



Vulnerabilities, Threat Vectors and Different Kinds of Attacks



Lecture – Housekeeping

- ❑ The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- ❑ No question is daft or silly - **ask them!**
- ❑ There are Q/A sessions midway and at the end of the session, should you wish to ask any follow-up questions.
- ❑ You can also submit questions here:
hyperiondev.com/sbc4-cs-questions
- ❑ For all non-academic questions, please submit a query:
www.hyperiondev.com/support
- ❑ Report a safeguarding incident:
hyperiondev.com/safeguardreporting
- ❑ We would love your feedback on lectures:
<https://hyperiondev.wufoo.com/forms/zsgv4m40ui4i0g/>

Previously:

- Recapped on Web Security









Objectives

- Define Vulnerability
- Differentiate between known and unknown Vulnerabilities
- Explore Threat Vectors, Types of attacks and vulnerabilities
- Overview of Defense Mechanisms and Detecting + Response

Introduction to Vulnerabilities

- A vulnerability is a weak point or flaw in the implementation or design of a system that can be used to compromise its security.
- Older software, incorrectly configured servers, sloppy, passwords, and unpatched systems are a few examples of vulnerabilities.
- Maintaining a secure system requires careful management of vulnerabilities.
- Hyperiondev

Known VS Unknown

Known vulnerabilities	Unknown vulnerabilities
 <ul style="list-style-type: none">Have been disclosed to the software vendor or security community	 <ul style="list-style-type: none">Have not been disclosed to the software vendor or security community
 <ul style="list-style-type: none">The NIST National Vulnerability Database (NVD) contains an updated list of known vulnerabilities	 <ul style="list-style-type: none">It's impossible to know how many exist today
 <ul style="list-style-type: none">Each one has a Common Vulnerabilities and Exposures (CVE) number	 <ul style="list-style-type: none">Unknown vulnerabilities are difficult to detect and, consequently, challenging to prevent
 <ul style="list-style-type: none">Software with known vulnerabilities can be fixed immediately with patches	 <ul style="list-style-type: none">These vulnerabilities don't have existing fixes or software patches available

Understanding Threat Vectors

- A threat vector is a way or route that a hacker can use to access a system.
- Social engineering techniques, phishing emails, and malicious websites are examples of common threat vectors.
- Organizations can take action to stop attacks and safeguard their systems by understanding the potential threat vectors.

Understanding Threat Vectors

- **Web applications** have become a top target for attackers due to the growing reliance on web-based applications. Web application flaws can be used to access private information or launch additional attacks.
- **Mobile devices** are a prime target for attackers due to their widespread use and the growing amount of sensitive data they store. Mobile devices are just a few of the targets that attackers can choose from, including malicious apps, network spoofing, and SMS-based attacks.
- As was already mentioned, **social engineering** is a strategy used by attackers to deceive victims into disclosing confidential information. Phishing emails, calls, and even physical attacks like tailgating—following a legitimate person into a secure area—can all be used to commit this crime.

Types of Attacks

- Malware, ransomware, phishing, and denial of service attacks are just a few examples of the various types of cyber attacks.
- Malware is malicious software that has the potential to corrupt systems or steal data.
- A form of malware known as ransomware encrypts a victim's data and demands payment to decrypt it.
- Phishing is a social engineering technique that uses phony emails or websites to deceive people into disclosing personal information.
- A system is overloaded with traffic during a denial of service attack, rendering it unavailable to users.

Types of Attacks

- Attacks known as denial of service (DoS) are attempts to prevent a system from performing as intended by overloading it with traffic or requests. This can be accomplished in a number of ways, such as by flooding the system with traffic, taking advantage of software flaws, or coordinating a massive attack using botnets.
- Man-in-the-middle (MitM) attacks: In this kind of attack, an attacker eavesdrops on a conversation between two parties or modifies the messages that are being sent. This can be accomplished using a variety of methods, including SSL stripping, ARP spoofing, and DNS spoofing.
- Phishing attacks: These attempts are made to convince users to divulge private information, including passwords, credit card numbers, or other sensitive data. Social engineering techniques like making fake login pages, phony emails, and phone calls while posing as a reliable person or organization are frequently used to accomplish this.

Exploiting Vulnerabilities

- Hackers can take advantage of weaknesses in a number of ways, including by using software exploits or brute-forcing passwords.
- When a vulnerability is exploited, the attacker can take over the system and access confidential data.
- Exploits can be carried out manually by knowledgeable hackers or automatically using attack tools.

Exploiting Vulnerabilities

- Hackers exploit vulnerabilities in software, hardware, or system configurations to gain unauthorized access or execute malicious actions.
- Common vulnerabilities include unpatched software, weak passwords, unsecured ports, and social engineering attacks.
- Attackers can use vulnerability scanners and other tools to identify weaknesses in a system.
- They may then use exploit kits or custom code to carry out attacks such as remote code execution, denial of service, or data theft.
- Preventative measures include implementing strong security protocols, regularly updating software and hardware, and conducting vulnerability assessments.
- Intrusion detection and response systems can help identify and respond to attacks in real-time.

Defense Mechanisms

- **Firewalls:** A network defense strategy must include firewalls as a key element. They can be utilized to filter traffic according to different factors like IP address, protocol, or port number.
- **Systems for detecting and preventing intrusions (IDPS):** IDPS are made to watch network traffic and find malicious activity. To stop traffic or warn administrators of potential dangers, they can be used.
- **Data can be protected both while it is in transit and while it is at rest by the use of encryption, which is a strong tool.** Encrypting data ensures that even if a hacker gets their hands on it, they will be unable to decrypt it without the key.

Detecting and Responding to Attacks

- Cybersecurity includes detecting attacks and taking appropriate action.
- Businesses should take precautions to monitor their networks and look for any unusual activity or attempted attacks.
- Additionally, they ought to have prepared incident response plans that specify what should be done in the event of an attack.
- These plans ought to include steps for containing infected systems, eliminating malware, and regaining access to compromised data and systems.
- Plans for responding to breaches should also include ways to reach out to stakeholders and regulatory bodies.
- Response plans can be kept current and effective by conducting regular testing and reviews.

Incident Response - Simplified



Wrapping Up.

- Maintaining a democratic society requires taking precautions against threats and assaults.
- Rule of Law: Keeping a secure environment requires adhering to established security protocols and laws.
- Individual Liberty: Individuals have the right to prevent unauthorized access to and use of their own data and information.
- Mutual Respect and Tolerance: To prevent and address threats, cybersecurity requires respect and cooperation between individuals and organizations.

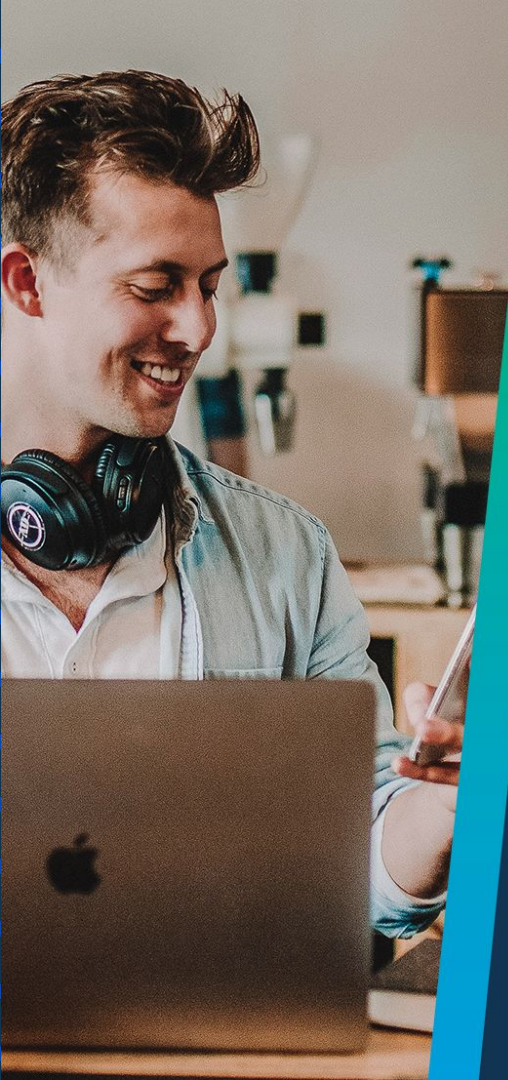
Next up

- Introduction to Ethical Hacking



Questions and Answers





Hyperiondev

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise