UNIVERSITY OF WESTMINSTER

Cyber Security Concepts and Principles

6COSC019W- Cyber Security

Dr Ayman El Hajjar

January 26, 2024

School of Computer Science and Engineering
University of Westminster

Outline

1. Information Systems
2. Cyber Security Fundamentals
3. Threat modelling
4. Fundamental security design principles
5. Hackers and Pen Testers

Information Systems

What are we trying to protect?

What are we trying to protect?

- Customer Data
- IT and Network Infrastructure
- Intellectual Property
- Financial Data
- Services availability and Productivity
- Reputation

INFORMATION SYSTEM ASSETS

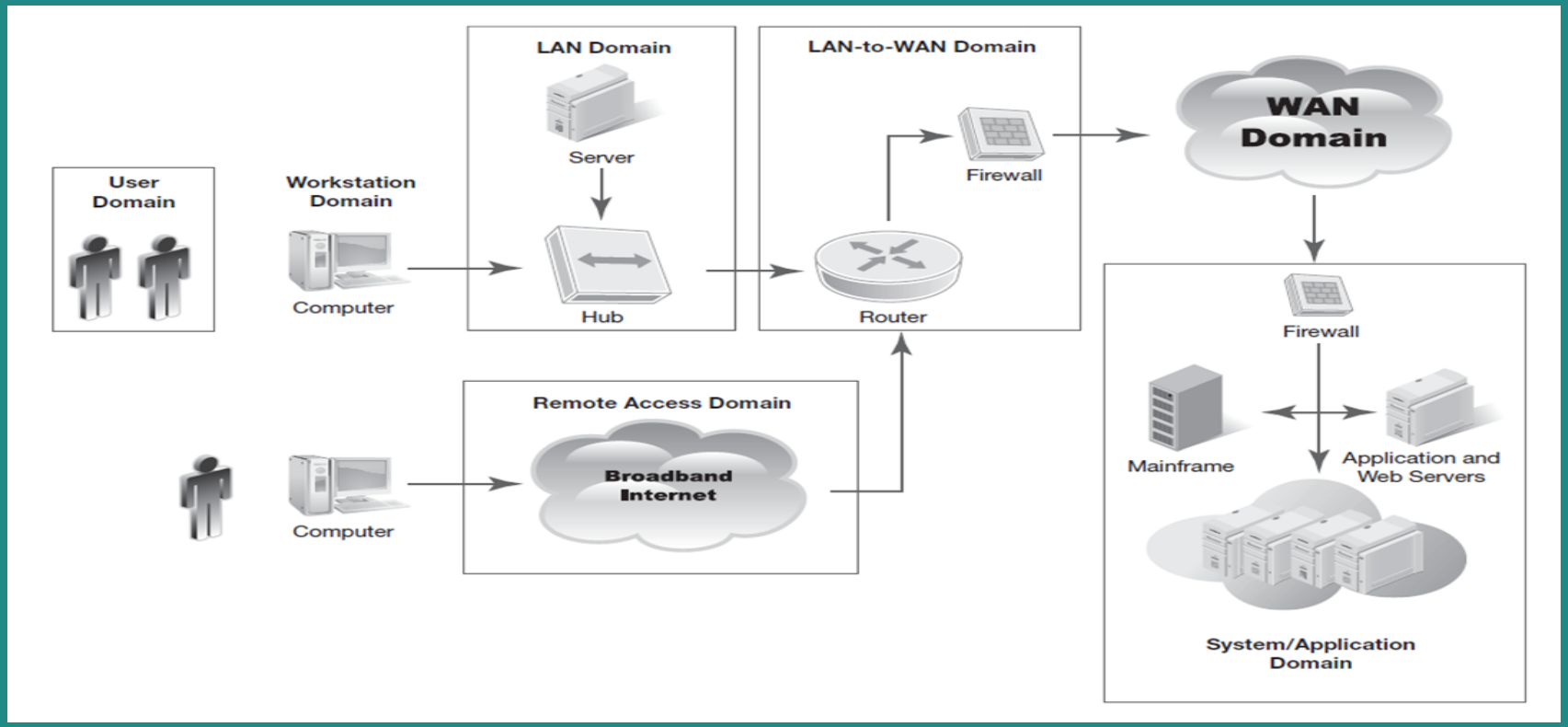


Figure 1: The Seven Domains of an Information System [1]

[1] David Kim, Michael Solomon, Fundamentals of Information Systems Security, Fourth Edition

Cyber Security Fundamentals

CYBER SECURITY- A DEFINITION

The NIST Computer Security Handbook definition

"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 (includes hardware, software, firmware, information/data, and telecommunications)"

THE CIA TRIAD

- **Confidentiality**, **Integrity**, **Availability** are the three concepts form what is often referred to as the CIA triad.

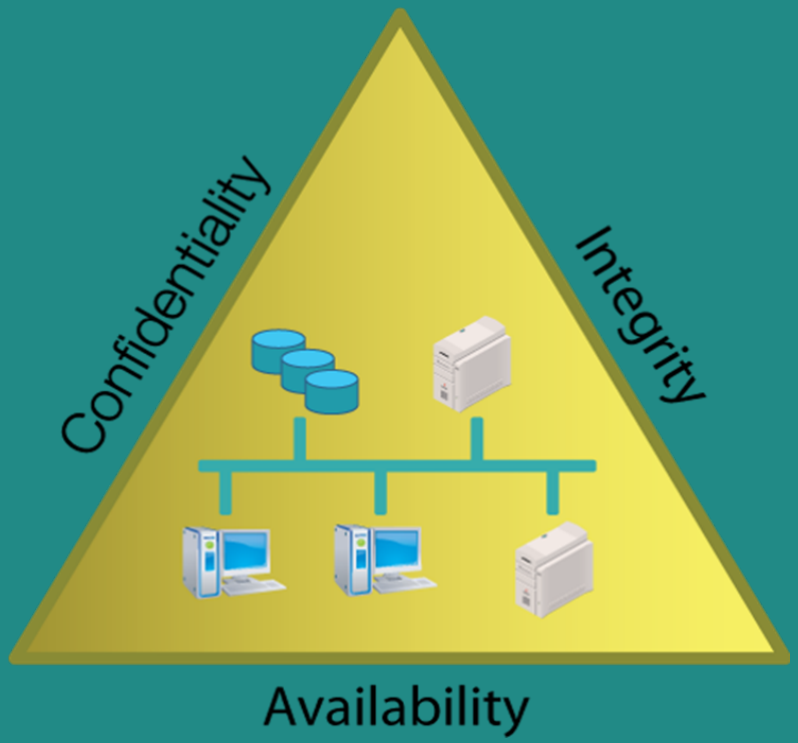


Figure 2: CIA Triad- Confidentiality, Integrity, Availability [a]

- **Confidentiality** Ensuring that only authorised subjects can access protected data
- **Integrity** Ensuring that only authorised subjects can modify protected data
- **Availability** Ensuring that information and the resources that manage information are available on demand to authorised subjects

[a] Chapter 1, Hacker Techniques, Tools, and Incident Handling

Cyber Security objectives

Confidentiality

- **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 and by whom and to whom that information may be disclosed

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

- **Availability** Assures that systems work promptly and service is not denied to authorised users

And some possible additional concepts Objectives

- Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

Authenticity

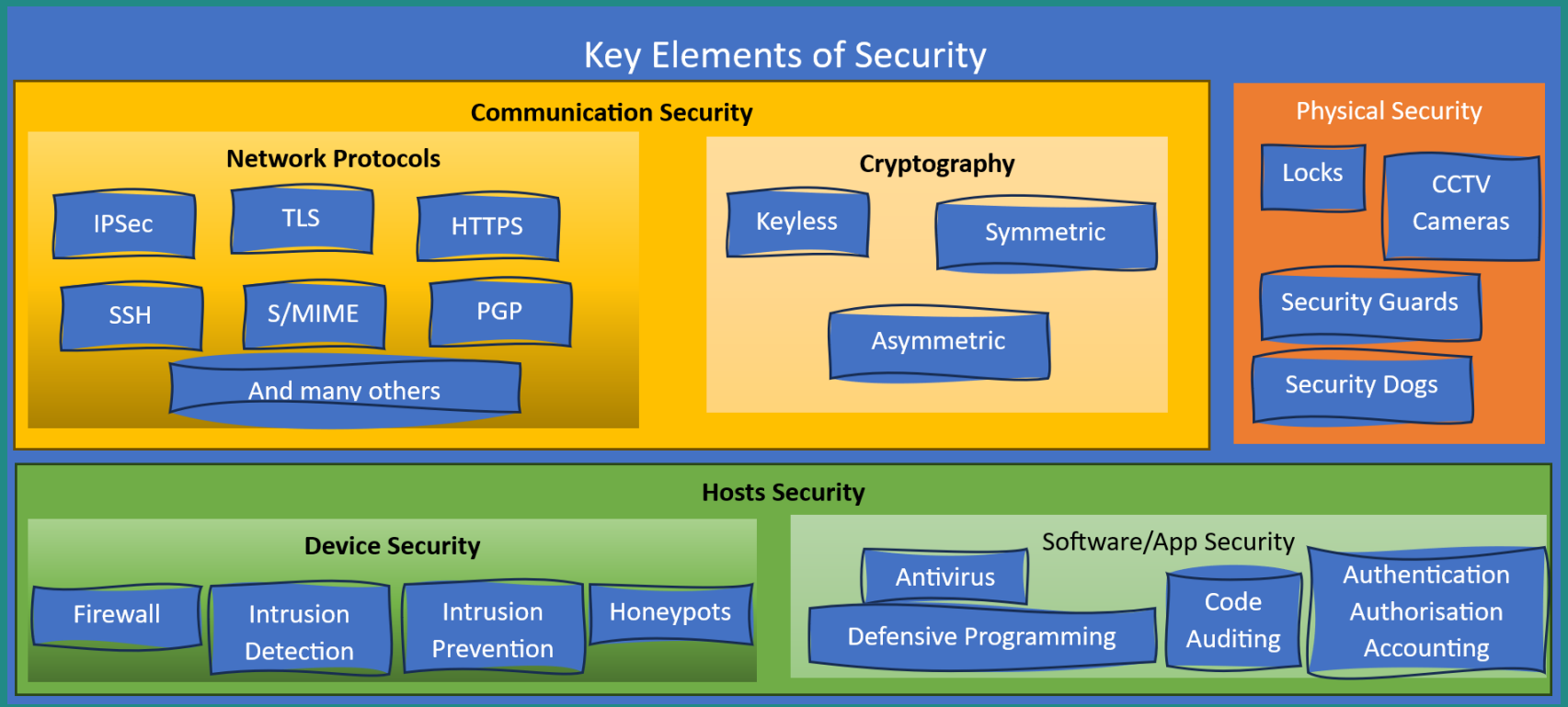
- **Authenticity** Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

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

Examples of Security Requirements

- **Confidentiality**
  - Student grade information is an asset whose confidentiality is considered to be highly important.
  - Regulated by the Data Protection Act in the UK.
- **Integrity**
  - Inaccurate Patients information could result in serious harm or death to patients and expose the hospital to massive liability.
  - A Web site that offers a forum to registered users to discuss some specific topic would be assigned a moderate level of integrity.
  - A low-integrity requirement example is an anonymous online poll
- **Availability**
  - Critical components need a high level of availability.
  - A moderate availability requirement is a public university Web site.
  - An online telephone directory lookup application would be classified as a low-availability requirement


Key Elements of Security
Communication Security
Network Protocols
IPSec
TLS
HTTPS
SSH
S/MIME
PGP
And many others
Cryptography
Keyless
Symmetric
Asymmetric
Physical Security
Locks
CCTV Cameras
Security Guards
Security Dogs
Hosts Security
Device Security
Firewall
Intrusion Detection
Intrusion Prevention
Honeypots
Software/App Security
Antivirus
Defensive Programming
Code Auditing
Authentication
Authorisation
Accounting

Threat modelling

TERMS AS DEFINED BY THE NCSC

Risk

- **Risk** is the possibility of loss, injury, or other adverse or welcome circumstance;

Threat

- Threats are vulnerabilities, events, individuals or organisations that could cause something bad to happen if exploited.
- They represent potential security harm to an asset

Breach

- If threats are exploited, they become a breach.
- A breach will result in a violation of any of the CIA security tenets

Countermeasure

- Countermeasures, also called **Security Controls** are technical and non-technical measures that are put in place to mitigate/courter identified risks.

VULNERABILITIES & ATTACKS

- A **vulnerability** is any weakness in a system that can be exploited by a threat actor, or can be affected by a hazard.
- **Categories of vulnerabilities**
  - 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 and Active Attacks

Passive Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted

Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream

Breaches Threats

- **Eavesdropping**: the interception of information intended for someone else during its transmission over a communication channel.
- **Alteration**: unauthorised modification of information.
- **Interruption**: the interruption or degradation of a data service or information access can cause a system to become unavailable.
- **Masquerading**: the fabrication of information that is purported to be from someone who is not actually the author.
- **Repudiation**: the denial of a commitment or data receipt.

Attack Surface

- Consists of the reachable and exploitable vulnerabilities in a system
- Can be categorised in the following way:
  - Network attack surface
    - This category refers to vulnerabilities over an enterprise network, wide-area network, or Internet
  - Software attack surface
    - Vulnerabilities in application, utility, or operating system code
  - Human attack surface
    - Refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

THREAT MODELLING: ATTACK TREES

- Refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

A branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities

The security incident that is the goal of the attack is represented as the root node of the tree

The ways that an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes of the tree

The final nodes on the paths outward from the root, the leaf nodes, represent different ways to initiate an attack

Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared

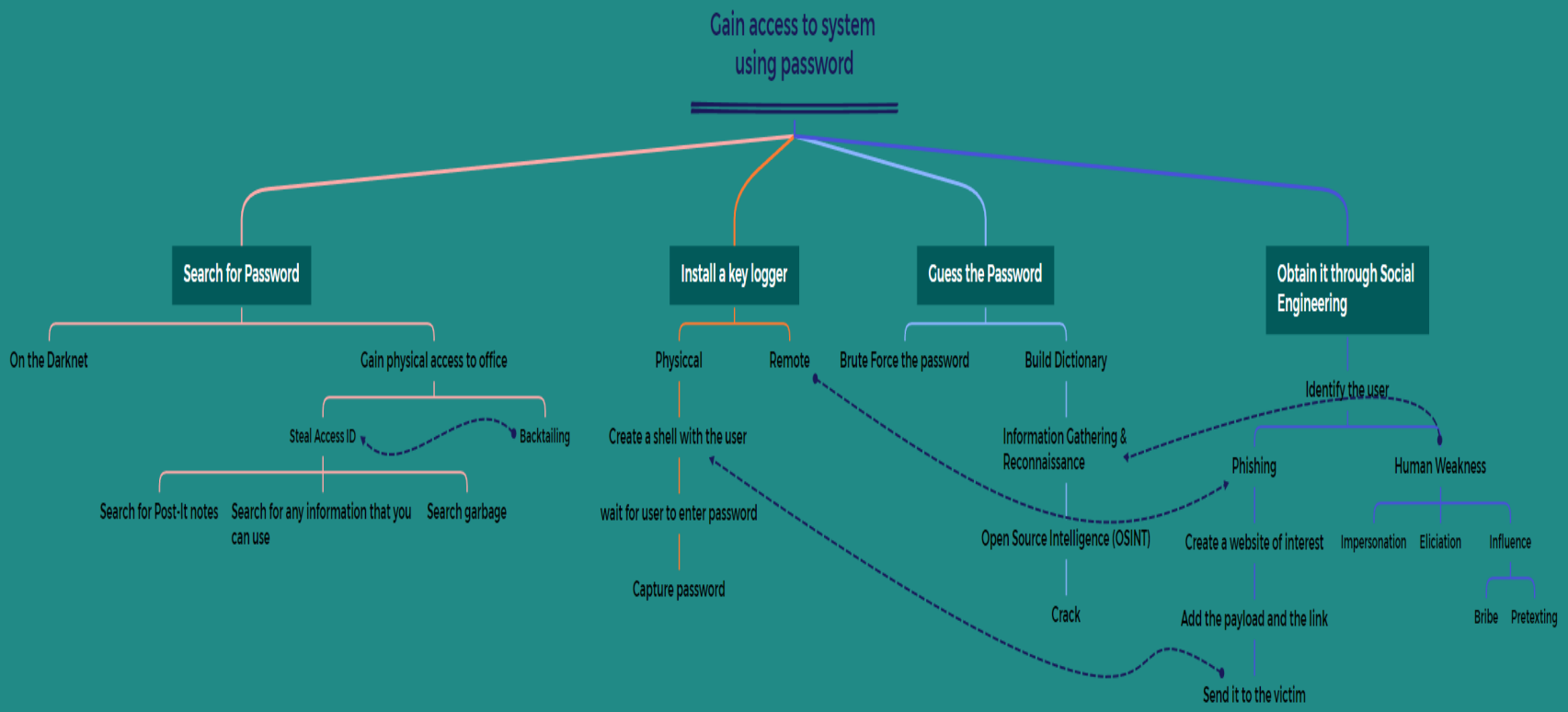


Figure 4: Attack Tree- Gaining Access by obtaining the password

Fundamental security design principles

THE TEN SECURITY PRINCIPLES

- The National Centres of Academic Excellence in Information Assurance/Cyber Defence adopted a modified **Saltzer and Schroeder Principles (1975)**. They list the following as fundamental security design principles:

Economy of mechanism

- The design of security measures embodied in both hardware and software should be as simple and small as possible

Fail-safe defaults

- Access decisions should be based on permission rather than exclusion—the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted

Complete mediation

- Every access must be checked against the access control mechanism

Open design

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

Separation of privilege

- This principle dictates that multiple conditions should be required to achieve access to restricted resources or have a program perform some action.

Least privilege

- Every process and every user of the system should operate using the least set of privileges necessary to perform the task (the bare minimum privileges)

Least common mechanism

- In systems with multiple users, mechanisms allowing resources to be shared by more than one user should be minimised.

Psychological acceptability

- This principle states that user interfaces should be well designed and intuitive, and all security-related settings should adhere to what an ordinary user might expect.

Work factor

- According to this principle, the cost of circumventing a security mechanism should be compared with the resources of an attacker when designing a security scheme.

Compromise recording

- This principle states that sometimes it is more desirable to record the details of an intrusion than to adopt more sophisticated measures to prevent it.

Hackers and Pen Testers

Profiles and Motives of Different Types of Hackers

- **White Hackers** are Information Security professionals who use hacking skills to expose vulnerabilities and makes their systems more secure
- **Amateurs** are entry-level hackers who use scripts and software from experienced hackers
  - **Hackers** are hackers, also called crackers, who conduct illegal activities for financial gain .
  - **Hacktivists** are activists hackers who conduct hacking activities for political or ideological goals
  - **Script Kiddies** are hackers who use other people tools. Their knowledge is usually limited. They perform a cyberattack without actually understanding it.
  - **State-sponsored** are hackers supported usually have a lot of resources and their attacks are complex. They usually have their own tools.

Figure 5: The hacker Mindset [2]

[2] Chapter 1, Hacker Techniques, Tools, and Incident Handling

MOTIVATIONS

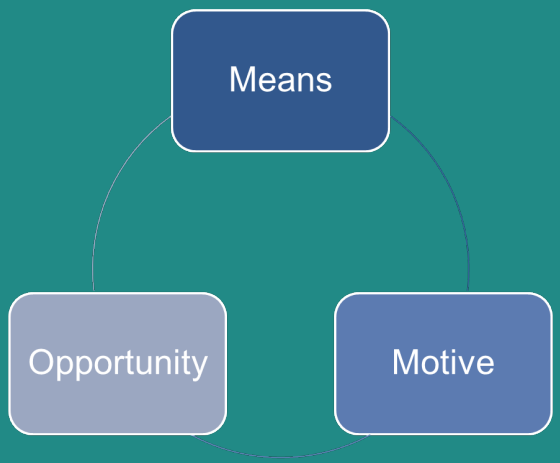


Figure 6: Motivations [a]

[a] Chapter 1, Hacker Techniques, Tools, and Incident Handling

- **Means** Does the attacker possess the ability to commit the crime in question?
- **Motive** Does the attacker have a reason to engage in the commission of the crime?
- **Opportunity** Does the attacker have the necessary access and time to commit the crime?

Modern Hacking and Cybercriminals

- Typically, hacking methodologies contains five distinct stages:
  - Reconnaissance
  - Scanning and enumeration
  - Gaining Access
  - Maintaining Access
  - Covering Tracks
- Each stage uses different tools and techniques.

  Modern hackers now use a more detailed hacking methodology.

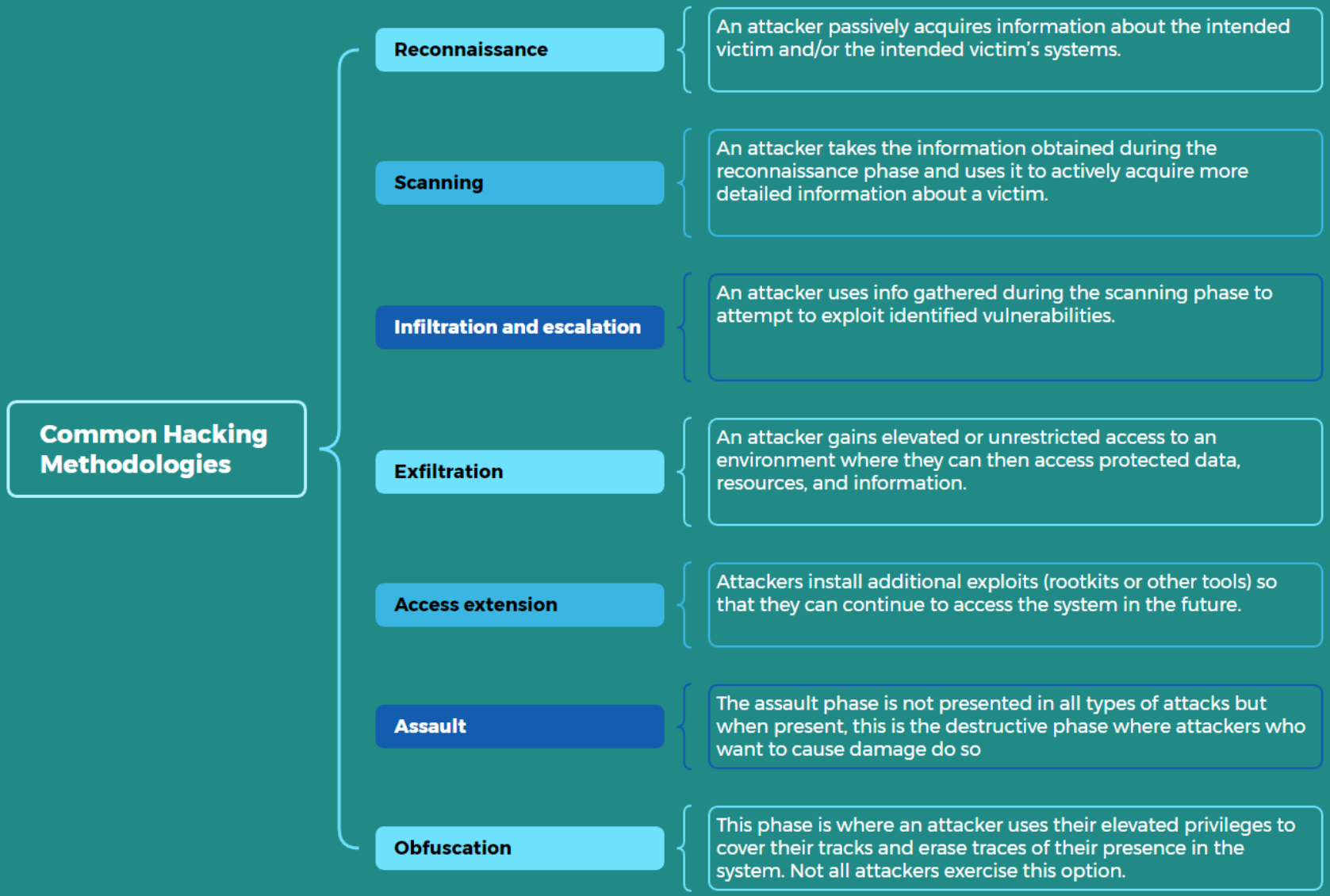


Figure 7: Common Hacking Methodologies: Hacking Steps

Ethical Hacking and Penetration Testing

- **Ethical hackers** require permission to engage in penetration testing
- **Penetration testing** is the structured and methodical means of investigating, uncovering, attacking, and reporting on a target system's strengths and vulnerabilities
- **Penetration tests** are commonly part of IT audits

Black-Box Testing

- Used to simulate how attacker views system
- No knowledge of system provided to testing team

White-Box Testing

- Advanced knowledge provided to testing team

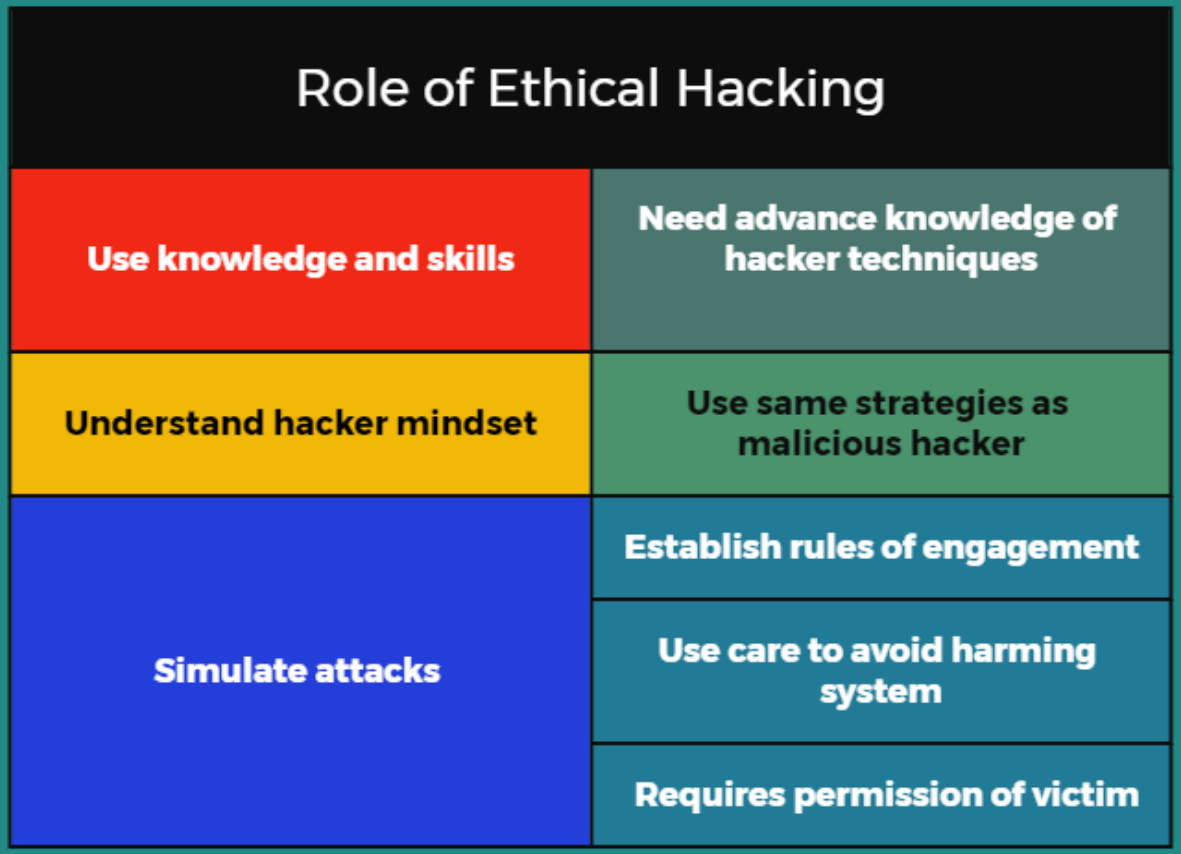


Figure 8: Role of Ethical hackers [3]

[3] Chapter 1, Hacker Techniques, Tools, and Incident Handling

Ethical Hacking Penetration testing Steps

- An ethical hacker, conducting a penetration testing goal is to audit an information system and its existing security controls (if any) and to identify any existing vulnerabilities
  - They will define the scope of the test and 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.
  - They can suggest security controls to mitigate discovered vulnerabilities

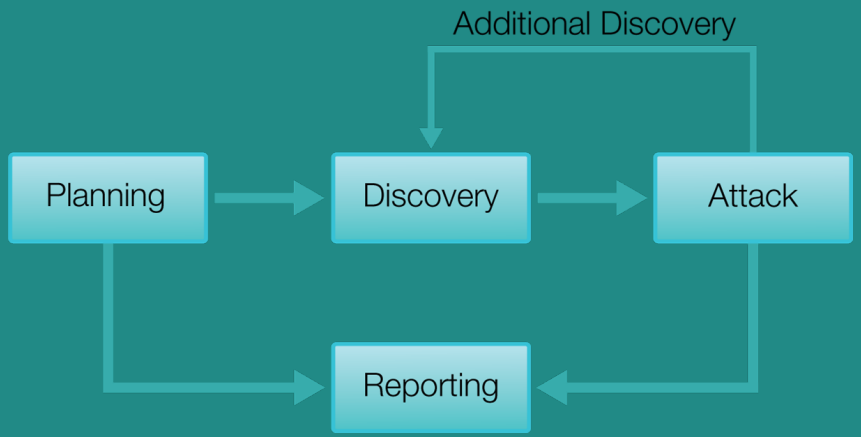


Figure 9: Ethical hacking penetration testing process

Performing a Penetration Test

- Tests that can be part of a penetration test include the following:
  - **Technical attack** Designed to simulate 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.

RECONNAISSANCE

- A large part of the information gathering stage is conducting using passive attacks such as by using public records and Open Source Intelligence (OSINT)
- Attackers then leverage information from a variety of factors to understand their target including identifying network layouts, domains, servers, infrastructure details).
- This will help the pen tester to understand how a network works, including its assets (applications, systems, devices, anything with an IP).
- The reconnaissance stage is crucial to thorough security testing because penetration testers can identify additional information that may have been overlooked, unknown, or not provided

SCANNING AND ENUMERATION OR (SCANNING)

- The next step is to **scan** an organisation's network to find entry points.
  - This step of the process usually goes slowly, sometimes lasting months, as the attackers search for vulnerabilities.
- **Enumeration** Enumeration is basically counting. A hacker establishes an active connection to the target host. The vulnerabilities are then counted and assessed. It is done mainly to search for attacks and threats to the target system.
  - Enumeration is used to collect usernames, hostnames, IP addresses, passwords, configurations, etc.
  - Enumeration is very important to programmers, as it poses significant challenges to the security of any system

Gaining Access or (Infiltration and Escalation)

- Attackers break into the network, delivering targeted malware to vulnerable systems and people, often without the user being aware they are a target.
- They then map the organisation's defences from the inside and create a battle plan for information they intend to target.
- Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorised access or other malicious activity is possible and identify which flaws pose a threat to the application.
- After interpreting the results from the vulnerability assessment, penetration testers use manual techniques, human intuition, and their backgrounds to validate, attack, and exploit those vulnerabilities.

Maintaining Access or (Exfiltration, Access Extension and Assault)

- Now that weaknesses in the target network are identified, the next step in the cyber attack is to gain access and then escalate.
- In almost all such cases, privileged access is needed because it allows the attackers to move freely within the environment.
- Once the attackers gain elevated privileges, the network is effectively taken over and is now ”owned” by the intruders.
- This is another stage where malware can be beneficial. You may need to install a rootkit
- **Data Exfiltration** is then conducted and the tester uses tools and techniques to extract data from the network, simulating the actions of hackers.

Covering Tracks or (Obfuscation)

- Covering your tracks is where you hide or delete any evidence to which you managed to get access.
- Additionally, you should cover up your continued access.
- This can be accomplished with malware that ensures that your actions are not logged or perhaps misreports system information, like network connections.

Social Engineering

With that knowledge in mind, here are questions that come up with regard to information gathering:

- How can you gather information?
- What sources exist for social engineers to gather information?
- What can you glean from this information to profile your targets?
- How can you locate, store, and catalogue all this information for the easiest level of use?

Social Engineering Examples

Elicitation

- Elicitation is ”the subtle extraction of information during an apparently normal and innocent conversation.

Pretexting-A good liar...

- Some people say Pretexting is just a story or lie during a **social engineering** engagement.

Influence: The Power of Persuasion

- Persuasion and influence involve emotions and beliefs . **You have to know how and what people are thinking.**

Social Engineering example: Blocking you out of your account
click here for Youtube video

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **The lecture notes are very detailed. If you attend the lecture, you should be able to understand the topics.**
- **You can use any of the recommended readings! You do not need to read all the chapters!**
- **Recommended Readings note:** Focus on what was covered in the class.
  - Chapter 1, Ethical Hacking, CEH v11 Certified Ethical Hacker Study Guide
  - Chapter 1, Information Systems Security, Fundamentals of Information Systems Security
  - Chapter 1 Introduction, CyBOK, The Cyber Security Body of Knowledge