Week 01:

A close-up of a blue sign

Description automatically generated

**CIA TRIAD – CONFIDENTIALITY INTEGRITY AVAILABILITY**

Confidentiality - Authorised subjects can access protected data.

* Regulated by the Data Protection Act in the UK.

Data Confidentiality - Assures that private information is not made available or disclosed to unauthorised individuals.

Privacy - Assures that individuals control or influence what information related to them may be collected and stored.

Integrity - Authorised subjects can modify protected data.

* A low-integrity requirement example is an anonymous online poll.
* A Web site that offers a forum to registered users to discuss some specifc topic would be assigned a moderate level of integrity.

Data Integrity - Assures that information and programs are changed only in a specified and authorised manner.

System integrity - Assures that a system performs its intended function in an unimpaired manner, free from any manipulation.

Availability - Information and the resources that manage information are available on demand to authorised subjects.

* A moderate availability requirement is a public university Web site.
* An online telephone directory lookup application would be classified as a low availability requirement.

**ADDITIONAL CONCEPTS OBJECTIVES**

Authenticity - Verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

**THREAT MODELLING**

Risk - possibility of loss, injury, or other adverse or welcome circumstance.

Threat - Vulnerability. Individuals, or organisations that could cause something bad to happen if exploited.

Breach - If threats are exploited, they become a breach. Result in a violation of the CIA security tenets.

Countermeasure – Also called Security Controls. Technical and non-technical measures that are put in place to mitigate/courter identified risks.

**VULNERABILITY**

A vulnerability is any weakness in a system that can be exploited by a threat actor or can be affected by a hazard.

Categories:

Corrupts data leads to integrity Violation.

Leaks data leads to Confidentiality Violation.

Loss of service leads to availability Violation.

**ATTACKS (THREATS CARRIED OUT)**

Passive attempt to learn or make use of information from the system that does not affect system resources.

Active attempt to alter system resources or affect their operation.

Insider initiated by an entity inside the security parameter.

Outsider initiated from outside the perimeter.

Passive attack - Eavesdropping on, or monitoring of, transmissions.

Active attack - Modification of the data stream or the creation of a false stream

**BREACHES THREATS**

Eavesdropping: Secretly listen to a conversation.

Alteration: unauthorised modification

Interruption: can cause a system to become unavailable.

Masquerading: pretend to be someone one is not - the fabrication of info that is purported to be from someone

Repudiation: denial of a commitment or data receipt.

**ATTACK SURFACE**

Consists of the reachable and exploitable vulnerabilities.

Categories:

Network attack surface.

* vulnerabilities over an enterprise network, wide-area network, or Internet.

Software attack surface

* Vulnerabilities in application, utility, or operating system code

Human attack surface

* vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders.

**THE TEN SECURITY PRINCIPLES**

Economy of mechanism - security measures embodied in both hardware and software should be as simple and small as possible.

Fail-safe defaults - the default state is one where access is not granted, and access is only permitted when explicitly allowed by the system's security policies.

Complete mediation -Every access must be checked against the access control mechanism.

Open design - design of a security mechanism should be open rather than secret.

Separation of privilege - This principle emphasizes that multiple conditions or factors should be required to achieve access to restricted resources or perform certain actions. - Implementing multiple layers of security controls

Least privilege - Users and processes should only have access to the resources and capabilities required to fulfil their designated functions and nothing more.

Least common mechanism - mechanisms allowing resources to be shared by more than one user should be minimised.

Psychological acceptability - user interfaces should be well designed and intuitive, and all security-related settings should adhere to what an ordinary user might expect.

Work factor - when designing security mechanisms, the cost or effort required for an attacker to circumvent the security measures should be considered in relation to the resources available to the attacker. By increasing the work factor—making it more difficult, time-consuming, or costly for an attacker to breach security—the effectiveness of the security scheme is improved.

Compromise recording - In some situations, it may be more desirable to focus on recording and analysing details of security breaches or intrusions rather than solely relying on preventive measures.

**HACKERS AND PEN TESTERS**

1. White Hackers are Information Security professionals who use hacking skills to expose vulnerabilities and makes their systems more secure.
2. Amateurs are entry-level hackers who use scripts and software from experienced hackers.
3. Hackers/ Crackers - who conduct illegal activities for financial gain.
4. Hacktivists - conduct hacking activities for political or ideological goals.
5. Script Kiddies - use other people tools. Their knowledge is usually limited. They perform a cyberattack without understanding it.
6. State-sponsored - a lot of resources and their attacks are complex. They usually have their own tools.
7. Someone who legally breaks into a system to assess security deficiencies is a "penetration tester" or ethical hacker.

**MOTIVATIONS**

Means - possess the ability to commit the crime in question?

Motive - a reason to engage in the commission of the crime.

Opportunity - the necessary access and time to commit the crime?

Ethical hackers require permission to engage in penetration testing – Need advance knowledge – Use same strategies s malicious hacker.

Penetration testing investigating, uncovering, attacking, and reporting on a target system’s strengths and vulnerabilities.

Penetration tests - part of IT audits.

[Plan their test in a way that do not disrupt the system or operation. Instead of exploiting a vulnerability (discovery), an ethical hacker will report it. suggest security controls to mitigate discovered vulnerabilities.

Black-Box Testing - Black-box testing aims to replicate how an attacker would interact with the system, focusing on understanding its behaviour and vulnerabilities from an external viewpoint.

No knowledge of system provided to testing team.

White-Box Testing - Advanced knowledge provided to testing team.

**PART OF A PENETRATION TEST INCLUDES THE FOLLOWING:**

Technical attack an attack against technology from either the inside or the outside depending on the goals and intentions of the client.

Administrative attack Designed to find loopholes or shortcomings in how tasks and operational processes are performed.

Physical attack Includes anything that targets physical equipment and facilities with actions such as theft, breaking and entering, or similar actions. Can also include actions against people, such as social engineering–related threats.

**HACKING METHODOLOGIES CONTAINS FIVE DISTINCT STAGES:**

* Reconnaissance
* Scanning and enumeration
* Gaining Access (INFILTRATION AND ESCALATION)
* Maintaining Access (EXFILTRATION, ACCESS EXTENSION AND ASSAULT)
* Covering Tracks (OBFUSCATION)

A screenshot of a computer

Description automatically generated

* RECONNAISSANCE

1. Reconnaissance involves gathering information about a target system.

2. Passive attacks, like OSINT, are commonly used in this stage.

3. Attackers aim to understand network layouts, domains, and infrastructure details.

4. Pen testers use reconnaissance to comprehend network assets and systems.

5. It's crucial for thorough security testing to uncover overlooked information.

* SCANNING AND ENUMERATION OR (SCANNING)

1. Scanning involves searching an organization's network for entry points.

2. This process can be lengthy, lasting months as attackers seek vulnerabilities.

3. Enumeration is about establishing active connections to assess vulnerabilities.

4. It's used to collect usernames, IP addresses, passwords, and configurations.

5. Enumeration poses significant security challenges for programmers.

6. Enumeration is the process to find out what is on a target system.

* GAINING ACCESS OR (INFILTRATION AND ESCALATION)

1. Attackers infiltrate the network, deploying targeted malware to exploit vulnerabilities.

2. They assess the organization's defences internally and plan their attack strategy.

3. Penetration tests aim to exploit system vulnerabilities to assess potential unauthorized access or malicious activity.

4. Testers use manual techniques and human intuition to validate, attack, and exploit vulnerabilities uncovered during the assessment.

\*\* Which activity do hackers conduct to map inside defences in an organisation? Infiltration

* MAINTAINING ACCESS OR (EXFILTRATION, ACCESS EXTENSION AND ASSAULT)

1. After identifying weaknesses, the next step is to gain access and escalate privileges.

2. Privileged access is often necessary for attackers to move freely within the environment.

3. Once elevated privileges are obtained, the network is effectively controlled by the intruders.

4. Malware, including rootkits, can be used to maintain access and control.

5. Data exfiltration is conducted, simulating hacker actions to extract data from the network.

* COVERING TRACKS OR (OBFUSCATION)

1. Covering tracks involves hiding or deleting any evidence of access.

2. It includes concealing continued access to the system.

3. Malware can be used to prevent logging of actions or misreport system information.

**SOCIAL ENGINEERING**

1. How to gather information? Use online research, phishing emails, dumpster diving, pretexting, and phone calls to gather information.

2. Sources for social engineers? Social media, company websites, public records, online forums, job listings, and networking events.

3. Profiling targets? Determine interests, job roles, relationships, and behavioural patterns to tailor attacks.

4. Locating, storing, and cataloguing information? Use spreadsheets, databases, and specialized tools to organize and manage gathered data securely.

**SOCIAL ENGINEERING EXAMPLES:**

1. Influence: The Power of Persuasion

- Social engineers use persuasion techniques to influence emotions and beliefs.

- Understanding people's thoughts and feelings is crucial for successful manipulation.

2. Elicitation: Pretexting

- Elicitation involves subtly extracting information during seemingly normal conversations.

- Pretexting is a form of deception where social engineers create a false story or lie to extract information during social engineering engagements.