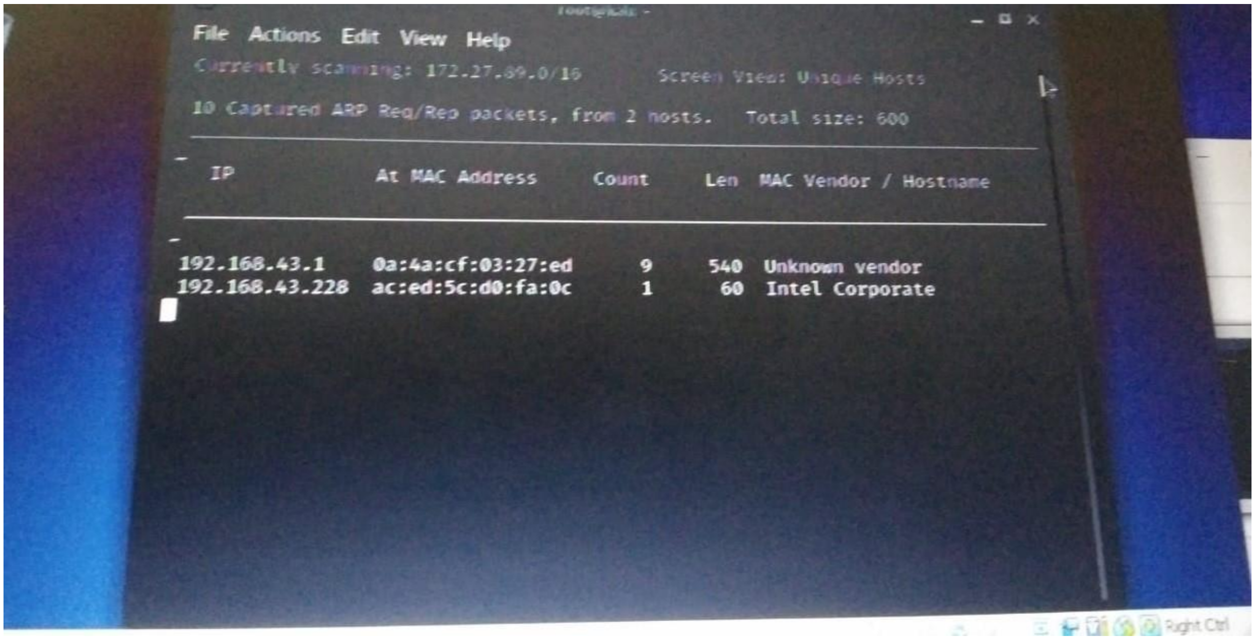
CYBER SECURITY

ROOT-KALI COMMANDS:

1. **NETDISCOVER:** Netdiscover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks.

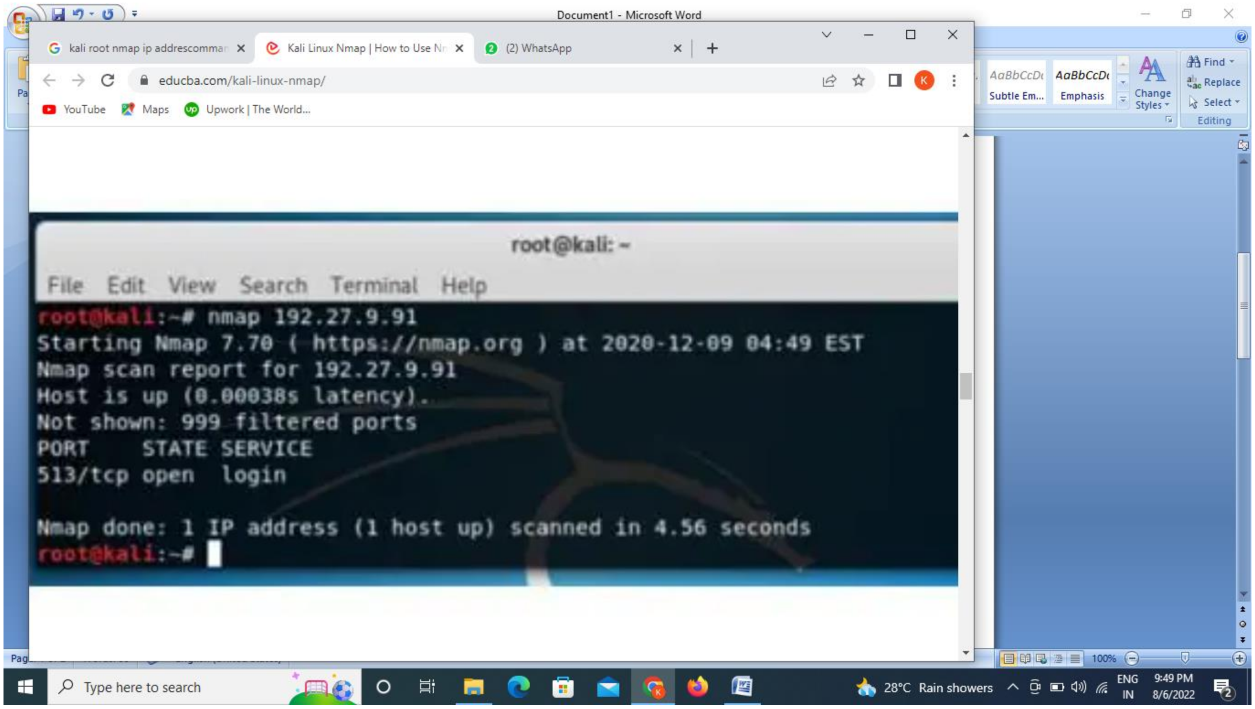
   SYNTAX: netdiscover



```
Currently scanning: 172.27.89.0/16      Screen View: Unique Hosts

10 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 600
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.43.1    0a:4a:cf:03:27:ed      9     540  Unknown vendor
192.168.43.228  ac:ed:5c:d0:fa:0c      1      60  Intel Corporate
```

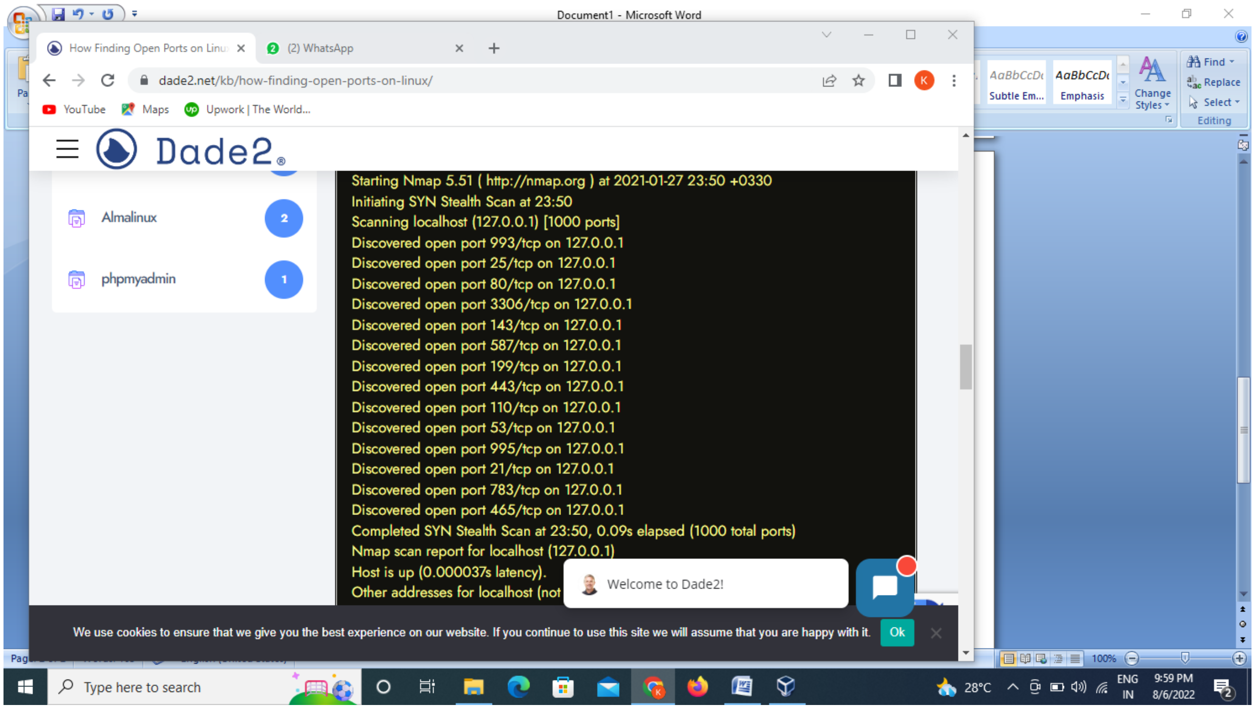
2. **NMAP IPADDRES:** Kali Linux Nmap is defined as a utility which is extensively used by penetration testers for network discovery and auditing the security of a system. In addition to the tasks mentioned earlier, users find the use of Nmap in various other tasks like network inventory, managing schedules for any service upgrades, host monitoring, service uptime tracking etc.

   SYNTAX: nmap ipaddress



```
root@kali:~# nmap 192.27.9.91
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-09 04:49 EST
Nmap scan report for 192.27.9.91
Host is up (0.00038s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
513/tcp open  login

Nmap done: 1 IP address (1 host up) scanned in 4.56 seconds
root@kali:~#
```

3. **NMAP -P IP:** Nmap builds on previous network auditing tools to provide quick, detailed scans of network traffic. It works by using IP packets to identify the hosts and IPs active on a network and then analyze these packets to provide information on each host and IP, as well as the operating systems they are running.



Almalinux 2

phpmyadmin 1

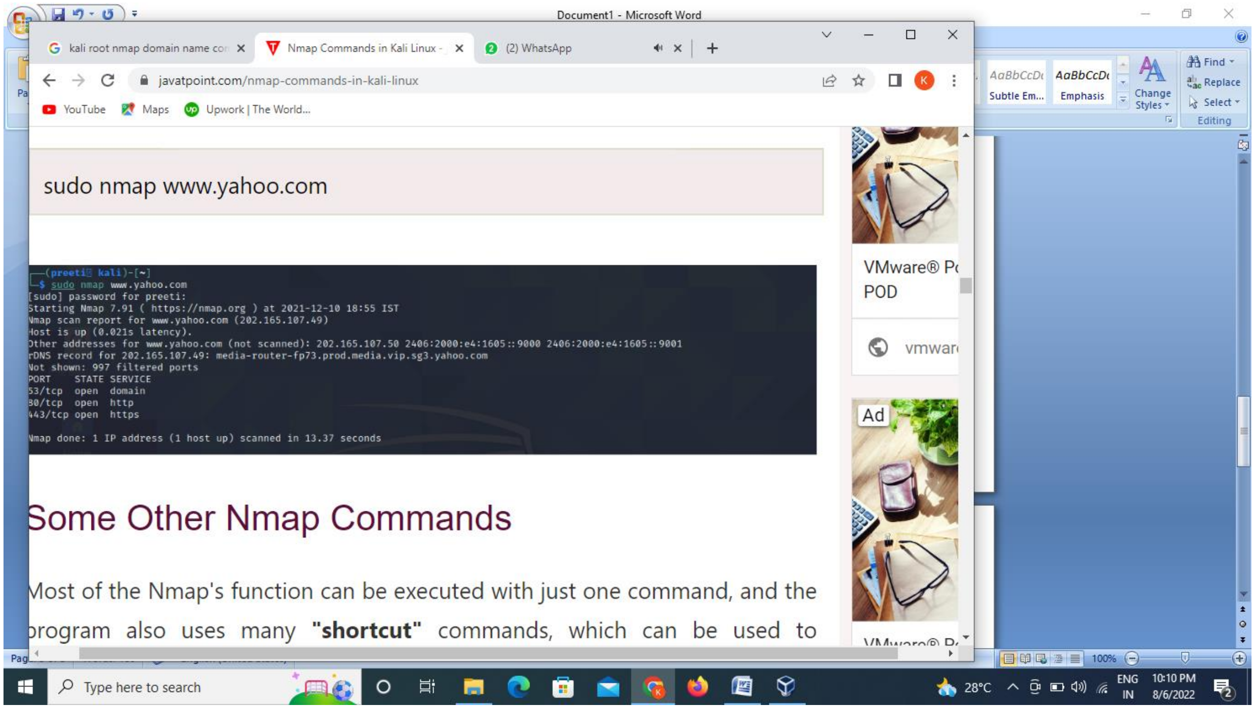
```
Starting Nmap 5.51 ( http://nmap.org ) at 2021-01-27 23:50 +0330
Initiating SYN Stealth Scan at 23:50
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 993/tcp on 127.0.0.1
Discovered open port 25/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 143/tcp on 127.0.0.1
Discovered open port 587/tcp on 127.0.0.1
Discovered open port 199/tcp on 127.0.0.1
Discovered open port 443/tcp on 127.0.0.1
Discovered open port 110/tcp on 127.0.0.1
Discovered open port 53/tcp on 127.0.0.1
Discovered open port 995/tcp on 127.0.0.1
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 783/tcp on 127.0.0.1
Discovered open port 465/tcp on 127.0.0.1
Completed SYN Stealth Scan at 23:50, 0.09s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000037s latency).
Other addresses for localhost (not
```

Welcome to Dade2!

We use cookies to ensure that we give you the best experience on our website. If you continue to use this site we will assume that you are happy with it. Ok

4. NMAP DOMAIN NAME: nmap for scanning a host

Syntax: sudo nmap www.yahoo.com



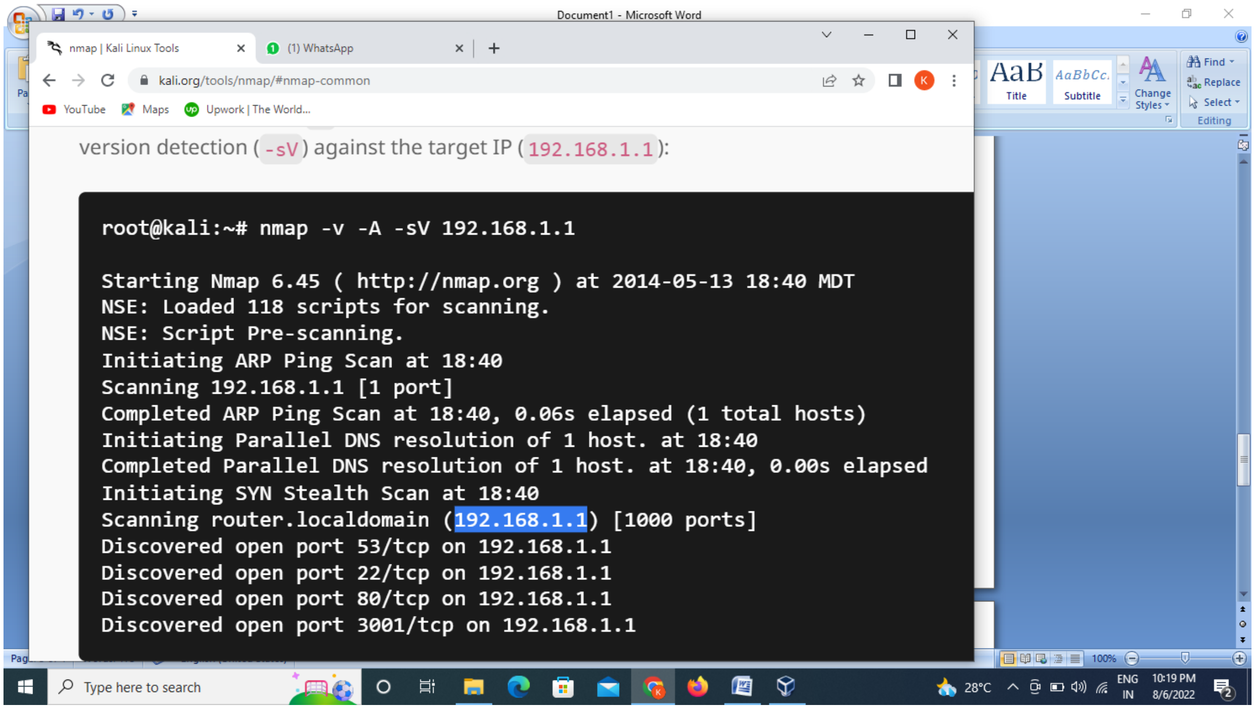
```
sudo nmap www.yahoo.com
```

```
┌──(preeti㉿ kali)-[~]
└─$ sudo nmap www.yahoo.com
[sudo] password for preeti:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:55 IST
Nmap scan report for www.yahoo.com (202.165.107.49)
Host is up (0.021s latency).
Other addresses for www.yahoo.com (not scanned): 202.165.107.50 2406:2000:e4:1605::9000 2406:2000:e4:1605::9001
rDNS record for 202.165.107.49: media-router-fp73.prod.media.vip.sg3.yahoo.com
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

Some Other Nmap Commands

Most of the Nmap's function can be executed with just one command, and the program also uses many **"shortcut"** commands, which can be used to

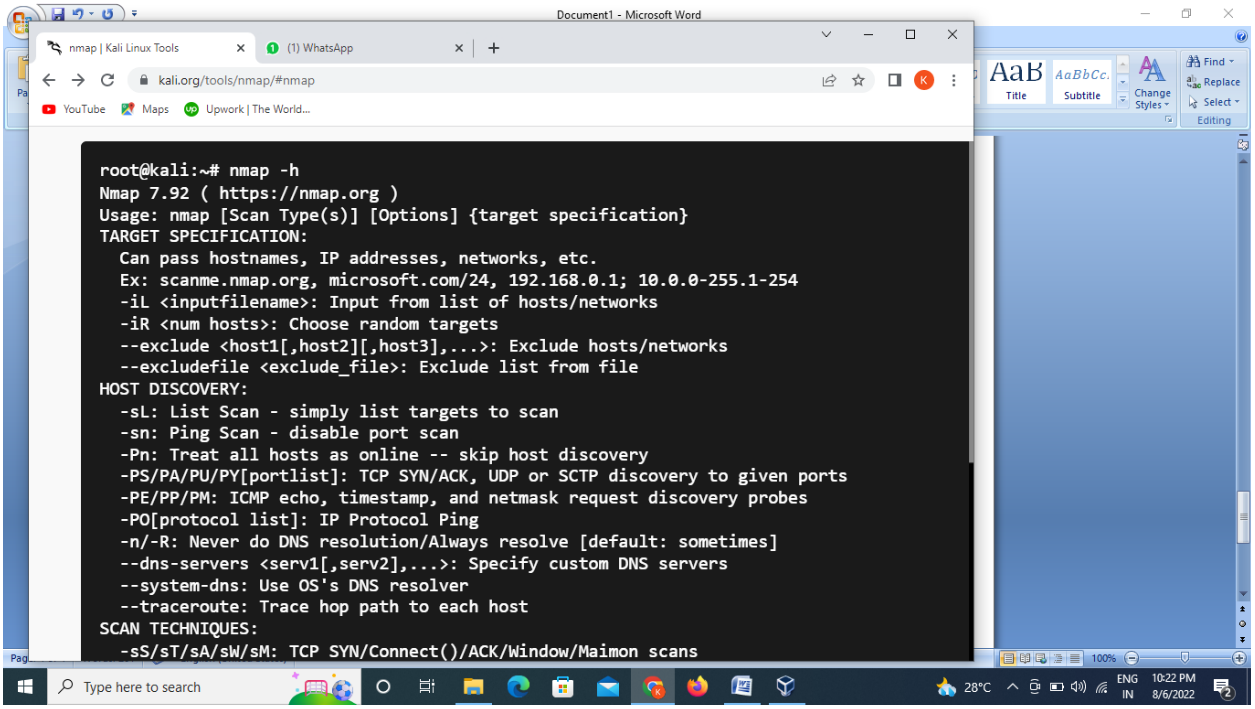
5. **NMAP –V –A –sV ip :** Scan in verbose mode (`–v`), enable OS detection, version detection, script scanning, and traceroute (–`A`), with version detection (`–sV`) against the target IP (`192.168.1.1`)



version detection (`-sV`) against the target IP (`192.168.1.1`):

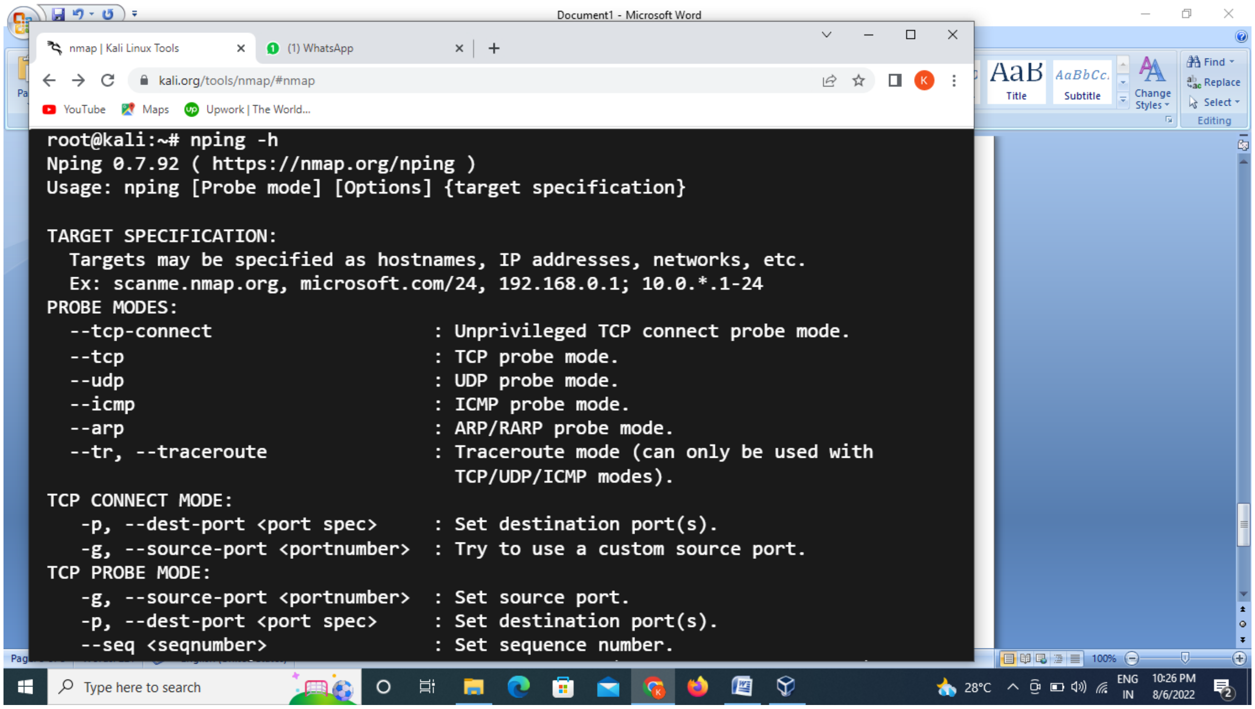
```
root@kali:~# nmap -v -A -sV 192.168.1.1

Starting Nmap 6.45 ( http://nmap.org ) at 2014-05-13 18:40 MDT
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 18:40
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 18:40, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:40
Completed Parallel DNS resolution of 1 host. at 18:40, 0.00s elapsed
Initiating SYN Stealth Scan at 18:40
Scanning router.localdomain (192.168.1.1) [1000 ports]
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 3001/tcp on 192.168.1.1
```

6. **NMAP –H:** Network exploration tool and security / port scanner.



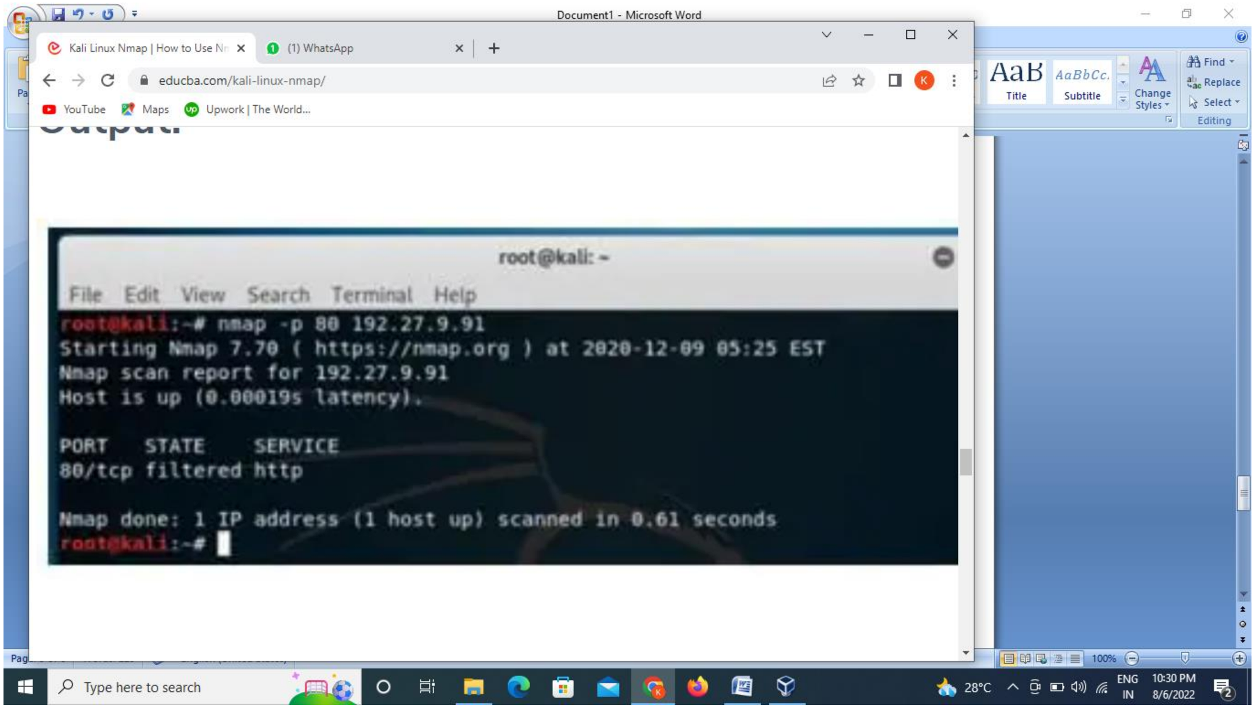
```
root@kali:~# nmap -h
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
```

7. ## NPING : Network packet generation tool / ping utility.



```
root@kali:~# nping -h
Nping 0.7.92 ( https://nmap.org/nping )
Usage: nping [Probe mode] [Options] {target specification}

TARGET SPECIFICATION:
  Targets may be specified as hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.*.1-24
PROBE MODES:
  --tcp-connect                    : Unprivileged TCP connect probe mode.
  --tcp                            : TCP probe mode.
  --udp                            : UDP probe mode.
  --icmp                           : ICMP probe mode.
  --arp                            : ARP/RARP probe mode.
  --tr, --traceroute               : Traceroute mode (can only be used with
                                     TCP/UDP/ICMP modes).
TCP CONNECT MODE:
   -p, --dest-port <port spec>     : Set destination port(s).
   -g, --source-port <portnumber>  : Try to use a custom source port.
TCP PROBE MODE:
   -g, --source-port <portnumber>  : Set source port.
   -p, --dest-port <port spec>     : Set destination port(s).
   --seq <seqnumber>               : Set sequence number.
```

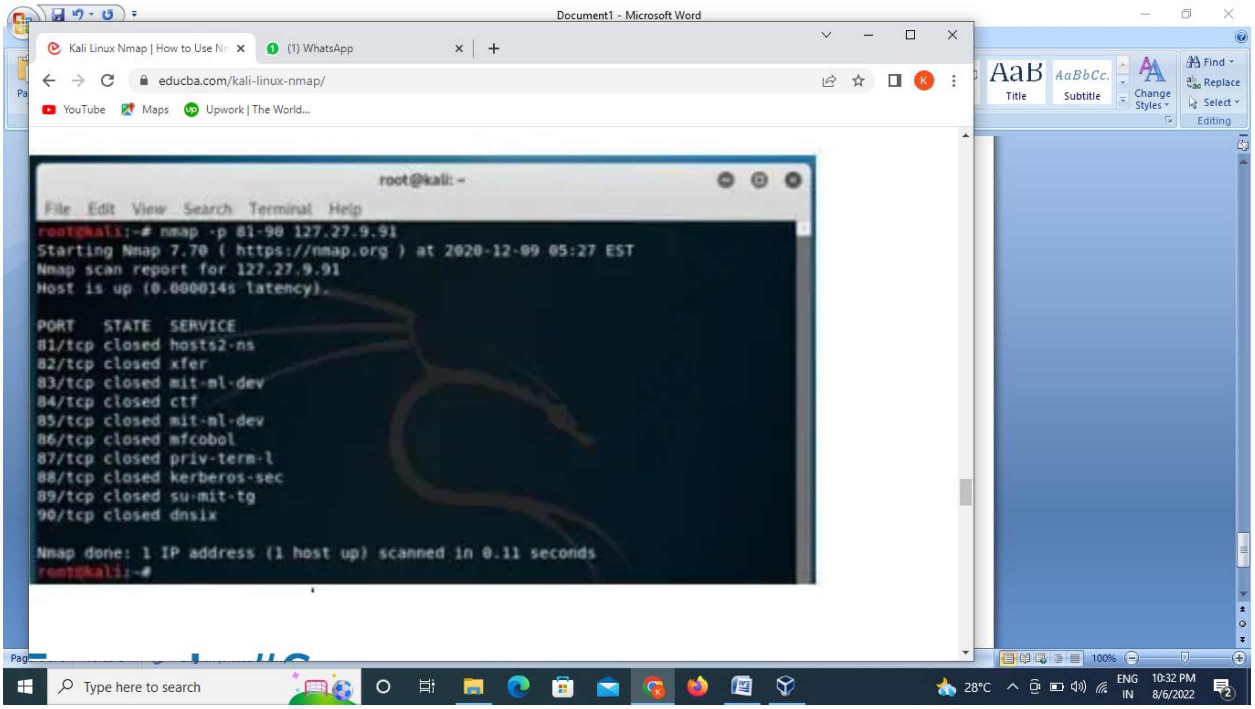
8. ## NMAP –P IPADDRES: nmap -p 80 192.27.9.91



```
root@kali:~# nmap -p 80 192.27.9.91
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-09 05:25 EST
Nmap scan report for 192.27.9.91
Host is up (0.00019s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
root@kali:~#
```

9. NMAP –P IPADDRES ANDRANGE: The scanning range of ports.

Syntax: nmap -p 81-90 127.27.9.91

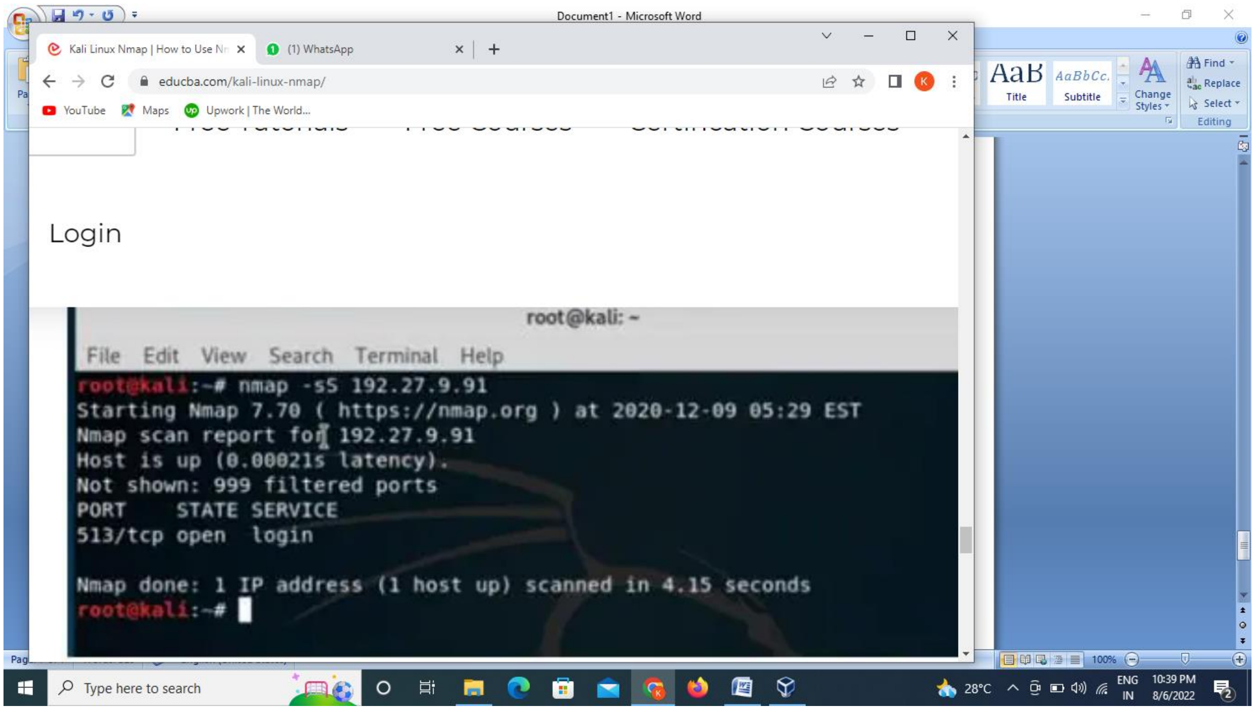


```
root@kali:~# nmap -p 81-90 127.27.9.91
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-09 05:27 EST
Nmap scan report for 127.27.9.91
Host is up (0.000014s latency).

PORT   STATE  SERVICE
81/tcp closed hosts2-ns
82/tcp closed xfer
83/tcp closed mit-ml-dev
84/tcp closed ctf
85/tcp closed mit-ml-dev
86/tcp closed mfcobol
87/tcp closed priv-term-l
88/tcp closed kerberos-sec
89/tcp closed su-mit-tg
90/tcp closed dnsix

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@kali:~#
```

10. NMAP –F IP :Scanning 100 most common ports.

Syntax:`nmap -f 192.27.9.91` . Using the details printed on the console, one can take a copy of the same into a text editor perform required analytics. Along with this, Kali Linux provides utility to get the entire result of the Nmap on a file and utilize it later for its numerous other uses. With just its one base command with multiple other options, Nmap helps users with loads of information to protect machines from unwanted attacks.

-



```
root@kali:~# nmap -sS 192.27.9.91
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-09 05:29 EST
Nmap scan report for 192.27.9.91
Host is up (0.00021s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE
513/tcp open  login

Nmap done: 1 IP address (1 host up) scanned in 4.15 seconds
root@kali:~#
```