* Chapter 1

1. What is Cyber Security?

It’s when processes and technologies are used to protect networks, devices, and data from unauthorized access, vulnerabilities, and attacks by cyber criminals.

1. What does Cyber stand for and Security stand for?

Cyber stands for Operating Systems, Networks, Applications, and Data.

Security stands for protection against attack or danger.

1. Describe Security in one word.

Security is LAYERS

1. What are the 5 layers of Security?

* Physical
* Personal
* Network
* Communications
* Information

1. What is the physical layer of security. Give an example.

* Protection: physical items, objects, and areas used to protect the system from attacks or unauthorized access.
* Example: Servers, Routers, biometrics, surveillance cameras,locks

1. What is the personal layer of security? Give examples.

Anything related to personnel access, who is authorized to access the organization and its operations?

Examples: Security engineers and system admins, security training for the employees (awareness), also firewalls and antiviruses

1. What is the Network Security Layer? Give examples.

Protecting the components of the network, connections, and content. Examples include Firewalls, VPNs, Encryption, Denial of Service Protection, and Network Monitoring and Logging.

1. What is Communication Security Layer? Give Examples

Protection of communication media, network components, and content.

Examples: Data Transmission, encrypt data that’s being transmitted by using protocols like SSL/TLS to prevent eavesdropping

Securing emailing by applying digital signature and end-to end encryption.

With Communication Security intact, Availability, Confidentiality, and Integrity are ensured.

1. What is Information Security?

Protection of information and its critical elements.

Examples: Backing up data, conducting vulnerability assessments like penetration testing.

1. Give the difference between data privacy and security?

|  |  |
| --- | --- |
| Data Security | Methods, policies, and means to protect personal data. |
| Data Privacy | Deals with how that protected data is being used. |

1. What are the 7 defenses in depth layers. List them and give examples:

* **Policies, Procedures, and awareness**: Passwords, Policies and data classification
* **Physical:** Locks, fences, and security guards
* **Perimeter:** Firewall, VPN, and Packet Filters
* **Internal Network:** Firewall, Intrusion Detection, and Encryption
* **Host:** Malware protection, platform OS
* **APP:** authentication and authorization
* **Data:** database, message, and content security

1. What are the three goals of security?

Confidentiality 🡪 Encryption

Integrity 🡪Hashing

Availability🡪Replication and Redundancy

1. Give examples of Advanced Persistent Threats’ objectives

* Espionage
* Data theft
* Network/system destruction.

1. What’s the difference between the red and blue teams?

Blue team is for defense and the red team is for offence.

1. What is penetration testing?

* Security assessment
* Simulated attacks on application
* Looking for vulnerabilities to exploit

1. What is the SOC?

Security Operations Center: Centralized unit that deals with security issues on the organizational and technical level.

1. What are Digital Forensics?

Application of science to investigate cyber attacks or crimes related to computers, intellectual property theft, cyber espionage, network, etc…

What does Digital Forensics focus on?

* File Systems: overwritten files, deleted files, etc…
* System Memory: contents of the memory
* System Logs: Which users?
* Network: what packets?

What is an Incident Response and what does it focus on?

* An incident: data breach or cyber-attack or misconfiguration or intrusion attempt
* An incident response tells us which approach or methodology we will use
* We want to recover and reduce damage.

What are the phases of the incident response?

1. **Preparation**: prevent and handle incidents
2. **Detection and Analysis**: analyze detected incident to identify severity of threat
3. **Containment, Eradication, and Recovery:** stop the spreading of the virus, clean it, and ensure recovery.
4. **Post-Incident Activity:** report is produced, and measures are taken to prevent mistakes like this from happening again.

What are examples of malware?

* Virus: a program that attaches itself to other files and can spread
* Trojan Horse: a malicious program that disguises as a useful software
* Ransomware: asks for money so you can take control of your device

What are the types of malware analysis?

1. Static analysis: inspecting malwares without running them
2. Dynamic analysis: Running the program in a controlled environment

What are the types of careers?

1. Incident handler
2. Penetration tester
3. Information Security Engineer

Security Terminology:

1. Vulnerability: weakness in the system that can be exploited
2. Risk: probability of a vulnerability being exploited

What causes vulnerabilities?

* **Familiarity:** if the code, system is too familiar, its prone to threats
* **Connectivity:** the more connected the device is, the more vulnerable it is
* **Poor Password Management:** weak passwords usage and the redundancy of passwords. All of this can be exploited using brute force.
* **Operating System Flaws:** authorization of access must be certain people.
* **People:** people can expose a system to vulnerabilities
* **Internet Usage:** spyware might be installed on your computer.
* **Software Bugs:** there might be exploitable bugs left unintentionally by the coder
* **Unchecked User Input**: not all inputs are safe.

What are Zero-Day Vulnerabilities?

* A hole in the software that is **unknown** to the vendor.
* It is exploited before the vendor knows.

What is Vulnerability Management?

* Detecting, Identifying, classifying, remediating, and mitigating security vulnerabilities

What are examples of Risks?

* **Information Theft**🡪 Exams
* **Identity Theft**🡪 Facebook Pages
* **Data Loss and Manipulation🡪**Destroy or alter results.
* **Disruption of Service🡪**Not allowing authorized and legitimate users to gain access to the files they’re supposed to get access to

What is the equation of Risk?

**Risk** = Threat **X** Vulnerabilities

How do you assess vulnerabilities?

1. **Identify Vulnerabilities:** analyze network scans, pen test scans, firewall logs🡪 to find anomalies.
2. **Verify Vulnerabilities:** Could it be exploited? How severe is it?
3. **Mitigate Vulnerabilities:** What should happen? What are the countermeasures?
4. **Remediate Vulnerabilities:** Update software or hardware