. Consensus: Attackers exploit people's tendency to follow others' actions.
4. Scarcity: Attackers create false urgency by claiming limited availability to force rushed decisions.
5. Familiarity: Attackers act friendly and relatable to gain trust.
6. Trust: Attackers establish themselves as honest and reliable sources.
7. Urgency: Attackers use threatening or time-sensitive situations to force quick actions.

▼ Malware Threat Vectors

1. Viruses: **virus** is a type of **malicious software (malware)** designed to spread from one computer to another and **infect files or systems**. It often attaches itself to legitimate programs or files and activates when the host file is run.
2. Worms: A **worm** is a type of harmful software (malware) that spreads by itself from one computer to another, usually through a network. Unlike a virus, it doesn't need you to open a file or run a program—it spreads automatically by taking advantage of security weaknesses in systems. Worms can slow down networks, damage files, or even install other malware.
3. Trojans: **Trojan horse**, is a type of malware that tricks you into thinking it's a safe or useful program. Once you download or run it, it can secretly do harmful things—like steal your data, give hackers control of your device, or install more malware. Unlike viruses or worms, Trojans don’t spread by themselves; you have to install them, usually by mistake.
4. PUP/PUA (Potentially Unwanted Program/Application): Software that is installed alongside the application a user intended to download. It is often referred to as **grayware** because it is not always malicious, but it can negatively affect system performance, display unwanted ads, or collect user data without clear permission.
5. RAT (Remote Access Trojan): A type of malware that gives a hacker remote control over an infected computer. Once installed, a RAT can let the attacker secretly access files, monitor activity, steal information, or even control the webcam and microphone—often without the user knowing. It's commonly used for spying or stealing sensitive data.

Unauthorized Access:

1. Backdoor: A type of network software or malware that opens a hidden communication channel (or port) on a compromised system. This allows attackers to access the system remotely, bypassing normal authentication and security measures. Backdoors are often used to maintain persistent access without detection.
2. Bot: An automated program or script that performs tasks without the user's knowledge. In cybersecurity, bots are often used for harmful activities like sending spam, stealing data, or launching attacks. Many bots can be controlled together as a **botnet** to carry out large-scale attacks, such as **DDoS (Distributed Denial of Service)**, which overwhelm a target with traffic to disrupt its normal function.
3. RootKit: Malicious software that hides deep within an operating system, allowing attackers to gain control of the system while remaining hidden and undetected. Rootkits can hide files, processes, and system data, making it very difficult to find and remove them. Because of this stealthy nature, rootkits are considered one of the most dangerous types of malware.

Attack On Password:

1. Dictionary: A **Dictionary Attack** is a technique where attackers try to guess a password by using a list of common words and passwords instead of random guesses. It's faster than brute force attacks and works well against simple or common passwords. To stay safe, use strong passwords with a mix of letters, numbers, and symbols.
2. Brute Force: A **Brute Force Attack** is a method where an attacker tries every possible combination of characters to guess a password. It's slow but guaranteed to work eventually if the password is weak or short. Using long, complex passwords helps protect against this attack.
3. Hybrid: A **Hybrid Attack** is a password guessing method that starts with a list of common words (like a dictionary attack) but also adds frequently used variations—such as numbers, symbols, or letter substitutions—to those words. This makes it more effective at cracking passwords that are slightly modified versions of common terms.
4. Rainbow-Table: A **Rainbow Table** is a pre-made database of encrypted password hashes generated from many possible passwords. Instead of

trying every password combination during an attack, hackers use this table to quickly find a match between a stored password hash and the original password. This method is much faster than brute force because it reuses previously calculated results.

Tools to get this attack successful.

1. Hydra:

```
# syntax for Hydra
# Used in Dictionary, Brute-Force, Hybrid

hydra -l <username> -p <password> IP_Address http-post-form "/login:us
er=^USER^&pass=^PASS^:Login Failed"

- -L  Dictionary of username
- -P Dictionary of password
```

Physical Security Threats

1. Malicious USB Cable: Modified USB cable that looks like a regular one but contains hidden components to compromised devices. when plugged in, it can execute commands, steal data, or control device remotely without the user's knowledge. Also know as `Rubber Ducky` or `BadUSB`
2. Flash Drives: This attack involves using a compromised USB flash drive that, when plugged into a computer, can automatically run malicious software. This malware can steal data, install harmful programs, or give attackers remote access to the device.
3. Card Cloning: When someone illegally copies the data from your credit card's magnetic strip to create a duplicate card. This allows the attackers to make unauthorized transactions using your information.
4. Skimming: A method used by criminals where they install a fake (counterfeit) card reader on top of a real ATM or point-of-sale machine. When you swipe or insert your card, the fake reader secretly captures your card information. Often, hidden cameras or fake keypads are also used to steal your PIN, allowing them to make unauthorized withdrawals or purchases.

Third Party Attacks

1. Supply Chain: A type of attack where attackers target less secure elements of an organization's supply chain—such as vendors, contractors, or third-party service providers—to gain access to the main target. They may compromise software, hardware, or services from these third parties to infiltrate the organization.
2. Cloud-based attack: Attackers target and exploit cloud services or infrastructure to gain unauthorized access to data, services, or misuse cloud resources for malicious activities.
3. Poorly Written APIs: Insecure or poorly developed APIs can create serious security risks by exposing sensitive data and allowing unauthorized access to systems. These vulnerabilities often result from weak authentication mechanisms, missing or improper input validation, and excessive data exposure in API responses. Attackers can exploit these flaws to steal data, bypass access controls, or even manipulate backend systems.

Cross-Site Scripting (XSS) → Most common & popular attack

XSS allows attackers to inject malicious scripts into web pages that are viewed by other users. These scripts can be used to steal data, manipulate page content, or spread malware.

- For More Details Refer This Page

> 💡 🐞 XSS (Cross-Site Scripting) | Hackers Handbook (1)

Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) is a type of web security vulnerability where an attacker tricks a logged-in user into performing unintended actions on a trusted web application without their knowledge or consent.

- How it works:

- A user logs into a trusted website (e.g., online banking) and the browser stores authentication cookies.
- Without logging out, the user visits a malicious website in another tab or window.
- The malicious site contains hidden code (such as an auto-submitting form or image request) that sends a crafted request to the trusted site.
- Since the user is still authenticated, the trusted site processes the request as if it were intentionally made by the user.
- This can result in unauthorized actions, like transferring money, changing account details, or deleting data.

- **XSS (Cross-Site Scripting):** Exploits the **user's trust in a website** by injecting malicious scripts that run in the user's browser.
- **CSRF (Cross-Site Request Forgery):** Exploits the **website's trust in the user** by tricking the user's browser into making unauthorized requests.

Network-Based Attacks

1. Fuzzing: **Fuzzing** is an automated software testing technique used to discover vulnerabilities by inputting large amounts of random, unexpected, or malformed data into an application. The goal is to observe how the application behaves—crashes, memory leaks, or unexpected responses may indicate a security flaw.
2. Port Scan: A **port scan** is a technique used to identify open ports and services running on a target system. Attackers send a series of requests to different ports to discover which ones are open, closed, or filtered. This information helps them map the network and identify potential vulnerabilities.

> While port scanning can be used by system administrators for network diagnostics, it is often the first step in a

> cyberattack to find exploitable services.

2. X-mas scan: An **Xmas scan** is a type of **TCP port scanning technique** used to identify open, closed, or filtered ports on a target system. It gets its name because it sets three specific TCP flags—**FIN**, **URG**, and **PUSH**—which, when viewed in a packet, appear "lit up" like a Christmas tree.
3. Man-in-the-Middle: A **Man-in-the-Middle** attack occurs when an attacker secretly intercepts, relays, or alters communication between two parties who believe they are directly communicating with each other. The attacker positions themselves between the sender and receiver without their knowledge.
    a. passive: (sniffing)
        - The attacker silently monitors and captures data being exchanged (e.g., usernames, passwords, session tokens).
        - No modification of the data; used mainly for eavesdropping and information gathering.
    b. Active: (session hijack)
        - The attacker intercepts and modifies communication in real time.
        - They can impersonate one or both parties, inject malicious content, or hijack sessions to gain unauthorized access.

Spoofing

1. **IP Spoofing**: IP Spoofing is a technique where an attacker **fakes the source IP address** in a packet to make it appear as if it's coming from a trusted source. This is done to **bypass security filters**, **impersonate other systems**, or **launch attacks** like Denial of Service (DoS) or Man-in-the-Middle.
2. **MAC Spoofing**: MAC Spoofing is a technique where an attacker **alters the Media Access Control (MAC) address** of their device to impersonate another device on the same network. This can be used to **bypass network access controls**, **evade tracking**, or **intercept network traffic**.
3. **Email Spoofing**: Email Spoofing is a technique where an attacker **forges the sender's email address** to make the message appear as if it came from a

trusted source. The goal is to **trick the recipient** into trusting the message, often used in **phishing attacks** or to spread **malware**.

4. **Caller ID Spoofing**: Caller ID Spoofing is a technique where an attacker **fakes the phone number displayed on the recipient's caller ID** to make the call appear as if it's coming from a trusted source (e.g., a bank, government agency, or known contact).
5. **Smurf Attack:**A **Smurf Attack** is a type of **Denial-of-Service (DoS)** attack that exploits the **Internet Control Message Protocol (ICMP)**, specifically **ICMP Echo Requests (ping)**.

> **How it works:**
>
> i. The attacker sends ICMP Echo Requests to a broadcast IP address (e.g., 192.168.1.255) using the **spoofed IP address** of the victim as the source.
>
> ii. All devices on the network respond to the ping request, sending replies back to the victim's IP address.
>
> iii. This results in a **flood of ICMP replies**, overwhelming the victim's system or network.

Vulnerability Scanners

Vulnerability scanners are tools used to **identify security weaknesses** in systems, networks, or applications. They scan devices to detect:

- **Known vulnerabilities and exploits**
- **Missing security patches or updates**
- **Misconfigured system settings**
- **Default credentials or insecure configurations**

> **Examples:** Nikto, Nessus, OpenVAS, Qualys, Nexpose

Honeypots

A **honeypot** is a **decoy system or resource** intentionally designed to appear vulnerable and attract attackers. It mimics real systems by running open ports and services, making it look like an easy target.

- **Pseudo Flaw:** A deliberately inserted vulnerability or loophole in the operating system or application, used to lure attackers.
- **Purpose:** To **distract attackers** from real production systems and to **observe, detect, and analyze** malicious behavior.
- **Attractiveness:** Honeypots often simulate common vulnerabilities and leave many ports/services open to appear realistic.

> Collection of Honeypots is called honeynet.

Penetration Testing

Penetration Testing is an **active and potentially intrusive** security assessment technique that involves **simulating real-world cyberattacks** to evaluate the effectiveness of an organization's defenses.

- penetration testers uses set of procedures and tools designed to test and possibly bypass security control of system.
- Goal is to measure an organization’s level of resistance to an attack and to uncover any weaknesses within the environments
- Testers emulate the **same tactics, techniques, and procedures (TTPs)** that real attackers would use.
- Penetration tests should only be conducted with **written approval** from senior management to ensure legality and reduce risk to production systems.

Degree of Knowledge

1. Black-Box (zero knowledge) : The pen testing team does not have any knowledge of the target and must start from ground zero.
2. Grey-Box (Partial knowledge): The pen testing team has some information about the target.

3. White-Box (Full knowledge): The testing team has **complete knowledge** of the target system, including source code, architecture, and network diagrams. This approach allows for a **deep and thorough assessment** of potential vulnerabilities.
4. Blind Test: In this scenario, the defenders (e.g., the security team) are **unaware that a test is being conducted**. This simulates a **real-world attack** and helps evaluate the organization's **detection and incident response capabilities**.
5. Target Test: A **focused assessment** on specific systems, applications, or components—often conducted before deploying a new system to production. This helps identify vulnerabilities in critical areas early in the development or deployment lifecycle.

Data Sovereignty

Data Sovereignty refers to the concept that **digital data is subject to the laws and regulations of the country where it is stored or processed**. This impacts how data is accessed, secured, and managed—especially across international borders.
Some countries require that data related to their citizens be **stored locally** to ensure **privacy**, **security**, and **compliance with national laws.**

Masking, Obfuscation, Anonymization and Tokenization

- Data Masking: The process of **hiding or replacing sensitive information** with fictional or scrambled data. Used primarily to protect data in non-production environments (e.g., testing or training).
- Obfuscation: Is the process of using specific characters to be hide certain parts of a specific dataset. **Example:** Showing only the last 4 digits of a Social Security Number (e.g., ***--1234).
- Data Anonymization: Is process of either encryption or removing personally identifiable information from data sets so that the people whom the data describe remain anonymous.
- Tokenization: Sensitive data is **replaced with a token** (a non-sensitive reference value). The actual data is stored securely elsewhere (often in a

private cloud or secure database). The token is meaningless if intercepted, ensuring **data protection during processing or transmission**.

- BitLocker: **BitLocker** is a full disk encryption feature built into Windows that allows users to **encrypt the entire drive**, protecting data from unauthorized access. The **encryption key is securely stored in the TPM (Trusted Platform Module)** chip on the computer's motherboard, ensuring that the drive can only be decrypted by authorized users on that specific device.

Virtualization

Virtualization is the process of creating **virtual instances of computing resources**—such as servers, operating systems, storage, or networks—on a single physical machine.

- Enables **logical isolation** in multi-tenant environments, allowing multiple virtual machines (VMs) to run independently on the same hardware.
- Provides a **safe and flexible environment** for testing software, updates, and configurations.
- Supports **snapshots**, which allow for quick backups and easy restoration of virtual machines.
- However, it can also introduce risks, as attackers may attempt to exploit vulnerabilities in virtual components to gain **unauthorized access** to data or systems.
- The overall security depends heavily on the **hypervisor**, the software layer that manages and isolates the virtual machines.

Hypervisor

A **Hypervisor**, also known as a **Virtual Machine Monitor (VMM)**, is software that **creates, manages, and runs virtual machines (VMs)** on a host system. It enables multiple operating systems to run **simultaneously on a single physical machine** by abstracting and allocating hardware resources (CPU, memory, storage, etc.) to each VM.

Types of Hypervisors:

1. **Type 1 (Bare-Metal Hypervisor):**

- Runs **directly on the physical hardware**.
- Does **not require a host operating system**.
- Offers better performance and security.
- Examples: VMware ESXi, Microsoft Hyper-V, Xen

2. **Type 2 (Hosted Hypervisor):**
   - Runs **on top of a host operating system**.
   - Easier to set up, but with slightly lower performance.
   - Examples: VMware Workstation, Oracle VirtualBox, Parallels

---

Cloud Computing

Cloud computing is the delivery of computing services—such as **servers, storage, networking, databases, software, and more**—over the **internet** ("the cloud"). It enables organizations and individuals to access scalable and flexible IT resources **on-demand**, without the need to manage physical infrastructure.

Key Benefits:

- **Faster innovation** and deployment
- **Flexible and scalable resources**
- **Cost efficiency** through pay-as-you-go models (economies of scale)
- **Global accessibility** and high availability

Redundancy

Redundancy is the practice of creating **duplicate systems, components, or backups** to ensure that **critical operations continue** in the event of a failure. It helps eliminate **single points of failure** and improves the **reliability and availability** of systems.

Purpose:

- Ensure business continuity
- Minimize downtime
- Enhance fault tolerance and system resilience

Examples:

- Backup power supplies (e.g., UPS, generators)
- RAID for disk redundancy → (**Redundant Array of Independent Disks)**
- Failover servers and network paths

Cryptography

Cryptography is the practice and study of techniques used to **secure communication and data** from unauthorized access. It ensures key security principles such as **confidentiality, integrity, availability**, and **non-repudiation**.

It works by transforming **readable information (plaintext)** into an **unreadable format (ciphertext)** using **encryption algorithms** and **cryptographic keys**.

Security Services Provided by Cryptography (P.A.I.N):

- **Privacy (Confidentiality):** Prevents unauthorized access or disclosure of information.
- **Authenticity:** Verifies the **identity** of the sender or source of the data.
- **Integrity:** Ensures that data has not been **altered**, **modified**, or **corrupted** during transmission or storage.
- **Non-Repudiation:** Guarantees that the **sender cannot deny** having sent the message or signed the document. It combines both authenticity and integrity.

Types of Cryptography

1. **Symmetric Cryptography**: In this type of encryption where same key is used for both encryption and decryption of data. This method relies on single, Shared secret key that must be known by both sender and receiver.
    a. **Advantage**
        i. **Fast Performance:** Efficient for encrypting and decrypting large volumes of data, making it ideal for bulk data transmission.

ii. **Strong Privacy:** Offers strong data confidentiality when using modern encryption algorithms (e.g., AES).

b. **Disadvantage**

i. **No Non-Repudiation:** Since the same key is shared by both parties, it's impossible to prove who actually sent the message.

ii. **Poor Scalability:** In a network with many users, each pair requires a unique key. This leads to **key explosion**—a large number of keys to generate, distribute, and manage.

iii. **Key Distribution Challenge:** A major limitation is the **secure exchange of the secret key**. If the key is intercepted during distribution, the security of the entire communication is compromised.

Types of Symmetric Algorithm

1. Stream Algorithm: A **stream cipher** encrypts data **one bit or byte at a time**, operating on a continuous stream of plaintext. It typically combines the plaintext with a **pseudo-random keystream** using XOR operations.

   Characteristics:

   - ✅ **Very fast and efficient** for real-time processing
   - ❌ **Less secure** than block ciphers if the keystream is reused
   - ✅ Ideal for **real-time communication** (e.g., audio/video streaming)
   - **RC4** – A well-known stream cipher

   > RC4 was widely used in wireless communications (e.g., WEP/WPA), but is now considered deprecated due to security flaws.

2. Block Cipher: A block cipher encrypts data in **fixed-size blocks** (commonly `64-bit or 128-bit`). Each block of plaintext is transformed into a block of ciphertext using a **symmetric key** and a **deterministic algorithm**.

The data is divided into chunks (blocks), and each block goes through a series of complex mathematical functions—often involving **substitution boxes (S-boxes)**—to ensure strong encryption.

Characteristics:

- ⏳ **Generally slower** than stream ciphers, but highly optimized for secure data encryption
- 🔒 Provides **stronger security** when implemented with proper modes of operation

> **Use Cases:**
>
> i. File encryption
>
> ii. Database and disk storage encryption
>
> iii. Secure email and document protection

2. **Asymmetric Cryptography:** Asymmetric cryptography (also known as **public-key cryptography**) is a type of encryption that uses a **pair of keys**: a **public key** and a **private key**.

   These keys are **mathematically related**, but not identical. Data encrypted with one key can only be decrypted with the other.

   Key Concepts:

   - 🔓 **Public Key:** Shared openly and can be used by anyone to encrypt data or verify a digital signature.
   - 🔐 **Private Key:** Kept **secret** by the owner and used to decrypt data encrypted with the corresponding public key or to create digital signatures.

   > Security relies on keeping the private key confidential. Even if the public key is widely available, the encrypted data remains secure unless the private key is compromised.

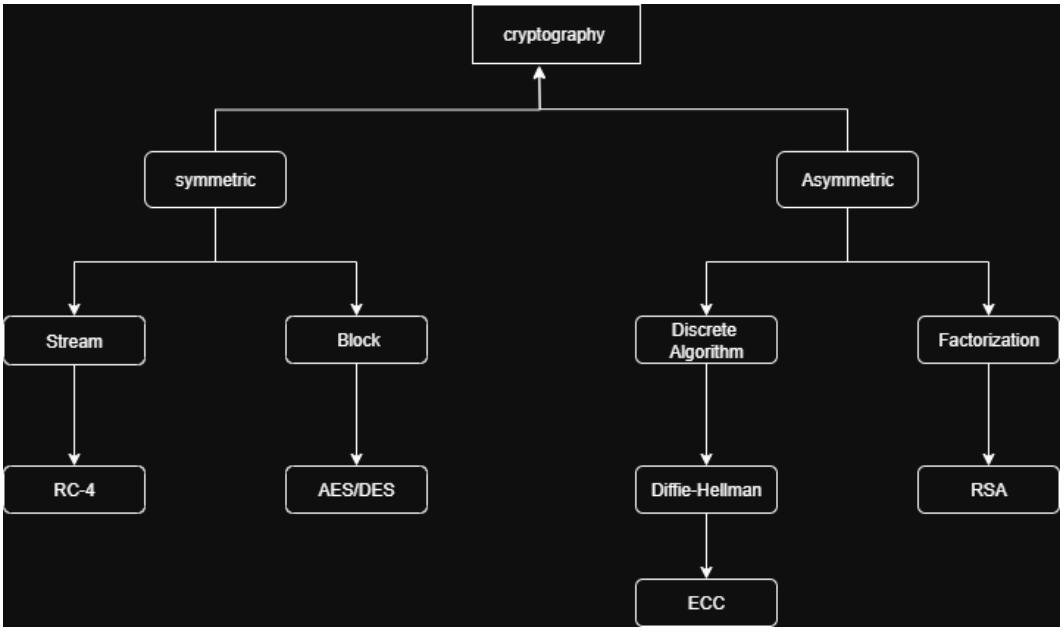
Hashing (Cryptographic Hash Function)

A **hash algorithm** is a one-way cryptographic function that takes an input (message) and returns a **fixed-size string of characters** called a **hash value** or **message digest**.

- The output is unique to the input (small changes in input drastically change the hash).
- Hashing is used for **data integrity verification**, **password storage**, and **digital signatures**.

Common Hash Algorithm

- **MD5 (Message Digest 5):**
  - Produces a **128-bit** hash value
  - **Very fast**, but vulnerable to **collision attacks**
  - Considered **insecure** and not recommended for cryptographic use
- **SHA-1 (Secure Hash Algorithm 1):**
  - Produces a **160-bit** hash value
  - More secure than MD5, but still **vulnerable to collisions**
  - Deprecated for most security applications
- **SHA-2 (Secure Hash Algorithm 2):**
  - Includes **SHA-224**, **SHA-256**, **SHA-384**, and **SHA-512**
  - Produces hash values of **224, 256, 384, and 512 bits** respectively
  - **SHA-256** and **SHA-512** are widely used and considered **secure**



3. **Hybrid Cryptography:** Hybrid Cryptography combines the strengths of both symmetric and asymmetric cryptography to provide efficient, secure communication.
    - **Asymmetric cryptography** is used to securely exchange or encrypt the **symmetric key.**
    - **Symmetric cryptography** is then used for **fast and efficient encryption** of the actual data.

Cryptographic Trust Services

- **Non-Repudiation**

  Non-Repudiation is a security measure that ensure someone cannot deny sending a message or signing a document. It's often achieved using a digital signature and timestamps, making it crucial for verifying the authenticity of digital communication and transactions.

- **PKI (Public Key infrastructure)**

  It is a framework that enables secure communication, authentication, and data integrity in digital environments. It uses a pair of cryptographic keys, consisting of **public-key** and a **private-key** to manage encryption and decryption.

- **Digital Certificate**

A **Digital Certificate** is an **electronic document** that uses a **digital signature** to link a **public key** with the identity of its owner (such as a person, device, or organization).

- It confirms that the public key belongs to the named entity.
- Issued by a trusted authority called a **Certificate Authority (CA)**.
- Used in **secure communications**, such as HTTPS and email encryption.

Protocols and Ports

1. FTP (File Transfer Protocol)

Ports: 20 (Data), 21 (Control)

- FTP is a **standard network protocol** used to **transfer files** between computers over a TCP/IP network.
- Based on a **client-server architecture**.
- **Not secure by default** — credentials and data are sent in plaintext.
- Can be made secure using:
  - **FTPS** (FTP Secure - via SSL/TLS)
  - **SFTP** (SSH File Transfer Protocol - via SSH)

How to Connect to FTP from Kali Linux

```
ftp <target_ip>
```

- **Anonymous Login (if allowed):**

```
ftp anonymous@<target_ip>
```

⚠️ Anonymous login only works if the server allows it (usually with default or no password).

---

2. SSH (Secure Shell)

Port: 22

- SSH is a **secure protocol** used to access and manage devices over **untrusted networks** (like the internet).
- Supports **remote command-line access** and **secure execution** of commands.
- Works on a **client-server architecture**.
- Data is **encrypted**, ensuring confidentiality and integrity.
- `scp` (Secure Copy) is used to **securely transfer files** between systems using SSH.

How to Connect via SSH

```
ssh username@IP
```

> Example: `ssh root@192.168.1.10`

---

3. Telnet

Port: 23

Stands for: *Teletype Network*

- One of the earliest Internet protocols for remote communication.
- Used to **remotely access devices** over a network (LAN or Internet).
- **Not secure** – transmits data, including passwords, in **plain text**.
- Operates over **TCP port 23**.
- Mostly replaced by **SSH** in modern systems due to security concerns.
- Useful in **legacy systems** or simple lab environments

How to Connect via Telnet

```
telnet <IP>
```

---

4. SMTP (Simple Mail Transfer Protocol)

Ports:

- `25` – Default port (commonly used between mail servers).

- `465` – SMTP over SSL (secure).
- `587` – SMTP with STARTTLS (secure and widely used today).
- Protocol used to **send emails** between mail clients and servers.
- Operates over **TCP** and functions at the **Application Layer**.
- Commonly used by **email servers** and **mail transfer agents (MTAs)**.
- **Does not** retrieve emails (that's handled by POP3 or IMAP).

---

5. DNS (Domain Name Service)

Port: `53` (TCP/UDP)

- DNS is the **"phonebook of the internet"** – it translates **human-readable domain names** (like `example.com`) into **IP addresses** that computers use to identify each other.
- Used by computers, services, and resources connected to the internet or private networks.
- Essential for accessing websites, sending emails, and other online services.
- Uses **UDP** for regular queries and **TCP** for larger data transfers like zone transfers.

---

6. DHCP (Dynamic Host Configuration Protocol)

Ports: `67` (Server), `68` (Client)

Layer: Application Layer

- DHCP is a **network management protocol** used to automatically assign **IP addresses** and **network configuration settings** (like subnet mask, gateway, DNS) to devices on a network.
- Eliminates the need for **manual IP configuration**.
- Ensures devices can **join a network and communicate** without user intervention.
- Commonly used in home routers, enterprise networks, and Wi-Fi systems.

---

7. HTTP (Hypertext Transfer Protocol)

Port: `80`

Protocol Type: TCP

Layer: Application Layer

- **HTTP** is an **application-layer protocol** used for transmitting hypermedia documents, such as HTML.
- It is the **foundation of communication on the World Wide Web (WWW)**.
- Operates on a **client-server model**: clients (like web browsers) send requests, and servers return responses (e.g., web pages, files).
- It is **stateless and unencrypted**, meaning each request is independent and data can be intercepted in transit.
- Enhancements like **HTTPS (on port 443)** add encryption for secure communication.

---

8. POP3 (Post Office Protocol 3)

Ports: `110` (POP3) / `995` (POP3S – POP3 over SSL)

Layer: Application Layer

Protocol Type: TCP

- POP3 is an **email retrieval protocol** used by client applications to **download emails** from a mail server.
- Once downloaded, **emails are typically deleted from the server**, meaning they are stored **locally** on the client device.
- Useful for **offline email access**, but **not ideal for syncing across multiple devices**.
- **POP3S** adds encryption via SSL/TLS for secure email retrieval.

---

9. NTP (Network Time Protocol)

Port: `123`

Layer: Application Layer

Protocol Type: UDP

- NTP is used to **synchronize the time** across devices in a computer network.

- Ensures **accurate timestamps**, which are crucial for **logging, security protocols (like Kerberos)**, and system operations.
- Helps maintain **time consistency** across servers, workstations, and network devices.
- NTP can adjust the system clock in milliseconds or even microseconds.

---

10. IMAP (Internet Mail Application Protocol)

Port: `143` (or `993` for IMAPS — IMAP over SSL)

Layer: Application Layer

Protocol Type: TCP

- IMAP is used for **advanced email synchronization** between a mail client and the mail server.
- Unlike POP3, IMAP **keeps the original emails on the server**, allowing access from multiple devices.
- Supports features like **folder management**, **search**, and **real-time updates**.
- Ideal for users who want to access their mail from various devices (PC, phone, webmail).

---

11. LDAP (Lightweight Directory Access Protocol)

Ports: `389` (LDAP), `636` (LDAPS – Secure LDAP)

Layer: Application Layer

Protocol Type: TCP

- LDAP is used to **access and manage directory information services** over a network.
- Follows a **hierarchical structure**, like a tree, to store data such as **usernames, passwords, email addresses, and devices**.
- Commonly used in **centralized authentication systems** like Microsoft Active Directory.
- Enables efficient **searching, querying, and modification** of directory entries.

---

12. RADIUS (Remote Authentication Dial-In-User Services)

Ports: `1812` (Authentication), `1813` (Accounting)

Layer: Application Layer

Protocol Type: UDP

- RADIUS provides **centralized Authentication, Authorization, and Accounting (AAA)** for users who connect to a network.
- Commonly used in **VPNs, Wi-Fi networks, and dial-up access**.
- Ensures that only **authorized users or devices** can connect.
- Works between a **NAS (Network Access Server)** and a **RADIUS server**.

> 🔐 Example Use Case: When connecting to enterprise Wi-Fi, RADIUS checks user credentials before granting access.

---

13. RDP (Remote Desktop Protocol)

Port: 3389

Layer: Application Layer

Protocol Type: TCP (also supports UDP)

- RDP allows a user to **remotely access** and control another computer with a **graphical interface**.
- Developed by Microsoft, commonly used for **remote administration and troubleshooting** on Windows systems.
- Supports features like **clipboard sharing**, **file transfer**, and **audio redirection**.
- **Encrypted communication** for security (uses TLS by default).

> 🖥️ Example: IT admins use RDP to manage remote Windows servers or assist users without being physically present.

Secure Network Design

1. **Hub (Layer 1 – Physical Layer)**

- A **basic networking device** that transmits incoming data packets to **all ports**, regardless of the destination.
- Operates at **Layer 1 (Physical Layer)** of the OSI model.
- It does **not filter** data or check MAC addresses—just broadcasts everything.
- **Network Interface Cards (NICs)** on connected devices check each frame to see if it's addressed to them.
- Hubs are **cheap**, but **inefficient and insecure**, as all data is visible to all devices.

> ⚠️ Replaced in modern networks by switches due to lack of intelligence and poor performance.

MAC (Media Access Control)

- A **MAC address** is a **unique hardware identifier** assigned to a device's **network interface card (NIC)**.
- Operates at the **Data Link Layer (Layer 2)** of the OSI model.
- Used to **identify and communicate** with devices on a **local network segment**.
- Typically written in **hexadecimal** format (e.g., `00:1A:2B:3C:4D:5E`).
- **Permanent** (burned into hardware) but can be **spoofed** in some cases.

> 📌 Think of it as the "physical address" of a device on a local network.

---

2. **Switches (Layer 2) of OSI model**
   - A **Layer 2 device** that uses **MAC addresses** to forward data to the correct destination.
   - Unlike hubs, switches **send data only to the intended recipient**, not all devices.
   - Helps reduce network congestion by creating **separate collision domains** for each connected device.

- Commonly used in **modern LANs** for efficient and secure communication.

> 📌 Think of a switch as a smart traffic director that knows exactly where each device is on the network.

3. **Routers (Layer 3) of OSI model**
   - A **Layer 3 device** that connects and routes traffic between **different networks**.
   - Uses **IP addresses** to determine the best path for data packets.
   - **Isolates broadcast traffic**, preventing it from spreading between networks.
   - Essential for communication across the internet and large networks.
   - **Drawback**: Routers are generally **more expensive** than switches or hubs.

> 📌 Think of a router as a network manager that decides where data should go based on IP addresses.

4. **VLANs (Virtual Local Area Networks)**
   - VLANs are used to **logically segment** a network, even if devices are physically connected to the same switch.
   - Commonly implemented on **Layer 3 switches**, offering routing-like features at a **lower cost** and with **simpler configuration**.
   - Help in **improving security**, **reducing broadcast traffic**, and **organizing** networks efficiently.
   - Nowadays, **routers are primarily used for WAN connectivity**, while VLANs handle internal segmentation.

> 📌 Think of VLANs as virtual rooms inside your network, keeping traffic organized and separate.

5. **NAT (Network Address Translation)**

- **NAT** is a technique used to **translate private IP addresses** (used inside a network) into a **public IP address** (used on the internet), and vice versa.
- It **modifies IP address information** in the packet header while it passes through a router or firewall.
- Commonly used in **home and office networks** to allow multiple devices to share a single public IP.

> 📌 Example: Your phone, laptop, and TV at home all access the internet using one public IP — that's NAT in action.

NAT hides private/internal IP addresses by translating them to a public IP, making internal devices invisible to the internet.

6. **PAT (Port Address Translation)**

   Also known as **NAT Overload**, PAT is a specific type of **Dynamic NAT** that allows **multiple devices** on a local network to share a **single public IP address**.

   - Each device is mapped using a **different port number** for each session.
   - This enables many internal devices to access the internet **simultaneously** using one IP.

   ✅ **Example**:

   If 3 devices are browsing the internet at the same time, PAT ensures they all appear to come from the same public IP, but with **unique port numbers**, like:

   ```
   PublicIP:4501 → Device1
   PublicIP:4502 → Device2
   PublicIP:4503 → Device3
   ```

Firewall

A firewall is a network security device or software designed to monitor and control incoming and outgoing network traffic based on predetermined security

rules.

It’s primary purpose is to establish a barrier between a trusted internal network and untrusted external network. Its main purpose is to **block unauthorized access** while allowing safe, legitimate communication.

✅ Firewalls can be **hardware-based**, **software-based**, or a **combination of both**.

Types of Firewalls

1. **Packet-Filtering Firewall (a.k.a. Stateless Firewall)**
    - Works at **Network Layer (Layer 3)** of the OSI model.
    - Checks each **incoming and outgoing packet** against a set of rules (e.g., IP address, port number, protocol).
    - **Does not inspect the content** of the packet.
    - ✅ **Fast** but limited in **security features**.

    > Example: Early firewalls built into routers.

---

2. **Stateful Inspection Firewall**
    - Works at **Network and Transport Layers (Layer 3 & 4)**.
    - Tracks the **state of active connections** and decides whether to allow or block traffic based on connection context.
    - **More secure** than packet-filtering.

    > Example: Monitors if a packet is part of an established session.

---

3. **Application-Level Firewall (Proxy Firewall)**
    - Works at the **Application Layer (Layer 7)**.
    - Filters traffic based on **specific applications or services** (like HTTP, FTP).
    - Acts as a **proxy** between users and the service — hides internal IPs.
    - ✅ Offers **deep inspection** of content.

- ❌ Slower due to detailed filtering.

> Example: Web proxy filtering social media access.

4. **Next-Generation Firewall (NGFW)**
   - Combines **stateful inspection** with advanced features like:
     - **Deep packet inspection (DPI)**
     - **Intrusion prevention (IPS)**
     - **Application awareness**
     - **TLS/SSL inspection**
   - Provides **layered protection** against modern threats.

> Used in modern enterprise environments.

5. **Cloud-Based Firewall (Firewall as a Service - FWaaS)**
   - Hosted on the **cloud**, not on-premises.
   - Scales easily with large or distributed networks.
   - Ideal for **remote or hybrid teams**.

🛡️ Forward & Reverse Proxies

1. **Forward Proxy**

- Acts on behalf of internal clients.
- Used to access external resources (like the internet).
- Can be used for content filtering, anonymity, or access control.
- Example use: A company proxy server filtering employee internet access.

2. **Reverse Proxy**

- Acts on behalf of internal servers.
- Handles requests from external clients and forwards them to internal servers.
- Commonly used for load balancing, caching, SSL termination, and hiding internal server details.

- Example use: A reverse proxy like Nginx routing traffic to multiple backend web servers.

IDS & IPS

🔍 **Intrusion Detection System (IDS)**

- A **passive** security monitoring tool.
- Primarily used to:
  - **Detect** suspicious or malicious activity.
  - **Log** network or system events for analysis.
  - **Alert** administrators about potential threats.
- Does **not** block or stop attacks directly.

🚫 Intrusion Prevention System (IPS)

- An **active** security tool that can **prevent** attacks in real time.
- Capable of:
  - Sending **TCP reset** packets to terminate malicious connections.
  - **Reconfiguring firewalls** to block IPs or ports.
  - Automatically **dropping packets** that match known attack signatures.

IDS Categories

1. 🖥️ HIDS (Host-Based Intrusion Detection System)
   - A **security system** that monitors and analyzes activity on a **single host** (computer or server).
   - It examines the system's internal behavior, including:
     - **System log files** and **audit records**
     - **Application logs**
     - **Usage of specific programs**
     - **CPU and memory usage**
     - **Incoming and outgoing network traffic**

✅ HIDS is useful for detecting insider threats, malware, or unauthorized changes on individual systems.

2. 🌐 NIDS (Network-Based Intrusion Detection System)
   - A **security system** that monitors **entire network traffic** to detect suspicious or malicious activity.
   - Works like a **sniffer** (packet capture) combined with an **analysis engine**.
   - Key features:
     - Monitors network segments in real time.
     - Easier to deploy across large networks.
     - Scalable for enterprise environments.
     - Detects **network-based attacks**, such as port scans, DDoS, and packet anomalies.

   ✅ NIDS complements Host-Based IDS by providing broader network visibility.

🎯 Honeypots (Decoy Systems)

A **honeypot** is a **security mechanism** that acts as a **decoy system or network** to lure attackers.

- Designed to appear as a **legitimate target**, like a server or service.
- Purpose:
  - **Detect and analyze** attack methods.
  - **Distract attackers** from real systems.
  - Gather intelligence on malicious behavior.
- Often used in **research**, **threat hunting**, and **intrusion detection**.

> Think of it as a trap set up to study and catch intruders without risking real systems.

🔐 VPN (Virtual Private Network)

A **VPN** is a technology that creates a **secure, encrypted tunnel** over an insecure or public network (like the internet).

- Ensures **privacy** and **data security** during online communication.
- **Hides your IP address**, masking your online identity.
- Enables **secure remote access** to private networks (e.g., office systems).
- Commonly used in **corporate environments**, **cybersecurity**, and for **personal online anonymity**.

> Think of it as a private tunnel through a public road.

🛠️ Tunneling (in VPNs)

Tunneling is a key function of VPNs where **one network protocol is encapsulated inside another**.

- Creates a **virtual pathway** (or tunnel) between two systems.
- **Encrypts** and **authenticates** data for secure communication.
- Allows transmission of **non-routable** or **private IP addresses** across public networks.
- Helps in **bypassing restrictions** or accessing internal resources remotely.

> Imagine mailing a sealed box inside another sealed box — only the receiver knows how to open both.

📶 Bluetooth

Bluetooth is a short-range **Personal Area Network (PAN)** protocol that allows wireless communication between devices, eliminating the need for physical cables.

Features

- **Bluetooth Modes:** Defines how devices operate (Active, Sniff, Park, etc.)
- **Discovery Modes:** Controls visibility to other Bluetooth devices.
- **Automatic Pairing:** Devices can connect without manual PIN entry in some configurations.

Common Bluetooth Attacks

1. **Bluejacking**
   - Sending **unsolicited messages** (spam) to nearby Bluetooth-enabled devices.
   - Harmless but annoying.
2. **Bluesnarfing**
   - **Unauthorized access** to information (contacts, calendar, messages).
   - Exploits misconfigured or open Bluetooth connections.
3. **Bluebugging**
   - **Most severe** form of attack.
   - Allows attackers to take **full control** of a device.
     - Make calls
     - Listen to calls (eavesdropping)
     - Access messages, contacts, etc.

Kerberos

- **Kerberos** is a secure network authentication protocol developed as part of **MIT's Project Athena**.
- It is widely used in **Windows (2000 and later)** and **some Unix/Linux environments**.
- Designed to provide strong authentication in **untrusted networks**.

🧩 Key Features:

- **Single Sign-On (SSO):** Users authenticate once and gain access to multiple services without re-entering credentials.
- **No Password Transmission:** Passwords are never sent over the network.
- **Symmetric Encryption:** Uses secret-key cryptography (typically AES) to verify identity.

- **Protection Against Replay Attacks:** Uses **timestamps** and **tickets** to prevent reuse of captured authentication data.

🛑 Indicators of Compromise (IOCs)

IOCs are signs or evidence that a system or network may have been breached or is under attack.

🔍 Examples of IOCs:

- Multiple user accounts getting locked out at the same time.
- A sudden surge in **invalid login attempts** in logs.
- **Unusual network traffic** patterns, especially to unknown IPs.
- **Privilege accounts** being created or accessed at odd hours.
- Detection of **malware files**, unexpected scripts, or unauthorized tools on endpoints.

> Security teams monitor IOCs to detect, investigate, and respond to potential threats quickly.

⚔️ Indicator of Attack (IOA)

IOA refers to evidence that shows an **attacker's intent, behavior, or activity** during an ongoing attack — **before** or **without** confirming damage or compromise.

🔍 Key Characteristics:

- Focuses on **what the attacker is doing**, not just what they've done.
- Helps in detecting **real-time** attacks or threats.
- Often used for **proactive detection** and **prevention**.

🧠 Example Behaviors:

- Use of **PowerShell** or scripting tools for suspicious automation.
- Attempting to **escalate privileges**.
- Trying to **disable antivirus** or security tools.
- **Lateral movement** between systems inside a network.

- Scanning ports or fingerprinting systems inside the network.

> While IOCs point to a system that's already affected, IOAs help stop attacks while they're in progress.

Metadata

- **Metadata** means *"data about data"* — it provides **contextual information** about a file, message, or digital content.
- It **doesn't contain the actual content**, but describes **properties** like:
  - **Who** created it
  - **When** it was created or modified
  - **Where** (location, IP, device info)
  - **What type** of file or data it is

Examples of Metadata:

- **Email:**
  - Sender, recipient, timestamp, subject, email server IP
- **Mobile:**
  - Call logs, SMS headers, app usage history, GPS location
- **Web:**
  - Browsing history, cookies, IP addresses, device type
- **File:**
  - File name, size, creation/modification dates, author, software used

> 🔐 Note: Metadata is often used in digital forensics and surveillance to trace actions or verify authenticity.

🔗 Cyber Kill Chain

The **Cyber Kill Chain**, developed by Lockheed Martin, is a **framework** that outlines the steps attackers take to compromise and exploit targets.

Understanding each phase helps defenders detect and respond effectively.

1. Reconnaissance

- The attacker selects a target, conducts research, and gathers information to identify vulnerabilities.
- This includes:
  - Scanning public info (websites, social media)
  - Using tools like **whois**, **nslookup**, **shodan**, **Google Dorking** etc.
  - Passive or active information gathering

2. Weaponization

- The attacker creates or customizes a **malware payload** (e.g., trojan, backdoor) to exploit the vulnerability discovered during **reconnaissance**.
- This step often includes:
  - Pairing malware with a **delivery method** (e.g., malicious PDF or Word doc)
  - Preparing tools for **exploitation** without direct contact with the target

3. Delivery

- The attacker delivers the malicious payload to the target system using various methods, such as:
  - **Email attachments** (phishing)
  - **Malicious websites**
  - **Removable media** (USB drives)
  - **Drive-by downloads**
- This is the **first direct interaction** with the target environment.

4. Exploitation

- The delivered malicious code is **triggered** on the target system.
- It **exploits one or more vulnerabilities** (e.g., software bugs, misconfigurations, or zero-days).

- This stage results in **initial compromise** of the host, allowing further attacker control.
- Common examples:
  - Buffer overflow
  - Remote code execution (RCE)
  - Privilege escalation

5. Installation

- The attacker installs **malware** or a **backdoor** to maintain persistent access to the compromised system.
- This stage ensures the attacker can **regain access later**, even if the system reboots or the initial exploit is patched.
- Common installation methods include:
  - Dropping a **Trojan** or **rootkit**
  - Installing **Remote Access Trojans (RATs)**
  - Creating **new services or scheduled tasks**

6. Command & Control (C2)

- The compromised system opens a **communication channel** with the attacker's system to receive instructions.
- This channel allows **persistent, remote control**, often referred to as "**hands-on-the-keyboard**" access.
- C2 communication can be:
  - **Encrypted** or disguised to avoid detection
  - Over common protocols (HTTP, HTTPS, DNS)
- At this stage, the attacker can:
  - Move laterally
  - Exfiltrate data
  - Deploy further payloads

7. Actions on Objectives

- The attacker **executes their final goal** after gaining persistent access.
- This goal can vary depending on the intent, such as:
  - **Data exfiltration** (stealing sensitive information)
  - **Data destruction** (wiping systems or files)
  - **Ransomware deployment** (encrypting data to demand payment)
  - **Service disruption** (causing downtime or denial-of-service)
- At this point, the attacker may also **cover their tracks** to avoid detection.

Information Security Risk Management (ISRM)

Information Security Risk Management (ISRM) is the structured process of identifying, assessing, and mitigating risks related to the use of information systems and technology.

- It helps protect the **Confidentiality, Integrity, and Availability (CIA)** of an organization's assets.
- ISRM is an ongoing process that aligns cybersecurity practices with **business goals and risk tolerance**.

Key Steps:

1. **Identify** risks (e.g., data breaches, unauthorized access, malware).
2. **Assess** the likelihood and impact of these risks.
3. **Treat or Mitigate** risks using controls (technical, administrative, or physical).
4. **Monitor** and **review** risks continuously.

Risk Definitions

1. **Asset**: Anything of value to the organization.
2. **Vulnerability**: A weakness or absence of a safeguard that could be exploited.
3. **Threat**: A potential cause of an unwanted impact or loss to an asset.
4. **Threat Agent**: The entity (e.g., person, software, or group) that carries out the threat.

5. **Exploit**: A specific instance where a vulnerability is used to compromise a system.
6. **Risk**: The likelihood of a threat exploiting a vulnerability and the resulting impact.
7. **Controls**: Measures used to protect assets. These can be:
    - **Physical** (e.g., locks, guards)
    - **Administrative** (e.g., policies, training)
    - **Technical** (e.g., firewalls, encryption)
    - Subtypes:
        - **Safeguard**: A preventive or deterrent measure.
        - **Countermeasure**: A detective or corrective measure.
8. **Total Risk**: The risk that exists before any controls or safeguards are applied.
9. **Residual Risk**: The remaining risk after implementing controls.
10. **Secondary Risk**: A new risk that arises as a result of addressing another risk.
    - **Incident**: A risk event that has actually occurred.