MODULE 1
INTRODUCTION TO ETHICAL HACKING

TOPICS TO BE COVERED

Basics of ethical hacking

Terminologies used in ethical hacking

Who are hackers and their types

Hacking phases

Networking and Linux OS basics

What is Hacking?

Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized and inappropriate access to the system resources.

It involves modifying system or application features to achieve a goal outside of the creator's original purpose

What is Ethical Hacking?

Ethical hacking involves the use of hacking tools, tricks and techniques to identify vulnerabilities so as to assume system security.

It focuses on simulating techniques used by attackers to verify the existence of exploitable vulnerabilities in the systems security

Who are Hackers?

A hackers are intelligent individuals who spend enormous amount of time researching and exploring computing resources like networks, websites, mobile devices etc.

Why is Ethical Hacking necessary?

To beat a hacker, you need to think like one

Ethical hacking is necessary because it allows the countering of attacks from malicious hackers by anticipating methods they can use to break into systems

- To prevent hackers from gaining access to information breaches
- To fight against terrorism and national security breaches
- To build a system that avoids hackers from penetrating
- To test if an organisations security settings are in fact secure

Terminology

Vulnerability : Vulnerability is a flaw or weakness in design or implementation error that can lead to unexpected and undesirable event compromising the security. In simple words, vulnerability is a loophole, weakness or limitation a source for attacker to enter into system by bypassing authentication mechanism

Exploit : An exploit is defined way to breach the security of an IT system through vulnerability. It takes advantage of vulnerability to cause unintended or unanticipated behaviour which allows attacker to gain access to data or information

Zero day attack : An attack that exploits computer application vulnerabilities before the developer released a patch for the vulnerability

Payload : A payload is an action or set of actions, that has to be done on the target once the exploit successfully launched. It can be any kind of control, Denial of Service or anything.

Types of Hackers

- White Hat Hackers
- Black Hat Hackers
- Grey Hat Hackers
- Script Kiddies
- State sponsored Hackers
- Hacktivists
- Suicide Hackers
- Spy Hackers

Elements of Information Security

- Confidentiality
- Integrity
- Availability

Security, Functionality and Usability Triangle

- Level of security in any system can be defined by the strength of three components:

Phases of hacking

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing tracks or Reporting

Building your practice lab

Virtualization

HyperV(Only for windows), VMWare & Virtualbox (All OS supported)

Depending on type of your virtualization software you need to download respective image of vdi or vmx from kali.org website

Network basics

What is a network

What are different types of networks

What is a MAC Address & IP Address? Classes of IP Address

Some protocols we will hear often like ARP, DHCP and DNS

ARP (Address Resolution Protocol)

The address resolution protocol (ARP) feature finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.

The ARP cache is a table in computer memory that maps a limited number of IP Addresses to their physical adapter addresses.

A computer’s ARP cache contains its own entry, entries for machines that have made ARP broadcasts to it, and entries for machines to which it has made broadcasts

PRACTICAL NETWORKING .NET

Server
10.0.0.33
0053.ffff.**cccc**

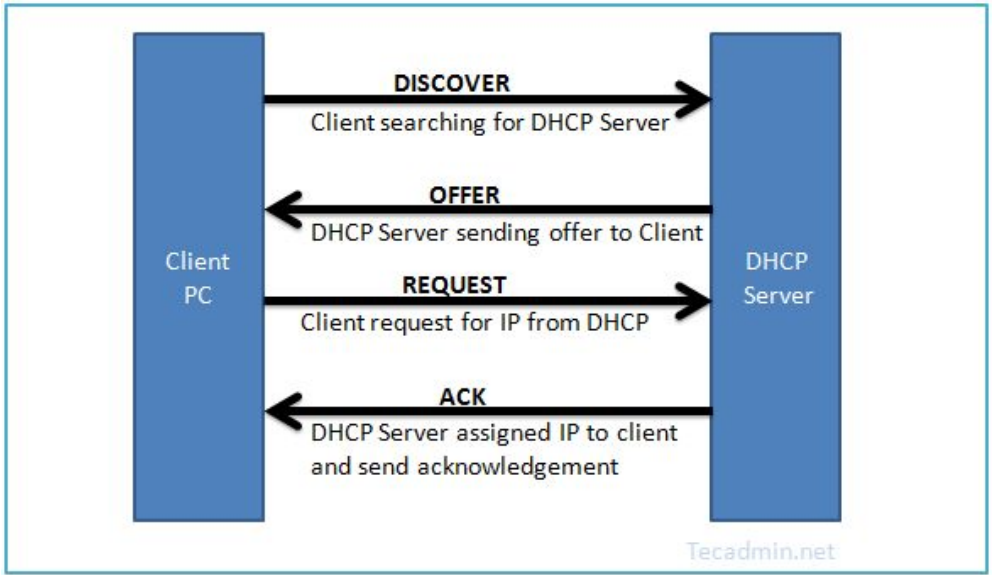
Router
10.0.0.99
0053.ffff.**9999**

Host A
10.0.0.11
0053.ffff.**aaaa**

Host B
10.0.0.22
0053.ffff.**bbbb**

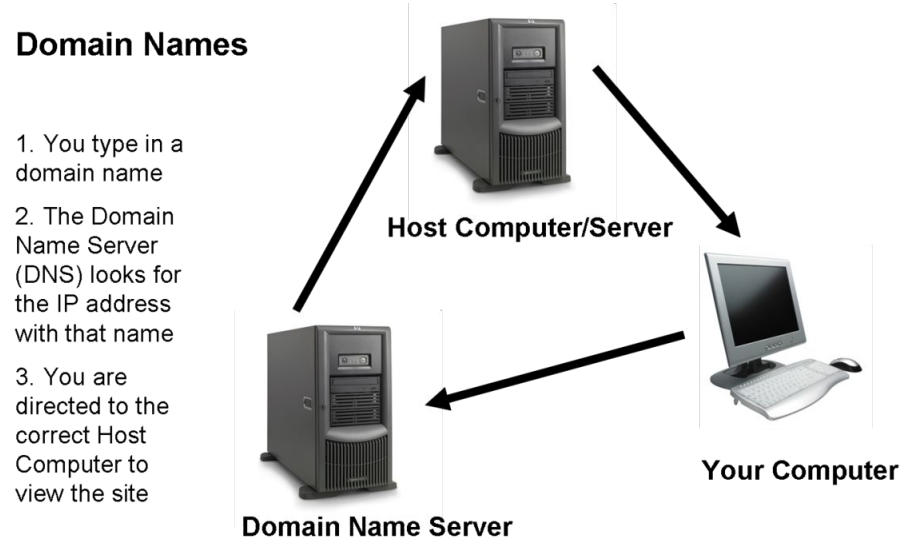
DHCP (Dynamic Host Configuration Protocol)

DHCP is the protocol responsible for management and automatic configuration of IP Addresses with n a network.



DNS (Domain Name Service)

DNS servers are equivalent of internet's phonebook. They maintain a directory of domain names and translate them to IP Address



Linux OS basics

File system structure

Some basic day to day linux commands

Permissions