TECHNOLOGY & THEORY

Cyber Security Fundamentals

By: Saad Aslam – Founder Tech Tology

Covered Today

A brief outline

What is Cyber?
Cyber Security Domains
Basic Terms and Terminologies of Security
Cyber Security Certifications
Network Models
Ethical Hacking and Pentesting
Cyber Threats
Getting Familiar to Kali Linux

Things to Understand

What is the meaning of Cyber
What is Cyber Security
What is the need of Cyber Security

Meaning of Cyber

- Cyber means anything that is digital.
- It can be your devices that are performing digital computation
- How big Cyber Space is?

What Is Cyber Security

- The term cyber security is used to refer to the security offered through on-line services to protect your online information
- Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals
- Though, cyber security is important for network, data and application security

Need for Cyber Security

- Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses
- With an increasing amount of people getting connected to Internet, the security threats that cause massive harm are increasing also.

Ransome Ware Attack

Things you should know

- First known Computer Virus?
- The first known computer virus appeared in 1971 and was dubbed the “**Creeper virus”.**
- The Creeper virus was eventually deleted with a program known as “**The Reaper”,** but it is important to note that the Reaper was actually a virus itself

Domains of Cyber Security

1. Access Control Systems and Methodology
2. Telecommunications and Network Security
3. Business Continuity Planning and Disaster Recovery Planning
4. Security Management Practices
5. Security Architecture and Models
6. Law, Investigation, and Ethics
7. Application and Systems Development Security
8. Cryptography
9. Computer Operations Security
10. Physical Security

Access Controls

Access controls authenticate and authorize individuals to access the information they are allowed to see and use

1. Something you know - (you know passwords)
2. Something you are - (biometric scan)
3. Something you have - (ATM card)
4. Something you do - (signature style)

CIA

- **Confidentiality:** It ensures that computer-related assets are accessed only by authorized parties sometimes called **secrecy** or **privacy**
- Technique used is **Encryption**
- Suppose we want to word “HELLO” ,we can apply encryption technique to replace every alphabet of HELLO with its neighbor alphabet like H replace with I ,E with F etc which makes the word not meaningful. Then we decrypt with the same technique used on other side

Encryption & Decryption

Encryption

Strongest line of defense in a layered security strategy

- Encryption is the process of making data unreadable and unusable to unauthorized users.
- To use or read the encrypted data ,it must be decrypted ,which requires the use of a secret key.
- There are two top-level types of encryption: **symmetric** and **asymmetric**.

Symmetric Encryption

- Uses the Same Key to encrypt or decrypt data.
- Consider a desktop password manager application. You enter your password and they encrypted with your own personal key. When the data is to be retrieved ,the same key is used, and the data is decrypted.

Asymmetric Encryption

- Uses a public key and private key pair.
- Either key can encrypt but a single key can’t decrypt its own decrypted data.To decrypt, you need the paired key.
- Asymmetric encryption is used for things like Transport Layer Security(TLS) used in HTTPS and data signing

Approaches of Encryption

ENCRYPTION AT REST

ENCRYPTION AT TRANSIT

CIA

- **Integrity:** It means that assets can be modified only by authorized parties or only in authorized ways.
- Technique used is **Hash**
- **Hash: Hash Calculator** which takes file as input and apply algorithm .The purpose of hashing is to show that the original file is not modified

Microsoft File Checksum Integrity Verifier

Important! Selecting a language below will dynamically change the complete page content to that language.

Language: **English**

Download

The Microsoft File Checksum Integrity Verifier tool is an unsupported command line utility that computes MD5 or SHA1 cryptographic hashes for files.

- Details
- System Requirements
- Install Instructions
- Related Resources

Hashing

Plaintext

Hash Function

Hashed text

CIA

Availability: It means that assets are accessible to authorized parties at appropriate times.
DOS (Denial of Service Attack)

Ping Command

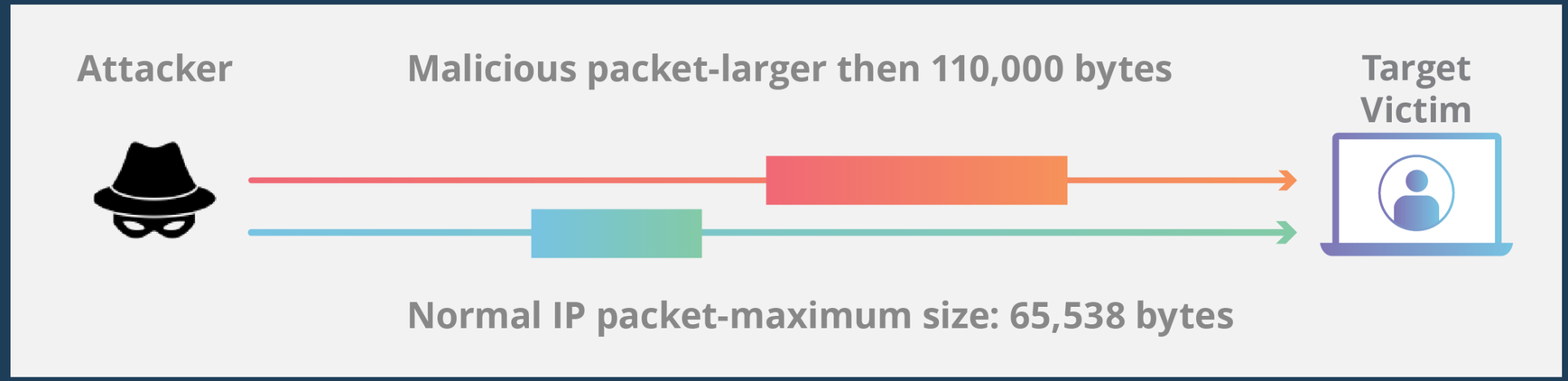
- Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network
- A simple way to verify that a computer can communicate over the network with another computer or network device
- Ping 127.0.0.1 (127.0.0.1 is a loopback address)

DOS Attacks

- Ping of Death
- Ping of Flood
- Smurf Attack
- Fraggle Attack

Ping of Death

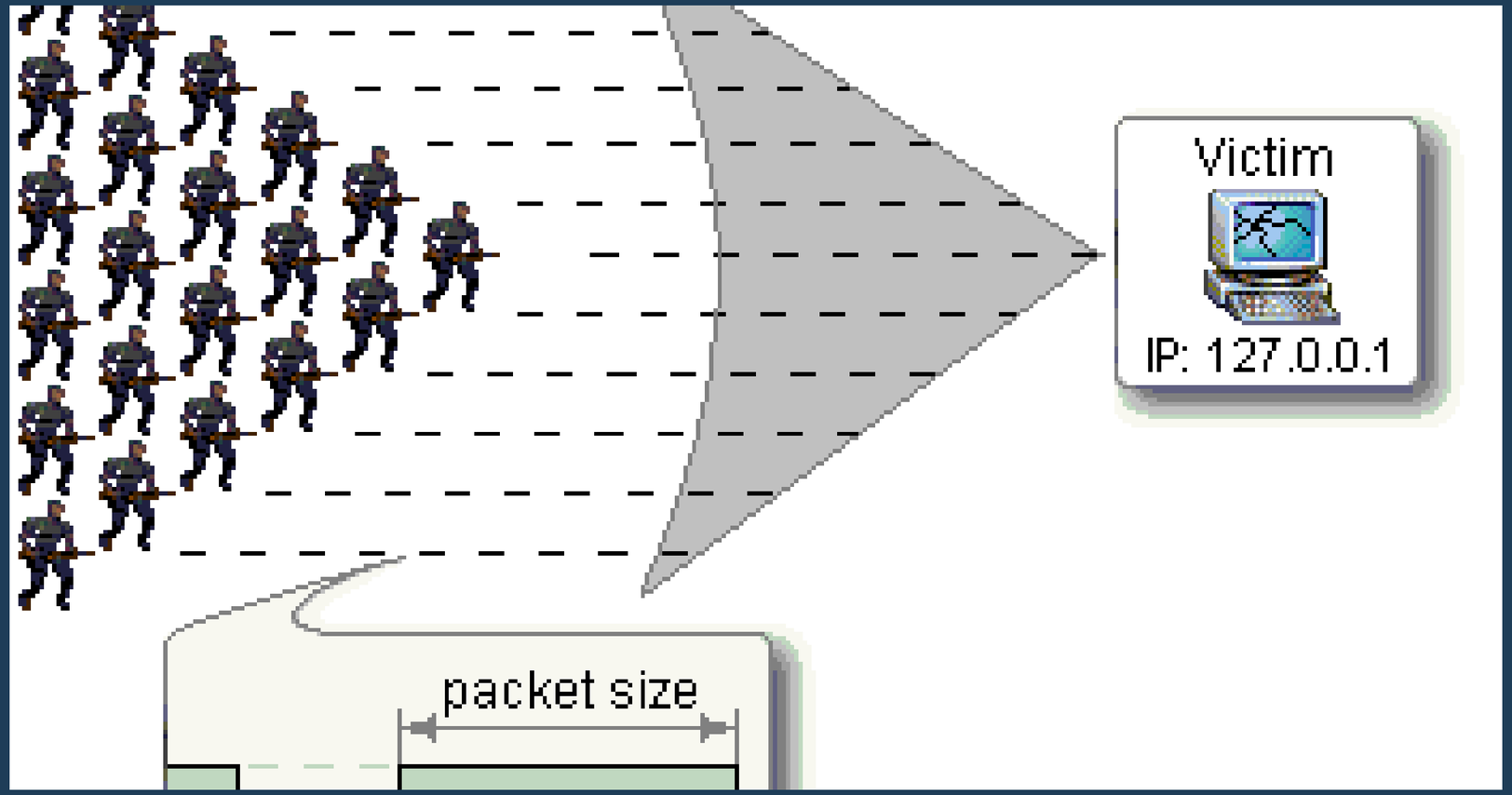
A Ping of Death attack is a denial-of-service (DoS) attack, in which the attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash



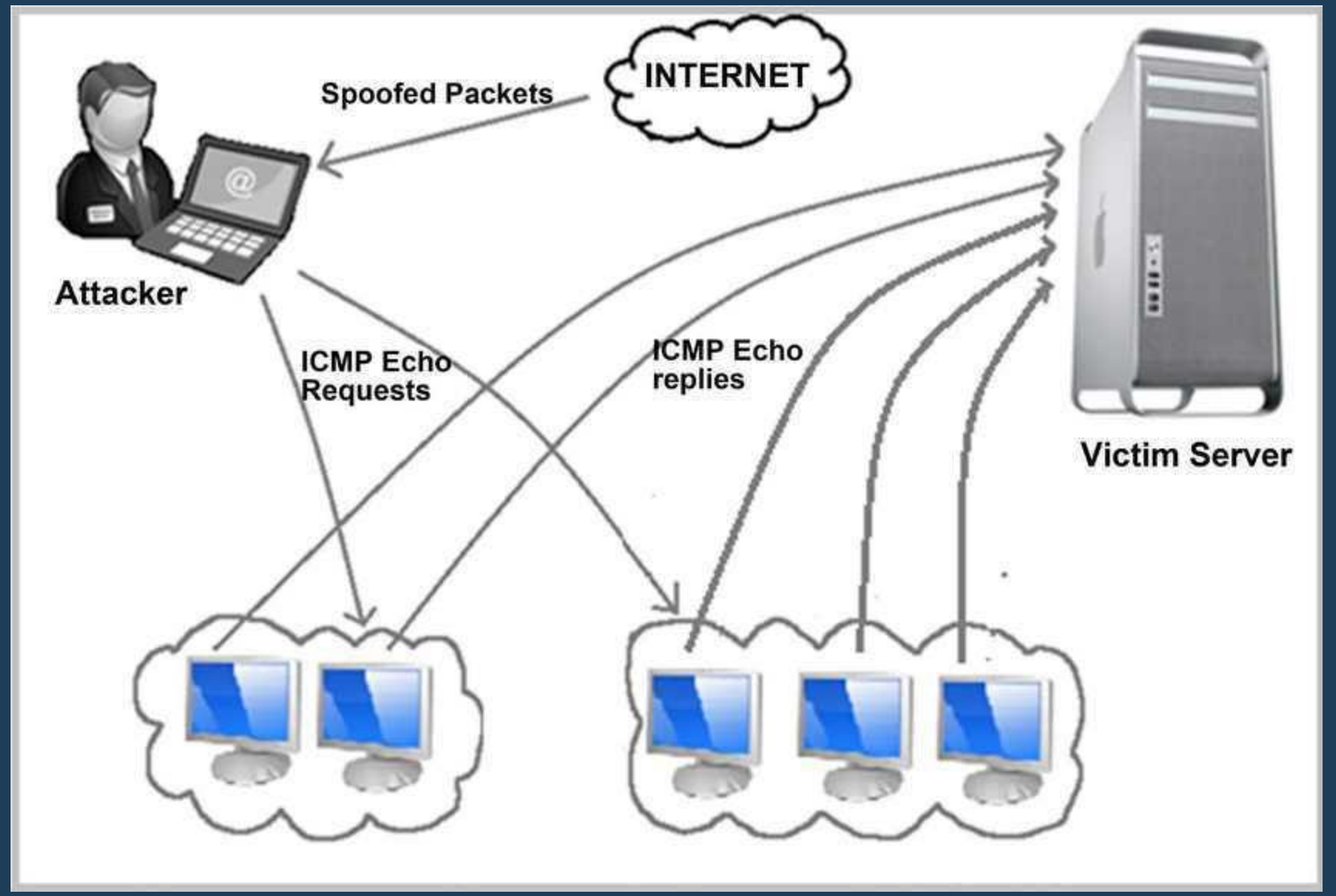
Ping of Flood

- Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim’s computer by overwhelming it with ICMP echo requests, also known as pings.
- Example: Education Board Website

Ping of Flood



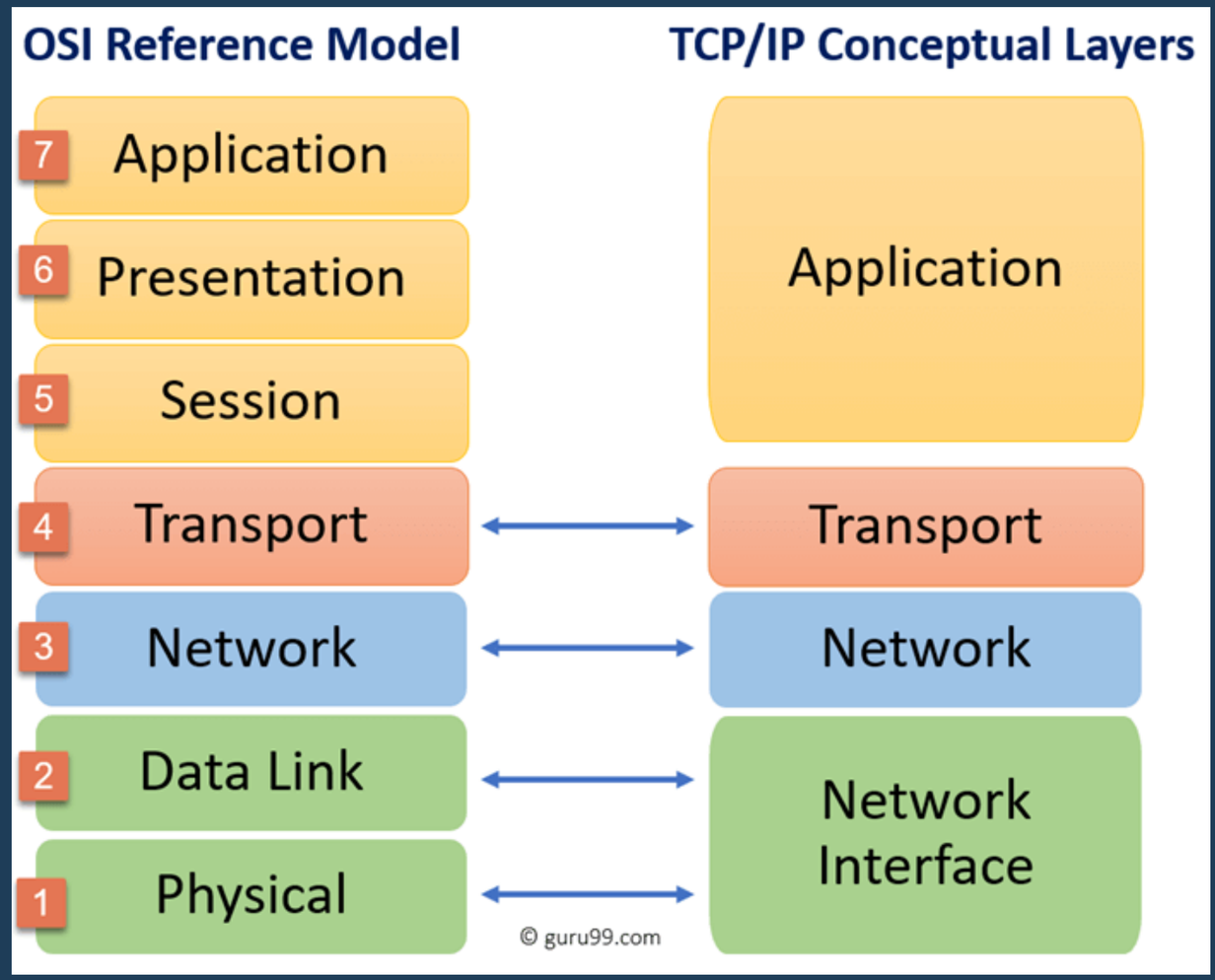
Fraggle Attack



Telecommunications

Focuses on communications, protocols, and network services, and the potential vulnerabilities associated with each.
Protocols:
1. TCP/IP
2. OSI Model

OSI VS TCP/IP


OSI Reference Model
TCP/IP Conceptual Layers
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Application
Transport
Network
Network Interface
© guru99.com

Contigency Planning

IR(Incident Response)-low level issue, there are multiple tears, first step is identification,contain,investigate(forensics),perform remedy, reporting(document)

DR(Disaster Recovery):high level issue, major disruption ,like floods, earthquakes.

BCP(Business Continuity Planning): when everything is destroyed in disaster, then how to continue the business

Laws, Investigations and Ethics

One of the more interesting security domains is Law, Investigation, and Ethics. As the name implies, this security domain covers the legal issues associated with computer security.

R(

Cryptography

One of the most widely used security techniques today is cryptography, the encryption of data. The Cryptography security domain is designed to help you understand how and when to use encryption

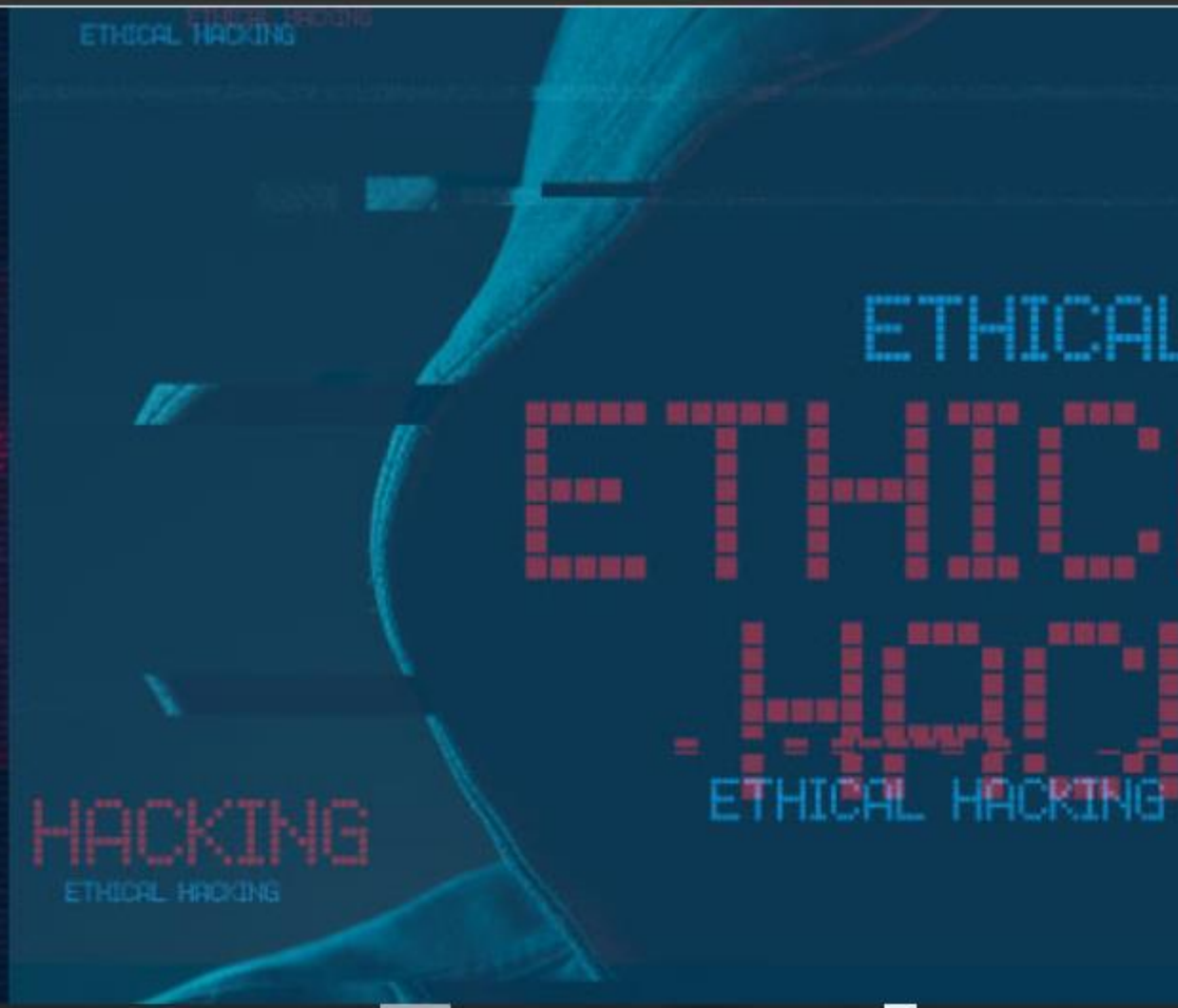
Types of Hackers

Ethical Hacking

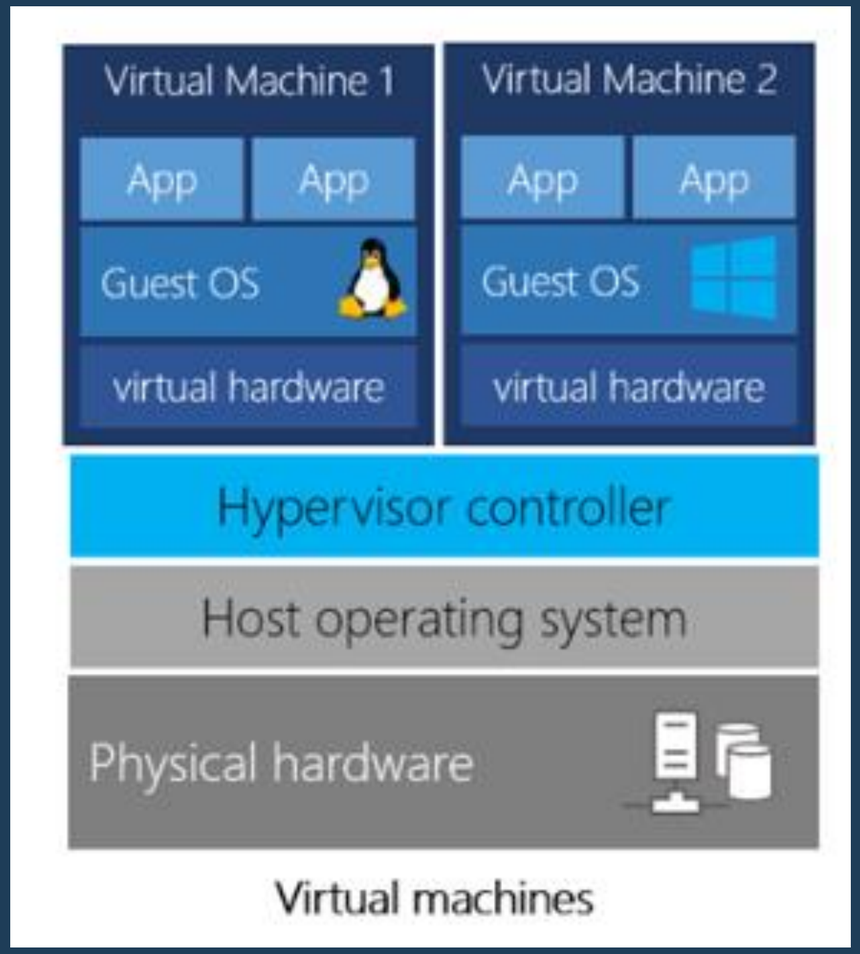
It is Legal
Permission is obtained from the target
Part of an overall security Program
Identify vulnerabilities from Internet at particular point of time.
Ethical Hackers possesses some skills, mindset and tools of a hacker but the attacks are done in a non-destructive manner.

What is Ethical Hacking?

The Certified Ethical Hacker (C|EH) credentialing and training program provided by EC-Council is a respected and trusted ethical hacking program in the industry. Since the inception of Certified Ethical Hacker in 2003, the credential has become one of the best options for industries and companies across the world. The C|EH exam is ANSI 17024 compliant, adding value and credibility to credential members. It is also listed as a baseline certification in the US Department of Defense (DoD) Directive 8570 and is a



Virtual Machine



Kali Linux

Kali Linux is a **Debian-Derived Linux Distribution** and a member of **UNIX OS Family.**
Maintained and Funded by Offensive Security Limited.
Primarily designed for **Penetration testing** and **Digital forensics**.