Week 1

- **What is the definition of cyber security according to the NIST Computer Security Handbook?**
- Answer: "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources."

- **What are the objectives of confidentiality in cyber security?**
- Answer: Data confidentiality and privacy.

- **What are the objectives of integrity in cyber security?**
- Answer: Data integrity and system integrity.

- **What is the objective of availability in cyber security?**
- Answer: Assuring those systems work promptly and service is not denied to authorized users.

- **Name two additional security objectives often mentioned in addition to the CIA triad.**
- Answer: Authenticity and accountability.

- **What does the CIA triad stand for in cyber security?**
- Answer: Confidentiality, Integrity, Availability.

- **Define a security breach.**
- Answer: Any event that results in a violation of any of the CIA security tenets.

- **What are the three levels of impact in a security breach?**
- Answer: High, Moderate, Low.

- **Give an example of a security requirement related to confidentiality.**
- Answer: Student grade information confidentiality regulated by the Data Protection Act in the UK.

- **Give an example of a security requirement related to integrity.**

- Answer: Inaccurate patient information that could result in harm or death to patients and expose the hospital to liability.

- **Give an example of a security requirement related to availability.**
- Answer: A public university website requiring a moderate level of availability.

- **Name the three categories of vulnerabilities.**
- Answer: Corrupted (loss of integrity), Leaky (loss of confidentiality), Unavailable or very slow (loss of availability).

- **What are threats in the context of cyber security?**
- Answer: Capable of exploiting vulnerabilities and represent potential security harm to an asset.

- **What are the four categories of active attacks?**
- Answer: Replay, Masquerade, Modification of messages, Denial of service.

- **What is a passive attack in cyber security?**
- Answer: An attempt to learn or make use of information from the system without affecting system resources.

- **What is an active attack in cyber security?**
- Answer: An attempt to alter system resources or affect their operation.

- **Give an example of a threat.**
- Answer: Various examples are possible.

- **What are some challenges in cyber security?**
- Answer: Security is not simple, potential attacks on security features, counter-intuitive procedures, deciding where to use security mechanisms, constant monitoring, security as an afterthought, etc.

- **What is attack surface?**
- Answer: The reachable and exploitable vulnerabilities in a system.

- **Name the three categories of attack surface.**

- Answer: Network attack surface, software attack surface, human attack surface.

- **What is an attack tree?**
- Answer: A hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.

- **Give an example of an attack tree analysis.**
- Answer: Various examples are possible.

- **True or False: Defense in depth and attack surface reduction complement each other in mitigating security risk.**
- Answer: True.

- **True or False: An attack tree analysis can be used to analyze the security of an internet banking authentication application.**
- Answer: True.

- **What is the main objective of confidentiality in cyber security?**
- Answer: To ensure that private information is not made available or disclosed to unauthorized individuals.

- **What is the main objective of integrity in cyber security?**
- Answer: To assure that information and programs are changed only in a specified and authorized manner and that a system performs its intended function in an unimpaired manner.

- **What is the main objective of availability in cyber security?**
- Answer: To ensure that systems work promptly and service is not denied to authorized users

- **What is the principle of economy of mechanism in security design?**
- Answer: The design of security measures should be as simple and small as possible.

- **What is the principle of fail-safe defaults in security design?**
- Answer: Access decisions should be based on permission rather than exclusion, with the default situation being lack of access.

- **What is the principle of complete mediation in security design?**
- Answer: Every access must be checked against the access control mechanism.

- **What is the principle of open design in security design?**
- Answer: The design of a security mechanism should be open rather than secret.

- **What is the principle of separation of privilege in security design?**
- Answer: Multiple conditions should be required to achieve access to restricted resources or perform certain actions.

- **What is the principle of least privilege in security design?**
- Answer: Every process and user should operate using the least set of privileges necessary to perform the task.

- **What is the principle of least common mechanism in security design?**
- Answer: Mechanisms allowing resources to be shared by more than one user should be minimized.

- **What is the principle of psychological acceptability in security design?**
- Answer: User interfaces should be well designed and intuitive, and security settings should adhere to user expectations.

- **What is the principle of work factor in security design?**
- Answer: The cost of circumventing a security mechanism should be compared with the resources of an attacker when designing a security scheme.

- **What is the principle of compromise recording in security design?**
- Answer: Sometimes it is more desirable to record the details of an intrusion than to adopt more sophisticated preventive measures.

- **Define penetration testing.**
- Answer: Penetration testing is a method for gaining assurance in the security of an IT system by attempting to breach its security using the same tools and techniques as an adversary might.

- **What is whitebox testing in penetration testing?**

- Answer: Whitebox testing involves sharing full information about the target system with testers to confirm the efficacy of internal vulnerability assessment and management controls.

- **What is blackbox testing in penetration testing?**
- Answer: Blackbox testing involves providing no information about the internals of the target system to testers, who perform the testing from an external perspective to identify ways to access internal IT assets.

- **What is the purpose of penetration testing?**
- Answer: The purpose of penetration testing is to mitigate risk, comply with legal requirements, validate/invalidate security controls, find and mitigate vulnerabilities, and prevent compromise.

- **What are the phases of an attack in penetration testing?**
- Answer: The phases are reconnaissance and footprinting, scanning and enumeration, gaining access, maintaining access, and covering tracks.

- **What is the purpose of the reconnaissance and footprinting phase in an attack?**
- Answer: This phase involves gathering information about the target system, such as network layouts, domains, and infrastructure details, to understand how the network works and identify potential vulnerabilities.

- **What is the purpose of the scanning and enumeration phase in an attack?**
- Answer: In this phase, attackers scan the network to find entry points and perform enumeration to count and assess vulnerabilities and gather information like usernames, hostnames, IP addresses, and configurations.

- **What is the purpose of the gaining access phase in an attack?**
- Answer: In this phase, attackers break into the network, deliver malware to vulnerable systems, and map the organization's defenses from the inside to create a plan for targeted information.

- **What is the purpose of the maintaining access phase in an attack?**
- Answer: Once attackers gain elevated privileges, they maintain access to the network and conduct data exfiltration to extract data from the network.

- **What is the purpose of the covering tracks phase in an attack?**

- Answer: In this phase, attackers hide or delete any evidence of their access and actions to cover their tracks.

- **Who adapted the concept of a kill chain to the information security space?**
- Answer: Lockheed Martin

- **What is the main idea behind the kill chain?**
- Answer: Identifying the attacker's stage in the process to adapt response tactics.

- **What term describes hackers who are not very sophisticated?**
- Answer: Amateurs

- **What is the motivation of crackers?**
- Answer: Accessing resources without permission.

- **What is the main goal of career criminals in hacking?**
- Answer: Well-planned attacks, usually for financial gain.

- **Why do military hackers engage in cyber attacks?**
- Answer: To disable opposing forces and gain strategic advantage.

- **What is casual snooping in the context of hacking?**
- Answer: Inquisitive crackers looking around without specific motives.

- **What is the motivation behind the act of disruption in hacking?**
- Answer: Preventing or inhibiting legitimate users from system use.

- **What does espionage involve in the context of hacking?**
- Answer: Attempting to extract information, possibly commercial, from a system.

- **What can be done once a system or network is compromised?**
- Answer: It can be used to launch attacks on other networks.

- **What is the motivation behind making a statement in hacking?**
- Answer: Social, political, anarchistic expression.

- **How can information be gathered in social engineering?**
- Answer: Through conversations and various research methods.

- **What sources exist for social engineers to gather information?**
- Answer: Social media, public records, and online databases.

- **What can you glean from gathered information in social engineering to profile your targets?**
- Answer: Information to better understand and profile the targets.

- **How can you locate, store, and catalog all this information for easy use?**
- Answer: By using organizational methods and digital tools for efficient storage and retrieval.

- **What is eliciation in social engineering?**
- Answer: The subtle extraction of information during normal conversations.

- **What is pretexting in social engineering?**
- Answer: Telling a story or lie during a social engineering engagement.

- **What role do emotions and beliefs play in social engineering?**
- Answer: They are used to influence and manipulate individuals.

- **What is the process of assessing a system's vulnerability called?**
- Answer: Penetration testing.

- **What are some examples of motivations behind hacking?**
- Answer: money, fame, political belief, revenge.

- **What is the main goal of social engineering?**
- Answer: Manipulating individuals to gain sensitive information or unauthorized access.

- **What is the purpose of gathering information in social engineering?**
- Answer: Understanding the targets better and tailoring manipulation techniques.

- **What is the technique of extracting information during normal conversations called?**
- Answer: Elicitation.

- **What role does persuasion and influence play in social engineering?**
- Answer: They are used to manipulate individuals' emotions and beliefs.