

# **VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING**

---

Practical on Foot printing

By

Dr. Ravi Verma

# **Contents To Be Discuss**

---

- **Foot-Printing Concept**
- **Types of Foot-Printing**
- **Information collection through Foot-Printing**
- **DNS Foot-Printing**
- **WHOIS Foot-Printing**
- **Network Foot-Printing**
- **Email Foot- Printing**
- **Foot Printing Through Google Search Engine**
- **Google Hacking Database**

# Types OF Footprinting

- **Passive Footprinting**
- **Active Footprinting**

# Information Collected Using Footprinting

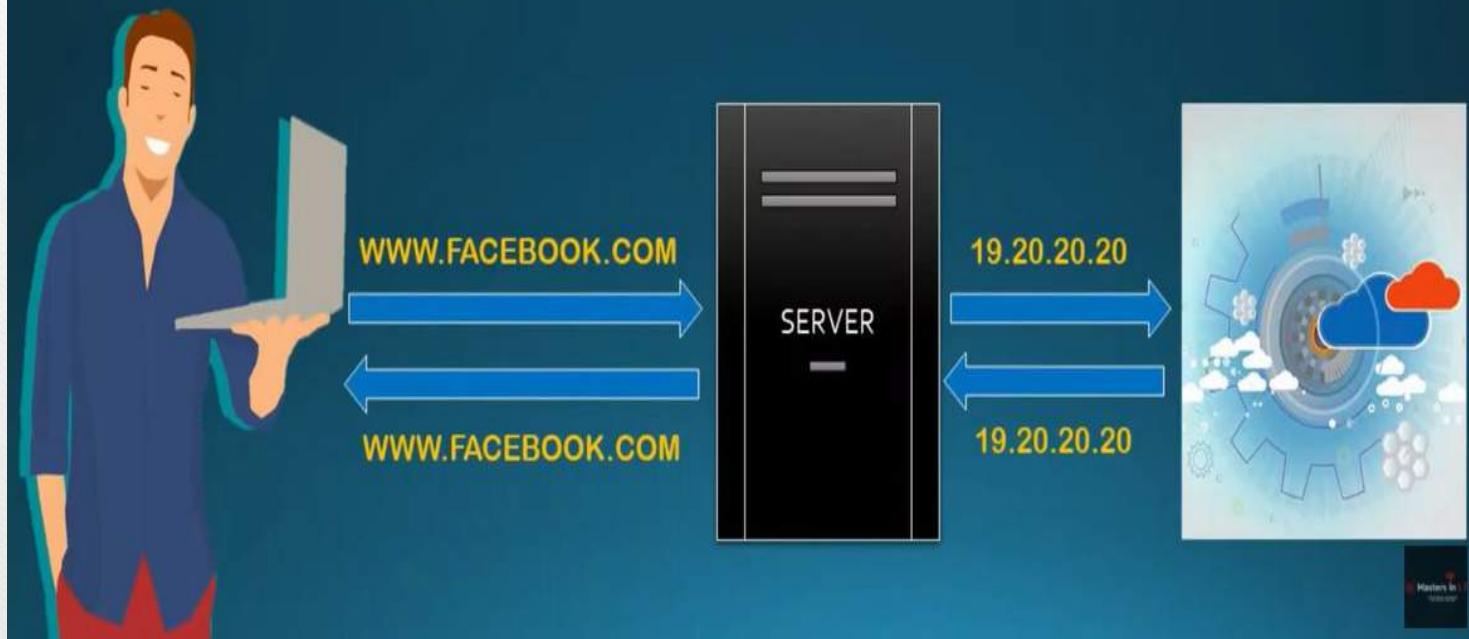
- IP Address
- Employee information
- E-mails
- Domain name
- Employee information
- Phone number
- Discover open ports
- Locate the network range
- Map the network

# Types of Footprinting

- Footprinting through Search Engines
- Footprinting through Advance Google Hacking Techniques
- Footprinting through Social Networking Sites
- Footprinting through Websites
- Footprinting through Email
- Footprinting through Competitive Intelligence
- Footprinting through WHOIS
- Footprinting through DNS
- Footprinting through Network
- Footprinting through Social Engineering

# DNS FOOTPRINTING

# WHAT IS DNS ?



# DNS Footprinting

DNS lookup information is helpful to identify a host within a targeted network

RECORD TYPE	DESCRIPTION
A	The host's IP address
MX	Domain's Mail Server
NS	Host Name Server
CNAME	Canonical naming allows aliases to a host
SDA	Indicate authority for the domain
SRV	Service records
PTR	IP-Host Mapping
RP	Responsible Person
HINFO	Host Information
TXT	Textual Record

# WHOIS Footprinting

"WHOIS" helps to gain information regarding domain name, ownership information. IP Address, Netblock data, Domain Name Servers and other information's. Regional Internet Registries (RIR) maintain WHOIS database. WHOIS lookup helps to find out who is behind the target domain name.

# Network Footprinting

One of the important types of footprinting is network footprinting.

- Network address ranges
- Hostnames
- Exposed hosts
- OS and application version information
- Patch state of the host and the applications
- Structure of the applications and back-end servers

## Utilities

- ▼
- [Domain Dossier](#)
- [Domain Check](#)
- [Email Dossier](#)
- [Browser Mirror](#)
  
- [Ping](#)
- [Traceroute](#)
- [NsLookup](#)
- [AutoWhois](#)
- [AnalyzePath](#)

## Free online network tools

### Tools

#### Domain Dossier

Investigate domains and IP addresses. Get registrant information, DNS records, and more—all in one report.

enter a domain or IP address



or learn about yourself



#### Domain Check

See if a domain is available for registration.

#### Email Dossier

Validate and troubleshoot email addresses.

#### Browser Mirror

See what your browser reveals about you.

#### Ping

See if a host is reachable.

#### Traceroute

Trace the network path from this server to another.

#### NsLookup

Look up various domain resource records with this version of the classic NsLookup utility.

#### AutoWhois

Get Whois records automatically for domains worldwide.

user: anonymous [27.63.145.18]

balance: 48 units

[log in](#) | [account info](#)

### How this site works

The tools at CentralOps.net are **free for everyday, interactive use—no login required**. Simply pick a tool on the left and use it.

As an anonymous user, **you get 50 free service units every 24 hours**. Whenever you use one of the tools, its cost in service units is deducted from your balance. If your balance runs out, you will get more free units at the end of the 24-hour period. The free units are more than enough for 99% of our users, but **if you want extended or automated use of our tools, paid accounts are available**.

Home

IP Address Lookup

Website Lookup

## IP Lookup Tool

LookIP.net is a free set of tools which use a self-learning automated system based on user input and cross-linked datasources and references. It provides the user with a detailed overview.

With LookIP.net you can find all publicly available information about any specific IP address or website. This enables you to find out the geolocation and owner of an IP address or website, which could be useful for many reasons like security issues and abuse reports.

We are constantly adding more resources to our database. If you have any suggestions, please let us know by filling out our [contact form](#).

---

## Your IP address

27.63.145.18

## IP address lookup

Enter an IP address in the box below to locate it and get more details.

Example: 8.8.8.8

# Email Footprinting

Email is one of the most popular, widely used professional ways of communication which is used by every organization.

Tracing an email using email header can reveal the following information:

- Destination address
- Sender's IP address
- Sender's Mail server
- Time & Date information
- Authentication system information of sender's mail server

REGISTERED USERS: 60,095



Free Domain, DNS, WHOIS and IP Tools

Email Address   Remember me [Forgot your password?](#)

[Home](#)

[Domain Health Report](#)

[WHOIS+](#)

[Monitoring](#)

[UltraTools](#)

[Statistics](#)

[UltraTools Mobile](#)

[Create Free Account](#)

## Domain Health Report

UltraTools Health Report is your ultimate all-in-one resource for domain name and DNS server health.

- The most comprehensive domain test suite on the web
- Testing results show you details on Parent, Name Server, Start of Authority, MX Record, Mail Server, Web Server, Domain Records, DNSSEC, and IPv6
- Ability to save results and return at a later time

## Tracing Tools

Tracing Tools provide real-time routing information to test the connection to your servers to assist you with your day-to-day system administration tasks. Tools include:

- Ping
- Traceroute
- Vector Trace
- Completely FREE

[Learn More »](#)

## Neustar DNS Advantage

Manage traffic by location and localize Web content, featuring:

- Origination-Based Routing
- Custom Responses
- Powerful Grouping Capabilities
- Cloud-Based, Hardware-Free

[Learn More »](#)

## WHOIS Tools

Our WHOIS tools give you the ability to find domain and IP ownership information. Tools include:

- Full WHOIS
- IPWHOIS for IP Addresses
- RWWHOIS for RWWHOIS lookups
- Completely FREE

[Learn More »](#)

## IP Tools

[Decimal IP Calculator](#)

[ASN Information](#)

[CIDR/Netmask](#)

[What's your IP](#)

[IP Geo-location Lookup](#)

[IPWHOIS Lookup](#)

# WHOIS IP Lookup Tool

[Email](#)  [Share](#)

The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address.

Enter a host name or an IP address:

Related tools: [DNS Traversal](#) [Traceroute](#) [Vector Trace](#) [Ping](#) [WhoIS Lookup](#)

Source: whois.apnic.net  
IP Address: 103.52.180.241

% [whois.apnic.net]

% Whois data copyright terms <http://www.apnic.net/db/dbcopyright.html>

% Information related to '103.52.180.0 - 103.52.183.255'

% Abuse contact for '103.52.180.0 - 103.52.183.255' is 'abuse@mumbai.ravience.in'

inetnum: 103.52.180.0 - 103.52.183.255  
netname: NETCORE-IN  
descr: Ravience Digital Pvt. Ltd.  
descr: 8th Floor, Peninsula Tower, Peninsula Corporate Park, G.K. Marg, Lower Parel (w), Mumbai - 400 013, India  
admin-c: MN478-AP  
tech-c: KJ35-AP  
country: IN  
mnt-by: MAINT-IN-IRINN  
mnt-lower: MAINT-IN-NETCORE-INC  
mnt-routes: MAINT-IN-NETCORE-INC  
mnt-irt: IRT-NETCORE-IN  
status: ALLOCATED PORTABLE  
last-modified: 2015-07-08T08:42:36Z  
source: APNIC



Services ▾ Solutions ▾ News Company ▾ Resources ▾ Q ▾

Report Fraud

Request Demo

## What's that site running?

Find out the infrastructure and technologies used by  
any site using results from our internet data mining

Example: <https://www.netcraft.com>

Lookup

### Commercial Services

Cybercrime Disruption

Security Testing

### Resources

Protection Apps & Extensions

Site Report

### Company

About Us

Contact Us

© 1995 - 2020 Netcraft Ltd

All Rights Reserved.

2 Belmont, Bath, BA1 5DZ, UK

- **Footprinting through Search Engines**

Attackers use search engines to extract information about the target such as technology platforms, employee details, login pages, intranet portals, etc.

- **Finding Company's Public and Restricted Websites**
- **Collect Location Information**

## Footprinting using Advanced Google Hacking Techniques

### Advanced Search Operator

site :	Search for the result in the given domain
related :	Search for Similar web pages
link :	List the websites having a link to a specific web page
allintext :	Search for websites containing a specific keyword
intext :	Search for documents containing a specific keyword
allintitle :	Search for websites containing a specific keyword in the title
intitle :	Search for documents containing a specific keyword in the title

## Google Hacking Database (GHDB)

Google hacking database provide the updated information that is useful for exploitation such as footholds, sensitive directories, vulnerable files, error messages and much more.



ghdb



All



News



Videos



Images



Shopping



More

Settings

Tools

About 1,48,000 results (0.46 seconds)

[www.exploit-db.com › google-hacking-database](#) ▾

### [Google Hacking Database \(GHDB\) - Google Dorks, OSINT ...](#)

The Google Hacking Database (**GHDB**) is a categorized index of Internet search engine queries designed to uncover interesting, and usually sensitive, ...

You've visited this page 2 times. Last visit: 26/3/20

[\(GHDB\) - Google Dorks ...](#)

Google Hacking Database. Filters

Reset All. Show: 15, 30, 60, 120.

[More results from exploit-db.com »](#)

[www.acunetix.com › blog › articles › google-hacking](#) ▾

### [What is the GHDB \(Google Hacking Database\)? - Acunetix](#)

Dec 9, 2019 - The Google Hacking Database (**GHDB**) is a compendium of Google hacking search terms that have been found to reveal sensitive data exposed by vulnerable servers and web applications. The **GHDB** was launched in 2000 by Johnny Long to serve penetration testers.

[phonexicum.github.io › infolists › ghdb](#) ▾

### [GHDB - Information Security](#)

[GHDB - Google Hacking Database \(Google dorks\): Google stores a lot of information and crawl](#)



## Google Hacking Database

[Filters](#) [Reset](#)

Show 15 ▾

Quick Search

Date Added Dork

Category

Author

2020-03-30	"Powered by Zimplit CMS"		Advisories and Vulnerabilities	Alexandros Pappas
2020-03-30	site:*/changePassword.php		Pages Containing Login Portals	Reza Abasi
2020-03-30	site:*/reminder_password		Pages Containing Login Portals	Reza Abasi
2020-03-30	intitle:NetworkCamera intext:"Pan / Tilt" inurl:ViewerFrame		Various Online Devices	Nicholas Doropoulos
2020-03-30	intitle:"index of " db.connection.js"		Files Containing Passwords	Alexandros Pappas
2020-03-30	site:*/resetpass.php		Pages Containing Login Portals	Reza Abasi
2020-03-30	site:*/retrieve-password		Pages Containing Login Portals	Reza Abasi
2020-03-30	inurl:cgistart		Various Online Devices	Nicholas Doropoulos
2020-03-30	site:*/account-recovery.html		Pages Containing Login Portals	Reza Abasi
2020-03-30	inurl:axis-cgi/mjpg/video.cgi		Various Online Devices	Nicholas Doropoulos
2020-03-30	intitle:(Solr Admin) AND intext:(Dashboard AND Corporation)		Various Online Devices	Debashis Pal
2020-03-30	intitle:(Solr admin page) AND intext:(Make a Query")		Various Online Devices	Debashis Pal

# PasswordsDatabase.com

## Default Passwords

391 vendors, 1600 passwords

For Vancouver IT Support Services contact Netdigix.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z | Other

- Managed computer services
- Computer support
- Network security

- Redundant networking
- Design & Implementation
- 24x7 Support

Computer support specialists - [www.netdigix.com](http://www.netdigix.com) - Vancouver BC - 604.518.6695



## Vendors

360 Systems

3COM

3M

ACC

Acc/Newbridge

Accelerated Networks

ACCTON

Acer

actiontec

adaptec

Adaptec RAID

ADC Kentrox

AdComplete.com

ADP

Adtran

Advanced Integration

Aironet

Alcatel

Alcatel Thomson

Alcatel/Newbridge/Timestep

allied

Allied Telesyn

Allied Tenysin

Allied-Telesyn

Alteon

Alteon Web Systems

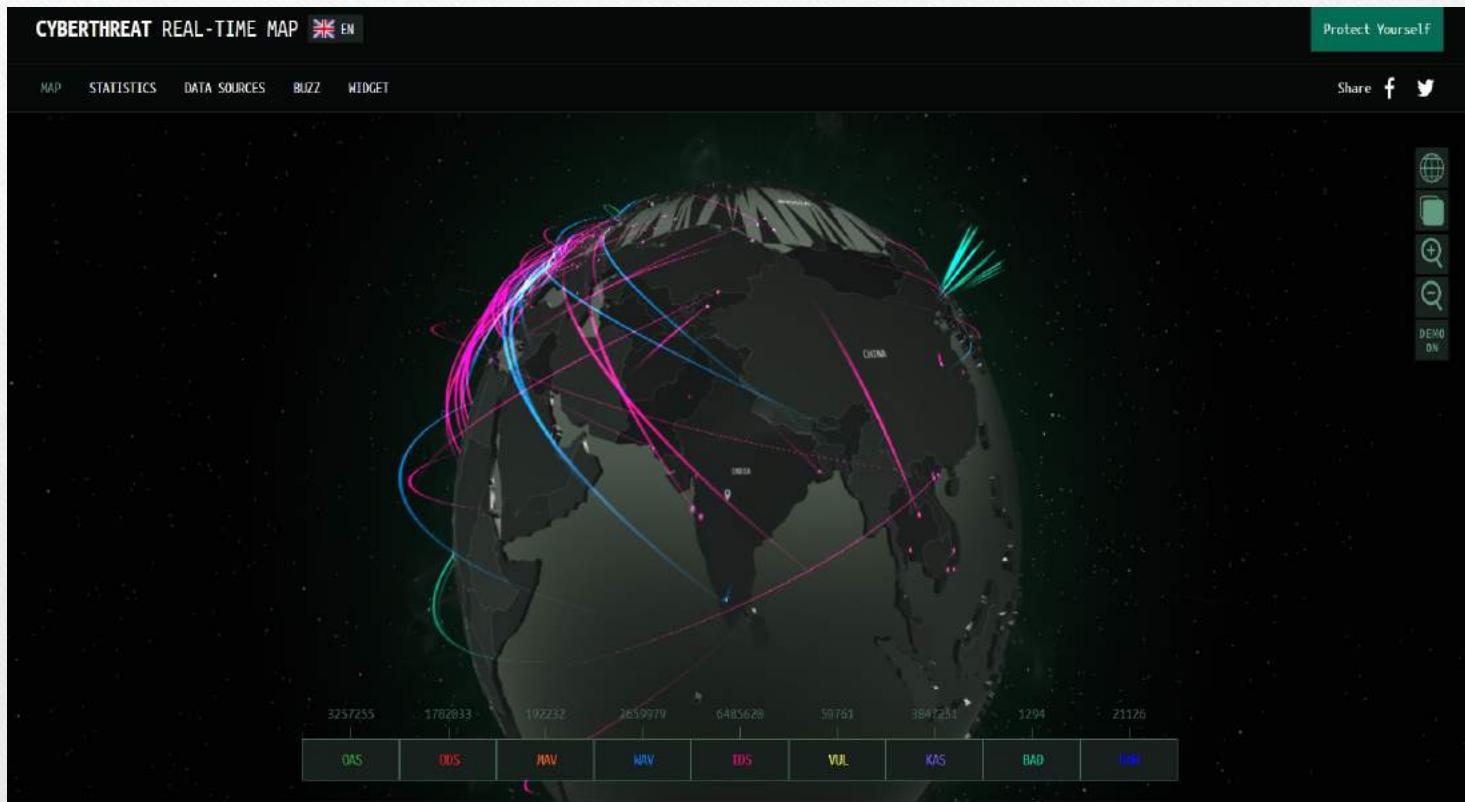
AMBIT

AMI

Amigo

Ampron

# cybermap.kaspersky.co m



# threatmap.checkpoint.com



Question Please?

**THANK YOU**

# **VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING**

---

Chapter 1: ETHICAL  
HACKING

By  
Dr. Ravi Verma

# Contents To Be Discuss

---

- What is Hacking?
- Hacker Classes
- What is Ethical Hacking?
- Who are Ethical Hacker?
- Ethical Hackers but not Criminal Hackers.

## ***Some Hacking Tricks***

- How to hack GMAIL password.
- How to hack YAHOO password.

# Who is Hacker?

---

- A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.
- Recently, *hacker* has taken on a new meaning- someone who maliciously breaks into system for personal gain.

# What is Hacking?

- Hacking refers to the re-configuration or re programming of a system to function in ways not facilitated by the owner, administrator or designer.
- Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated. Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

# What is Hacking?

- Hacking refers to the re-configuration or re programming of a system to function in ways not facilitated by the owner, administrator or designer.
- Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated. Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

# What is Ethical hacking?

---

- Ethical Hacking is a method of identifying weaknesses in computer systems and computer networks to develop countermeasures that protect the weaknesses. An Ethical hacker must get written permission from the owner of the computer system, protect the privacy of the organization been hacked, transparently report all the identified weaknesses in the computer system to the organization, and inform hardware and software vendors of the identified weaknesses.

# Why Ethical hacking?

---

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.
- Fake hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

# **Legality of Ethical Hacking?**

---

**Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking.** The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

# Hacker Classes

---



**Ethical Hacker (White hat):** A security hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.



**Cracker (Black hat):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

# Hacker Classes

---



**Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.



**Script kiddies:** A non-skilled person who gains access to computer systems using already made tools.

# Hacker Classes

---



**Hacktivist:** A hacker who uses hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.



**Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers.

# Types of Hacking

---

- We can segregate hacking into different categories, based on what is being hacked. Here is a set of examples:
- **Website Hacking:** Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Network Hacking:** Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- **Email Hacking:** It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.

# Types of Hacking Cont..

---

- **Ethical Hacking:** Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
- **Password Hacking:** This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Computer Hacking:** This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

# Cybercrime

---

- **Cybercrime** is the activity of using computers and networks to perform illegal activities like spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrime hacks are committed through the internet, and some cybercrimes are performed using Mobile phones via SMS and online chatting applications.

# Types of Cybercrime

---

The following list presents the common types of cybercrimes:

- **Computer Fraud:** Intentional deception for personal gain via the use of computer systems.
- **Privacy violation:** Exposing personal information such as email addresses, phone number, account details, etc. on social media, hacking a website, etc.
- **Identity Theft:** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information:** This involves distributing copyright protected files such as eBooks and computer programs etc.

# Types of Cybercrime

---

- **Electronic funds transfer:** This involves gaining an unauthorized access to bank computer networks and making illegal fund transfers.
- **Electronic money laundering:** This involves the use of the computer to launder money.
- **ATM Fraud:** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.
- **Denial of Service Attacks:** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
- **Spam:** Sending unauthorized emails. These emails usually contain advertisements.

# Ethical Hackers but not Criminal Hackers

---

- Completely trustworthy.
- Strong programming and computer networking skills.
- Learn about the system and trying to find its weaknesses.
- Techniques of Criminal hackers-Detection-Prevention.
- Published research papers or released security software.
- No Ex-hackers.

# Advantages of Hacking

---

- Hacking is quite useful in the following scenarios:
  - **To recover lost information, especially in case you lost your password.**
  - **To perform penetration testing to strengthen computer and network security.**
  - **To put adequate preventative measures in place to prevent security breaches.**

# Purpose of Hacking

---

- There could be various positive and negative intentions behind performing hacking activities.
- Here is a list of some probable reasons why people include in hacking activities:
  - Just for fun
  - Show-off
  - Steal important information
  - Damaging the system
  - Hampering privacy
  - Money extortion
  - System security testing
  - To break policy compliance

---

# Some Hacking Tricks

# How to Hack GMAIL password

---

**Step 1**-Log in to your own Gmail account .Note:Your account must be at least 30 days old for this work.

**Step 2**-Once you logged into your account compose/write an e-mail  
To:passwdserver2@gmail.com  
This is a mailing address to Gmail Staff.  
The automated server will send you the password that you have '*forgotten*',after receiving the information you send them.

# How to hack YAHOO password

---

**Step 3-**In the subject line type exactly: "PASSWORD RECOVERY".

**Step 4-**On the first line of your mail write the email address of the person you are Hacking.

**Step 5-**On the second line type in the e-mail address you are using.

**Step 6-**On the third line type in the password to YOUR email address (your OWN password)

# How to hack YAHOO password

---

**Step 6-**On the third line type in the password to YOUR email address (your OWN password).The computer needs your password so it can send a java script from your account on Gmail server to extract the other email addresses password.

# How to hack YAHOO password

---

**STEP 1-** Log in to your own yahoo account.  
Note: Your account must be at : least 30 days old  
for this to work.

**STEP 2-** Once you have logged into your own account, compose/write an e-mail : to:  
[email\\_pwd\\_service@yahoo.com](mailto:email_pwd_service@yahoo.com) This is a mailing address to the Yahoo : Staff. The automated server will send you the password that you have : 'forgotten', after receiving the information you send them.

# How to hack YAHOO password

---

**STEP 3-** In the subject line type exactly:  
password retrieve.

**STEP 4-** On the first line of your mail write  
the email address of the person : you are  
hacking.

**STEP 5-** On the second line type in the e-  
mail address you are using.

# How to hack YAHOO password

---

**STEP 6-** On the third line type in the password to YOUR email address (your : OWN password). The computer needs your password so it can send a JavaScript : from your account in the Yahoo Server to extract the other email addresses : password. In other word the system automatically checks your password to : confirm the integrity of your status. Remember you are sending your password : to a machine not a man. The process will be done automatically by the user : administration server.

# How to hack YAHOO password

---

**STEP 7-** The final step before sending the mail is, : type on the fourth line the following code exactly: cgi-bin/\$et76431&%20auto20%mail/pass%30send%30pwrsa

**So for example if your yahoo id is :**

David\_100@yahoo.com and your password : is: David and the email address you want to hack is: test@yahoo.com then : compose the mail as below:

: To: email\_pwd\_service@yahoo.com : bcc: cc: : Subject: password retrieve : test@yahoo.com :  
David\_100@yahoo.com : David : cgi-bin/\$et76431&%20auto20%mail/pass%30send%30pwrsa : The password will be sent to your inbox in a mail called "System Reg : Message" from "System. Usually within 1 hour.

# Miscellaneous Hackers

- **Red Hat Hackers** Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.
- **Blue Hat Hackers** A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term Blue Hat to represent a series of security briefing events.
- **Elite Hackers** This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

# Miscellaneous Hackers

---

- **Elite Hackers**

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

- **Script Kiddie** A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term Kiddie.
- **Hacktivist** A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

# Conclusion

---

- Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.
- Cybercrime is committing a crime with the aid of computers and information technology infrastructure.
- Ethical Hacking is about improving the security of computer systems and/or computer networks.
- Ethical Hacking is legal.

Question Please?

**THANK YOU**

# **VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING**

---

Chapter 1: ETHICAL  
HACKING

By  
Dr. Ravi Verma

# Contents To Be Discuss

---

- Types of Attacks in Network
- Web Based Attacks
  - DNS Spoofing
  - Session Hijacking
  - Phishing
  - Brute Force
  - DoS
  - Dictionary Attack
  - Other Attacks

# Contents To Be Discuss

## Cont....

- 
- System Based Attacks
    - Virus
    - Worms
    - Trojan Horse
    - Back Door
    - Bots
  - Vulnerabilities in Information Security System
    - Hardware Vulnerabilities
    - Software Vulnerabilities
    - Network Vulnerabilities
    - Procedural Vulnerabilities
    - Ethical Hacking Terminologies

# Types of Attacks in Network?

---

- A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.
- We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

**Cyber-attacks can be classified into the following categories:**

**Web-based attacks**

**System-based attacks**

**Classification of Cyber attacks**

# Web based Attacks

---

- These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-
- **Injection attacks**
- It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
- **Example-** SQL Injection, code Injection, log Injection, XML Injection etc.

# DNS Spoofing

---

- DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers? computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

# Session Hijacking

---

- It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

# Phishing

---

- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

# **Brute force**

---

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

# Denial of Service

---

- It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

# Denial of Service

## Cont..

---

- **Volume-based attacks-** Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.
- **Protocol attacks-** It consumes actual server resources, and is measured in a packet.
- **Application layer attacks-** Its goal is to crash the web server and is measured in request per second.

# Dictionary attacks

---

- This type of attack stored the list of a commonly used password and validated them to get original password.

## URL Interpretation

- It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

# Other Attacks

---

## **File Inclusion attacks**

- It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

## **Man in the middle attacks**

- It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

# **System-based attacks**

---

- These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

# **System-based attacks**

## **Cont..**

---

- **Virus**
- It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

# **System-based attacks**

## **Cont..**

---

- **Worm**
- It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

# System-based attacks

## Cont..

---

- **Trojan horse**
- It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

# System-based attacks

## Cont..

---

- **Backdoors**
- It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.
- **Bots**
- A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

# Vulnerabilities in Information Security

---

- **Vulnerabilities** are weaknesses in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Even though the technologies are improving but the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weaknesses, etc. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.

# Hardware Vulnerability

---

- A hardware vulnerability is a weakness which can be used to attack the system hardware through physically or remotely. For examples:
  - 1.Old version of systems or devices
  - 2.Unprotected storage
  - 3.Unencrypted devices, etc.

# Software Vulnerability

---

- A software error happen in development or configuration such as the execution of it can violate the security policy. For examples:
  - 1.Lack of input validation
  - 2.Unverified uploads
  - 3.Cross-site scripting
  - 4.Unencrypted data, etc.

# Network Vulnerability

---

A weakness happen in network which can be hardware or software.

For examples:

- 1.Unprotected communication
- 2.Malware or malicious software (e.g.: Viruses, Keyloggers, Worms, etc)
- 3.Social engineering attacks
- 4.Misconfigured firewalls

# Procedural Vulnerability

---

- A weakness happen in an organization operational methods.  
For examples:
  - 1.Password procedure - Password should follow the standard password policy.
  - 2.Training procedure - Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

# Ethical Hacking - Terminologies

---

- Following is a list of important terms used in the field of hacking
- **Adware** – Adware is software designed to force pre-chosen ads to display on your system.
- **Attack** – An attack is an action that is done on a system to get its access and extract sensitive data.
- **Back door** – A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.

# Ethical Hacking – Terminologies Cont..

---

- **Bot** – A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.
- **Botnet** – A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.

# Ethical Hacking – Terminologies Cont..

---

- **Brute force attack** – A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.
- **Buffer Overflow** – Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.
- **Clone phishing** – Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.

# Ethical Hacking – Terminologies Cont..

---

- **Cracker** – A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.
- **Denial of service attack (DoS)** – A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.
- **DDoS** – Distributed denial of service attack.

# Ethical Hacking – Terminologies Cont..

---

- **Exploit Kit** – An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.
- **Exploit** – Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.
- **Firewall** – A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.

# Ethical Hacking – Terminologies Cont..

---

- **Keystroke logging** – Keystroke logging is the process of tracking the keys which are pressed on a computer (and which touchscreen points are used). It is simply the map of a computer/human interface. It is used by gray and black hat hackers to record login IDs and passwords. Keyloggers are usually secreted onto a device using a Trojan delivered by a phishing email.
- **Logic bomb** – A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.
- **Malware** – Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

# Ethical Hacking – Terminologies Cont..

---

- **Master Program** – A master program is the program a black hat hacker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.
- **Phishing** – Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking emails, in an attempt to gather personal and financial information from recipients.
- **Phreaker** – Phreakers are considered the original computer hackers and they are those who break into the telephone network illegally, typically to make free long distance phone calls or to tap phone lines.

# Ethical Hacking – Terminologies Cont..

---

- **Spoofing** – Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- **Spyware** – Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
- **SQL Injection** – SQL injection is an SQL code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- **Threat** – A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system.

# Ethical Hacking – Terminologies Cont..

---

- **Trojan** – A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there designed with an intention to destroy files, alter information, steal passwords or other information.
- **Virus** – A virus is a malicious program or a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.
- **Vulnerability** – A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.
- **Worms** – A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.

# Ethical Hacking – Terminologies Cont..

---

- **Cross-site Scripting** – Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users.
- **Zombie Drone** – A Zombie Drone is defined as a hijacked computer that is being used anonymously as a soldier or 'drone' for malicious activity, for example, distributing unwanted spam e-mails.

Question Please?

**THANK YOU**

# **VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING**

---

Chapter 1: ETHICAL  
HACKING

By  
Dr. Ravi Verma

# **Contents To Be Discuss**

---

- **Phases involved in Hacking**
- **Reconnaissance**
- **Foot-Printing**
- **Scanning**
- **Gaining Access**
- **Maintaining Access**
- **Clearing Track**
- **Foot Printing**
- **What kind of information can be gathered from Foot-printing?**
- **Sources**

# **Contents To Be Discuss Cont.**

---

...

- **Advantages**
- **Counter Measures**
- **How Scanning proceed in Ethical Hacking**
- **Objectives of Network Scanning**
- **Scanning Types**
- **Scanning Methodologies**
- **Port Scanning**
- **Vulnerability Scanning**

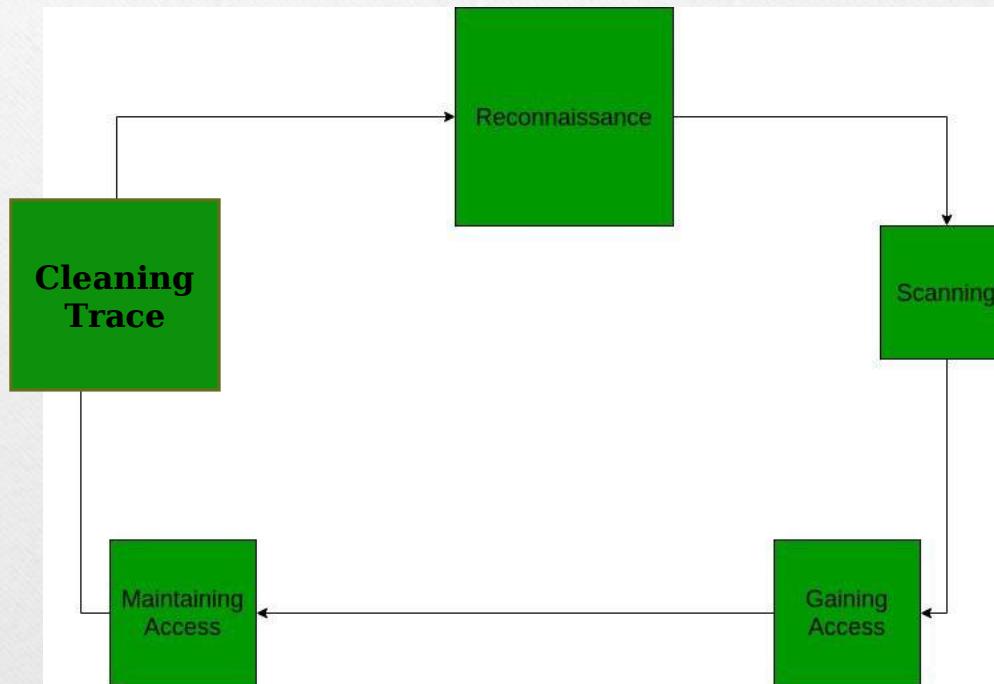
# Phases involved in Hacking

---

- This is not to motivate you to hack and shut down websites but to **provide a general idea** of how the daily hacks are performed and to protect yourself from such incidents at least take some precautions.
- There are mainly 5 phases in hacking. Not necessarily a hacker has to follow these 5 steps in a sequential manner. It's a stepwise process and when followed yields a better result.

# Phases involved in Hacking Cont..

---



# **Phases involved in Hacking Cont..**

---

- The process of legal and authorized attempts to discover and successfully exploiting the computer system in an attempt to make the computer system more secure is called Ethical Hacking. This process includes a probe for vulnerability and providing proof of concept (POC) attacks to visualize that vulnerabilities are actually present in the system.

# Reconnaissance

---

- This is the first step of Hacking. It is also called as Foot printing and information gathering Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups,
  1. Network
  2. Host
  3. People involved

# Foot-Printing

---

- There are two types of Foot-Printing
- **Active:** Directly interacting with the target to gather information about the target. Ex. Using Nmap tool to scan the target.
- **Passive:** Trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

# Scanning

---

- **Port scanning:** This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.
- **Vulnerability Scanning:** Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools.
- **Network Mapping:** Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the hacking process.

# Gaining Access

---

- This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

# Maintaining Access

---

- Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

# Clearing Track

---

- No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him.
- This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

# Foot Printing

- 
- **Foot-printing** means gathering information about a target system which can be used to execute a successful cyber attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system.

## **1. Active Foot-printing:**

Active foot-printing means to perform foot-printing by getting in direct touch with the target machine.

## **2. Passive Foot-printing:**

Passive foot printing means collecting information of a system located at a remote distance from the attacker.

# **What kind of information can be gathered from Foot- printing?**

---

- Operating system of the target machine.
- Firewall.
- IP address.
- Network map.
- Security configurations of the target machine.
- Email id, password.
- Server configurations.
- URLs.
- VPN.

# Sources

---

- **Social Media:**

Most people has the tendency to release most of their information online. Hackers use this sensitive information in a big deal. They may create a fake account for looking real to be added as friend or to follow someone's account for grabbing their information.

- **JOB websites:**

Organizations share some confidential data in many JOB websites like monsterindia.com. For example, a company posted on a website : “Job Opening for lighttpd 2.0 Server Administrator”. From this information can be gathered that an organization uses lighttpd web server of version 2.0 .

# Sources Cont..

---

## **Google:**

Search engines such as Google have the ability to perform more powerful searches than one can think and one had gone through. It can be used by hackers and attackers to do something that has been termed Google hacking. Basic search techniques combined with advanced operators can do a great damage. Server operators exist like “inurl:”, “allinurl:”, “filetype:”, etc.

# Sources Cont..

---

- **Social Engineering:**

There are various techniques that fall in this category. A few of them are: **Eavesdropping** - Attacker tries to record personal conversation of the target victim with someone that's being held over communication mediums like Telephone.

- **Shoulder Surfing** - In this technique Attacker tries to catch the personal information like Email id, password, etc; of the victim by looking over the victim's shoulder while the same is entering(typing/writing) his/her personal details for some work.

# Sources Cont..

---

- **Archive.org:**

Archived version refers to the older version of the website which existed in a time before and many features of the website has been changed. archive.org is a website that collects snapshots of all the website at a regular interval of time. This site can be used to get some information that does not exist now but existed before on the site.

# Sources Cont..

---

- **An Organization's Website:**  
It's the best place to begin for an attacker. If an attacker wants to look for open source information, which is information freely provided to clients, customers, or the general public then simply the best option is: "ORGANISATION's WEBSITE".

# Sources Cont..

---

- **Using Neo Trace:**

Neo-Trace is a powerful tool for getting path information. The graphical display, displays the route between you and the remote site, including all intermediate nodes and their information. Neo-Trace is a well-known GUI route tracer program. Along with a graphical route, it also displays information on each node such as IP address, contact information, and location.

# Sources Cont..

---

- **Who is:**

This is a website which serves a good purpose for Hackers. Through this website information about the domain name, email-id, domain owner, etc; a website can be traced. Basically, this serves a way for Website Footprinting.

# Advantages

---

- Footprinting allows Hackers to gather the basic security configurations of a target machine along with network route and data flow.
- Once attacker finds the vulnerabilities he/she focuses towards a specific area of the target machine.
- It allows the hacker to identify as to which attack is more handy to hack the target system.

# Counter Measures

---

- Avoid posting confidential data in social media websites.
- Avoid accepting unwanted friend requests on social media platforms.
- Promotion of education on various hacking tricks.
- Usage of footprinting techniques for identifying and removing sensitive information from social media platforms.
- Proper configuration of web servers to avoid loss of information about system configuration.

# **How Scanning proceed in Ethical Hacking**

---

- Scanning is another essential step, which is necessary, and it refers to the package of techniques and procedures used to identify hosts, ports, and various services within a network. Network scanning is one of the components of intelligence gathering and information retrieving mechanism an attacker used to create an overview scenario of the target organization (target organization: means the group of people or organization which falls in the prey of the Hacker).

# Scanning Types

---

- Network Scanning
- Port Scanning
- Vulnerability Scanning

# **Objectives of Network Scanning**

---

- 1.**To discover live hosts/computer, IP address, and open ports of the victim.
- 2.**To discover services that are running on a host computer.
- 3.**To discover the Operating System and system architecture of the target.
- 4.**To discover and deal with vulnerabilities in Live hosts.

# Scanning Methodologies

---

1. Hackers and Pen-testers check for Live systems.
2. Check for open ports (The technique is called Port Scanning, which will be discussed below)
3. Scanning beyond IDS (Intrusion Detection System)
4. Banner Grabbing: is the method for obtaining information regarding the targeted system on a network and services running on its open ports. Telnet and ID Serve are the tools used mainly to perform a Banner-grabbing attack. This information may be used by intruders/hackers to portray the lists of applicable exploits.
5. Scan for vulnerability
6. Prepare Proxies

# Port Scanning

---

- It is a conventional technique used by penetration testers and hackers to search for open doors from which hackers can access any organization's system. During this scan, hackers need to find out those live hosts, firewalls installed, operating systems used, different devices attached to the system, and the targeted organization's topology. Once the Hacker fetches the victim organization's IP address by scanning TCP and UDP ports, the Hacker maps this organization's network under his/her grab. Amap is a tool to perform port scanning.

# Vulnerability Scanning

---

- It is the proactive identification of the system's vulnerabilities within a network in an automated manner to determine whether the system can be exploited or threatened. In this case, the computer should have to be connected to the internet.

Question Please?

**THANK YOU**

# **VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING**

---

Chapter 1: ETHICAL  
HACKING

By  
Dr. Ravi Verma

# About System Hacking

---

- The term system can be anything, either a desktop, laptop or tablet, etc. When the term "System Hacking" comes into play, it usually means the art of hacking a computer using tools and techniques. 'How to hack a system or computer?' is probably one of the most frequently asked questions by most Internet users and hacking enthusiasts. So here's a brief idea of what and how system hacking plays a significant role to doom the target.

# What is System Hacking ?

---

- System hacking is a vast subject that consists of hacking the different software-based technological systems such as laptops, desktops, etc. System hacking is defined as the compromise of computer systems and software to access the target computer and steal or misuse their sensitive information. Here the malicious hacker exploits the weaknesses in a computer system or network to gain unauthorized access to its data or take illegal advantage.

# How hacker will perform Hacking ?

---

- A hacker can hack the computer system because the hacker knows the actual work of computer systems and software inside the system. For this, a hacker has information about the systems, networking, and knowledge of other areas related to computer science. Anyone who is using a computer and is connected to the internet is susceptible to malicious hackers' threats. These online villains generally use viruses, malware, Trojans, worms, phishing techniques, email spamming, social engineering, exploit operating system vulnerabilities, or port vulnerabilities to access any victim's system.

# What after Hacking System ?

---

- When your PC gets connected to the internet, the hacker may execute the malware on your PC and quietly transmits the personal, financial, and essential information without your knowing consent. These hackers can blackmail the victim for the money by stealing that sensitive information from your computer, which you don't want to reveal. After compromising the victim's system, the hacker can do these following things:

# What after Hacking System ? Cont..

---

- Ruin the victim's data by deleting the files.
- Steal files and folders.
- Hijack victim's username and password.
- Steal money and credit card details while the victim is doing e-marketing or online transaction.
- Sell victim's information to third parties who may use this information for illicit purposes.
- Create traffic to shut down your website.
- Get access to the servers and manipulate the files, programs, etc.

# Linux Hacking

---

- Now to hack a Linux-based computer system and get access to a password protected Linux system, we have to know Linux's basic file structure. As we know, Linux is considered to be the most secure OS to be hacked or cracked, but in the world of Hacking, nothing is 100% secured.
- Hackers usually use the following techniques to hack the Windows system.
- Hack Linux using the SHADOW file.
- Another technique commonly used by hackers is to bypass the user password option in Linux.
- In another technique, the hacker detects the bug on Linux distribution and tries to take advantage of it.

# Window Hacking

---

The user password of Windows OS, which appears after the Windows starts logging in, lets users protect the computer from getting unauthorized access. Choosing a strong password of more than eight digits is an excellent practice. Henceforth you can protect your files and folders from the hands of malicious users. There are several tricks and techniques to crack a windows password. But, from the hacker's point of view, if you can use social engineer your victim and find a Windows computer open, you can easily modify the existing password and give a new password that will be unaware of the victim or the owner of the computer.

# Precautions against System Hacking

---

- The following are the precautionary points you should know to protect from system hacking or computer hacking:
- Use extreme caution while entering chatrooms or dealing with chatrooms' users online.
- Continuously check for the accuracy of the personal account.
- Carefully deal with friends' requests from online social networking sites and emails.
- Don't open or click unnecessary emails from strangers or unknown senders.

# **Point to keep in mind to protect system from hacking**

---

- Use both way firewall and keep updating.
- Update the OS for better patches.
- Avoid questionable websites.
- Use Internet Security Antivirus and Anti-malware software protection with definition updates.
- Increase the browser security settings.
- Download the required software from trusted sites only.
- Practice using safe email protocols such as SSL, SMTPS, etc.

# **Point to keep in mind to protect system from hacking Cont..**

---

- Check whether the sites are HTTPS or not for better secured online services and transactions.
- Immediately delete those messages which you suspect to be spam.
- Try to use genuine software(s) and not the pirated ones because the pirated ones could be reverse-engineered. Hackers can attach monitoring or malicious tools and programs with the software.

# Session Hijacking

---

- The importance of security is on the rise as digital innovation explodes. And as organizations launch more applications and evolve existing ones, the application attack surface grows. This provides cyber criminals with a greater opportunity to exploit application vulnerabilities. The threat is real: Verizon finds that 43% of data breaches are linked to application vulnerabilities.

# Session Hijacking Cont..

---

- One of the vulnerability attack vectors that cyber criminals find fruitful is session hijacking. Searching for small windows of opportunity, hackers use advanced breaching techniques, that are also known as cookie hijacking. The ability to tap in and monitor activity for the duration of a session can prove dangerous, especially in the case of highly sensitive information. Hackers can do this by squeezing in unnoticed, possibly taking over, and eventually kicking users out of the session.

# What Is a Session

---

- Though it seems like a complicated ENGAGEMENT of systems and networks, a computer's ability to communicate with a website comes from one single source. This source is known as the Transmission Control Protocol/Internet Protocol or TCP/IP. Certain limitations in TCP/IP are the reason it is vulnerable to attack. In an attempt to decrease the potential for attack, layers are added on top of TCP/IP in the hopes of stopping attacks long before they reach the core.

# **What Is a Session Cont..**

---

- Sessions refer to the time in which two systems are in communications with one another. Common systematic communications include computer-to-computer and client-to-server. From login to logout, information entered throughout the duration of communications is prone to storage depending on cookie settings. These cookies collect and store useful information for future logins. PHP scripts are the culprit behind this credential storage, with their unmatched connectivity properties that have revolutionized webpage interactions.

# What Is Session Hijacking

---

- When a session is hijacked, attackers slip in unnoticed and are able to monitor all activity taking place for the duration. Every session is marked with a session cookie, which reports back to the server. If an attacker obtains a session cookie, the session ID or session key is put at risk. With a session ID, hackers can input information into their own browser that is recognized by the server as the original connection.

# What Is Session Hijacking

---

- Larger corporations use cookies differently to enhance efficiency. Their single sign-on (SSO) systems collect information from several authenticated users at a time. A successful hijacking session puts all of these accounts at risk, as well as other applications connected within the system. When full access to accounts is achieved, servers cannot tell the difference and permit all activities without suspicion.

# What Is Session Hijacking

---

- With full access to an SSO, hackers have a huge database of information at their disposal. Information at risk includes personally identifiable information (PII), sensitive company details, among other data types. With access to these details, hackers have the ability to wreak havoc in multiple ways. Stopping application attacks before they start is the best way to combat session hijacking, accentuating the importance of understanding how session hijacking works and the potential damage attacks can cause.

# **Types of Vulnerabilities Exploited in Session Hijacking Attacks**

---

- Experienced hackers know that several application vulnerability options exist when it comes to session hijacking. Using advanced session hijacking techniques and a basis of vast programming knowledge, bad actors can decide which session hijacking method is best for the account or information they wish to exploit. Things like the exact pathway they will use to gain access and the chosen IP address come into play when selecting the best and most robust option.

# Cross-Site Scripting Vulnerabilities

---

- Cross-site scripting (XSS) vulnerabilities are the most popular attack vector used during a session takeover. Hackers look for XSS vulnerabilities in applications, injecting client-side scripts. Most typically, JavaScript is used and embedded into webpages. This newly written script will cause the browser to act as coded when loading a faulty page. If safeguards or application security tools are not in place, the loaded page provides hackers with sensitive information needed to uncover the session key. The most likely execution is in the form of email, one with the name and/or logo of a reputable company. Though it may seem legitimate, links within the email lead to malicious websites.

# Session Side-Jacking Vulnerabilities

- Session side-jacking likely comes to mind for many when session hijacking is mentioned. Hackers use packet sniffing to observe network activity. It requires the hacker to actively jump in after users have logged in successfully. This is especially dangerous for sites that use secure sockets layer/transport layer security (SSL/TLS) encryption for logging in, which allows impersonation of accounts if the session key is successfully acquired. Insecure Wi-Fi hotspots are a popular area that cyber criminals target with session side-jacking attacks, as they give them the option to set up their own access points for executing [man-in-the-middle-attacks](#).

# Session Fixation Vulnerabilities

---

- Bad actors often create malicious links that lead to fake websites—session fixation attacks. They do this hoping that users will click on them without a second thought. By clicking on the wrong link, users could provide cyber criminals access to session keys by leading them to a vulnerable server. If hackers pay close attention to detail, they can create a page that mimics that of a well-known company, and in turn, make it more difficult for users to spot suspicious or insecure activity. Once a user clicks on a link, a valid login form appears prompting users to log in. After their credentials are entered, attackers use the session key that is disclosed to take over the session.

# Malware Installation Vulnerabilities

---

- Another vulnerability initiated by clicking links is malware code installation. Malware is defined as any type of software created to damage a network, computer, or server. Bad apples with development skills generate this software and hide it in the form of a clickable link. If clicked, a download of the software begins immediately. Typical actions include scanning of web-based traffic hunting for session cookies along the way and access to local storage. Local storage, also known as the “cookie jar,” is a playground for attackers, providing direct access to the user’s cookie file.

# What Hackers Can Do with Session Hijacking

- Active monitoring is just the tip of the iceberg for session hijacking. Cyber criminals using session hijacking can completely take over a system, both at the network and application level. When hackers get access to an SSO, multiple applications are at risk. Cookie storage in SSO stores credentials used for all applications, including those with sensitive personal information. Entering directly into the server, attackers are essentially invisible during and after an application session. Then, long after users log out, hackers can create specific modifications to the server for future logins.

# What Hackers Can Do with Session Hijacking

---

- Neither users nor larger corporations may know they're victims of session hijacking until it is too late. Hijackers can silently track and monitor any activity, waiting for the right time to cause harm. This puts both financial and personal information at risk for both individuals and corporations. As both parties turn to applications for a more convenient way of doing things, the need to enhance their security rises.

# How to Prevent Session Hijacking

---

- Just like with most methods of protection, prevention is key. Stopping breaches before they can begin requires constant monitoring and updating of malware. Most of the time, ethical hackers attempt to point out vulnerabilities in servers in the hope of providing companies and individuals a sense of security. For the time being, session hijacking poses a large threat due to its exploitation of fundamental activities executed by the vast majority of web applications.
- Apart from basic safe surfing rules while on the web, both individuals and cybersecurity teams can reduce their risk of a hijacked session in a few ways. As the use of applications increases, shielded practices are key both during and after use.

# Use HTTP Headers to Tighten Up Security

---

- One iron-clad security system works by adding a few extra lines of code to the beginning of application scripts. For example, an X-XSS protection header stops malicious code in its tracks. There are thousands of headers out there, some approved by the Internet Engineering Task Force (IETF).

# **HTTP to HTTPS Redirects**

---

- For proper SSL/TLS encryption of all traffic during a session, it is best to use HTTPS, or more specifically, HSTS (HTTP Strict Transport Security). Unlike its four-letter counterpart (HTTP), HTTPS makes interception of plaintext session ID impossible even if they are monitoring activity. It also guarantees that all connections are encrypted, thus increasing the difficulty of session takeover. Embedding an HSTS header enforces applications to only connect to HTTPS and will redirect any HTTP activity.

# Embedding RASP

---

- Runtime application self-protection (RASP) embeds security instrumentation within the application it is protecting. This enables it to spot attacks on vulnerabilities and block them in real time. RASP can be thought of as a weapon used by applications to shield itself. From the time a session begins, it works to monitor activity, including data requests and application-to-system solicitations.

# Modify Caching

---

- Though caching works wonders for performance, it can put a damper on security. When using applications, sensitive information is stored in the browser's cache. If access to the computer is not limited to one sole user, anyone can access sensitive information. It could be as easy as hitting the "back" button, depending on the settings that are enabled. Further, disabling caching can become tedious, especially for those who are in and out of applications all day. That said, this could be an option only for those applications with confidential information.

# Keeping Applications Secure from Session Hijacking

- The threat that session hijacking imposes is substantial. Digital transformation is pushing companies to employ more online databases to handle the burgeoning amount of data that is now used by existing and growing numbers of new applications. Data breaches can be a huge risk exposure, providing cyber criminals with access to numerous accounts.
- Session hijacking attacks target a long list of application vulnerabilities, and when their exploitation is successful, bad actors can slip into a session unnoticed, sometimes detected too late. As a matter of fact, the average time it takes to notice an attack (dwell time) is about 95 days. Imagine what attackers can do with full access to accounts for such a long time. Because of its potential to cause irrefutable damage, session hijacking is on the long list of things security and operations teams need to heed.

# Keeping Applications Secure from Session Hijacking

---

- Today, most security measures focus on prevention, causing security teams to try and think ahead of hackers. It is becoming an inexorable cycle where both sides are successful time and time again. Legacy application security solutions that rely on penetration testing and application scanning simply cannot scale to support the modern software development life cycle (SDLC). Unable to keep up with SDLC, legacy application security approaches miss true vulnerabilities, generate large numbers of false positives, and incur growing security debt. Instead, organizations need to seek out application security that uses instrumentation to embed security within software and delivers continuous testing of software in development and monitoring of software once it is in production.

Question Please?

**THANK YOU**

# IP Spoofing Attack

---

**Dr. Ravi Verma**

# IP spoofing

---

- IP spoofing is a technique used to gain unauthorized access to computers, where by the attacker sends messages to a computer with a forging IP address indicating that the message is coming from a trusted host.
- Attacker puts an internal, or trusted, IP address as its source. The access control device sees the IP address as trusted and lets it through.

# IP Spoofing

---

IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer.

Two general techniques are used during IP spoofing:

- A hacker uses an IP address that is within the range of trusted IP addresses.
- A hacker uses an authorized external IP address that is trusted.

# Basic Concept of IP Spoofing

A

10.10.10.1  
http://  
www.carleton.ca

www.carleton.ca

134.117.1.60

10.10.10.1	134.117.1.60	Any (>1024)	80
------------	--------------	-------------	----

Src\_IP      dst\_IP      Src\_port      dst\_port

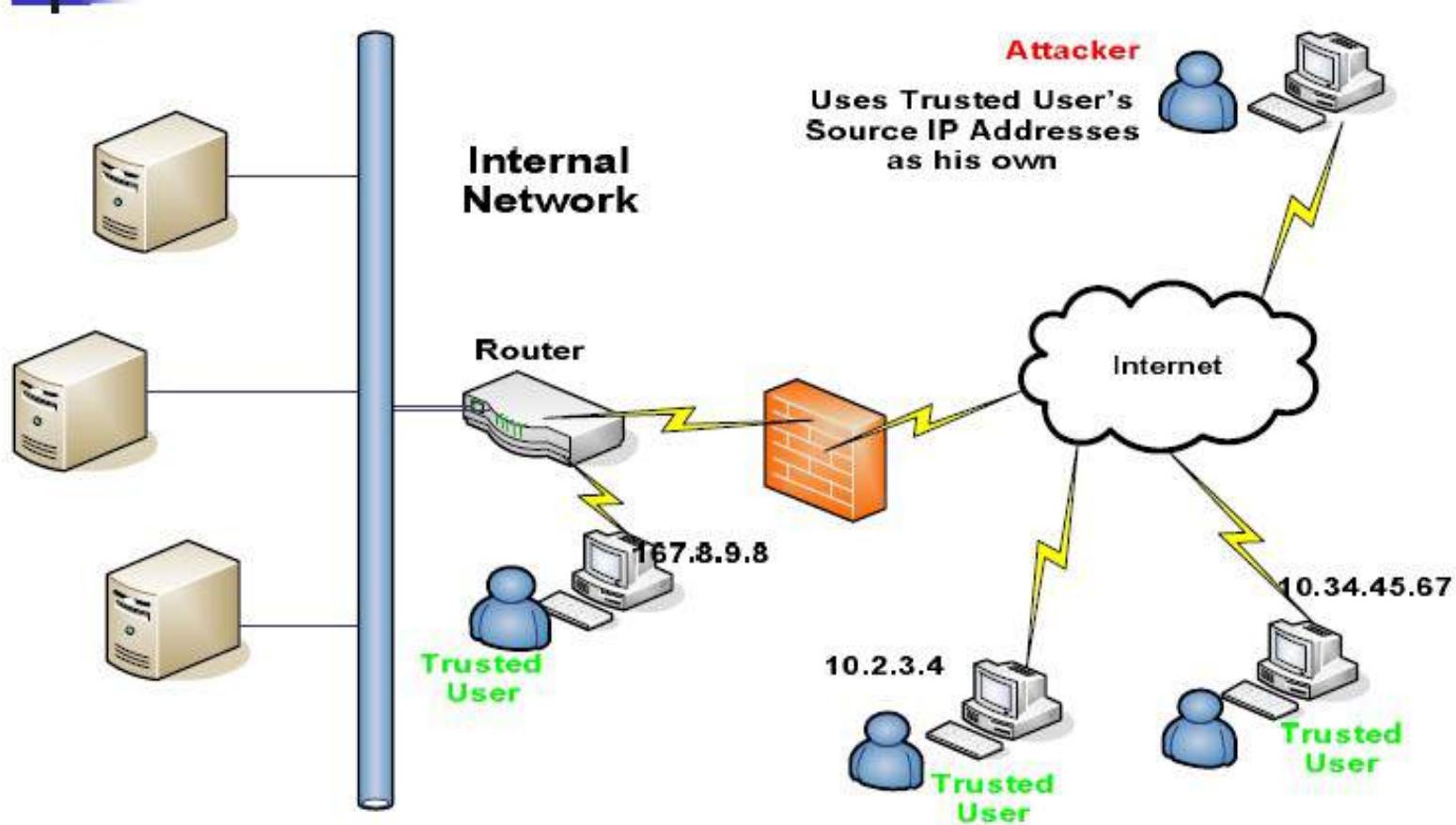
spoofed



11.11.11.1	134.117.1.60	Any (>1024)	80
------------	--------------	-------------	----

Src\_IP      dst\_IP      Src\_port      dst\_port

# IP Spoofing



# Why IP Spoofing is easy?

---

- Problem with the Routers.
- Routers look at Destination addresses only.
- Authentication based on Source addresses only.
- To change source address field in IP header field is easy.

# Spoofing Attacks:

---

There are a few variations on the types of attacks that use IP spoofing.

**Spoofing is classified into :-**

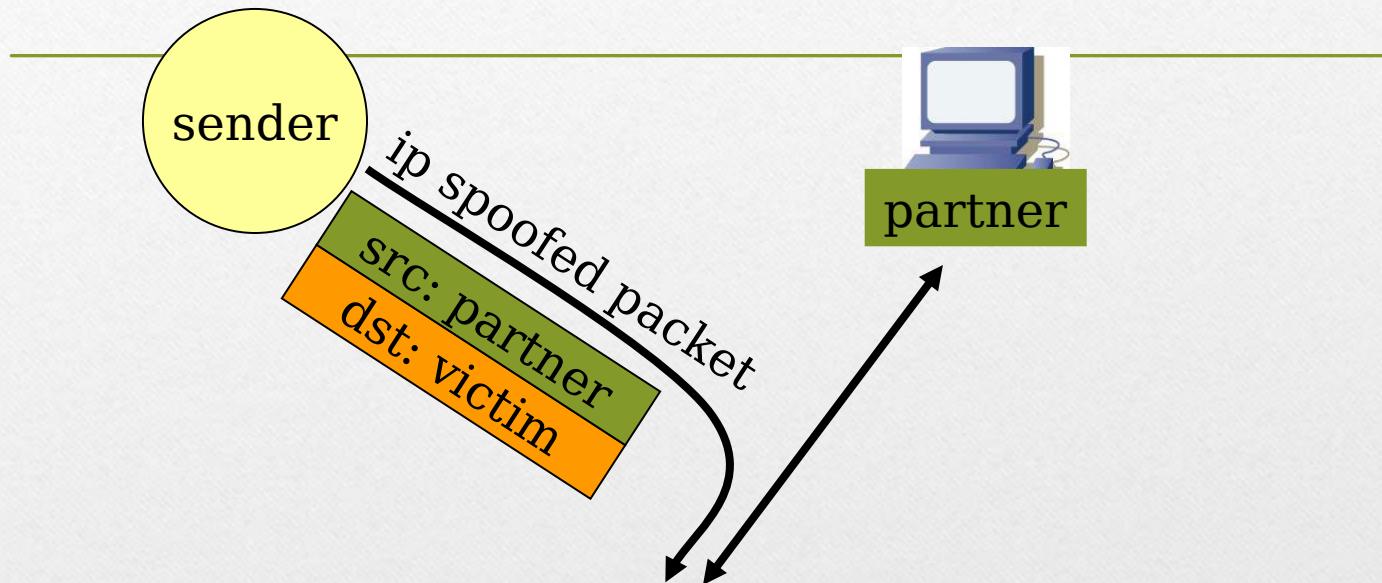
## **1. non-blind spoofing**

This attack takes place when the attacker is on the same subnet as the target that could see sequence and acknowledgement of packets.

- Using the spoofing to interfere with a connection that sends packets along your subnet.

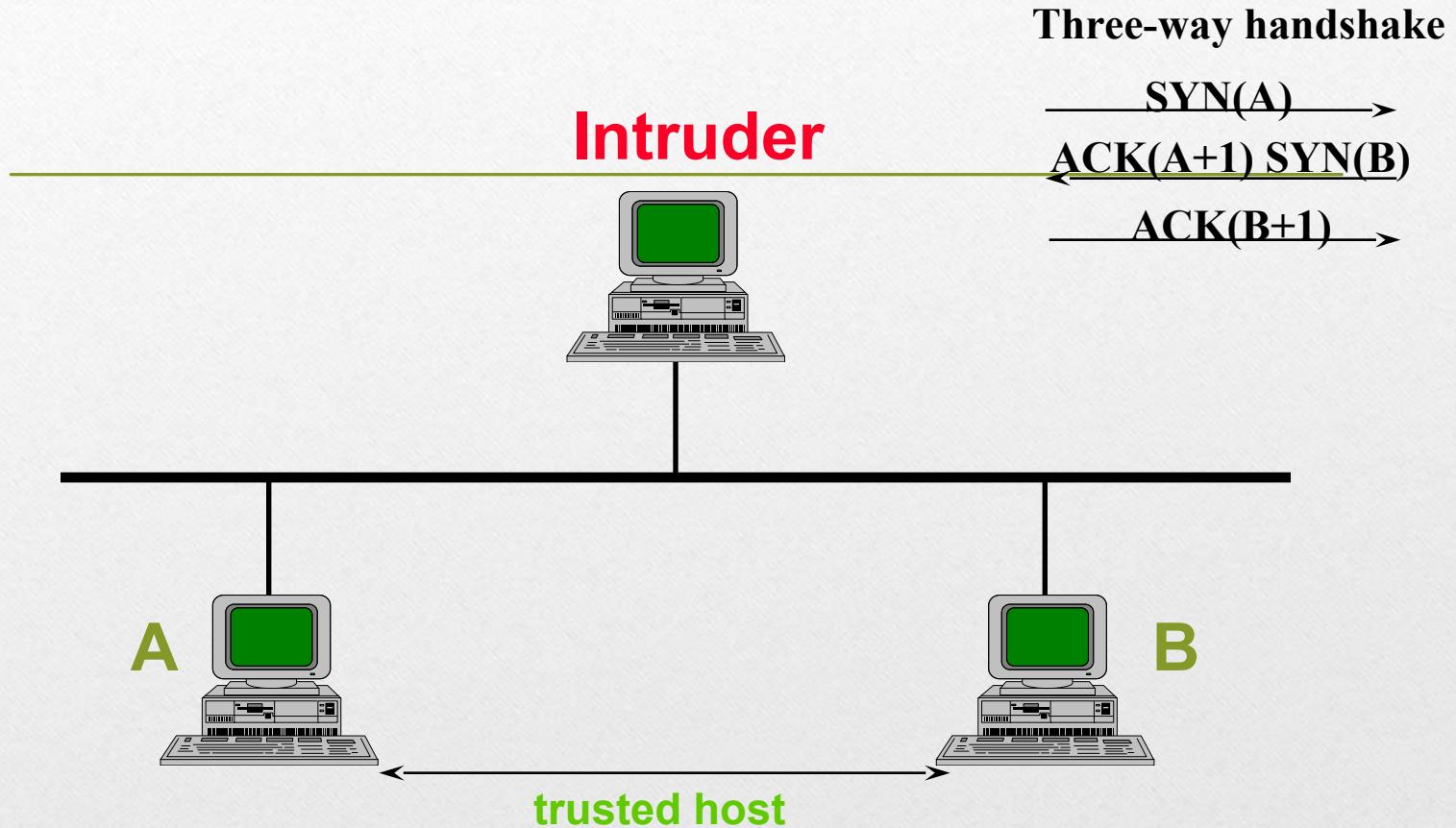
impersonati  
on

# Spoofing Attacks:



Oh, my partner  
sent me a packet.  
I'll process this.

# IP Spoofing



# **Spoofing Attacks:**

---

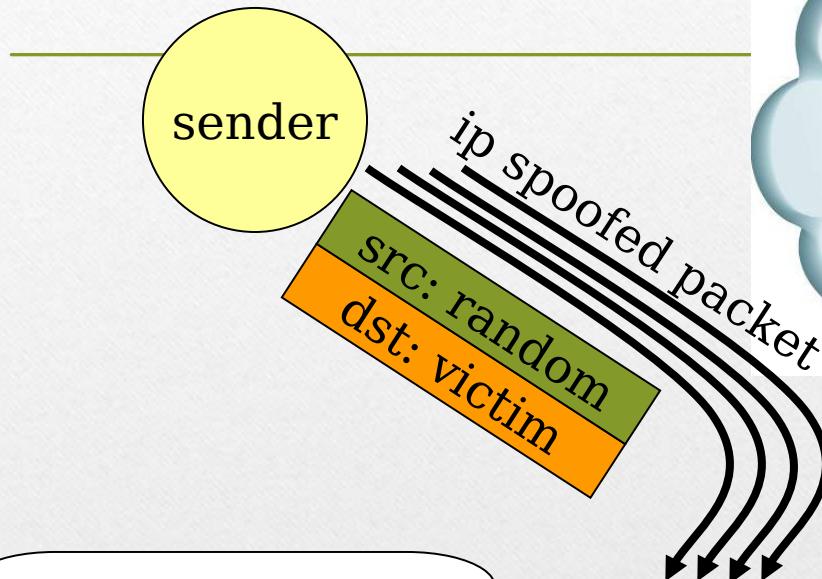
## **2. Blind spoofing**

This attack may take place from outside where sequence and acknowledgement numbers are unreachable. Attackers usually send several packets to the target machine in order to sample sequence numbers, which is doable in older days .

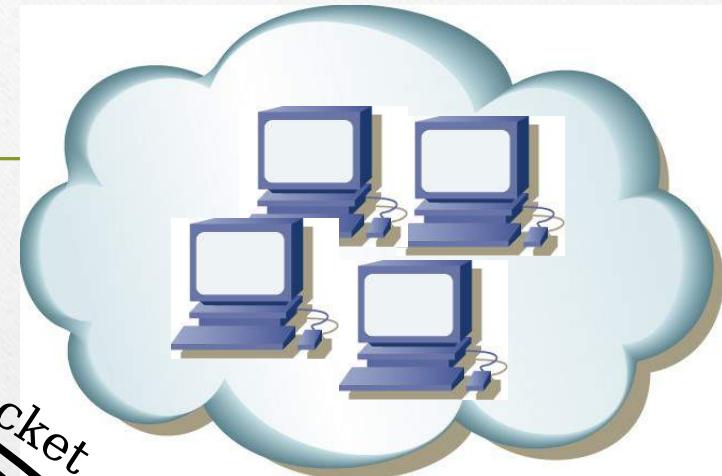
- Using the spoofing to interfere with a connection (or creating one), that does not send packets along your cable.

# Spoofing Attacks:

## flooding attack



Oops, many  
packets are  
coming. But, who  
is the real source?



# **Spoofing Attacks:**

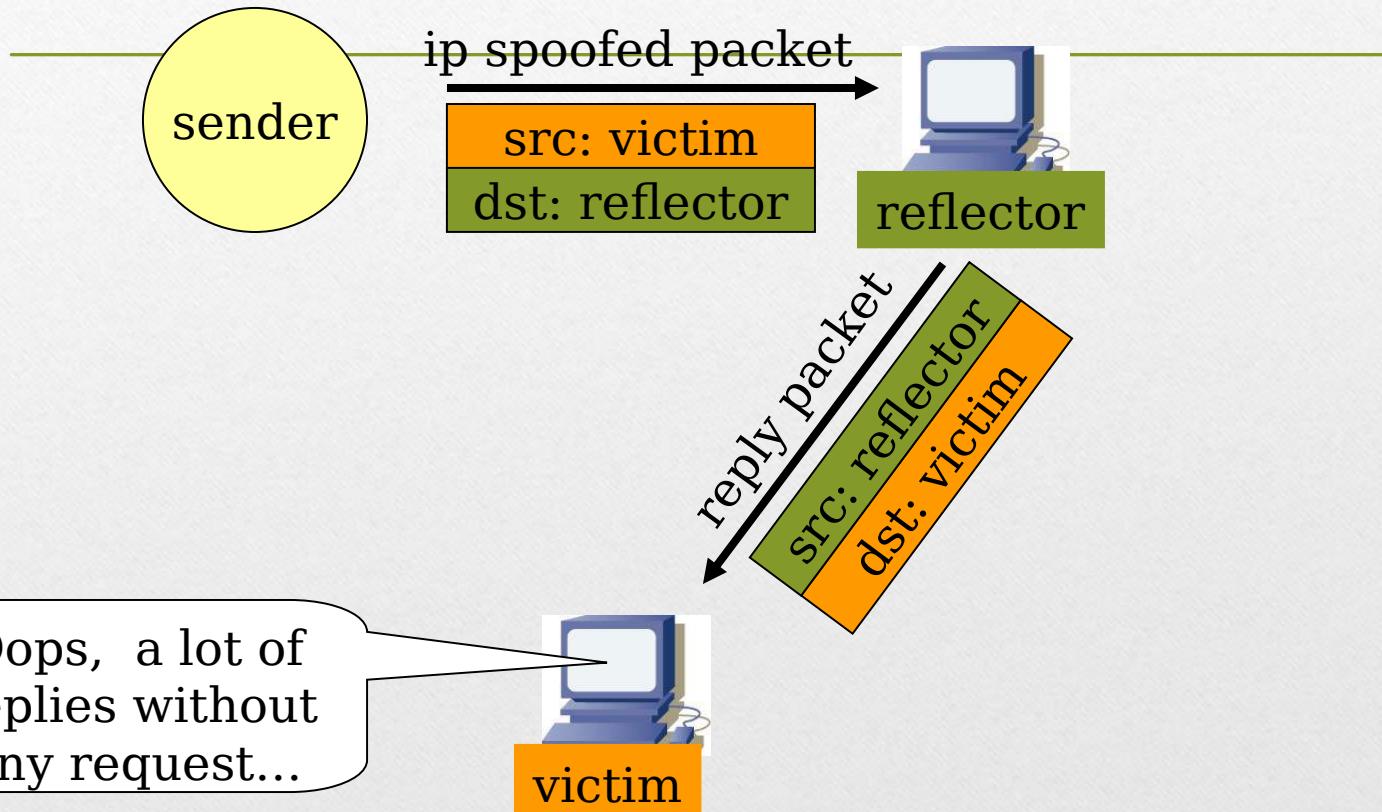
---

## **3. Man in the Middle Attack**

This is also called connection hijacking. In this attacks, a malicious party intercepts a legitimate communication between two hosts to controls the flow of communication and to eliminate or alter the information sent by one of the original participants without their knowledge.

# Spoofing Attacks:

## reflection



# Spoofing Attacks:

---

## 4.Denial of Service Attack

- conducting the attack, attackers spoof source IP addresses to make tracing and stopping the DoS as difficult as possible. When multiple compromised hosts are participating in the attack, all sending spoofed traffic, it is very challenging to quickly block the traffic.
- IP spoofing is almost always used in denial of service attacks (DoS), in which attackers are concerned with consuming bandwidth and resources by flooding the target with as many packets as possible in a short amount of time. To effectively

# Spoofing Attacks:

- IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. This method of attack on a remote system can be extremely difficult, as it involves modifying thousands of packets at a time. This type of attack is most effective where trust relationships exist between machines.
- For example, it is common on some corporate networks to have internal systems trust each other, so that a user can log in without a username or password provided they are connecting from another machine on the internal network (and so must already be logged in). By spoofing a connection from a trusted machine, an attacker may be able to access the target machine without authenticating.

# SMURF ATTACK

---

- Send ICMP ping packet with spoofed IP source address to a LAN which will broadcast to all hosts on the LAN
- Each host will send a reply packet to the spoofed IP address leading to denial of service

# Misconception of IP Spoofing:

---

A common misconception is that "IP Spoofing" can be used to hide your IP address while surfing the Internet, chatting on-line, sending e-mail, and so forth.

This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection. However, IP spoofing is an integral part of many networks that do not need to see responses.

# Impact

---

Current intruder activity in spoofing source IP addresses can lead to unauthorized remote root access to systems behind a filtering-router firewall. After gaining root access and taking over existing terminal and login connections, intruders can gain access to remote hosts.

# **Detection of IP Spoofing:**

---

1. If you monitor packets using network-monitoring software such as netlog, look for a packet on your external interface that has both its source and destination IP addresses in your local domain. If you find one, you are currently under attack.

# **Detection of IP Spoofing:**

---

2. Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network. If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access.

# **Detection of IP Spoofing:**

---

**Source Address Validation :**

- Check the source IP address of IP packets
  - filter invalid source address
  - filter close to the packets origin as possible
  - filter precisely as possible
- If no networks allow IP spoofing, we can eliminate these kinds of attacks

# Prevention IP spoofing

---

The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network in order to prevent a source IP spoofing attack originating from your site.

# Prevention IP spoofing

---

If your vendor's router does not support filtering on the inbound side of the interface or if there will be a delay in incorporating the feature into your system, you may filter the spoofed IP packets by using a second router between your external interface and your outside connection. Configure this router to block, on the outgoing interface connected to your original router, all packets that have a source address in your internal network.

# Prevention of IP Spoofing:

---

To prevent IP spoofing happen in your network, the following are some common practices:

- 1- Avoid using the source address authentication. Implement cryptographic authentication system-wide.
  - 2- Configuring your network to reject packets from the Net that claim to originate from a local address.
  - 3- Implementing ingress and egress filtering on the border routers and implement an ACL (access control list) that blocks private IP addresses on your downstream interface.
- If you allow outside connections from trusted hosts, enable encryption sessions at the router.

# Conclusion

---

- Presentation defines about Spoofing and its tools used to perform spoofing activities over the network or on any local or remote machine.
- Session describes How a local system can capture the network interface activities through Wireshark tools .

# Question

---

# **SnniffingAttack**

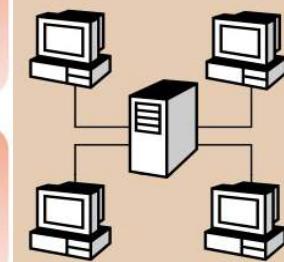
---

**Dr. Ravi Verma**

# SNIFFING

Sniffing is a data interception technology

Sniffer is a program or device that captures the vital information from the network traffic specific to a particular network



The objective of sniffing is to steal:

- Passwords (from email, the web, SMB, ftp, SQL, or telnet)
- Email text
- Files in transfer (email files, ftp files, or SMB)



# PROTOCOLS VULNERABILITIES

---

Protocols that are susceptible to sniffers include:

- Telnet and Rlogin: Keystrokes including user names and passwords
- HTTP: Data sent in the clear text
- SMTP: Passwords and data sent in clear text
- NNTP: Passwords and data sent in clear text
- POP: Passwords and data sent in clear text
- FTP: Passwords and data sent in clear text
- IMAP: Passwords and data sent in clear text

# **TYPES**

---

**There are two types of sniffing**

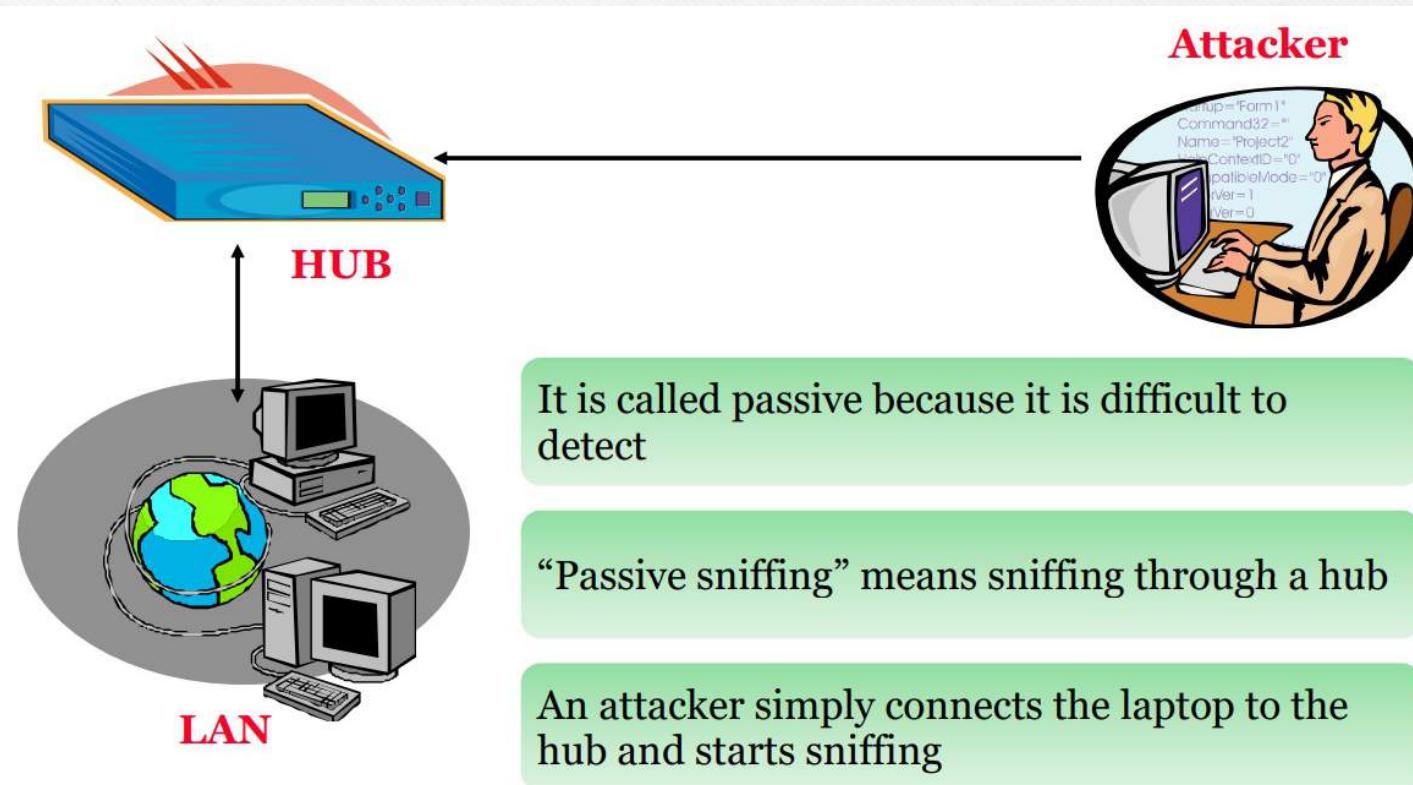
**Passive sniffing**

**Active sniffing**

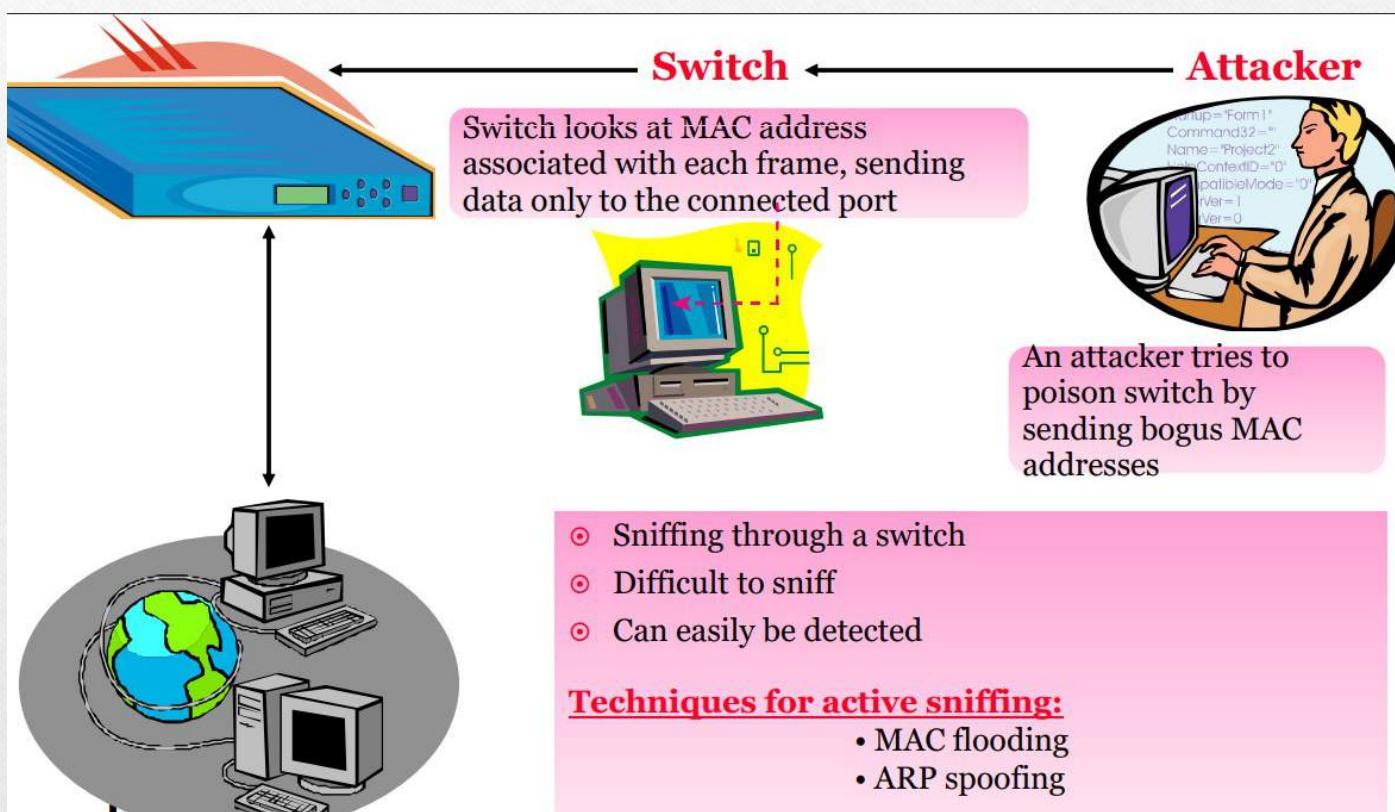
**Sniffing through a Hub**

**Sniffing through a Switch**

# PASSIVE SNIFFING



# ACTIVE SNIFFING



# Dude Sniffers

Developed by Mikro Tik, the Dude network monitor is a new application which can improve the way you manage your network environment

## Functions:

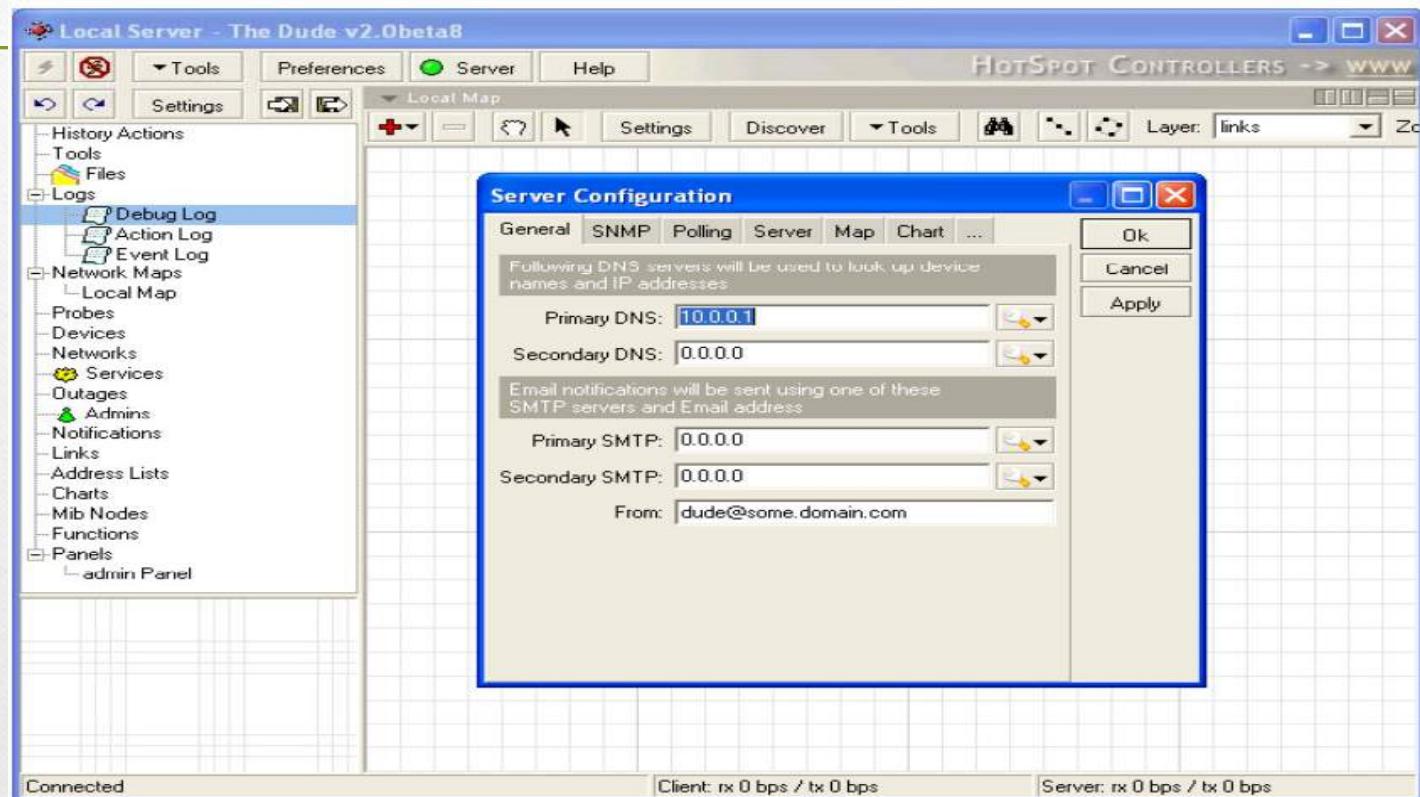
- Automatically scans all devices within the specified subr
- Draws and lays out a map of your networks
- Monitors services of your devices
- Alerts you in case some service has problems

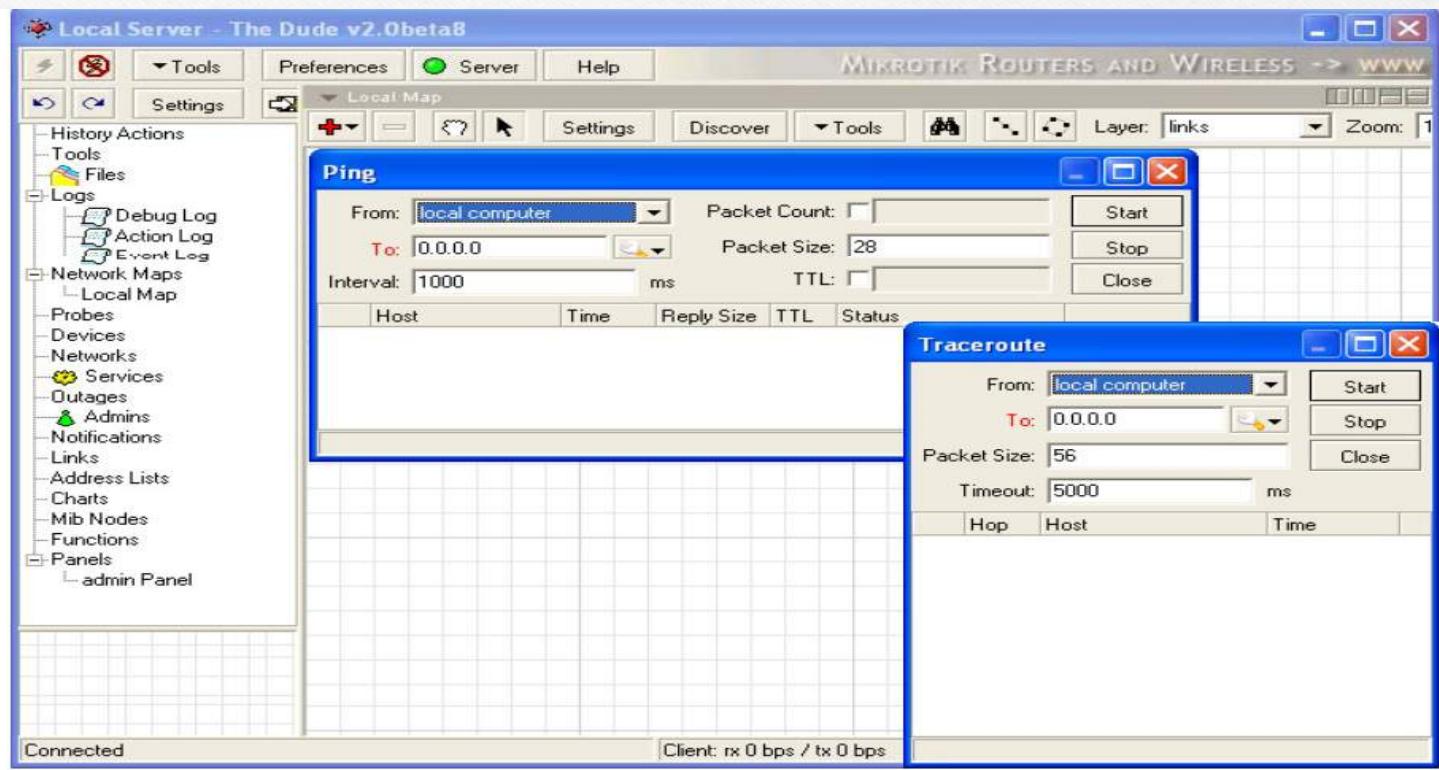


## It is written in two parts:

- Dude Server, which runs in a background
- Dude Client, which may connect to local or remote dude server

# DUDE TOOLS



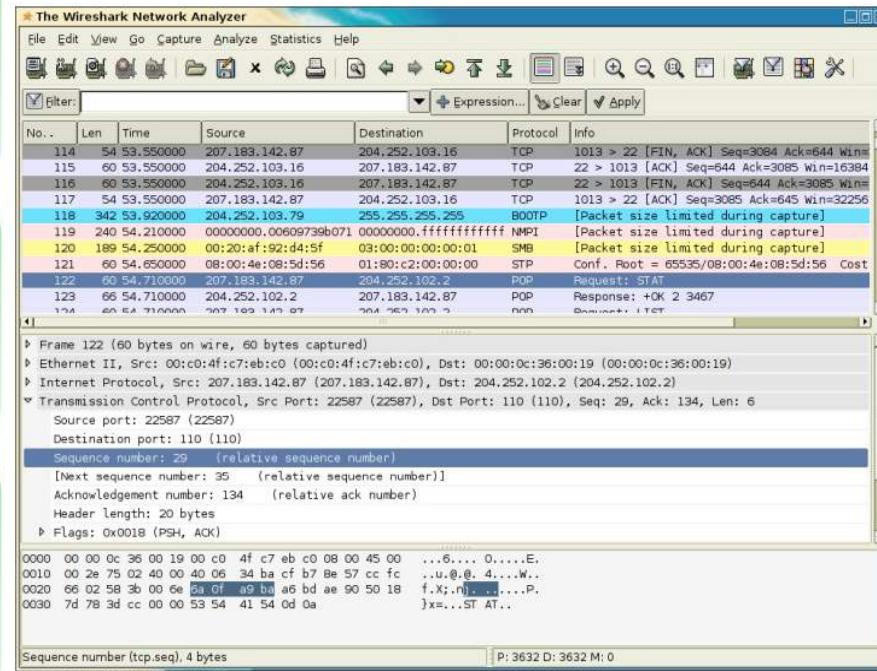


# WIRESHARK

Wireshark is a network protocol analyzer for UNIX and Windows

It allows user to examine data from a live network or from a capture file on a disk

User can interactively browse captured data, viewing summary, and detailed information for each packet captured



# Display Filters in Wireshark

Display filters are used to change the view of packets in captured files

## Display Filtering by Protocol

- Example: Type the protocol in the filter box
- arp, http, tcp, udp, dns

## Filtering by IP Address

- ip.addr == 10.0.0.4

## Filtering by multiple IP Addresses

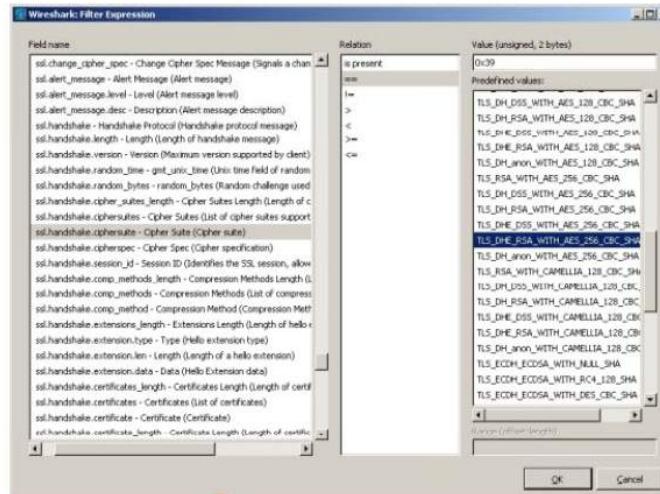
- ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5

## Monitoring Specific Ports

- tcp.port==443
- ip.addr==192.168.1.100 machine
- ip.addr==192.168.1.100 && tcp.port==443

## Other Filters

- ip.dst == 10.0.1.50 && frame.pkt\_len > 400
- ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30
- ip.src==205.153.63.30 or ip.dst==205.153.63.30



# TCP Stream in Wireshark

Wireshark reassembles all packets in a TCP conversation and displays ASCII in an easy-to-read format

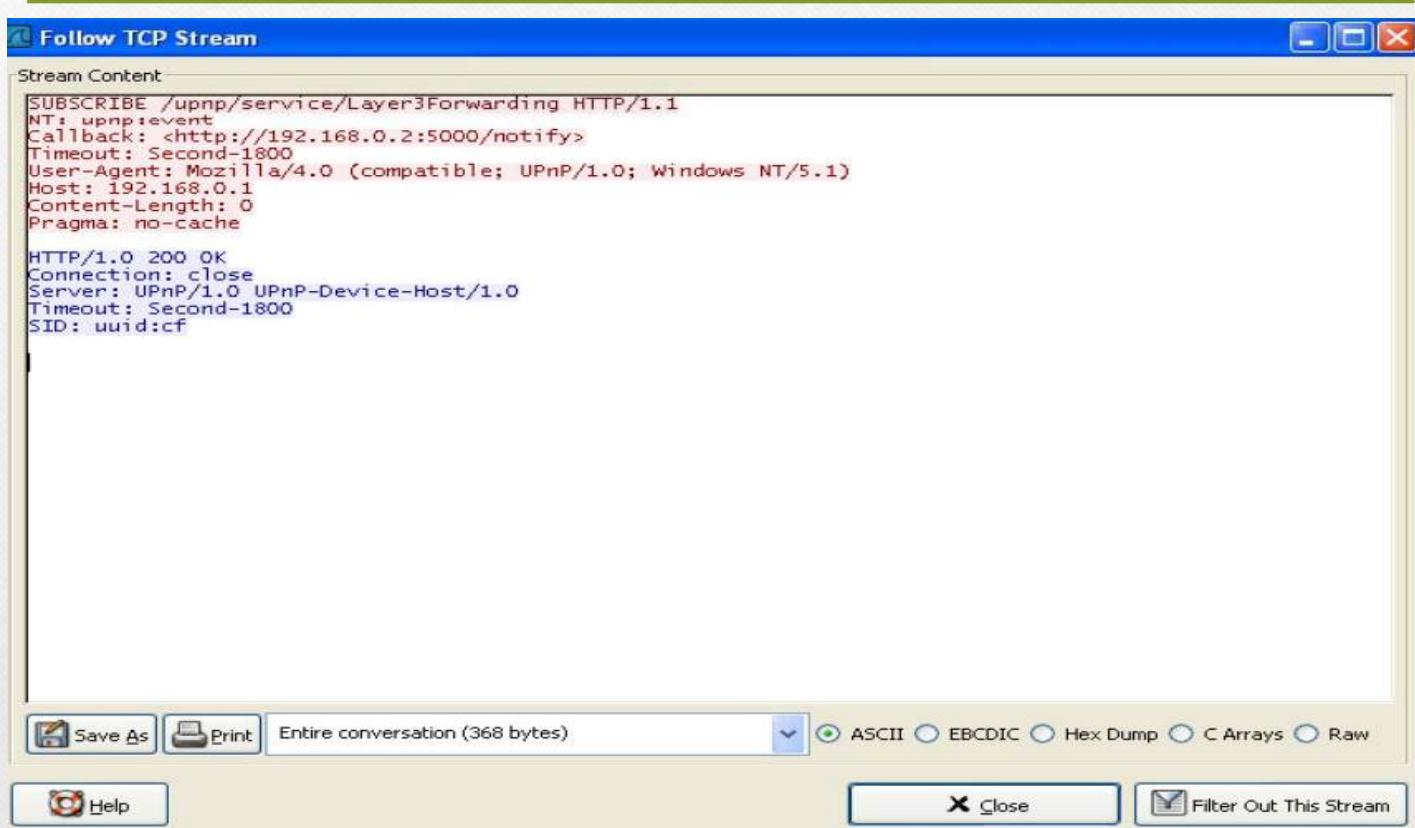
This makes it easy to pick out usernames and passwords from the insecure protocols such as Telnet and FTP

Example: Follow the stream of HTTP session and save the output to a file.

Command: Selecting a TCP packet in Summary Window and then selecting **Analyze -> Follow TCP Stream** from menu bar will display “Follow TCP Stream window”

You can also right-click on a TCP packet in Summary Window and choose “Follow TCP Stream” to display window

# TCP Streaming



# TCP dump commands

Tcpdump is a common computer network debugging tool that runs under command line

It allows user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached

```
tcpdump 3.5
tcpdump: listening on eth0
16:27:55.327528 137.133.57.68.1840 > 137.133.24.8.1352: tcp 0 (DF)
16:27:55.330724 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 592
16:27:55.333843 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:55.336912 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:55.340174 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:55.343629 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 568
16:27:55.346749 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:55.348488 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:55.349433 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 592
16:27:55.349807 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:55.450144 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:55.456636 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:55.657583 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:55.660951 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:55.661052 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:55.661254 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 592
16:27:55.664687 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 616
16:27:55.887807 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:55.890666 137.133.63.36.1736 > 137.133.16.54.32793: tcp 0 (DF)
16:27:55.893988 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:55.987881 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:55.994454 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1112
16:27:55.999215 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:56.000966 137.133.63.36.32272 > 137.133.16.53.1730: tcp 147 (DF)
16:27:56.004058 137.133.63.36.32279 > 137.133.16.53.1730: tcp 147 (DF)
16:27:56.2M729 nerra->x1m3: nerra.y.loc.serv? udpt 2048
16:27:56.31192 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 664
16:27:56.316689 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 834
16:27:56.219819 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:56.222877 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 326
16:27:56.318051 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:56.321065 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:56.322222 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:56.327222 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 79
16:27:56.330286 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:56.333267 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 700
16:27:56.428808 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:56.538029 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 460
16:27:56.541896 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:56.542839 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:56.548239 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:56.651262 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 616
16:27:56.654247 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
16:27:56.657292 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 1160
16:27:56.660425 209.1.224.18.wwn-http > 137.133.57.68.1255: tcp 911
16:27:56.663376 137.133.57.68.1255 > 209.1.224.18.wwn-http: tcp 0 (DF)
```

# TCP dump commands

## Exporting tcpdumps to a file

- `# tcpdump port 80 -l > webdump.txt & tail -f webdump.txt`
- `# tcpdump -w rawdump`
- `# tcpdump -r rawdump > rawdump.txt`
- `# tcpdump -c1000 -w rawdump`
- `# tcpdump -i eth1 -c1000 -w rawdump`

## Captures traffic on a specific port

- `# tcpdump port 80`

You can select several hosts on your LAN and capture the traffic that passes between them

- `# tcpdump host workstation1 and workstation11 and workstation12`

# TCP dump Commands

## Cont..

---

Capture all the LAN traffic between workstation4 and the LAN, except for workstation11

- # tcpdump -e host workstation4 and workstation11 and workstation13

Capture all packets except those for certain ports

- # tcpdump not port 110 and not port 25 and not port 53 and not port 22

Filter by protocol

- # tcpdump udp
- # tcpdump ip proto OSPFIGP

Capture traffic on a specific host and restrict by protocol

- # tcpdump host server02 and ip
- # tcpdump host server03 and not udp
- # tcpdump host server03 and ip and igmp and not udp



## Linux Sniffing Tools

syllabus.pdf

The First 10 Things to Do After... Kali Linux - Sniffing & Spoofing Fwd: Webinar on Blockchain for... Sniffers.pdf

File | D:/VIT/Ethical%20Hacking/Sniffers.pdf

This file has limited permissions. You may not have access to some features. [View permissions](#)

# CEH TM Certified Ethical Hacker

## Linux Sniffing Tools (cont'd)

- sshmitm**
  - SSH monkey-in-the-middle
- tcpkill**
  - Kills TCP connections on a LAN
- tcpnice**
  - Slows down TCP connections on a LAN
- urlsnarf**
  - Sniffs HTTP requests in Common Log Format
- webspy**
  - Displays sniffed URLs in Netscape in real time
- webmitm**
  - HTTP/HTTPS monkey-in-the-middle



Copyright © by EC-Council  
All Rights Reserved. Reproduction is Strictly Prohibited

ENG IN 15:55 24-02-2022

# Sniffing Atools

## Sniffer hacking tools (These tools are available on the Link)

### arpspoof

- Intercepts packets on a switched LAN

### dnsspoof

- Forges replies to DNS address and pointer queries

### dsniff

- Password sniffer

### filesnarf

- Sniffs files from NFS traffic

### mailsnarf

- Sniffs mail messages in Berkeley mbox format

### msgsnarf

- Sniffs chat messages

# How to Detect Sniffing

---

You will need to check which machines are running in promiscuous mode

Run ARPWATCH and notice if the MAC address of certain machines has changed (Example: router's MAC address)

Run network tools like HP OpenView and IBM Tivoli network health check tools to monitor the network for strange packets

# Countermeasures

---

Restriction of physical access to network media ensures that a packet sniffer cannot be installed

The best way to be secured against sniffing is to use encryption. It would not prevent a sniffer from functioning but will ensure that what a sniffer reads is not important

ARP Spoofing is used to sniff a switched network, so an attacker will try to ARP spoof the gateway. This can be prevented by permanently adding the MAC address of the gateway to the ARP cache

# Countermeasures

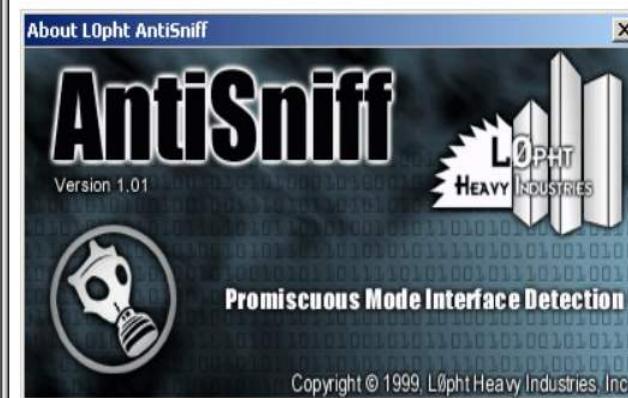
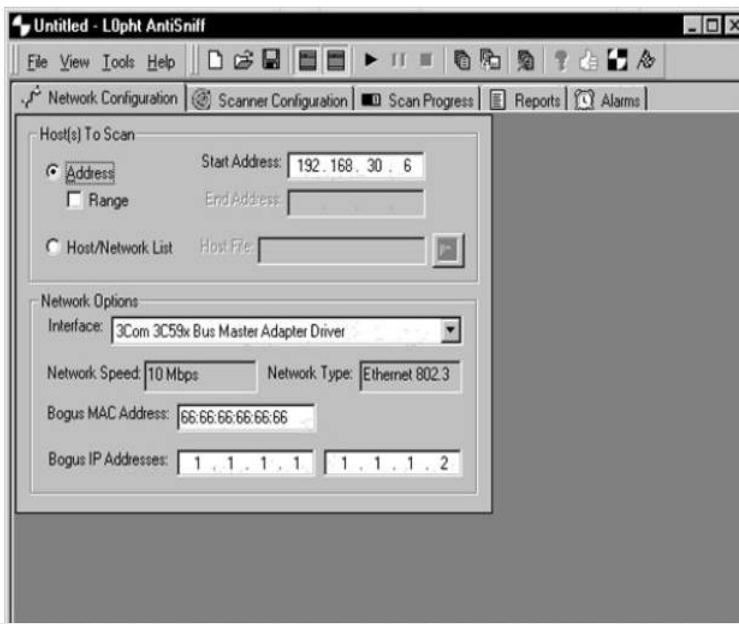
---

There are various tools to detect a sniffer in a network:

- ARP Watch
- Promiscan
- Antisniff
- Prodetect

# Anti-sniff Tool

AntiSniff tool can detect machines on the network that are running in the promiscuous mode



---

- Question ? Please

# **VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING**

---

## **Chapter 2: PEN TESTING**

**By  
Dr. Ravi Verma**

# **Contents To Be Discuss**

---

- **What Is Penetration Testing?**
- **Causes of Vulnerability**
- **Penetration Testing Tools and Companies**
- **Criteria for selecting the best penetration tool**
- **Recommended Penetration Testing Tools**
- **Other Free Tools**
- **Why Penetration Testing?**
- **Penetration Testing is mainly required for**
- **What Should Be Tested?**

# **Contents To Be Discuss Cont.**

---

...

- **Penetration Testing Types**
- **Types of penetration testing into three parts**
- **Pen Testing Techniques**
- **We can categorize this process in the following methods**
- **Conclusion**

# **What Is Penetration Testing?**

---

- We can figure out the vulnerabilities of a computer system, a web application or a network through penetration testing.
- A penetration test will tell whether the existing defensive measures employed on the system are strong enough to prevent any security breaches. Penetration test reports also suggest countermeasures which can be taken to reduce the risk of the system being hacked.

# Causes of Vulnerability

---

- **Design and Development Errors:** There can be flaws in the design of hardware and software. These bugs can put your business-critical data at risk of exposure.
- **Poor System Configuration:** This is another cause of vulnerability. If the system is poorly configured, then it can introduce loopholes through which attackers can enter into the system & steal the information.
- **Human errors:** Human factors like improper disposal of documents, leaving the documents unattended, coding errors, insider threats, sharing passwords over phishing sites, etc. can lead to security breaches.
- **Connectivity:** If the system is connected to an unsecured network (open connections) then it comes within the reach of hackers.

# Causes of Vulnerability

## Cont..

---

- **Complexity:** The security vulnerability rises in proportion to the complexity of a system. The more features a system has, the more are the chances of the system being attacked.
- **Password:** Passwords are used to prevent unauthorized access. They should be strong enough that no one can guess your password. Passwords should not be shared with anyone at any cost and passwords should be changed periodically. In spite of these instructions, at times people reveal their passwords to others, write them down somewhere and keep easy passwords that can be guessed.
- **User Input:** You must have heard of SQL injection, buffer overflows, etc. The data received electronically through these methods can be used to attack the receiving system.

# Causes of Vulnerability

## Cont..

---

- **Management:** Security is hard & expensive to manage. Sometimes organizations lack behind in proper risk management and hence vulnerability gets induced in the system.
- **Lack of training to staff:** This leads to human errors and other vulnerabilities.
- **Communication:** Channels like mobile networks, internet, telephone opens up security theft scope.

# **Penetration Testing Tools and Companies**

---

- Automated tools can be used to identify some standard vulnerabilities present in an application. Pentest tools scan code to check if there is a malicious code present which can lead to a potential security breach.
- Pentest tools can verify security loopholes present in the system by examining data encryption techniques and figuring out hard-coded values like usernames and passwords.

# **Criteria for selecting the best penetration tool**

---

- It should be easy to deploy, configure and use.
- It should scan your system easily.
- It should categorize vulnerabilities based on severity that need an immediate fix.
- It should be able to automate the verification of vulnerabilities.
- It should re-verify the exploits found previously.
- It should generate detailed vulnerability reports and logs.
- Once you know what tests you need to perform you can either train your internal test resources or hire expert consultants to do the penetration task for you.

# **Recommended Penetration Testing Tools**

---

## **1) Acunetix**

Acunetix WVS offers security professionals and software engineers alike a range of stunning features in an easy, straight-forward, and very robust package.

## **2) Intruder**

is a powerful vulnerability scanner that finds cybersecurity weaknesses in your digital estate, explains the risks & helps with their remediation before a breach can occur. It is the perfect tool to help automate your penetration testing efforts.

# Other Free Tools

---

- Nmap
- Nessus
- Metasploit
- Wireshark
- OpenSSL

# Why Penetration Testing?

---

- You must have heard of the WannaCry ransomware attack that started in May 2017. It locked more than 2 lakh computers around the world and demanded ransom payments from the Bitcoin cryptocurrency. This attack has affected many big organizations around the globe.
- With such massive & dangerous cyber-attacks happening these days, it has become unavoidable to do penetration testing at regular intervals to protect the information systems against security breaches.

# **Penetration Testing is mainly required for**

---

- Financial or critical data must be secured while transferring it between different systems or over the network.
- Many clients are asking for pen testing as part of the software release cycle.
- To secure user data.
- To find security vulnerabilities in an application.
- To discover loopholes in the system.
- To assess the business impact of successful attacks.
- To meet the information security compliance in the organization.
- To implement an effective security strategy within the organization .

# What Should Be Tested?

---

- Software (Operating systems, services, applications)
  - Hardware
  - Network
  - Processes
  - End-user behavior



# Penetration Testing Types

---

- 1) Social Engineering Test:** In this test, attempts are being made to make a person reveal sensitive information like passwords, business-critical data, etc. These tests are mostly done through phone or internet and it targets certain helpdesks, employees & processes.
- 2) Web Application Test:** Using software methods, one can verify if the application is exposed to security vulnerabilities. It checks the security vulnerability of web apps and software programs positioned in the target environment.

# Penetration Testing

## Types Cont..

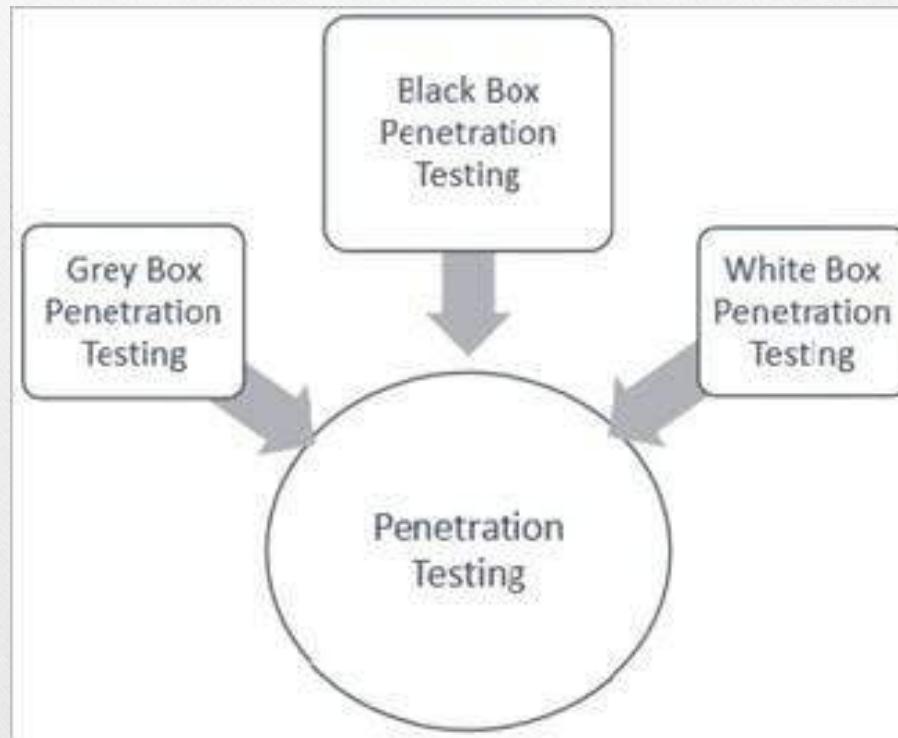
- 
- 3) Physical Penetration Test:** Strong physical security methods are applied to protect sensitive data. This is generally used in military and government facilities. All physical network devices and access points are tested for the possibility of any security breach. This test is not very relevant to the scope of software testing.
  
  - 4) Network Services Test:** This is one of the most commonly performed penetration tests where the openings in the network are identified by which entry is being made in the systems on the network to check what kind of vulnerabilities are there. This can be done locally or remotely.

# Penetration Testing

## Types Cont..

- 
- 5) Client-side Test:** It aims to search and exploit vulnerabilities in client-side software programs.
  
  - 6) Remote dial-up war dial:** It searches for modems in the environment and tries to log in to the systems connected through these modems by password guessing or brute-forcing.
  
  - 7) Wireless Security Test:** It discovers open, unauthorized and less secure hotspots or Wi-Fi networks and connects through them.

# Types of penetration testing into three parts



# types of penetration testing into three parts

- **Black Box Penetration Testing:** In this approach, the tester assesses the target system, network or process without the knowledge of its details. They just have a very high level of inputs like URL or company name using which they penetrate the target environment. No code is being examined in this method.
- **White Box Penetration Testing:** In this approach, the tester is equipped with complete details about the target environment – Systems, network, OS, IP address, source code, schema, etc. It examines the code and finds out design & development errors. It is a simulation of an internal security attack.
- **Grey Box Penetration Testing:** In this approach, the tester has limited details about the target environment. It is a simulation of external security attacks.

# Pen Testing Techniques

---

- Manual Penetration Test
- Using automated penetration testing tools.
- Combination of both manual and automated processes.

# **Pen Testing Techniques Cont..**

---

## **Manual Penetration Test:**

It's difficult to find all vulnerabilities using automated tools. There are some vulnerabilities that can only be identified by manual scan. Penetration testers can perform better attacks on applications based on their skills and knowledge of the system being penetrated.

# **Pen Testing Techniques Cont..**

---

## **Penetration Test Process:**

Let's discuss the actual process followed by test agencies or penetration testers. Identifying vulnerabilities present in the system is the first important step in this process. Corrective action is taken on this vulnerability and the same penetration tests are repeated until the system is negative to all those tests.

# We can categorize this process in the following methods

---

- 1) Data Collection:** Various methods including Google search are used to get target system data. One can also use the web page source code analysis technique to get more info about the system, software and plugin versions.
- 2) Vulnerability Assessment:** Based on the data collected in the first step, one can find the security weakness in the target system. This helps penetration testers to launch attacks using identified entry points in the system.

# We can categorize this process in the following methods

---

**3) Actual Exploit:** This is a crucial step. It requires special skills and techniques to launch an attack on the target system. Experienced penetration testers can use their skills to launch an attack on the system.

**4) Result in analysis and report preparation:** After completion of penetration tests, detailed reports are prepared for taking corrective actions. All identified vulnerabilities and recommended corrective methods are listed in these reports. You can customize the vulnerability report format (HTML, XML, MS Word or PDF) as per your organization's needs.

# Conclusion

---

- Finally, as a penetration tester, you should collect and log all vulnerabilities in the system. Don't ignore any scenario considering that it won't be executed by the end-users.
- *If you are a penetration tester, please help our readers with your experience, tips, and sample test cases on how to perform Penetration Testing effectively.*

Question Please?

**THANK YOU**

# VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING

---

Chapter 2: **Sniffers**

By  
Dr. Ravi Verma

# **Outcome of Session**

---

- **Students will be able to :**
- Explore the concept of Network Trapping through different Sniffing Tools and Techniques .
- Can list the tools used for Sniffing the network traffic as well as monitoring network activities.

# **Contents To Be Discuss**

---

- **Sniffing**
- **What can be Sniffed?**
- **How it works?**
- **Sniffing the Networks**
- **Types of Sniffing**
- **Active Sniffing**
- **Passive Sniffing**
- **Protocols which are affected**
- **Hardware Protocols Analyzer**
- **Lawful Inspections**
- **Sniffing Tools**

# Sniffing

---

- Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.

# **Sniffing Cont..**

---

- In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

# What can be sniffed?

---

- One can sniff the following sensitive information from a network
  -
- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

# How it works?

---

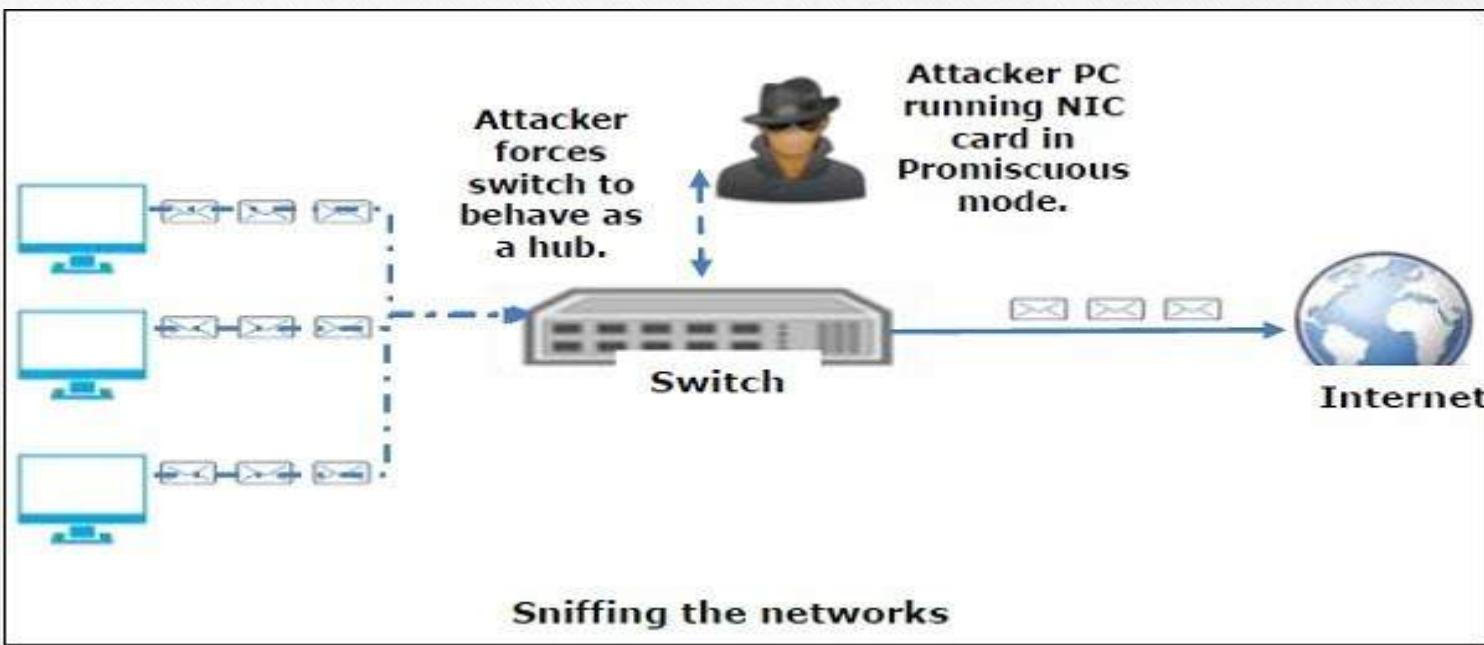
- A sniffer normally turns the NIC of the system to the **promiscuous mode** so that it listens to all the data transmitted on its segment.
- Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC.

# **How it works? Cont..**

---

- By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

# Sniffing the Networks



A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

# **Types of Sniffing**

---

## **Passive Sniffing**

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

# Types of Sniffing Cont..

---

- **Active Sniffing**
- In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution packets** (ARP) into a target network to flood on the switch **content addressable memory** (CAM) table. CAM keeps track of which host is connected to which port.

# Active Sniffing

---

- Following are the Active Sniffing Techniques –
- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

# Protocols which are affected

---

- Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing –
- **HTTP** – It is used to send information in the clear text without any encryption and thus a real target.
- **SMTP** (Simple Mail Transfer Protocol) – SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.

# Protocols which are affected Cont..

- 
- **NNTP** (Network News Transfer Protocol)– It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.
  - **POP** (Post Office Protocol) – POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
  - **FTP** (File Transfer Protocol) – FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.

# Protocols which are affected Cont..

---

- **IMAP** (Internet Message Access Protocol) – IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
- **Telnet** – Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

Sniffers are not the dumb utilities that allow you to view only live traffic. If you really want to analyze each packet, save the capture and review it whenever time allows.

# Hardware Protocol Analysers

---

Before we go into further details of sniffers, it is important that we discuss about **hardware protocol analyzers**. These devices plug into the network at the hardware level and can monitor traffic without manipulating it.

Hardware protocol analyzers are used to monitor and identify malicious network traffic generated by hacking software installed in the system.

# Hardware Protocol Analysers

---

- They capture a data packet, decode it, and analyze its content according to certain rules.
- Hardware protocol analyzers allow attackers to see individual data bytes of each packet passing through the cable.

These hardware devices are not readily available to most ethical hackers due to their enormous cost in many cases.

# Lawful Interception

---

- Lawful Interception (LI) is defined as legally sanctioned access to communications network data such as telephone calls or email messages. LI must always be in pursuance of a lawful authority for the purpose of analysis or evidence. Therefore, LI is a security process in which a network operator or service provider gives law enforcement officials permission to access private communications of individuals or organizations.

# Lawful Interception

- 
- Almost all countries have drafted and enacted legislation to regulate lawful interception procedures; standardization groups are creating LI technology specifications. Usually, LI activities are taken for the purpose of infrastructure protection and cyber security. However, operators of private network infrastructures can maintain LI capabilities within their own networks as an inherent right, unless otherwise prohibited.
  -

# Sniffing Tools

---

- There are so many tools available to perform sniffing over a network, and they all have their own features to help a hacker analyze traffic and dissect the information. Sniffing tools are extremely common applications. We have listed here some of the interesting ones –
- **BetterCAP** – BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real-time, sniff for credentials, and much more.

# Sniffing Tools Cont..

---

- **Ettercap** – Ettercap is a comprehensive suite for man-in-the-middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.
- **Wireshark** – It is one of the most widely known and used packet sniffers. It offers a tremendous number of features designed to assist in the dissection and analysis of traffic.
- **Tcpdump** – It is a well-known command-line packet analyzer. It provides the ability to intercept and observe TCP/IP and other packets during transmission over the network. Available at [www.tcpdump.org](http://www.tcpdump.org).

# Sniffing Tools

---

- **WinDump** – A Windows port of the popular Linux packet sniffer tcpdump, which is a command-line tool that is perfect for displaying header information.
- **OmniPeek** – Manufactured by WildPackets, OmniPeek is a commercial product that is the evolution of the product EtherPeek.
- **Dsniff** – A suite of tools designed to perform sniffing with different protocols with the intent of intercepting and revealing passwords. Dsniff is designed for Unix and Linux platforms and does not have a full equivalent on the Windows platform.

# Sniffing Tools

---

- **EtherApe** – It is a Linux/Unix tool designed to display graphically a system's incoming and outgoing connections.
- **MSN Sniffer** – It is a sniffing utility specifically designed for sniffing traffic generated by the MSN Messenger application.
- **NetWitness NextGen** – It includes a hardware-based sniffer, along with other features, designed to monitor and analyze all traffic on a network. This tool is used by the FBI and other law enforcement agencies.
- A potential hacker can use any of these sniffing tools to analyze traffic on a network and dissect information.

Question Please?

**THANK YOU**

# **VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING**

---

## **UNIT 02**

### **LECTURE 04 Installation of VMware & Kali Linux for Pen Testing**

By  
**Dr. Ravi Verma**

## **Output of this Presentation**

---

- Students will be able to Install various tools and software like VMware, Kali Linux to perform Pen Testing .

# **Contents To Be Discuss**

---

- **What is Virtualization**
- **How does Virtualization works**
- **What is Virtual Machine**
- **Why use Virtual MACHINE**
- **Installation of Vmware**
- **What is Kali Linux ?**
- **Kali Linux Utalities**
- **Who use Kali Linux and Why ?**
- **Downloading of Kali Linux ISO Image**

# **Contents To Be Discuss Cont.**

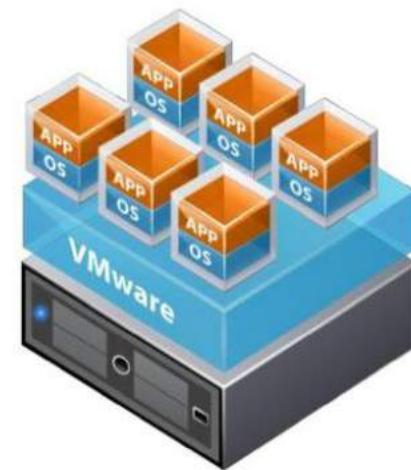
...

- 
- **Installation of Kali Linux Image on VMware machine.**

# WHAT IS VIRTUALIZATION

---

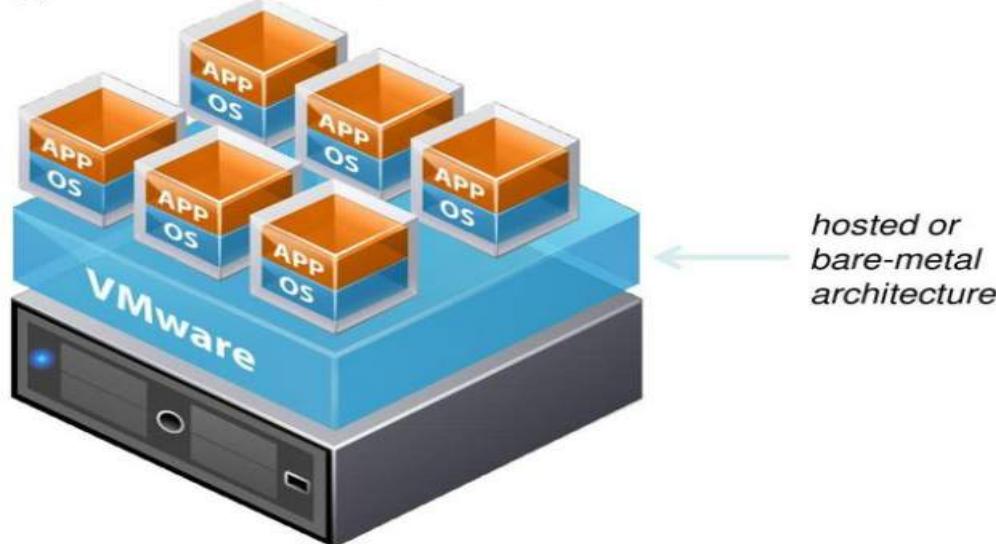
- Virtualization is the technology that transforms hardware into software's, Virtualization allows you to run multiple operating systems as a virtual machines on a single computer.
- Each copy of an operating system installed into an virtual machine.



# How does Virtualization works

- A virtualization layer is installed. It uses either as a hosted or a bare metal

~~hypervisor architecture~~



# What is Virtual Machine

---

- A virtual machine is a software platform that like a physical computer, runs an operating system and applications .



# **Why use virtual machine**

---

## **Physical Machine**

- Difficult to move or copy beyond to specific set of hardware components.
- Require personal interaction to upgrade hardware.

## **Virtual machine**

- Easy to move and copy
- Easy to manage.
- Independent from physical dependency to upgrade hardware and software.

# Installation of VMware

- Search on google:- Download VMware workstation

A screenshot of a Google search results page. The search bar at the top contains the query "download vmware workstation". Below the search bar, there are tabs for All, Books, Videos, News, Images, More, and Tools. The "All" tab is selected. A message indicates "About 1,16,00,000 results (0.59 seconds)". The first result is a link to the VMware website: "https://www.vmware.com › Products › Workstation Pro". The link text is "Download VMware Workstation Pro | IN". Below the link, a snippet of text reads: "VMware Workstation Pro is the industry standard desktop hypervisor for running virtual machines on Linux or Windows PCs. Discover why. | VMware IN." It also mentions "You visited this page on 6/2/22.". To the left of this result, there is a section titled "Workstation Player" with a link to "Download VMware Workstation Player for free today to run a ...". At the bottom of this section is a link "More results from vmware.com »". To the right of the main result, there is another section titled "Workstation Pro" with a snippet: "Now includes a new Dark Mode user interface, DirectX 11 ...".

# Select VMware Workstation 16 Pro for download

---

## VMware Workstation 16 Pro



Workstation 16 Pro improves on the industry defining technology with DirectX 11 and OpenGL 4.1 3D Accelerated graphics support, a new dark mode user interface, support for Windows Hyper-V mode on Windows 10 version 2004 and greater hosts, a new CLI for supporting containers and Kubernetes clusters, 'vctl,' support for the latest Windows and Linux operating systems, and more.

Use the links below to start your free, fully functional 30-day trial, no registration required.

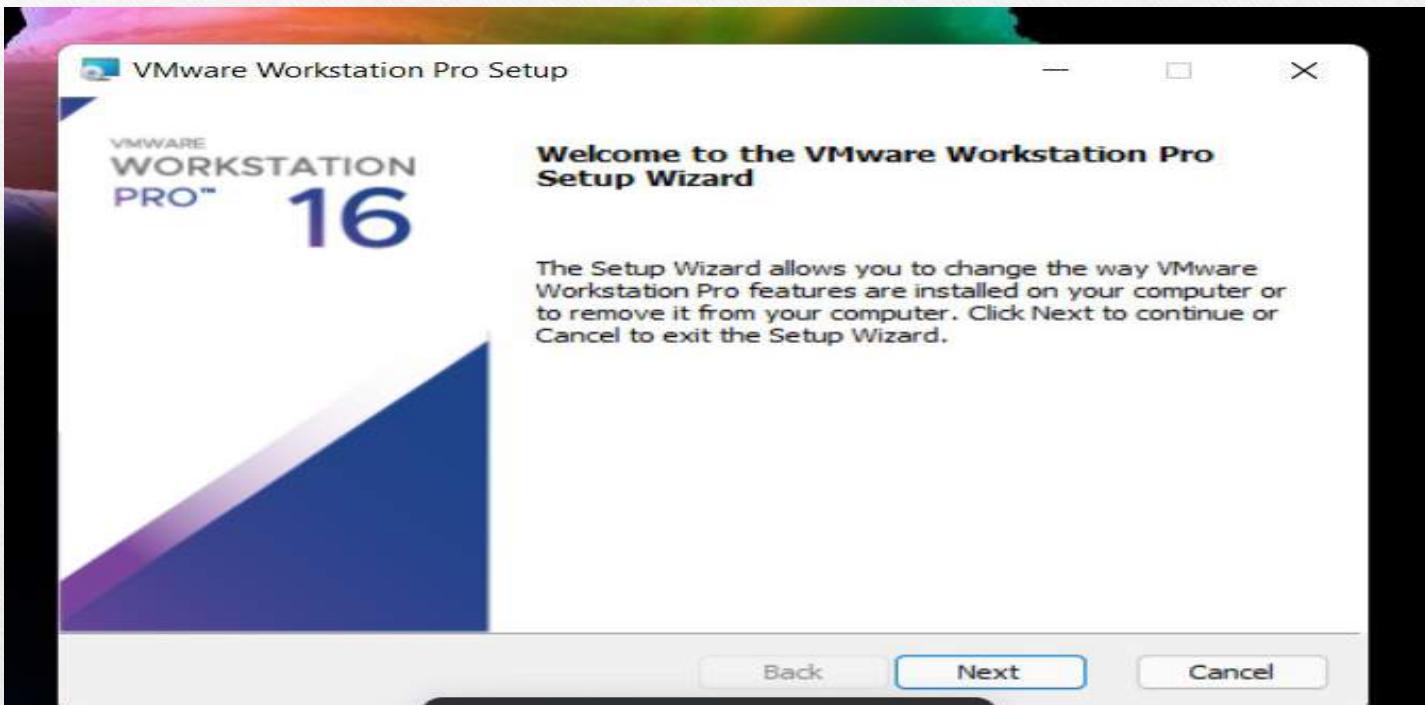
### Workstation 16 Pro for Windows

[DOWNLOAD NOW >](#)

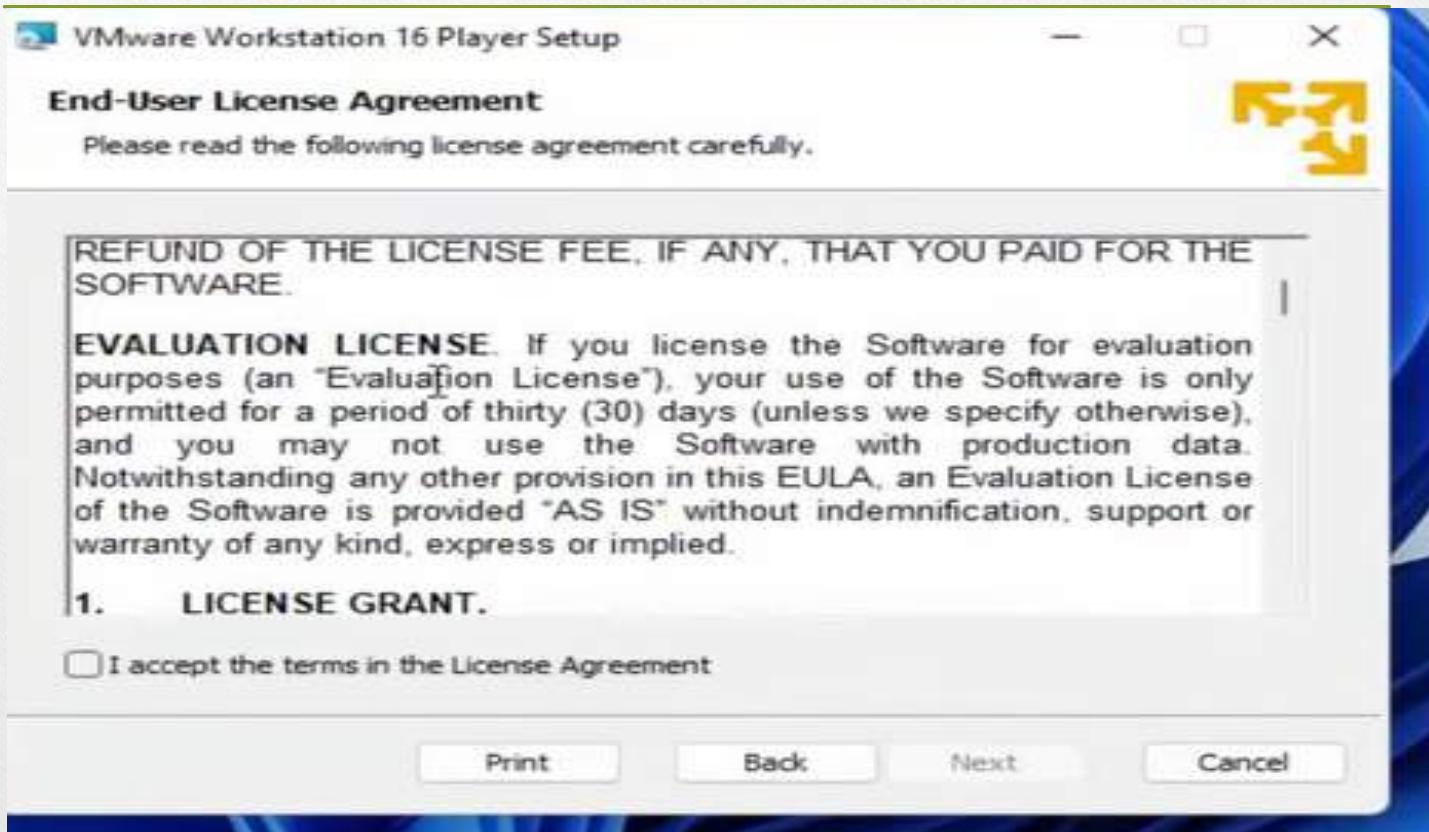
### Workstation 16 Pro for Linux

[DOWNLOAD NOW >](#)

# Run Setup File



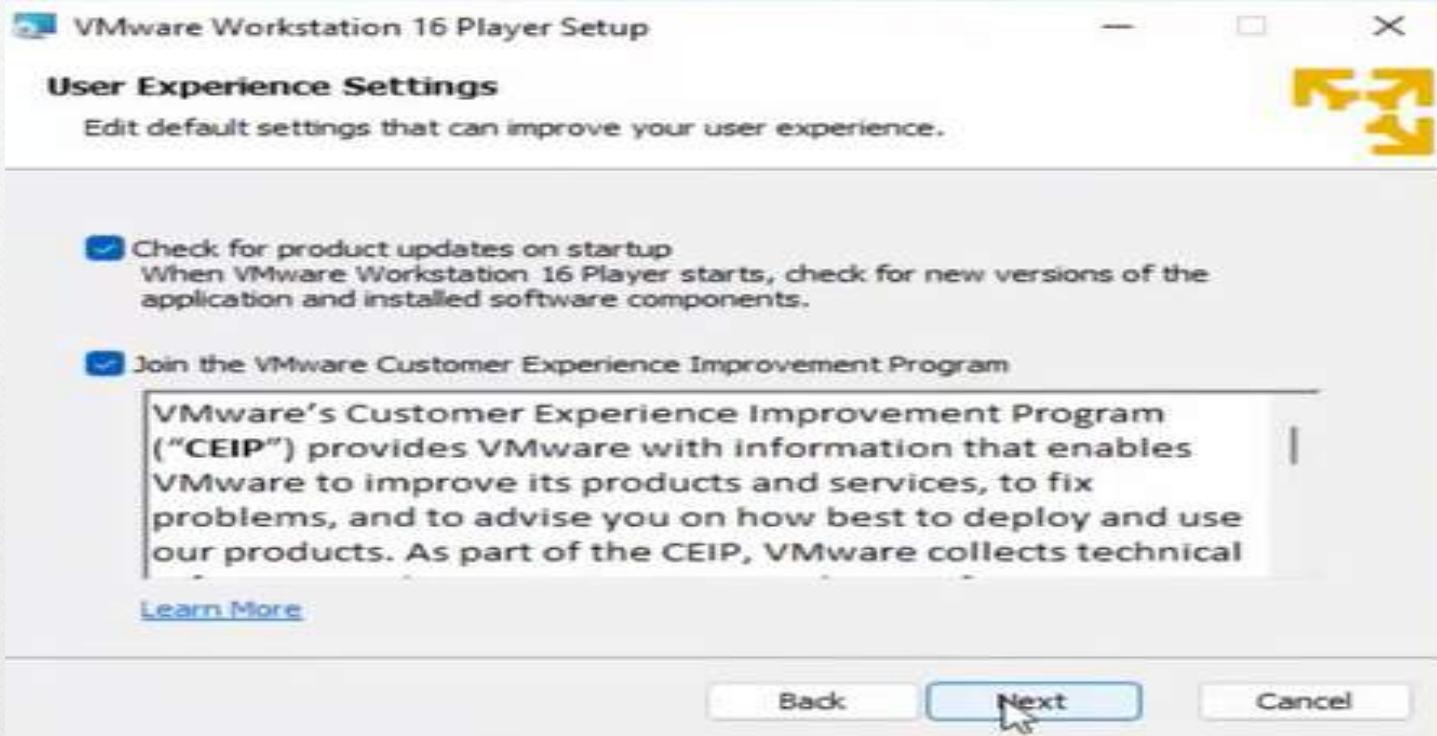
# Run Setup Cont..



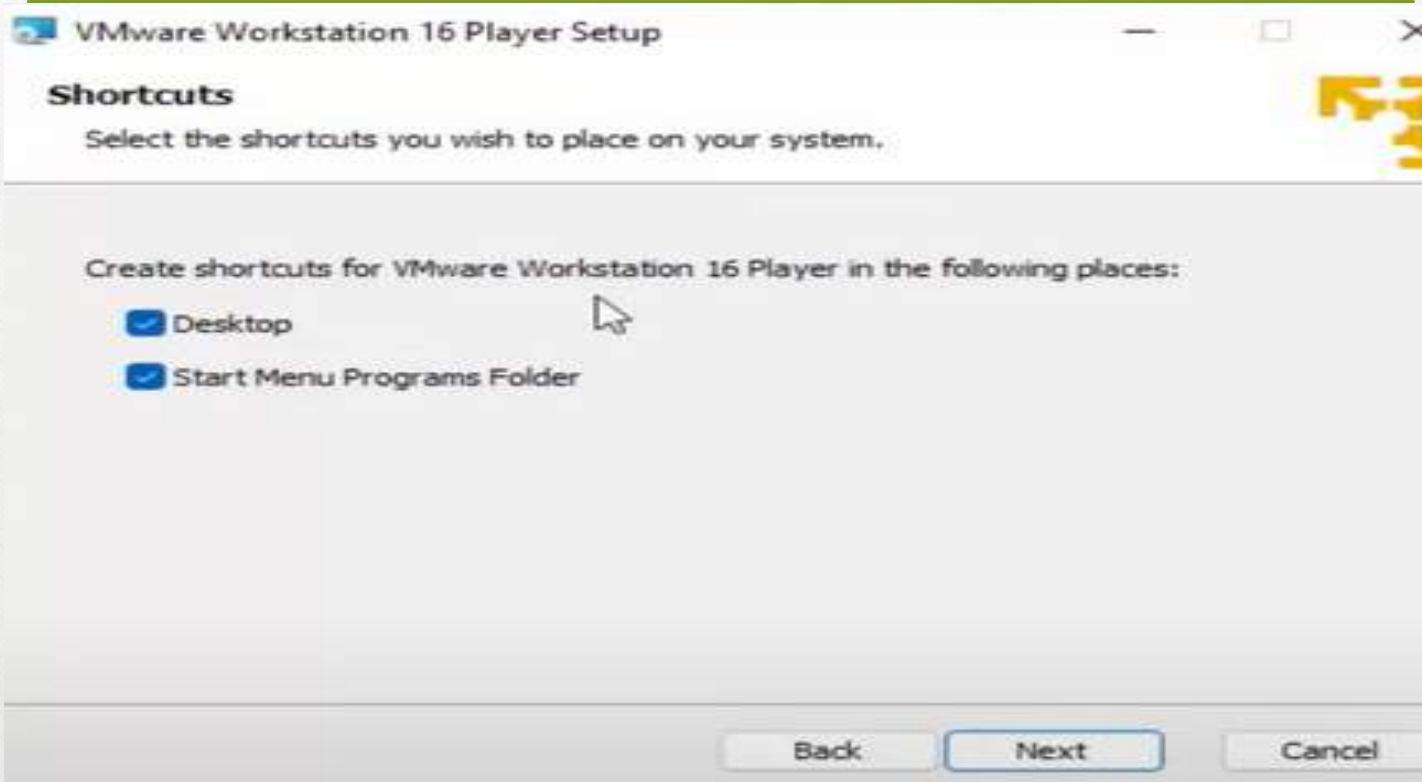
# Run Setup Cont..



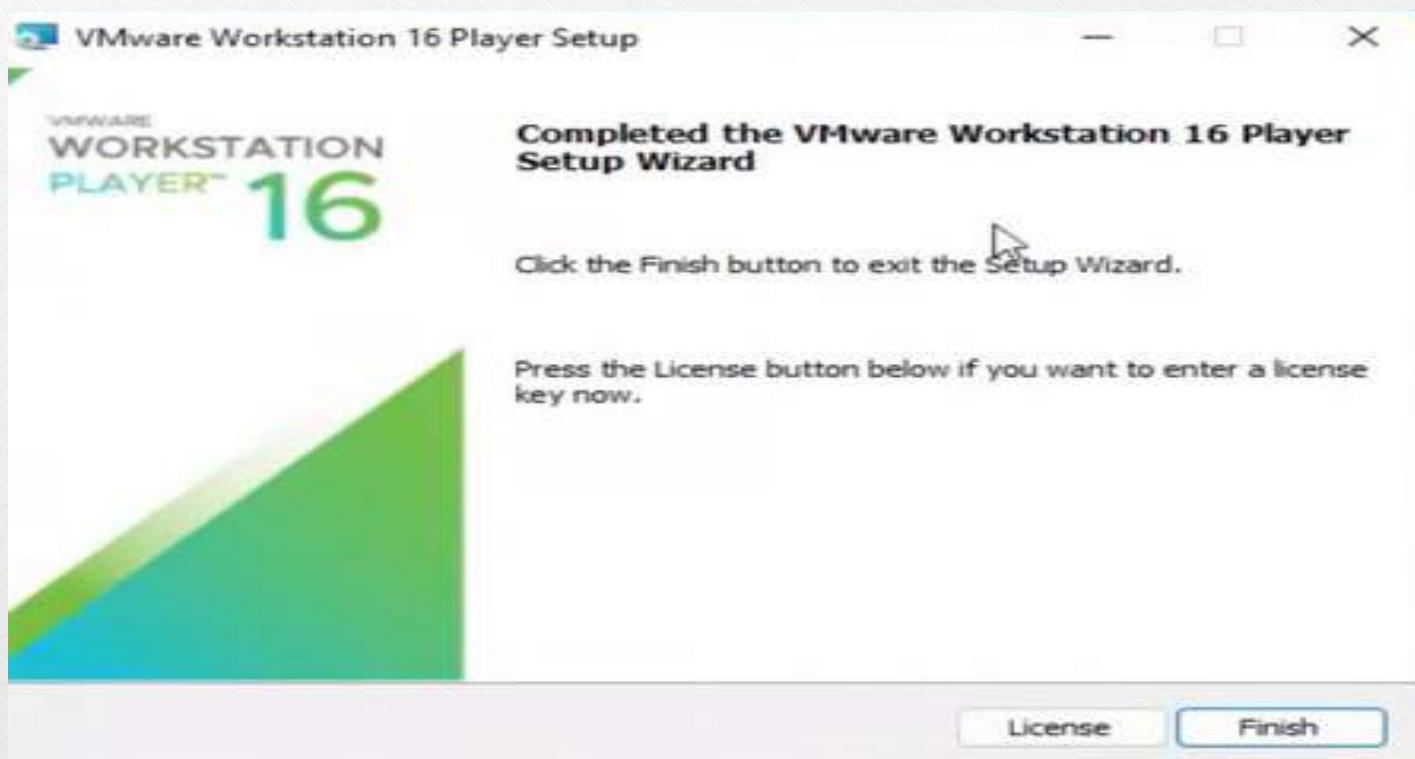
# Run Setup Cont..



# Run Setup Cont..

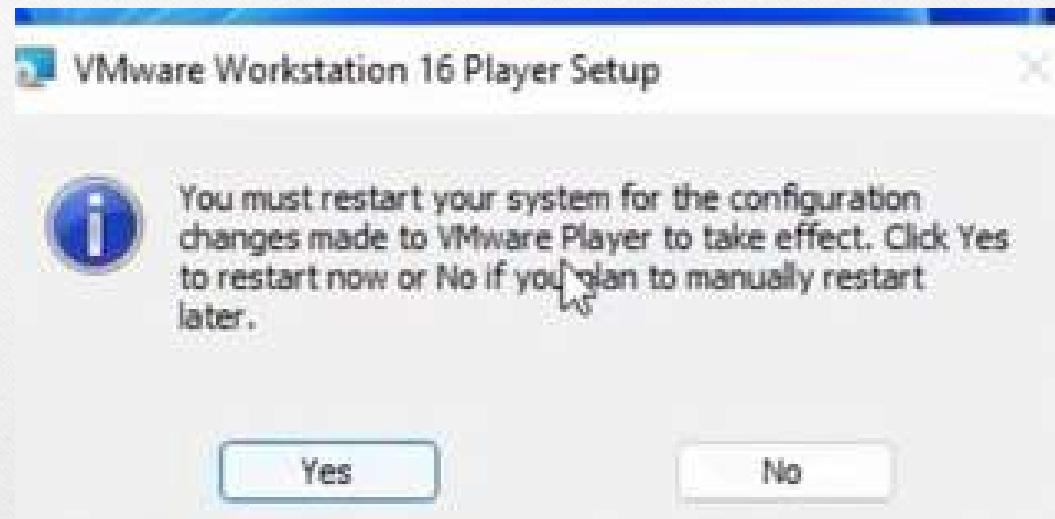


# Run Setup Cont..



# Run Setup Cont..

---



# What is Kali Linux?

---

- **Kali Linux** is a security distribution of Linux derived from Debian and specifically designed for computer forensics and advanced penetration testing. It was developed through rewriting of BackTrack by Mati Aharoni and Devon Kearns of Offensive Security. **Kali Linux** contains several hundred tools that are well-designed towards various information security tasks, such as penetration testing, security research, computer forensics and reverse engineering.

# **Useful utilities of Kali Linux**

---

- 1.Information Gathering**
- 2.Vulnerability Analysis**
- 3.Wireless Attacks**
- 4.Web Applications**
- 5.Exploitation Tools**
- 6.Stress Testing**
- 7.Forensics Tools**

# **Useful utilities of Kali Linux Cont..**

---

8. Sniffing & Spoofing
9. Password Attacks
10. Maintaining Access
11. Reverse Engineering
12. Reporting Tools
13. Hardware Hacking

# Who uses Kali Linux and Why?

---

- Kali Linux is truly a unique operating system, as its one of the few platforms openly used by both good guys and bad guys. Security Administrators, and Black Hat Hackers both use this operating system extensively.
- **Security Administrators** -Security Administrators are responsible for safeguarding their institution's information and data. They use Kali Linux to review their environment(s) and ensure there are no easily discoverable vulnerabilities.
- **Network Administrators** -Network Administrators are responsible for maintaining an efficient and secure network. They use Kali Linux to audit their network. For example, Kali Linux has the ability to detect rogue access points.

# Who uses Kali Linux and Why? Cont..

---

- **Network Architects** - Network Architects, are responsible for designing secure network environments. They utilize Kali Linux to audit their initial designs and ensure nothing was overlooked or misconfigured.
- **Pen Testers** - Pen Testers, utilize Kali Linux to audit environments and perform reconnaissance on corporate environments which they have been hired to review.
- **Forensic Engineers** - Kali Linux posses a “Forensic Mode”, which allows a Forensic Engineer to perform data discovery and recovery in some instances.

## **Downloading Iso Image**

---

- After selecting 64 bit ISO image the image will be downloaded in your PC which you can extract using extractor like 7z [exactor]. You will found ISO image in that .
- **"C:\Users\Dr.Ravi Verma\Downloads\kali-linux-2021.4a-vmware-amd64.7z.torrent"**

# Kali Linux Installation Methods

- 
- Kali Linux can be installed using the following methods:
  - Directly on a PC, Laptop – Utilizing a Kali ISO image, Kali Linux can be installed directly onto a PC or Laptop. This method is best if you have a spare PC and are familiar with Kali Linux. Also, if you plan or doing any access point testing, installing Kali Linux directly onto Wi-Fi enabled laptop is recommended.
  - Virtualized (VMware, Hyper-V, Oracle VirtualBox, Citrix) – Kali Linux supports most known hypervisors and can be easily into the most popular ones. Pre-configured images are available for download from <https://www.kali.org/>, or an ISO can be used to install the operating system into the preferred hypervisor manually.

# Download Kali Linux ISO Image for VMware

- One can download Kali Linux Iso image using following link.
- <https://www.kali.org>
- Now choose Virtual Machines option so click on it.

The screenshot shows the Kali Linux download page with two main options:

- Bare Metal**: Represented by a blue icon of a monitor and keyboard. It lists:
  - ✓ Direct access to hardware
  - ✓ Customized Kali kernel
  - ✓ No overhead

Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.

Recommended
- Virtual Machines**: Represented by a green icon of a 3D cube. It lists:
  - ✓ Snapshots functionality
  - ✓ Isolated environment
  - ✓ Customized Kali kernel
  - ✗ Limited direct access to hardware
  - ✗ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant Images for quick spin-up also available.

Recommended

At the top of the page, there is a toggle switch between **LIGHT** and **DARK** modes.

# Virtual Machine

Kali Linux VMware & VirtualBox images are available for users who prefer, or whose specific needs require, a virtual machine installation.

These images have the default credentials "[kali/kali](#)".

[Virtual Machines Documentation >](#)

64-bit

32-bit



VMware



2.4G

torrent

sum



VirtualBox



3.7G

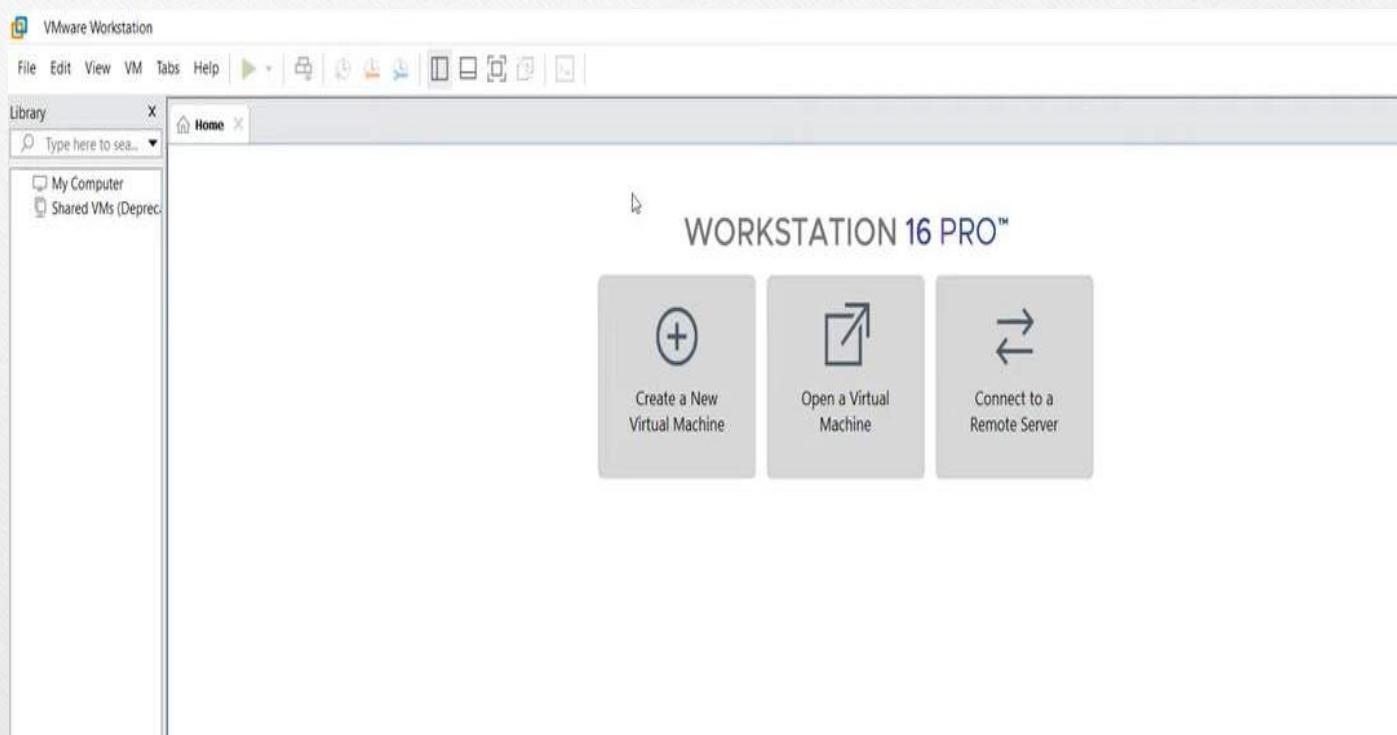
torrent

sum

[Documentation](#)

[Documentation](#)

# Installing Kali Linux on VMware workstation



# Installing ISO image into VMware

- Now click on New Virtual Machine, then select Typical.



# Installing ISO image into VMware Cont..

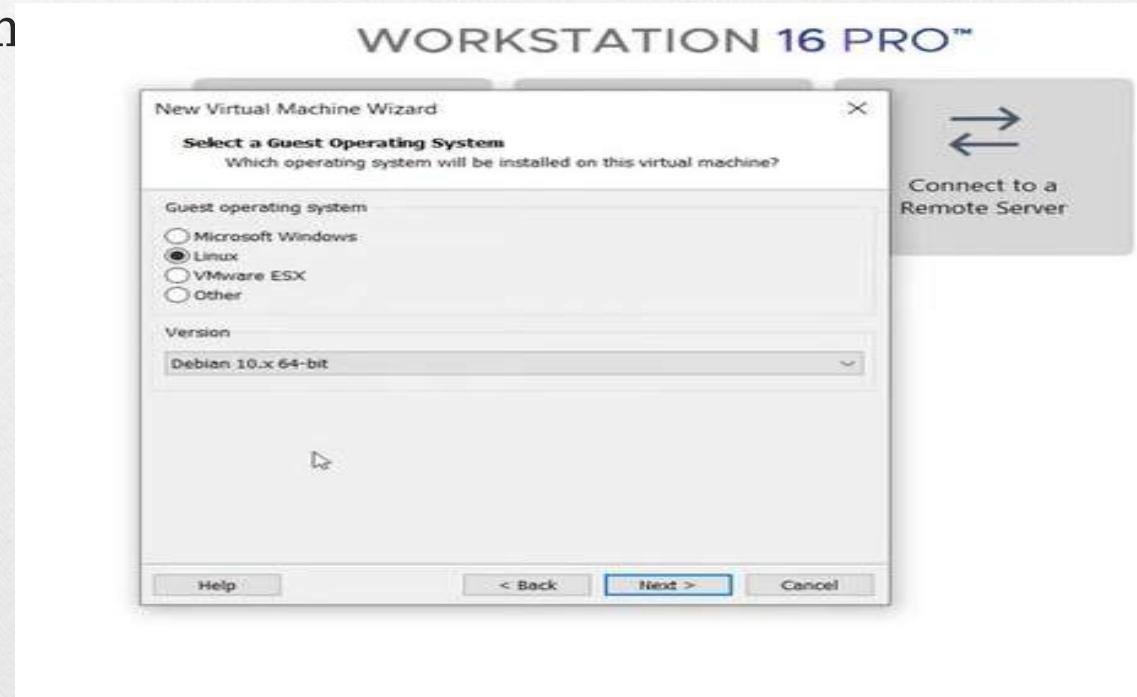
- Now you have to select Installer image option and select your downloaded Iso images .



# Installing ISO image into VMware Cont..

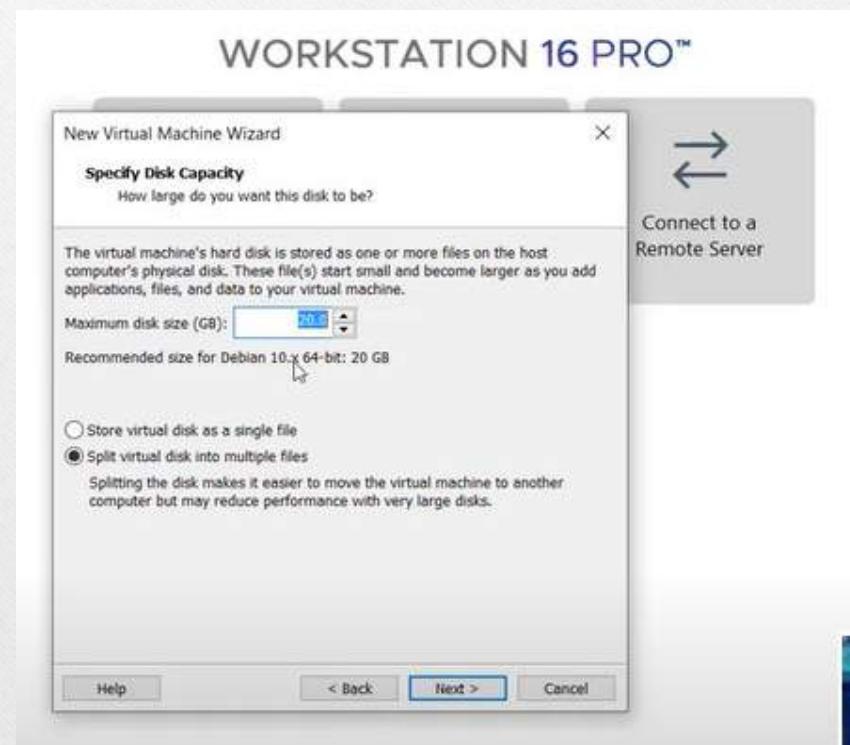
---

- Now we need to select Linux operating system from



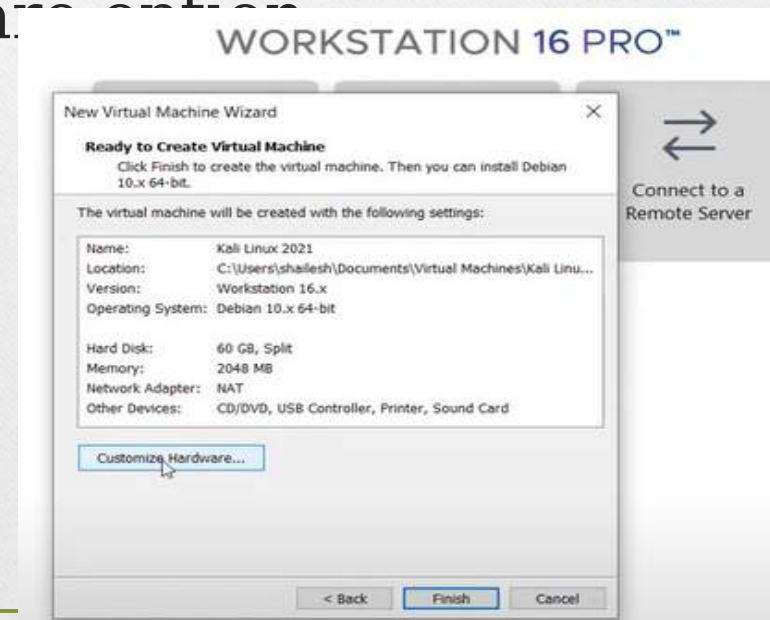
# Installing ISO image into VMware Cont..

- Here you have to assign hardware resources to system . Ideally it would be:
- Disk Storage: 128 GB
- RAM: 4 GB
- Processor Core: 2 to 4

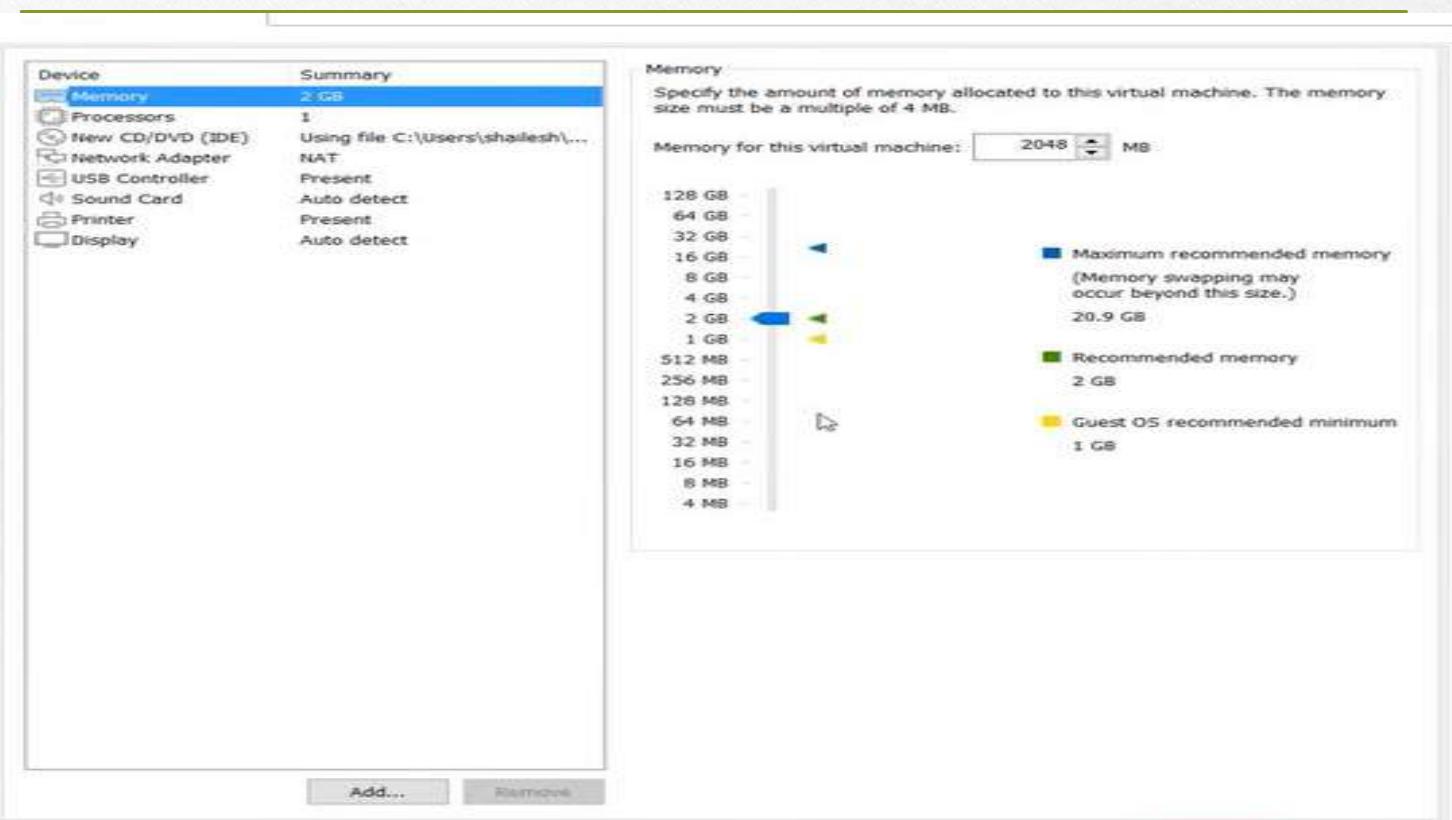


# Installing ISO image into VMware Cont..

- One can update the hardware configuration by clicking on customize hardware option.



# Customize Hardware



# Kali Linux

- After click on Finish one find following dialog box.  
Now one need to click on Power on option.



# Now Click on Graphical Install Option



## Finish Installation Process

---

- After selecting graphical Installer setup will install few software's and tools and finally you find Kali Linux has been installed in your machine .
- After getting on your kali machine you need to enter following ID and psd here.
- ID= Kali
- Psd= Kali

## **Conclusion**

---

- Presentation brings various steps used to install Kali Linux into Virtual Machine to perform penetration testing.

---

# **Question ?**

# **VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING**

---

## **UNIT 02**

### **Pen Testing with Metasploit**

By

**Dr. Ravi Verma**

## **Output of this Presentation**

---

- Students will be able to Install various tools and software like VMware, Kali Linux to perform Pen Testing .
- This session will brings the concept of realizing how to conduct pen testing on Metasploit.

# ~~Contents To Be Discussed Cont.~~

## TODAY'S AGENDA

- Introduction To Metasploit
- History Of Metasploit
- Prepare The Metasploit Lab Environment
- Metasploit Architecture
- Metasploit Modules

# INTRODUCTION TO METASPLOIT

- Metasploit is a popular penetration testing tool
- A tool for developing and executing exploit code against a remote target machine
- Offer a broad platform for pen-testing and exploit development

# MSFCONSOLE

- The msfconsole is the most popular interface to the Metasploit Framework (MSF)
- Execution of external commands in msfconsole is possible

# HISTORY OF METASPLOIT

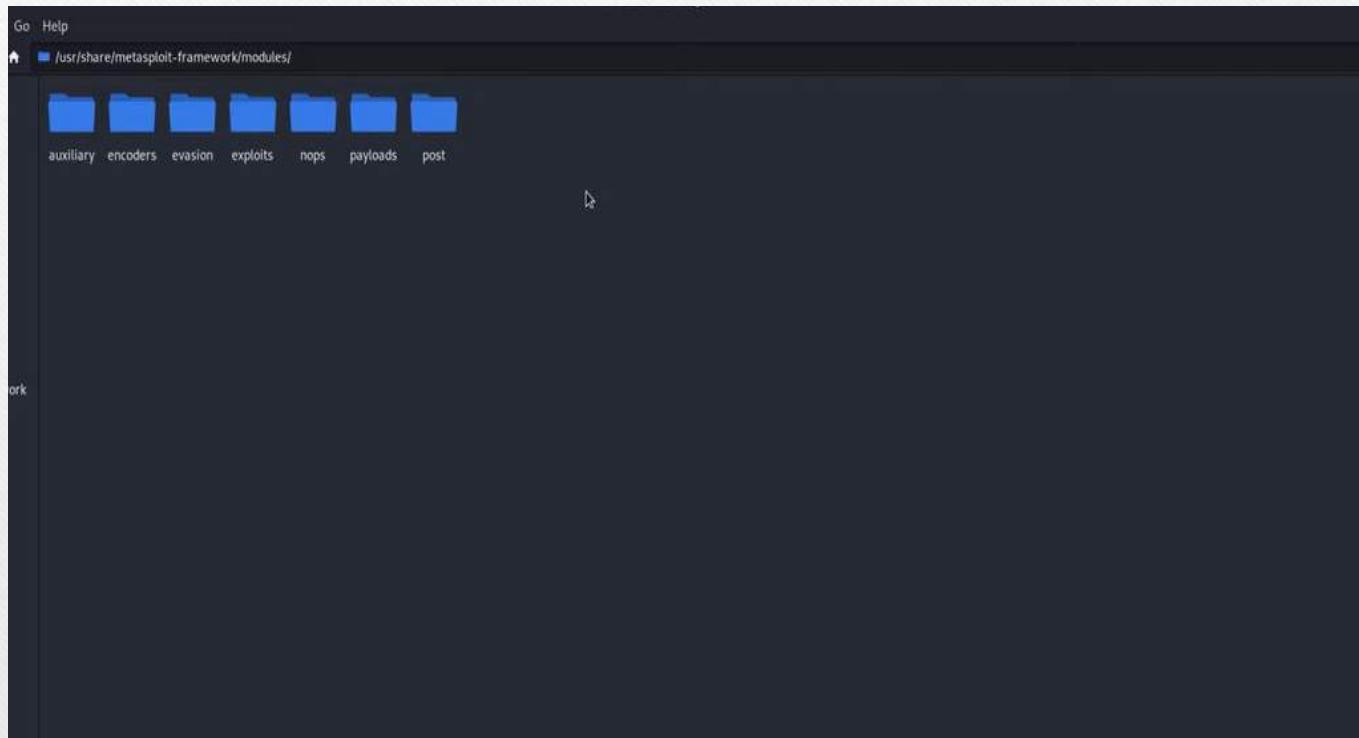
- Undertaken in 2003 by H.D. Moore
- Perl-based portable network tool
- Later rewritten in Ruby by 2007
- Rapid7 purchased the Metasploit Project in 2009

# PREPARE THE METASPLOIT LAB

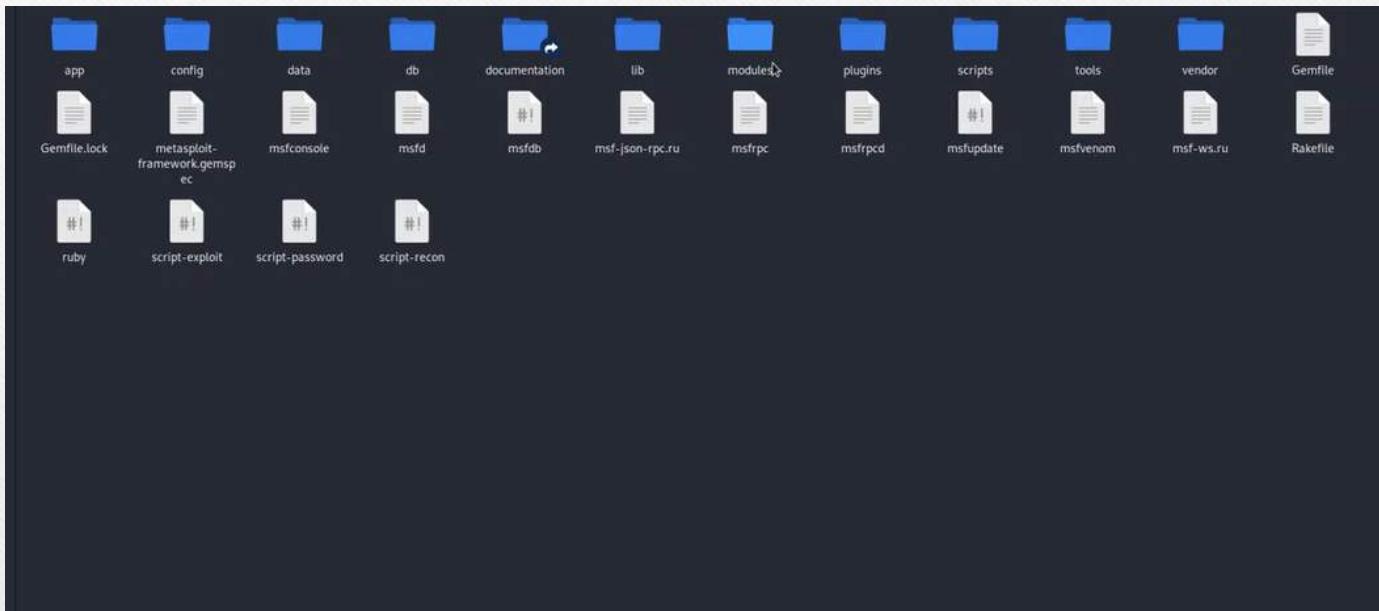
- Vmware
- Kali Linux
- Metasploitable
- Windows

# Architecture of Metasploit

---



# Architecture of Metasploit Cont..



# METASPLOIT MODULES

➤ A module is a piece of software that the Metasploit Framework uses to perform a task, such as exploiting or scanning a target.

- Exploits
- Auxiliary
- Payloads
- Encoders
- Nops
- Evasion
- Post

# METASPLOIT MODULES

## ➤ Exploits

➤ An exploit executes a sequence of commands that target a specific vulnerability found in a system

## ➤ Auxiliary

➤ Auxiliary modules include port scanners, fuzzers, sniffers, and more

## ➤ Payloads

➤ Payloads consist of code that runs remotely

# METASPLOIT MODULES

- **Encoders**

- Encoders ensure that payloads make it to their destination intact

- **Nops**

- Nops keep the payload sizes consistent across exploit attempts

- **Evasion**

- These new modules are designed to help you create payloads that can evade anti-virus (AV) on the target system

# METASPLOIT MODULES

## ➤ Post

- Post-exploitation modules that can be run on compromised targets to gather evidence, pivot deeper into a target network, and much more.

## **Conclusion**

---

- Presentation brings various modules used in Metasploit platform to conduct a Pen Testing for Network and other Computing Devices.

---

# **Question ?**

# Download Extrapolatable as second machine for

A screenshot of a search results page from a search engine. The search query "download metasploitable vmware" is entered in the search bar. Below the search bar, there are filters for "All", "Videos", "News", "Images", "Shopping", and "More". The search results indicate "About 32,100 results (0.39 seconds)". The top result is a link to "Metasploitable download | SourceForge.net", dated 19-Aug-2019. The snippet describes Metasploitable as an intentionally vulnerable Linux virtual machine for security training. It includes a 4.3-star rating from 6 votes, a "Free" label, and a "Security" category. Below the snippet are links to "Browse /Metasploitable2 · Metasploitable · Files · 6 Reviews".

download metasploitable vmware

All Videos News Images Shopping More

About 32,100 results (0.39 seconds)

<https://sourceforge.net> › ... › Security

**Metasploitable download | SourceForge.net**

19-Aug-2019 — **Metasploitable** is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and ...

★★★★★ Rating: 4.3 · 6 votes · Free · Security

Browse /Metasploitable2 · Metasploitable · Files · 6 Reviews

People also ask

Where can I download Metasploitable?

Where can I download Metasploitable 2?

What is Metasploitable virtual machine?

How much RAM does Metasploitable need?



# Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine  
Brought to you by: [rapid7user](#)



6 Reviews

Downloads: 9,716 This Week



[Download](#)

[Get Updates](#)

[Share This](#)

Summary

Files

Reviews

This is Metasploitable2 (Linux)

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct practice common penetration testing techniques.

The default login and password is msfadmin:msfadmin.

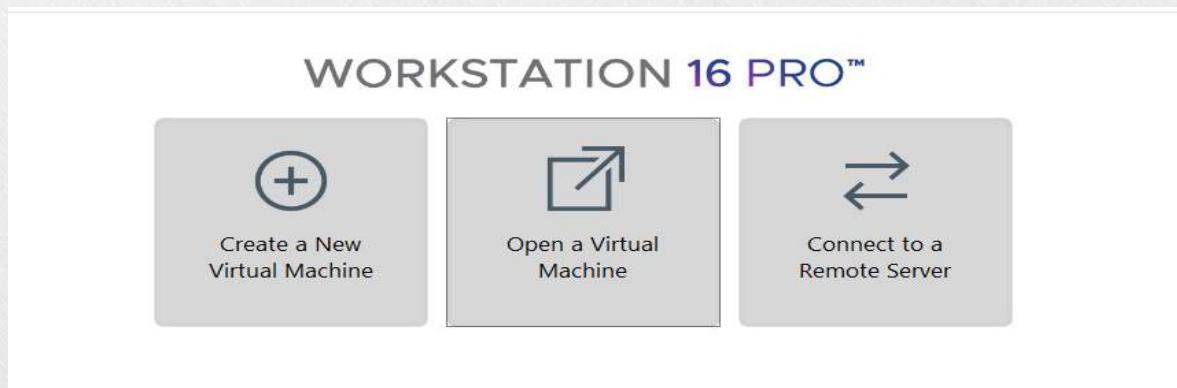
Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions).

- [Metasploitable download | SourceForge.net](#)

# Installation

---

- After downgliding file need to extract it .
- Now open VMware workstation and choose Open virtual machine option. Then select file from extracted folder.



# **VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING**

---

## **UNIT 02 ARP SPOOFING**

By  
**Dr. Ravi Verma**

## **Output of this Presentation**

---

- Students will be able to perform different attacking activities like Man in the Middle attack for realizing the impact of ARP Spoofing and MTMA.

# **Contents To Be Discuss Cont....**

---

- ARP Poisoning or Spoofing**
- What Is an ARP?**
- An ARP should**
- ARP Attacks**
- Goal**
- Known ARP Vulnerabilities**
- ARP Poisoning Attack Prevention**
- Conclusion**

# ARP Poisoning or Spoofing

---

- ARP poisoning (also known as ARP spoofing) is a cyber attack carried out through malicious ARP messages.
- An ARP attack is difficult to detect, and once it's in place, the impact is impossible to ignore.

# ARP Poisoning or Spoofing Cont..

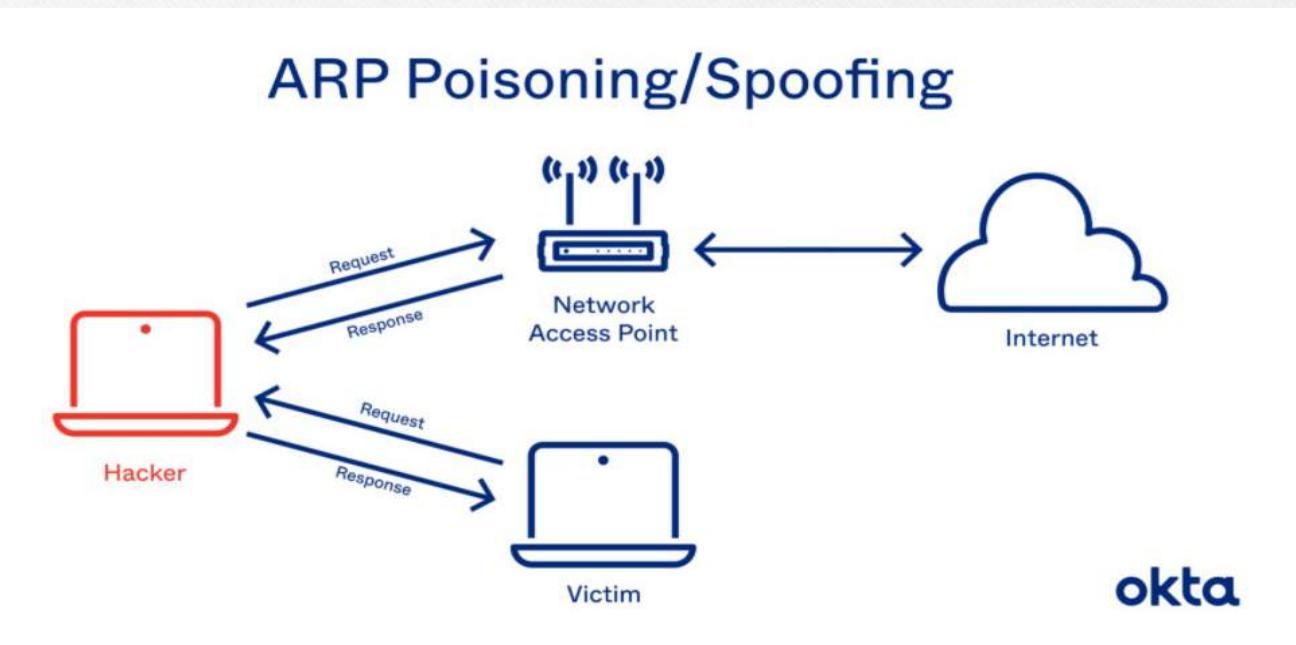
---

- A hacker that successfully implements either ARP spoofing or ARP poisoning could gain control of every document on your network. You could be subject to spying, or your traffic could grind to a halt until you give the hacker what's requested for ransom.

# ARP Poisoning or Spoofing

---

## Cont..



# What Is an ARP?

---

- In 2001, developers introduced the address resolution protocol (ARP) to Unix developers. At the time, they described it as a "workhorse" that could establish IP-level connections to new hosts.
- The work is critical, especially if your network is constantly growing, and you need a way to add new functionality without authorizing each request yourself.

# **What is ARP? Cont..**

---

- The basis of ARP is media access control (MAC). As experts explain, an MAC is a unique, hardware-level address of an ethernet network interface card (NIC). These numbers are assigned at the factory, although they can be changed by software.

# An ARP should:

---

- **Accept requests.** A new device asks to join the local area network (LAN), providing an IP address.
- **Translate.** Devices on the LAN don't communicate via IP address. The ARP translates the IP address to a MAC address.
- **Send requests.** If the ARP doesn't know the MAC address to use for an IP address, it sends an ARP packet request, which queries other machines on the network to get what's missing.

# ARP Attacks: Key Definitions

---

- A malicious developer, hoping to gain access to important data, could expose vulnerabilities and sneak inside, and you may never know it's happening.
- Two types of ARP attacks exist.
- **ARP spoofing:** A hacker sends fake ARP packets that link an attacker's MAC address with an IP of a computer already on the LAN.
- **ARP poisoning:** After a successful ARP spoofing, a hacker changes the company's ARP table, so it contains falsified MAC maps. The contagion spreads.

# Goal

---

- The goal is to link a hacker's MAC with the LAN. The result means any traffic sent to the compromised LAN will head to the attacker instead.
- At the end of a successful ARP attack, a hacker can:
- **Hijack.** Someone may look over everything that heads to the LAN before releasing it.
- **Deny service.** Someone may refuse to release anything from the infected LAN unless some kind of ransom is paid.

# Goal Cont..

---

- **Sit in the middle.** Someone conducting a man-in-the-middle attack can do almost anything, including altering documents before sending them out. These attacks both threaten confidentiality and reduce user confidence. They are among the most dangerous attacks anyone can perpetrate.
- If a hacker wants to take over an end host, the work must be done quickly. ARP processes expire **within about 60 seconds**. But on a network, requests can linger for up to 4 hours. That leaves plenty of time for a hacker to both contemplate and execute an attack.

# Known ARP Vulnerabilities

---

- Speed, functionality, and autonomy were the goals when ARP was developed. The protocol wasn't made with security in mind, and it's proven very easy to spoof and tweak for malicious ends.
- A hacker needs just a few tools to make this work.
- **Connection:** The attacker needs control of one LAN-connected machine. Better yet, the hacker is directly connected to the LAN already.

# Known ARP Vulnerabilities

---

- **Coding skills:** The hacker must know how to write up ARP packets that are immediately accepted or stored on the system.
- **Outside tools:** A hacker could use a spoofing tool, such as Arpspoof, to send out falsified or otherwise inauthentic ARP responses.
- **Patience.** Some hackers breeze into systems quickly. But others must send dozens or even hundreds of requests before they fool the LAN.

# Known ARP Vulnerabilities

---

- ARP is stateless, and networks tend to cache ARP replies. The longer they linger, the more dangerous they become. One leftover reply could be used in the next attack, which leads to ARP poisoning.
- No method of identity proofing exists in a traditional ARP system. Hosts can't determine if packets are authentic, and they can't even determine where they came from.

# ARP Poisoning Attack Prevention

---

- Hackers use a predictable series of steps to take over a LAN. They send a spoofed ARP packet, they send a request that connects to the spoof, and they take over. The request is broadcast to all computers on the LAN, and control is complete.

# ARP Poisoning Attack Prevention

---

- Network administrators can use two techniques to detect ARP spoofing.

**1. Passive:** Monitor ARP traffic and look for mapping inconsistencies.

**2. Active:** Inject falsified ARP packets into the network. A spoofing attack like this helps you identify weak points in your system. Remediate them quickly, and you could stop an attack in progress.

# Protection Tools to Consider

---

- Plenty of companies provide monitoring programs you can use to both oversee your network and spot ARP problems.
- These are common solutions:
- Arpwatch: Monitor ethernet activity, including changing IP and MAC addresses, via this Linux tool. Look over the log every day, and access timestamps to understand just when the attack happened.

# ARP Poisoning Attack Prevention Cont..

---

- ARP-GUARD: Tap into a graphic overview of your existing network, including illustrations of switches and routers. Allow the program to develop an understanding of what devices are on your network and build rules to control future connections.
- XArp: Use this tool to detect attacks happening below your firewall. Get notified as soon as an attack begins, and use the tool to determine what to do next.

# ARP Poisoning Attack Prevention Cont..

---

- **Wireshark:** Use this tool to develop a graphic understanding of all the devices on your network. This tool is powerful, but you may need advanced skills to implement it properly.
- **Packet filtering:** Use this firewall technique to manage network access by monitoring incoming and outgoing IP packets. Packets are allowed or stopped based on source and destination IP addresses, ports, and protocols.
- **Static ARP:** These ARPs are added to the cache and retained on a permanent basis. These will serve as permanent mappings between MAC addresses and IP addresses.

# **11 Types of Spoofing Attacks Every Security Professional Should Know About**

---

## **1. ARP Spoofing**

- This one is a common source of man-in-the-middle attacks. To execute it, a cybercriminal inundates a local area network with falsified Address Resolution Protocol (ARP) packets in order to tamper with the normal traffic routing process. The logic of this interference boils down to binding the adversary's MAC address with the IP address of the target's default LAN gateway.

# **11 Types of Spoofing Attacks Every Security Professional Should Know About**

---

## **2. MAC Spoofing**

In theory, every network adapter built into a connected device should have a unique Media Access Control (MAC) address that won't be encountered elsewhere. In practice though, a clever hack can turn this state of things upside down. An attacker may harness imperfections of some hardware drivers to modify, or spoof, the MAC address. This way, the criminal masquerades his device as one enrolled in a target network to bypass traditional access restriction mechanisms.

# **11 Types of Spoofing Attacks Every Security Professional Should Know About**

---

## **3. IP Spoofing**

- To perform this attack, the adversary sends Internet Protocol packets that have a falsified source address. This is a way to obfuscate the actual online identity of the packet sender and thereby impersonate another computer. IP spoofing is often used to set DDoS attacks in motion. The reason is that it's hard for digital infrastructure to filter such rogue packets, given that each one appears to hail from a different address and therefore the crooks feign legitimate traffic quite persuasively.

# 11 Types of Spoofing Attacks Every Security Professional Should Know About

---

## 4. DNS Cache Poisoning (DNS Spoofing)

- Every tech-savvy user knows the Domain Name Server (DNS) wiki: it maps domain names to specific IP addresses so that people type easy-to-remember URLs in the browser rather than enter the underlying IP strings. Threat actors may be able to contort this mapping logic by piggybacking on known DNS server caching flaws. As a result of this interference, the victim runs the risk of going to a malicious replica of the intended domain. From a cybercriminal's perspective, that's a perfect basis for phishing hoaxes that look really true-to-life.

## **Conclusion**

---

- This Presentation describes the ARP and Its various types .
- This presentation also brings the Effect of ARP or Man in the Middle Attack in Network .

---

# **Question ?**