PXS HEXID
MUS UNI NON FIDIT ANTRO

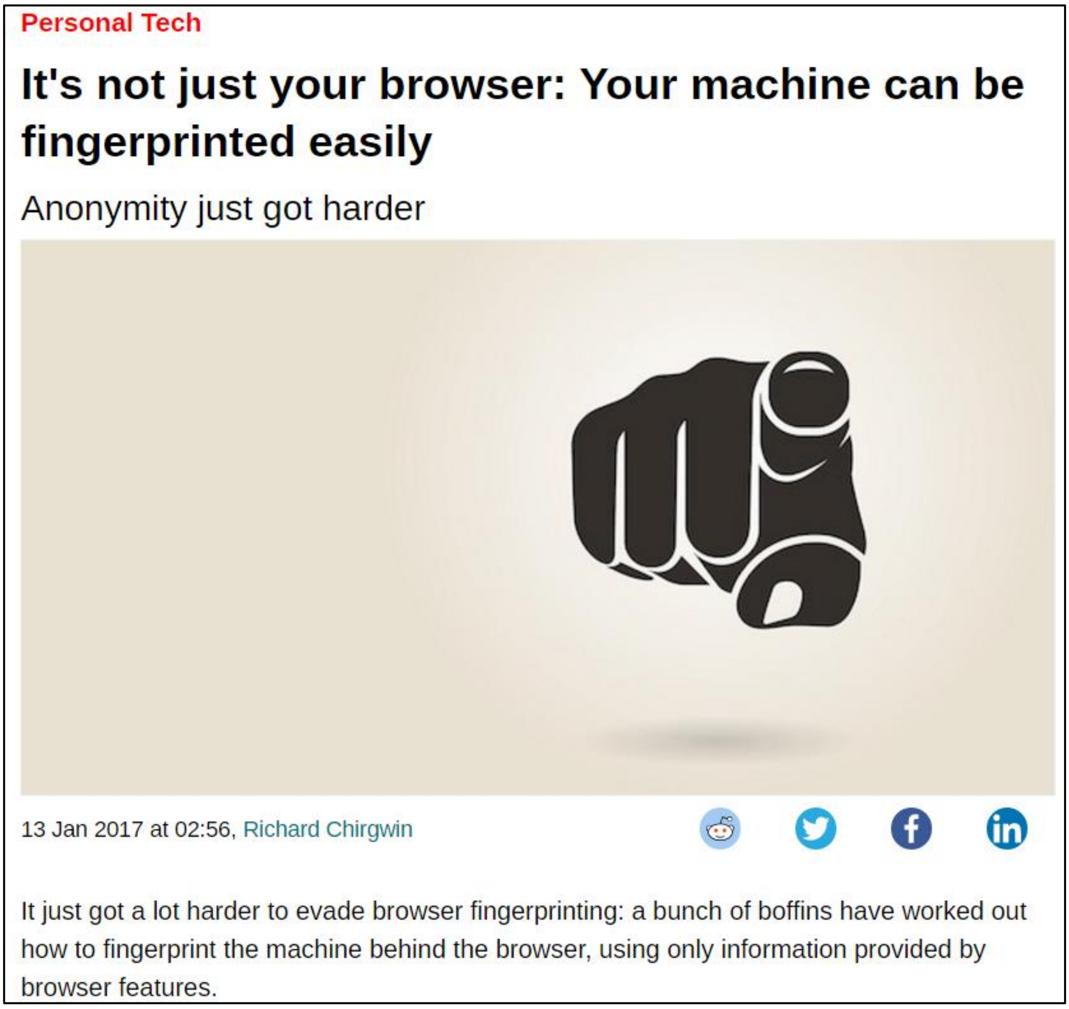
HEXID:

Enumeration.

These materials were developed to support the Hacking Explained and Intrusion Detection ("HEXID") course at the Telindus High-Tech Institute ("THTI"), the John Cordier Academy ("JCA"), the Proximus ICT Academy ("PIA"), the Proximus Corporate University ("PCU") and "Learning@Proximus" since 2001. All materials were build and created within the related and dedicated lab environment.These materials can only be used for educational purposes and cyber security awareness. By using these materials, you confirm that the information obtained will be used in an ethical and responsible manner. All the information is offered "AS IS", without any warranty of any kind and disclaiming any liability for damages resulting this information.

1. ENUMERATION.

- **Case:** "It's not just your browser: your machine can be fingerprinted easily", The Register, 2017.
- Reference: https://www.theregister.co.uk/2017/01/13/its_not_just_your_browser_your_machine_can_be_fingerprinted_easily/.



Personal Tech

It's not just your browser: Your machine can be fingerprinted easily

Anonymity just got harder

13 Jan 2017 at 02:56, Richard Chirgwin

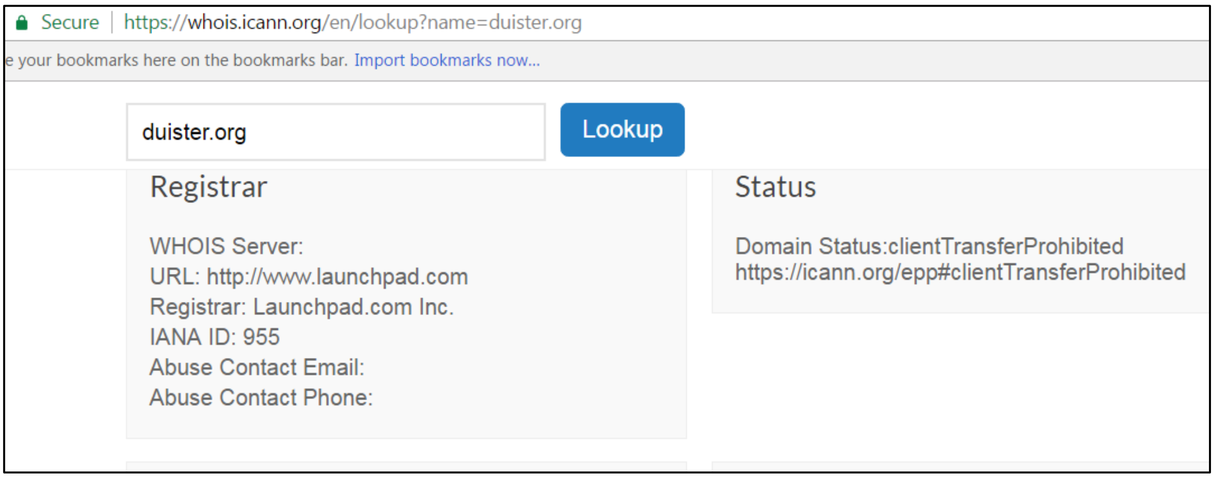
It just got a lot harder to evade browser fingerprinting: a bunch of boffins have worked out how to fingerprint the machine behind the browser, using only information provided by browser features.

- **Requires:** "HEXID_GW", "HEXID_R1", "HEXID_R2", "HEXID_SERVICES", "HEXID_METASPLOITABLE", "HEXID_WIN7", "HEXID_WIN10", "HEXID_KALI_20171".

- **Goal:** consult and execute some classic information gathering techniques.

Sensitivity: Unrestricted

- Using a web browser:
  - Use Google to find some online "WHOIS" lookup sites to fingerprint some basic information about a website. Take a closer look at the WHOIS information where available. It might be that some providers will shield their information as a privacy protection.



Secure | https://whois.icann.org/en/lookup?name=duister.org

e your bookmarks here on the bookmarks bar. Import bookmarks now...

duister.org

Lookup

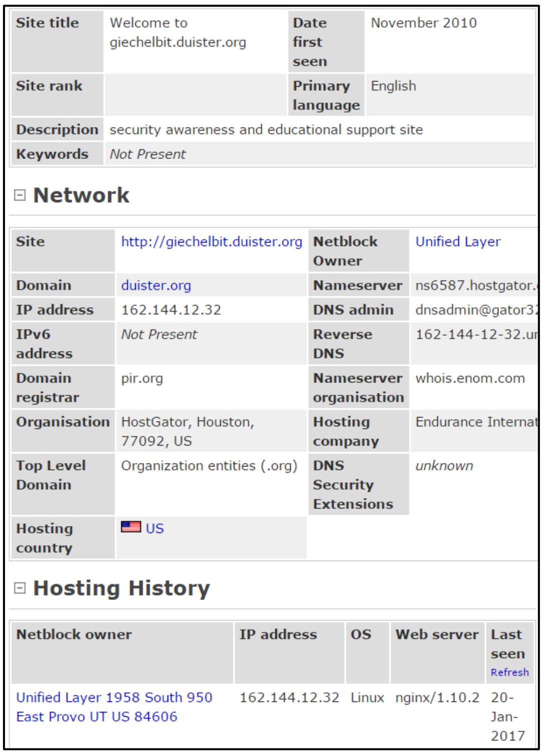
Registrar

WHOIS Server:
URL: http://www.launchpad.com
Registrar: Launchpad.com Inc.
IANA ID: 955
Abuse Contact Email:
Abuse Contact Phone:

Status

Domain Status:clientTransferProhibited
https://icann.org/epp#clientTransferProhibited

  - Visit the RIPE website at "http://www.ripe.net" and "https://apps.db.ripe.net/search/query.html", try to fingerprint some information both IP address information and DNS information.
  - Visit the website "https://www.netcraft.com" to browse around for information. Visit the URL "http://toolbar.netcraft.com/site_report?" to have access to the site reports that have been made available.
    Pay attention to hosters, whois information, IP addresses, Operating systems, web server information and more.



Site title	Welcome to giechelbit.duister.org	**Date first seen**	November 2010
Site rank		**Primary language**	English
Description	security awareness and educational support site		
Keywords	*Not Present*		

⊟ **Network**

Site	http://giechelbit.duister.org	**Netblock Owner**	Unified Layer
Domain	duister.org	**Nameserver**	ns6587.hostgator.
IP address	162.144.12.32	**DNS admin**	dnsadmin@gator3
IPv6 address	*Not Present*	**Reverse DNS**	162-144-12-32.u
Domain registrar	pir.org	**Nameserver organisation**	whois.enom.com
Organisation	HostGator, Houston, 77092, US	**Hosting company**	Endurance Internat
Top Level Domain	Organization entities (.org)	**DNS Security Extensions**	*unknown*
Hosting country	US		

⊟ **Hosting History**

Netblock owner	IP address	OS	Web server	Last seen Refresh
Unified Layer 1958 South 950 East Provo UT US 84606	162.144.12.32	Linux	nginx/1.10.2	20-Jan-2017

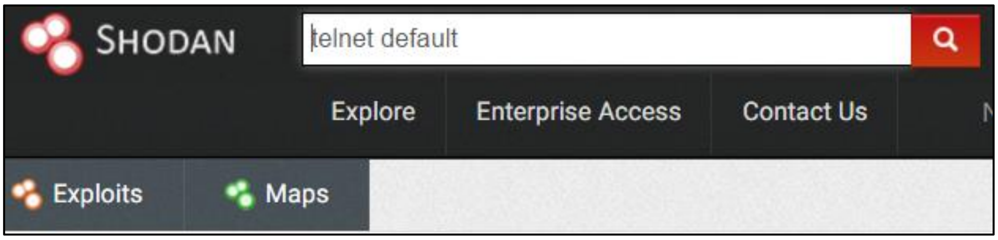
Sensitivity: Unrestricted

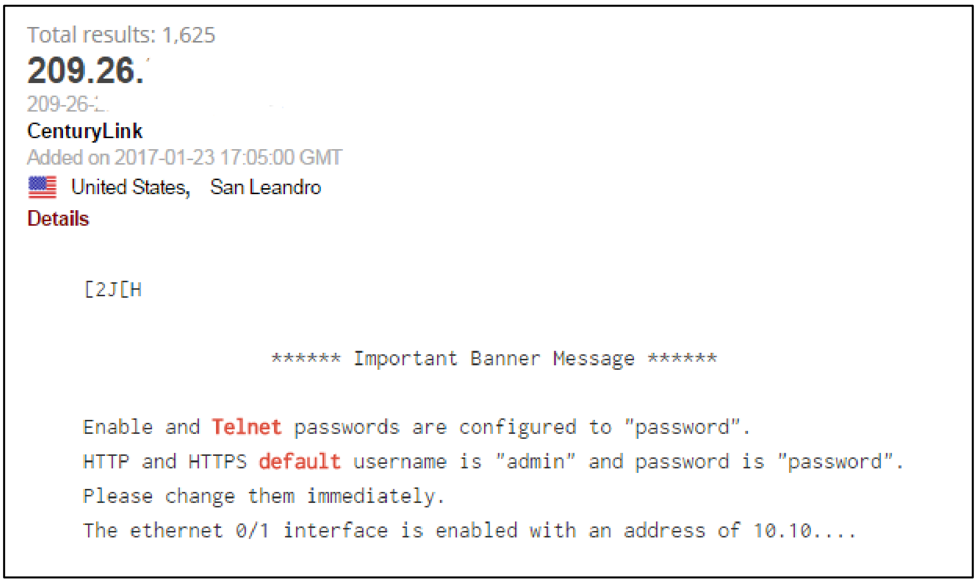
- Visit the a Google Hacking Database (GHD) and browse around. Do not click on the displayed links and queries.
  Example databases can be found on:
  - "https://www.exploit-db.com/google-hacking-database/".
  - "http://www.hackersforcharity.org/ghdb/".

  - Try to find a query in order to perform a "portscan" by using Google.

- Visit website defacement sites:
  - "http://www.zone-h.org/archive?zh=1".
  - "http://attrition.org/mirror/".

- Visit the Shodan website on "https://www.shodan.io" and check some of the examples.





Total results: 1,625

209.26.

209-26-

CenturyLink

Added on 2017-01-23 17:05:00 GMT

United States, San Leandro

Details

```
[2J[H

                  ****** Important Banner Message ******

Enable and Telnet passwords are configured to "password".
HTTP and HTTPS default username is "admin" and password is "password".
Please change them immediately.
The ethernet 0/1 interface is enabled with an address of 10.10....
```

  - Note: general rule, do not attempt to access or approach any location outside of your assigned lab network.

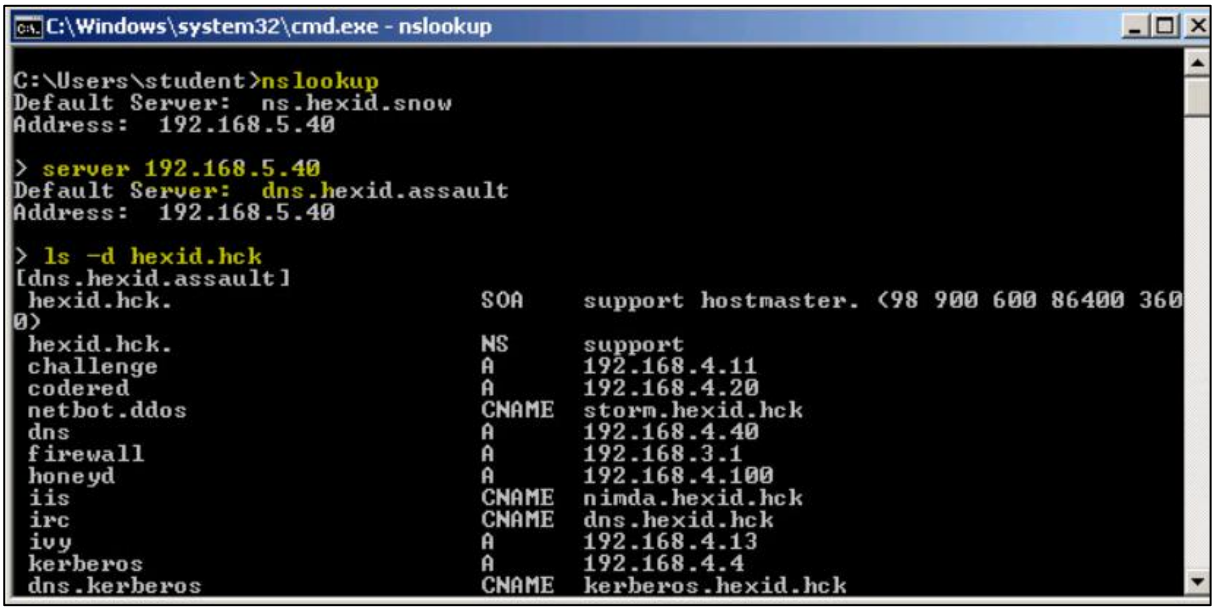
- Visit the websites:
  - https://scans.io.
  - https://censys.io.
  - http://www.zoomeye.org.
  - http://web.archive.org
  - https://www.usersearch.org
  - http://webmii.com.

Sensitivity: Unrestricted

  - Consult jobsites like Monster and LinkedIn to check the information that is leaked through job offers.

  - Use Google, to find some websites that allow you to perform online traceroutes.

- On "HEXID_WIN7":
  - Login with the credentials "student"/"student".
  - Open a DOS prompt and perform a traceroute operation to the IP address 192.168.1.1. The command to be used is "tracert 192.168.1.1".
  - In your DOS prompt, attempt to perform a zone transfer using "nslookup" for the domain "hexid.hck".

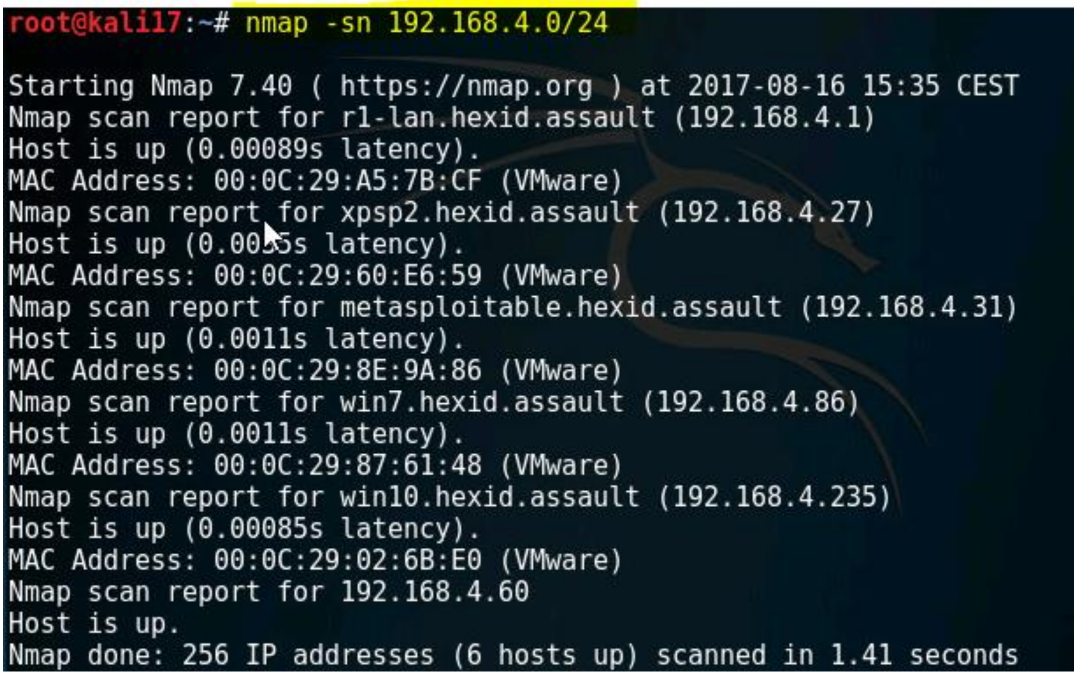


```
C:\Users\student>nslookup
Default Server:  ns.hexid.snow
Address:  192.168.5.40

> server 192.168.5.40
Default Server:  dns.hexid.assault
Address:  192.168.5.40

> ls -d hexid.hck
[dns.hexid.assault]
 hexid.hck.                     SOA    support hostmaster. (98 900 600 86400 360
0)
 hexid.hck.                     NS     support
 challenge                      A      192.168.4.11
 codered                        A      192.168.4.20
 netbot.ddos                    CNAME  storm.hexid.hck
 dns                            A      192.168.4.40
 firewall                       A      192.168.3.1
 honeyd                         A      192.168.4.100
 iis                            CNAME  nimda.hexid.hck
 irc                            CNAME  dns.hexid.hck
 ivy                            A      192.168.4.13
 kerberos                       A      192.168.4.4
 dns.kerberos                   CNAME  kerberos.hexid.hck
```

- On "HEXID_KALI_20171":

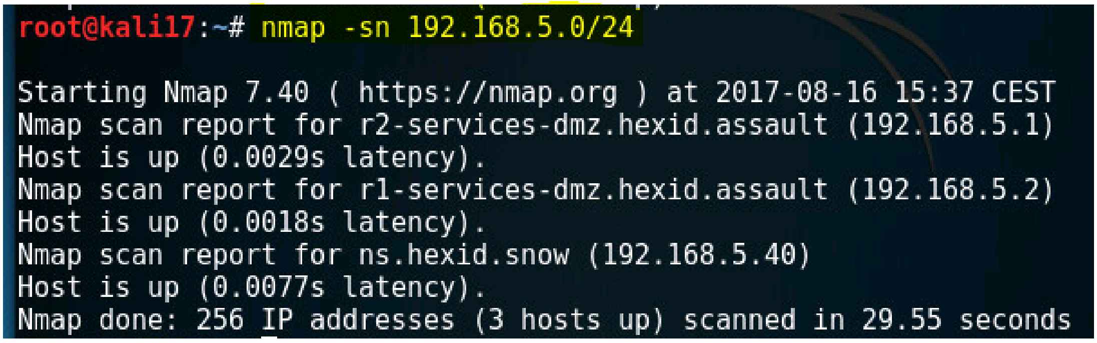
Sensitivity: Unrestricted

- Login with the credentials "root"/"student".
- Open a new shell to start scanning with Nmap.
- With Nmap, discover live hosts on the target networks 192.168.4.0/24 and 192.168.5.0/24 using a basic ping scan.
    - The options "-sn" disables port scanning - but leaves the discovery phase enabled. This will make Nmap perform a ping sweep on the netwerk.
    - Command: "#nmap -sn 192.168.4.0/24".



```
root@kali17:~# nmap -sn 192.168.4.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 15:35 CEST
Nmap scan report for r1-lan.hexid.assault (192.168.4.1)
Host is up (0.00089s latency).
MAC Address: 00:0C:29:A5:7B:CF (VMware)
Nmap scan report for xpsp2.hexid.assault (192.168.4.27)
Host is up (0.0035s latency).
MAC Address: 00:0C:29:60:E6:59 (VMware)
Nmap scan report for metasploitable.hexid.assault (192.168.4.31)
Host is up (0.0011s latency).
MAC Address: 00:0C:29:8E:9A:86 (VMware)
Nmap scan report for win7.hexid.assault (192.168.4.86)
Host is up (0.0011s latency).
MAC Address: 00:0C:29:87:61:48 (VMware)
Nmap scan report for win10.hexid.assault (192.168.4.235)
Host is up (0.00085s latency).
MAC Address: 00:0C:29:02:6B:E0 (VMware)
Nmap scan report for 192.168.4.60
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.41 seconds
```

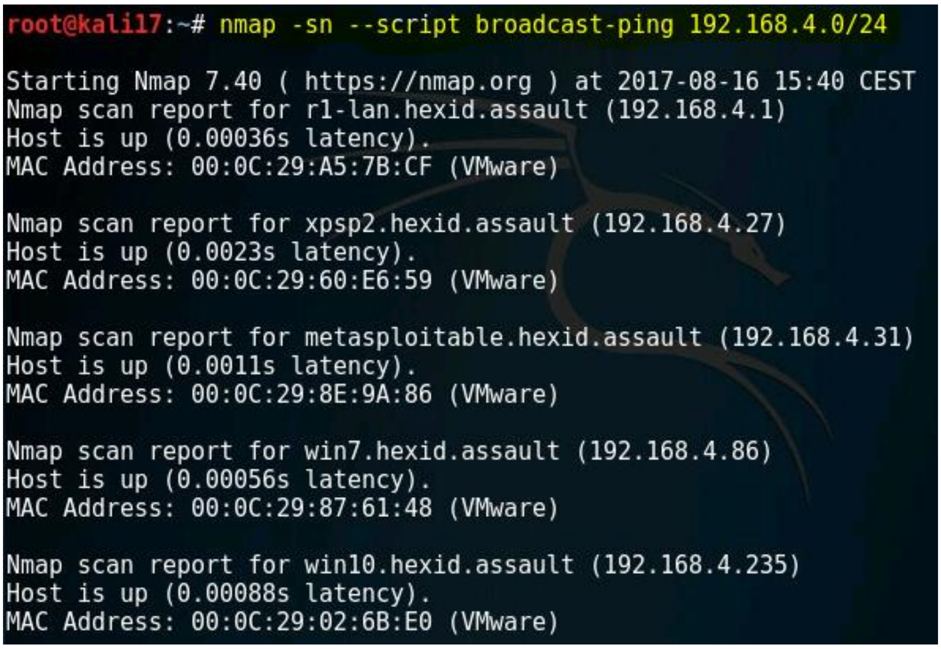
- Command: "#nmap -sn 192.168.5.0/24".



```
root@kali17:~# nmap -sn 192.168.5.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 15:37 CEST
Nmap scan report for r2-services-dmz.hexid.assault (192.168.5.1)
Host is up (0.0029s latency).
Nmap scan report for r1-services-dmz.hexid.assault (192.168.5.2)
Host is up (0.0018s latency).
Nmap scan report for ns.hexid.snow (192.168.5.40)
Host is up (0.0077s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 29.55 seconds
```

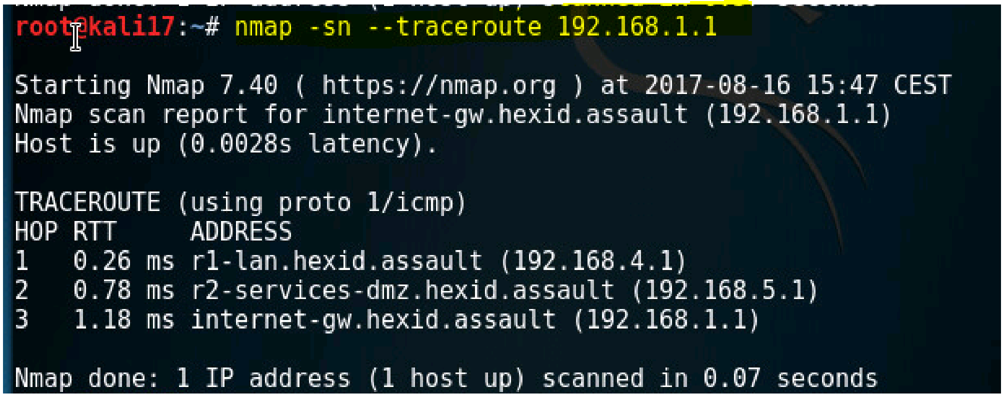
Sensitivity: Unrestricted

- With Nmap, perform a broadcast-ping scan of the 192.168.4.0/24 network, using a NSE script.
  - Command: "#nmap -sn --script broadcast-ping 192.168.4.0/24".



```
root@kali17:~# nmap -sn --script broadcast-ping 192.168.4.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 15:40 CEST
Nmap scan report for r1-lan.hexid.assault (192.168.4.1)
Host is up (0.00036s latency).
MAC Address: 00:0C:29:A5:7B:CF (VMware)

Nmap scan report for xpsp2.hexid.assault (192.168.4.27)
Host is up (0.0023s latency).
MAC Address: 00:0C:29:60:E6:59 (VMware)

Nmap scan report for metasploitable.hexid.assault (192.168.4.31)
Host is up (0.0011s latency).
MAC Address: 00:0C:29:8E:9A:86 (VMware)

Nmap scan report for win7.hexid.assault (192.168.4.86)
Host is up (0.00056s latency).
MAC Address: 00:0C:29:87:61:48 (VMware)

Nmap scan report for win10.hexid.assault (192.168.4.235)
Host is up (0.00088s latency).
MAC Address: 00:0C:29:02:6B:E0 (VMware)
```

- With Nmap, perform a traceroute to the IP 192.168.1.1 in the lab network.
  - Command: "#nmap -sn --traceroute 192.168.1.1".

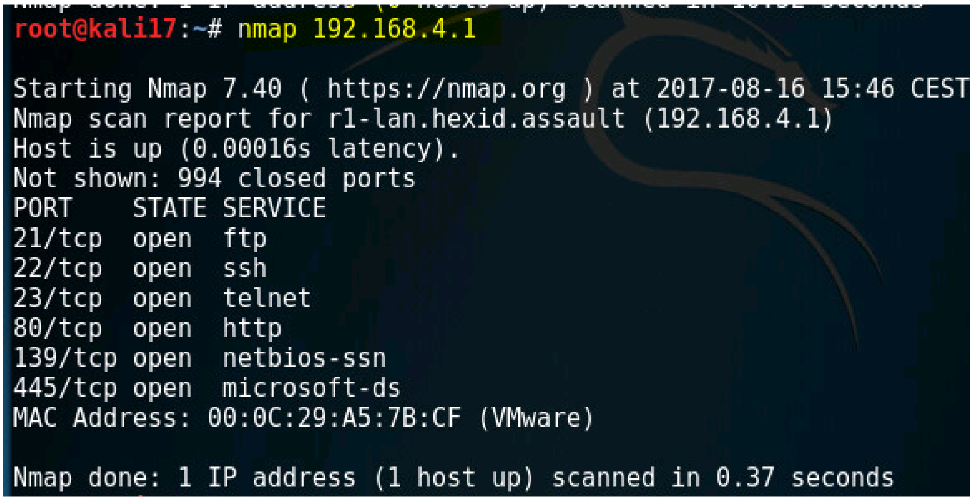


```
root@kali17:~# nmap -sn --traceroute 192.168.1.1

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 15:47 CEST
Nmap scan report for internet-gw.hexid.assault (192.168.1.1)
Host is up (0.0028s latency).

TRACEROUTE (using proto 1/icmp)
HOP RTT     ADDRESS
1   0.26 ms r1-lan.hexid.assault (192.168.4.1)
2   0.78 ms r2-services-dmz.hexid.assault (192.168.5.1)
3   1.18 ms internet-gw.hexid.assault (192.168.1.1)

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

- With Nmap, perform a default scan of the hosts "HEXID_METASPLOITABLE", "HEXID_SERVICES", "HEXID_WIN7", "HEXID_WIN10", "HEXID_R1".
  - Command: "#nmap 192.168.4.1" ("HEXID_R1").
  - Command: "#nmap 192.168.4.86" ("HEXID_WIN7").
  - Command: "#nmap 192.168.5.40" ("HEXID_SERVICES").
  - Command: "#nmap 192.168.4.31" ("HEXID_METASPOITABLE").

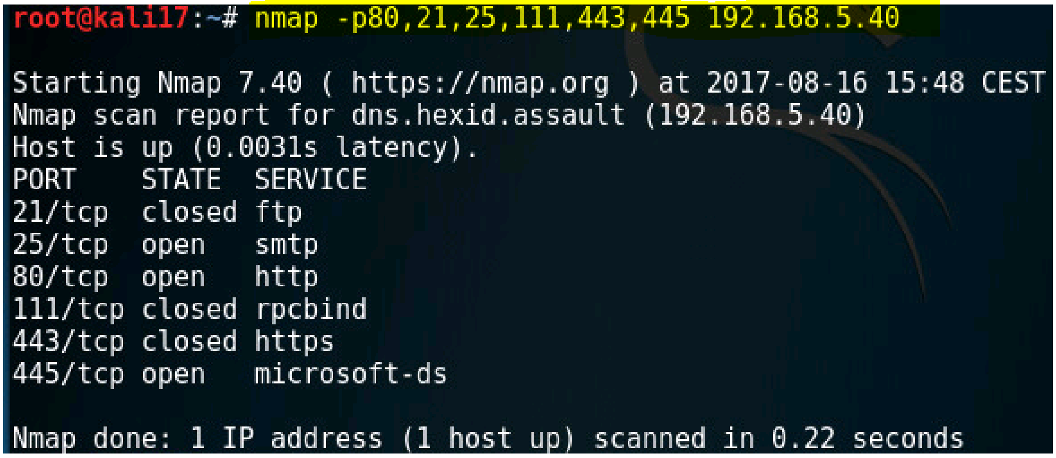
Sensitivity: Unrestricted

    - Command: "#nmap 192.168.4.235" ("HEXD_WIN10").



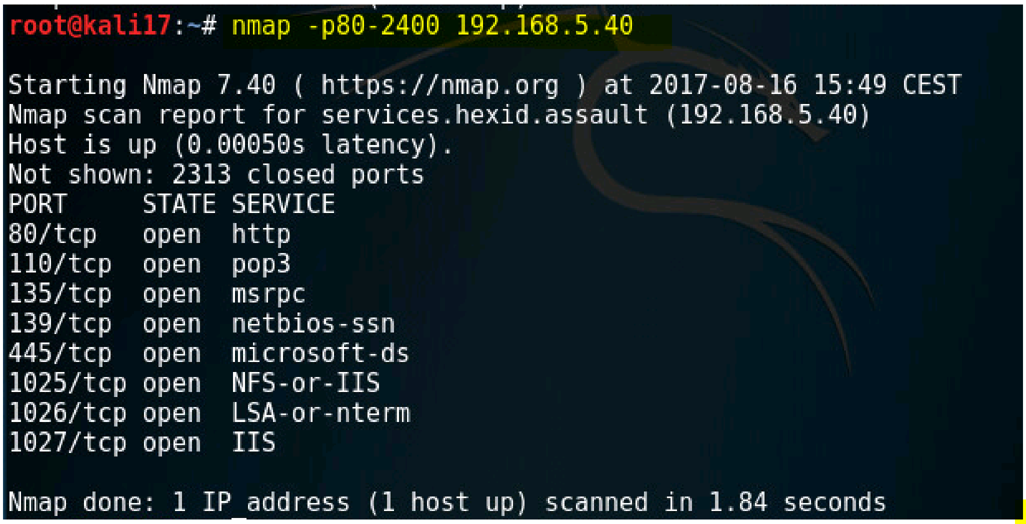
```
root@kali17:~# nmap 192.168.4.1

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 15:46 CEST
Nmap scan report for r1-lan.hexid.assault (192.168.4.1)
Host is up (0.00016s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:A5:7B:CF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

- With Nmap, scan a specific port range on "HEXID_SERVICES", scan the ports 80, 21, 25, 111, 443,445/TCP.
    - Command: "#nmap -p80,21,25,111,443,445 192.168.5.40".



```
root@kali17:~# nmap -p80,21,25,111,443,445 192.168.5.40

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 15:48 CEST
Nmap scan report for dns.hexid.assault (192.168.5.40)
Host is up (0.0031s latency).
PORT    STATE  SERVICE
21/tcp  closed ftp
25/tcp  open   smtp
80/tcp  open   http
111/tcp closed rpcbind
443/tcp closed https
445/tcp open   microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

- With NMap, scan a specific port rnage on "HEXID_SERVICES", scan the port range 80 to 2400/TCP.

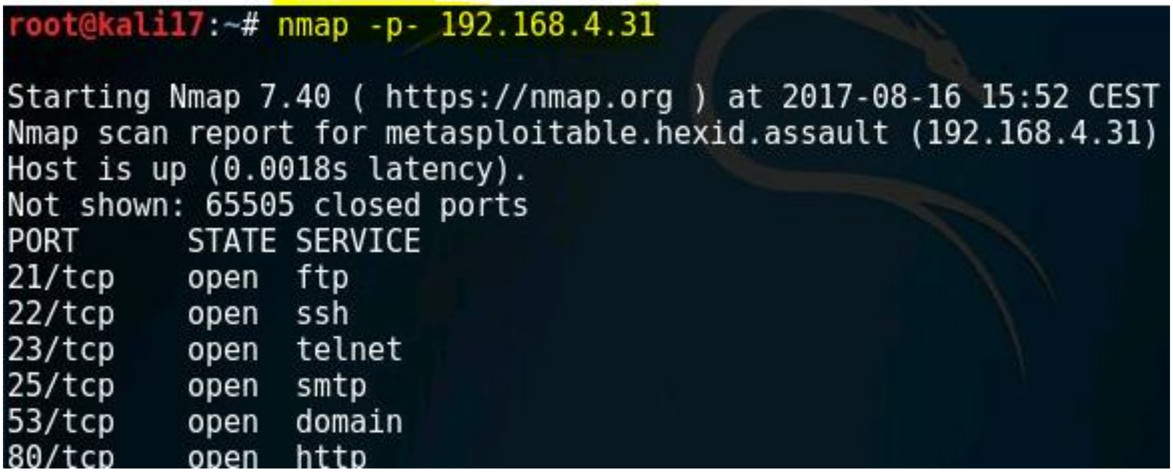


```
root@kali17:~# nmap -p80-2400 192.168.5.40

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 15:49 CEST
Nmap scan report for services.hexid.assault (192.168.5.40)
Host is up (0.00050s latency).
Not shown: 2313 closed ports
PORT     STATE SERVICE
80/tcp   open  http
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS

Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
```

    - Command: "#nmap -p80-2400 192.168.5.40".

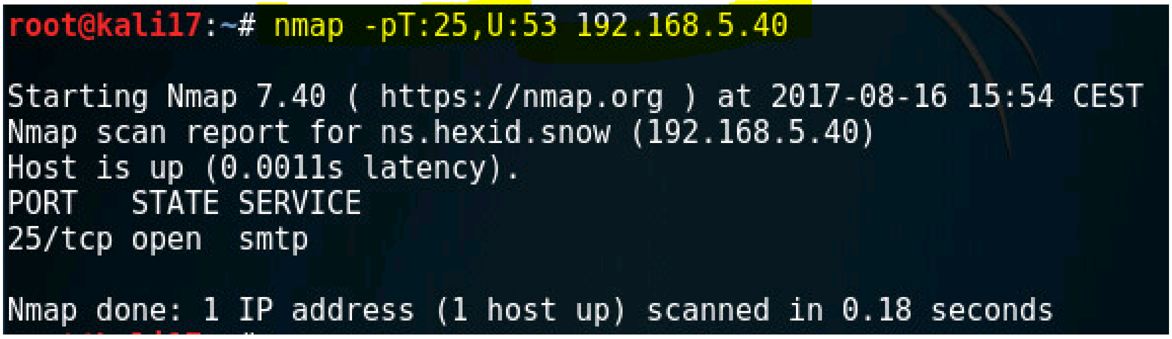
Sensitivity: Unrestricted

- Perform a default scan of all ports on "HEXID_METASPLOITABLE".
  - Command: "#nmap -p- 192.168.4.31".



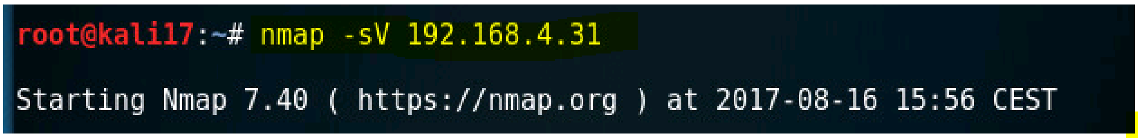
```
root@kali17:~# nmap -p- 192.168.4.31

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 15:52 CEST
Nmap scan report for metasploitable.hexid.assault (192.168.4.31)
Host is up (0.0018s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
```

- Peform a scan of port 25/TCP and port 53/UDP on "HEXID_SERVICES".
  - Command: "#nmap -pT:25,U:53 192.168.5.40".



```
root@kali17:~# nmap -pT:25,U:53 192.168.5.40

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 15:54 CEST
Nmap scan report for ns.hexid.snow (192.168.5.40)
Host is up (0.0011s latency).
PORT   STATE SERVICE
25/tcp open  smtp

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

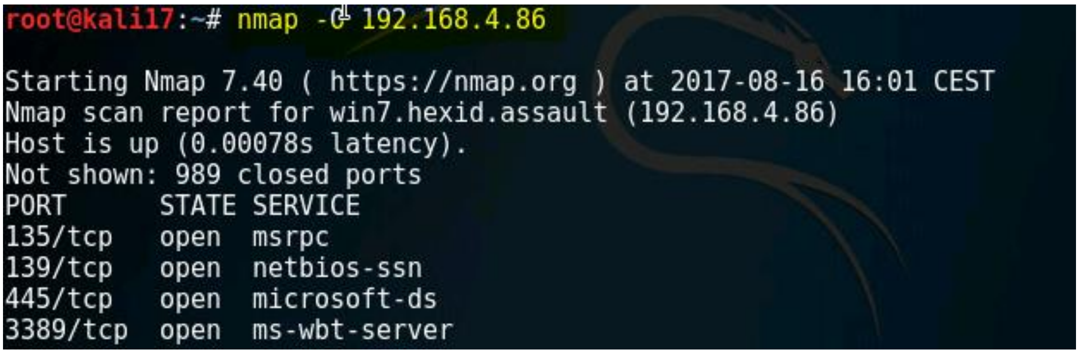
- Enable service detection on add the "-sV" option to scan all the ports on "HEXID_METASPLOITABLE".



```
root@kali17:~# nmap -sV 192.168.4.31

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 15:56 CEST
```

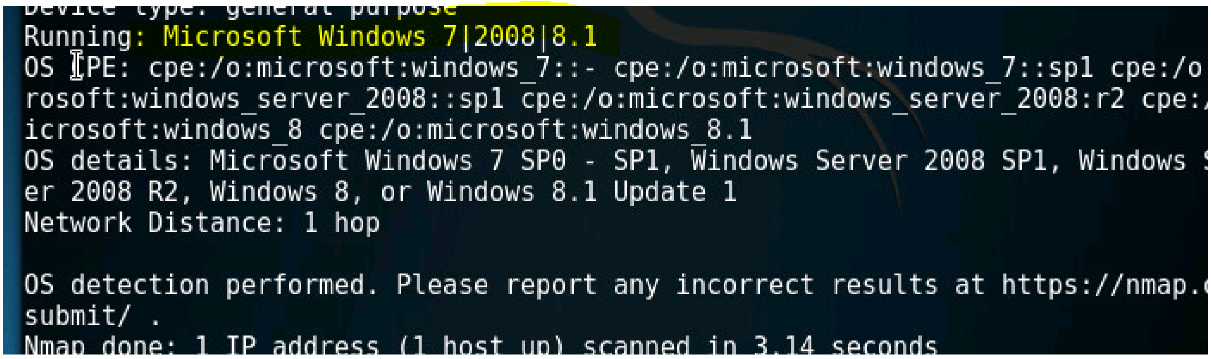
Sensitivity: Unrestricted

- Enable OS detection, by using the "-O" scan against "HEXID_WIN7".



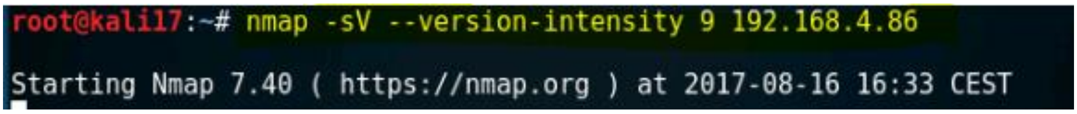
```
root@kali17:~# nmap -O 192.168.4.86

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 16:01 CEST
Nmap scan report for win7.hexid.assault (192.168.4.86)
Host is up (0.00078s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
```

  - Note: if the OS detection fails, you can use the argument "--osscan-guess" to force Nmap to guess the operating system.



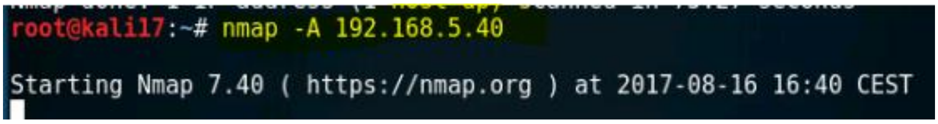
```
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/
icrosoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows S
er 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.14 seconds
```

  - Note: you can activate verbose mode by using the "-v" flag.
- Enable OS detection against "HEXID_WIN7", with increased intensity (9).
  - Command: "nmap -sV --version-intensity 9 192.168.4.86".



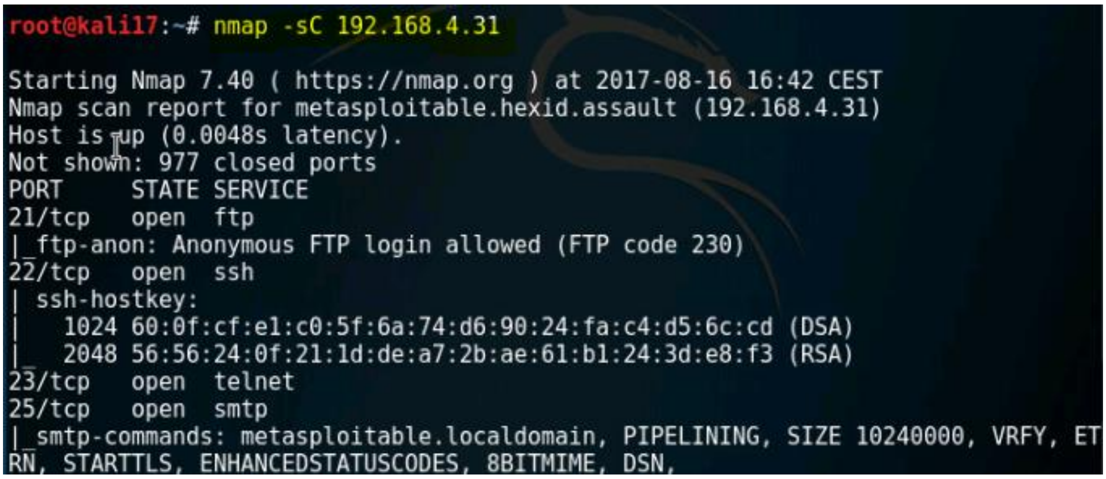
```
root@kali17:~# nmap -sV --version-intensity 9 192.168.4.86

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 16:33 CEST
```

    - Hunting for non-default ports etc.
- Deploy aggressive mode against 192.168.5.40 ("-A"). It will combine OS detection ("-o"), version detection ("-sV"), script scanning ("-sC") and traceroute ("--traceroute").



```
root@kali17:~# nmap -A 192.168.5.40

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 16:40 CEST
```

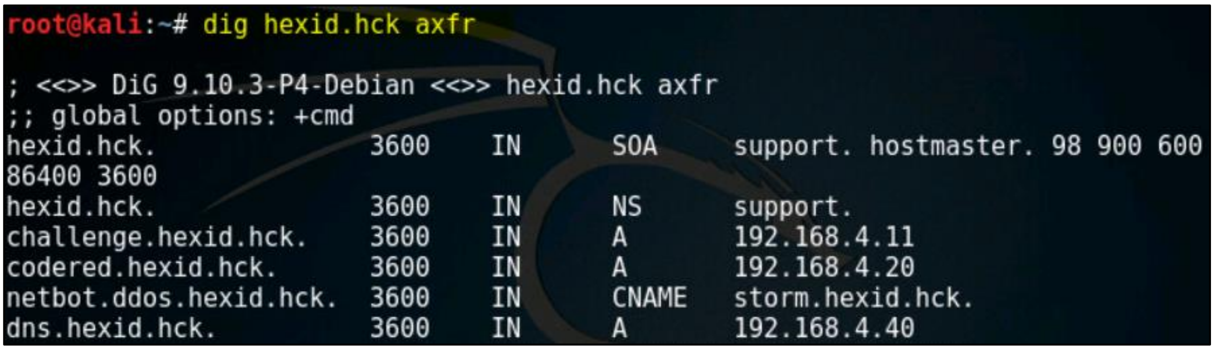
- Deploy all the default NMap NSE scripts against "HEXID_METASPLOITABLE".
  - Note: number of scripts depend on the target host or port rules of the scripts.



```
root@kali17:~# nmap -sC 192.168.4.31

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 16:42 CEST
Nmap scan report for metasploitable.hexid.assault (192.168.4.31)
Host is up (0.0048s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ET
RN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
```

- Check that the DNS client configuration file contains an entry for the local lab DNS server 192.168.5.40:
  - Command: "#cat /etc/resolv.conf".

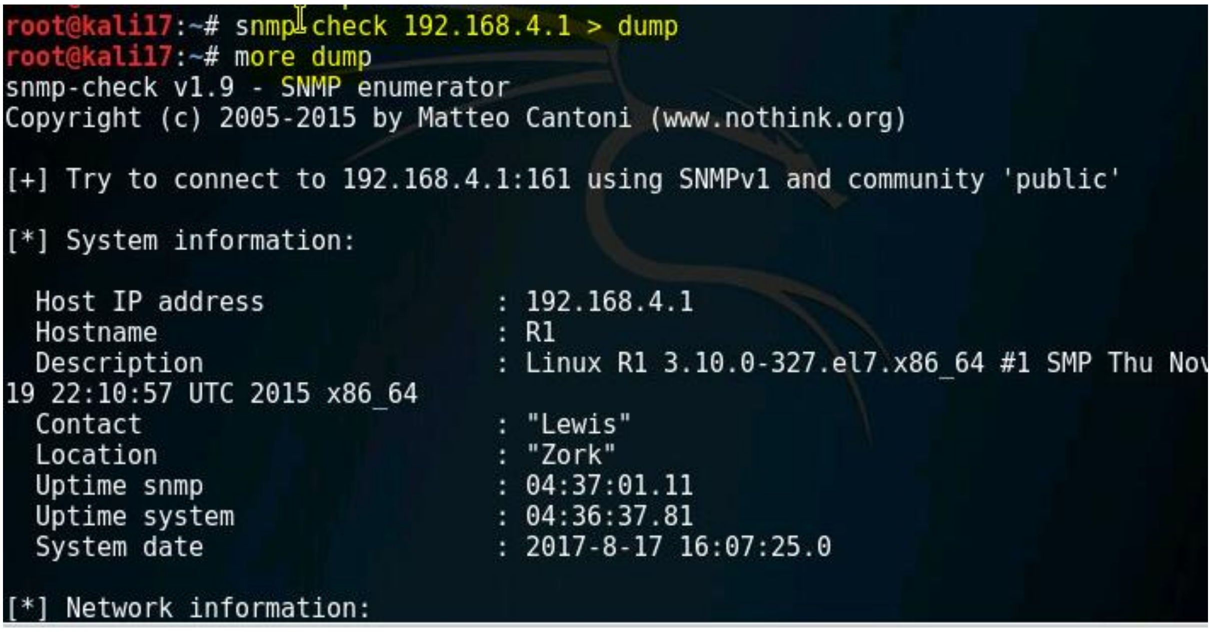
- Perform a DNS zone transfer on the default lab DNS server for the domains "hexid.hck" and "hexid.assault".
  - Command: "#dig hexid.hck axfr".
  - Command: "#dig hexid.assault axfr".



```
root@kali:~# dig hexid.hck axfr

; <<>> DiG 9.10.3-P4-Debian <<>> hexid.hck axfr
;; global options: +cmd
hexid.hck.              3600    IN      SOA     support. hostmaster. 98 900 600
86400 3600
hexid.hck.              3600    IN      NS      support.
challenge.hexid.hck.    3600    IN      A       192.168.4.11
codered.hexid.hck.      3600    IN      A       192.168.4.20
netbot.ddos.hexid.hck.  3600    IN      CNAME   storm.hexid.hck.
dns.hexid.hck.          3600    IN      A       192.168.4.40
```

- Test if the default gateway is running "snmp" with a default snmp community string, "public".
  - Command: "snmp-check 192.168.4.1 > dump".
  - Command: "more dump".

Sensitivity: Unrestricted



```
root@kali17:~# snmp-check 192.168.4.1 > dump
root@kali17:~# more dump
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.4.1:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 192.168.4.1
  Hostname                      : R1
  Description                   : Linux R1 3.10.0-327.el7.x86_64 #1 SMP Thu Nov
19 22:10:57 UTC 2015 x86_64
  Contact                       : "Lewis"
  Location                      : "Zork"
  Uptime snmp                   : 04:37:01.11
  Uptime system                 : 04:36:37.81
  System date                   : 2017-8-17 16:07:25.0

[*] Network information:
```

Sensitivity: Unrestricted