Ethical Hacking

Session 1

Ethical Hacking

Learning Objective

1 • Explain key issues plaguing the information security world

2 • Describe the essential elements of information security

3 • Define ethical hacking

4 • List the types of hacking/types of hackers

5 • Explain the types of attacks

6 • Explain the purpose of ethical hacking

7 • Describe the phases of ethical hacking

8 • Explain laws related to hacking

9 • Describe Penetration Testing

Introduction to Ethical Hacking

❑ Ethical hacking is a process where an ethical hacker:

- Works for an organisation or appointed as reliable person.
- Enter in the computer network or system by using the same method as a hacker and checks the security vulnerabilities.
- Identifies and eliminates the potential threats and weak areas where the hacker can exploit the network or the data in the system.

Key Issues Plaguing the Information Security World

- ❑ In last 10 years, there is a rapid growth of computer technology.
- ❑ People have easy access to Internet, as a result security issues and attacks are rising in various ways.
- ❑ People as well as organisations have become target of these cyber attacks.
- ❑ The purpose of these attacks are to steal the data or perform cyber crime in various ways.

Cyber Crime 1-12

- Cyber Crime:
  - Is illegal as well as criminal activity performed by the hacker or attacker by using unauthorised access of computers and the Internet.
  - Involves attack on information about individuals, corporations or governments.
  - Perform actions can occur in jurisdictions separated by vast distances.
  - For example: An attacker uses illegal online account of user to steal money from the account.

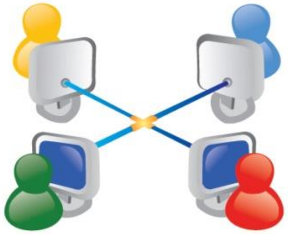
Cyber Crime 2-12

- Attacker performs many illegal activities such as:

Stealing important data.

Changing the data structure and so on.

Spreading viruses and malware in the system or network.



Cyber Crime 3-12

- Based on the role played by the computer, there are three broad categories of cyber crime:

The computer is used as an accessory.

For example: Using a computer to store illegal or stolen information.

The computer is used as a weapon.

For example: Using a computer to commit crimes such as illegal gambling or fraud.

Computer is the target.

For example: Using the computer to attack other computers, with an intention of causing damage such as spreading viruses.

Cyber Crime 4-12

- The Australian Institute of Criminology has identified eight types of cyber crimes and they are as follows:

- Theft of telecommunication services
- Communications in furtherance of criminal conspiracies
- Telecommunication Piracy
- Dissemination of offensive material
- Electronic vandalism, extortion and terrorism
- Sales and Investment fraud
- Illegal interception of communication
- Electronic funds transfer fraud

Cyber Crime 5-12

Theft of telecommunication services

❑ Cyber criminals can obtain access:

- By gaining access to an organisation’s telephone switchboard.
- To dial-in/dial-out circuits and make their own calls or sell call time to third parties.
- To the switchboard by using software available on the Internet.
- Find loop between PBX systems to evade detection by some sophisticated offenders.
- Resort to capturing ’calling card’ details.

Cyber Crime 6-12

Communications in furtherance of criminal conspiracies

- ❑ Criminal organisations and people:
  - – Enhance their activities by using information systems for communication and record keeping.
  - – Use Internet in organised way for illegal activities such as drug trafficking, gambling, money laundering, illegal trade in weapons and so on.
  - – Use encryption technology for criminal communications beyond the reach of law enforcement.

Cyber Crime 7-12

Telecommunication Piracy

- ❑ Digital technology allows reproduction and easy dissemination of print, graphics, sound and multimedia combinations.
- ❑ The temptation to reproduce copyrighted material for personal use, for sale at a lower price or for free distribution, has proven irresistible to many.
- ❑ Billions of dollars are lost by industry every year to illegal reproduction and distribution/sale of copyrighted material.

Cyber Crime 8-12

Dissemination of offensive material

- ❑ Cyberspace abounds in material considered to be offensive or objectionable by many people.
- ❑ Racist propaganda, sexually explicit material and instructions for making explosive devices are examples of such offensive material.

Cyber Crime 9-12

Electronic vandalism, extortion and terrorism

- ❑ Any damage to or interference with these systems can lead to catastrophic consequences.
- ❑ A number of incidents of hacking and defacing of Websites of governmental and commercial organisations have been reported worldwide.
- ❑ Offenders have been known to threaten Internet service providers and held them to ransom by breaking into their sites and disrupting services offered by these service providers.
- ❑ Individuals have been held to ransom by hackers who have obtained their credit card details by hacking popular online retail sites and e-commerce sites.

Cyber Crime 10-12

Sales and Investment fraud

❑ Cyber criminals:

- Targets electronic commerce.
- Advertise attractive investment opportunities by fraudulent operators, duping investors into parting with their money.
- Access to millions of Internet users at minimal costs.

Cyber Crime 11-12

Illegal interception of communication

- ❑ The cyberspace provides new opportunities for electronic eavesdropping.
- ❑ Telecommunication interception has increasing application, from surveillance of individuals to industrial and political espionage.

Cyber Crime 12-12

Electronic funds transfer fraud

❑ Cyber criminals:

- Attack on electronic fund transfer used for banking and retail purchase or business-to-business fund transfers.
- Intercept credit card details, passwords or other digital security information during transmission.
- Misuse to perpetrate fraudulent transactions.

Data Stolen

- ❑ **Data theft:**
  - – Refers to the theft of confidential data of commercial value from a company
  - – Perpetrated by employee(s) of the company with the intention of personal gain through sale of data to competitors of the company

- ❑ **Suitable atmosphere/people for data theft:**
  - – Office workers with access to desktops and hand held devices are naturally suited for such crimes.
  - – Cheap and ready availability of pen/USB drives and other suitable storage.
  - – Employees who steal data without being aware of their crime.

Essential Elements of Information Security 1-2

- **Information security:**
  - Broadly refers to the practice of protecting information from unauthorised access, disclosure, use or destruction.
  - Refers to information irrespective of the medium of storage (electronic as well as non-electronic) in general.
  - Refers to electronically stored and used information only here.

Essential Elements of Information Security 2-2

❑ The domain of information security has two main attributes:

Computer Security

- Is about application of information security to technology, typically computer systems.
- Is mandatory for all major enterprises/organisations, due to the nature and value of data available in such establishments.

Information Assurance

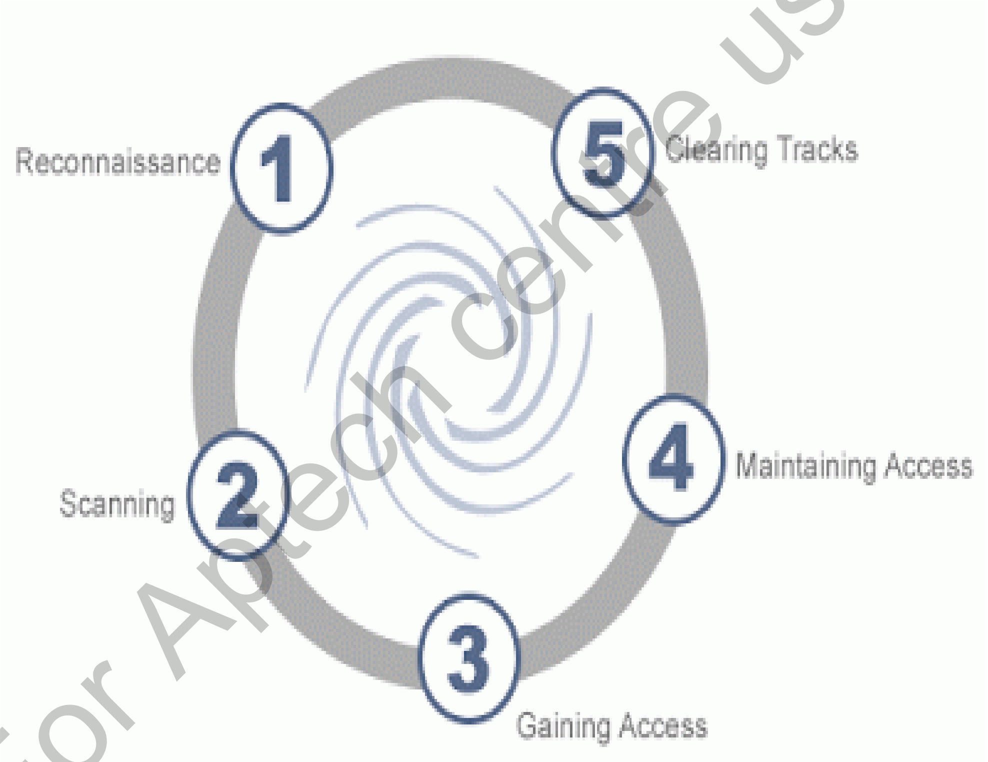
- Is an attribute of information security concerns itself while ensuring that information or data is not lost when critical events take place.
- Is also implemented by IT security specialists.

Ethical Hacking 1-2

- Ethical hacking:
  - Is unauthorised access and use of a computer.
  - Denotes the presence of malevolent intentions.
  - Is an act of breaking into a computer system with the intention of testing the system's vulnerability to attacks by hackers.
  - Helps identify weaknesses in a computer system that might be exploited by hackers.
  - Works as a tool for computer systems security professionals who then work towards eliminating weaknesses in the systems.
  - Is a way of doing a security assessment and fits into the security life cycle.

Ethical Hacking 2-2

- The security life cycle is shown as follows:



Types of Hacking/Hackers 1-12

- ❑ Hackers:
  - Use their skills and capabilities to access the computer system or networks to make some profit in various ways.
  - Have different purposes of hacking the systems and networks.
  - They work differently based on the skills, types of targets, counter measures and so on.

Types of Hacking/Hackers 2-12

- The three main types of hackers are:

White Hats

Black Hats

Gray Hats

Types of Hacking/Hackers 3-12

White Hats

- Use their hacking skills for defensive purposes.
- Are computer security professionals who are employed by enterprises and organisations.
- Perform completely legal activities since they have the enterprise/organisations permission to engage in hacking activities.
- Locate weaknesses in computer systems and implement counter measures.
- Are paid for their services.

Types of Hacking/Hackers 4-12

Black Hats

Are the malicious hackers, also known as 'Crackers', who break into computer systems with malicious intentions.

Access to the computer system in unauthorised way and therefore, illegal.

Hack into computer systems with the intention of stealing information or destroying data or denying service to legitimate users.

Types of Hacking/Hackers 5-12

Gray Hats

Are hackers who may work defensively (ethically) or offensively (unethically), depending on the situation.

May simply be interested in hacking tools and technologies and not have malicious intentions like black hats.

Are self-proclaimed ethical hackers, with academic interest or curiosity for hacking tools and technology.

Types of Hacking/Hackers 6-12

❑ Following are some more categories of hackers:

Elite Hacker

- Is one with a prominent position due to his/her hacking skills.
- Confer such status on their members by their groups.

Script Kiddie

- Is a non-expert, inexperienced hacker who breaks into computer systems by using pre-packaged automated tools written by others.
- Usually have little understanding of the underlying concepts of hacking.

Blue Hat

- Are persons outside computer security consulting firms.
- Conduct bug tests on systems prior to launch, helping to detect and close any weaknesses in the systems before launch.

Hacktivist

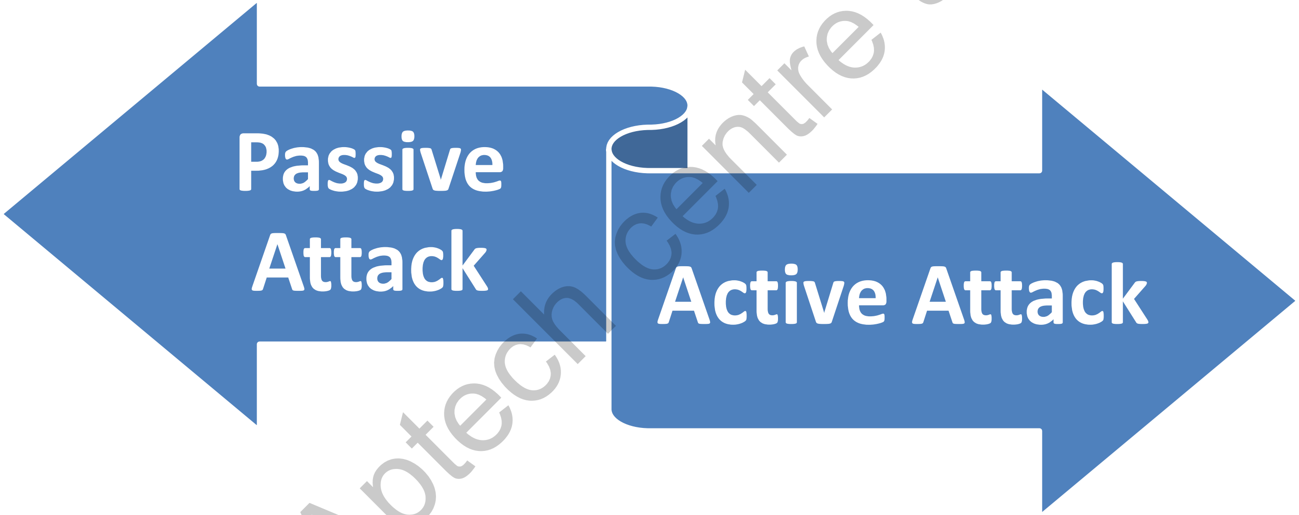
- Is a hacker who utilises technology to announce a social, ideological, religious or political message.
- Involves Website defacement or denial-of-service attacks.

Types of Hacking/Hackers 7-12

- ❑ The Hacking attacks:
  - – Can be classified according to their origin, whether they are conducted using one or more computers.
  - – Can be focused on network elements of host features.
  - – Covered Physical thefts or damage of equipment.
- ❑ When multiple computers are used, it is known as a distributed attack.
- ❑ Botnet is an example of distributed attack.
- ❑ Other criteria for classification of attacks include the procedure used and the type of vulnerability exploited.

Types of Hacking/Hackers 8-12

- ❑ The attacks are broadly classified in to two types:



Types of Hacking/Hackers 9-12

- ❑ **Passive Attack:**

  In this attack, hacker:

  - Monitors unencrypted traffic and search passwords.
  - Logins information and sensitive data that would be useful in some other attacks.
  - Displays information or data files to hacker without the help of user's knowledge.
  - Targets on networks.

    For example: eavesdropping, wire-tapping, port scanning and idle scanning.

Types of Hacking/Hackers 10-12

- The types of passive attacks are:

Traffic analysis monitor

Unprotected communications’ check-up

Decryption of weakly encrypted traffic

Authentication information capture

Types of Hacking/Hackers 11-12

- **Active Attack**:

  In this attack, hacker:

  - Attempts to bypass or break into authorised systems.
  - Uses viruses, stealth, worms or Trojan horses to perform this activity.
  - Harms a network area.
  - Exploit information in data transfer.
  - Penetrates an enclave or attack authorised user on the remote distance.
  - Displays disclosure or distribution of data files, modified data, DoS and so on.

    Examples: Denial-of-Service attacks, spoofing, ARP poisoning, ping flood, ping of death and smurf attacks.

Types of Hacking/Hackers 12-12

- The types of active attack attempts are as follows:

To circumvent or break protection features

To introduce malicious code

To steal or modify information

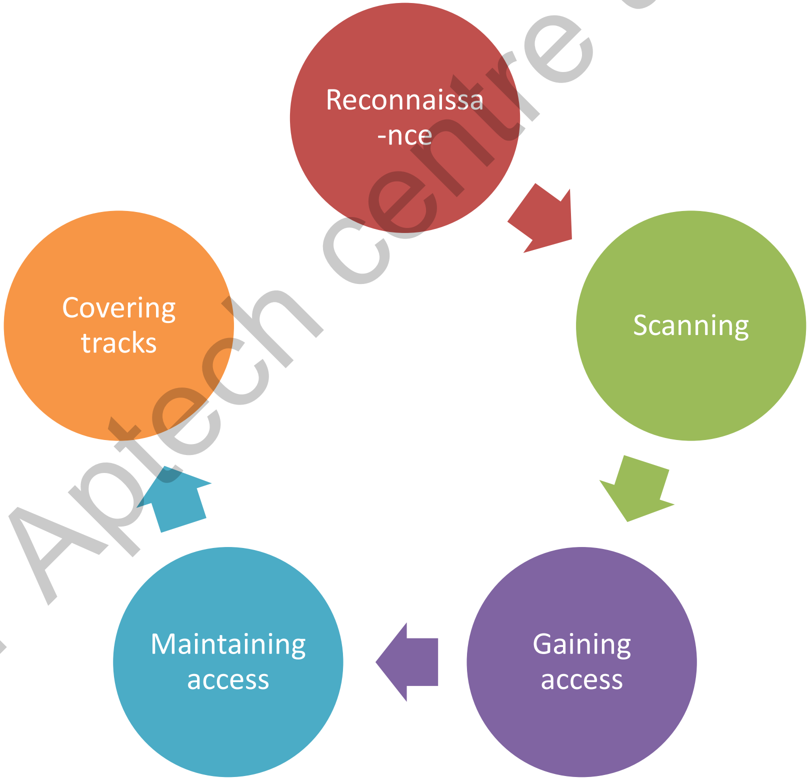
Phases of Ethical Hacking 1-9

❑ The advance in technology has made hacking, an activity that requires advanced skills and a systematic approach/methodology.

❑ The modern-day hacker invariably adopts a methodical approach to hack into targets.

Phases of Ethical Hacking 2-9

- An intruder passes through five phases while progressing through an attack and they are as follows:



Phases of Ethical Hacking 3-9

- **Phase 1 (Reconnaissance)**:
  - A preparatory phase.
  - An attacker gathers information about the target before launching the attack.
  - It involve network scanning, either external or internal, without authorisation.
  - The potential attacker strategises the attack.
  - Part of this reconnaissance may involve social engineering.

Reconnaissance

Phases of Ethical Hacking 4-9

Reconnaissance

- **Dumpster diving**:
  - Is another technique used in reconnaissance.
  - Involves going through an organisation's trash for discarded but still sensitive information.
  - Attackers can use the Internet to gather information such as:
    - employee's contact information
    - names of business partners
    - technologies used and other critical business information

Phases of Ethical Hacking 5-9

Scanning

❑ **Phase 2 (Scanning):**

– A logical extension (and overlap) of the active reconnaissance phase.

Before attacking a network, a hacker:

- Scans the system.
- Uses the details gathered during reconnaissance to identify vulnerabilities.
- Uses automated tools such as network/host scanners and war dialers to locate systems to discover vulnerabilities.
- Gathers critical network information.
- Uses tools such as Cheops and Port scanners.

Phases of Ethical Hacking 6-9

Scanning

- **Phase 2 (Scanning)**:
  - The primary defense technique:
    - Shut down services that are not required.
    - Appropriate filtering.
  - **Vulnerability scanners** are most commonly used tools that:
    - Search for several known vulnerabilities on a target network.
    - Can potentially detect several weak spots in the system.

Phases of Ethical Hacking 7-9

Gaining access

- **Phase 3 (Gaining Access)**:
  - Hackers may not always gain access to the system with the intention of causing damage.
  - Services can be stopped by killing processes, using a logic/time bomb or even reconfiguring and crashing the system.
  - The hacker may cause resources to be exhausted locally by filling up outgoing communication links.
  - The exploit can occur locally, offline, over a LAN or the Internet, as a deception or theft.
  - Examples:
    - Stack-based buffer overflows
    - Denial-Of-Service
    - Session hijacking

Phases of Ethical Hacking 8-9

Maintaining access

❑ Phase 4 (Maintaining Access):

- Attacker can:
  - Choose to use the system as well as its resources.
  - Use the system as a launching pad for scanning and exploiting other systems.
  - Keep a low profile and continue exploiting the system. (Both these actions are harmful for the organisation.)
  - For example: The attacker can use a sniffer to capture all network traffic, including telnet and ftp sessions with other systems.
- To evade detection, attackers:
  - Remove evidence of their entry
  - Use a backdoor or a Trojan to gain repeat access
  - Install rootkits at the kernel level to gain super user access

Phases of Ethical Hacking 9-9

Covering tracks

- **Phase 5 (Covering Tracks)**:

  In this phase, attackers:

  - Destroy evidence of their presence and activities.
  - Erase evidence of a break-in is a necessary requirement for any attacker who would like to remain undetected.
  - Erase the contaminated logins and any possible error messages that may have been generated from the attack process.
  - For example: A buffer overflow attack usually leaves a message in the system log and therefore needs to be removed.

Laws Related to Hacking 1-8

- Following are some of the laws enacted in US to address the issues related to hacking:

- The Computer Fraud and Abuse Act (CFAA)
- The National Information Infrastructure Protection Act
- The Electronic Communications Privacy Act (ECPA)
- Economic Espionage Act (EEA)
- Wire Fraud Act
- The National Stolen Property Act (NSPA)
- Identity Theft and Assumption Deterrence Act (ITADA) [18 U.S.C. Section 1028(a)(7)]

Laws Related to Hacking 2-8

The Computer Fraud and Abuse Act (CFAA):

- Makes it illegal for anyone to distribute computer code or place it in the stream of commerce.
- Addresses code's damage to computer systems and the associated economic losses.
- Provides for criminal penalties for releasing computer viruses into computers used in interstate commerce, either knowingly or recklessly.

  (Anybody convicted under the CFAA will be imprisoned upto 20 years and fined up to $250,000.)

Laws Related to Hacking 3-8

The National Information Infrastructure Protection Act:

- Was made into a law in 1996, significantly amended the CFAA.
- Expanded definition of a ‘protected computer’ to effectively include any computer connected to the Internet.
- Is defined in the original form (damages must reach $5,000, but that requirement is waived if the intrusion obstructs medical care, harms anyone or poses a threat to national security).

Laws Related to Hacking 4-8

The Electronic Communications Privacy Act (ECPA):

- Became a law in 1986, amended the Federal Wiretap Act to account for the increasing amount of communications and data that was transferred and stored on computer systems.
- Provides protection against the unlawful interception of any wire communications.
- Includes protections for stored electronic messages, for example, email messages that are archived on servers.
- Under this law, unauthorised access to computer messages, whether in transit or in storage, is a federal crime.

Laws Related to Hacking 5-8

Economic Espionage Act (EEA):

- Enacted In 1996.
- Has domestic as well as international components and addresses foreign espionage as well as theft of trade secrets.
- Addresses industrial espionage of any kind, both traditional as well as electronic pilferage.

  (Under this act, any downloading, receiving or possession of trade secrets without the explicit permission of its owner(s) is a federal crime.)

Laws Related to Hacking 6-8

Wire Fraud Act:

- Is illegal to fraudulently obtain money or property using an interstate wire communication system.
- Includes the Internet and any other computer-aided system that uses interstate wires (communication system).

Laws Related to Hacking 7-8

The National Stolen Property Act (NSPA):

- Prohibits the transportation in interstate commerce of ‘any goods, wares, securities or money’ valued at $5,000 or more that are known to be stolen or fraudulently obtained.
- Covers computerised transfers of funds.

Laws Related to Hacking 8-8

Identity Theft and Assumption Deterrence Act (ITADA) [18 U.S.C. Section 1028(a)(7)]:

- Passed in 1998 by the US Congress.
- Addresses restitution and relief for the victims.
- Considers all forms of identity theft as crimes and courts can assess the losses suffered by individual consumers.

  (A federal crime to steal any name or number that may be used to identify an individual.)

Necessity for Ethical Hacking 1-3

- ❑ Ethical Hacking and effective information security practices are needed as:
  - Instances of security breaches being increasingly reported all over the world.
  - Enterprises are facing security threats when adopting new technologies such as cloud computing, virtualisation or IT outsourcing.
  - There is a need for a comprehensive, real-world assessment of an organisation’s security position.
- ❑ Ethical Hacking:
  - Is one of the options available to enterprises and organisations in addressing security concerns.
  - Is a means to detect vulnerability of systems and networks.
  - Is increasingly adopted as essential or even standards practice in many organisations.

Necessity for Ethical Hacking 2-3

- The major challenge for businesses worldwide is the complexity of security requirements due to:
  - Changing hacking techniques
  - Evolving business practices
  - Numerous security vulnerabilities
  - Emerging security technologies
  - New business technologies

Necessity for Ethical Hacking 3-3

- ❑ Ethical hackers needs to:
  - Gather information in the course of their work
  - Scan the systems for weaknesses
  - Test entry points
  - Prioritise targets
  - Develop a strategy that utilises their resources optimally

- ❑ In Ethical Hacking:
  - The resulting evaluation of the security preparedness of the target organisation benefits hugely from such objectivity.
  - Effectiveness is used as a means for carrying out an objective analysis of an organisation’s security preparedness and expertise.

Computer Security Incident

- A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies or standard security practices.

- Some examples of computer security incidents are as follows:
  - An attacker commands a botnet to send high volumes of connection requests to a Web server, causing it to crash.
  - Users are tricked into opening a ‘quarterly report’ sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
  - An attacker obtains sensitive data and threatens that the details will be released publicly if the organisation does not pay a designated sum of money.

Penetration Testing

- ❑ Penetration testing:
  - – Is the process of identifying security vulnerabilities in an application by evaluating the system or network with various malicious techniques.
- ❑ The purposes of Penetration testing:
  - – Is to secure important data from hackers who can gain unauthorised access to the systems.
  - – Is to Exploit the weaknesses of the system to gain access to sensitive information.
- ❑ The common causes for vulnerability include:
  - – Design and development errors
  - – Poor system configuration and human errors

Need for Penetration Testing

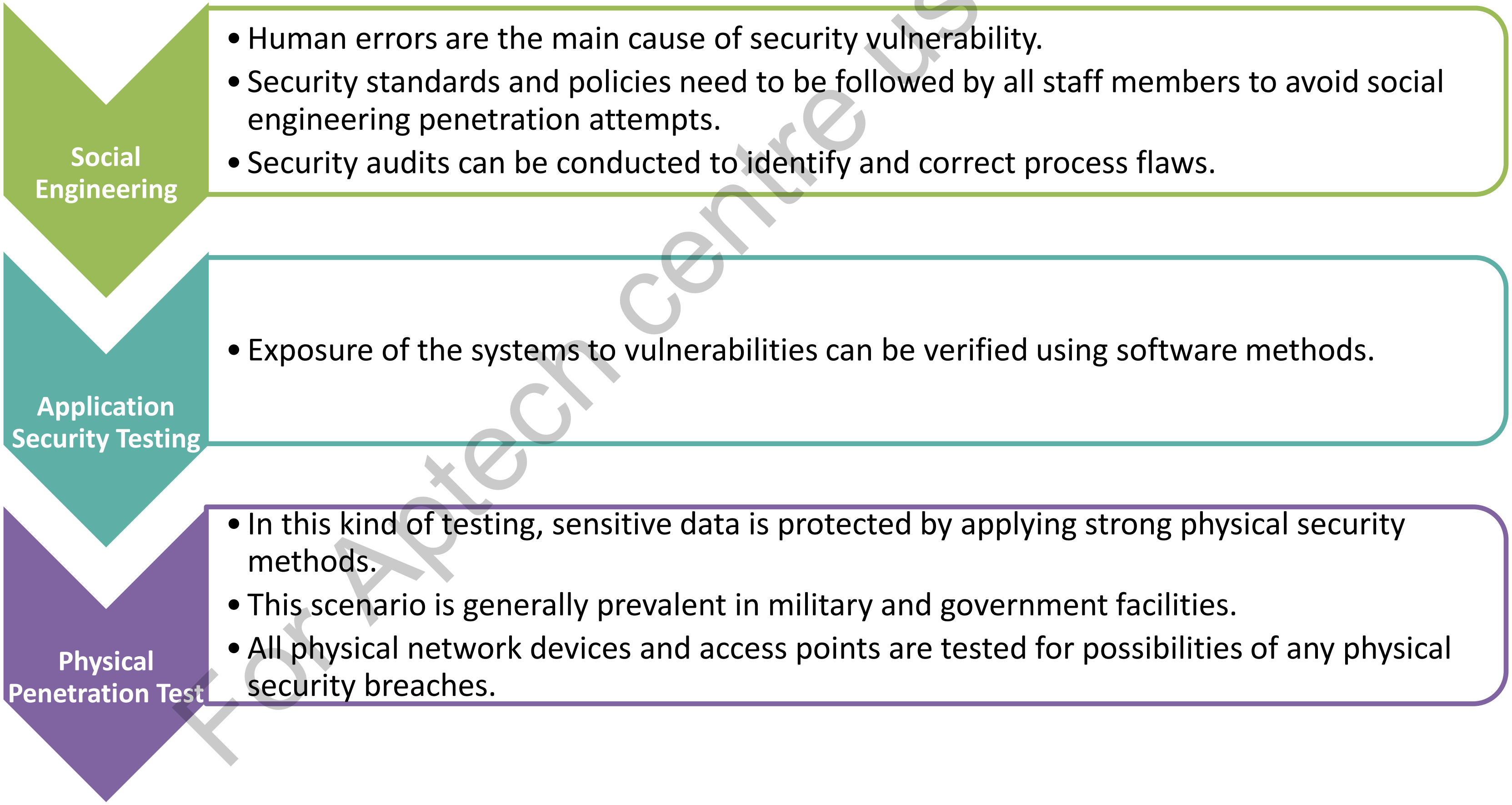
- **Reasons for Penetration Testing:**
  - Some industries and types of data are regulated and must be handled securely (for example, financial sector or credit-card data).
  - A product vendor, such as a Web developer, may have a client who is regulated and therefore, insist on the vendor undergoing a penetration test on their behalf.
  - An organisation may suspect (or know) that its systems have been compromised and may now want to find out more about the threats to its systems, so that it can reduce the risk of another successful attack.
  - An organisation may simply decide to be proactive and find out about the threats to its systems in advance.

Computer Security Incident 1-3

- **What should be tested?**
  - Anything that holds information can be tested.
  - Off-the-shelf products such as servers, smart phones, firewalls and routers.
  - Bespoke software development such as Web sites, mobile applications and games.
  - Telephone equipments such as exchanges, smart phones, VOIP and fax servers.
  - Wireless systems such as WIFI networks, RFID tokens and contactless cash.
  - Physical protection such as CCTV, door entry systems and mechanical locks.

Computer Security Incident 2-3

❑ Types of Penetration Testing:



Social Engineering

- Human errors are the main cause of security vulnerability.
- Security standards and policies need to be followed by all staff members to avoid social engineering penetration attempts.
- Security audits can be conducted to identify and correct process flaws.

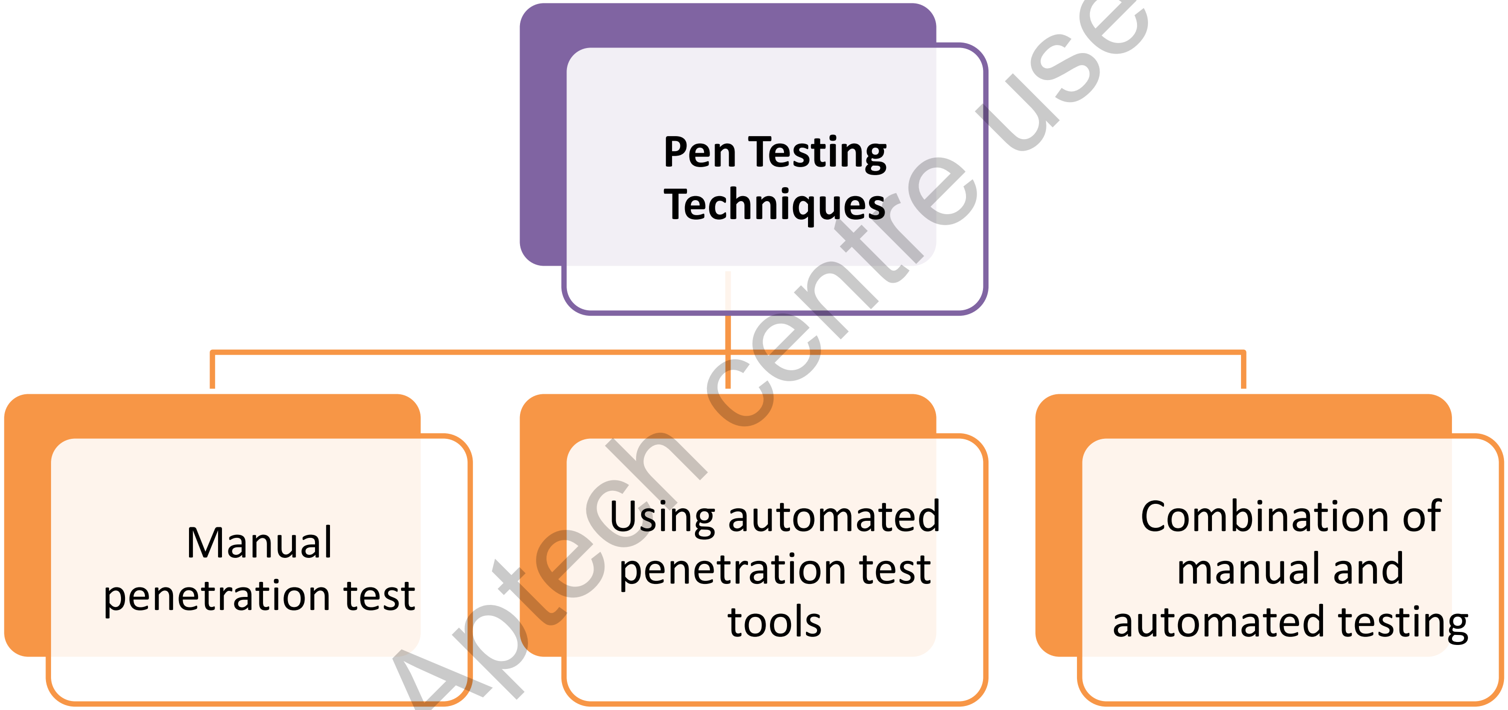
Application Security Testing

- Exposure of the systems to vulnerabilities can be verified using software methods.

Physical Penetration Test

- In this kind of testing, sensitive data is protected by applying strong physical security methods.
- This scenario is generally prevalent in military and government facilities.
- All physical network devices and access points are tested for possibilities of any physical security breaches.

Computer Security Incident 3-3


Pen Testing Techniques
Manual penetration test
Using automated penetration test tools
Combination of manual and automated testing

Penetration Testing Methodology 1-8

- ❑ Penetration testing:
  - Is a complex set of activities and requires a methodical approach.
  - Can be done independently or as a part of an IT security risk management process that may be incorporated into a regular development lifecycle.
- ❑ The methodology:
  - A road map with proven practices and practical ideas.
- ❑ The output:
  - Contains a report which is divided into several sections addressing the weaknesses found in the current state of a system, followed by their countermeasures and recommendations.

Penetration Testing Methodology 2-8

- The two most widely accepted approaches to penetration testing are:

Black Box

White Box

Penetration Testing Methodology 3-8

Black Box

- Is also known as External Testing.
- Helps assesses the network infrastructure from a remote location to the security auditor.
- Is not aware of any internal technologies deployed by the concerned organisation.
- Employ a variety of real world hacker techniques.
- follow through organised test phases.
- May reveal some known and unknown set of vulnerabilities which may otherwise exist on the network.

Penetration Testing Methodology 4-8

Black Box

- An auditor dealing with black-box testing is also known as a black-hat.
- An auditor should understand and classify the vulnerabilities according to their level of risk (low/medium/high).
- The risk can be measured according to the threat imposed by the vulnerability and the financial loss.
- Once the test process is completed, a report is generated with all the necessary information regarding:
  - The target security assessment
  - categorising and translating the identified risks into the business context

Penetration Testing Methodology 5-8

White Box

- Is also referred to as Internal Testing.
- Helps auditor to be aware of all the internal and underlying technologies used by the target environment.
- opens up a wide window to view and critically evaluate the security vulnerabilities with minimum possible efforts.
- Brings more value to the organisation as compared to the black box approach
- Eliminates any internal security issues lying at the target infrastructure environment
- Makes it more difficult for malicious adversaries to infiltrate from the outside.

Penetration Testing Methodology 6-8

White Box

- An auditor engaged with white-box testing is also known as a white-hat.
- The number of steps involved in white-box testing is similar to that of black-box testing (except that the use of the target scoping, information gathering and identification phases can be excluded).
- Moreover, the white-box approach can easily be integrated into a regular development lifecycle.
- It eliminate any possible security issues at an early stage before they get detected and exploited by intruders.
- The time and cost required to find and resolve the security vulnerabilities is comparably less than in the black-box approach.

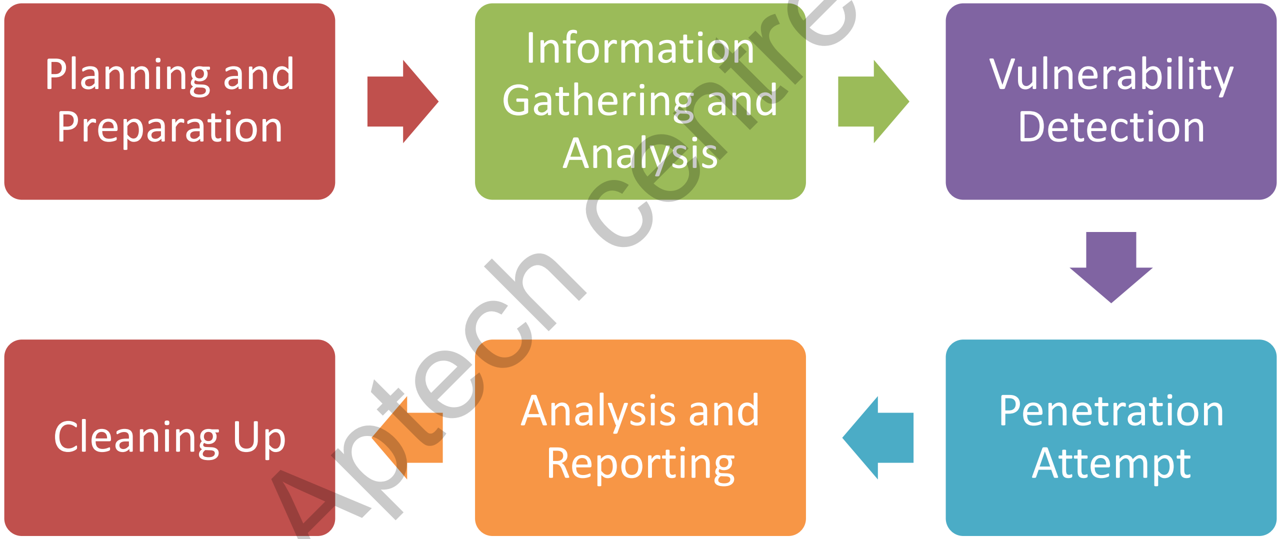
Penetration Testing Methodology 7-8

Gray Box

- **Combination of White Box and Black Box:**
  - Provides a powerful insight for internal and external security viewpoints.
  - Is known as Grey Box testing and the auditor engaged with Gray Box testing is also known as a Grey Hat.
- **Gray Box testing:**
  - Is a set of advantages posed by both approaches.
  - Requires an auditor with limited knowledge of an internal system to choose the best way to assess its overall security.
  - Can help in making better decisions and test choices as the auditor is informed and aware of the underlying technology.

Penetration Testing Methodology 8-8

- The process of penetration consists of six stages and they are as follows:



Summary 1-2

- ❑ Cyber crime is increasingly becoming common and sophisticated with development of new technologies.

- ❑ Ethical hacking is gaining importance in the fight against cyber crime and has become indispensable as a means to protect establishments against hacking.

- ❑ Ethical hacking refers to the act of breaking into a computer system with the intention of testing the system’s vulnerability to attacks by hackers.

- ❑ Ethical hacking helps identify weaknesses in a computer system that might be exploited by hackers.

Summary 2-2

- ❑ A hacker passes through five phases while hacking into a system and they as follows:
  - Reconnaissance
  - Scanning
  - Gaining access
  - Maintaining access
  - Covering tracks
- ❑ There are laws in every country of the world that deal with cyber crimes.
- ❑ The process of Penetration testing progresses through six stages and they are as follows:
  - Planning and Preparation
  - Information Gathering and Analysis
  - Vulnerability Detection
  - Penetration Attempt
  - Analysis and Reporting
  - Cleaning up