MAJOR – SEP

Name – Anjali Kuamri

Email – [anjalirajwar101@gmail.com](mailto:anjalirajwar101@gmail.com)

College Name – BIT Sindri

**Cyber Security Major Project**

1. Perform Scanning Module by using Nmap tool (Download from Internet) and scan kalilinux and

Windows 7 machine and find the open/closed ports and services running on machine

Hacker Machine : Windows 10

Victim machine : Kali Linux and Windows 7

* Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.

To run a ping scan -> nmap -sp 192.100.1.1/24

To run a host scan -> nmap -sp <target IP range>

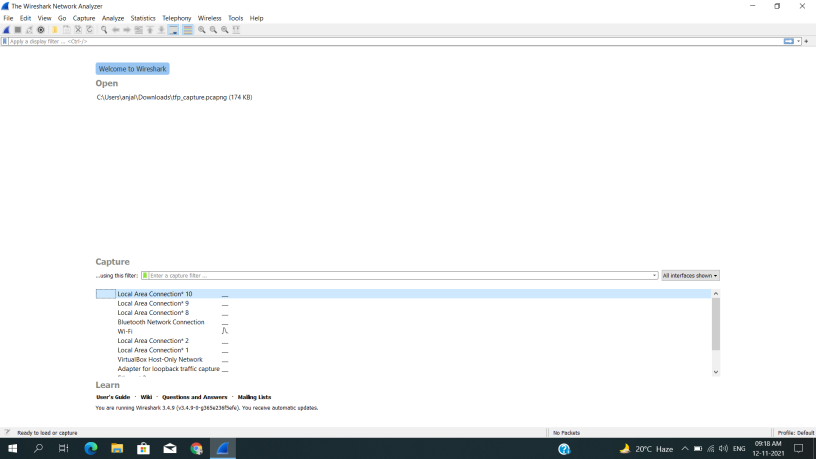
If you see anything unusual in this list, you can then run a DNS query on a specific host, by using -> namp -sL <IP address>

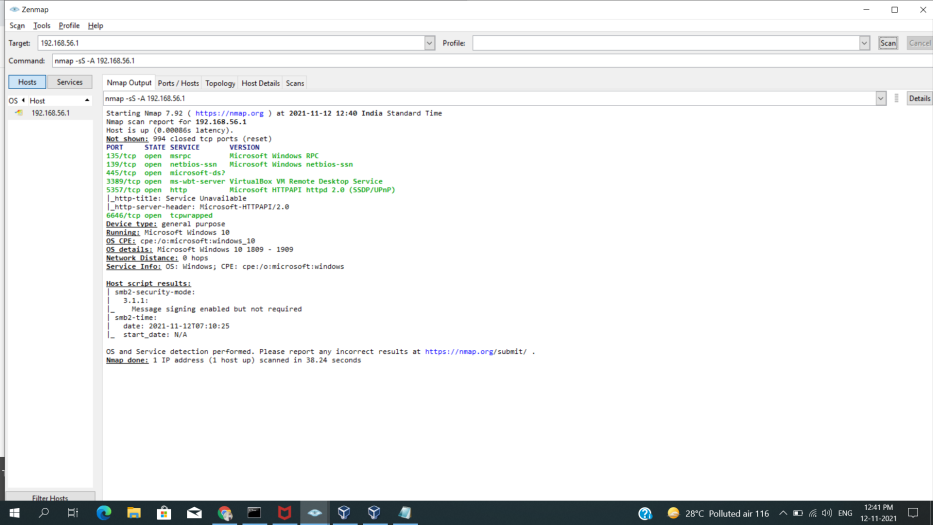
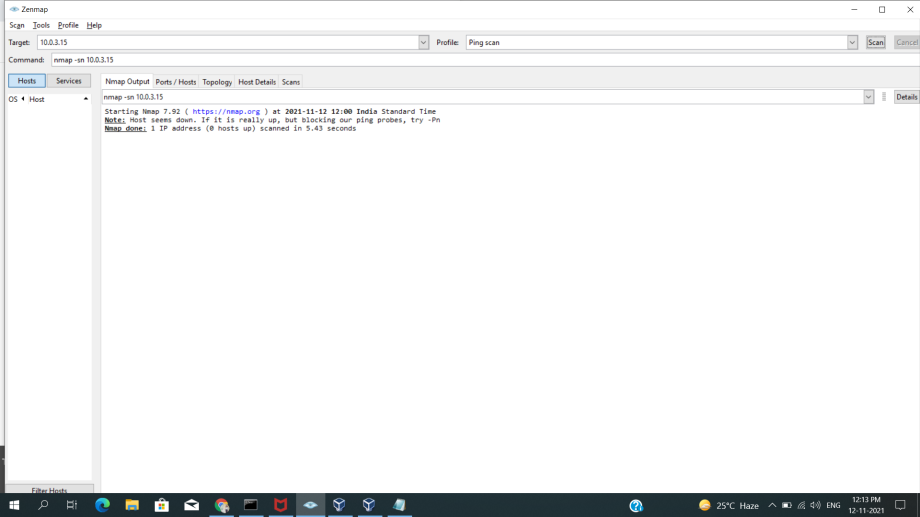
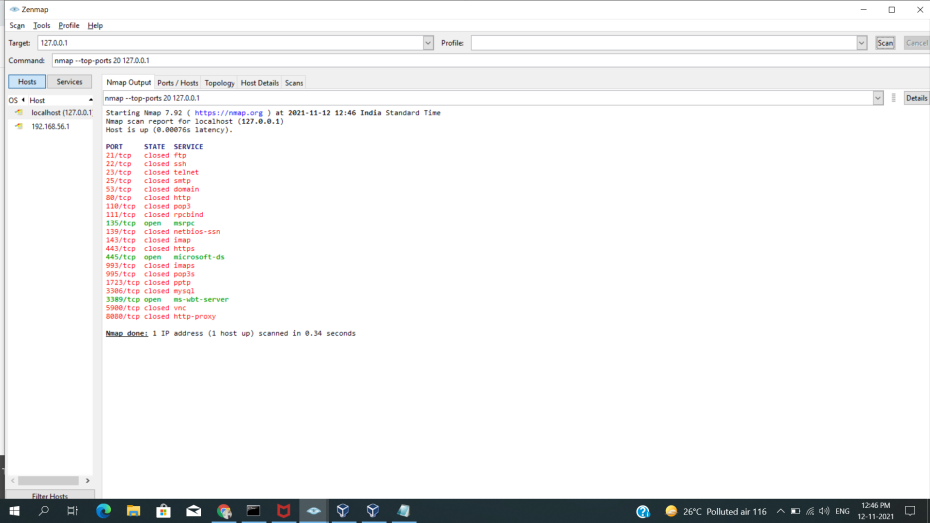
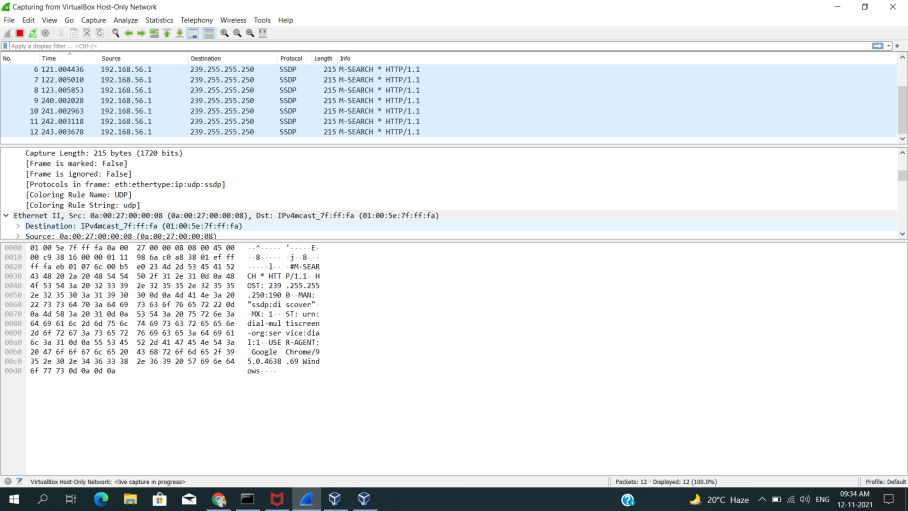
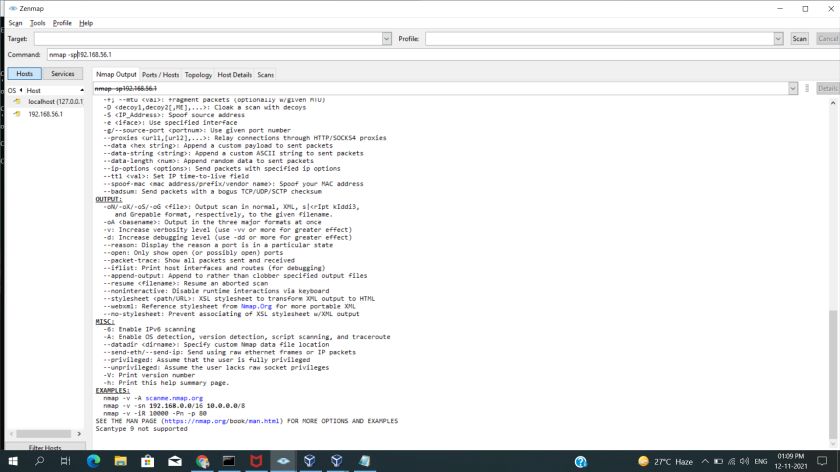
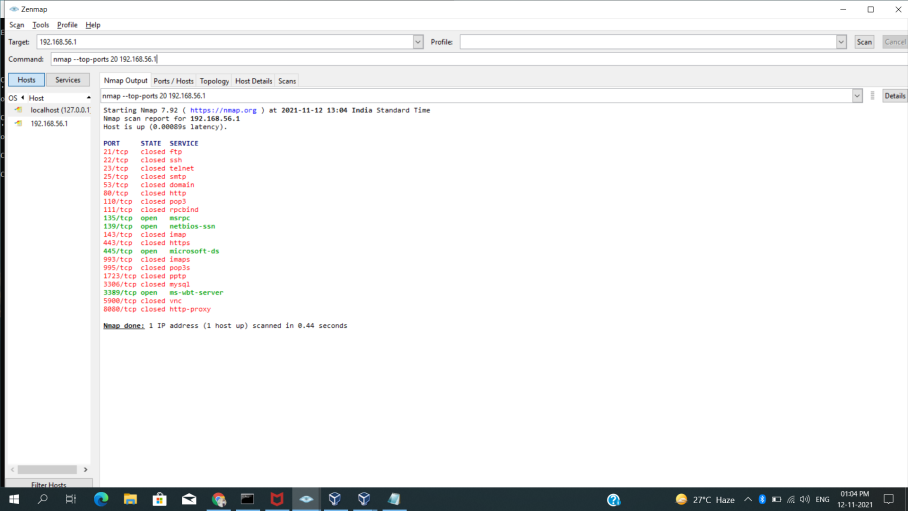
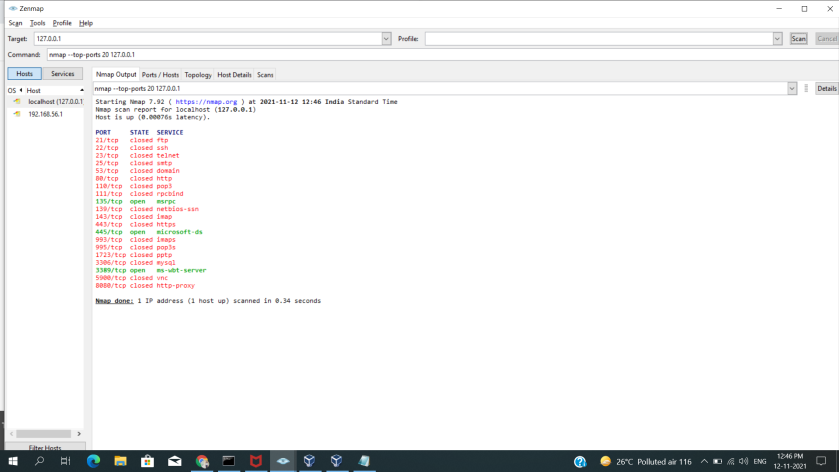
Host Scanning **->** nmap -sp <target IP range>

**OS Scanning ->** nmap –O <target IP>

**Scan The Most Popular Ports ->** nmap --top-ports 20 192.168.1.106

### Disable DNS Name Resolution -> nmap -sp -n 192.100.1.1/24





**Nmap port scan command = nmap** **-p** 80 **X**.X.X.X

### **Basic Nmap Scan against IP or host =** nmap 1.1.1.1

nmap cloudflare.com

### **Nmap Ping Scan** = nmap -sp 192.168.5.0/24

### **Scan specific ports or scan entire port ranges on a local or remote server**

### = nmap -p 1-65535 localhost

### = nmap -p 80,443 8.8.8.8

### **Scan multiple IP addresses**

= nmap 1.1.1.1 8.8.8.8

= nmap 1.1.1.1,2,3,4

### **Scan IP ranges**

= nmap 8.8.8.0/28

= nmap 8.8.8.1-14

= nmap 8.8.8.\*

### **Scan the most popular ports**

= nmap --top-ports 20 192.168.1.106

### **Scan hosts and IP addresses reading from a text file**

= nmap -iL list.txt

### **Save your Nmap scan results to a file**

= nmap -oN output.txt securitytrails.com

= nmap -oX output.xml securitytrails.com

### **Disabling DNS name resolution**

=

### **Scan + OS and service detection with fast execution**

= nmap -A -T4 cloudflare.com

### **Detect service/daemon versions**

= nmap -sV localhost

### **Scan using TCP or UDP protocols**

=

### **CVE detection using Nmap**

= nmap -Pn --script vuln 192.168.1.105

### **Launching DOS with Nmap**

= **nmap** 192.168.1.105 -max-parallelism 800 -Pn --script http-slowloris --script-args http-slowloris.runforever=true

### **Launching brute force attacks**

= **nmap** -sV --script http-wordpress-brute --script-args 'userdb=users.txt,passdb=passwds.txt,http-wordpress-brute.hostname=domain.com, http-wordpress-brute.threads=3,brute.firstonly=true' 192.168.1.105

= **nmap** -p 1433 --script ms-sql-brute --script-args userdb=customuser.txt,passdb=custompass.txt 192.168.1.105

= nmap --script ftp-brute -p 21 192.168.1.105

### **Detecting malware infections on remote hosts**

= nmap -sV --script=http-malware-host 192.168.1.105

= nmap -p80 --script http-google-malware infectedsite.com

= 80/tcp open http

|\_http-google-malware.nse: Host **is** known **for** distributing malware.

**Thank You…**