Network Reconnaissance

and

Information Gathering

A

PROJECT SUBMITTED TO

Ankit Fadia Certified Ethical Hacking Program 9.0

BATCH-7

BY

PARTH LAKHLANI

E-Mail : parthlakhalani2000@gmail.com

FOR

For successful course completion

CONTENT

AIM

Perform a detailed Network Reconnaissance and Information Gathering scan of www.penguinbooksindia.com

In this project I try my best to cover all the Network Reconnaissance and Information Gathering tools, techniques and methods that were discussed in the course including PING, TraceRoute, Port Scanning, Daemon Banner Grabbing, OS Fingerprinting, Security Auditing and others.

Introduction

Network Reconnaissance and Information Gathering is the process of finding out as much information about victim as possible. Attacker tries to find out following information about victim.

- Victim is online/offline
- Network Topography
- DNS information
- List of open ports
- Software running on open ports (including names and versions)
- OS details
- Find out Loopholes

Process of Network Reconnaissance and Information Gathering

Step No.	Name	Tool/Software use
1	Victim is online/ offline	Ping
2	Topography Information	Traceroute/Tracert
3	DNS Information	DNS tools
4	List of open Ports	Port Scanner (Nmap/Zenmap)
5	Software Names & Version	Daemon Banner Grabbing (Nmap/Zemap)
6	OS detection / Fingerprinting	Nmap/Zenmap
7	Finding Loopholes	Security Auditing Tools

Detailed Step by Step Process of Network Reconnaissance and Information Gathering for

www.penguinbooksindia.com

- **Step-1 Victim is Online/Offline**

To find out that victim is online or offline the software called "**PING**" is used this process also known as "Ping Sweeping".

What is Ping?

Ping is used to check network connectivity between your computer and network computer.

- Whether you are online.
- Whether victim is online.
- Whether any connectivity between both you.

It makes use of the Internet Control Message Protocol (ICMP) in the following manner.

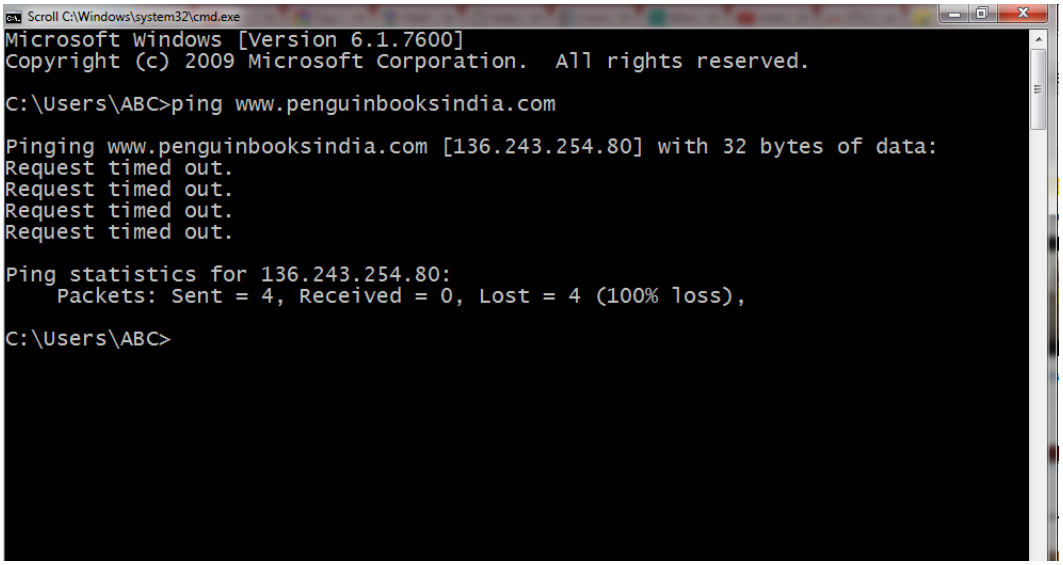
1. First ATTACKER sends ICMP Echo Request to TARGET/Victim.
2. If TAEGET/Victim is online then sand back ICMP Echoreply to ATTACKER.

Popular Ping Sweeping tools are NetScan Tools, SuperScan, Angry IP Scanner, **Nmap** and online websites like www.ping.eu

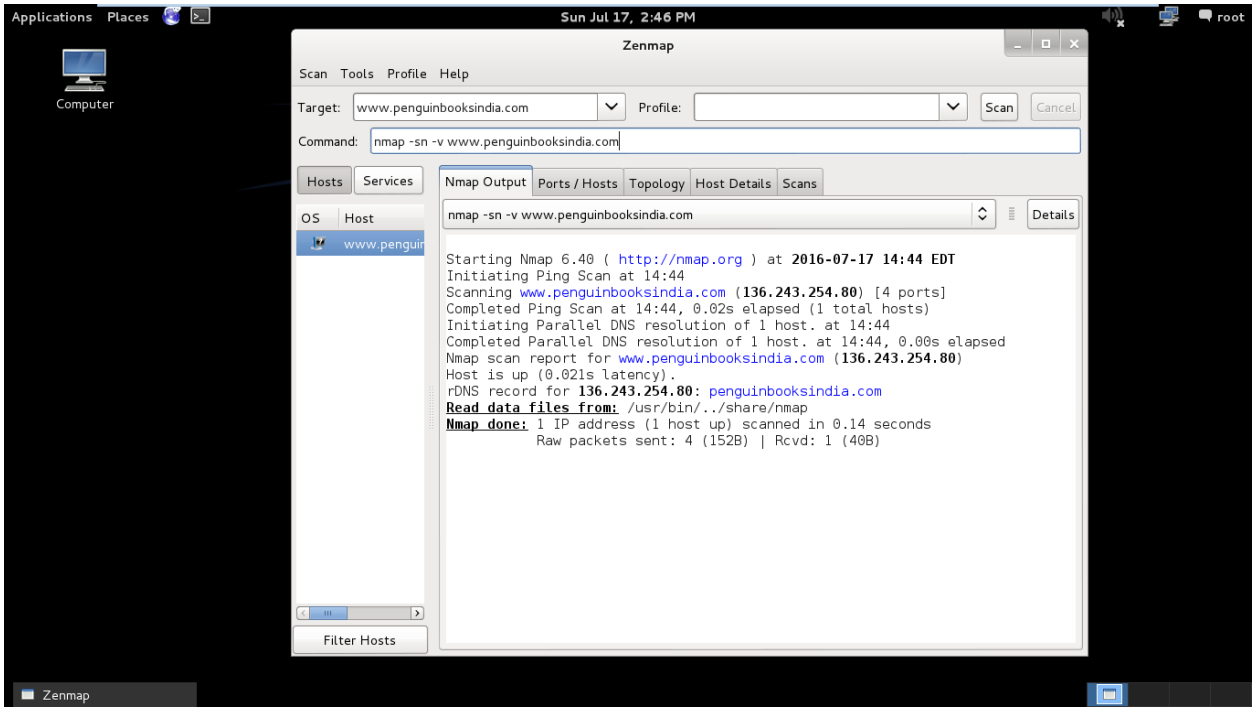
Command use for ping in MS-DOS is "ping + TARGET WEBSITE/IP ADDRESS"

In Nmap or Zenmap is "nmap –sn –v + TARGET WEBSITE/IP ADDRESS" or to bypass ping "nmap –sn –v **-Pn** + TARGET WEBSITE/IP ADDRESS" means no ping.

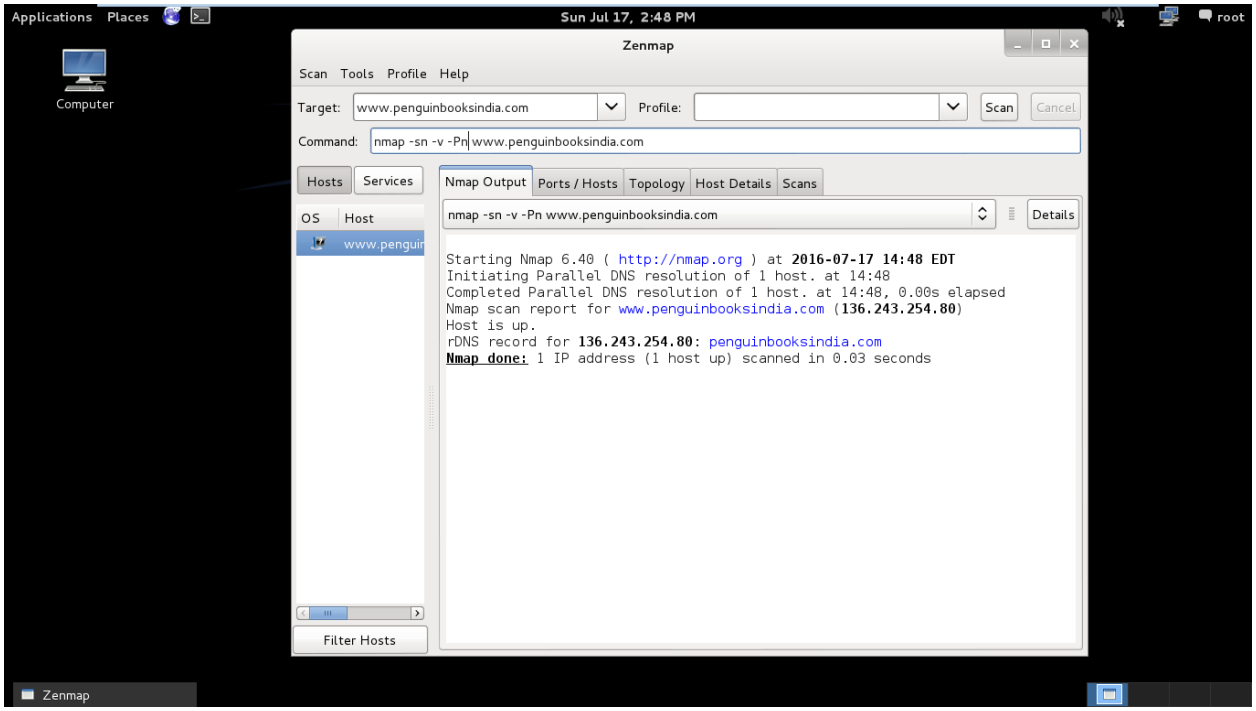
Analyzing www.penguinbooksindia.com by different ping options.



1.1 Preforming ping using MS-DOS



1.2 Preforming ping using Zenmap (Kali-linux)



1.3 Preforming ping using Zenmap (Kali-linux) by bypass ping using additional command "-Pn"

In Fig 1.1, there is no response by host server that shows that some firewall is blocking ping packets but if we apply same process by Zenmap using kali linux by bypass ping, it clearly shows that host is online.

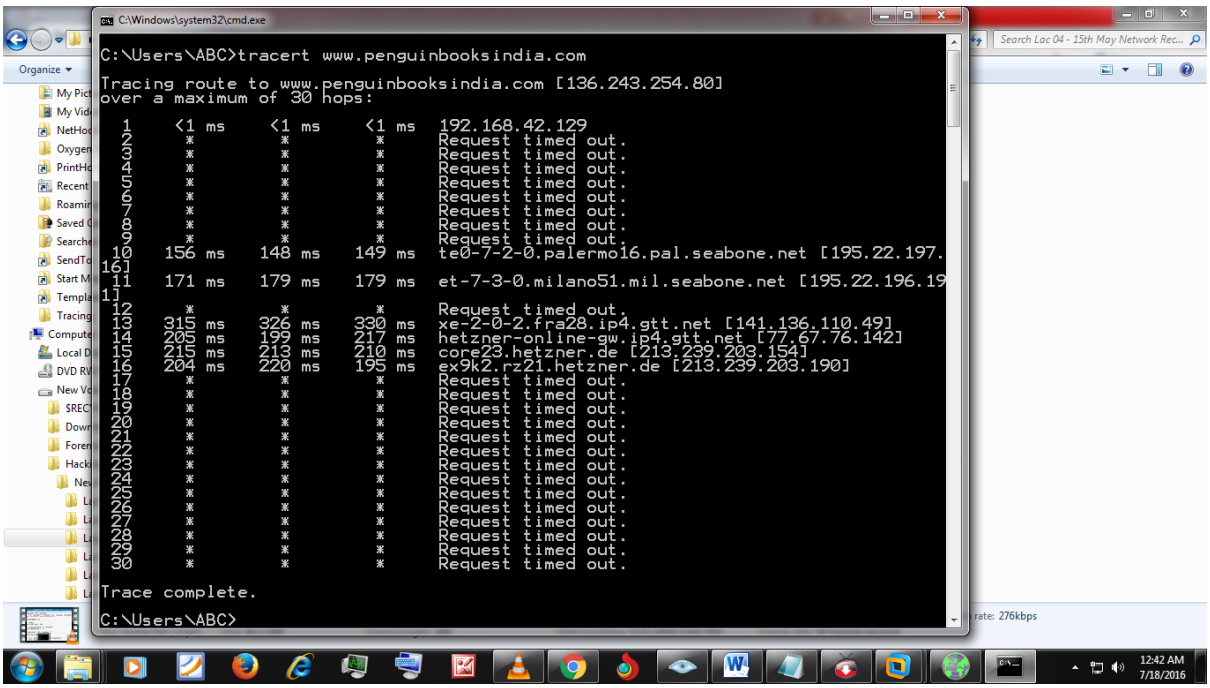
- **Step 2 Topography Information**

To find out Topography Information the tool use “Traceroute”.

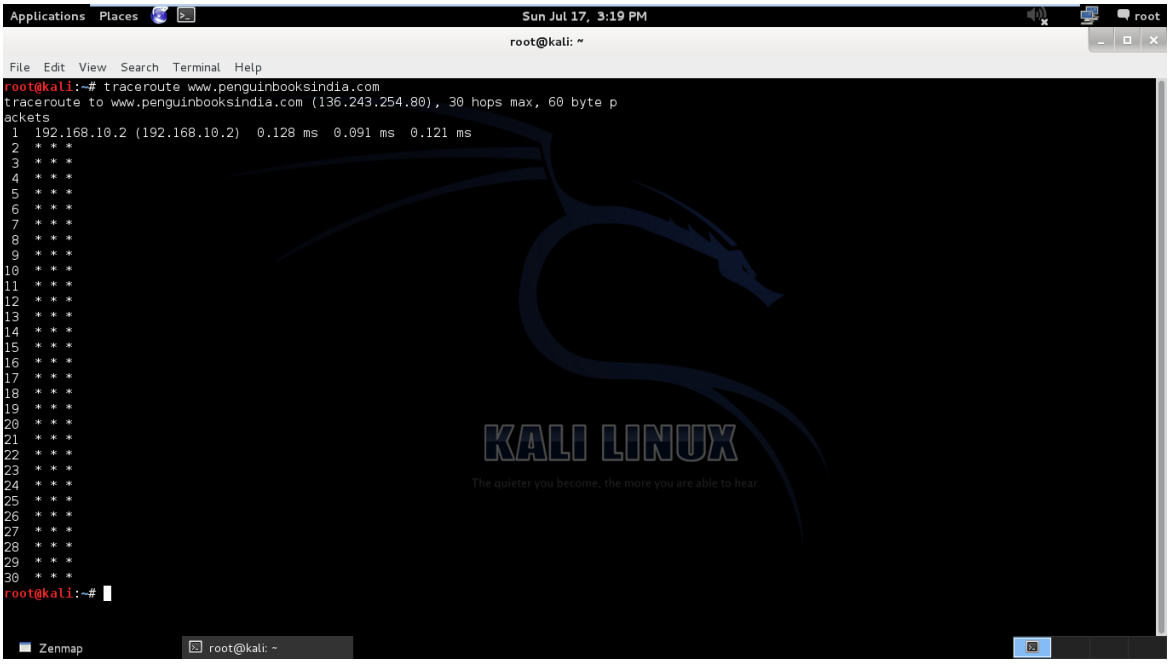
What is Traceroute?

Traceroute allows you to trace the path between two systems. It can be perform by using MS-DOS or Nmap/Zenmap.

Command for MS-DOS is “tracert + TARGET WEBSITE/IP ADDRESS”



2.1 Traceroute using MS-DOS



2.2 Traceroute using Nmap (Kali Linux)

Working of traceroute

Traceroute uses following data packets to carry out tracing process.

- The Time to Live (TTL) value of data packets represent. Its maximum possible age (number of routers it can pass) before it is dropped. Prevents infinite loop of data packets. Each router reduces the TTL value of the packet by 1. Hence, it has now become a hop counter.

Important of traceroute with ping

The importance of traceroute is they assign to data packets and different Operating System has different TTL values. So by tracing route of this data packet we can judge the OS running on victim's website. This is most important step in Network Reconnaissance and Information Gathering.

But here if you see that some firewall is blocking ping and traceroute. So we cannot find out that which OS running on victim's computer. So we have to apply different OS fingerprinting tools to find out OS running on victim's computer.

➢ Step 3 DNS Information

A DNS (Domain Name Server) lookup is a query sent by a user (browser or IMor email client) to a DNS server to concert a particular domain name into its respective IP address.

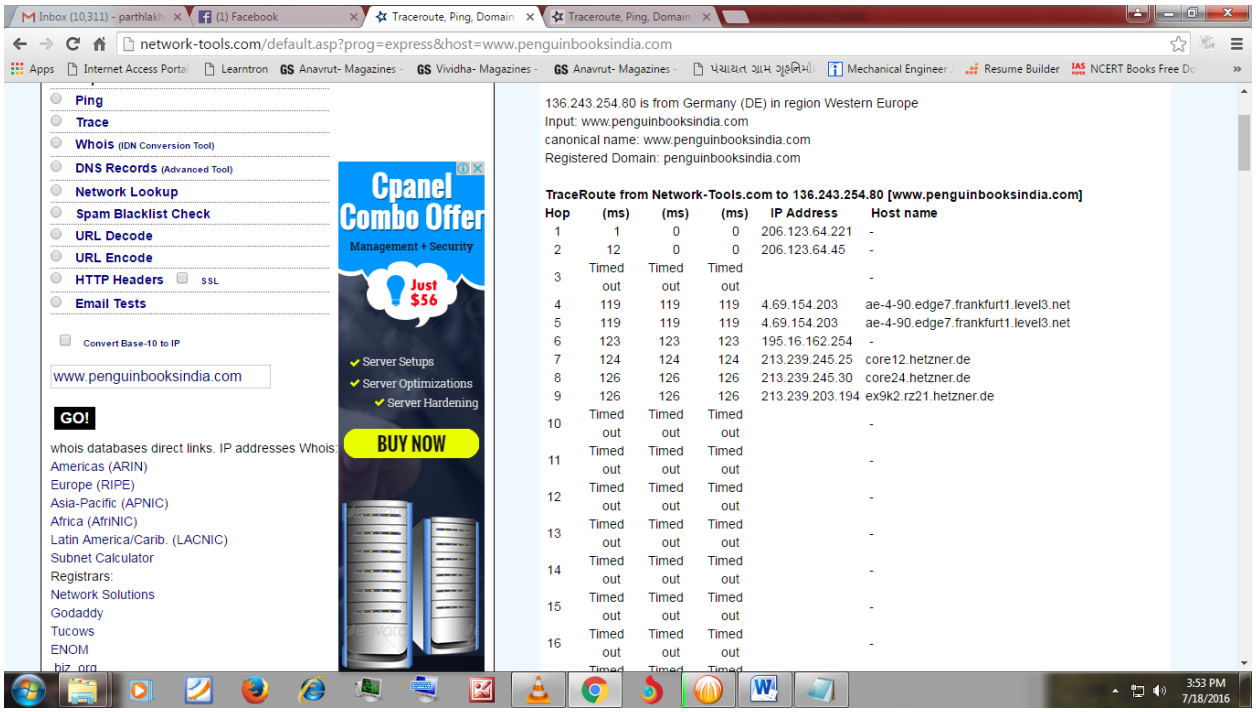
A reverse DNS lookup is a query sent by a user to a DNS server to convert an IP address into its reactive domain.

What is WHOIS query?

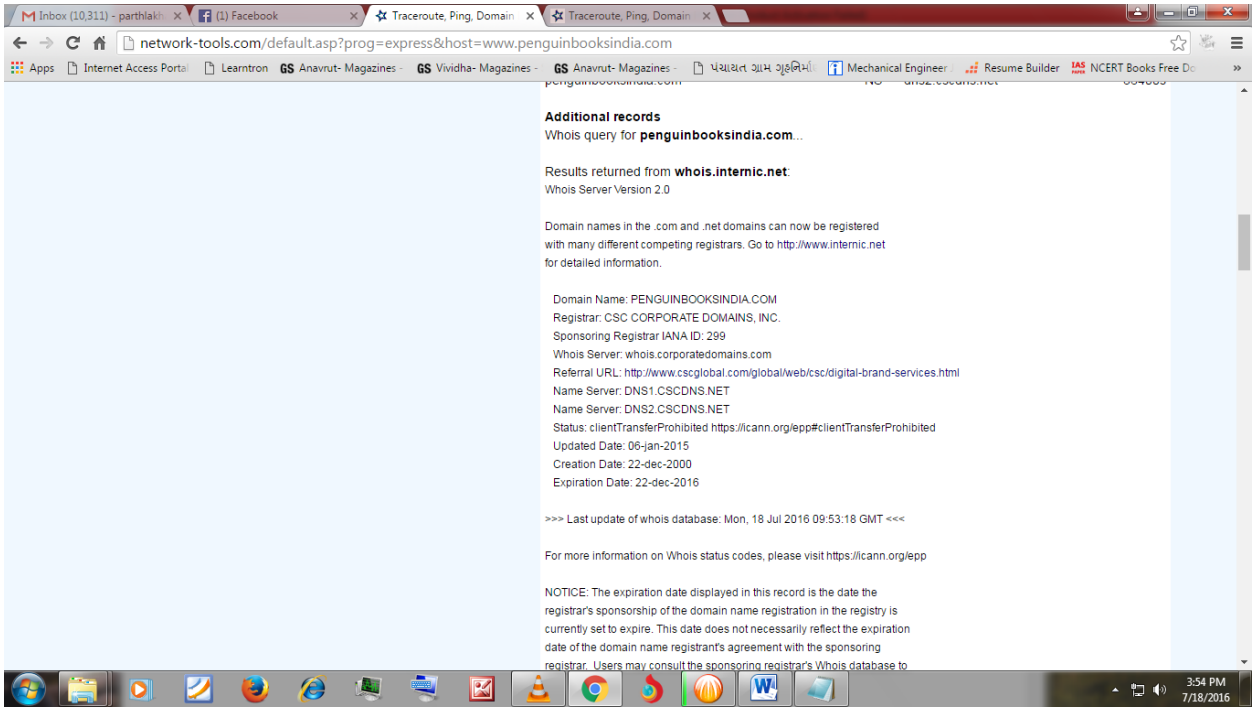
It is query returns information about who has registered a particular domain name, Typically a WHOIS query will return contact details of Domain Owner (like telephone, address, email address etc), DNS servers and other domain name in formation.

There various websites that allows you to play around with DNS:

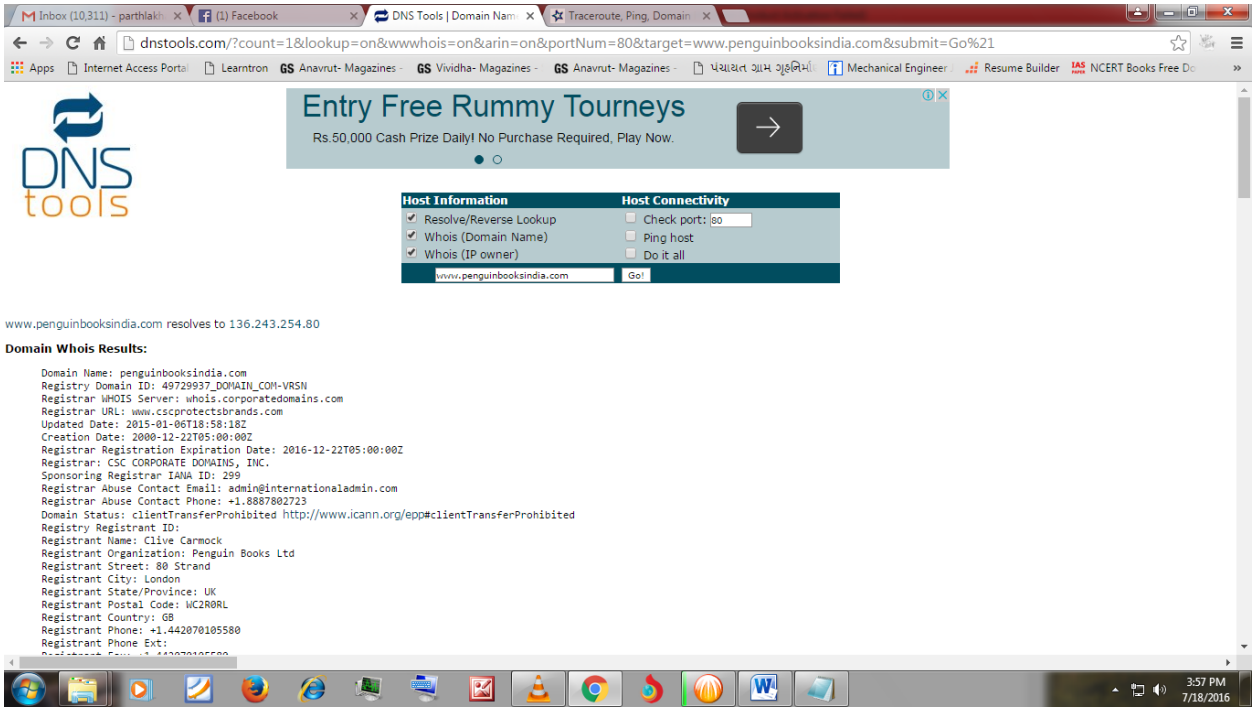
- www.whois.net
- www.iptools.com
- www.betterwhois.com
- www.dnsstuff.com
- www.dnstools.com
- www.network-tools.com



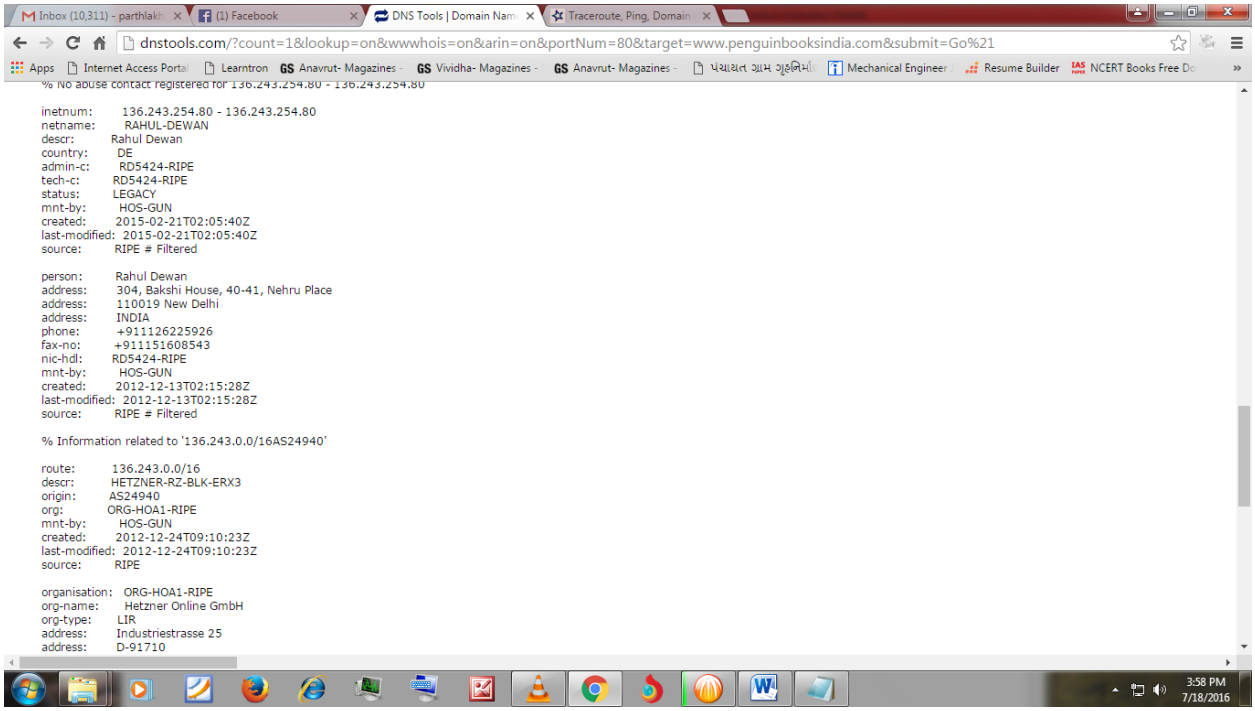
3.1 DNS lookup using network-tools



3.2 DNS lookup using network-tools shows information about domain



3.3 DNS lookup using dnstools.com shows information about domain



3.4 DNS lookup using dnstools.com shows information about admin contact details

➢ Step 4 List of open Ports

Port scanning is the art of scanning a remote target system to abtain a list of open virtual ports on it that are listening for connections. This is usually one of the first few steps every criminal takes.

Why is port scanning Important?

It allows a criminal to identify any potential entry points into a target computer.

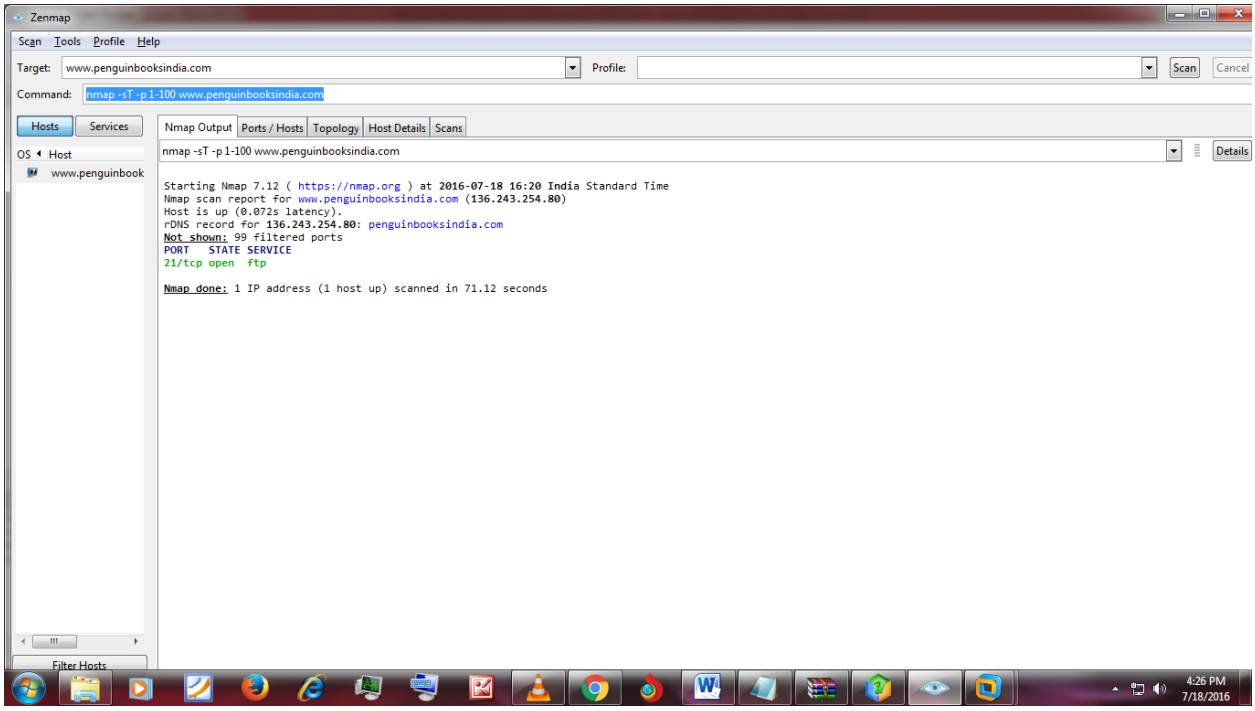
Types of port scan

1) **TCP CONNACT port scan**
2) **TCP SYN port scan**
3) **TCP FIN port scan**
4) **ACK port scan**

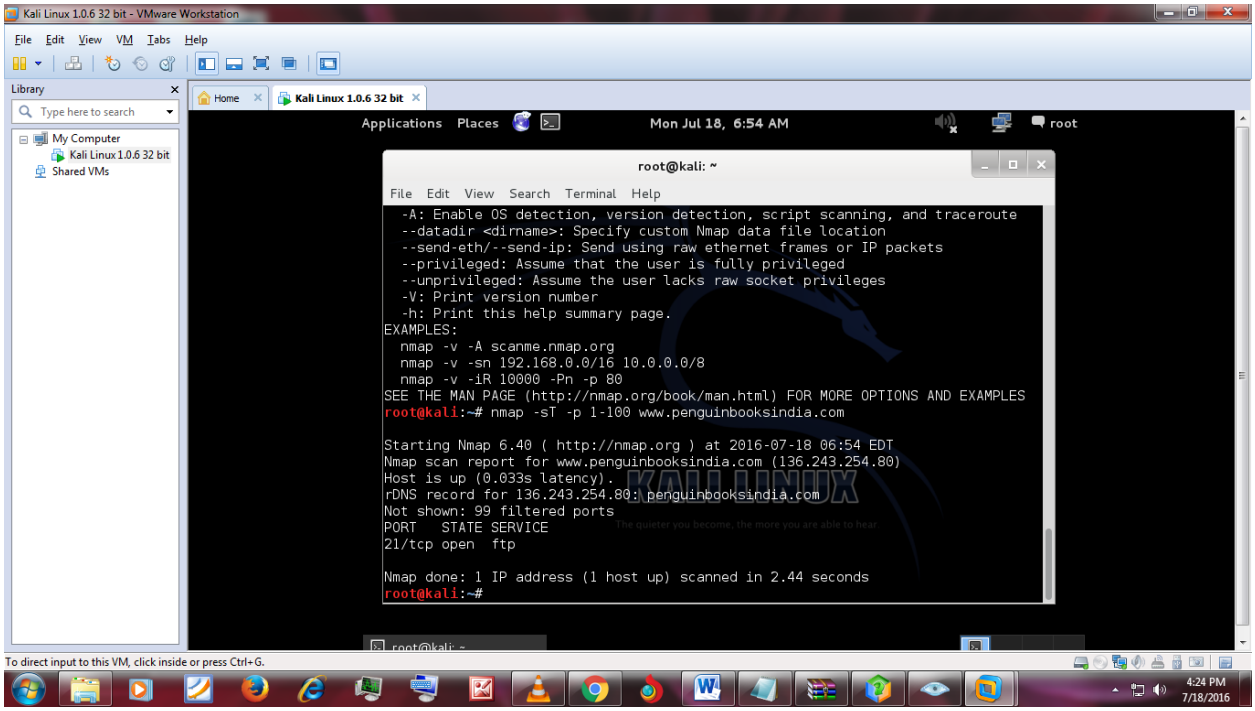
1) TCP CONNACT port scan

This is popular method for port scanning using CONNACT port scan which can be perform by nmap or zenmap using command

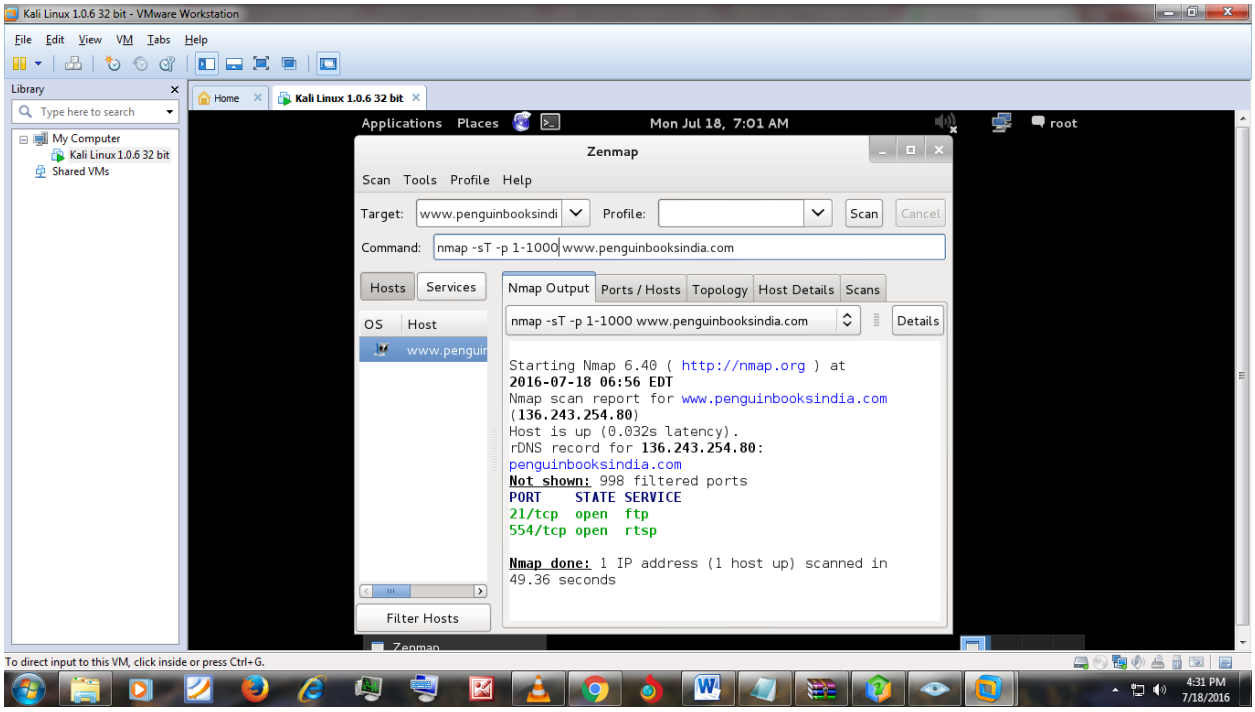
"nmap –sT 1-100(range of ports) TARGET WEBSITE/IP ADDRESS"



4.1 Port scanning using zenmap by TCP CONNACT port scan



4.2 Port scanning usingnmap (kali-linux) by TCP CONNACT port scan



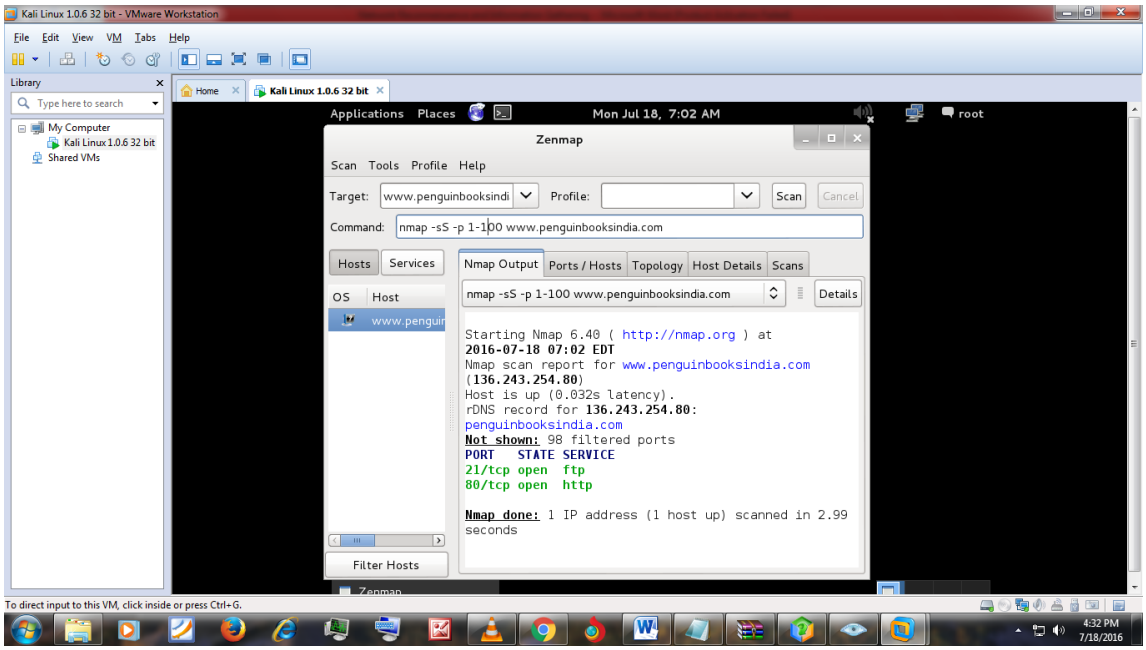
4.3 First 1000 Port scanning using zenmap by TCP CONNACT port scan

Here, there are 3 different methods used for port scanning. Open ports are

No.	Port No.	Service
1	21/tcp	ftp (File Transfer Protocol)
2	554/tcp	rtsp (Real Time Streaming Protocol)

2) TCP SYN port scan/ Halp-open scanning

This is another popular method for port scanning using SYN port scan which can be perform by nmap or zenmap using command "nmap –sS 1-100(range of ports) TARGET WEBSITE/IP ADDRESS"



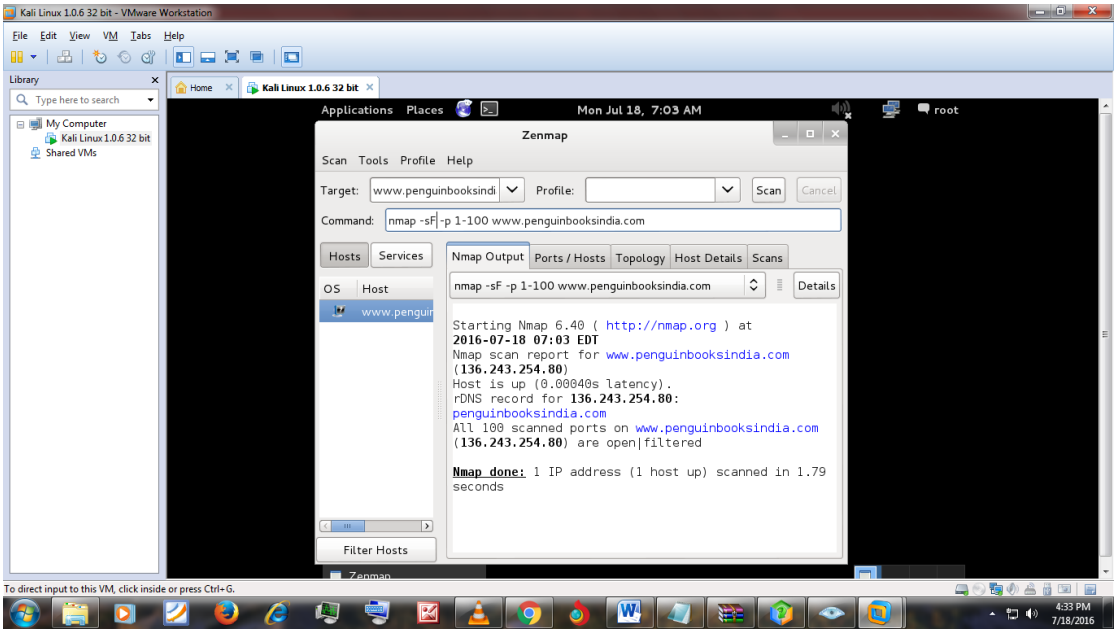
Open ports are

No.	Port No.	Service
1	21/tcp	ftp (File Transfer Protocol)
2	80/tcp	http (Hyper Text Transfer Protocol)

(3) TCP FIN port scan

This is another method for port scanning using FIN port. It is not very reliable port scan which can be perform by nmap or zenmap using command

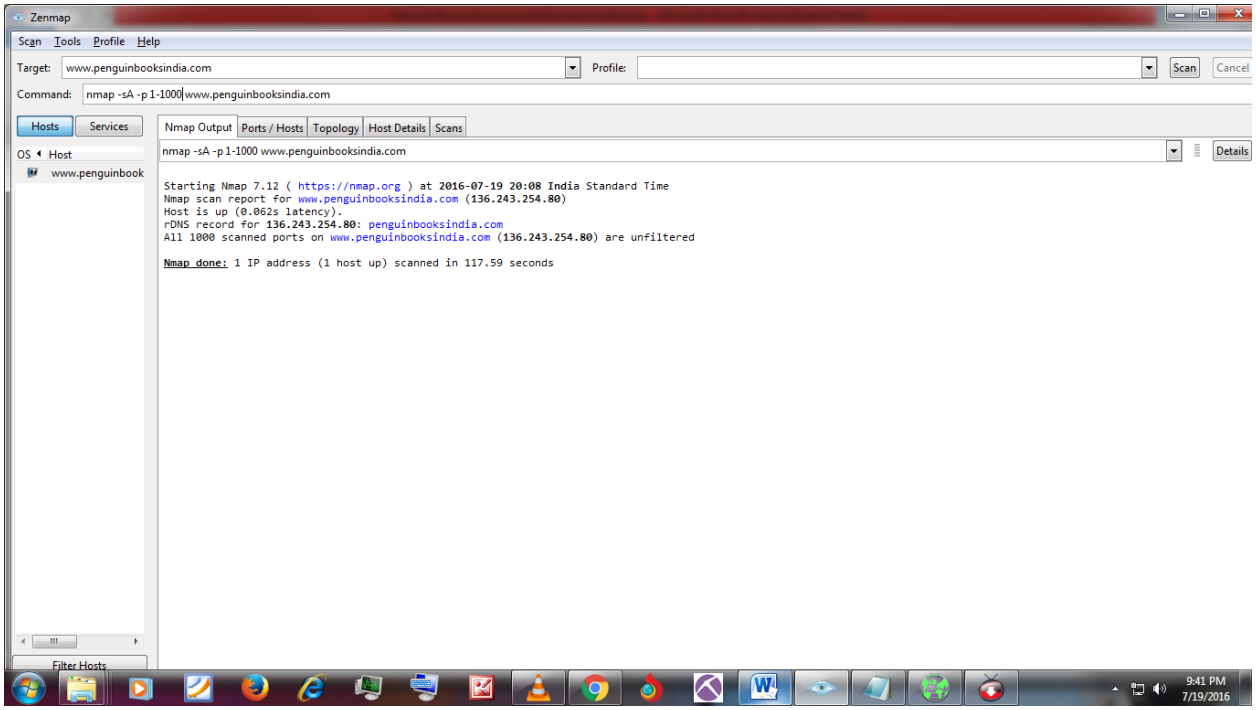
"nmap –sS 1-100(range of ports) TARGET WEBSITE/IP ADDRESS"



(4) ACK port scan for firewall detection

This is another popular method for port scanning using SYN port scan which can be perform by nmap or zenmap using command

"nmap –sA 1-100(range of ports) TARGET WEBSITE/IP ADDRESS"



➢ **Step 5 Software Names & Version**

(1) Daemon Banner Grabbing

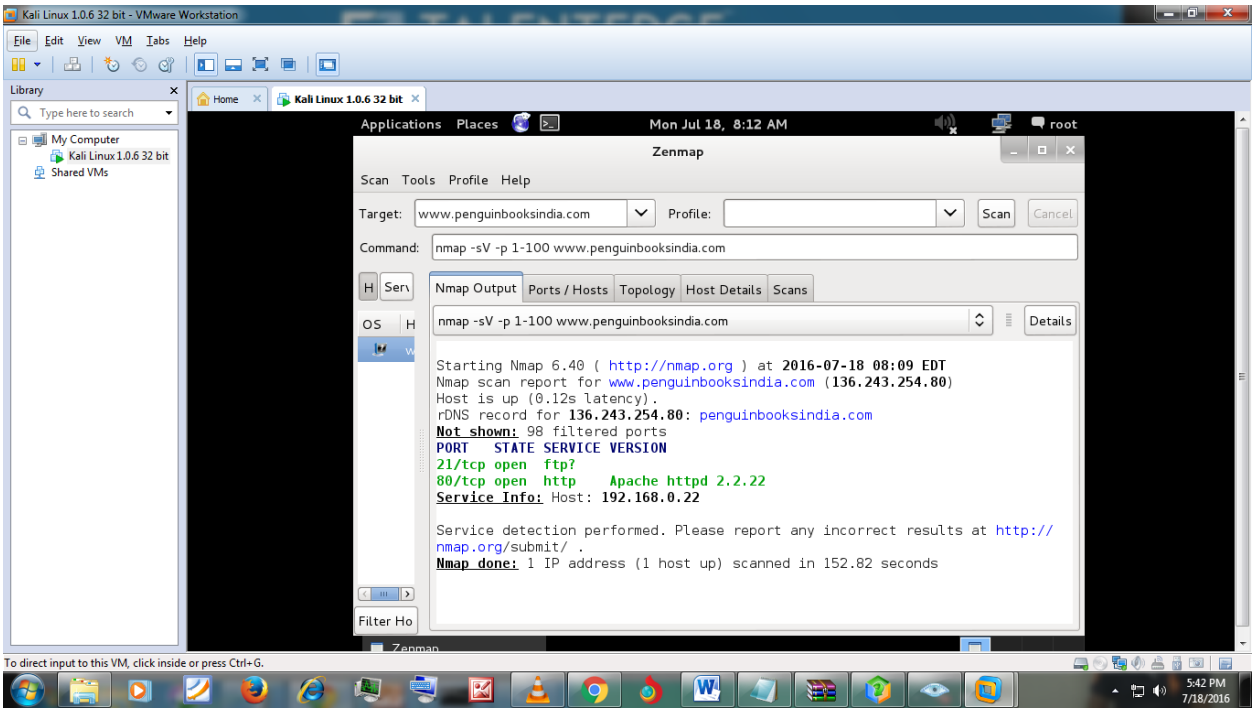
The process of getting useful information about the target system by recording the welcome banners of the daemons running on its various ports.

It can be used to get the following information about target system

- Daemon name and version number.
- OS system information.
- Most importantly, to identify possible points of entry.

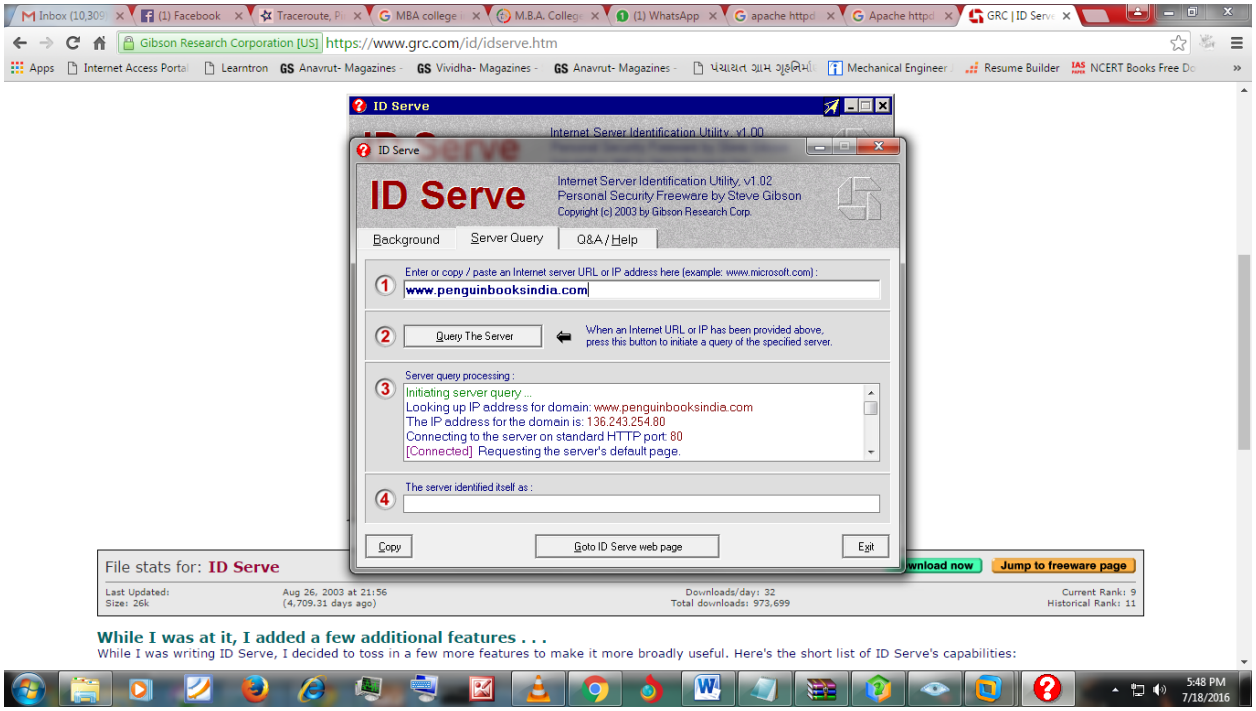
Daemon Banner Grabbing can perform using Nmap or Zenmap or software like ID serve. The command use for Daemon Banner Grabbing in Nmap or Zenmap is

"nmap –sV –p 1-100(range of ports) TARGET WEBSITE/IP ADDRESS"



5.1 Daemon Banner Grabbing using zenmap

Hear you can see that TCP port 80 is open and software Apache httpd version no 2.2.22 is running on port 80.



5.2 Daemon Banner Grabbing using ID Serve

Hear ID Serve does not showing any server.

➢ **Step 6 OS detection**

Very important for an attacker to determine the OS running on the target system. Different OS have different stacks. Hence different OS respond differently to the same packet sent to it by some system.

There are two most effective OS detection techniques are

1) Active fingerprinting
2) Passive fingerprinting.

1) Active Fingerprinting

Active OS fingerprinting is the art of actively sending data packets to the target system to generate a response, which is then analysed and compared to the list of known responses to determine the OS running on the target system.

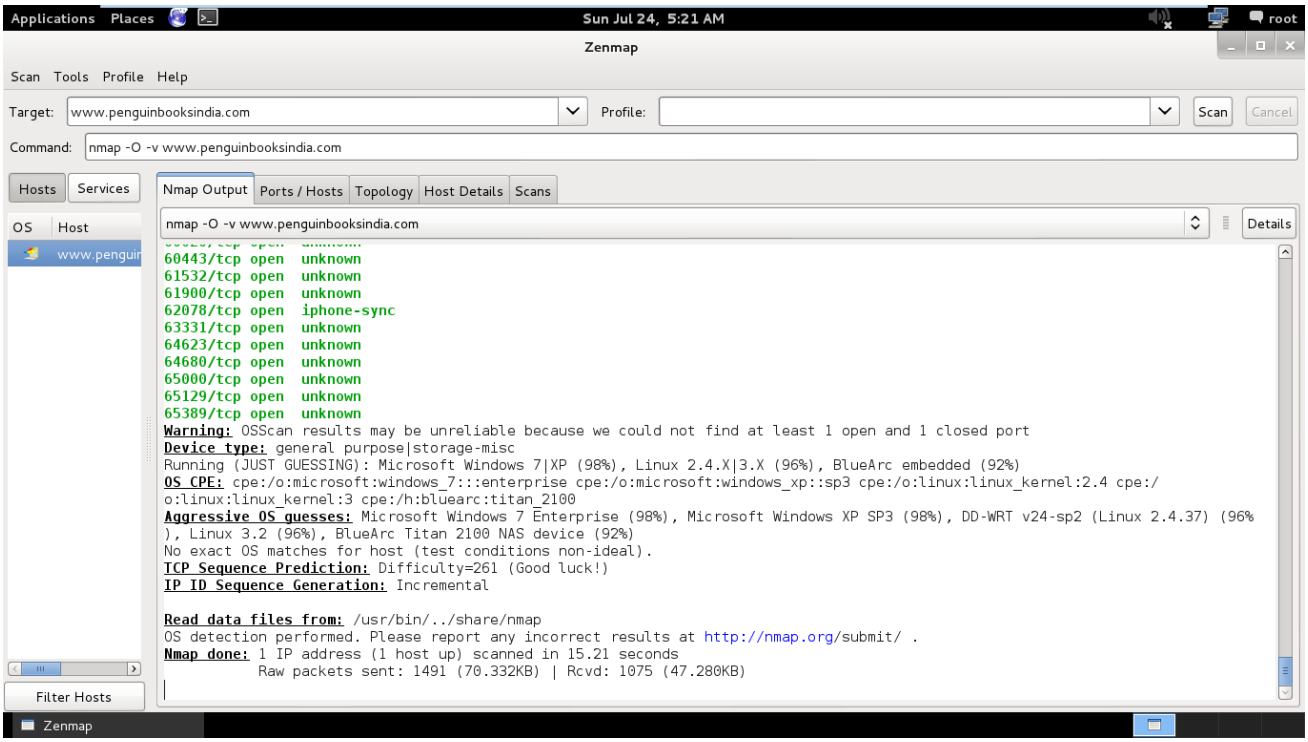
Typically, while analyzing the responses, the following fields and techniques can prove to be helpful.

- TCP initial window size of packets
- TTL values
- ACK values of packets
- Initial sequence number (ISN) values etc.

Active fingerprinting can be performed using zenmap using command like

" nmap –O –v TARGET WEBSITE/IP ADDRESS"

" nmap –A –v TARGET WEBSITE/IP ADDRESS"



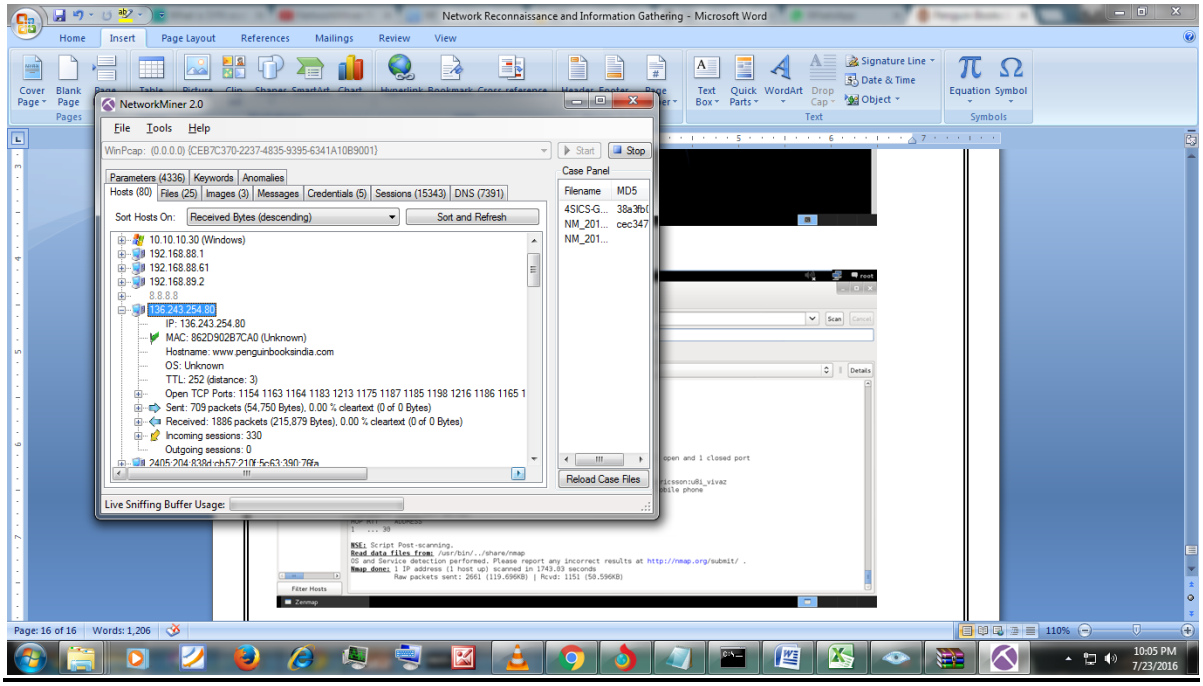
6.1 Active OS fingerprinting using zenmap (Kali-linux)

2) Passive Fingerprinting

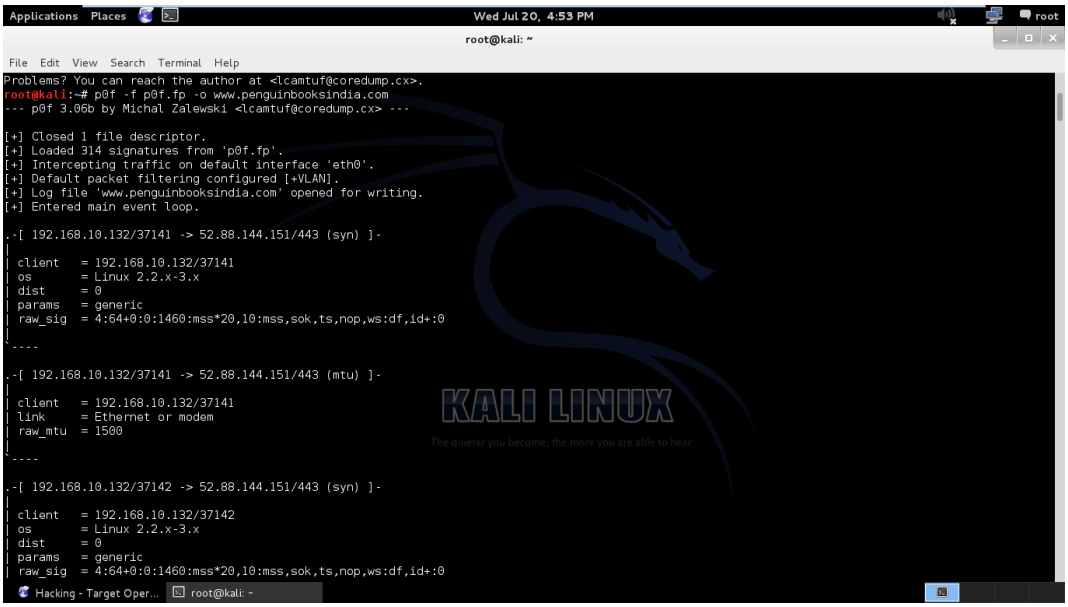
The problem with active fingerprinting is that an attacker needs to actively send messages to the target computer and records its responses, Hence, it is not anonymous. So attacker use Passive fingerprinting rather than Active fingerprinting.

In Passive Fingerprinting, the OS detection tool will try to determine the OS information by simply analyzing the data packets sent by the target system and find out which OS running on target system.

Passive Fingerprinting can be perform using software like network minor or tools like p0f.



6.2 Passive fingerprinting of OS by NetworkMiner



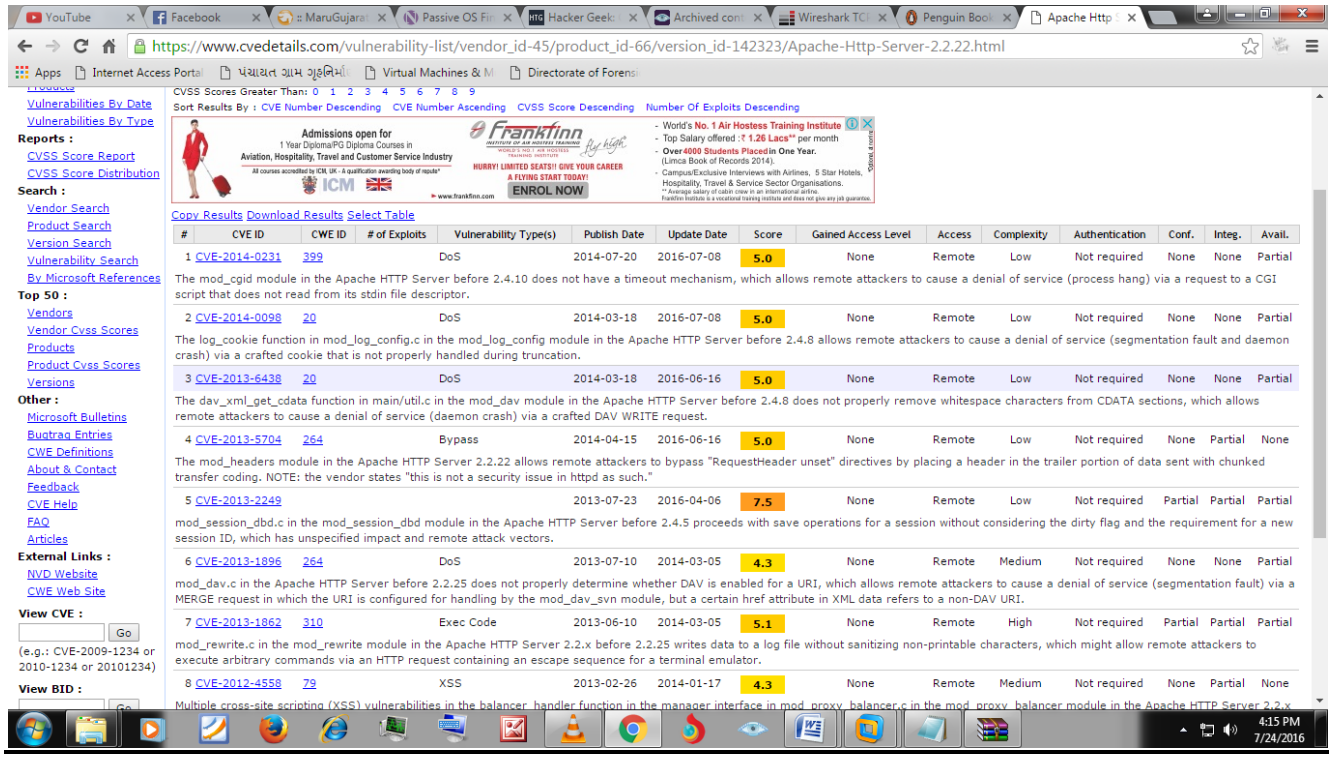
6.3 OS detection using p0f (Kali Linux)

➢ Step 7 Finding Loopholes

After find out OS, software and version, We can find out loopholes using security Auditing tools which scan the victim computer for any potential security loopholes that may exist on it, using which an attacker can hack into it.

It can be done by two methods

1) Security Auditing tools like Nessus, GFI Languard, Retina Scan, SAINT, Core Impact, NSAuditor etc
2) Mannual google search



7.1 Find out different vulnerabilities of apache httpd version no 2.2.22 using google

Detail list of Observations

Observation Table for www.penguinbooksindia.com			
Step No.	**Name**	**Tool/Software use**	**Observation**
1	Victim is online/ offline	Ping using DOS and Zenmap	By bypassing ping using zenmap, clearly shows that host is online
2	Topography Information	Traceroute/Tracert	Not working effectively.
3	DNS Information	DNS tools like network-tools, DNS lookup etc	shows information about domain, admin contact details, telephone, address, email address etc
4	List of open Ports	Port Scanner of different ports like TCP CONNACT port TCP SYN port TCP FIN port ACK port using Zenmap	List of open ports are 21/tcp ftp (File Transfer Protocol) 80/tcp http (Hyper Text Transfer Protocol) 554/tcprtsp (Real Time Streaming Protocol)
5	Software Names & Version	Daemon Banner Grabbing using Zemap and ID serve	TCP port 80 is open and software Apache httpd version no 2.2.22 is running on port 80.
6	OS detection / Fingerprinting	Active OS fingerprinting using Zenmap	Microsoft windows 7 Enterprise (98%), Microsoft windows XP SP3 (98%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), BlueArc Titan 2100 NAS device embedded(92%)
		Passive fingerprinting using network Minor and p0f	Does not show any effective result.
7	Finding Loopholes	Security Auditing Tools	Shows different vulnerabilities of apache httpd version no 2.2.22 using google

Results

The project successfully applied various network reconnaissance and information-gathering techniques to analyze the target website, www.penguinbooksindia.com. Key findings include the identification of open ports (e.g., FTP and HTTP) and the detection of software details such as Apache httpd version 2.2.22. Active and passive OS fingerprinting revealed potential operating systems running on the server, including Windows 7 Enterprise and Linux-based systems, though some limitations were encountered due to firewall restrictions.

Despite these challenges, bypassing ping restrictions and leveraging tools like Zenmap, Nmap, and DNS lookup services provided valuable insights into the network topology, DNS records, and vulnerabilities. Observations also highlighted that while traceroute was limited by security measures, alternative methods helped gather crucial details about the system.

In summary, the project demonstrated how methodical reconnaissance can uncover vulnerabilities, providing actionable intelligence for securing the network. These findings emphasize the importance of ethical hacking practices in proactively identifying and addressing potential security risks.