Parul® University

Fundamentals of Information Security

Prof. Jigar Gajjar
Certified Ethical Hacker (EC-Council), ISO 27001 ISMS Lead Auditor
CSE – Cybersecurity

Parul®
University

DIGITAL LEARNING CONTENT

CHAPTER-1

Introduction

Parul®
University

DIGITAL LEARNING CONTENT

Why is this unit required?

- Fundamental understanding of cybersecurity and ethical hacking.
- Recognize the significance of protecting digital assets and data.
- Relate the CIA Triad to data and information protection.
- Describe security architecture.
- Define security governance and its importance.
- Understand its role in identifying vulnerabilities and ensuring compliance.
- Gain knowledge of cybersecurity regulations and frameworks.
- Define ethical hacking and its objectives.
- Differentiate between black hat, white hat, and gray hat hackers. Understand the systematic approach for vulnerability identification.
- Understand the systematic approach for vulnerability identification.
- Define penetration testing and its significance.
- Describe white box, black box, and gray box testing.

What is Cyber Security?

- Cybersecurity is the state or process of protecting and recovering computer systems, networks, devices, and programs from any type of cyber attack. Cyber attacks are an increasingly sophisticated and evolving danger to your sensitive data, as attackers employ new methods powered by social engineering and artificial intelligence (AI) to circumvent traditional data security controls.

OR

- Cybersecurity is the practice of securing system devices, network and data that are in the electronic form/ systems.

What is Information Security?

- Information security is “the state of the well-being of information and infrastructure in which the possibility of theft, tampering, or disruption of information and services is kept low or tolerable.”

OR

- Information security refers to the protection or safeguarding of information and information systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction.

- Information Security is the protection of the information available in the electronic systems and physical form.
- Infosec deals with information, regardless of its format (it encompasses paper documents, digital and intellectual property in people's minds, and verbal or visual communications.

Parul® University

DIGITAL LEARNING CONTENT

What is Information Security?

- Information security, sometimes shortened to **InfoSec**, is the practice of protecting information by mitigating information risks. It is part of information risk management.

OR

- Information security refers to the protection or safeguarding of information and information
  systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction.

What is Data and Information?

- **Data** is a collection of raw, unorganised facts and details like text, observations, figures, symbols and descriptions of things etc.
- In other words, data does not carry any specific purpose and has no significance by itself. Moreover, data is measured in terms of bits and bytes – which are basic units of information in the context of computer storage and processing.

- **Information** is processed, organised and structured data. It provides context for data and enables decision making. For example, a single customer's sale at a restaurant is data – this becomes information when the business is able to identify the most popular or least popular dish.

Difference between data and information?

Data	Information
Data is unorganised and unrefined facts	Information comprises processed, organised data presented in a meaningful context
Data is an individual unit that contains raw materials which do not carry any specific meaning.	Information is a group of data that collectively carries a logical meaning.
Data doesn't depend on information.	Information depends on data.
Raw data alone is insufficient for decision making	Information is sufficient for decision making
An example of data is a student's test score	The average score of a class is the information derived from the given data.

Difference between Cybersecurity & Information Security

Cybersecurity?

- Network Security
- Application Security
- Cloud Security
- Critical Infrastructure

Information Security?

- Inclusive of Cybersecurity &..
- Procedural Controls
- Access Controls
- Technical Controls
- Compliance Controls

Parul® University

DIGITAL LEARNING CONTENT

Difference between Cybersecurity & Information Security

Parameters	CYBER SECURITY	INFORMATION SECURITY
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.
Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Defense	Acts as first line of defense.	Comes into play when security is breached.

Need for Cybersecurity

Cybersecurity is important because it protects all categories of data from theft and damage.

- Evolution of technology, focused on ease of use
- Rely on the use of computers for accessing, providing, or just storing information
- Increased network environment and network-based applications
- Direct impact of security breach on the corporate asset base and goodwill
- Increasing complexity of computer infrastructure administration and management

Need for Cybersecurity

- **Rising Cyber Threats:** The proliferation of cyber threats poses a growing risk to the security and integrity of digital systems and data.
- **Intellectual Property Protection:** Safeguarding intellectual property is crucial due to the risk of cyberattacks leading to IP theft or compromise.
- **Disruption of Operations:** Cybersecurity incidents can disrupt business operations, causing downtime and productivity loss.
- **Human Error Vulnerabilities:** Human mistakes play a significant role in cybersecurity incidents, highlighting the importance of training and awareness.
- **Reputation Damage:** Cybersecurity breaches can severely damage an individual's or organization's reputation and trustworthiness in the eyes of the public.

Need for Cybersecurity

- **Economic Costs:** Theft of intellectual property, corporate information, disruption in trading, and the cost of repairing damaged systems.
- **Regulatory Costs:** GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes.
- **Supply Chain Vulnerabilities:** Organizations are interconnected through supply chains, and a breach in one organization can affect others in the chain, causing a ripple effect.

Security Assurance: CIA TRIAD

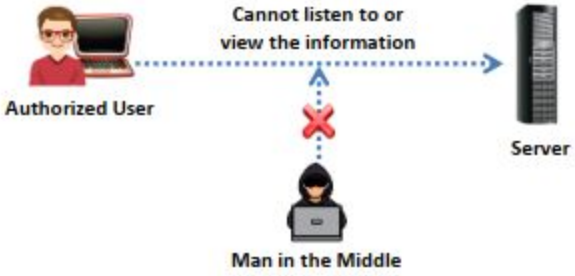
- Information assurance (IA) principles act as enablers for an organization's security activities to protect and defend its network from security attacks.
- They facilitate the adoption of appropriate countermeasures and response actions upon a threat alert or detection. Therefore, network operators must use IA principles to identify data that is sensitive, and to counter events that may have security implications for the network.

- Information assurance is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information.

Security Assurance: CIA TRIAD

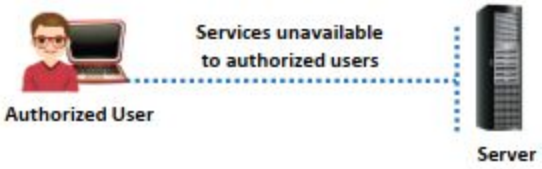
Confidentiality

- Ensures information is not **disclosed** to unauthorized parties



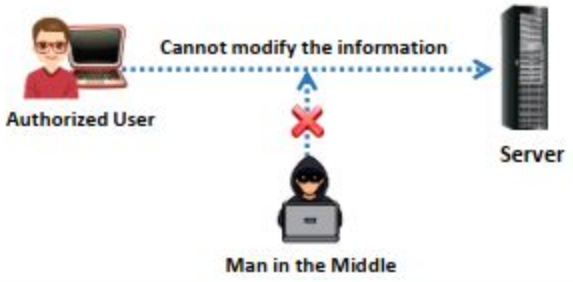
Availability

- Ensures information is **available** to authorized parties without any disruption



Integrity

- Ensures information is not **modified** or **tampered** with by unauthorized parties



Security Assurance: CIA TRIAD

Non-repudiation

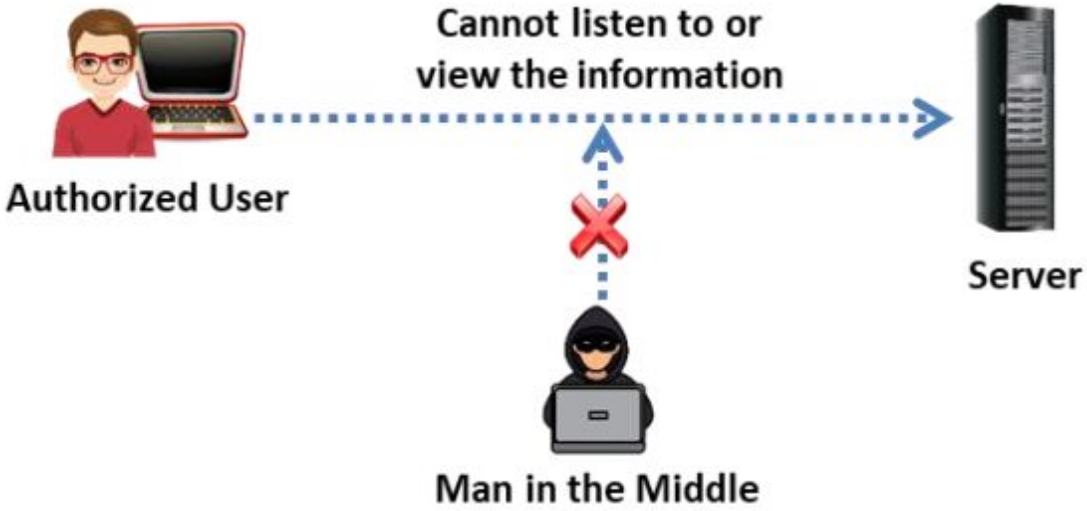
- Ensures that a party in a communication cannot deny **sending** the message

Authentication

- Ensures the **identity** of an individual is verified by the system or service

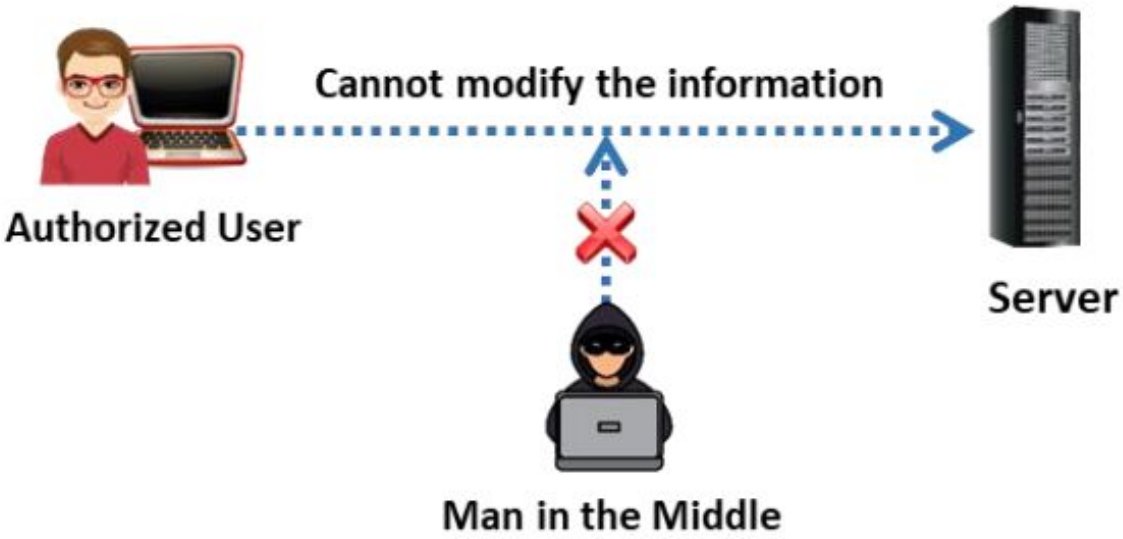
Security Assurance: CIA TRIAD

Confidentiality: Confidentiality permits only authorized users to access, use or copy information. Authentication is crucial for confidentiality. If an unauthorized user accesses protected information, it implies that a breach of confidentiality has occurred.



Security Assurance: CIA TRIAD

Integrity: Integrity protects data and does not allow modification, deletion, or corruption of data without proper authorization. This information assurance principle also relies on authentication to function properly.



Security Assurance: CIA TRIAD

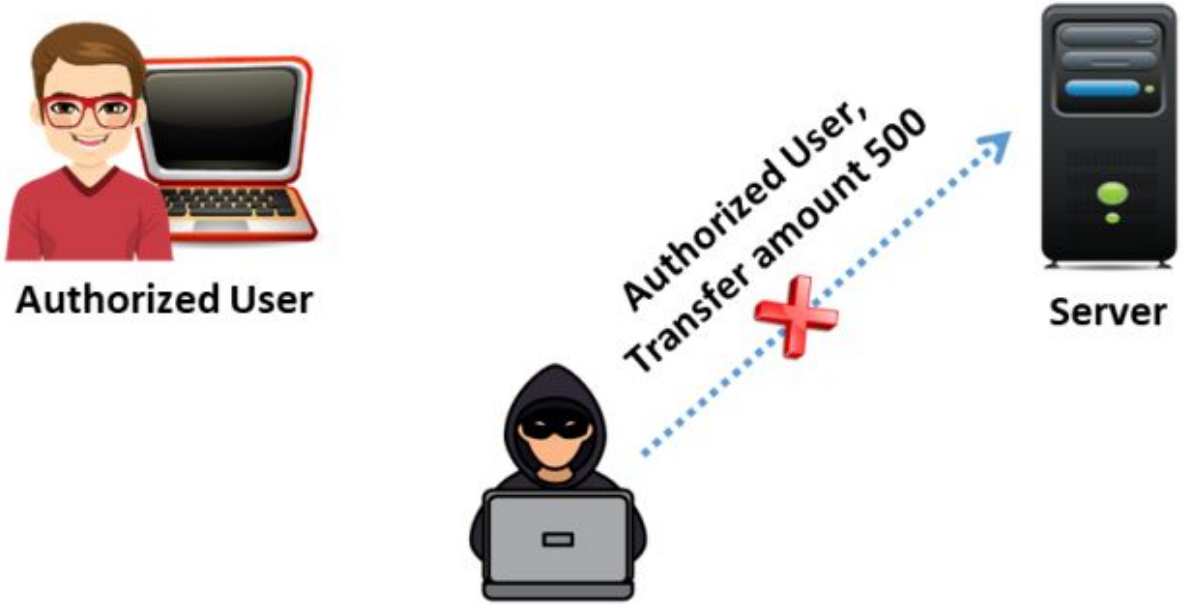
Availability: Availability is the process of protecting information systems or networks that store sensitive data, to make them available for the end users whenever they request access.

Security Assurance: CIA TRIAD

Non-repudiation: Non-repudiation is a service that validates the integrity of a digital signature's transmission, starting from where it originated to where it arrived. Non-repudiation grants access to protected information by validating that the digital signature is from the intended party.

Security Assurance: CIA TRIAD

Authentication: Authentication is a process of authorizing users with the credentials provided, by comparing them to those in a database of authorized users on an authentication server, to grant access to the network. It guarantees that the files or data passing through the network is safe.



Hacking

- Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to a system's resources.
- It involves modifying system or application features to achieve a goal outside of the creator's original purpose.
- Hacking on computer networks is generally done using scripts or other network programming.
- Network hacking techniques include creating viruses and worms, performing denial-of-service (DoS) attacks, establishing unauthorized remote access connections to a device using Trojans or backdoors, creating botnets, packet sniffing, phishing, and password cracking.

Ethical Hacking

- Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data.
- Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers.
- This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

Who is Hacker?

- An intelligent individual with excellent computer skills who can create and explore computer software and hardware.
- For some hackers, hacking is a hobby to see how many computers or networks they can compromise.
- Some hackers' intentions can either be to gain knowledge or to probe and do illegal things

What is Ethical Hacker?

- Hackers identify and exploit gaps and weaknesses in computer systems.
- Ethical hackers identify the same weaknesses, but do so with the intention of fixing them.
- The roles of malicious hacker and ethical hacker require similar skills, traits, and techniques, but their motivations are quite different.

Types of Hackers

Black Hat:
Criminal
Hackers

White Hat:
Authorized
Hackers

Gray Hat:
"Just for Fun"
Hackers

Green Hat:
Hackers-in-Training

Blue Hat:
Authorized
Software Hackers

Red Hat:
Government-Hired
Hackers

Types of Hackers

Black Hat: These are cybercriminals. Black hat hackers attack vulnerabilities with malicious intent.

White Hat: Also known as security specialists, white hat hackers look for the same vulnerabilities as black hats but determine how to fix the issues and prevent future attacks. Sometimes, black hats become white hats.

Gray Hat: Gray hats have mixed motivations. They enjoy hacking and often do so without authorization, but they don’t act maliciously. Grey hats often view hacking as sport.

Types of Hackers

Blue Hat: Tech companies hire blue hat hackers to test products and find security issues. Microsoft hosts an annual BlueHat convention.

Red Hat: Also known as vigilante hackers, red hats act aggressively to stop the black hats and employ some of their strategies. Government agencies hire red hats for their mission focus.

Green Hat: These are the hacking beginners who want to become white, blue, or red hats (but hopefully not black hats). How do they learn? Let's take a look.

Phases of Ethical Hacking

In general, there are five phases of hacking:

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing Tracks

Phases of Ethical Hacking: Reconnaissance

- Reconnaissance is the first phase of ethical hacking, also known as the footprinting and information gathering phase.
- This is the preliminary phase where white hat hackers gather as much information as possible and implement security measures into the targeted system or network.
- The information gathered by white hat hackers usually is about three groups: network, host, and people.

Phases of Ethical Hacking: Reconnaissance (Information you can get)

1. **Network Information:** IP addresses, Subdomains, Open ports: Determine open ports and running services.
2. **Organizational Information:** Company details
3. **Employee information:** Find key personnel, roles, and contact details.
4. **Domain Information:** Domain registration details
5. **DNS records:** Gain insights into domain structure and mail servers.
6. **Server and Service Information:** Server banners
7. **Service versions:** Identify software and service versions.
8. **Social Media Information:** Employee profiles and connections
9. **Email Addresses**
10. **Security Information:** Security measures: Determine security technologies and potential vulnerabilities.
11. **Vulnerabilities:** Identify known software vulnerabilities.
12. **Technology Stack:** including CMS, web frameworks, and databases.

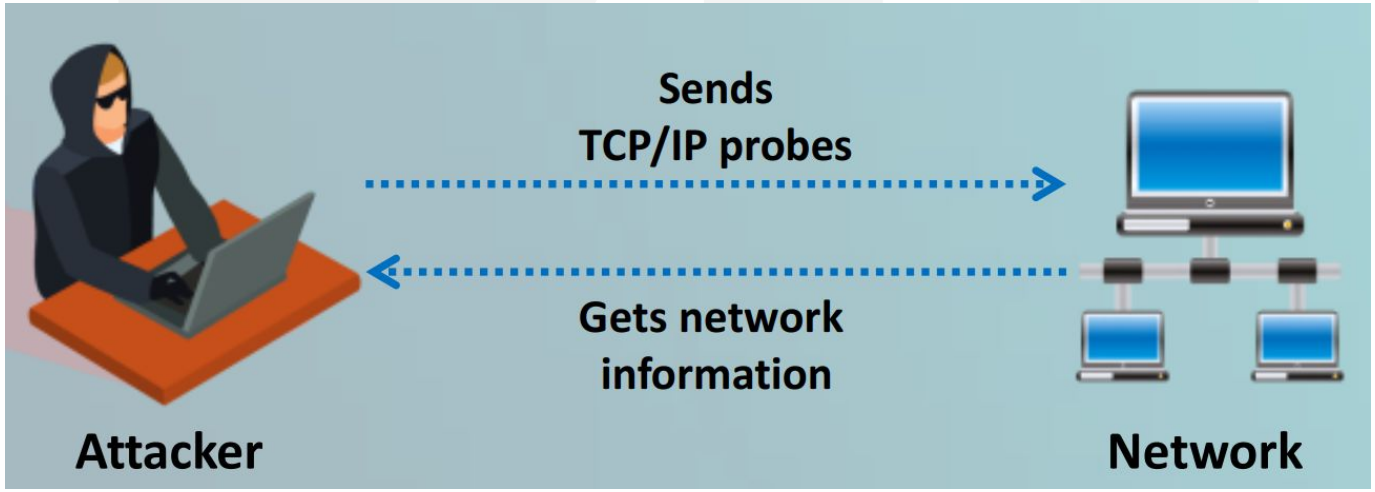
Phases of Ethical Hacking: Reconnaissance Types

1. **Active footprinting:** Communicate with the target directly to gather information about the target.

2. **Passive footprinting:** Seeking to get information about the target without gaining direct access to the target. Hackers exploit social media, public websites, and other public resources.

Phases of Ethical Hacking: Scanning

- The scanning phase is the second step in an ethical hacker's methodology. It entails applying all the knowledge learned during the reconnaissance phase to the target location to search for vulnerabilities. Hackers search for data such as user accounts, credentials, IP addresses, etc.



Phases of Ethical Hacking: Scanning Types

- There are three types of scanning, which include:
- **Port scanning:** During this stage, the target is scanned for data such as open ports, live systems, and other services active on the host.
- **Vulnerability scanning:** This scanning technique identifies a target's vulnerabilities and weak points and attempts to exploit those bugs in various ways. It is carried out using automated tools such as Netsparker, OpenVAS, Nmap, and others.
- **Network scanning:** This method includes locating the organization's firewall and other routers and networks to assist them in their hacking operations.

Phases of Ethical Hacking: Gaining Access

- In this phase, the hacker creates the blueprint for the target's network using the data gathered in Phases 1 and 2. Now the hacker has all of the information he requires. So he creates the network map and decides how to carry out the attack? There are various alternatives, such as:
- Phishing attacks
- Brute force attack
- Spoofing attack
- Man in the middle attack
- Dos attack
- Session hijacking
- Buffer overflow attacks

Phases of Ethical Hacking: Maintaining Access

- When a hacker gains access, they choose to maintain it for future exploitation and attack. In addition, the hacker gains access to the organization's Rootkits and Trojans and utilizes them to execute more network attacks. An ethical hacker attempts to keep access to the target until they have completed the activities or intend to complete in that target.

Phases of Ethical Hacking: Clearing Tracks

Once a hacker has obtained access, they leave no trace to prevent detection by the security team. They execute this by deleting cache and cookies, interfering with log files, and closing all open ports. This incorporates some of the steps an ethical hacker uses to cover and eliminate their footprint.

- Deleting/corrupting all logs
- Changing the values of logs or registries
- Removing all of the folders established by the ethical hacker
- Uninstalling all the applications

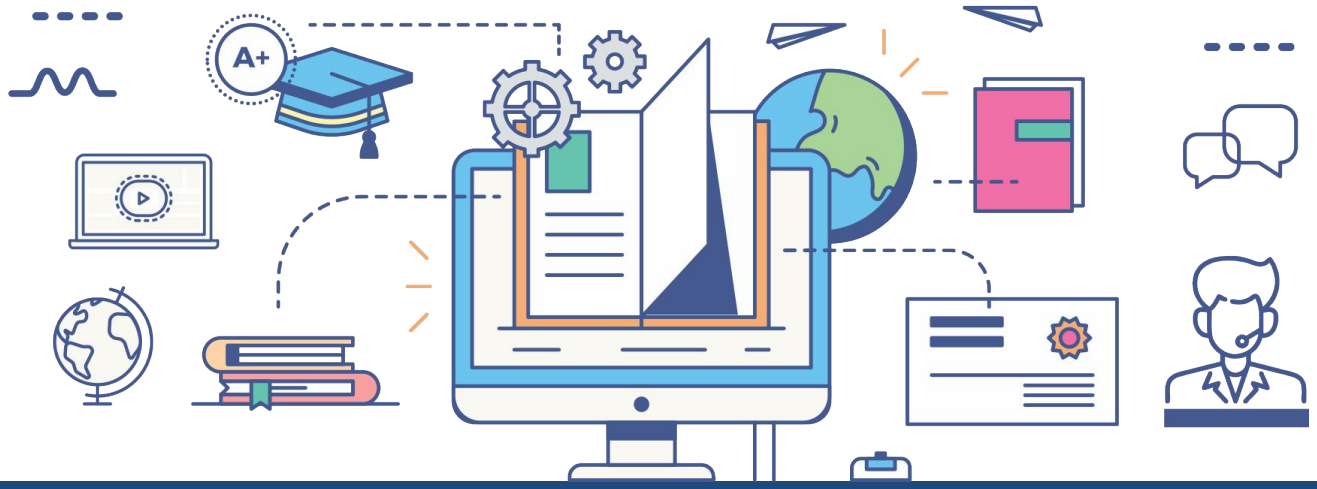
Ethical hackers use the following methods to hide their tracks in ethical hacking:

- Using reverse HTTP shell
- Tunneling with ICMP (Internet Control Message Protocol)

References

1. https://www.synopsys.com/glossary/what-is-ethical-hacking.html
2. https://www.eccouncil.org/cybersecurity/what-is-ethical-hacking/
3. https://bootcamp.du.edu/blog/the-complete-guide-to-ethical-hacking/
4. https://byjus.com/biology/difference-between-data-and-information/
5. https://mrcet.com/downloads/digital_notes/EEE/CyberSecurity.pdf
6. https://www.slideshare.net/LuisHerrera199/introduction-to-cybersecurity-fundamentals

DIGITAL LEARNING CONTENT



Parul® University

www.paruluniversity.ac.in