Css Notes CS, SILA

Introduction to Cybersecurity

Q. What Is Cybersecurity?

. is Organizational Data?

**Q. Types of Organizational Data**

* **Traditional Data**
* **Internet of Things (IoT)**
* **Big Data**

**Q. The Foundational Principles for protecting Information**

* **Confidentiality**
* **Integrity**
* **Availability**

**Q. The protection of information in each state**

* **Processing**
* **Storage**
* **Transmission**

**Q. What is Security Breach?**

**Q. Consequences of a Security**

* **Potential risks,**
* **Vandalism**
* **Reputation Damage**
* **unauthorized access**
* **data loss,**
* **financial damage,**
* **reputation harm**

**Q. What are cyber Attackers**

**Cyber attackers come in various forms, each with their own methods, motivations, and expertise. Here are some common types:**

* **Hackers**
* **Hacktivist**
* **Phishers**
* **Malware Authors**
* **Insiders**
* **Cybercriminal organization**
* **Cyber welfare units**
* **Non state**
* **Scammers**
* **Script kiddies**

**External Threats: Hackers, Internal Threats:**

* **Employees,**
* **Contractors,**
* **Insiders,**
* **Privileged Users,**
* **Human Error,**
* **Malicious Insiders.**
* **Malware,**
* **Phishing,**
* **DDoS Attacks,**
* **State-Sponsored Actors,**
* **Supply Chain Attacks**

**. Here are some common types of malware:**

* **Virus**
* **Worm**
* **Trojans**
* **Ransomware**
* **Spyware**
* **Adware**
* **Bonnets**
* **rookits**

**State Symptoms of Malware**

* **Unexplained problem with your computer networks**
* **Decrease in web browsing**
* **Slow computer performance**
* **Programs turning off or reconfiguring themselves**
* **Strange changes to files or settings**
* **Unexpected pop-up ads**
* **Frequent crashes or freezes**
* **Corrupted file**
* **Email being sent without your knowledge**

**Examples of Virus Include**

* **Email Attachments**
* **Infected USB Drives(Universal Serial Bus)**
* **Fake software downloads**

**Here are some examples of phishing:**

* **Email Phishing**
* **Social media phishing**
* **SMS/Text message Phishing (smishing)**
* **Voice Phishing**

**Q. Methods of Espionage?**

* **Social Engineering**
* **Insider Threats**
* **Supply Chain Attacks**
* **Malware deployment**
* **Hacking and penetration**
* **Advanced Persistent Threats (APTs):**
* **Network Surveillance and Eavesdropping**
* **Steganography:**

**Here are social, Engineering types:**

* **phishing**
* **pretexting**
* **Reverse social Engineering**
* **Quid Pro Quo**
* **Baiting**
* **Tailgating (or Piggybacking)**
* **Watering Hole Attack**
* **Impersonation:**

**Example of Cyber Warfare:**

* **Targeted Cyber attacks**
* **Propaganda and Disinformation**
* **Cyber Espionage**
* **Denial of Service Attacks**

**Here are some key characteristics of targeted cyber attacks in cyber warfare:**

* **Specific targets**
* **Advanced techniques**
* **Convert operations**
* **Strategic objective**
* **Persistence & adaptation**
* **Geopolitical implication**

Q. What’s a Botnet?

**Q. On-Path Attacks**

**Q. SEO poisoning, or search engine poisoning,?**

**Q. Here's SEO it works:**

**1. Injecting malicious links or contents**

**2. Redirecting users to malicious websites**

**3.manupulating results**

**4. Exploiting Trust in Search Engines**

**Q. Wi-Fi Password Cracking s what in simple words as used in cybersecurity?**

**1. Capturing Wi-Fi Traffic:**

**2. Analyzing Captured Data**

**3. Brute Force or Dictionary**

**4. Exploiting Weaknesses**

**5. Gaining Access:**

**Q. Password cracking methods?**

**1. Guess passwords**

**2. Brute force attacks**

**3. Dictionary Attacks**

**4. Phishing and social Engineering**

**5. Password spraying**

**6. Credential Stuffing**

**7 Traffic injection**

**8. Rainbow attacks**

Q. What does Cracking times mean?

What does Password cracking mean?

What does Access time mean?

What does time detection mean?

**Ways of Reducing cracking times**

1. **Implementation of strong authentication mechanism**
2. **Regular passwords update**
3. **Security awareness training**
4. **Proactive monitoring for suspicious activities**

**Advanced Persistent Threat(APTs)**

* **Advanced-**
* **Persistent-**
* **Threat –**

**Security vulnerabilities and exploits means what?**

**Hardware vulnerabilities refer to?**

**Types of Hardware Vulnerabilities**

1. **Capacitors**
2. **Rowhammer- DRAM**
3. **Meltdown & specture**

**Meltdown primarily affects Intel processors, while Spectre impacts a wider range of processors including those made by Intel, AMD, and ARM**

What is Intel

What is **Advanced Micro Devices (AMD)**

**What is ARM Holdings**

**SOFTWARE VULNERABILITIES???**

**Examples of software vulnerabilities include**

1. Buffer Overflow
2. **SQL (Structured Query Language)**
3. Cross-Site Scripting (XSS)
4. Authentication Bypass**:**
5. Remote Code Execution (RCE)
6. Insecure Cryptography
7. Denial of Service (DoS)

**Software vulnerabilities can be categorized in various ways based on different criteria.**

1. By impact
2. By Type
3. By Attack Vector
4. By source
5. By software Component

BY IMPACT

* Critical
* High
* Medium
* Low

BY TYPE: