Different types of threats occured by hackers

1. Malware

- **Viruses**: Malicious code that attaches itself to legitimate software and spreads to other systems. It can corrupt files, steal data, or damage the system.
- **Worms**: Standalone malicious programs that replicate themselves and spread across networks without needing a host file. They can consume bandwidth and cause network congestion.
- **Trojans**: Malware disguised as legitimate software. Once installed, it can provide unauthorized access to the hacker, steal information, or perform other malicious actions.
- **Ransomware**: A type of malware that encrypts the victim's data and demands a ransom for decryption. Notable examples include WannaCry and REvil.
- **Spyware**: Malware designed to spy on the victim's activities, such as keystrokes, screen captures, or data exfiltration.

2. Phishing

- **Email Phishing**: Hackers send fraudulent emails pretending to be from a legitimate source to trick recipients into providing sensitive information, such as passwords or credit card details.
- **Spear Phishing**: A targeted form of phishing where hackers personalize the attack to a specific individual or organization, making it more convincing.
- **Whaling**: A type of spear phishing targeting high-profile individuals, such as executives, with the intent of stealing sensitive corporate information.
- **Smishing and Vishing**: Phishing attacks conducted via SMS (smishing) or voice calls (vishing) to trick victims into divulging personal information.

3. Man-in-the-Middle (MitM) Attacks

- **Eavesdropping**: Hackers intercept and listen to communication between two parties to steal sensitive information.
- **Session Hijacking**: An attacker takes control of a user's session by stealing session cookies, enabling them to act as the legitimate user.
- **SSL Stripping**: Downgrading a secure HTTPS connection to an insecure HTTP connection, making it easier for the hacker to intercept and manipulate data.

4. Denial of Service (DoS) and Distributed Denial of Service (DDoS)

- **DoS**: Overwhelming a system or network with excessive requests or data, causing it to crash or become unavailable to legitimate users.
- **DDoS**: Similar to DoS but launched from multiple compromised systems (often part of a botnet), making it harder to defend against.

5. SQL Injection

- Hackers exploit vulnerabilities in web applications to inject malicious SQL queries, enabling them to access, modify, or delete data from the database.

6. Cross-Site Scripting (XSS)

- Attackers inject malicious scripts into web pages viewed by other users. These scripts can steal session cookies, redirect users to malicious websites, or perform other unauthorized actions.

7. Credential Stuffing

- Hackers use stolen username and password combinations, often obtained from data breaches, to gain unauthorized access to accounts on different websites where users might reuse the same credentials.

8. Social Engineering

- **Baiting**: Using enticing offers or promises (like free software) to trick users into downloading malware or revealing sensitive information.
- **Pretexting**: Creating a fabricated scenario to trick the victim into divulging information or performing an action.
- **Quid Pro Quo**: Offering something in return for information, such as free tech support in exchange for login credentials.

9. Advanced Persistent Threats (APTs)

- Highly skilled and organized groups of hackers, often state-sponsored, who gain unauthorized access to a network and remain undetected for an extended period. Their goal is to steal sensitive data, disrupt operations, or conduct espionage.

10. Zero-Day Exploits

- Attacks that exploit previously unknown vulnerabilities in software or hardware before the vendor has issued a patch. These are particularly dangerous because there is no immediate defense against them.

11. Insider Threats

- Malicious insiders, such as disgruntled employees or contractors, who have authorized access to the system and misuse it to steal data, sabotage operations, or leak sensitive information.

12. Cryptojacking

- Hackers secretly use the victim's computing resources to mine cryptocurrency without their knowledge. This can slow down the victim's system and increase electricity costs.

13. Rootkits

- Malicious software designed to hide the existence of certain processes or programs from normal methods of detection, allowing the hacker to maintain privileged access to the system.

14. Brute Force Attacks

- Hackers attempt to gain access to accounts by systematically trying all possible combinations of passwords or encryption keys until the correct one is found.

15. Data Breaches

- Unauthorized access to confidential data, such as personal information, financial records, or intellectual property. Data breaches can result from hacking, social engineering, or poor security practices.

16. Botnets

- Networks of compromised computers (bots) controlled by a hacker. Botnets are often used to conduct large-scale attacks like DDoS, send spam, or distribute malware.

17. Exploit Kits

- Toolkits that automate the process of exploiting vulnerabilities in systems or applications. They are often used to deliver malware to unsuspecting users visiting compromised websites.

18. Rogue Software

- Fake or malicious software that pretends to be legitimate but is designed to steal information, install additional malware, or take control of the victim's system.