Unit 1

Attacker Techniques and Motivation:

- Attackers employ various techniques, such as malware, social engineering, and phishing, to compromise systems.
- Their motivations include financial gain, hacktivism, espionage, and personal satisfaction.

How Hackers Cover Their Tracks:

- Attackers use techniques like cleaning logs, using proxies, and employing encryption to hide their activities.
- They may also attempt to erase or alter their digital footprint.

Fraud Techniques:

- Fraud can take various forms, such as identity theft, credit card fraud, and phishing schemes.
- Attackers often aim to steal sensitive information for financial gain.

Threat Infrastructure:

- Threat infrastructure refers to the tools, servers, and networks that attackers use to orchestrate cyberattacks.
- It may involve the use of botnets, command and control servers, and anonymizing services.

Exploitation Techniques:

- Attackers exploit vulnerabilities in software or hardware to gain unauthorized access to systems.
- Common exploits include zero-day vulnerabilities and SQL injection attacks.

Techniques to Gain a Foothold:

- Attackers use tactics like spear-phishing, password cracking, and backdoors to establish a foothold in a target system.
- Once inside, they can further their attack.

Misdirection:

- Misdirection involves diverting attention away from the real attack vector.
- Attackers may launch decoy attacks or create false alerts to confuse defenders.

Reconnaissance:

- Reconnaissance is the process of gathering information about a target system.
- Attackers use tools and methods like port scanning, open-source intelligence, and social engineering to gather data.

Disruption Methods:

- Attackers may disrupt systems and networks using distributed denial of service (DDoS) attacks.
- This can result in service outages and financial losses.

Cyber Attacks and Threats

Attacker Techniques and Motivation

- Attackers employ a variety of techniques to compromise computer systems, including malware, social engineering, and phishing.
- Their motivations can range from financial gain, hacktivism, and espionage to personal satisfaction and notoriety.
- The choice of technique and motivation may vary depending on the attacker's goals and values.

How Hackers Cover Their Tracks

- Attackers often try to conceal their activities by various means, including cleaning logs, using proxies or VPNs, and encrypting their communications.
- They may attempt to erase or alter their digital footprint, making it difficult for investigators to trace their actions.
- Effective track-covering is essential for maintaining anonymity and avoiding prosecution.

Fraud Techniques

- Fraud encompasses a broad spectrum of activities, such as identity theft, credit card fraud, and phishing schemes.
- Attackers use fraudulent methods to obtain sensitive information, which can lead to financial gain at the victim's expense.
- Phishing, for example, involves tricking individuals into revealing personal and financial information through deceptive emails or websites.

Threat Infrastructure

- Threat infrastructure refers to the collection of tools, servers, and networks that attackers use to orchestrate and control their cyberattacks.
- Components of threat infrastructure can include botnets, command and control (C&C) servers, and anonymizing services like Tor.
- This infrastructure provides attackers with the necessary resources to coordinate their efforts and maintain operational security.

Exploitation Techniques

- Attackers exploit vulnerabilities in software or hardware to gain unauthorized access to systems.
- Zero-day vulnerabilities, which are unknown to the vendor and, therefore, unpatched, can be highly valuable to attackers.
- SQL injection attacks, a type of exploitation, manipulate a web application's database by injecting malicious SQL code into user input fields.

Techniques to Gain a Foothold

- Attackers employ a range of tactics to establish a foothold in a target system.
- Spear-phishing is a highly targeted form of phishing, often personalized to deceive a specific individual.

- Password cracking involves attempting to discover passwords through brute-force methods or dictionary attacks.
- Backdoors are hidden entry points that allow attackers to maintain access to a compromised system.

Misdirection

- Misdirection involves diverting attention away from the actual attack vector, making it harder for defenders to detect and respond.
- Decoy attacks may be launched to draw security resources away from the primary target.
- False alerts or red herrings can confuse investigators and waste their time on non-critical issues.

Reconnaissance

- Reconnaissance is the process of gathering information about a target system or organization.
- Attackers use a variety of tools and methods, such as port scanning, to identify weaknesses and potential entry points.
- Open-source intelligence (OSINT) refers to publicly available information, including social media profiles and company websites, which can aid attackers in gathering valuable data.

Disruption Methods

- Attackers may use distributed denial of service (DDoS) attacks to disrupt systems and networks.
- DDoS attacks overwhelm a target's resources with a flood of traffic, causing service outages and financial losses.
- Attackers may employ DDoS attacks as a smokescreen to hide other, more nefarious activities.