SIES COLLEGE OF ARTS, SCIENCE & COMMERCE
(EMPOWERED AUTONOMOUS)
SION(W), MUMBAI – 22

DEPARTMENT OF INFORMATION TECHNOLOGY

M.Sc. (I.T.) PART – II, SEMESTER – IV

Practical Journal
for
the subject

Ethical Hacking

Submitted by

Asai Prathamesh Mangesh
SMIT2324003

For the academic year
2023-2024

SIES College of Arts, Science & Commerce
RISE WITH EDUCATION
Sion (West), Mumbai – 400022.
(Autonomous)

SIES College of Arts, Science and Commerce (Autonomous),

Sion (W), Mumbai – 400 022.

Department of Information Technology

CERTIFICATE

This is to certify that **Mr. Asai Prathamesh Mangesh** of M.Sc. [Information Technology], Part – II, Seat No. **SMIT2324003** has successfully completed the practicals and submitted it online in Microsoft Teams for the subject of **Ethical Hacking** as a partial fulfilment of the degree M.Sc. (I.T.) during the academic year 2023-24.

Anam Khan	**Anam Khan**
Faculty-in-Charge	Internal Examiner

Date: 12/04/2024 College Seal External Examiner

INDEX

Sr. No.	Practical Topics	Sign
1	Utilize the Nessus Vulnerability Scanner	
2	Implement Network Scanning	
3	Implement NET-BIOS Enumeration	
4	Implement SMTP Enumeration	
5	Implement Password Cracking	
6	Perform IP Scanning	
7	Perform Network Mapping	
8	Perform Brute Force Attack	

Practical No. 01 – Utilize the Nessus Vulnerability Scanner

As Nessus is a paid tool, we will be using an alternative tool for vulnerability scanning

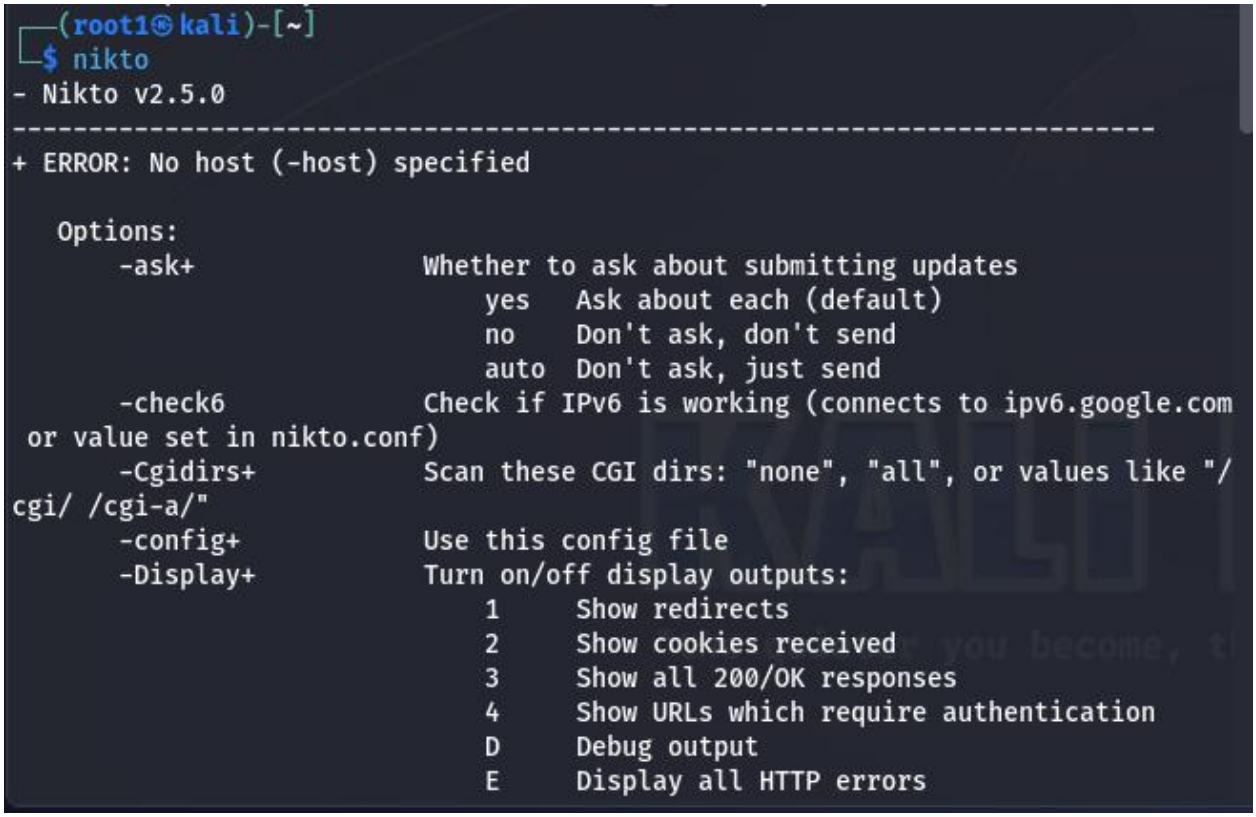
Tool Used for this practical is NIKTO

Step 1: Open Kali Linux Vmware

Step 2: Go to Terminal Write a command

$ nikto

(This command will help you to know different operation you can perform with nikto tool)



```
                              S     Scrub output of IPs and hostnames
                              V     Verbose output
       -dbcheck               Check database and other key files for syntax errors
       -evasion+              Encoding technique:
                              1     Random URI encoding (non-UTF8)
                              2     Directory self-reference (/./)
                              3     Premature URL ending
                              4     Prepend long random string
                              5     Fake parameter
                              6     TAB as request spacer
                              7     Change the case of the URL
                              8     Use Windows directory separator (\)
                              A     Use a carriage return (0x0d) as a request s
pacer
                              B     Use binary value 0x0b as a request spacer
        -followredirects      Follow 3xx redirects to new location
        -Format+              Save file (-o) format:
                              csv   Comma-separated-value
                              json  JSON Format
                              htm   HTML Format
                              nbe   Nessus NBE format
                              sql   Generic SQL (see docs for schema)
                              txt   Plain text
```

```
                              (if not specified the format will be taken from t
he file extension passed to -output)
       -Help                  This help information
       -host+                 Target host/URL
       -id+                   Host authentication to use, format is id:pass or id:pa
ss:realm
       -ipv4                     IPv4 Only
       -ipv6                     IPv6 Only
       -key+                  Client certificate key file
       -list-plugins          List all available plugins, perform no testing
       -maxtime+              Maximum testing time per host (e.g., 1h, 60m, 3600s)
       -mutate+               Guess additional file names:
       -mutate-options        Provide information for mutates
       -nointeractive         Disables interactive features
       -nolookup              Disables DNS lookups
       -nossl                 Disables the use of SSL
       -noslash               Strip trailing slash from URL (e.g., '/admin/' to '/ad
min')
       -no404                 Disables nikto attempting to guess a 404 page
       -Option                Over-ride an option in nikto.conf, can be issued multi
ple times
       -output+               Write output to this file ('.' for auto-name)
       -Pause+                Pause between tests (seconds)
```

```
       -ssl                 Force ssl mode on port
       -Tuning+             Scan tuning:
                                 1     Interesting File / Seen in logs
                                 2     Misconfiguration / Default File
                                 3     Information Disclosure
                                 4     Injection (XSS/Script/HTML)
                                 5     Remote File Retrieval - Inside Web Root
                                 6     Denial of Service
                                 7     Remote File Retrieval - Server Wide
                                 8     Command Execution / Remote Shell
                                 9     SQL Injection
                                 0     File Upload
                                 a     Authentication Bypass
                                 b     Software Identification
                                 c     Remote Source Inclusion
                                 d     WebService
                                 e     Administrative Console
                                 x     Reverse Tuning Options (i.e., include all e
xcept specified)
       -timeout+            Timeout for requests (default 10 seconds)
       -Userdbs             Load only user databases, not the standard databases
                                 all   Disable standard dbs and load only user dbs
                                 tests Disable only db_tests and load udb_tests
```

Step 3: Perform a vulnerability scanning for the target organization by writing IP address or host name

$ nikto -h siesascs.edu.in

```
┌──(root1㉿kali)-[~]
└─$ nikto -h siesascs.edu.in
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          169.38.89.3
+ Target Hostname:    siesascs.edu.in
+ Target Port:        80
+ Start Time:         2024-01-31 15:57:23 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ /: Retrieved via header: HTTP/1.1 forward.http.proxy:3128.
+ /: Retrieved x-powered-by header: PHP/8.0.0.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://d
eveloper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type. Se
e: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-
content-type-header/
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.
mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page / redirects to: https://siesascs.edu.in/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Step 4: Perform a SSL vulnerability scanning for the target organization by writing IP address or host name with -ssl

$ nikto -h siesascs.edu.in -ssl

```
┌──(root1㉿kali)-[~]
└─$ nikto -h siesascs.edu.in -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          169.38.89.3
+ Target Hostname:    siesascs.edu.in
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=siesascs.edu.in
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=BE/O=GlobalSign nv-sa/CN=AlphaSSL CA - SHA256 -
G4
+ Start Time:         2024-01-31 16:01:20 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ /: Retrieved x-powered-by header: PHP/8.0.0.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://d
eveloper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defi
ned. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Trans
port-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type. Se
e: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-
```

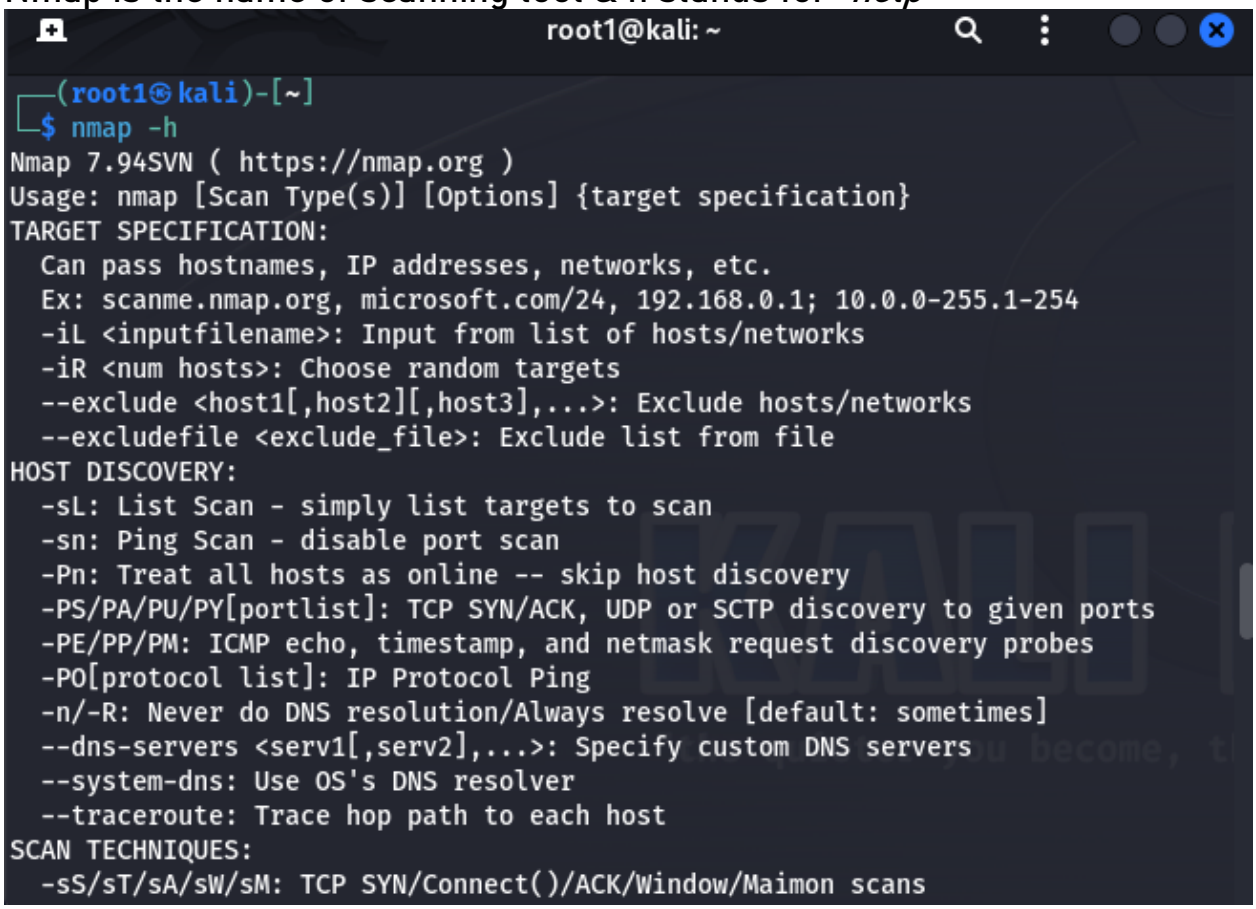
```
port-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type. Se
e: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-
content-type-header/
+ /: Cookie PHPSESSID created without the secure flag. See: https://developer.mo
zilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.
mozilla.org/en-US/docs/Web/HTTP/Cookies
```

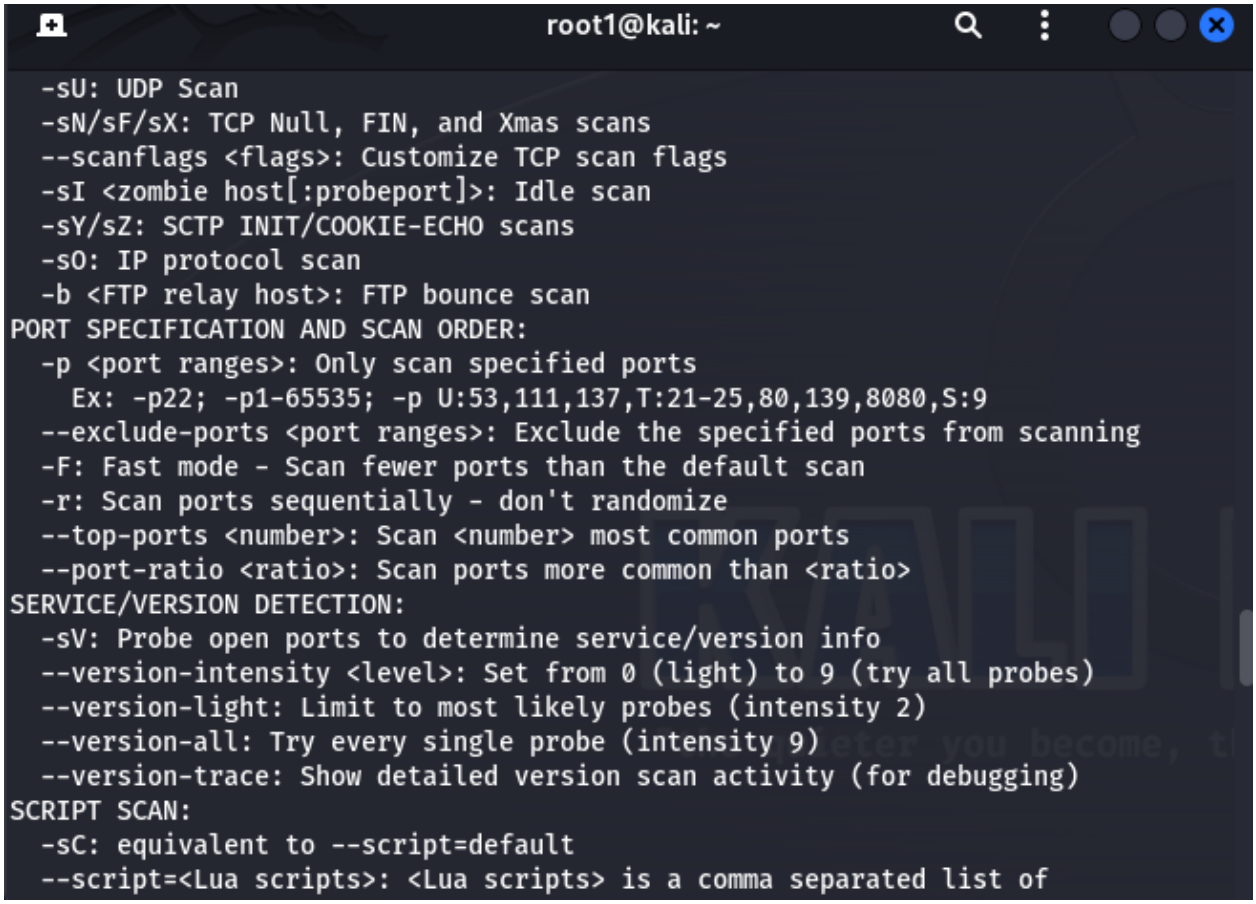
Practical No. 02 - Implement Network Scanning

a. Using Nmap command
b. Using nmap Tool
c. Using window cmd
d. Using Kali Linux For DNS
e. Using who.is
f. Using Kali Linux for netstat
g. Using Hping 3

A. Using Nmap command

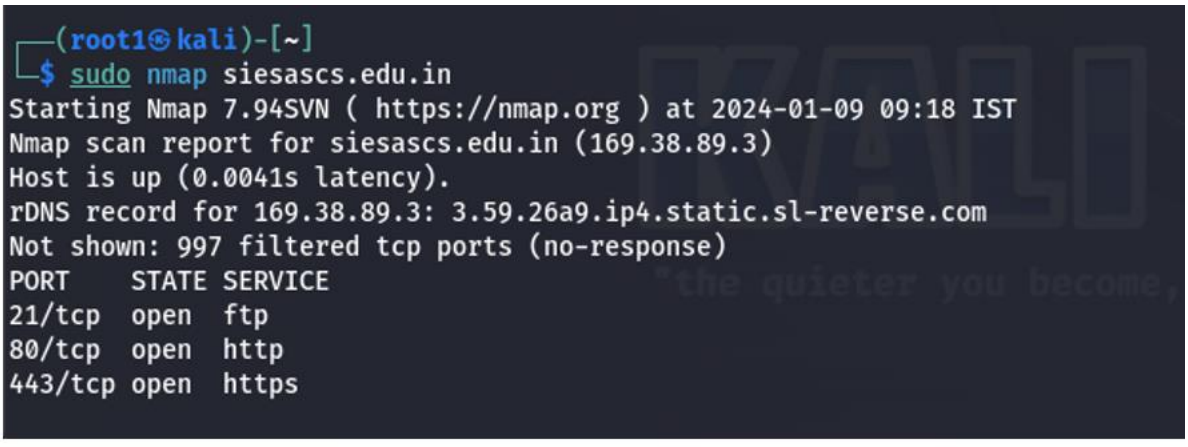
Step 1: Open Kali Linux
Step 2: Goto terminal
Write a Command
$ nmap -h
Nmap is the name of scanning tool & h stands for *"help"*





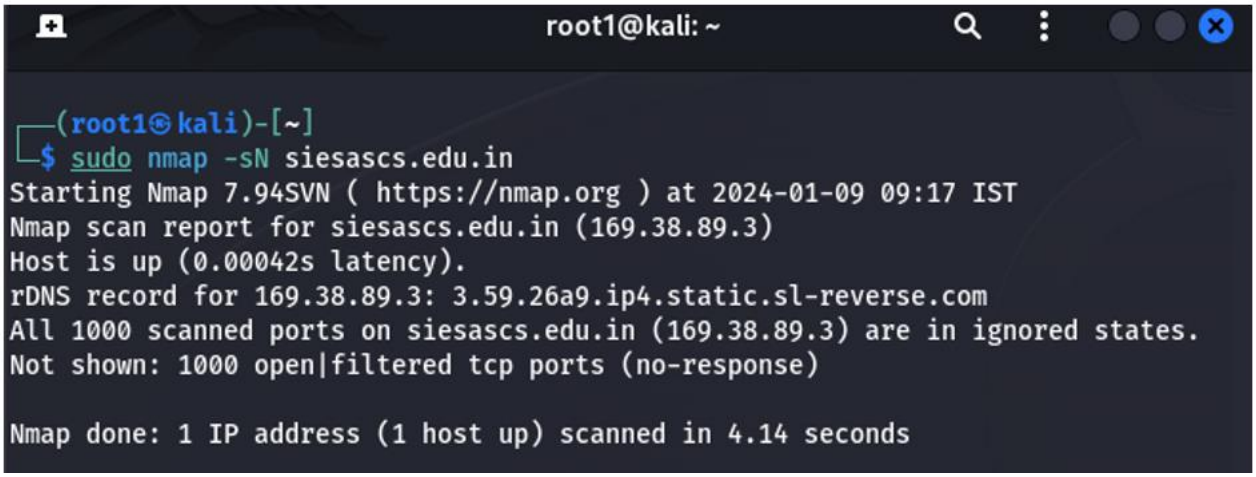
Step 3: Perform a simple scan for the target organization by writing IP address or host name

$ sudo nmap siesascs.edu.in



Step 4: Perform a TCP Null, FIN and XMAS scanning for the target organization by writing IP address or host name

$ sudo nmap -sN siesascs.edu.in

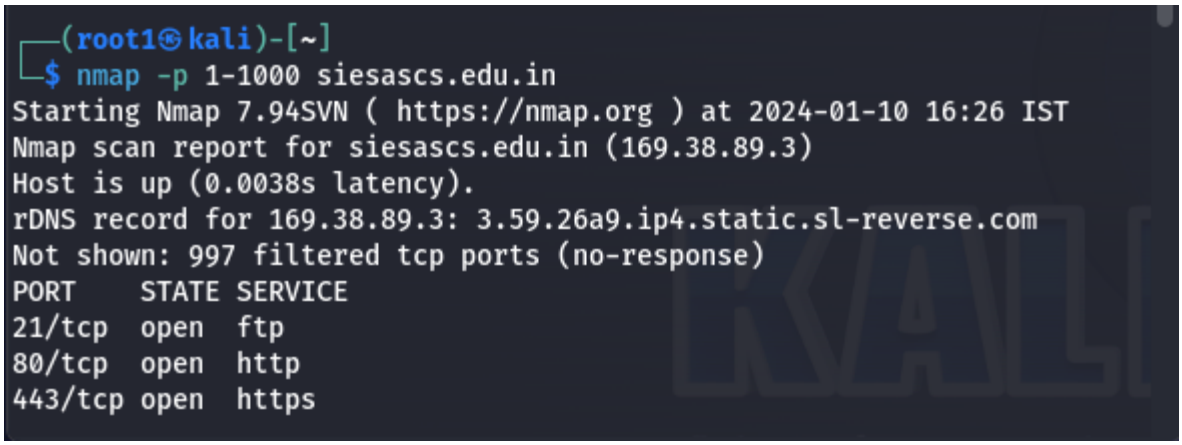


Step 5: Perform a port scanning for the target organization by writing IP address or host name

$ nmap -p 1-1000 siesascs.edu.in

-p: ports

1-1000: 1 to 1000 port will be scanned



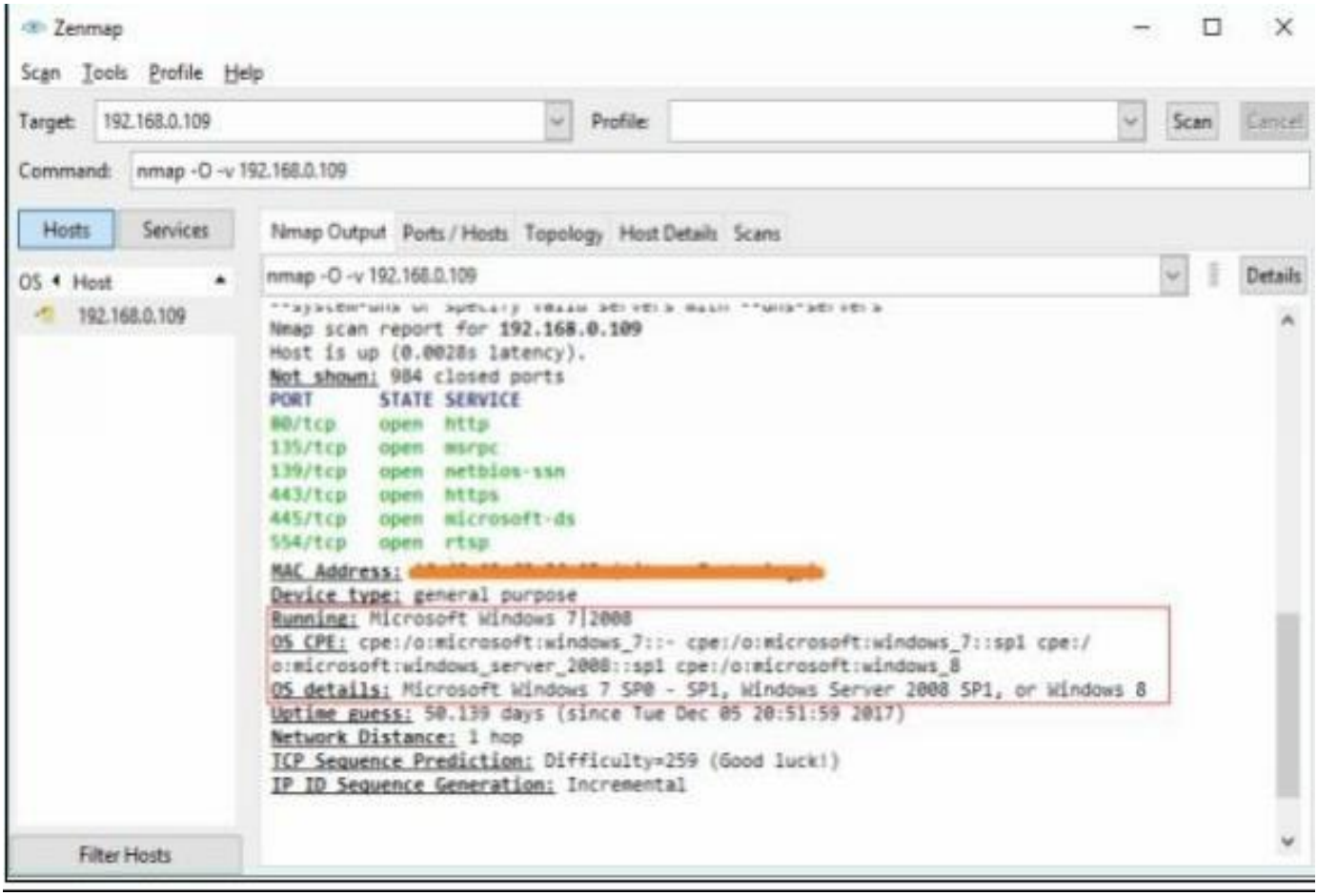
B. Using Nmap Tool

Step 1: Open Nmap tool in windows

Step 2: Write a target ip address

Step 3: Select a scanning type from drop down list

Step 4: Click on scan



C. Using Window cmd

Step 1: Check IP address of the machine

>ipconfig

```
C:\Users\sies>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d4e8:f697:7374:4c2b%12
   IPv4 Address. . . . . . . . . . . : 192.168.11.120
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 192.168.10.2

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::757f:28d1:5b9:1ac4%13
   IPv4 Address. . . . . . . . . . . : 192.168.199.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ce4:5605:48a3:f98%6
   IPv4 Address. . . . . . . . . . . : 192.168.127.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Step 2: Check network status of the machine

>netstat

```
C:\Users\sies>hostname
DESKTOP-NUJUK7F

C:\Users\sies>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49685        DESKTOP-NUJUK7F:49686  ESTABLISHED
  TCP    127.0.0.1:49686        DESKTOP-NUJUK7F:49685  ESTABLISHED
  TCP    127.0.0.1:49687        DESKTOP-NUJUK7F:49688  ESTABLISHED
  TCP    127.0.0.1:49688        DESKTOP-NUJUK7F:49687  ESTABLISHED
  TCP    127.0.0.1:49763        DESKTOP-NUJUK7F:49764  ESTABLISHED
  TCP    127.0.0.1:49764        DESKTOP-NUJUK7F:49763  ESTABLISHED
  TCP    127.0.0.1:50033        DESKTOP-NUJUK7F:50034  ESTABLISHED
  TCP    127.0.0.1:50034        DESKTOP-NUJUK7F:50033  ESTABLISHED
  TCP    127.0.0.1:56010        DESKTOP-NUJUK7F:56011  ESTABLISHED
  TCP    127.0.0.1:56011        DESKTOP-NUJUK7F:56010  ESTABLISHED
  TCP    127.0.0.1:56281        DESKTOP-NUJUK7F:56282  ESTABLISHED
  TCP    127.0.0.1:56282        DESKTOP-NUJUK7F:56281  ESTABLISHED
  TCP    127.0.0.1:56283        DESKTOP-NUJUK7F:56284  ESTABLISHED
  TCP    127.0.0.1:56284        DESKTOP-NUJUK7F:56283  ESTABLISHED
  TCP    127.0.0.1:56285        DESKTOP-NUJUK7F:56286  ESTABLISHED
  TCP    127.0.0.1:56286        DESKTOP-NUJUK7F:56285  ESTABLISHED
  TCP    127.0.0.1:56287        DESKTOP-NUJUK7F:56288  ESTABLISHED
  TCP    127.0.0.1:56288        DESKTOP-NUJUK7F:56287  ESTABLISHED
  TCP    127.0.0.1:56289        DESKTOP-NUJUK7F:56290  ESTABLISHED
  TCP    127.0.0.1:56290        DESKTOP-NUJUK7F:56289  ESTABLISHED
  TCP    127.0.0.1:56291        DESKTOP-NUJUK7F:56292  ESTABLISHED
  TCP    127.0.0.1:56292        DESKTOP-NUJUK7F:56291  ESTABLISHED
  TCP    127.0.0.1:56293        DESKTOP-NUJUK7F:56294  ESTABLISHED
  TCP    127.0.0.1:56294        DESKTOP-NUJUK7F:56293  ESTABLISHED
  TCP    127.0.0.1:56295        DESKTOP-NUJUK7F:56296  ESTABLISHED
  TCP    127.0.0.1:56296        DESKTOP-NUJUK7F:56295  ESTABLISHED
  TCP    127.0.0.1:56297        DESKTOP-NUJUK7F:56298  ESTABLISHED
  TCP    127.0.0.1:56298        DESKTOP-NUJUK7F:56297  ESTABLISHED
  TCP    127.0.0.1:56299        DESKTOP-NUJUK7F:56300  ESTABLISHED
  TCP    127.0.0.1:56300        DESKTOP-NUJUK7F:56299  ESTABLISHED
  TCP    127.0.0.1:56301        DESKTOP-NUJUK7F:56302  ESTABLISHED
  TCP    127.0.0.1:56302        DESKTOP-NUJUK7F:56301  ESTABLISHED
  TCP    127.0.0.1:56303        DESKTOP-NUJUK7F:56304  ESTABLISHED
  TCP    127.0.0.1:56304        DESKTOP-NUJUK7F:56303  ESTABLISHED
  TCP    127.0.0.1:56305        DESKTOP-NUJUK7F:56306  ESTABLISHED
  TCP    127.0.0.1:56306        DESKTOP-NUJUK7F:56305  ESTABLISHED
  TCP    127.0.0.1:56307        DESKTOP-NUJUK7F:56308  ESTABLISHED
  TCP    127.0.0.1:56308        DESKTOP-NUJUK7F:56307  ESTABLISHED
  TCP    127.0.0.1:56309        DESKTOP-NUJUK7F:56310  ESTABLISHED
  TCP    127.0.0.1:56310        DESKTOP-NUJUK7F:56309  ESTABLISHED
  TCP    127.0.0.1:56311        DESKTOP-NUJUK7F:56312  ESTABLISHED
```

Step 3: Check network status of the machine
>netstat -aon

```
C:\Users\sies>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1272
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       4900
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       4900
  TCP    0.0.0.0:1158           0.0.0.0:0              LISTENING       11832
  TCP    0.0.0.0:1521           0.0.0.0:0              LISTENING       3972
  TCP    0.0.0.0:1831           0.0.0.0:0              LISTENING       9384
  TCP    0.0.0.0:1832           0.0.0.0:0              LISTENING       9540
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       5440
  TCP    0.0.0.0:3938           0.0.0.0:0              LISTENING       7428
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       8380
  TCP    0.0.0.0:5501           0.0.0.0:0              LISTENING       7800
  TCP    0.0.0.0:5502           0.0.0.0:0              LISTENING       3076
  TCP    0.0.0.0:5520           0.0.0.0:0              LISTENING       11832
  TCP    0.0.0.0:5522           0.0.0.0:0              LISTENING       7800
  TCP    0.0.0.0:5523           0.0.0.0:0              LISTENING       3076
  TCP    0.0.0.0:23232          0.0.0.0:0              LISTENING       15624
  TCP    0.0.0.0:33060          0.0.0.0:0              LISTENING       5440
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       996
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       696
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1620
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2324
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3268
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING       3828
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING       4012
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING       4020
  TCP    0.0.0.0:49675          0.0.0.0:0              LISTENING       3984
  TCP    0.0.0.0:49676          0.0.0.0:0              LISTENING       3996
```

Step 3: Check complete system information of the machine
>systeminfo

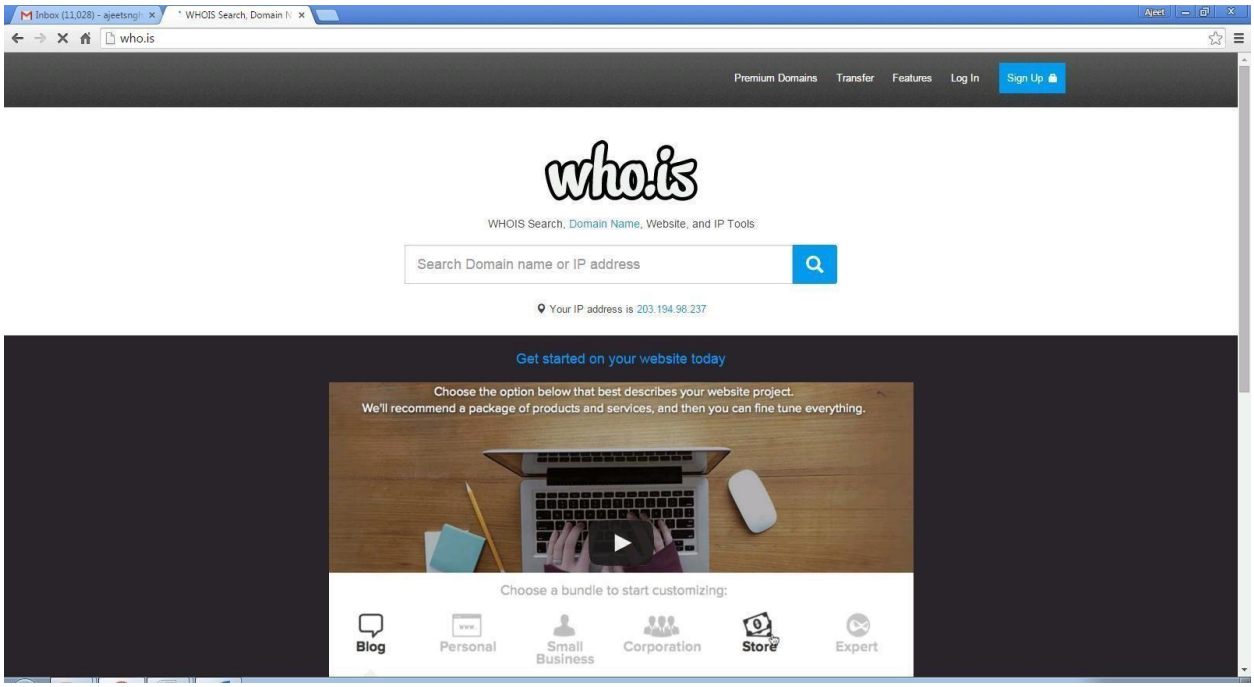
```
Microsoft Windows [Version 10.0.22621.525]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sies>systeminfo

Host Name:                 DESKTOP-NUJUK7F
OS Name:                   Microsoft Windows 11 Pro
OS Version:                10.0.22621 N/A Build 22621
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          sies
Registered Organization:
Product ID:                00331-20210-00000-AA302
Original Install Date:     17-08-2023, 13:04:53
System Boot Time:          05-09-2023, 15:23:32
System Manufacturer:       Dell Inc.
System Model:              OptiPlex 3090
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 165 Stepping 3 GenuineIntel ~3701 Mhz
BIOS Version:              Dell Inc. 2.0.7, 25-11-2021
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     7,904 MB
Available Physical Memory: 1,543 MB
Virtual Memory: Max Size:  12,768 MB
Virtual Memory: Available: 2,190 MB
Virtual Memory: In Use:    10,578 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-NUJUK7F
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB5017026
                           [02]: KB5019311
                           [03]: KB5017233
Network Card(s):           3 NIC(s) Installed.
                           [01]: Realtek PCIe GbE Family Controller
                                 Connection Name: Ethernet
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.10.2
                                 IP address(es)
                                 [01]: 192.168.11.120
                                 [02]: fe80::d4e8:f697:7374:4c2b
                           [02]: VMware Virtual Ethernet Adapter for VMnet1
                                 Connection Name: Ethernet 3
                                 DHCP Enabled:    No
```

D. Using Kali Linux for DNS

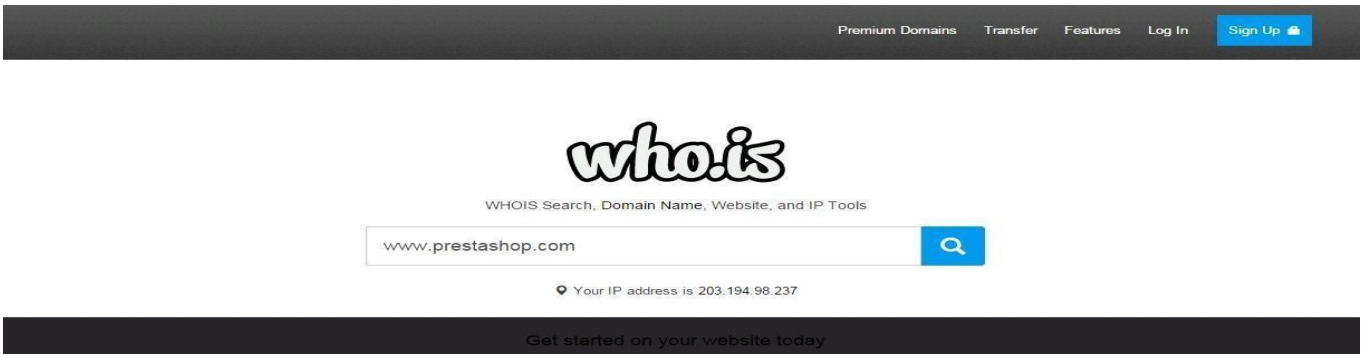
```
root1@kali: ~

┌──(root1㉿kali)-[~]
└─$ sudo nslookup
> siesascs.edu.in
Server:         192.168.40.2
Address:        192.168.40.2#53

Non-authoritative answer:
Name:   siesascs.edu.in
Address: 169.38.89.3
>
zsh: suspended  sudo nslookup
```

E. Using Who.is

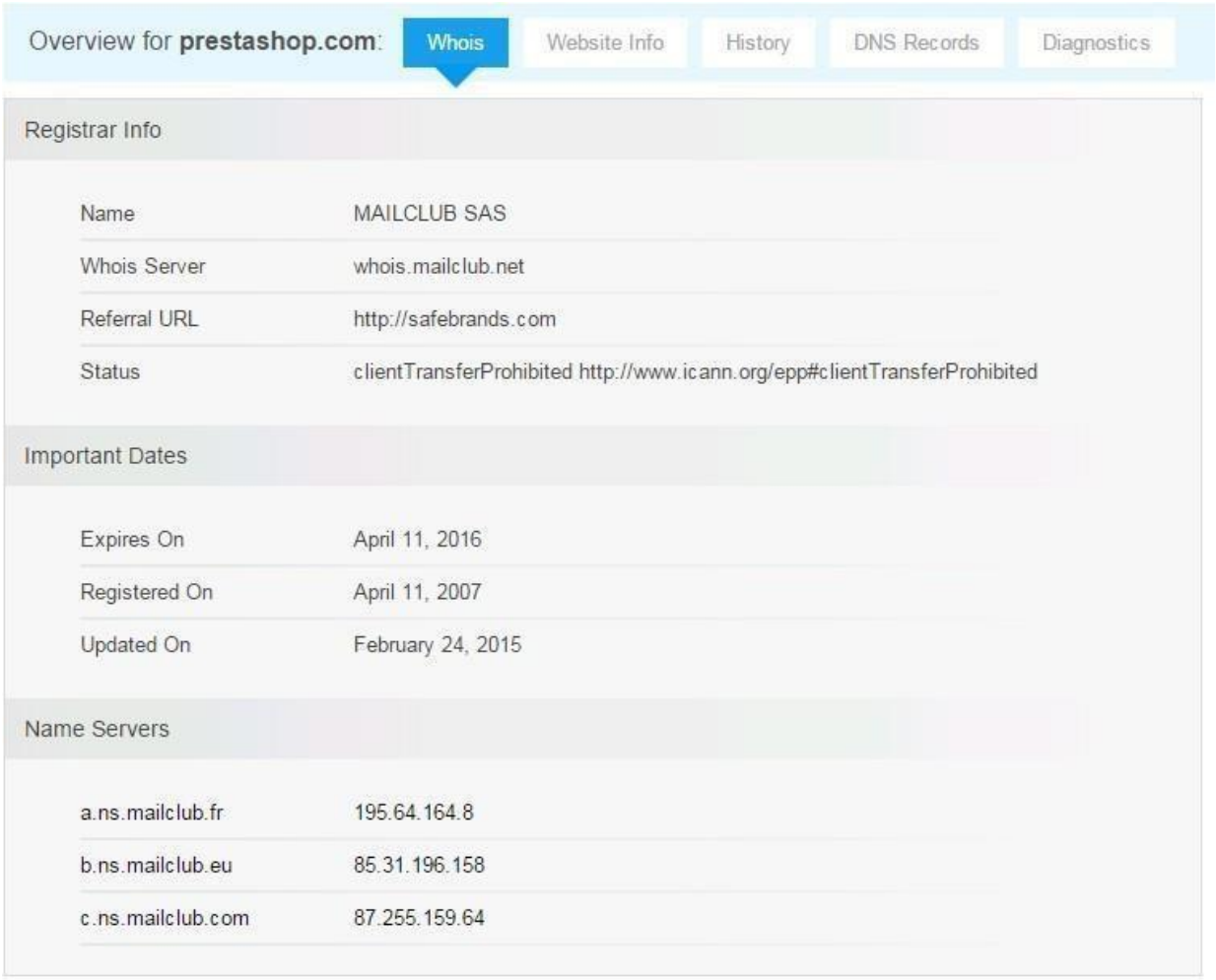
Step1: Open the WHO.is website



Step 2: Enter the website name and hit the “Enter button”.



Step 3: Show you information about www.prestashop.com



Raw Registrar Data

```
Domain Name: PRESTASHOP.COM
Registry Domain ID: 920363578_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.mailclub.net
Registrar URL: http://www.mailclub.fr
Updated Date: 2015-02-24T05:43:34Z
Creation Date: 2007-04-11T08:59:05Z
Registrar Registration Expiration Date: 2016-04-11T08:59:05Z
Registrar: Mailclub SAS
Registrar IANA ID: 1290
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: NOMS DE DOMAINE Responsable
Registrant Organization: PRESTASHOP
Registrant Street: 12, rue d'Amsterdam
Registrant City: Paris
Registrant State/Province:
Registrant Postal Code: 75009
Registrant Country: FR
Registrant Phone: +33.140183004
Registrant Phone Ext:
Registrant Fax: +33.972111878
Registrant Fax Ext:
Registrant Email: domains@prestashop.com
Registry Admin ID:
Admin Name: NOMS DE DOMAINE Responsable
Admin Organization: PRESTASHOP
Admin Street: 12, rue d'Amsterdam
Admin City: Paris
Admin State/Province:
Admin Postal Code: 75009
Admin Country: FR
Admin Phone: +33.140183004
Admin Phone Ext:
Admin Fax: +33.972111878
Admin Fax Ext:
Admin Email: domains@prestashop.com
Registry Tech ID:
Tech Name: TINE, Charles
Tech Organization: MAILCLUB S.A.S.
Tech Street: Pole Media de la Belle de Mai 37 rue Guibal
Tech City: Marseille
Tech State/Province:
```

F. Using Kali Linux for netstat

Step 1: Check ip address

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.40.130  netmask 255.255.255.0  broadcast 192.168.40.255
        inet6 fe80::20c:29ff:fe2d:f8d3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:2d:f8:d3  txqueuelen 1000  (Ethernet)
        RX packets 51  bytes 4904 (4.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 65  bytes 8657 (8.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 2: Check network status for all

$ sudo netstat -a

```
┌──(root1㉿kali)-[~]
└─$ sudo netstat -a
[sudo] password for root1:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6       0      0 [::]:1716               [::]:*                  LISTEN
udp        0      0 kali:bootpc             192.168.40.254:bootps   ESTABLISHED
udp6       0      0 [::]:1716               [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     29290
unix  3      [ ]         STREAM     CONNECTED     27575    /run/dbus/system_bus_s
ocket
unix  2      [ ]         DGRAM                    24611
unix  3      [ ]         STREAM     CONNECTED     30906    /run/dbus/system_bus_s
ocket
unix  3      [ ]         STREAM     CONNECTED     30064    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     30016
unix  3      [ ]         STREAM     CONNECTED     29783
unix  3      [ ]         STREAM     CONNECTED     29740    /run/systemd/journal/s
tdout
unix  3      [ ]         STREAM     CONNECTED     29444    /run/systemd/journal/s
```

Step 3: Check groups

$ netstat -g

```
┌──(root1㉿kali)-[~]
└─$ netstat -g
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      all-systems.mcast.net
eth0            1      all-systems.mcast.net
lo              1      ip6-allnodes
lo              1      ff01::1
eth0            1      ff02::1:ff2d:f8d3
eth0            1      ip6-allnodes
eth0            1      ff01::1

┌──(root1㉿kali)-[~]
└─$
```

Step 4: Check interface

$ netstat -i

```
┌──(root1㉿kali)-[~]
└─$ netstat -i
Kernel Interface table
Iface             MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR
 Flg
eth0             1500       46      0      0 0             60      0      0      0
 BMRU
lo              65536       24      0      0 0             24      0      0      0
 LRU

┌──(root1㉿kali)-[~]
└─$
```

Step 5: Check routing information

$ netstat -r

```
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 eth0
192.168.40.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0

┌──(root1㉿kali)-[~]
└─$
```

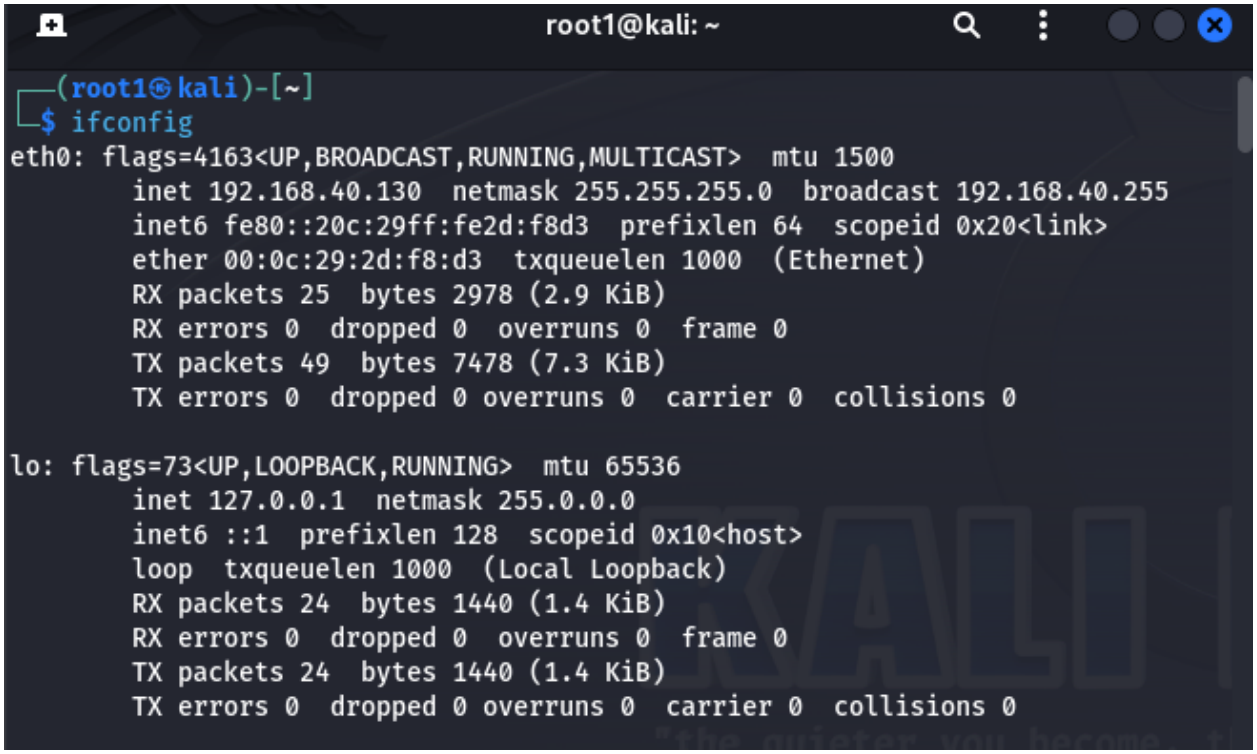
Step 6: For Help

$ netstat -h

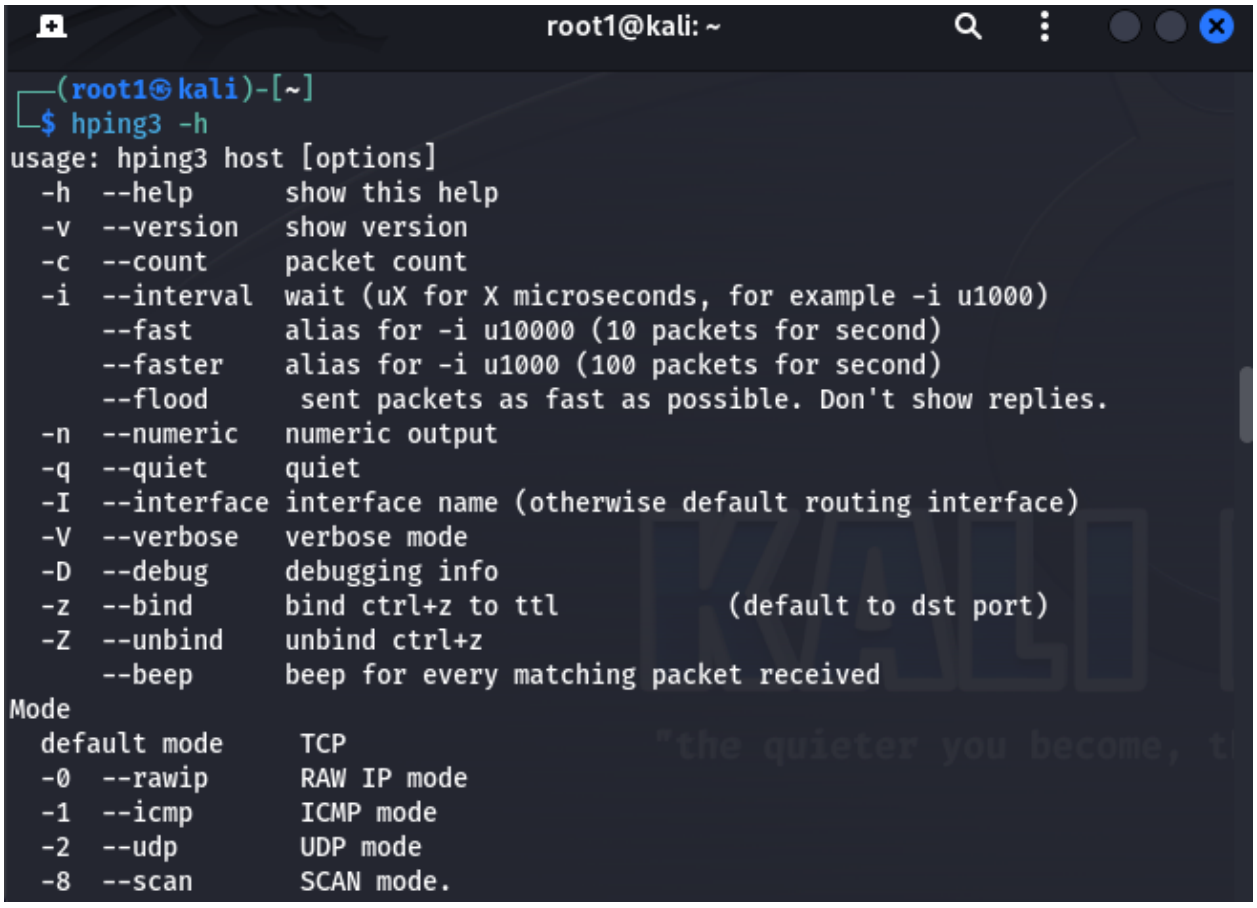
```
┌──(root1㉿kali)-[~]
└─$ netstat -h
usage: netstat [-vWeenNcCF] [<Af>] -r         netstat {-V|--version|-h|--help}
       netstat [-vWnNcaeol] [<Socket> ...]
       netstat { [-vWeenNac] -i | [-cnNe] -M | -s [-6tuw] }

        -r, --route              display routing table
        -i, --interfaces         display interface table
        -g, --groups             display multicast group memberships
        -s, --statistics         display networking statistics (like SNMP)
        -M, --masquerade         display masqueraded connections

        -v, --verbose            be verbose
        -W, --wide               don't truncate IP addresses
        -n, --numeric            don't resolve names
        --numeric-hosts          don't resolve host names
        --numeric-ports          don't resolve port names
        --numeric-users          don't resolve user names
        -N, --symbolic           resolve hardware names
        -e, --extend             display other/more information
        -p, --programs           display PID/Program name for sockets
        -o, --timers             display timers
```

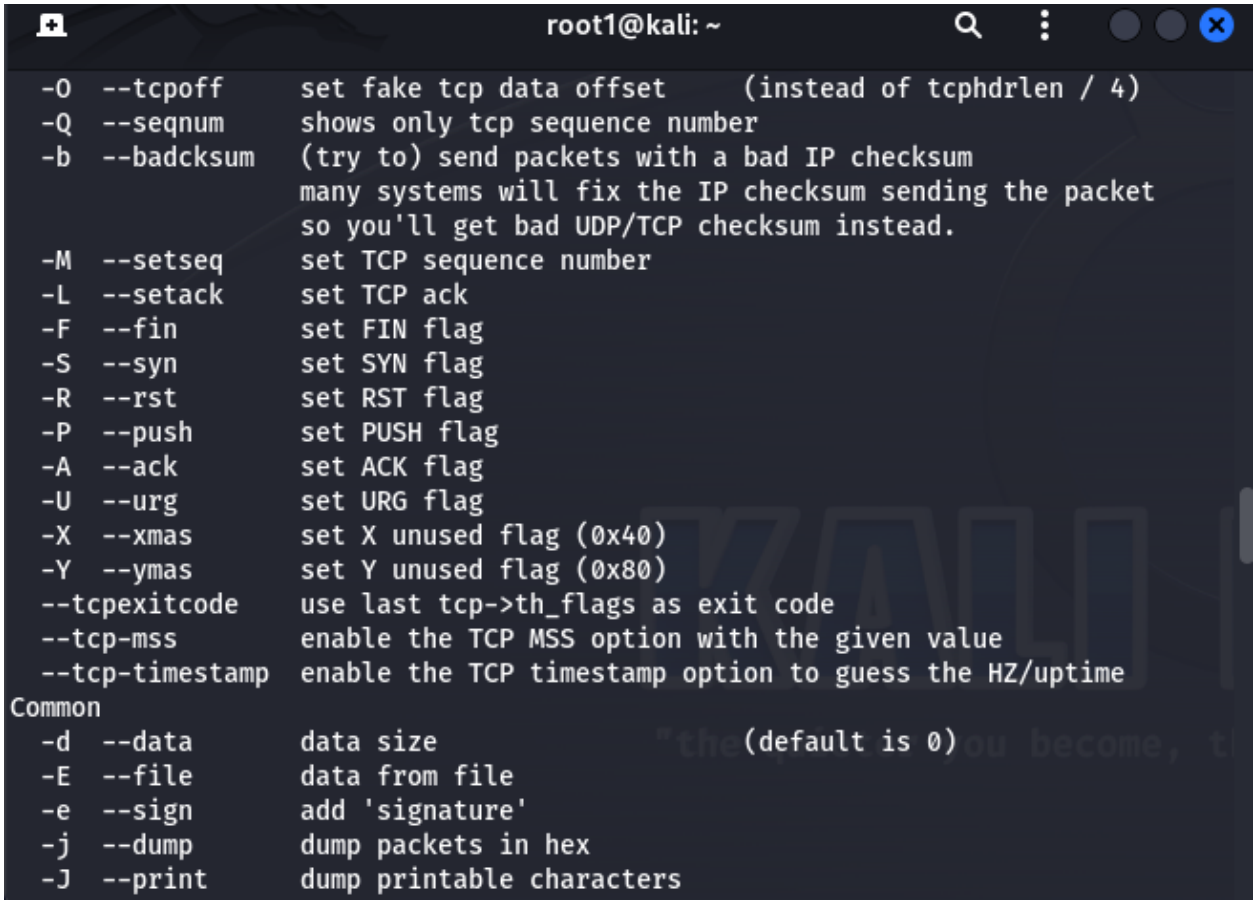
G. Using Hping 3

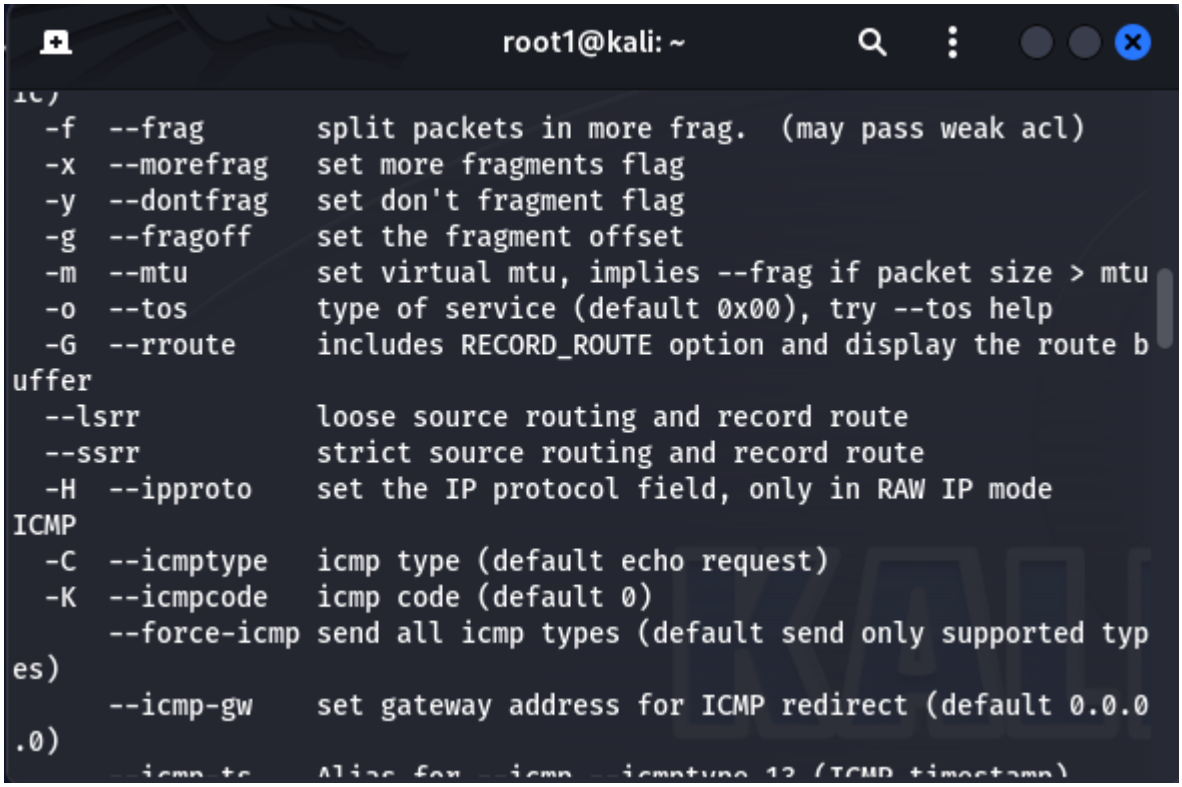
Step 1: Check ipaddress



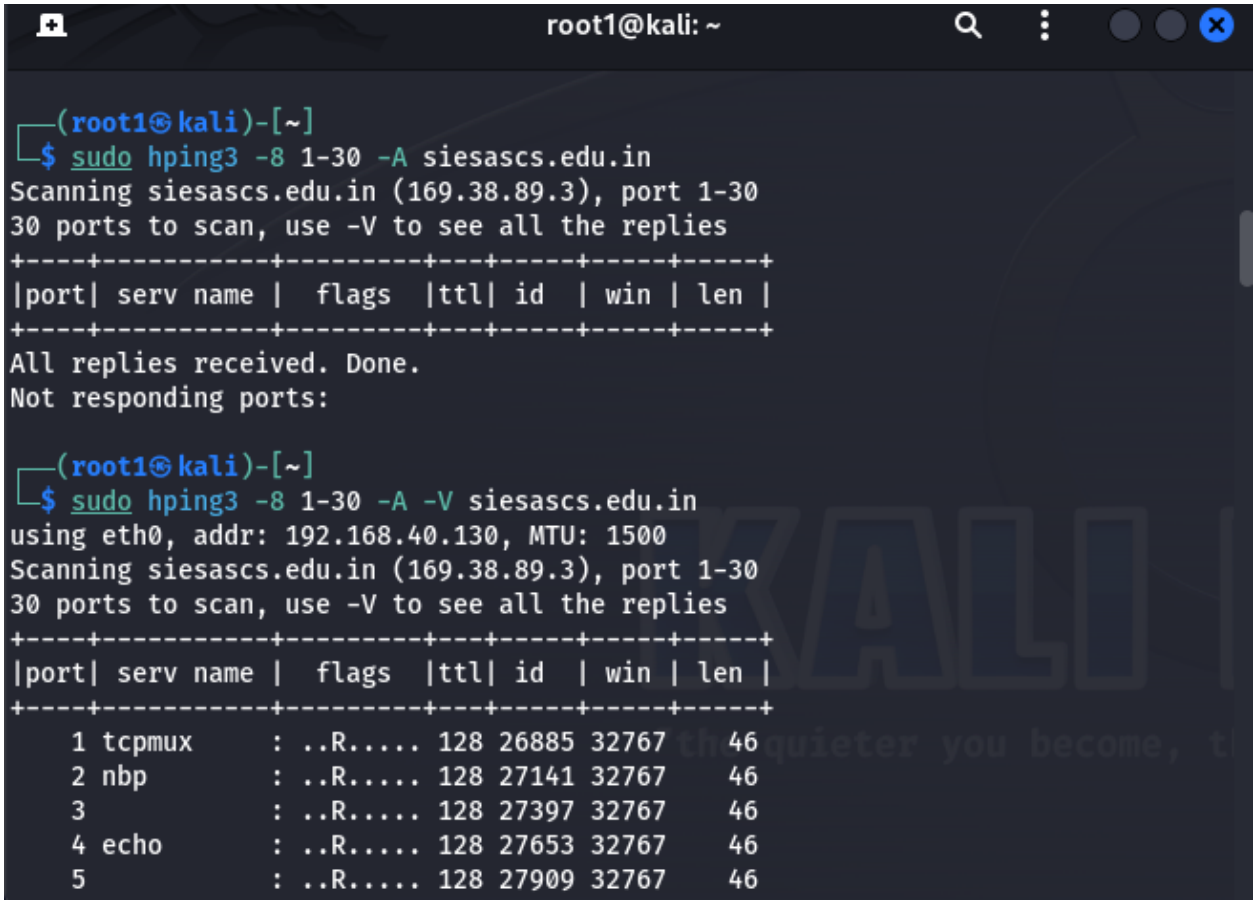
Step 2: Check different operation that can be performed by hping 3



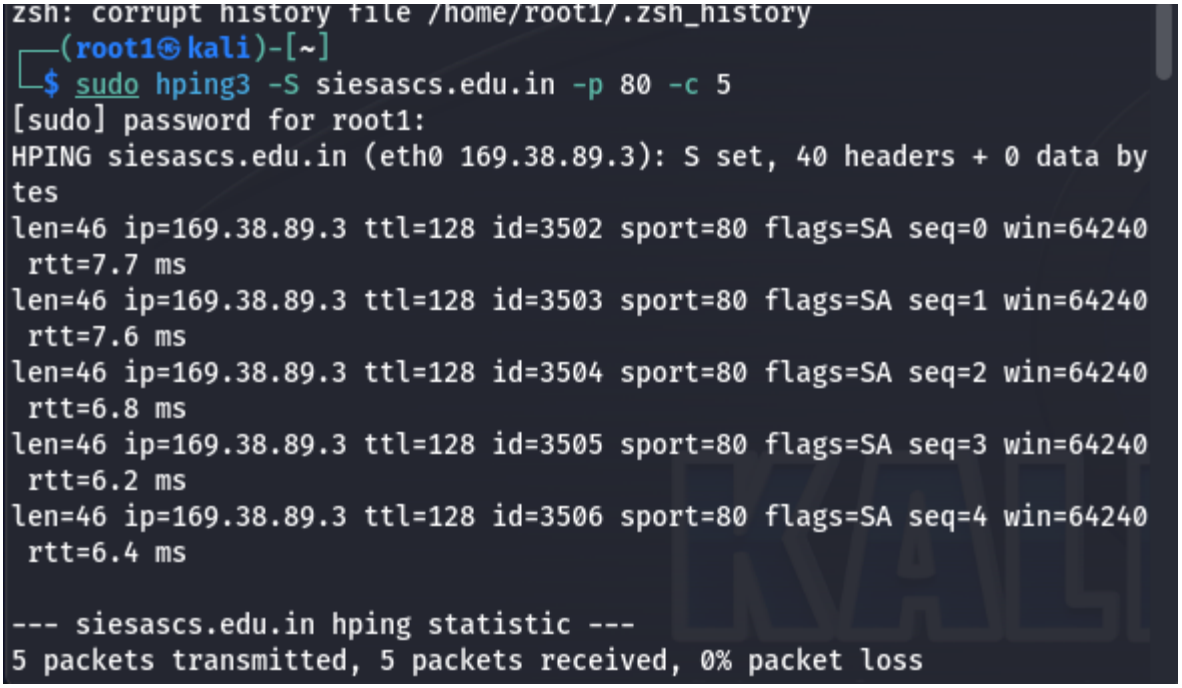




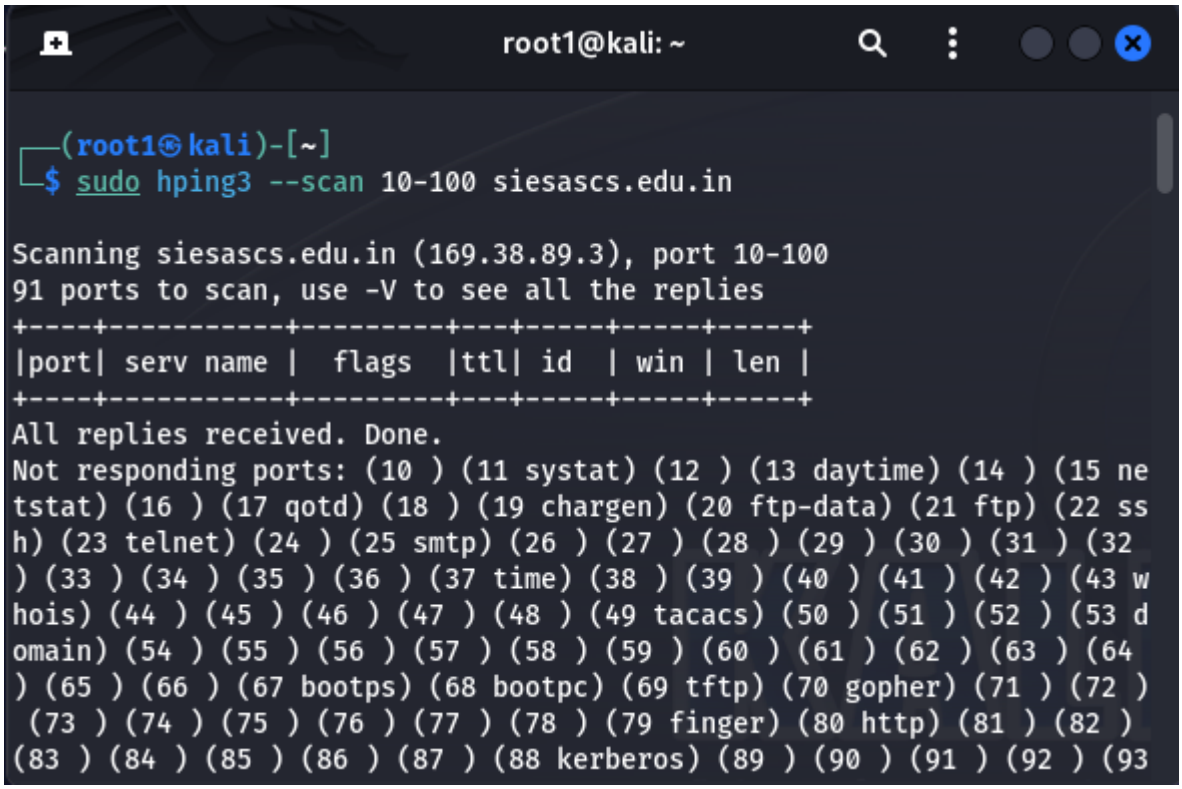
Step 3: Scan 1 to 30 ports of the target system

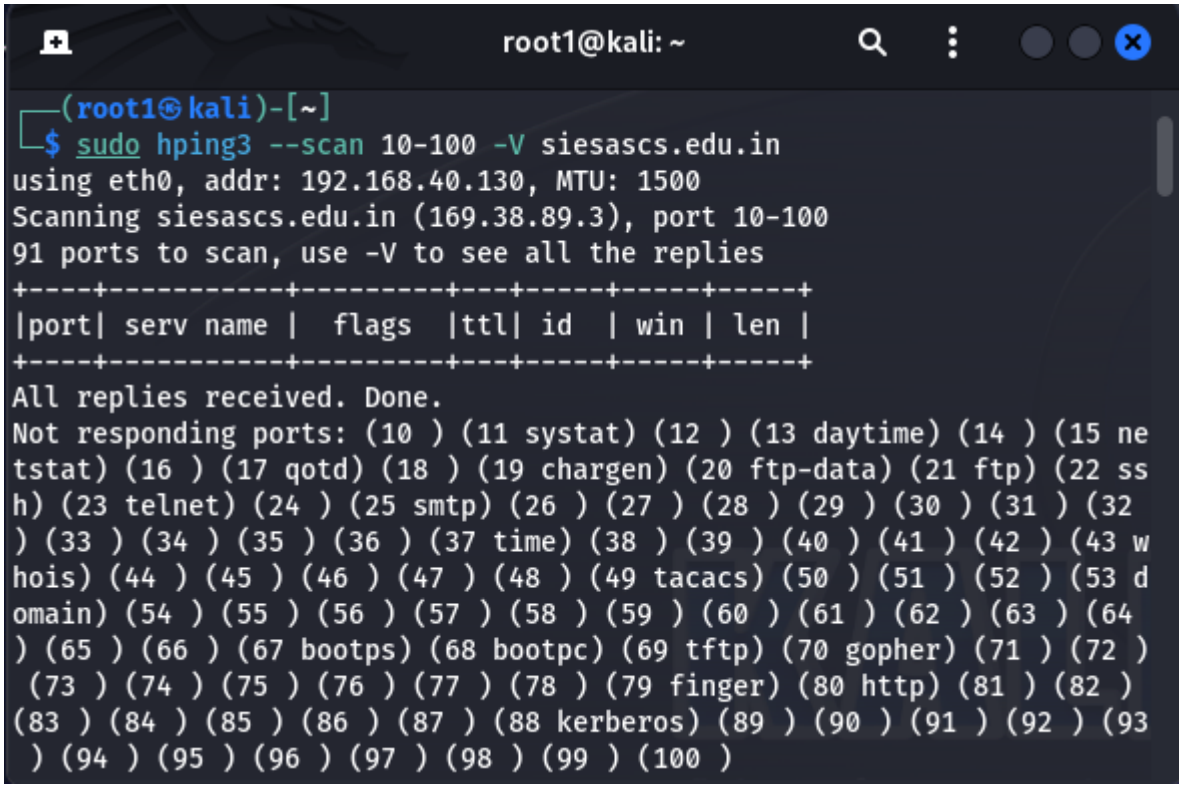


Step 4: Craft your own packet & sent it to attacker



Step 5: Scan 100 ports of the target system





Step 6: Craft your own packet & time to live

```
┌──(root1㉿kali)-[~]
└─$ sudo hping3 -c 1 -S -p 80 --win 514 --ttl 60 siesascs.edu.in
HPING siesascs.edu.in (eth0 169.38.89.3): S set, 40 headers + 0 data by
tes
len=46 ip=169.38.89.3 ttl=128 id=4302 sport=80 flags=SA seq=0 win=64240
 rtt=12.5 ms

--- siesascs.edu.in hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.5/12.5/12.5 ms
```

Step 7: Scan port number 4444

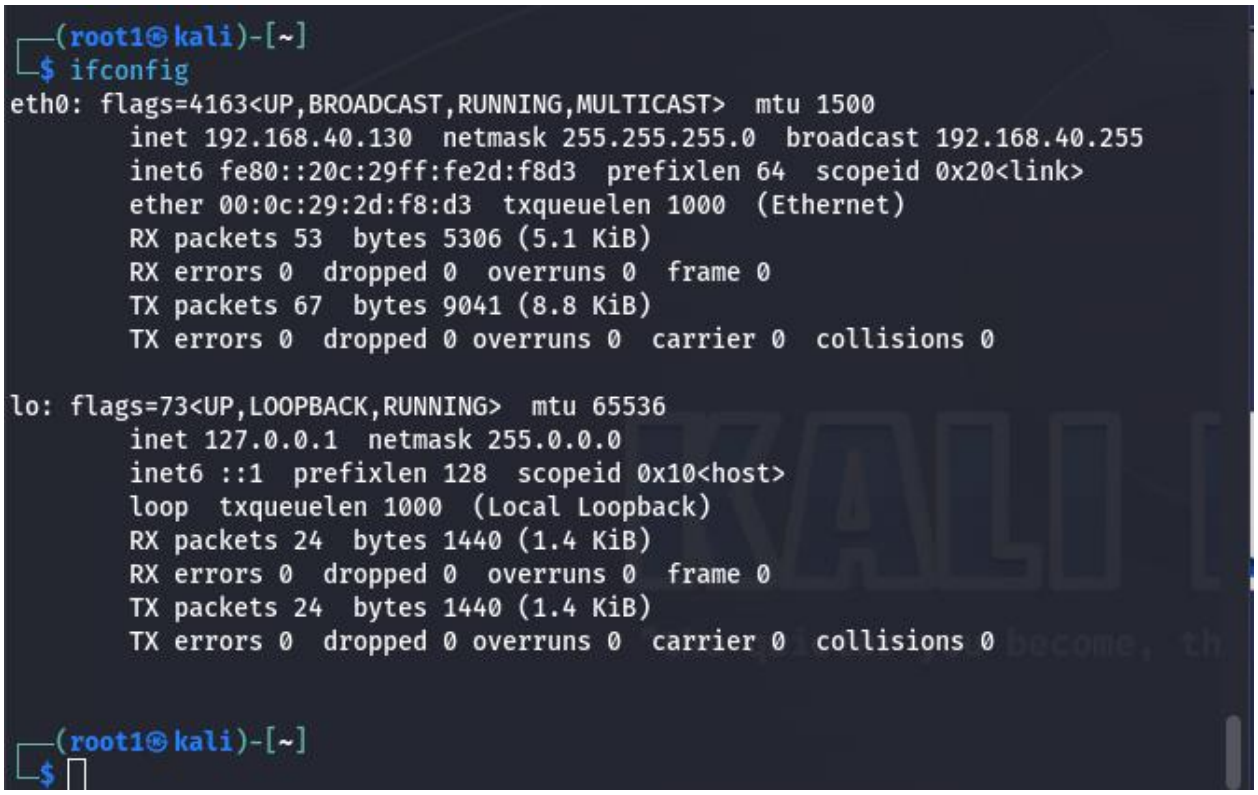
```
root1@kali: ~
┌──(root1㉿kali)-[~]
└─$ sudo hping3 -S -p 4444 siesascs.edu.in
HPING siesascs.edu.in (eth0 169.38.89.3): S set, 40 headers + 0 data by
tes
len=46 ip=169.38.89.3 ttl=128 id=4304 sport=4444 flags=RA seq=0 win=642
40 rtt=21047.5 ms
len=46 ip=169.38.89.3 ttl=128 id=4305 sport=4444 flags=RA seq=1 win=642
40 rtt=21047.2 ms
len=46 ip=169.38.89.3 ttl=128 id=4306 sport=4444 flags=RA seq=2 win=642
40 rtt=21051.2 ms
len=46 ip=169.38.89.3 ttl=128 id=4307 sport=4444 flags=RA seq=3 win=642
40 rtt=21050.5 ms
len=46 ip=169.38.89.3 ttl=128 id=4308 sport=4444 flags=RA seq=4 win=642
40 rtt=21042.1 ms
len=46 ip=169.38.89.3 ttl=128 id=4309 sport=4444 flags=RA seq=5 win=642
40 rtt=21041.6 ms
len=46 ip=169.38.89.3 ttl=128 id=4310 sport=4444 flags=RA seq=6 win=642
40 rtt=21049.4 ms
len=46 ip=169.38.89.3 ttl=128 id=4311 sport=4444 flags=RA seq=7 win=642
```

Practical No. 03 - Implement NET-BIOS Enumeration

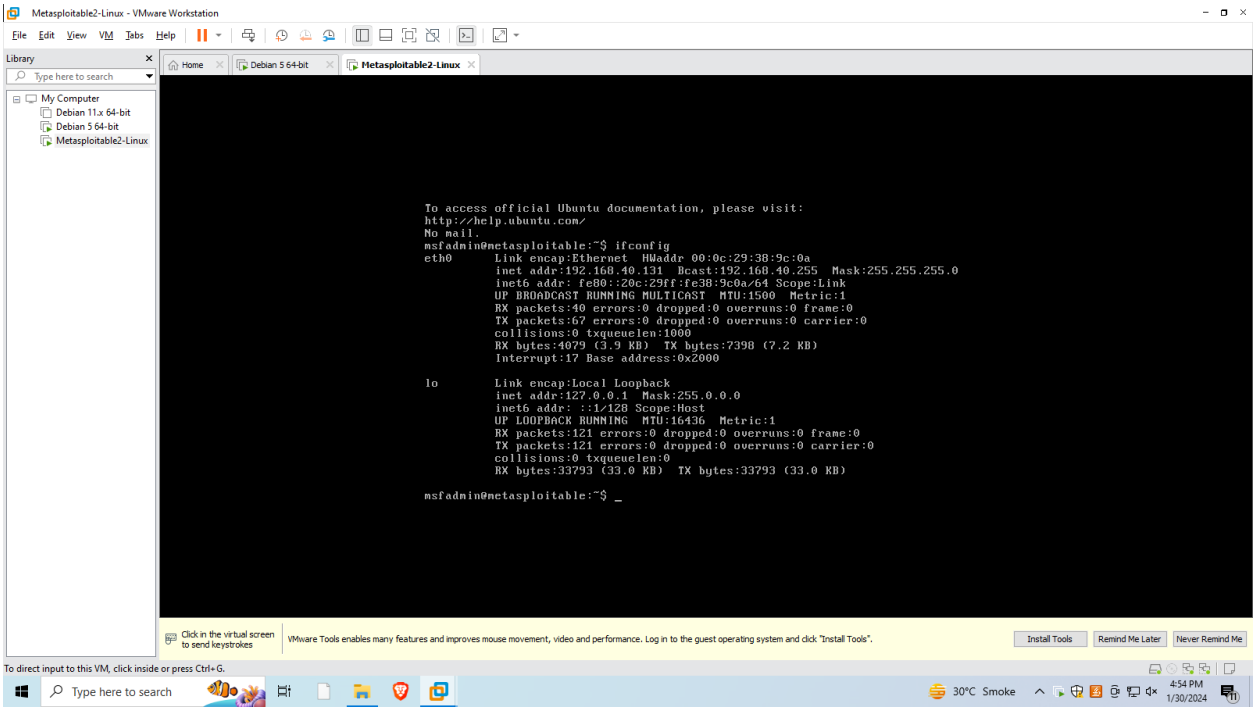
a. Using NBT Scan

Step 1: Open Kali Linux
Step 2: Open terminal check IP address

$ifconfig

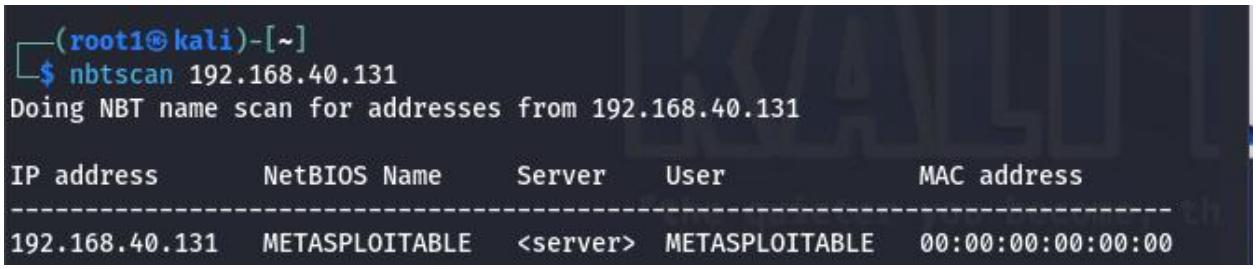


Step 3: Open Metasploit VMWare
Step 4: Login using username & password
Step 5: Check IP address of Metasploit
$ifconfig

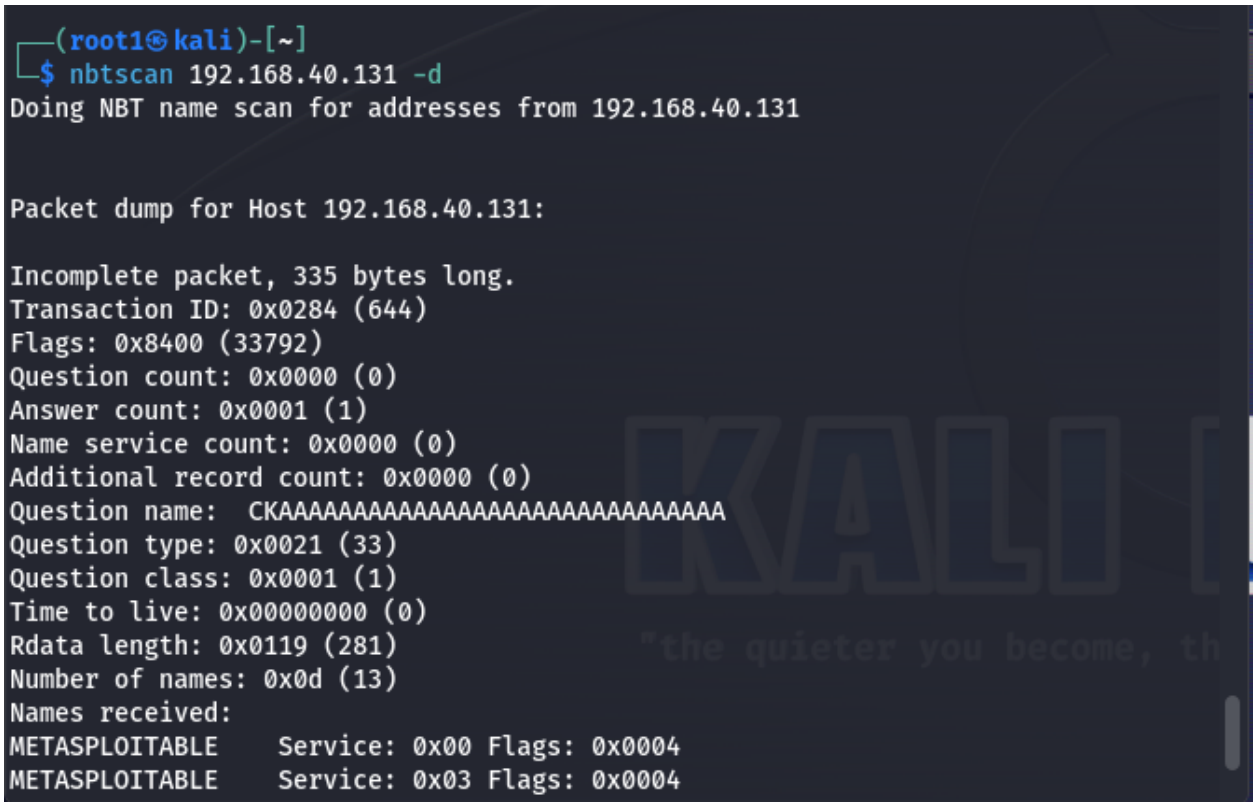


Step 6: Perform enumeration on Metasploit

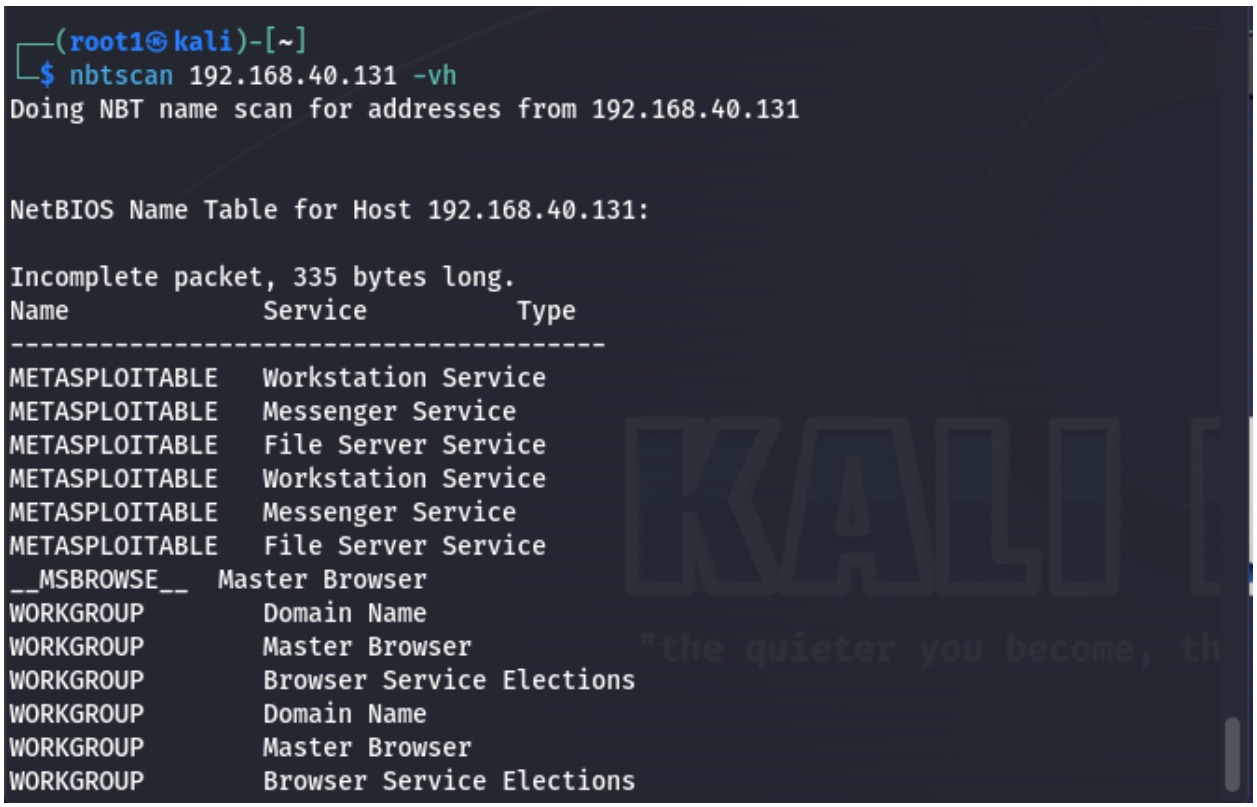
$ nbtscan 192.168.40.131



Step 7: Perform enumeration on Metasploit & dump all the packets
$ nbtscan 192.168.40.131 -d



Step 8: Perform enumeration on Metasploit & check verbose
$ nbtscan 192.168.40.131 -vh



Step 9: Perform enumeration on Metasploit & check verbose
$ nbtscan -h

```
└─$ nbtscan -h
"Human-readable service names" (-h) option cannot be used without verbose (-v) op
tion.
Usage:
nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator]
[-m retransmits] (-f filename)|(<scan_range>)
        -v              verbose output. Print all names received
                        from each host
        -d              dump packets. Print whole packet contents.
        -e              Format output in /etc/hosts format.
        -l              Format output in lmhosts format.
                        Cannot be used with -v, -s or -h options.
        -t timeout      wait timeout milliseconds for response.
                        Default 1000.
        -b bandwidth    Output throttling. Slow down output
                        so that it uses no more that bandwidth bps.
                        Useful on slow links, so that ougoing queries
                        don't get dropped.
        -r              use local port 137 for scans. Win95 boxes
                        respond to this only.
                        You need to be root to use this option on Unix.
        -q              Suppress banners and error messages,
        -s separator    Script-friendly output. Don't print
```

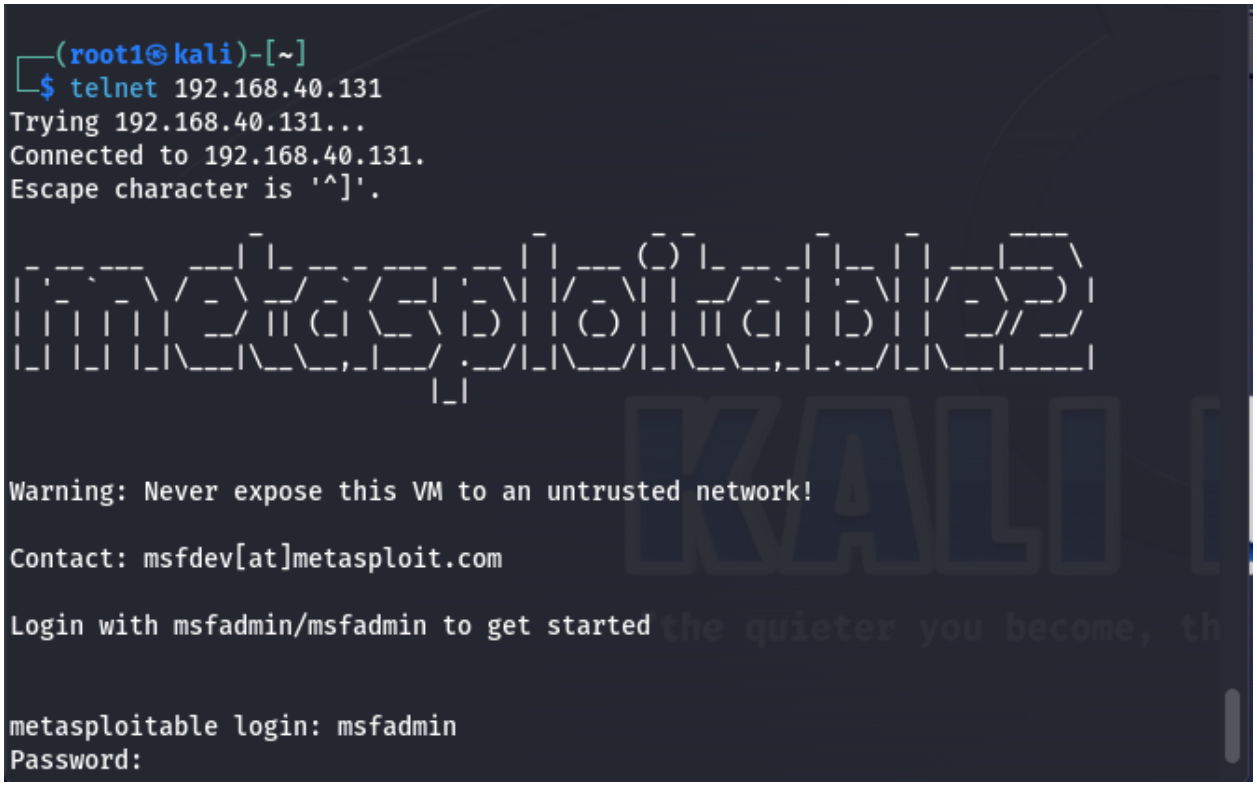
Step 10: Perform enumeration on your own Kali Linux
$ nbtscan 192.168.40.130

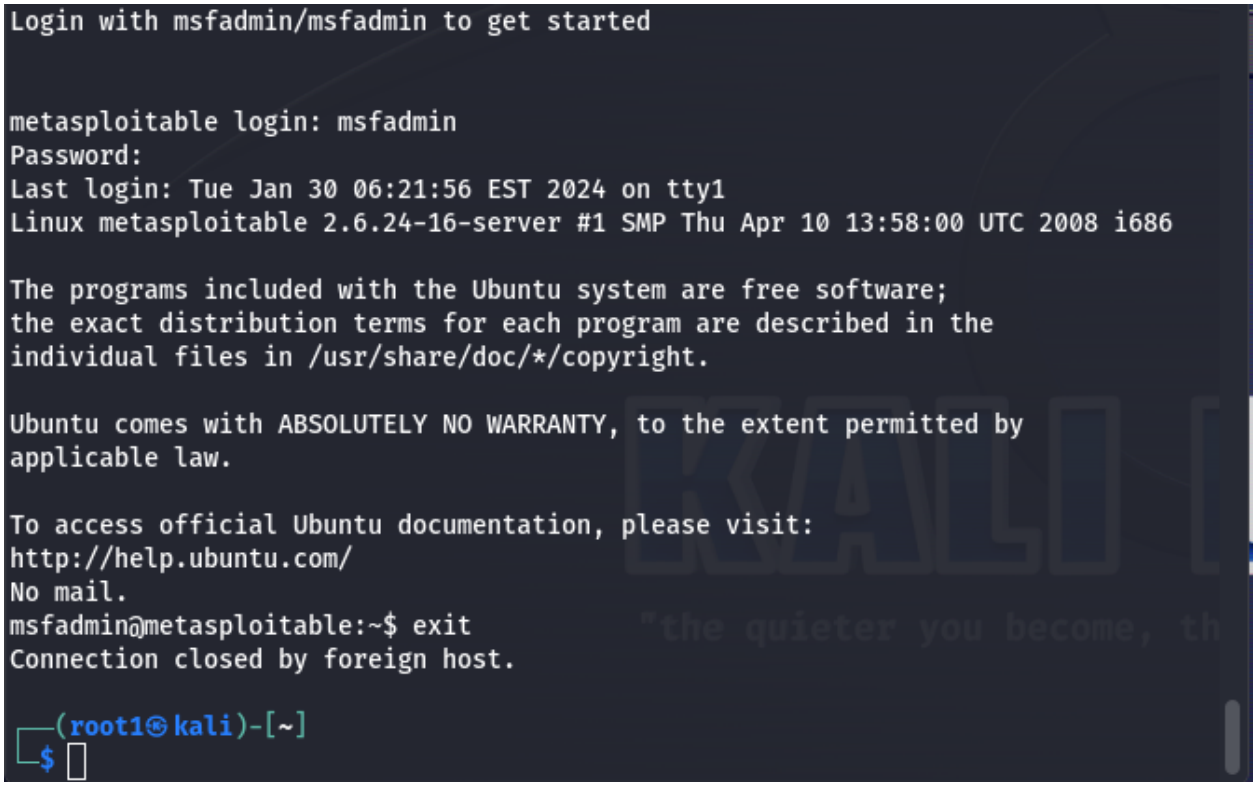
```
┌──(root1㉿kali)-[~]
└─$ nbtscan 192.168.40.130
Doing NBT name scan for addresses from 192.168.40.130

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------

┌──(root1㉿kali)-[~]
└─$
```

Step 11: Perform enumeration on your own Kali Linux
$ nbtscan 192.168.40.130 -vh

```
------------------------------------------------------------------------------

┌──(root1㉿kali)-[~]
└─$ nbtscan 192.168.40.130 -vh
Doing NBT name scan for addresses from 192.168.40.130


┌──(root1㉿kali)-[~]
└─$
```

Step 12: Perform enumeration on telnet
$ telnet 192.168.40.131





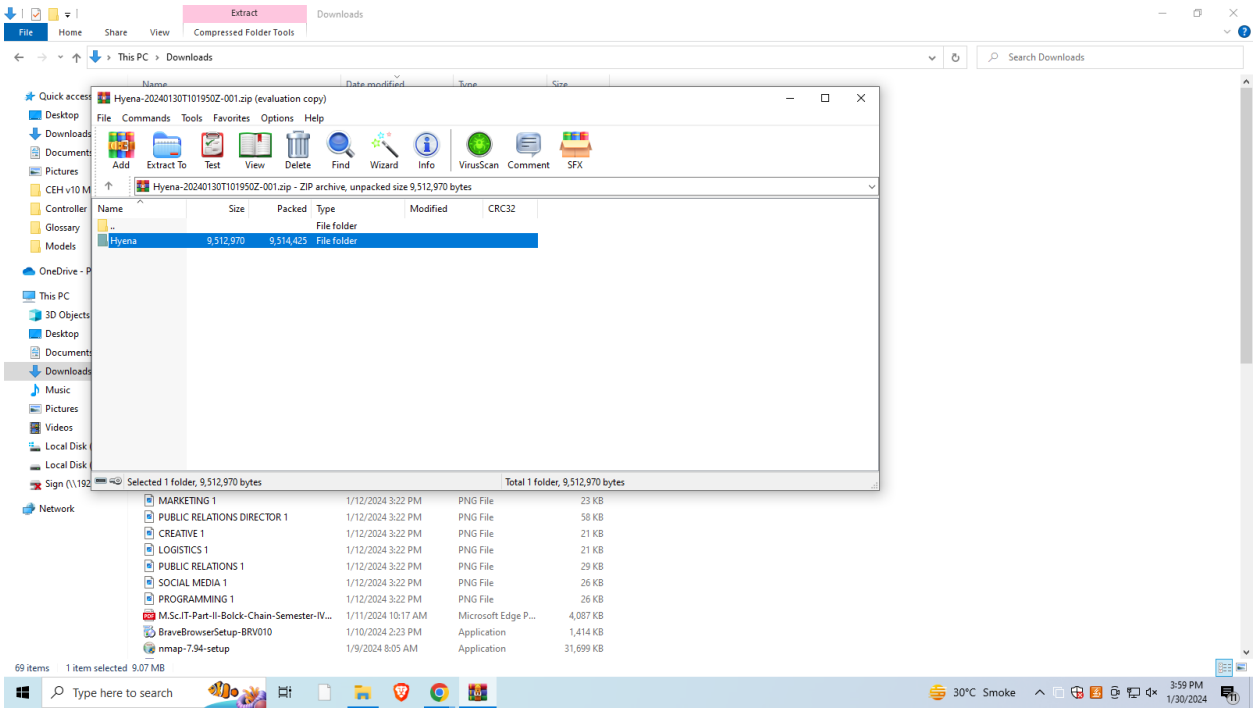
Step 13: Perform enumeration on telnet, write a port number.
$ telnet 192.168.40.131 25

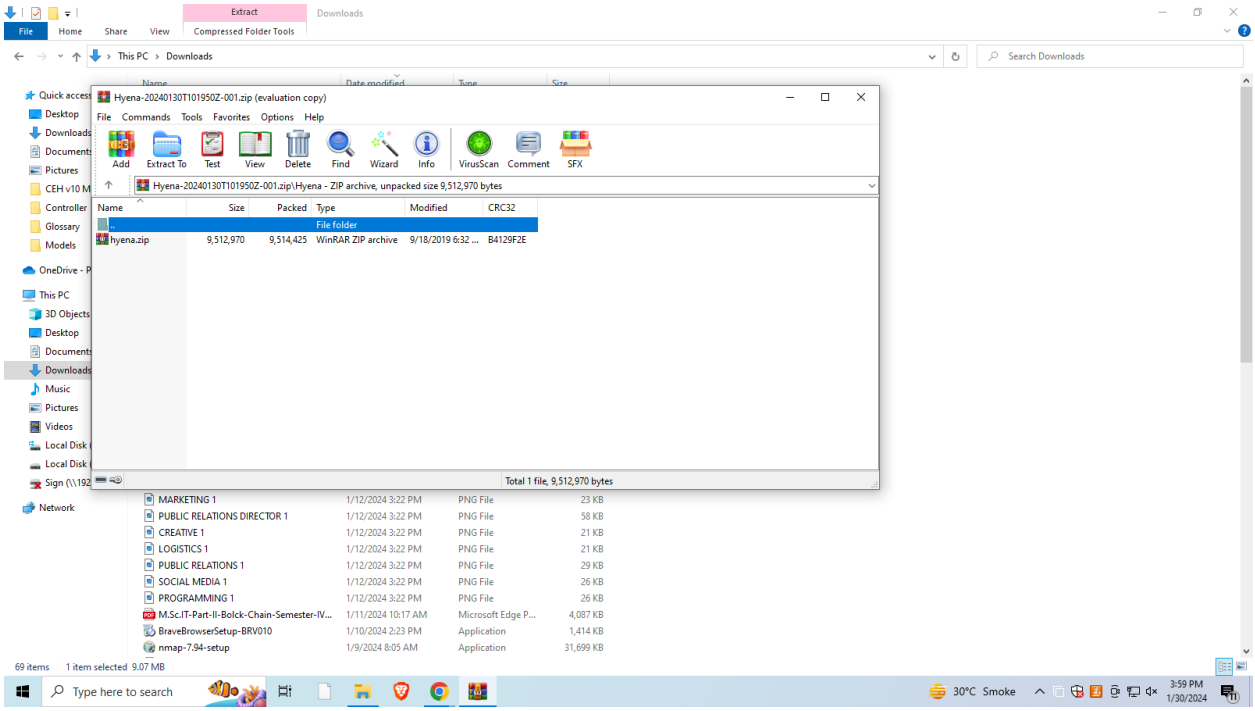
```
┌──(root1㉿kali)-[~]
└─$ telnet 192.168.40.131 25
Trying 192.168.40.131...
Connected to 192.168.40.131.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

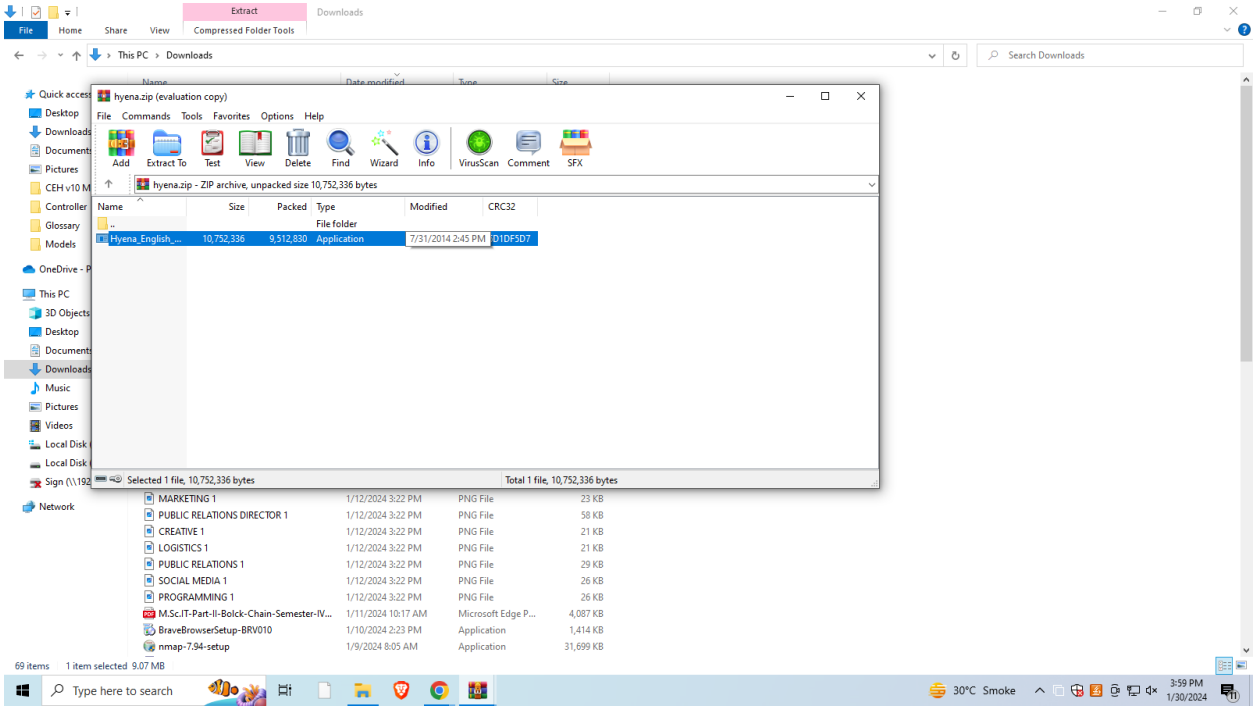
B. Hyena

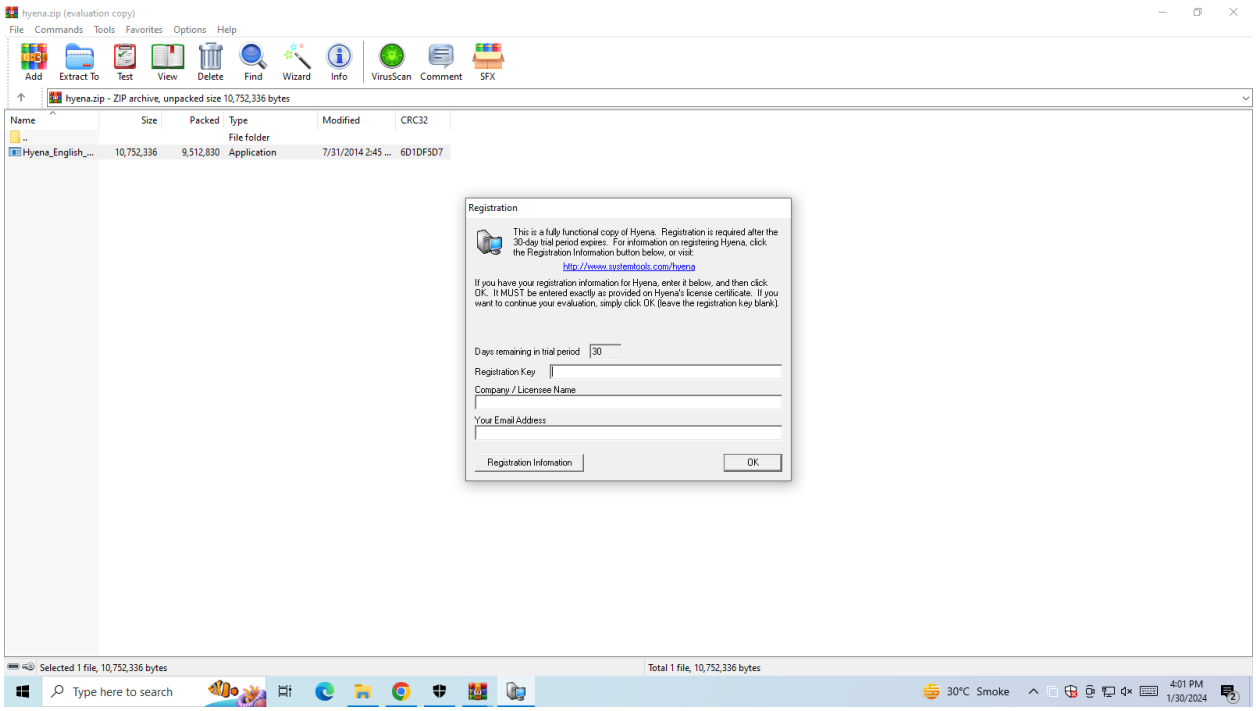
Step 1: Open Hyena tool

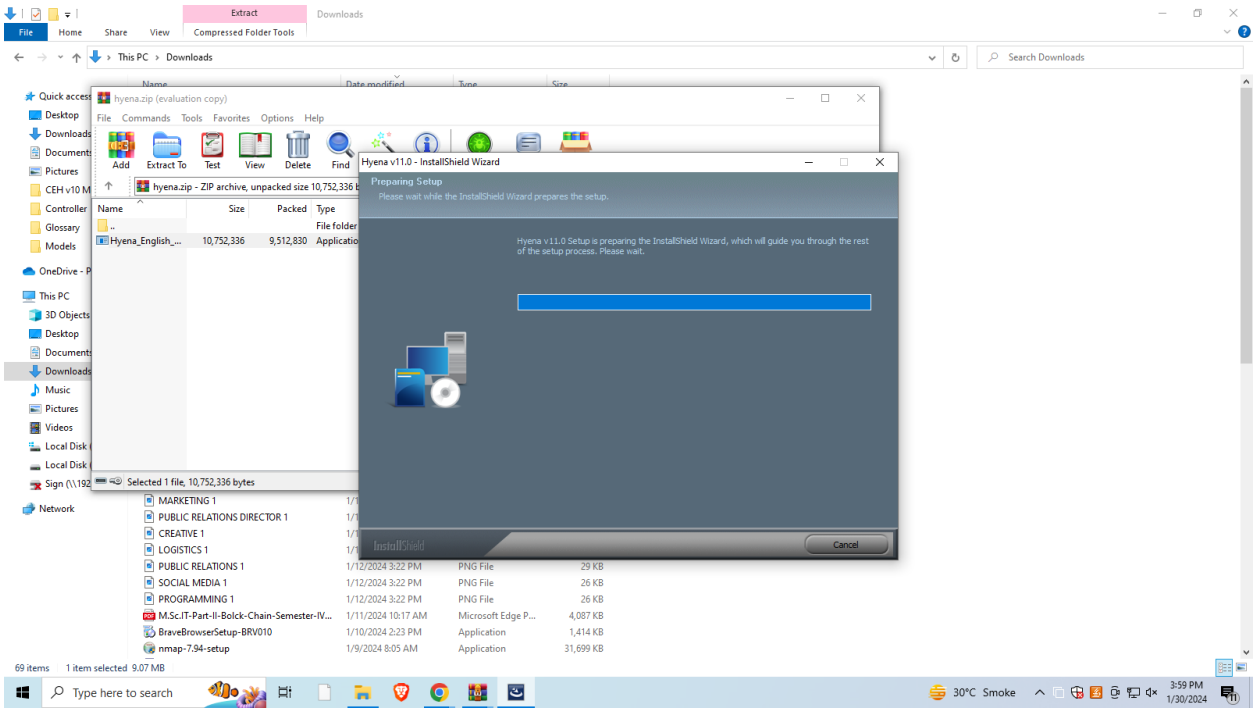
Step 2: Check all the files

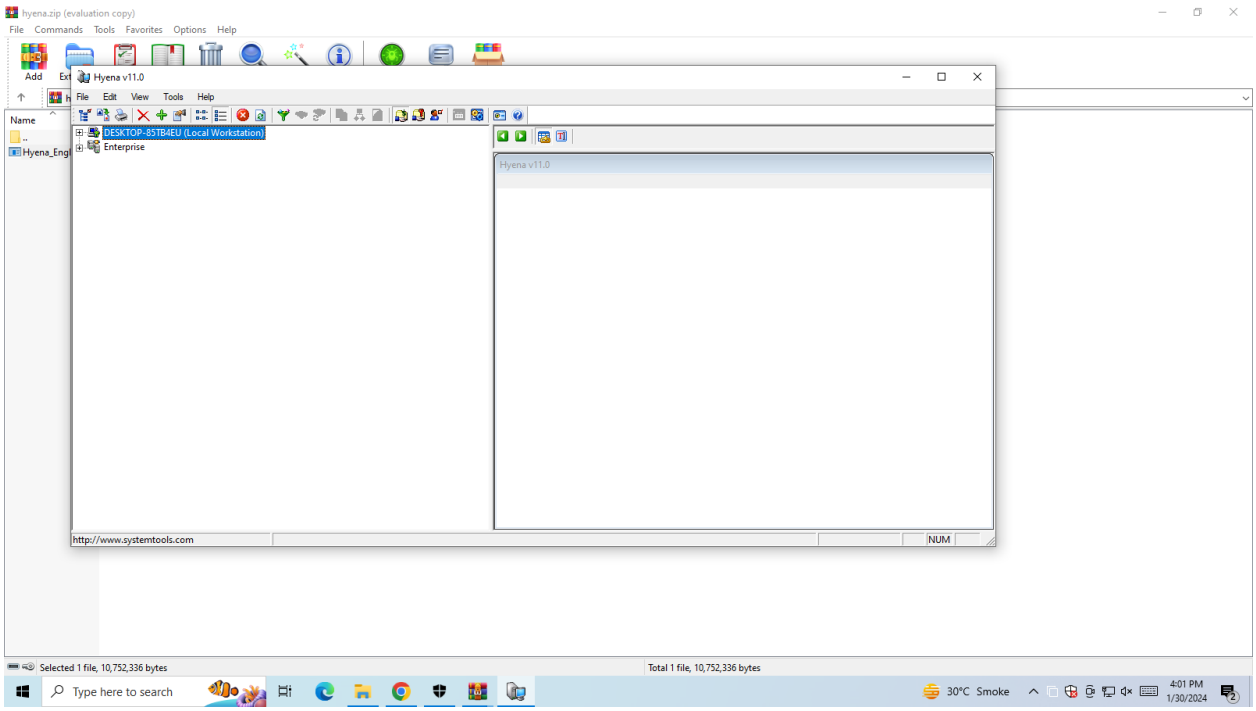


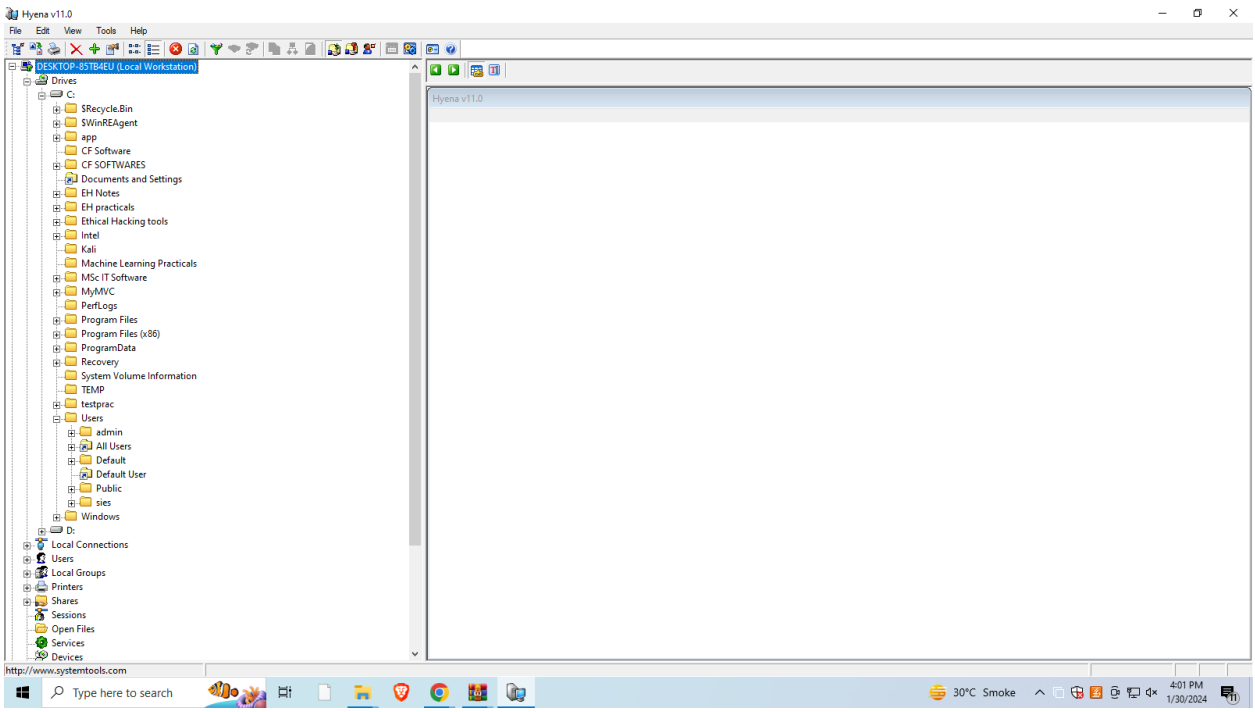

Hyena-20240130T101950Z-001.zip (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX
Hyena-20240130T101950Z-001.zip\Hyena - ZIP archive, unpacked size 9,512,970 bytes
Name Size Packed Type Modified CRC32
File folder
hyena.zip 9,512,970 9,514,425 WinRAR ZIP archive 9/18/2019 6:32 ... B4129F2E
Total 1 file, 9,512,970 bytes
MARKETING 1 1/12/2024 3:22 PM PNG File 23 KB
PUBLIC RELATIONS DIRECTOR 1 1/12/2024 3:22 PM PNG File 58 KB
CREATIVE 1 1/12/2024 3:22 PM PNG File 21 KB
LOGISTICS 1 1/12/2024 3:22 PM PNG File 21 KB
PUBLIC RELATIONS 1 1/12/2024 3:22 PM PNG File 29 KB
SOCIAL MEDIA 1 1/12/2024 3:22 PM PNG File 26 KB
PROGRAMMING 1 1/12/2024 3:22 PM PNG File 26 KB
M.Sc.IT-Part-II-Bolck-Chain-Semester-IV... 1/11/2024 10:17 AM Microsoft Edge P... 4,087 KB
BraveBrowserSetup-BRV010 1/10/2024 2:23 PM Application 1,414 KB
nmap-7.94-setup 1/9/2024 8:05 AM Application 31,699 KB
69 items 1 item selected 9.07 MB
Type here to search
30°C Smoke
3:59 PM 1/30/2024

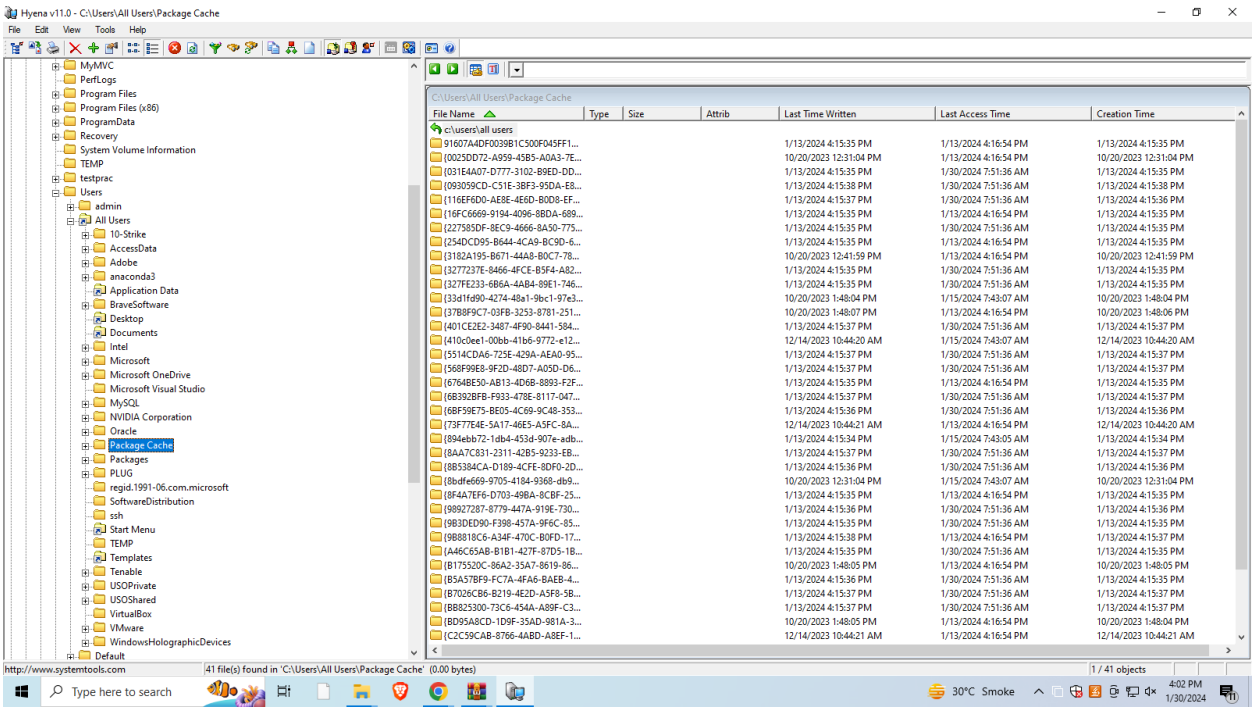

hyena.zip (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX
hyena.zip - ZIP archive, unpacked size 10,752,336 bytes
Name Size Packed Type Modified CRC32
File folder
Hyena_English_... 10,752,336 9,512,830 Application 7/31/2014 2:45 PM D1DF5D7
Selected 1 file, 10,752,336 bytes
Total 1 file, 10,752,336 bytes
MARKETING 1 1/12/2024 3:22 PM PNG File 23 KB
PUBLIC RELATIONS DIRECTOR 1 1/12/2024 3:22 PM PNG File 58 KB
CREATIVE 1 1/12/2024 3:22 PM PNG File 21 KB
LOGISTICS 1 1/12/2024 3:22 PM PNG File 21 KB
PUBLIC RELATIONS 1 1/12/2024 3:22 PM PNG File 29 KB
SOCIAL MEDIA 1 1/12/2024 3:22 PM PNG File 26 KB
PROGRAMMING 1 1/12/2024 3:22 PM PNG File 26 KB
M.Sc.IT-Part-II-Bolck-Chain-Semester-IV... 1/11/2024 10:17 AM Microsoft Edge P... 4,087 KB
BraveBrowserSetup-BRV010 1/10/2024 2:23 PM Application 1,414 KB
nmap-7.94-setup 1/9/2024 8:05 AM Application 31,699 KB
69 items 1 item selected 9.07 MB
Type here to search
30°C Smoke
3:59 PM 1/30/2024

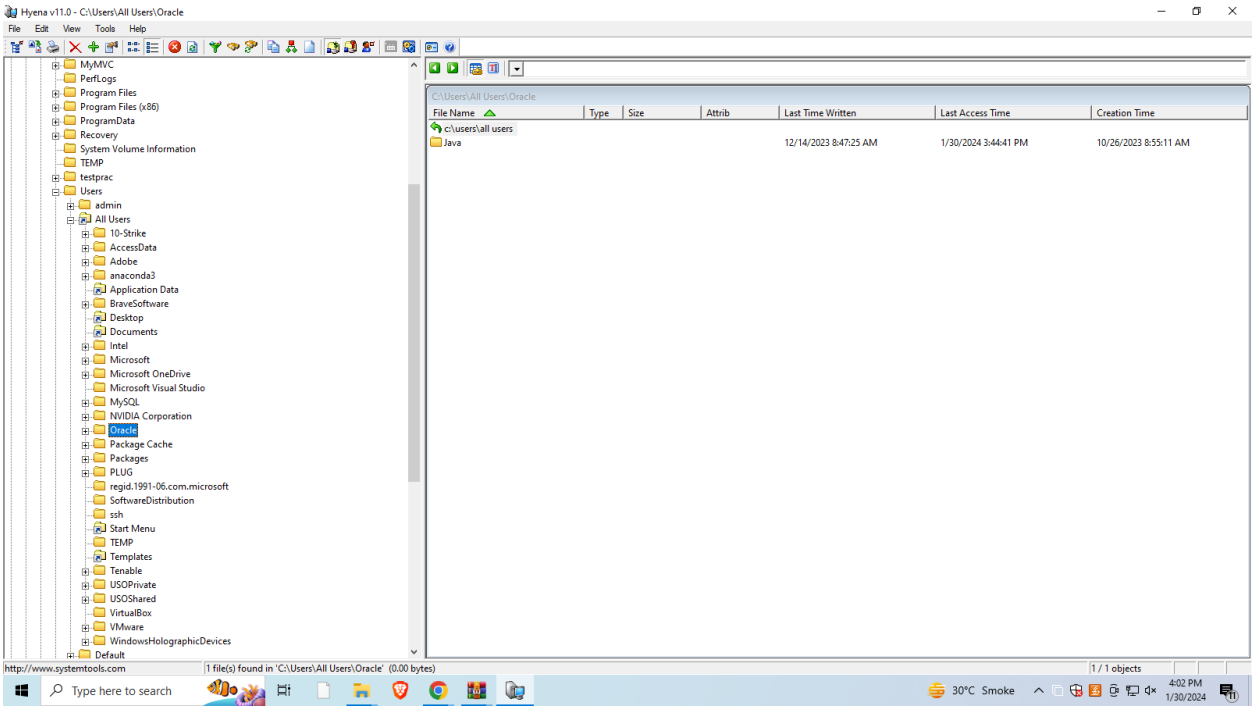

hyena.zip (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX
hyena.zip - ZIP archive, unpacked size 10,752,336 bytes
Name Size Packed Type Modified CRC32
Hyena_English_... 10,752,336 9,512,830 Application 7/31/2014 2:45 ... 6D1DF5D7
Registration
This is a fully functional copy of Hyena. Registration is required after the 30-day trial period expires. For information on registering Hyena, click the Registration Information button below, or visit:
http://www.systemtools.com/hyena
If you have your registration information for Hyena, enter it below, and then click OK. It MUST be entered exactly as provided on Hyena's license certificate. If you want to continue your evaluation, simply click OK (leave the registration key blank).
Days remaining in trial period 30
Registration Key
Company / Licensee Name
Your Email Address
Registration Information
OK
Selected 1 file, 10,752,336 bytes
Total 1 file, 10,752,336 bytes
Type here to search
30°C Smoke
4:01 PM
1/30/2024

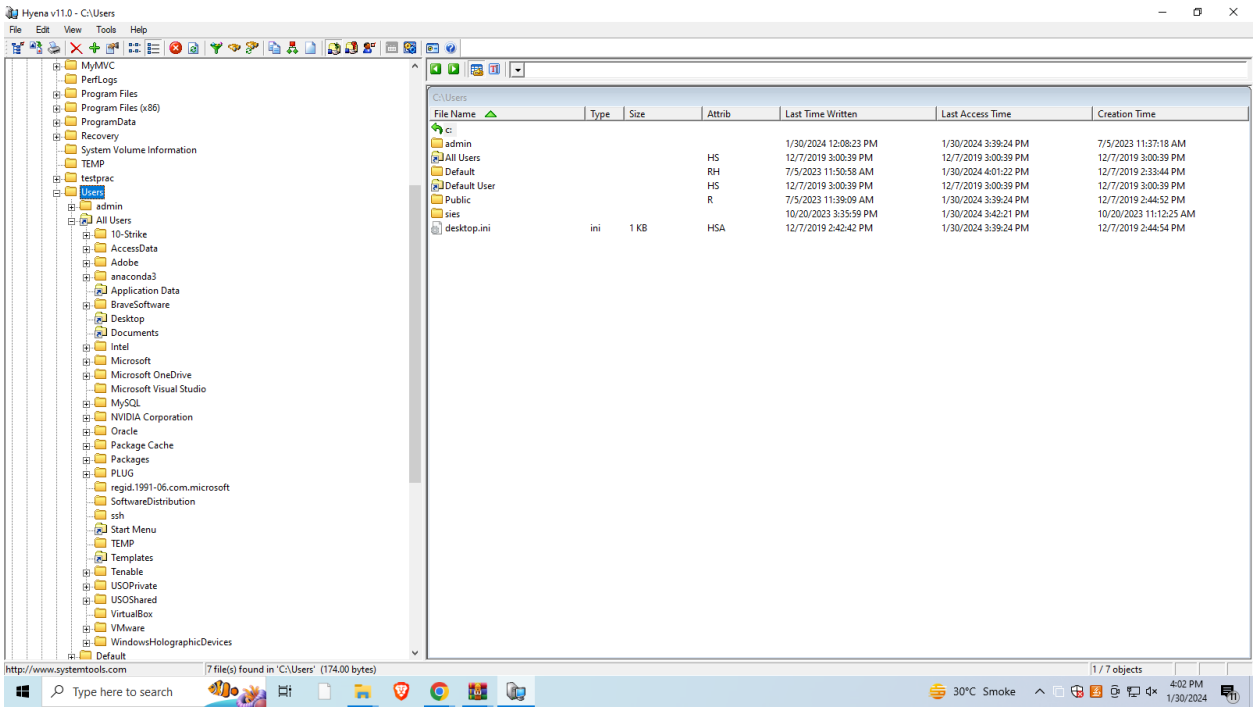

Extract
Downloads
File Home Share View Compressed Folder Tools
This PC › Downloads
Search Downloads
hyena.zip (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find
Hyena v11.0 - InstallShield Wizard
Preparing Setup
Please wait while the InstallShield Wizard prepares the setup.
Hyena v11.0 Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.
InstallShield
Cancel
Selected 1 file, 10,752,336 bytes
MARKETING 1
PUBLIC RELATIONS DIRECTOR 1
CREATIVE 1
LOGISTICS 1
PUBLIC RELATIONS 1 1/12/2024 3:22 PM PNG File 29 KB
SOCIAL MEDIA 1 1/12/2024 3:22 PM PNG File 26 KB
PROGRAMMING 1 1/12/2024 3:22 PM PNG File 26 KB
M.Sc.IT-Part-II-Bolck-Chain-Semester-IV... 1/11/2024 10:17 AM Microsoft Edge P... 4,087 KB
BraveBrowserSetup-BRV010 1/10/2024 2:23 PM Application 1,414 KB
nmap-7.94-setup 1/9/2024 8:05 AM Application 31,699 KB
69 items 1 item selected 9.07 MB
Type here to search
30°C Smoke
3:59 PM
1/30/2024


hyena.zip (evaluation copy)
File Commands Tools Favorites Options Help
Add
Hyena v11.0
File Edit View Tools Help
DESKTOP-85TB4EU (Local Workstation)
Enterprise
Hyena v11.0
http://www.systemtools.com
NUM
Name
Hyena_Engl
Selected 1 file, 10,752,336 bytes
Total 1 file, 10,752,336 bytes
Type here to search
30°C Smoke
4:01 PM
1/30/2024


Hyena v11.0
File Edit View Tools Help
DESKTOP-85TB4EU (Local Workstation)
Drives
C:
$Recycle.Bin
$WinREAgent
app
CF Software
CF SOFTWARES
Documents and Settings
EH Notes
EH practicals
Ethical Hacking tools
Intel
Kali
Machine Learning Practicals
MSc IT Software
MyMVC
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
System Volume Information
TEMP
testprac
Users
admin
All Users
Default
Default User
Public
sies
Windows
D:
Local Connections
Users
Local Groups
Printers
Shares
Sessions
Open Files
Services
Devices
Hyena v11.0
http://www.systemtools.com
Type here to search
30°C Smoke
4:01 PM
1/30/2024


Hyena v11.0 - C:\Users\All Users\Package Cache
File Edit View Tools Help
MyMVC
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
System Volume Information
TEMP
testprac
Users
admin
All Users
10-Strike
AccessData
Adobe
anaconda3
Application Data
BraveSoftware
Desktop
Documents
Intel
Microsoft
Microsoft OneDrive
Microsoft Visual Studio
MySQL
NVIDIA Corporation
Oracle
Package Cache
Packages
PLUG
regid.1991-06.com.microsoft
SoftwareDistribution
ssh
Start Menu
TEMP
Templates
Tenable
USOPrivate
USOShared
VirtualBox
VMware
WindowsHolographicDevices
Default
C:\Users\All Users\Package Cache
File Name
Type
Size
Attrib
Last Time Written
Last Access Time
Creation Time
c:\users\all users
91607A4DF0039B1C500F045FF1...
{0025DD72-A959-45B5-A0A3-7E...
{031E4A07-D777-3102-B9ED-DD...
{093059CD-C51E-3BF3-95DA-E8...
{116EF6D0-AE8E-4E6D-B0D8-EF...
{16FC6669-9194-4096-8BDA-689...
{227585DF-8EC9-4666-8A50-775...
{254DCD95-B644-4CA9-BC9D-6...
{3182A195-B671-44A8-B0C7-78...
{3277237E-8466-4FCE-B5F4-A82...
{327FE233-6B6A-4AB4-89E1-746...
{33d1fd90-4274-48a1-9bc1-97e3...
{37B8F9C7-03FB-3253-8781-251...
{401CE2E2-3487-4F90-8441-584...
{410c0ee1-00bb-41b6-9772-e12...
{5514CDA6-725E-429A-AEA0-95...
{568F99E8-9F2D-48D7-A05D-D6...
{6764BE50-AB13-4D6B-8893-F2F...
{6B392BFB-F933-478E-8117-047...
{6BF59E75-BE05-4C69-9C48-353...
{73F77E4E-5A17-46E5-A5FC-8A...
{894ebb72-1db4-453d-907e-adb...
{8AA7C831-2311-42B5-9233-EB...
{8B5384CA-D189-4CFE-8DF0-2D...
{8bdfe669-9705-4184-9368-db9...
{8F4A7EF6-D703-49BA-8CBF-25...
{98927287-8779-447A-919E-730...
{9B3DED90-F398-457A-9F6C-85...
{9B8818C6-A34F-470C-B0FD-17...
{A46C65AB-B1B1-427F-87D5-1B...
{B175520C-86A2-35A7-8619-86...
{B5A57BF9-FC7A-4FA6-BAEB-4...
{B7026CB6-B219-4E2D-A5F8-5B...
{BB825300-73C6-454A-A89F-C3...
{BD95A8CD-1D9F-35AD-981A-3...
{C2C59CAB-8766-4ABD-A8EF-1...
1/13/2024 4:15:35 PM
10/20/2023 12:31:04 PM
1/13/2024 4:15:35 PM
1/13/2024 4:15:38 PM
1/13/2024 4:15:37 PM
1/13/2024 4:15:35 PM
1/13/2024 4:15:35 PM
1/13/2024 4:15:35 PM
10/20/2023 12:41:59 PM
1/13/2024 4:15:35 PM
1/13/2024 4:15:35 PM
10/20/2023 1:48:04 PM
10/20/2023 1:48:07 PM
1/13/2024 4:15:37 PM
12/14/2023 10:44:20 AM
1/13/2024 4:15:37 PM
1/13/2024 4:15:37 PM
1/13/2024 4:15:35 PM
1/13/2024 4:15:37 PM
1/13/2024 4:15:36 PM
12/14/2023 10:44:21 AM
1/13/2024 4:15:34 PM
1/13/2024 4:15:37 PM
1/13/2024 4:15:36 PM
10/20/2023 12:31:04 PM
1/13/2024 4:15:35 PM
1/13/2024 4:15:36 PM
1/13/2024 4:15:35 PM
1/13/2024 4:15:38 PM
1/13/2024 4:15:35 PM
10/20/2023 1:48:05 PM
1/13/2024 4:15:36 PM
1/13/2024 4:15:37 PM
1/13/2024 4:15:37 PM
10/20/2023 1:48:05 PM
12/14/2023 10:44:21 AM
1/30/2024 7:51:36 AM
1/15/2024 7:43:07 AM
1/15/2024 7:43:05 AM
1/30/2024 3:44:41 PM
1/13/2024 4:16:54 PM
10/20/2023 12:31:04 PM
10/20/2023 1:48:04 PM
10/20/2023 1:48:06 PM
10/20/2023 12:41:59 PM
10/26/2023 8:55:11 AM
12/14/2023 8:47:25 AM
http://www.systemtools.com
41 file(s) found in 'C:\Users\All Users\Package Cache' (0.00 bytes)
1 / 41 objects
Type here to search
30°C Smoke
4:02 PM
1/30/2024

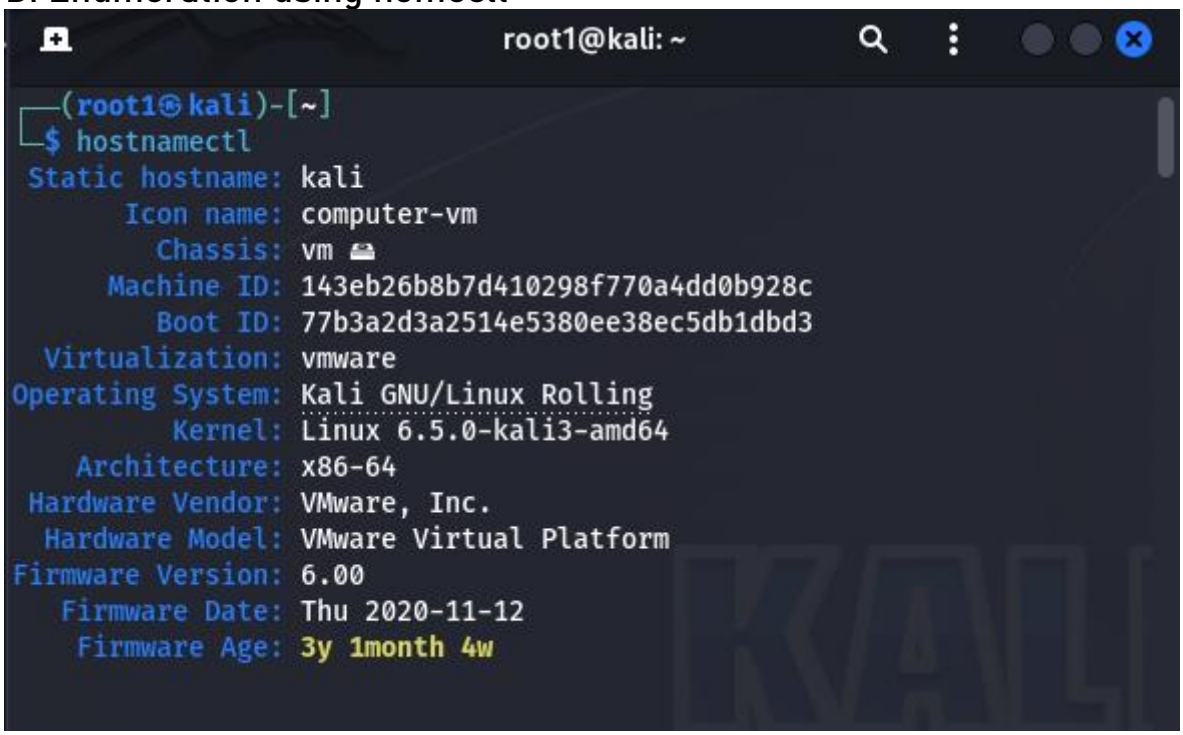

Hyena v11.0 - C:\Users\All Users\Oracle
File Edit View Tools Help
MyMVC
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
System Volume Information
TEMP
testprac
Users
admin
All Users
10-Strike
AccessData
Adobe
anaconda3
Application Data
BraveSoftware
Desktop
Documents
Intel
Microsoft
Microsoft OneDrive
Microsoft Visual Studio
MySQL
NVIDIA Corporation
Oracle
Package Cache
Packages
PLUG
regid.1991-06.com.microsoft
SoftwareDistribution
ssh
Start Menu
TEMP
Templates
Tenable
USOPrivate
USOShared
VirtualBox
VMware
WindowsHolographicDevices
Default
C:\Users\All Users\Oracle
File Name
Type
Size
Attrib
Last Time Written
Last Access Time
Creation Time
c:\users\all users
Java
12/14/2023 8:47:25 AM
1/30/2024 3:44:41 PM
10/26/2023 8:55:11 AM
http://www.systemtools.com
1 file(s) found in 'C:\Users\All Users\Oracle' (0.00 bytes)
1 / 1 objects
Type here to search
30°C Smoke
4:02 PM
1/30/2024



C. Enumeration using Whatweb

```
zsh: corrupt history file /home/root1/.zsh_history
┌──(root1㉿kali)-[~]
└─$ sudo whatweb siesascs.edu.in
[sudo] password for root1:
http://siesascs.edu.in [302 Found] Cookies[PHPSESSID], Country[SWITZERLAND][CH],
 HTTPServer[Microsoft-IIS/10.0], IP[169.38.89.3], Microsoft-IIS[10.0], PHP[8.0.0
], RedirectLocation[https://siesascs.edu.in/], Via-Proxy[HTTP/1.1 forward.http.p
roxy:3128], X-Powered-By[PHP/8.0.0]
https://siesascs.edu.in/ [200 OK] Bootstrap, Cookies[PHPSESSID], Country[SWITZER
LAND][CH], Email[principalascs@sies.edu.in], Google-Analytics[UA-36251023-1], HT
ML5, HTTPServer[Microsoft-IIS/10.0], IP[169.38.89.3], JQuery[2.1.4], Lightbox, M
icrosoft-IIS[10.0], Modernizr, Open-Graph-Protocol, PHP[8.0.0], Script[text/java
script], Title[SIES College of Arts, Science & Commerce (Empowered Autonomous)],
 X-Powered-By[PHP/8.0.0]
```

D. Enumeration using homectl



Practical No. 04 - Implement SMNP Enumeration

A] Using Hostnamectl

```
┌──(root1㉿kali)-[~]
└─$ hostnamectl
 Static hostname: kali
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 143eb26b8b7d410298f770a4dd0b928c
         Boot ID: 7360aec3aa1748c9ae012a82ea9b913f
  Virtualization: vmware
Operating System: Kali GNU/Linux Rolling
          Kernel: Linux 6.5.0-kali3-amd64
    Architecture: x86-64
 Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform
Firmware Version: 6.00
   Firmware Date: Thu 2020-11-12
    Firmware Age: 3y 2month 3w 3d
```

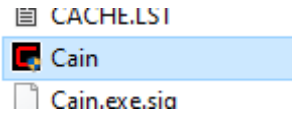
B] Using Net View

```
C:\Users\admin>net view \\192.168.10.7
Shared resources at \\192.168.10.7


Share name           Type  Used as  Comment

-------------------------------------------------------------------------------
Backup IT            Disk
BMS SET_P            Disk
BMS SET_Q            Disk
BMS SET_R            Disk
Capture Image        Disk
FY Web pracs         Disk
MSC                  Disk
MscIT                Disk
NETLOGON             Disk           Logon server share
old share            Disk
Photo                Disk
python-3.11.0-arm64  Disk
python-3.11.4-arm64  Disk
REMINST              Disk           Windows Deployment Services Share
share                Disk
Sign                 Disk  Z:
SYSVOL               Disk           Logon server share
The command completed successfully.
```

C] Using NMAP in cmd

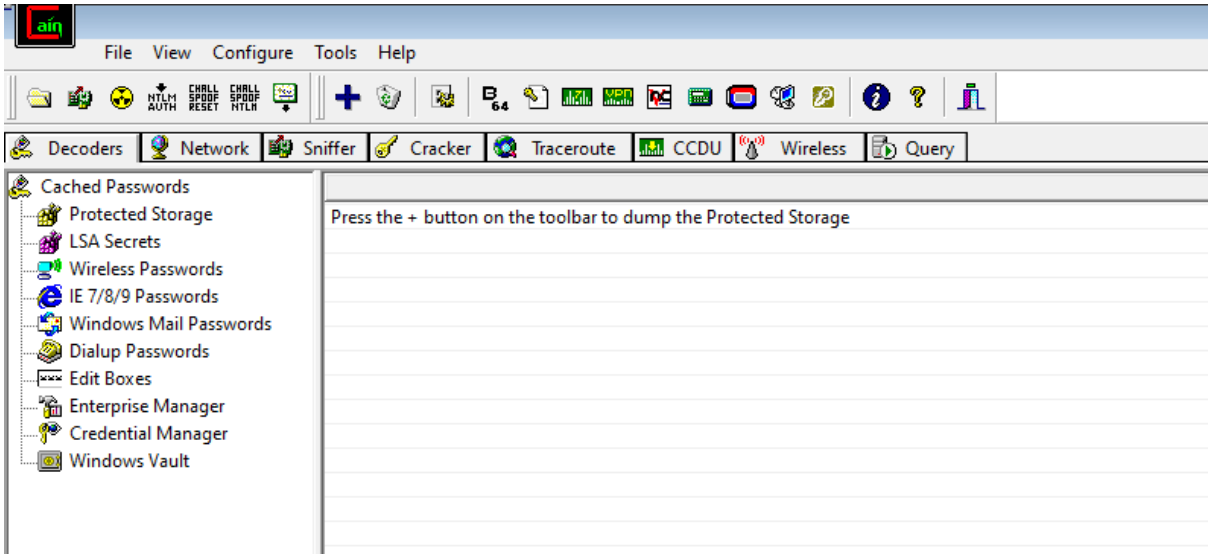
```
C:\Users\admin>nmap -sU -p 161 169.38.89.3
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-06 09:01 India Standard Time
Nmap scan report for 3.59.26a9.ip4.static.sl-reverse.com (169.38.89.3)
Host is up (0.0010s latency).

PORT    STATE         SERVICE
161/udp open|filtered snmp

Nmap done: 1 IP address (1 host up) scanned in 3.44 seconds
```

Practical No. 05 – Implement Password Cracking

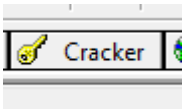


Install this in E: drive

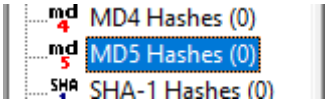
After installation it looks likes this.



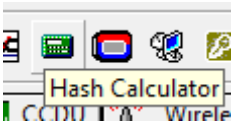
Then go to Cracker



Select this

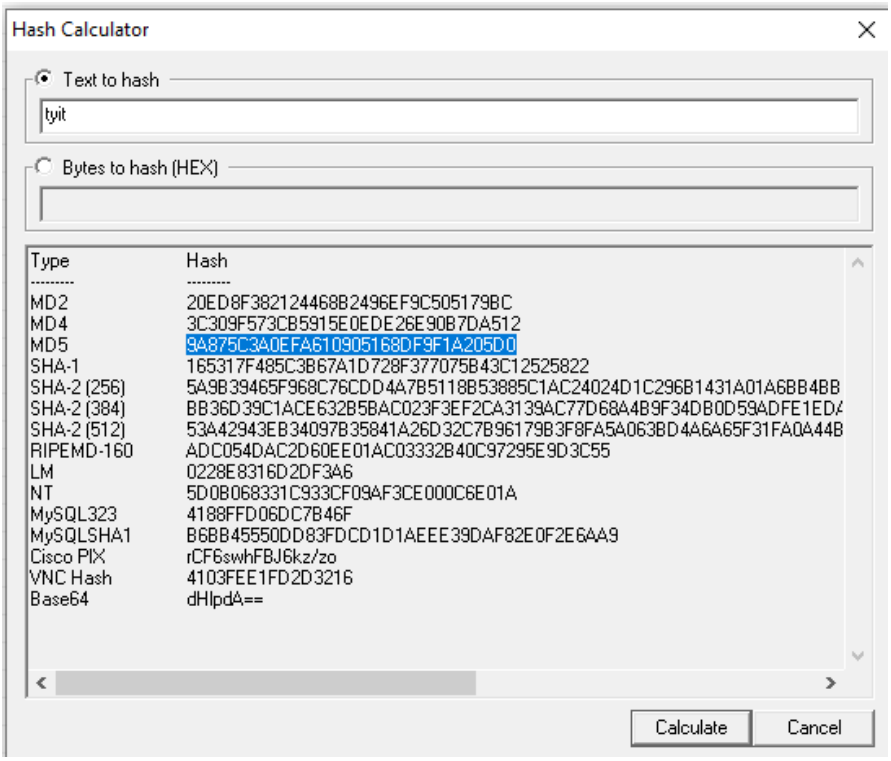


Click hash calculator

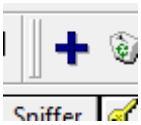


Then write any text and click calculate.

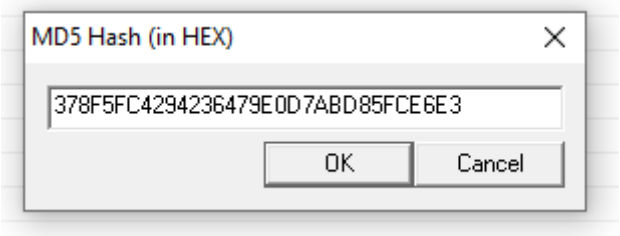
Copy MD5 hash value (ciphered text) then click cancel.



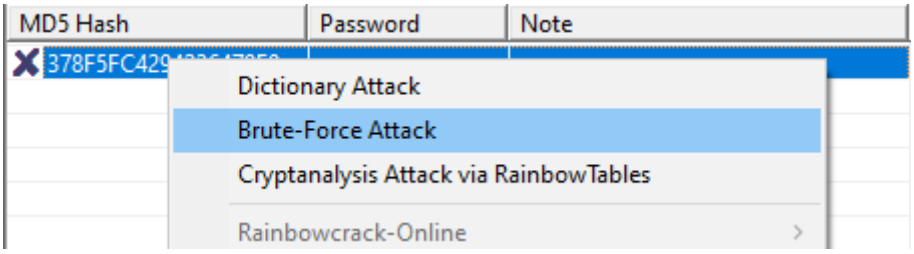
Click on this



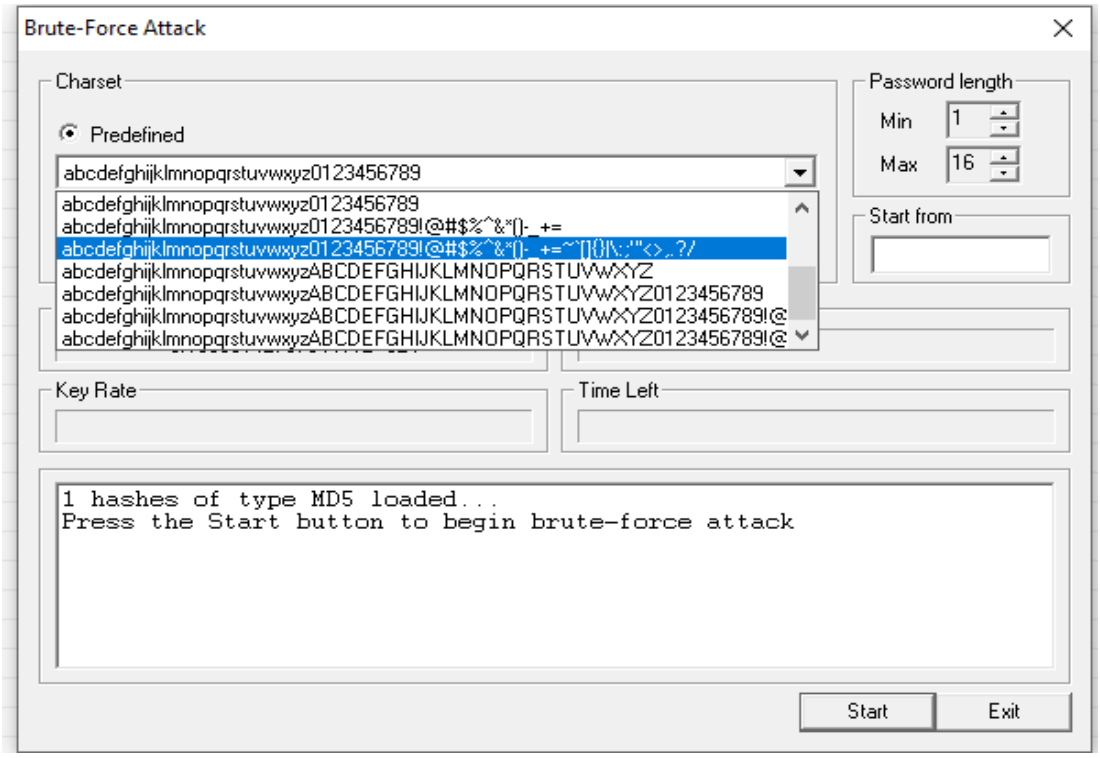
Paste the copied hash value then click OK



Right click on this and select this.

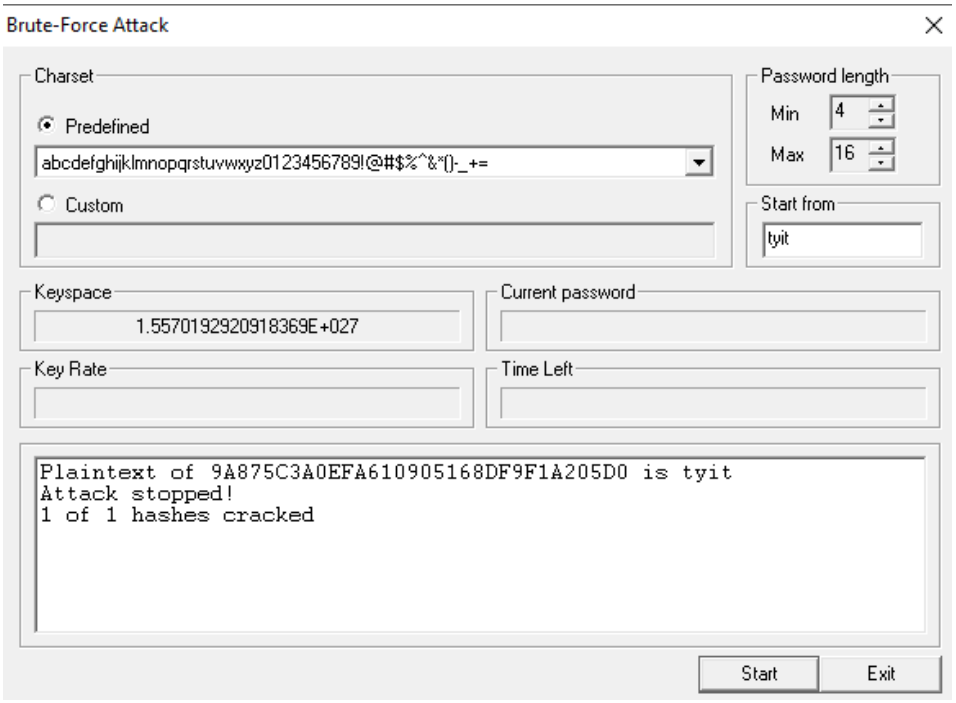


Then



Then click start

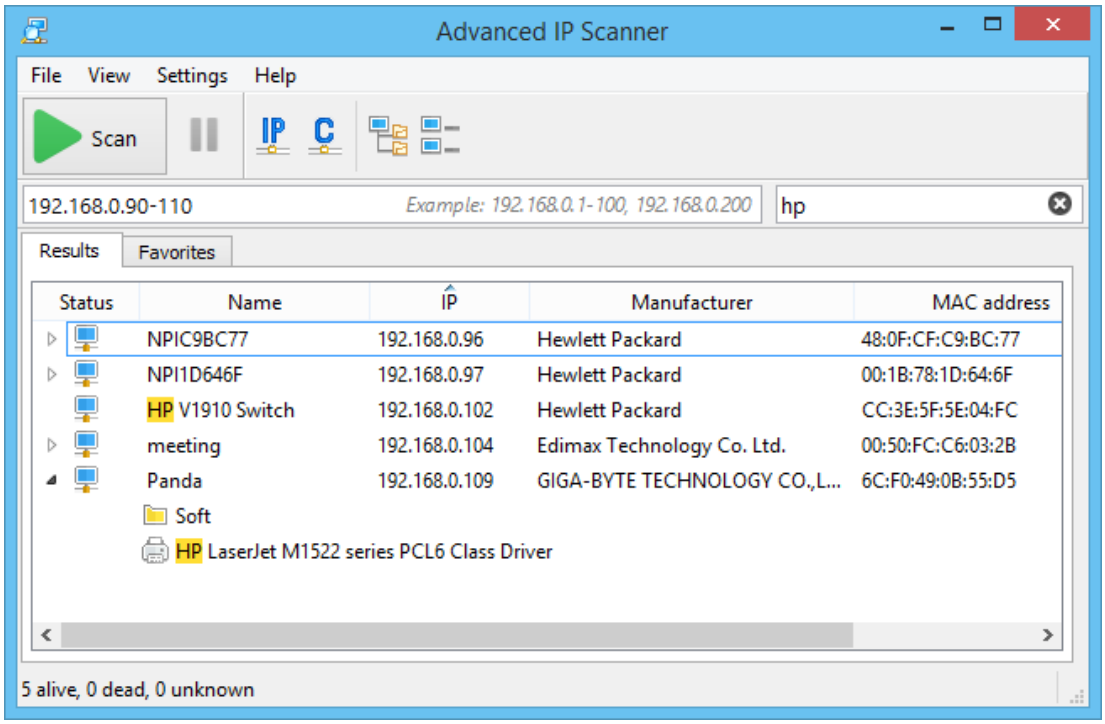
The text will be seen here



Practical No. 06 - Perform IP Scanning

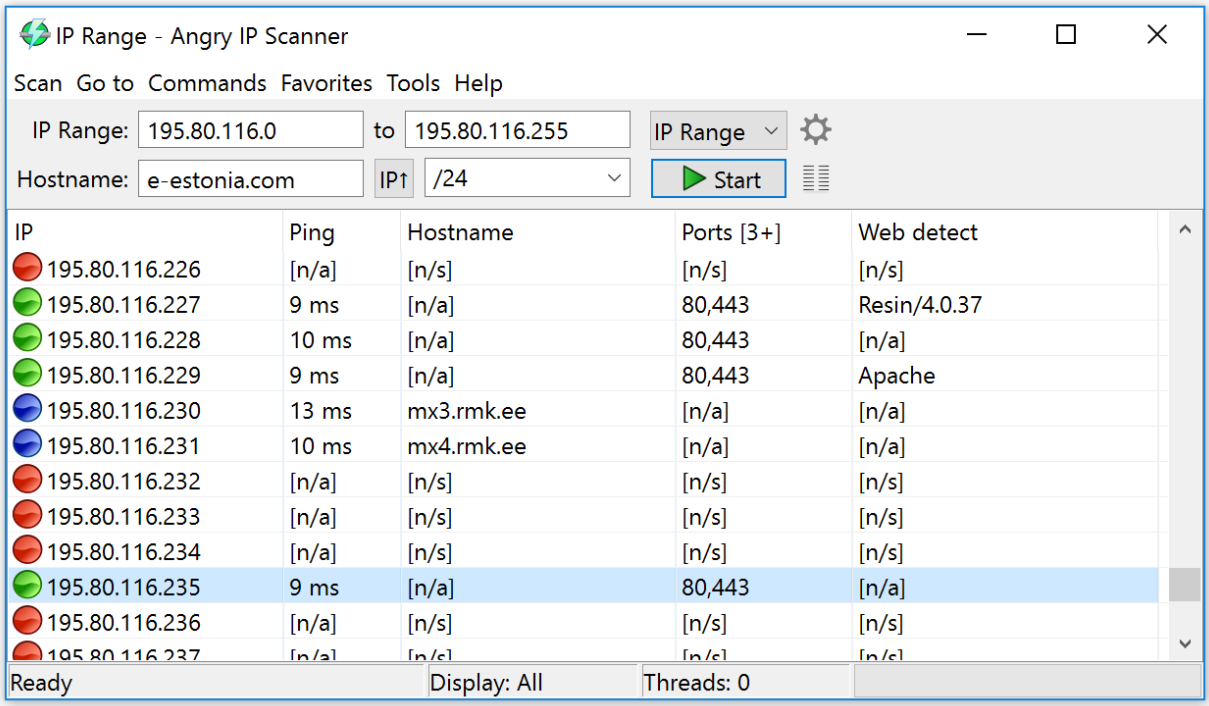
Using Advanced IP Scanning

Advanced IP Scanner is a fast and powerful network scanner with a user-friendly interface.In seconds, Advanced IP Scanner can locate all computers on your wired or wireless local network and scan their ports. The program provides easy access to various network resources such as HTTP, HTTPS, FTP, and shared folders.

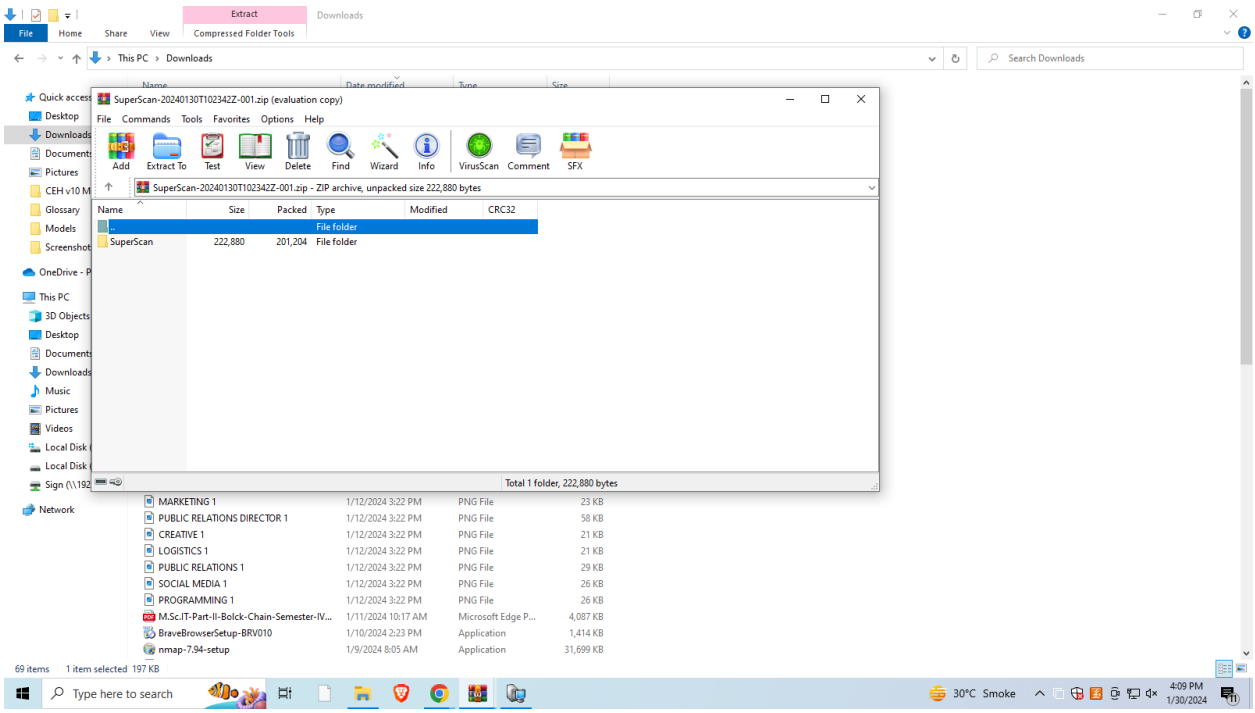


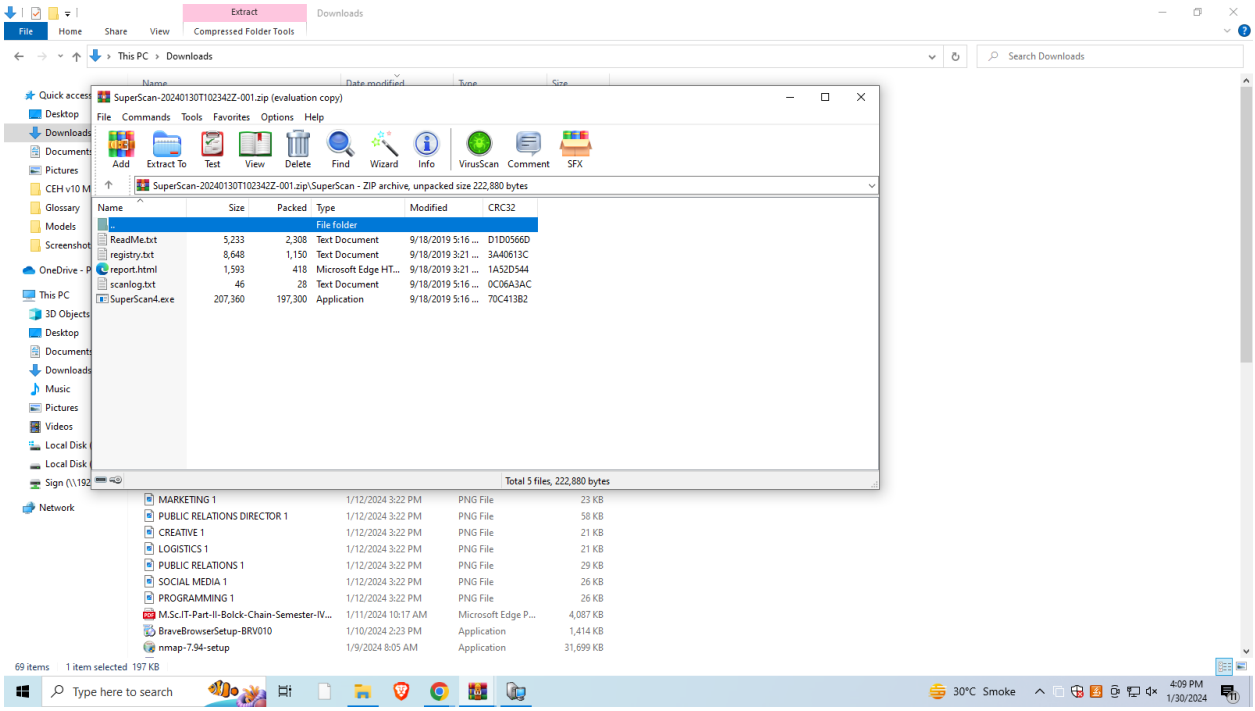
Using Angry IP Scanning

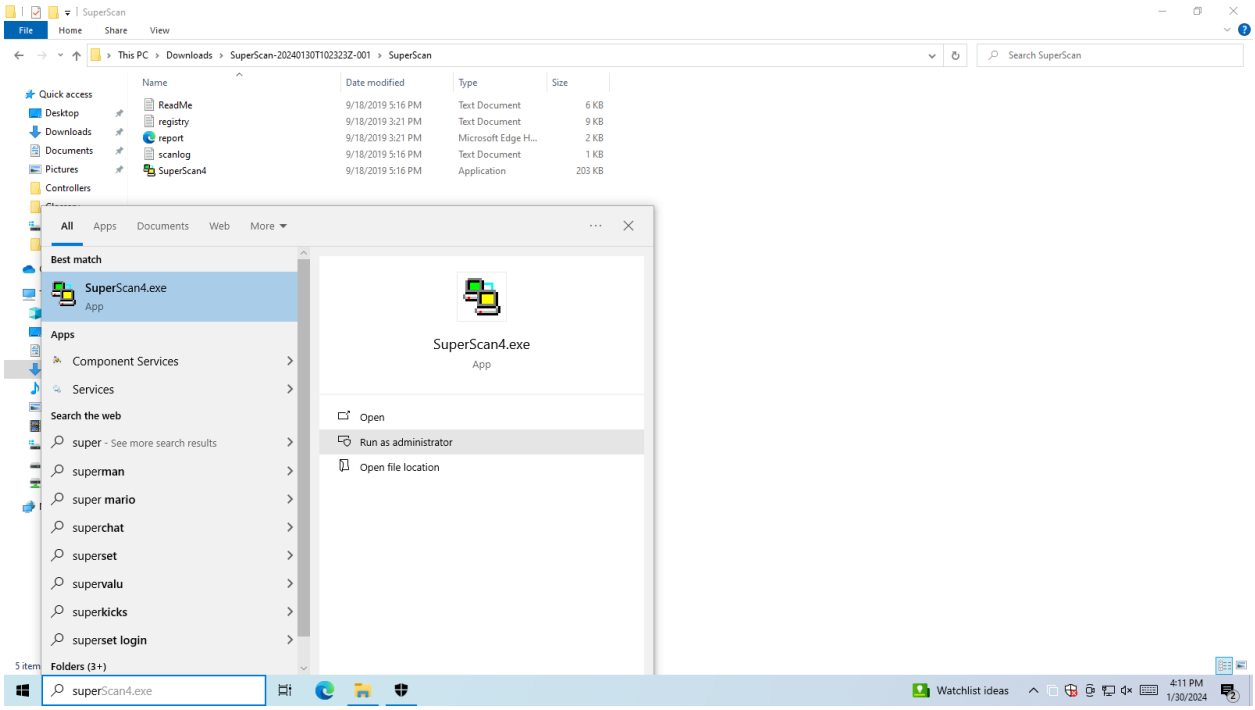
Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has many otherfeatures. It is widely used by network administrators and just curious users around the world, includinglarge and small enterprises, banks, and government agencies. It runs on Linux, Windows, and Mac OS X, possibly supporting other platforms as well.

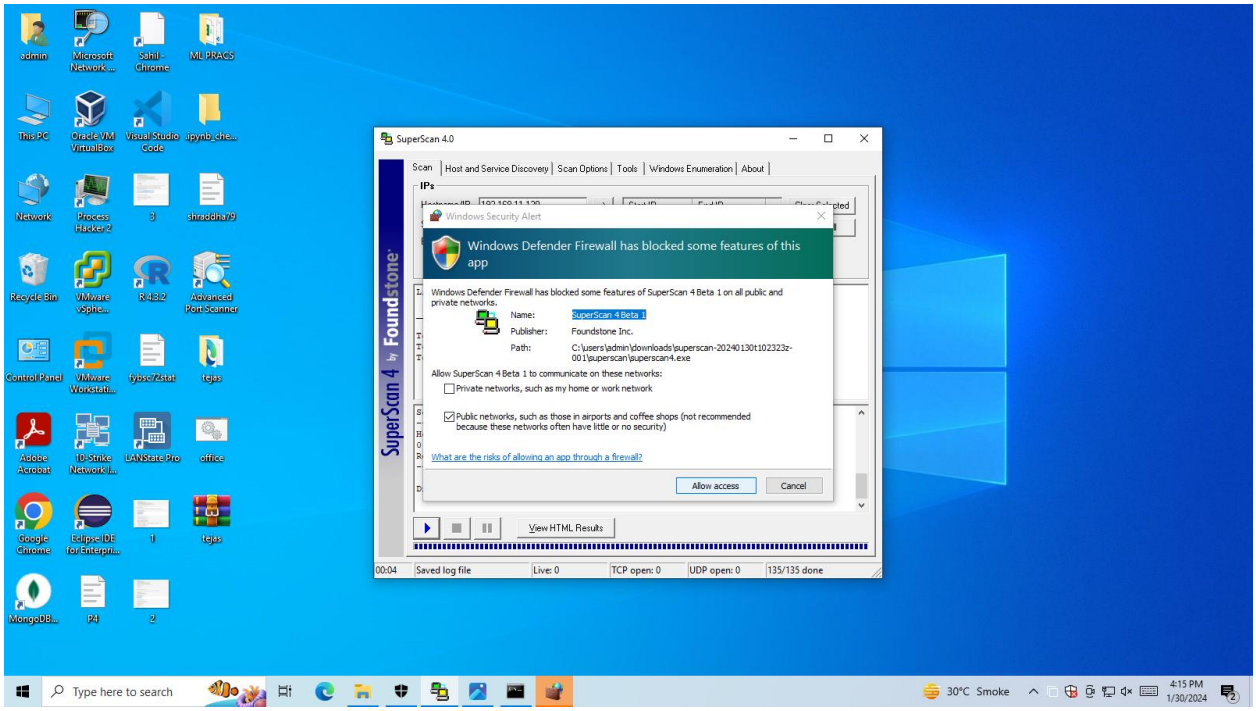


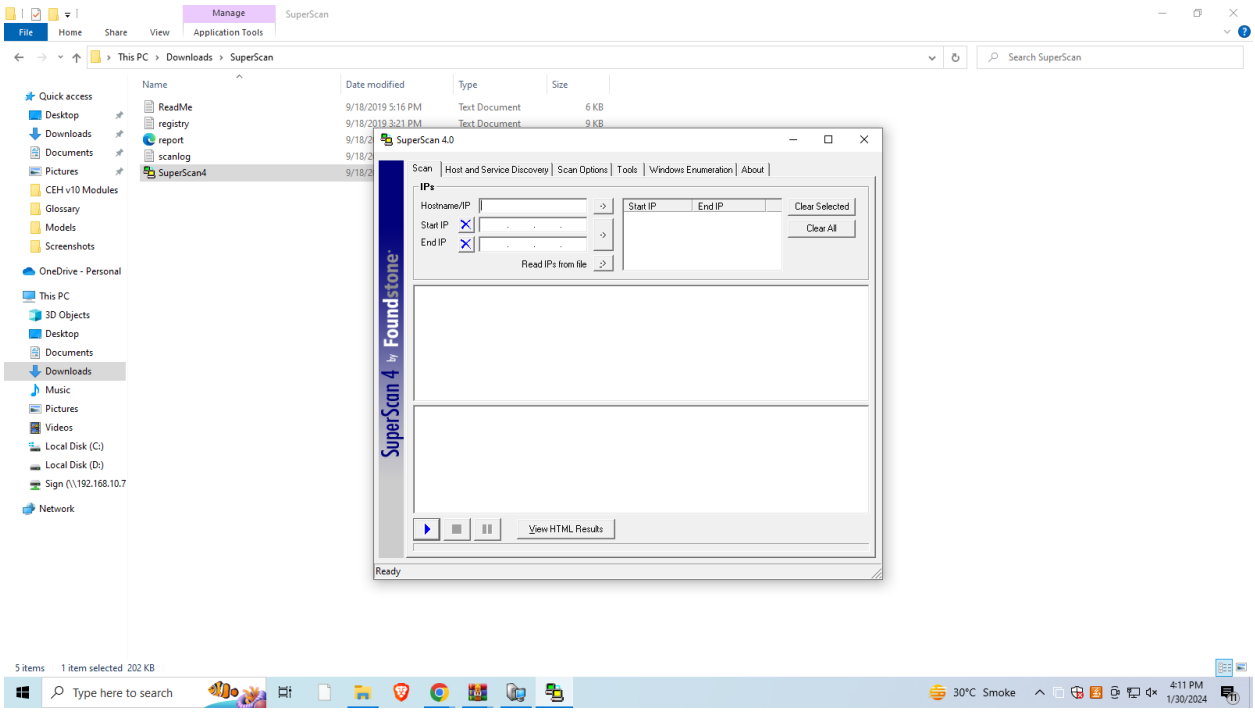
Using Super Scan

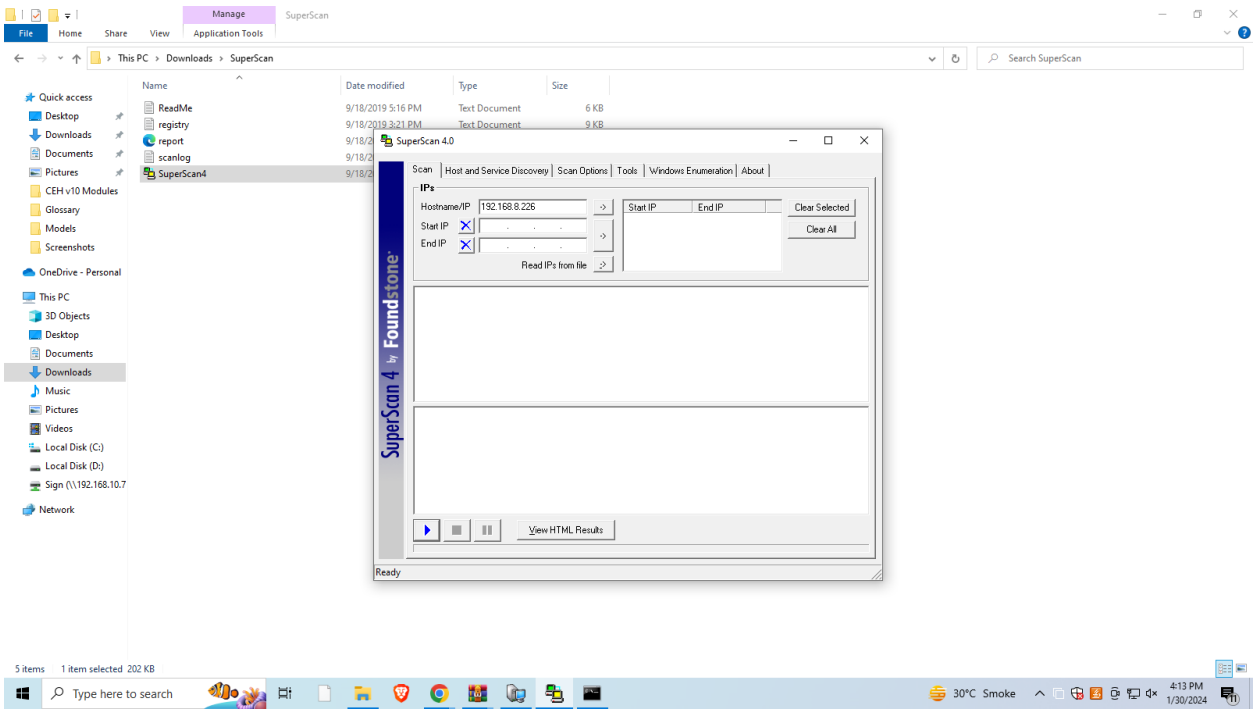


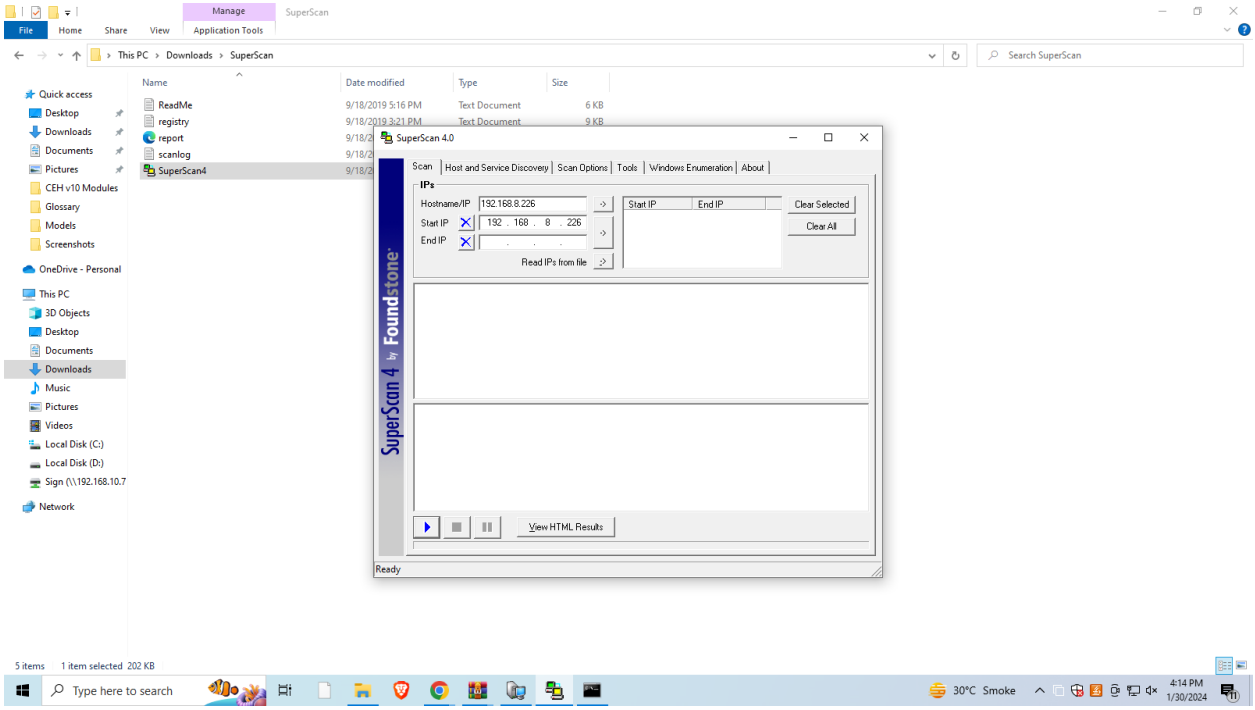

SuperScan-20240130T102342Z-001.zip (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX
SuperScan-20240130T102342Z-001.zip\SuperScan - ZIP archive, unpacked size 222,880 bytes
Name Size Packed Type Modified CRC32
File folder
ReadMe.txt 5,233 2,308 Text Document 9/18/2019 5:16 ... D1D0566D
registry.txt 8,648 1,150 Text Document 9/18/2019 3:21 ... 3A40613C
report.html 1,593 418 Microsoft Edge HT... 9/18/2019 3:21 ... 1A52D544
scanlog.txt 46 28 Text Document 9/18/2019 5:16 ... 0C06A3AC
SuperScan4.exe 207,360 197,300 Application 9/18/2019 5:16 ... 70C413B2
Total 5 files, 222,880 bytes
MARKETING 1 1/12/2024 3:22 PM PNG File 23 KB
PUBLIC RELATIONS DIRECTOR 1 1/12/2024 3:22 PM PNG File 58 KB
CREATIVE 1 1/12/2024 3:22 PM PNG File 21 KB
LOGISTICS 1 1/12/2024 3:22 PM PNG File 21 KB
PUBLIC RELATIONS 1 1/12/2024 3:22 PM PNG File 29 KB
SOCIAL MEDIA 1 1/12/2024 3:22 PM PNG File 26 KB
PROGRAMMING 1 1/12/2024 3:22 PM PNG File 26 KB
M.Sc.IT-Part-II-Bolck-Chain-Semester-IV... 1/11/2024 10:17 AM Microsoft Edge P... 4,087 KB
BraveBrowserSetup-BRV010 1/10/2024 2:23 PM Application 1,414 KB
nmap-7.94-setup 1/9/2024 8:05 AM Application 31,699 KB
69 items 1 item selected 197 KB
Type here to search
30°C Smoke
4:09 PM 1/30/2024

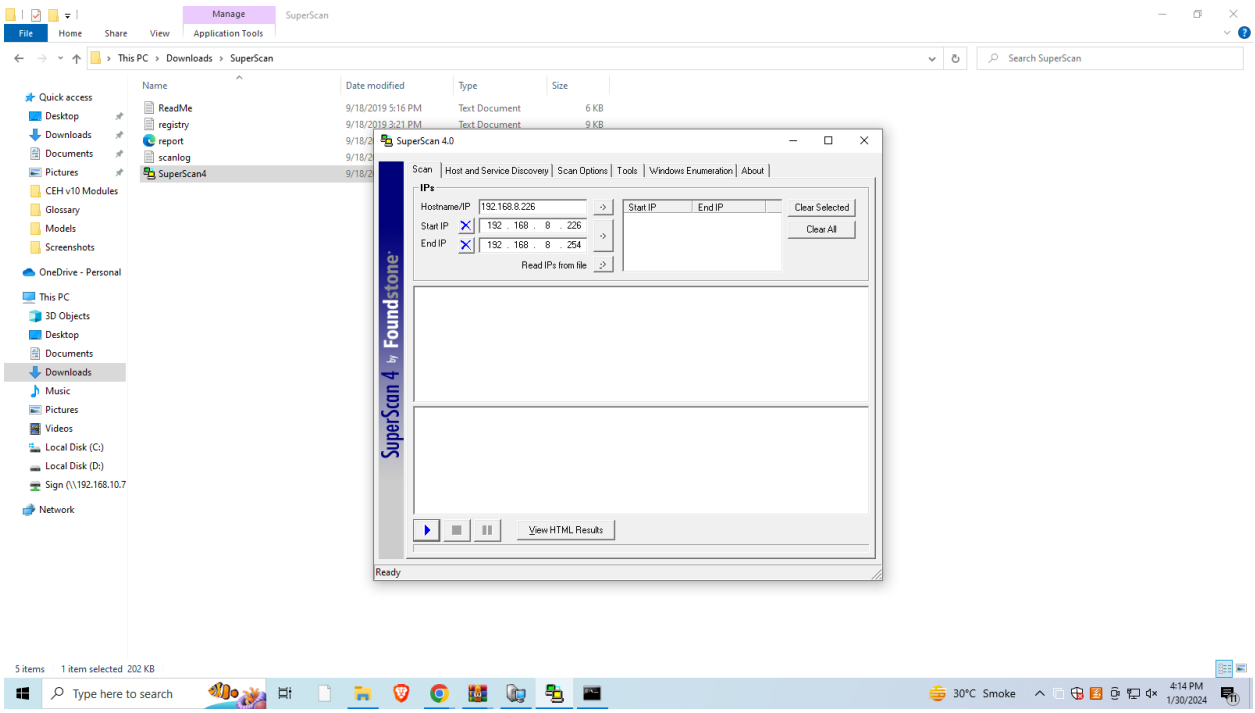

SuperScan
File Home Share View
This PC › Downloads › SuperScan-20240130T102323Z-001 › SuperScan
Search SuperScan
Name Date modified Type Size
ReadMe 9/18/2019 5:16 PM Text Document 6 KB
registry 9/18/2019 3:21 PM Text Document 9 KB
report 9/18/2019 3:21 PM Microsoft Edge H... 2 KB
scanlog 9/18/2019 5:16 PM Text Document 1 KB
SuperScan4 9/18/2019 5:16 PM Application 203 KB
All Apps Documents Web More
Best match
SuperScan4.exe
App
Apps
Component Services
Services
Search the web
super - See more search results
superman
super mario
superchat
superset
supervalu
superkicks
superset login
Folders (3+)
SuperScan4.exe
App
Open
Run as administrator
Open file location
5 items
superScan4.exe
Watchlist ideas
4:11 PM 1/30/2024

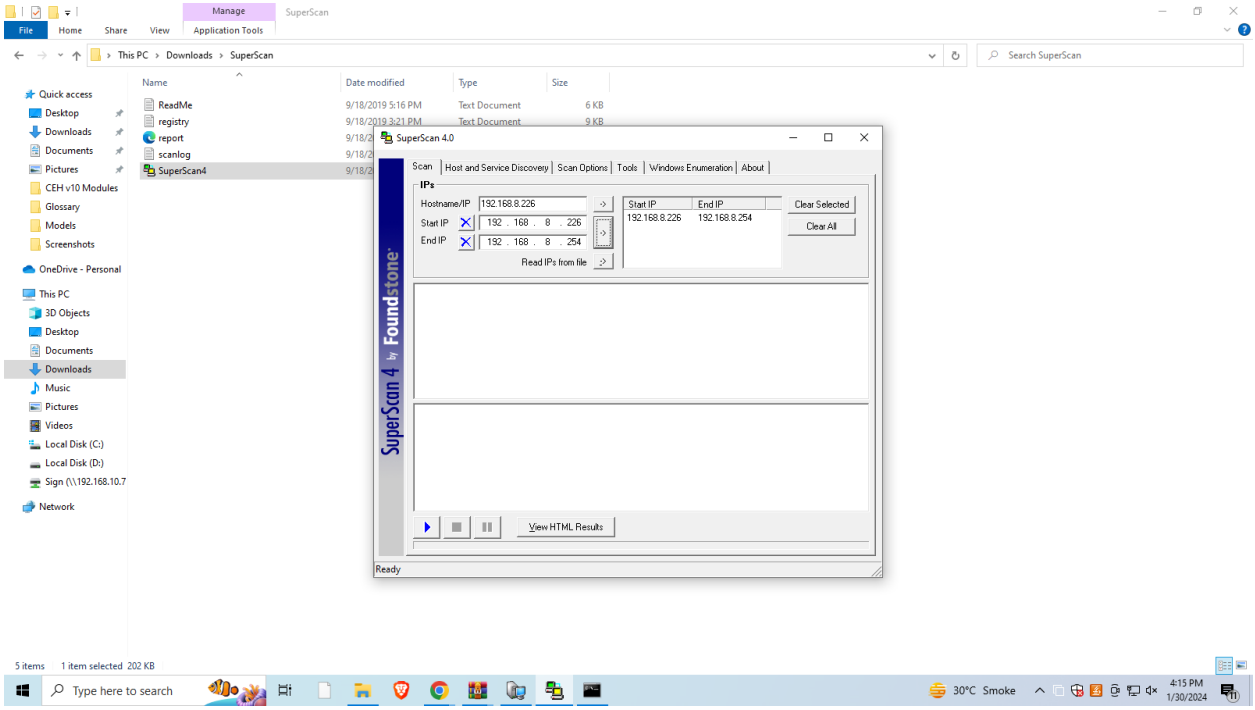

admin
Microsoft Network ...
Sahil - Chrome
ML PRACS
This PC
Oracle VM VirtualBox
Visual Studio Code
ipynb_che...
Network
Process Hacker 2
3
shraddha79
Recycle Bin
VMware vSphe...
R 4.3.2
Advanced Port Scanner
Control Panel
VMware Workstati...
fybsc72stat
tejas
Adobe Acrobat
10-Strike Network la...
LANState Pro
office
Google Chrome
Eclipse IDE for Enterpri...
1
tejas
MongoDB...
P4
2
SuperScan 4.0
Scan
Host and Service Discovery
Scan Options
Tools
Windows Enumeration
About
IPs
Windows Security Alert
Windows Defender Firewall has blocked some features of this app
Windows Defender Firewall has blocked some features of SuperScan 4 Beta 1 on all public and private networks.
Name: SuperScan 4 Beta 1
Publisher: Foundstone Inc.
Path: C:\users\admin\downloads\superscan-20240130t102323z-001\superscan\superscan4.exe
Allow SuperScan 4 Beta 1 to communicate on these networks:
Private networks, such as my home or work network
Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)
What are the risks of allowing an app through a firewall?
Allow access
Cancel
View HTML Results
SuperScan 4 by Foundstone
00:04
Saved log file
Live: 0
TCP open: 0
UDP open: 0
135/135 done
Type here to search
30°C Smoke
4:15 PM
1/30/2024

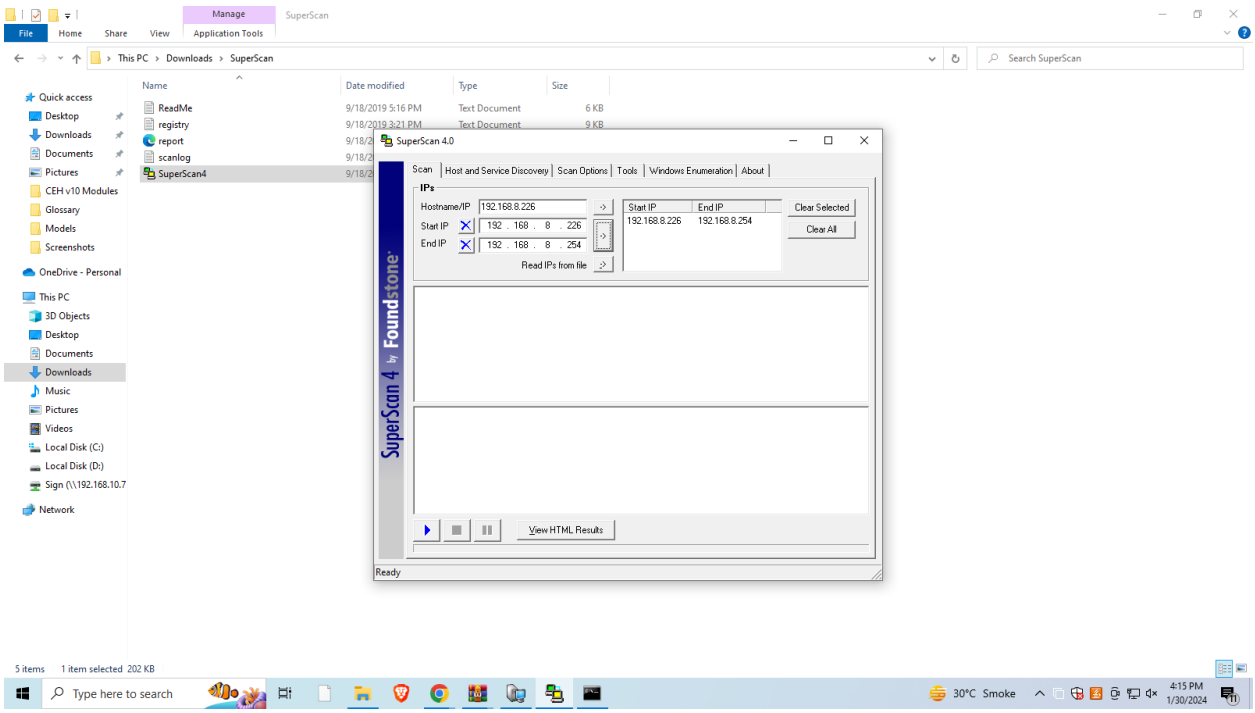

Manage
SuperScan
File
Home
Share
View
Application Tools
This PC > Downloads > SuperScan
Search SuperScan
Quick access
Desktop
Downloads
Documents
Pictures
CEH v10 Modules
Glossary
Models
Screenshots
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (D:)
Sign (\\192.168.10.7
Network
Name
Date modified
Type
Size
ReadMe
9/18/2019 5:16 PM
Text Document
6 KB
registry
9/18/2019 3:21 PM
Text Document
9 KB
report
scanlog
SuperScan4
SuperScan 4.0
Scan
Host and Service Discovery
Scan Options
Tools
Windows Enumeration
About
IPs
Hostname/IP
Start IP
End IP
Read IPs from file
Clear Selected
Clear All
View HTML Results
SuperScan 4 by Foundstone
Ready
5 items
1 item selected 202 KB
Type here to search
30°C Smoke
4:11 PM
1/30/2024

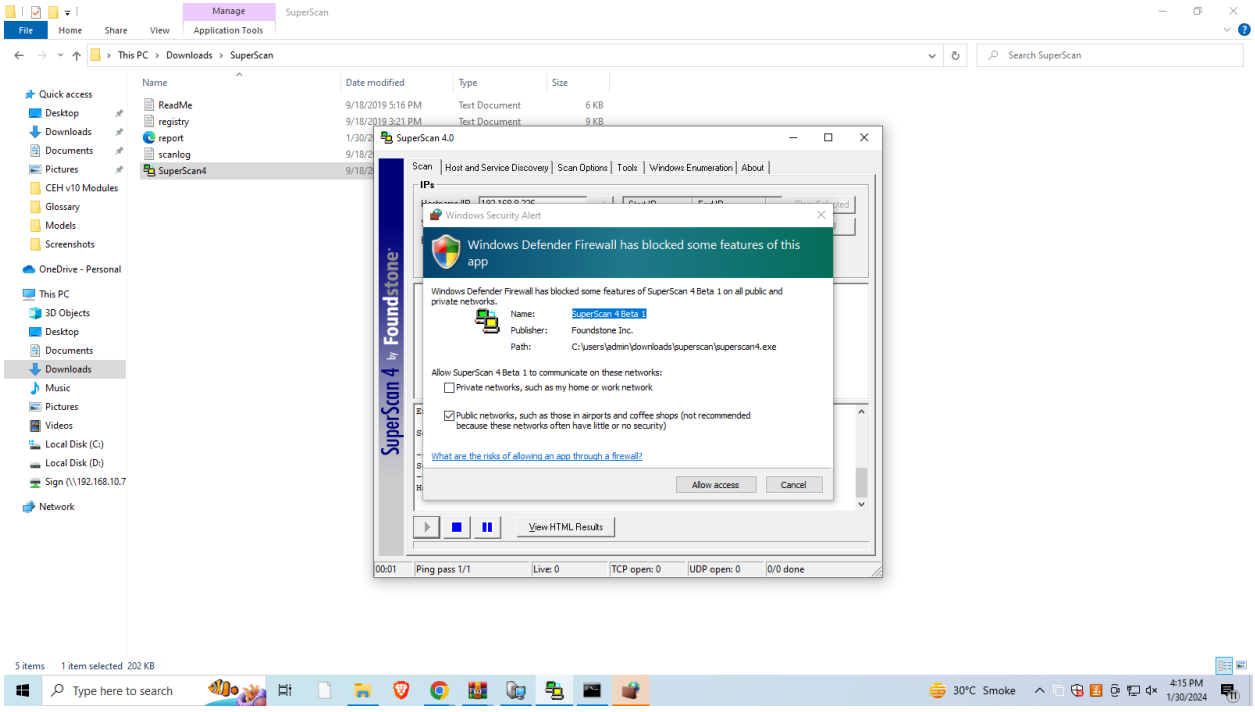

Manage
SuperScan
File
Home
Share
View
Application Tools
This PC › Downloads › SuperScan
Search SuperScan
Quick access
Desktop
Downloads
Documents
Pictures
CEH v10 Modules
Glossary
Models
Screenshots
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (D:)
Sign (\\192.168.10.7
Network
Name
Date modified
Type
Size
ReadMe
9/18/2019 5:16 PM
Text Document
6 KB
registry
9/18/2019 3:21 PM
Text Document
9 KB
report
scanlog
SuperScan4
SuperScan 4.0
Scan
Host and Service Discovery
Scan Options
Tools
Windows Enumeration
About
IPs
Hostname/IP
192.168.8.226
Start IP
End IP
Read IPs from file
Start IP
End IP
Clear Selected
Clear All
SuperScan 4 by Foundstone
View HTML Results
Ready
5 items
1 item selected 202 KB
Type here to search
30°C Smoke
4:13 PM
1/30/2024

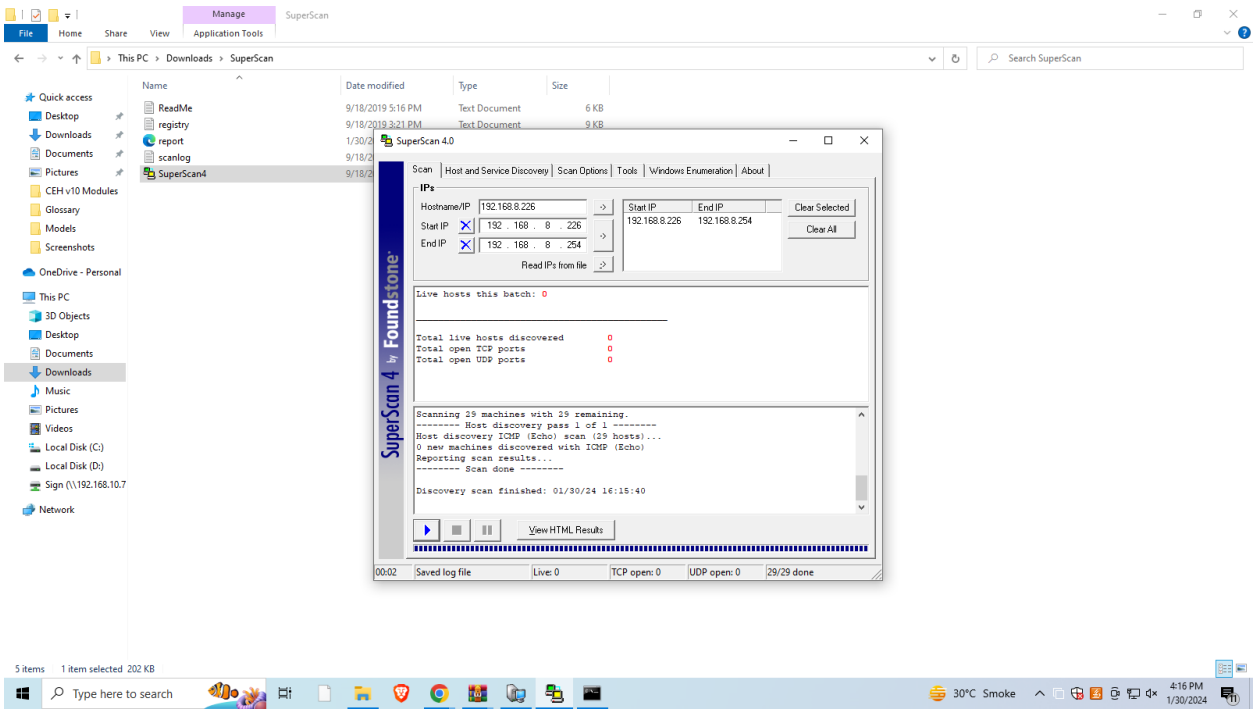

Manage
SuperScan
File
Home
Share
View
Application Tools
This PC › Downloads › SuperScan
Search SuperScan
Quick access
Desktop
Downloads
Documents
Pictures
CEH v10 Modules
Glossary
Models
Screenshots
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (D:)
Sign (\\192.168.10.7
Network
Name
Date modified
Type
Size
ReadMe
9/18/2019 5:16 PM
Text Document
6 KB
registry
9/18/2019 3:21 PM
Text Document
9 KB
report
scanlog
SuperScan4
SuperScan 4.0
Scan
Host and Service Discovery
Scan Options
Tools
Windows Enumeration
About
IPs
Hostname/IP
192.168.8.226
Start IP
192 . 168 . 8 . 226
End IP
Read IPs from file
Start IP
End IP
Clear Selected
Clear All
SuperScan 4 by Foundstone
View HTML Results
Ready
5 items
1 item selected 202 KB
Type here to search
30°C Smoke
4:14 PM
1/30/2024

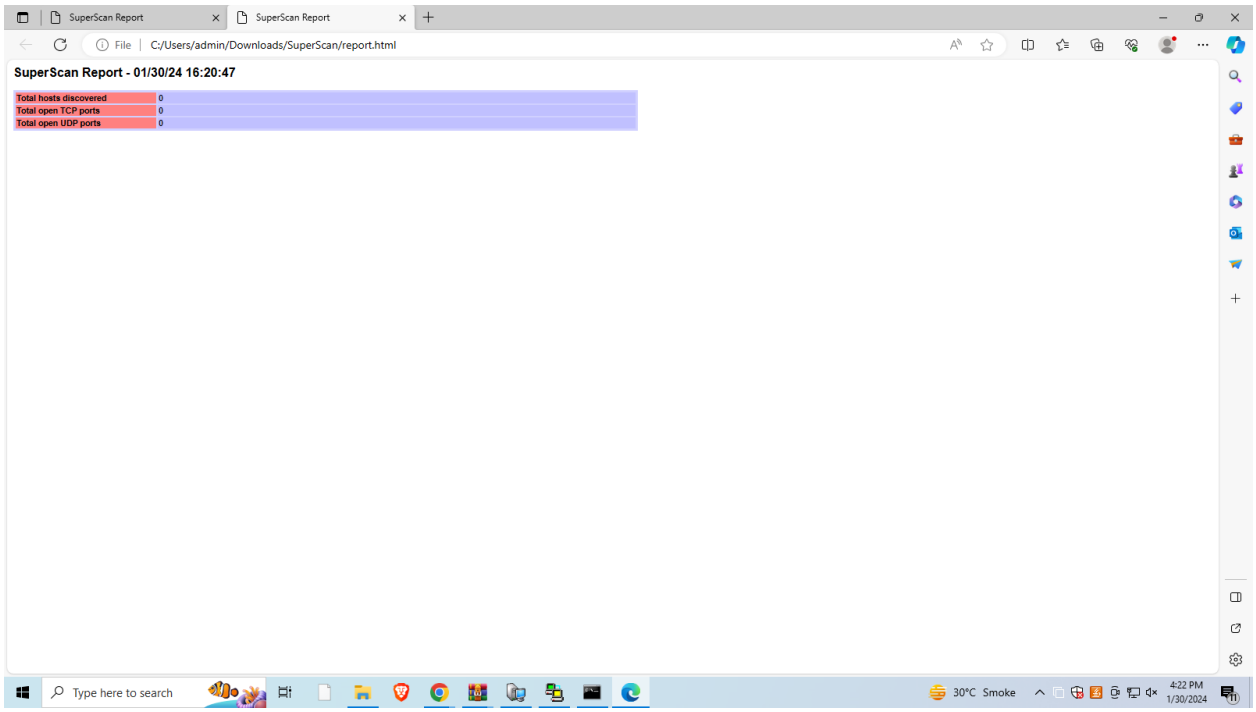

Manage
SuperScan
File
Home
Share
View
Application Tools
This PC › Downloads › SuperScan
Search SuperScan
Quick access
Desktop
Downloads
Documents
Pictures
CEH v10 Modules
Glossary
Models
Screenshots
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (D:)
Sign (\\192.168.10.7
Network
Name
Date modified
Type
Size
ReadMe
9/18/2019 5:16 PM
Text Document
6 KB
registry
9/18/2019 3:21 PM
Text Document
9 KB
report
scanlog
SuperScan4
SuperScan 4.0
Scan
Host and Service Discovery
Scan Options
Tools
Windows Enumeration
About
IPs
Hostname/IP
192.168.8.226
Start IP
192 . 168 . 8 . 226
End IP
192 . 168 . 8 . 254
Read IPs from file
Start IP
End IP
Clear Selected
Clear All
View HTML Results
Ready
SuperScan 4 by Foundstone
5 items
1 item selected 202 KB
Type here to search
30°C Smoke
4:14 PM
1/30/2024


Manage
SuperScan
File
Home
Share
View
Application Tools
This PC › Downloads › SuperScan
Search SuperScan
Quick access
Desktop
Downloads
Documents
Pictures
CEH v10 Modules
Glossary
Models
Screenshots
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (D:)
Sign (\\192.168.10.7
Network
Name
Date modified
Type
Size
ReadMe
9/18/2019 5:16 PM
Text Document
6 KB
registry
9/18/2019 3:21 PM
Text Document
9 KB
report
scanlog
SuperScan4
SuperScan 4.0
Scan
Host and Service Discovery
Scan Options
Tools
Windows Enumeration
About
IPs
Hostname/IP
192.168.8.226
Start IP
192 . 168 . 8 . 226
End IP
192 . 168 . 8 . 254
Read IPs from file
Start IP
End IP
192.168.8.226
192.168.8.254
Clear Selected
Clear All
View HTML Results
Ready
SuperScan 4 by Foundstone
5 items
1 item selected 202 KB
Type here to search
30°C Smoke
4:15 PM
1/30/2024


Manage
SuperScan
File
Home
Share
View
Application Tools
This PC › Downloads › SuperScan
Search SuperScan
Quick access
Desktop
Downloads
Documents
Pictures
CEH v10 Modules
Glossary
Models
Screenshots
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (D:)
Sign (\\192.168.10.7
Network
Name
Date modified
Type
Size
ReadMe
9/18/2019 5:16 PM
Text Document
6 KB
registry
9/18/2019 3:21 PM
Text Document
9 KB
report
scanlog
SuperScan4
SuperScan 4.0
Scan
Host and Service Discovery
Scan Options
Tools
Windows Enumeration
About
IPs
Hostname/IP
192.168.8.226
Start IP
192 . 168 . 8 . 226
End IP
192 . 168 . 8 . 254
Read IPs from file
Start IP
End IP
192.168.8.226
192.168.8.254
Clear Selected
Clear All
SuperScan 4 by Foundstone
View HTML Results
Ready
5 items
1 item selected 202 KB
Type here to search
30°C Smoke
4:15 PM
1/30/2024


Manage
SuperScan
File
Home
Share
View
Application Tools
This PC › Downloads › SuperScan
Search SuperScan
Quick access
Desktop
Downloads
Documents
Pictures
CEH v10 Modules
Glossary
Models
Screenshots
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (D:)
Sign (\\192.168.10.7
Network
Name
Date modified
Type
Size
ReadMe
9/18/2019 5:16 PM
Text Document
6 KB
registry
9/18/2019 3:21 PM
Text Document
9 KB
report
1/30/2
scanlog
SuperScan4
SuperScan 4.0
Scan
Host and Service Discovery
Scan Options
Tools
Windows Enumeration
About
IPs
Windows Security Alert
Windows Defender Firewall has blocked some features of this app
Windows Defender Firewall has blocked some features of SuperScan 4 Beta 1 on all public and private networks.
Name:
SuperScan 4 Beta 1
Publisher:
Foundstone Inc.
Path:
C:\users\admin\downloads\superscan\superscan4.exe
Allow SuperScan 4 Beta 1 to communicate on these networks:
Private networks, such as my home or work network
Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)
What are the risks of allowing an app through a firewall?
Allow access
Cancel
SuperScan 4 by Foundstone
View HTML Results
00:01
Ping pass 1/1
Live: 0
TCP open: 0
UDP open: 0
0/0 done
5 items
1 item selected 202 KB
Type here to search
30°C Smoke
4:15 PM
1/30/2024

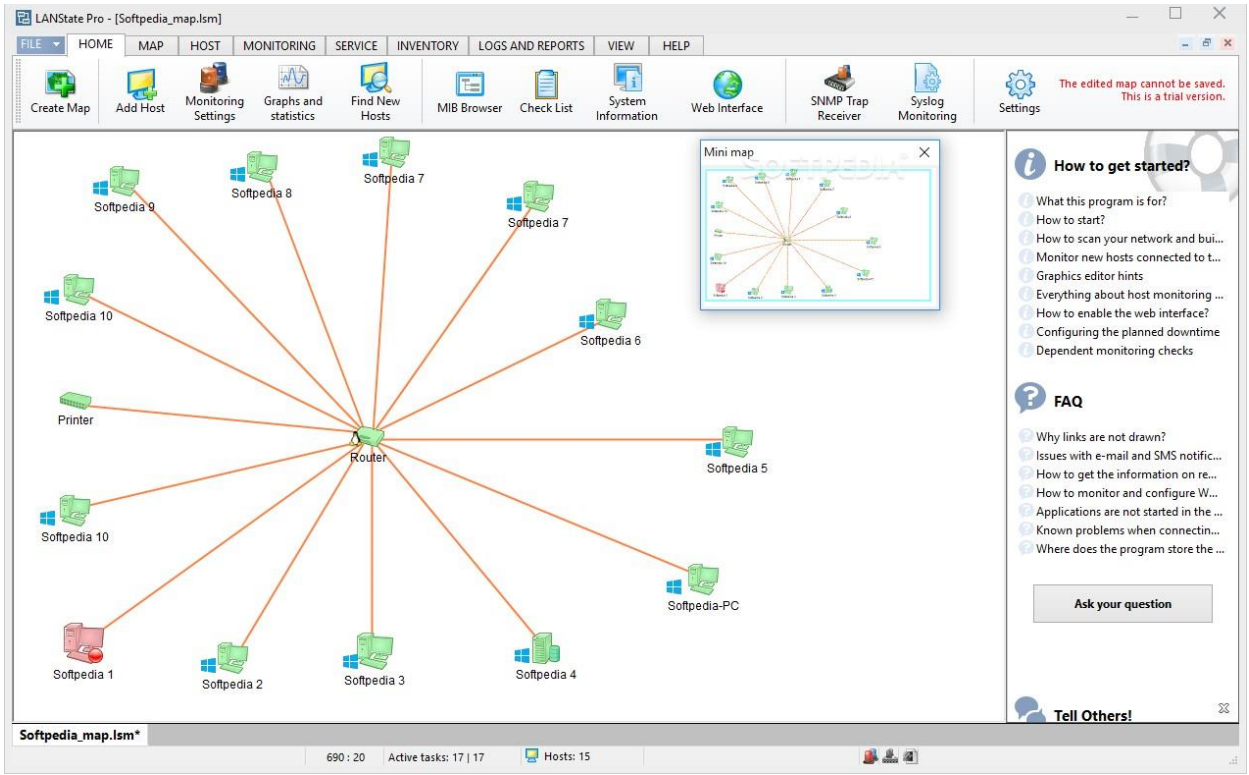

SuperScan 4.0
Scan
Host and Service Discovery
Scan Options
Tools
Windows Enumeration
About
IPs
Hostname/IP 192.168.8.226
Start IP 192 . 168 . 8 . 226
End IP 192 . 168 . 8 . 254
Read IPs from file
Start IP
End IP
192.168.8.226
192.168.8.254
Clear Selected
Clear All
Live hosts this batch: 0
Total live hosts discovered 0
Total open TCP ports 0
Total open UDP ports 0
Scanning 29 machines with 29 remaining.
-------- Host discovery pass 1 of 1 --------
Host discovery ICMP (Echo) scan (29 hosts)...
0 new machines discovered with ICMP (Echo)
Reporting scan results...
-------- Scan done --------
Discovery scan finished: 01/30/24 16:15:40
View HTML Results
00:02
Saved log file
Live: 0
TCP open: 0
UDP open: 0
29/29 done
SuperScan 4 by Foundstone
ReadMe
registry
report
scanlog
SuperScan4
5 items
1 item selected 202 KB
Type here to search
30°C Smoke
4:16 PM
1/30/2024


SuperScan Report
SuperScan Report
File C:/Users/admin/Downloads/SuperScan/report.html
SuperScan Report - 01/30/24 16:20:47
Total hosts discovered 0
Total open TCP ports 0
Total open UDP ports 0
Type here to search
30°C Smoke
4:22 PM
1/30/2024

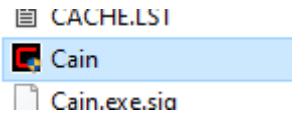
Practical No. 07 - Perform Network Mapping

LANState is a simple network topology mapping, host monitoring, and management program.

Monitor the service availability. Manage servers, computers, switches, and otherdevices easier using the graphic map. Access devices' properties, RDP, web UI faster.

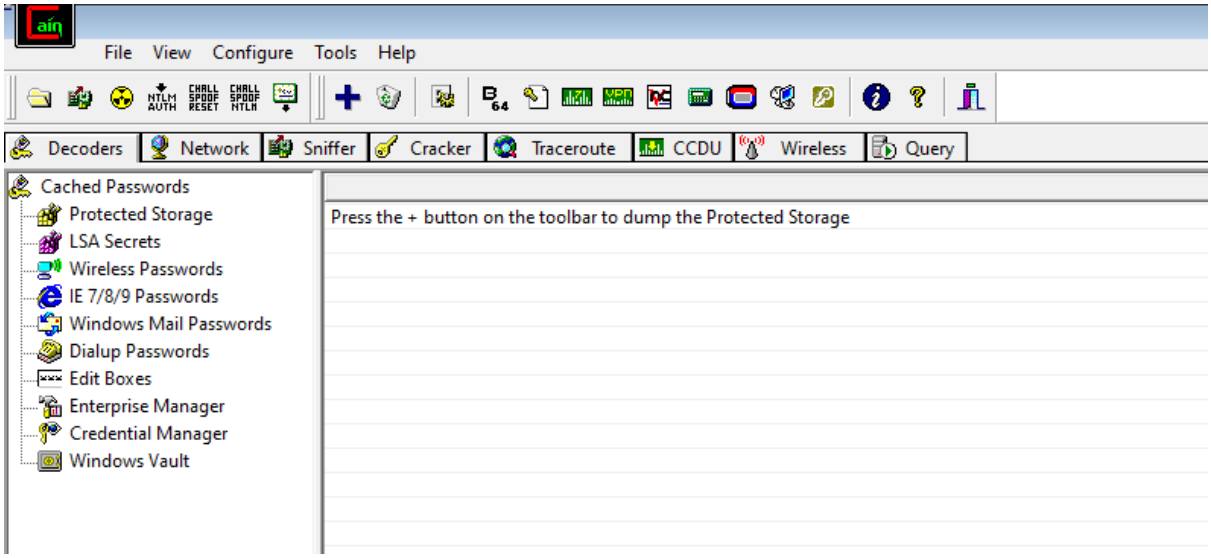


Practical No. 08 - Perform Brute Force Attack

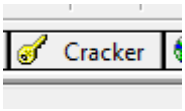


Install this in E: drive

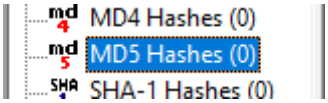
After installation it looks likes this.



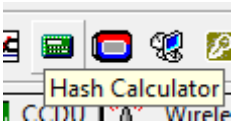
Then go to Cracker



Select this

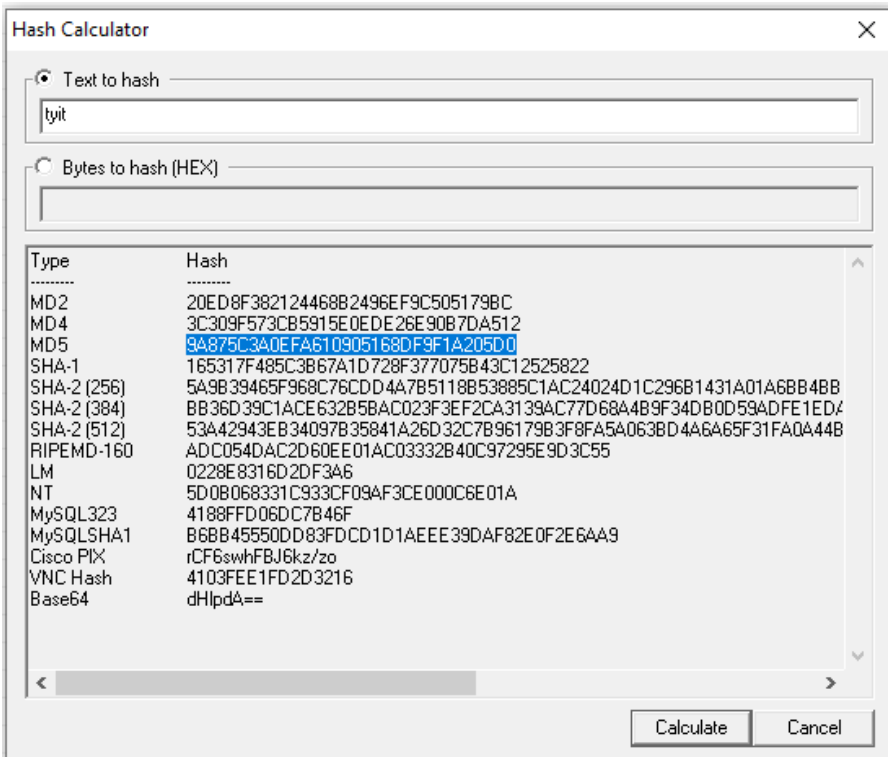


Click hash calculator

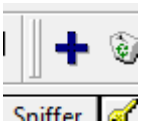


Then write any text and click calculate.

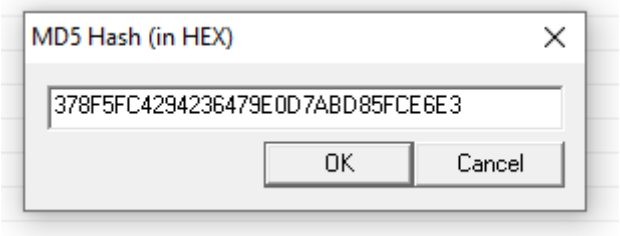
Copy MD5 hash value (ciphered text) then click cancel.



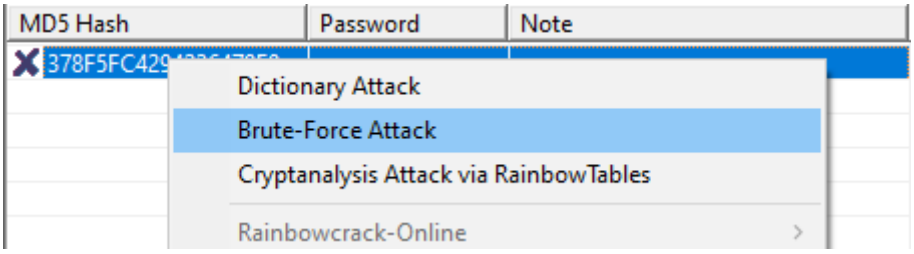
Click on this



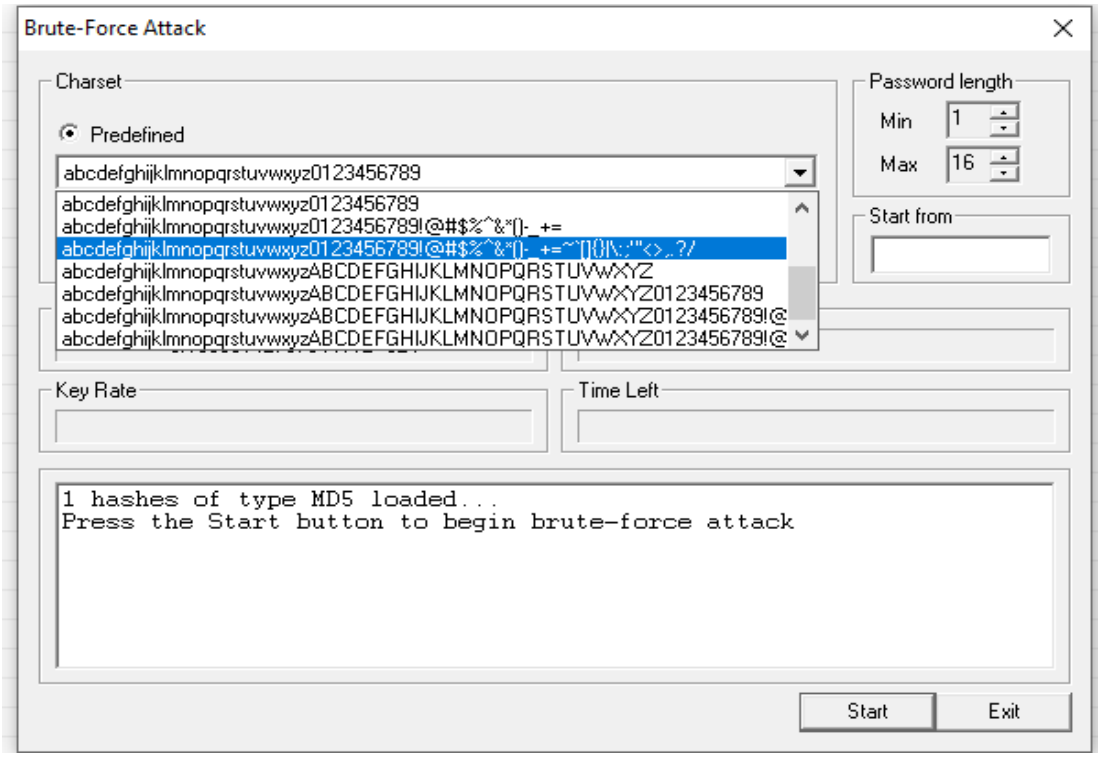
Paste the copied hash value then click OK



Right click on this and select this.



Then



Then click start

The text will be seen here