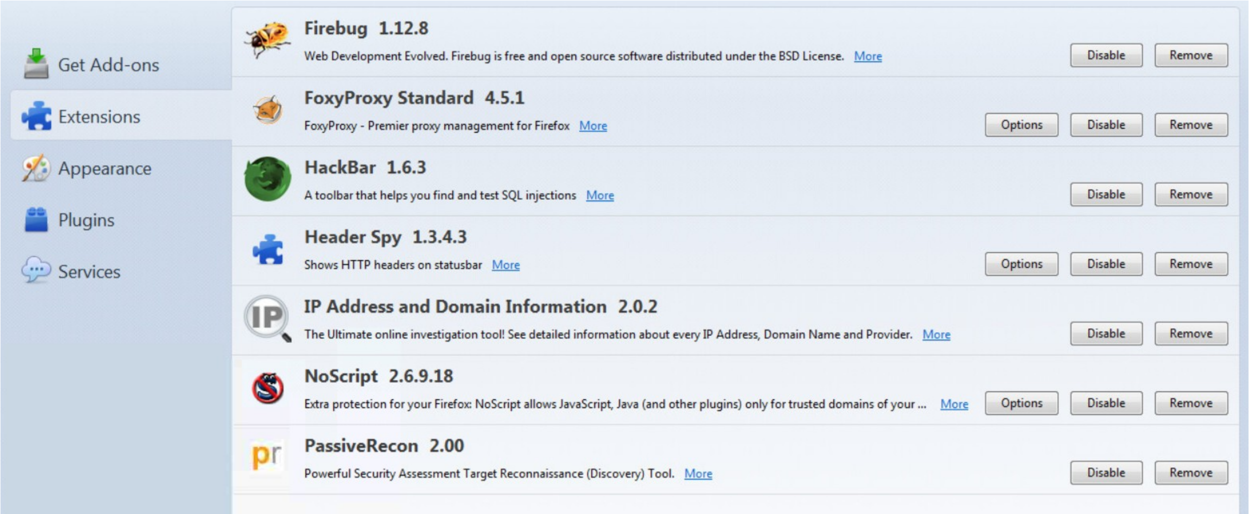
Lab 03 Report

Documentation

Information Gathering

3.1 Passive Reconnaissance

Tools/Add-ons



Firebug 1.12.8
Web Development Evolved. Firebug is free and open source software distributed under the BSD License. More

FoxyProxy Standard 4.5.1
FoxyProxy - Premier proxy management for Firefox More

HackBar 1.6.3
A toolbar that helps you find and test SQL injections More

Header Spy 1.3.4.3
Shows HTTP headers on statusbar More

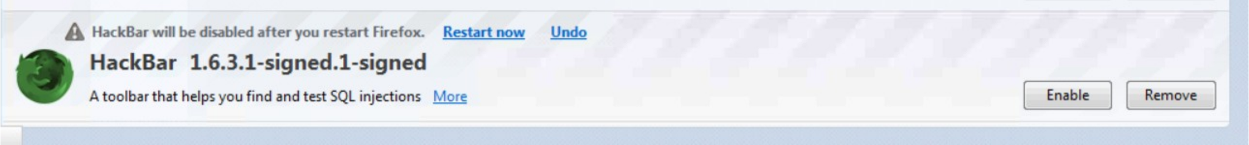
IP Address and Domain Information 2.0.2
The Ultimate online investigation tool! See detailed information about every IP Address, Domain Name and Provider. More

NoScript 2.6.9.18
Extra protection for your Firefox: NoScript allows JavaScript, Java (and other plugins) only for trusted domains of your ... More

PassiveRecon 2.00
Powerful Security Assessment Target Reconnaissance (Discovery) Tool. More

I clicked on “More” link for each Firefox extension to see how it might be useful during a Pen Test but didn’t find showIP 2.0. And couldn’t install it from online either because of no internet connections

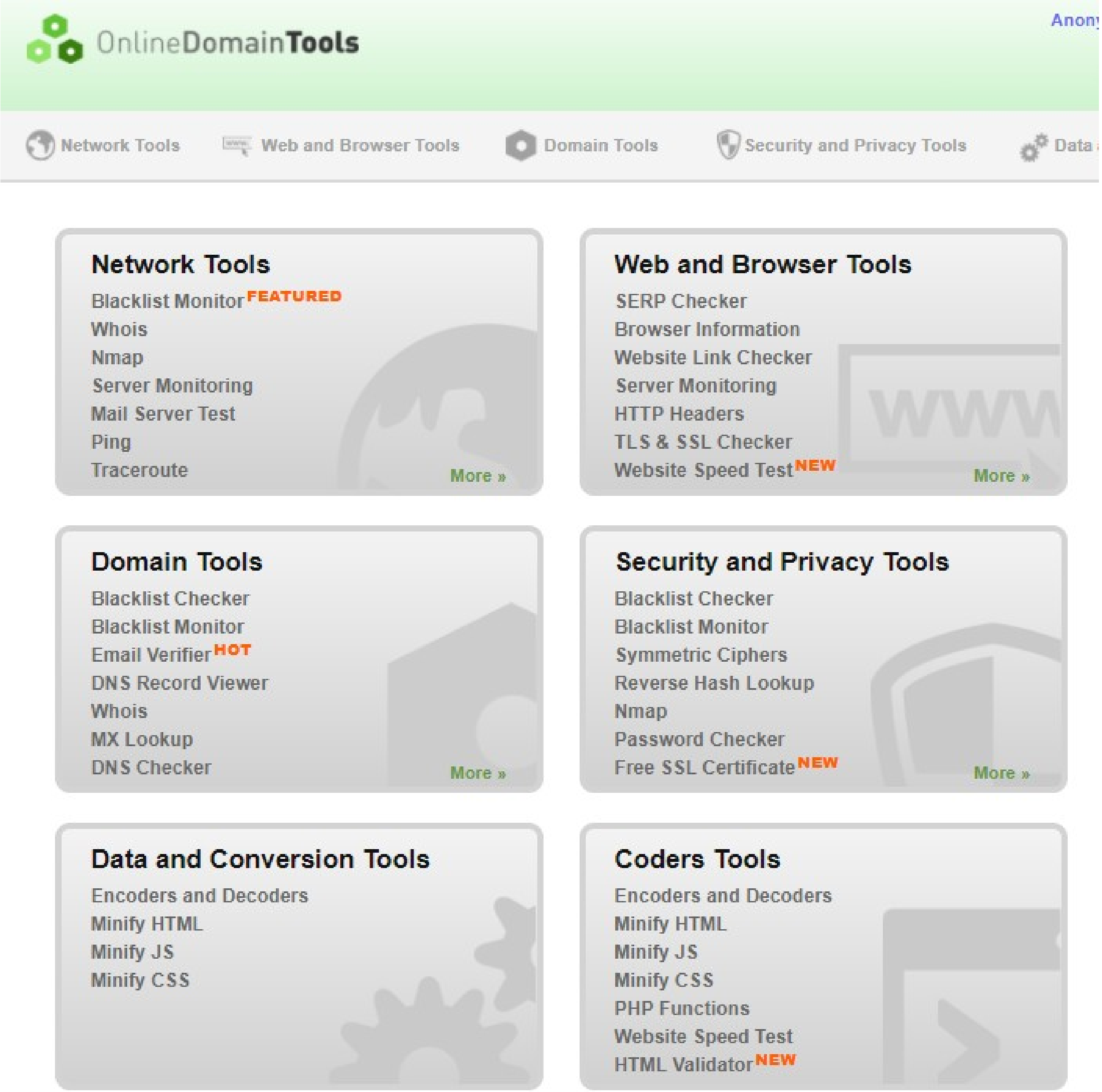
At some point after looking at the add-ons, I have disable the Hackbar toolbar.



HackBar will be disabled after you restart Firefox. Restart now Undo

HackBar 1.6.3.1-signed.1-signed
A toolbar that helps you find and test SQL injections More

2. From *my own computer,* I visited to this URL http://online-domain-tools.com **to see some of the fee tools available to gather information on my targets.**



Network Tools

- Blacklist Monitor FEATURED
- Whois
- Nmap
- Server Monitoring
- Mail Server Test
- Ping
- Traceroute

More »

Web and Browser Tools

- SERP Checker
- Browser Information
- Website Link Checker
- Server Monitoring
- HTTP Headers
- TLS & SSL Checker
- Website Speed Test NEW

More »

Domain Tools

- Blacklist Checker
- Blacklist Monitor
- Email Verifier HOT
- DNS Record Viewer
- Whois
- MX Lookup
- DNS Checker

More »

Security and Privacy Tools

- Blacklist Checker
- Blacklist Monitor
- Symmetric Ciphers
- Reverse Hash Lookup
- Nmap
- Password Checker
- Free SSL Certificate NEW

More »

Data and Conversion Tools

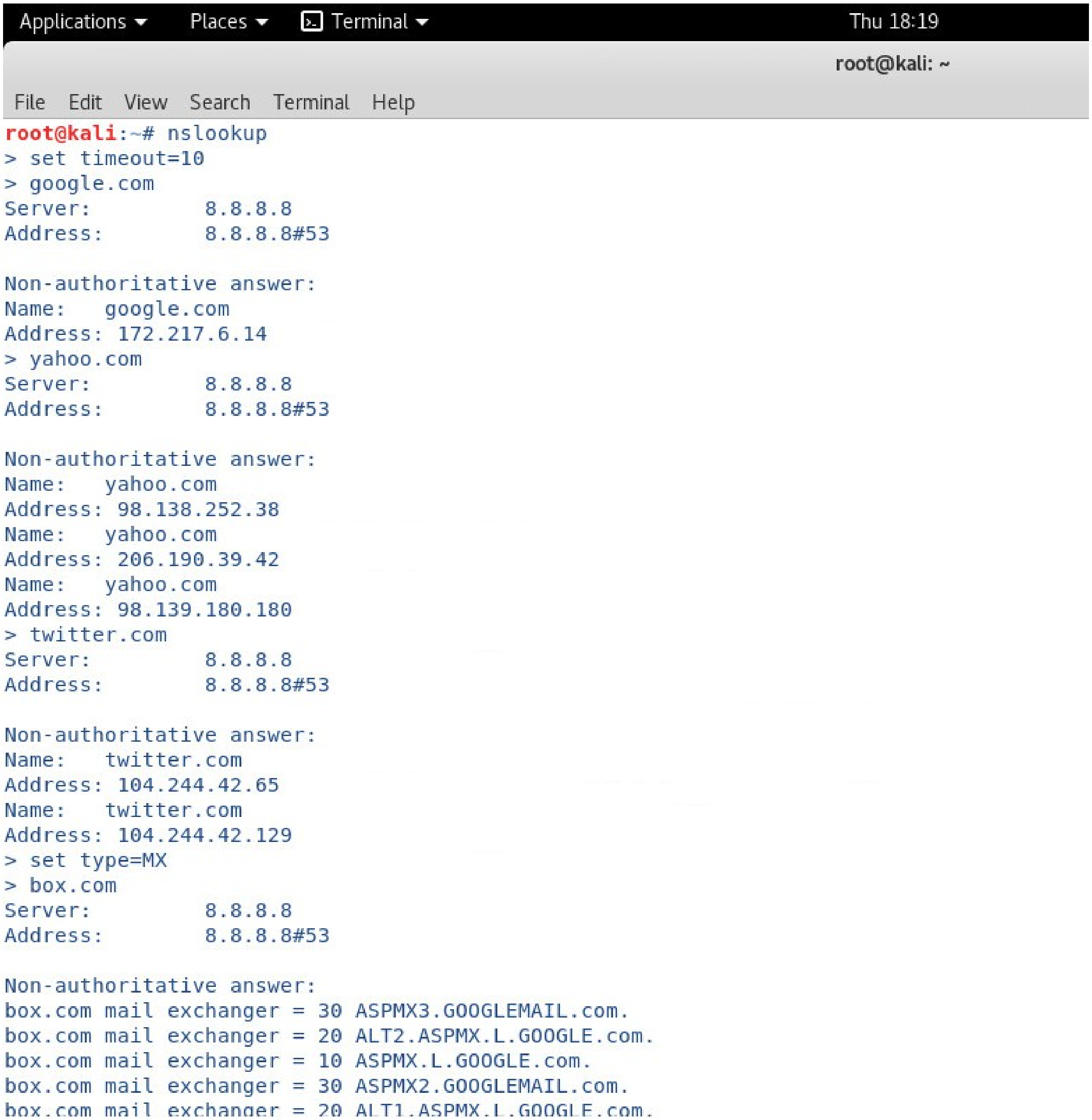
- Encoders and Decoders
- Minify HTML
- Minify JS
- Minify CSS

Coders Tools

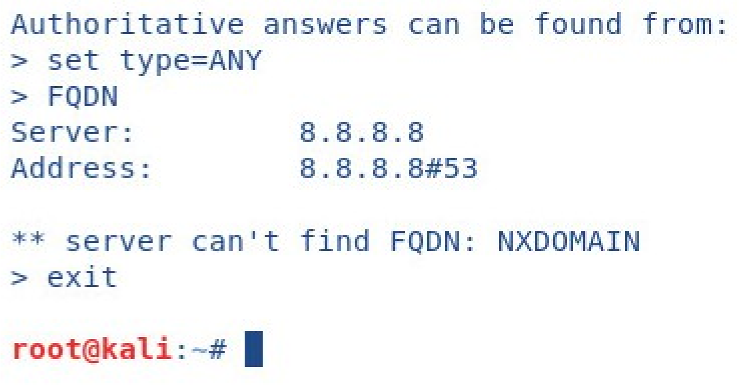
- Encoders and Decoders
- Minify HTML
- Minify JS
- Minify CSS
- PHP Functions
- Website Speed Test
- HTML Validator NEW

3. Using Nslookup

CPEH-LinuxAttack



```
root@kali:~# nslookup
> set timeout=10
> google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.6.14
> yahoo.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   yahoo.com
Address: 98.138.252.38
Name:   yahoo.com
Address: 206.190.39.42
Name:   yahoo.com
Address: 98.139.180.180
> twitter.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   twitter.com
Address: 104.244.42.65
Name:   twitter.com
Address: 104.244.42.129
> set type=MX
> box.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
box.com mail exchanger = 30 ASPMX3.GOOGLEMAIL.com.
box.com mail exchanger = 20 ALT2.ASPMX.L.GOOGLE.com.
box.com mail exchanger = 10 ASPMX.L.GOOGLE.com.
box.com mail exchanger = 30 ASPMX2.GOOGLEMAIL.com.
box.com mail exchanger = 20 ALT1.ASPMX.L.GOOGLE.com.
```



```
Authoritative answers can be found from:
> set type=ANY
> FQDN
Server:         8.8.8.8
Address:        8.8.8.8#53

** server can't find FQDN: NXDOMAIN
> exit

root@kali:~#
```

3.2 Google Queries

1. Gather information from Aegon

I. Members of the Executive Board of AEGON N.V. and AEGON USA

Alexander R. Wynaendts

CEO and Chairman of the Executive and Management Board

Alex joined Aegon in 1997 and was appointed as a member of Aegon´s Executive Board in 2003

Matthew J. Rider

CFO and member of the Executive Board

Was appointed on May 19, 2017.

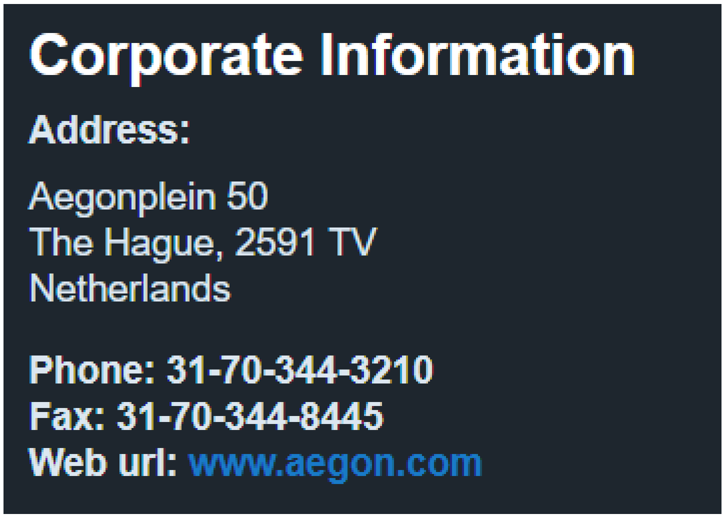
https://www.aegon.com/en/Home/Investors/News-releases/2016/aegon-to-appoint-matthew-rider-as-cfo/

II. Educational Background of the CEO

- **Ecole Superieure D'electricite** Graduated, 1984
- **Paris - Sorbonne University** Graduated, Economics, 1983

III. Find out the office location, telephone and name of the CEO.

Alexander R. Wynaendts, CEO



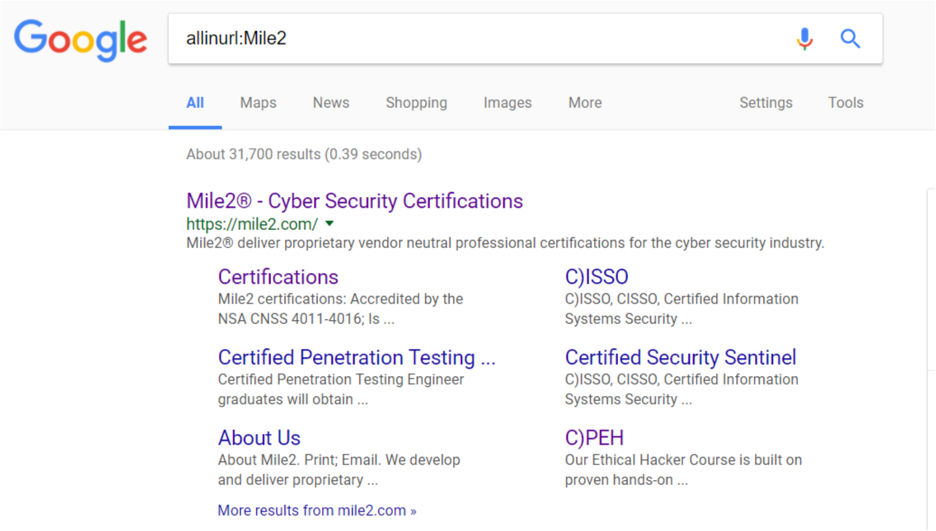
Corporate Information

Address:

Aegonplein 50
The Hague, 2591 TV
Netherlands

Phone: 31-70-344-3210
Fax: 31-70-344-8445
Web url: www.aegon.com

2. Practice utilizing the following Google Queries (screenshots are shown below)



About 31,700 results (0.39 seconds)

Mile2® - Cyber Security Certifications
https://mile2.com/
Mile2® deliver proprietary vendor neutral professional certifications for the cyber security industry.

Certifications
Mile2 certifications: Accredited by the NSA CNSS 4011-4016; Is ...

C)ISSO
C)ISSO, CISSO, Certified Information Systems Security ...

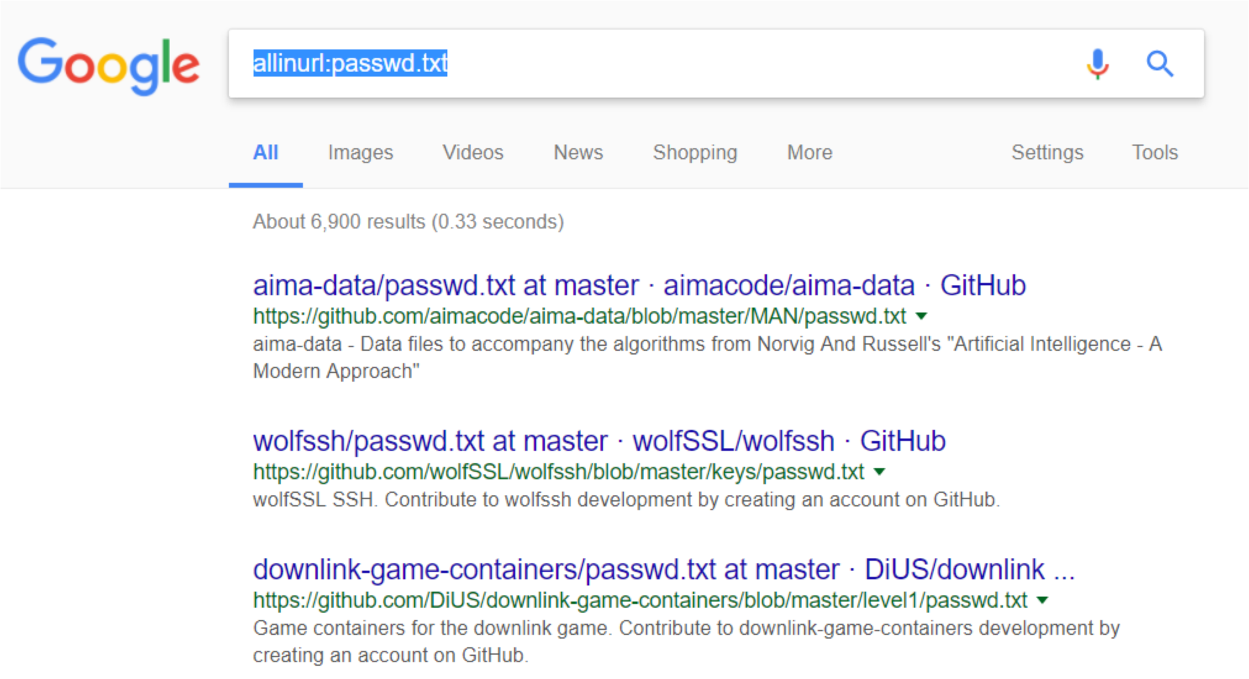
Certified Penetration Testing ...
Certified Penetration Testing Engineer graduates will obtain ...

Certified Security Sentinel
C)ISSO, CISSO, Certified Information Systems Security ...

About Us
About Mile2. Print; Email. We develop and deliver proprietary ...

C)PEH
Our Ethical Hacker Course is built on proven hands-on ...

More results from mile2.com »



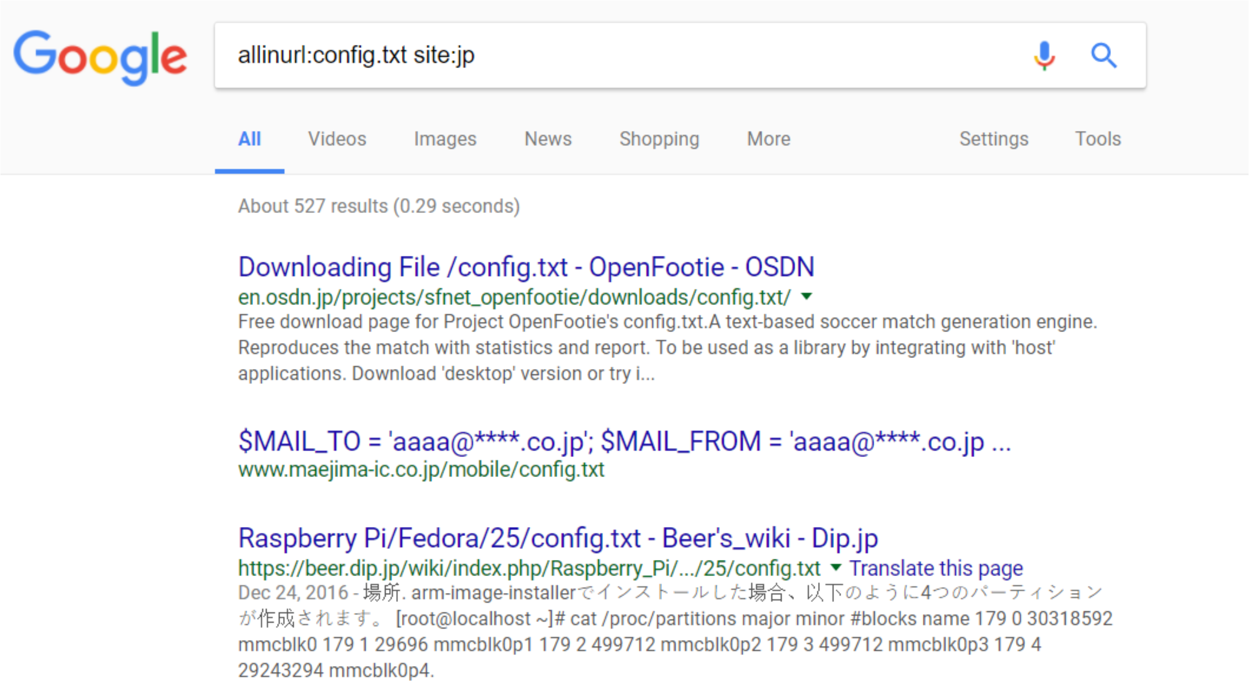
allinurl:passwd.txt

About 6,900 results (0.33 seconds)

aima-data/passwd.txt at master · aimacode/aima-data · GitHub
https://github.com/aimacode/aima-data/blob/master/MAN/passwd.txt
aima-data - Data files to accompany the algorithms from Norvig And Russell's "Artificial Intelligence - A Modern Approach"

wolfssh/passwd.txt at master · wolfSSL/wolfssh · GitHub
https://github.com/wolfSSL/wolfssh/blob/master/keys/passwd.txt
wolfSSL SSH. Contribute to wolfssh development by creating an account on GitHub.

downlink-game-containers/passwd.txt at master · DiUS/downlink ...
https://github.com/DiUS/downlink-game-containers/blob/master/level1/passwd.txt
Game containers for the downlink game. Contribute to downlink-game-containers development by creating an account on GitHub.



allinurl:config.txt site:jp

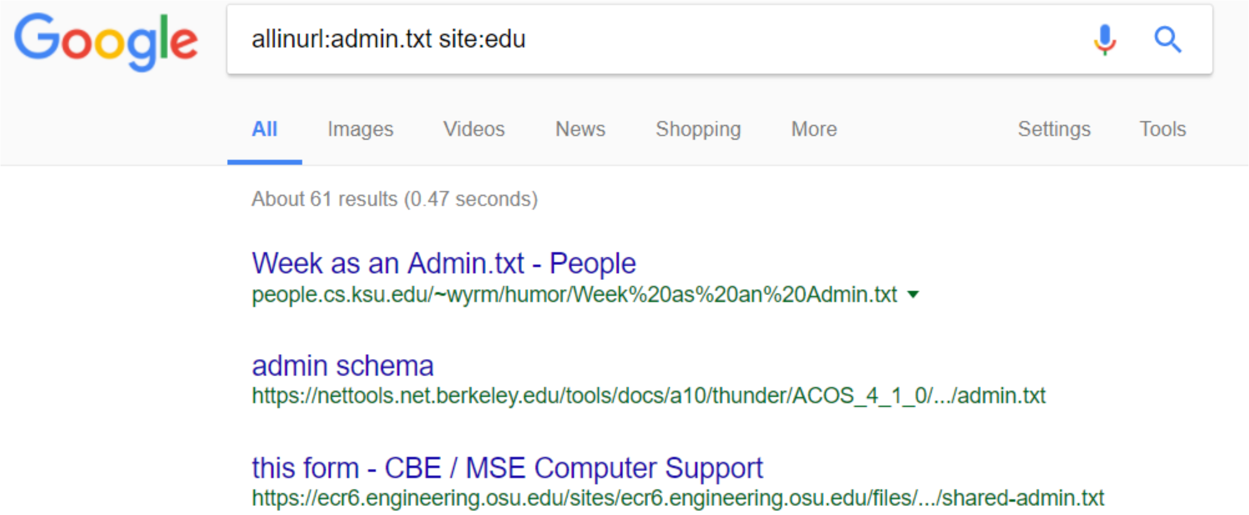
About 527 results (0.29 seconds)

Downloading File /config.txt - OpenFootie - OSDN
en.osdn.jp/projects/sfnet_openfootie/downloads/config.txt/
Free download page for Project OpenFootie's config.txt.A text-based soccer match generation engine. Reproduces the match with statistics and report. To be used as a library by integrating with 'host' applications. Download 'desktop' version or try i...

$MAIL_TO = 'aaaa@****.co.jp'; $MAIL_FROM = 'aaaa@****.co.jp ...
www.maejima-ic.co.jp/mobile/config.txt

Raspberry Pi/Fedora/25/config.txt - Beer's_wiki - Dip.jp
https://beer.dip.jp/wiki/index.php/Raspberry_Pi/.../25/config.txt Translate this page
Dec 24, 2016 - 場所. arm-image-installerでインストールした場合、以下のように4つのパーティションが作成されます。 [root@localhost ~]# cat /proc/partitions major minor #blocks name 179 0 30318592 mmcblk0 179 1 29696 mmcblk0p1 179 2 499712 mmcblk0p2 179 3 499712 mmcblk0p3 179 4 29243294 mmcblk0p4.

Lab 03 Report



allinurl:admin.txt site:edu

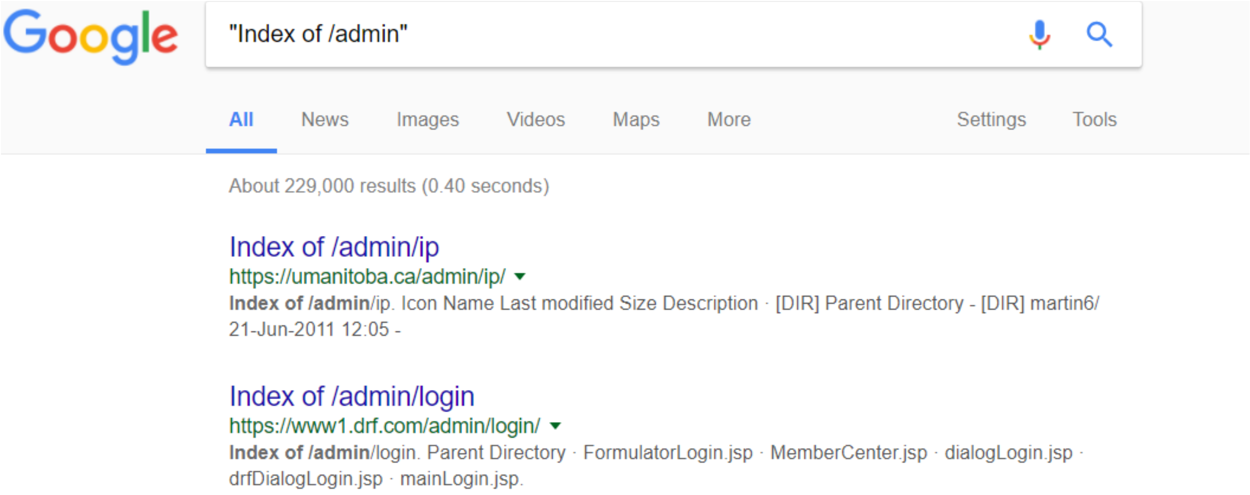
About 61 results (0.47 seconds)

Week as an Admin.txt - People
people.cs.ksu.edu/~wyrm/humor/Week%20as%20an%20Admin.txt

admin schema
https://nettools.net.berkeley.edu/tools/docs/a10/thunder/ACOS_4_1_0/.../admin.txt

this form - CBE / MSE Computer Support
https://ecr6.engineering.osu.edu/sites/ecr6.engineering.osu.edu/files/.../shared-admin.txt

3. Practicing index browsing enabled directories (Screenshots are below)

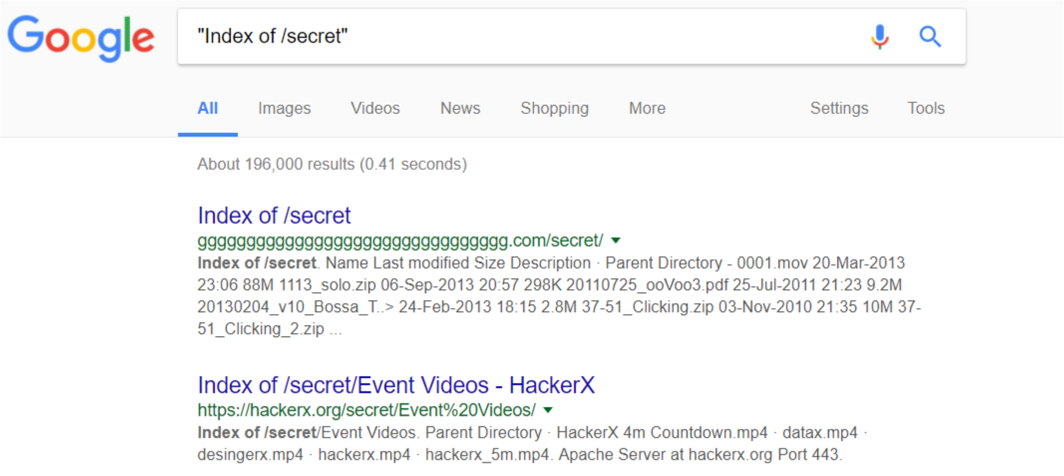


"Index of /admin"

About 229,000 results (0.40 seconds)

Index of /admin/ip
https://umanitoba.ca/admin/ip/
Index of /admin/ip. Icon Name Last modified Size Description · [DIR] Parent Directory - [DIR] martin6/ 21-Jun-2011 12:05 -

Index of /admin/login
https://www1.drf.com/admin/login/
Index of /admin/login. Parent Directory · FormulatorLogin.jsp · MemberCenter.jsp · dialogLogin.jsp · drfDialogLogin.jsp · mainLogin.jsp.

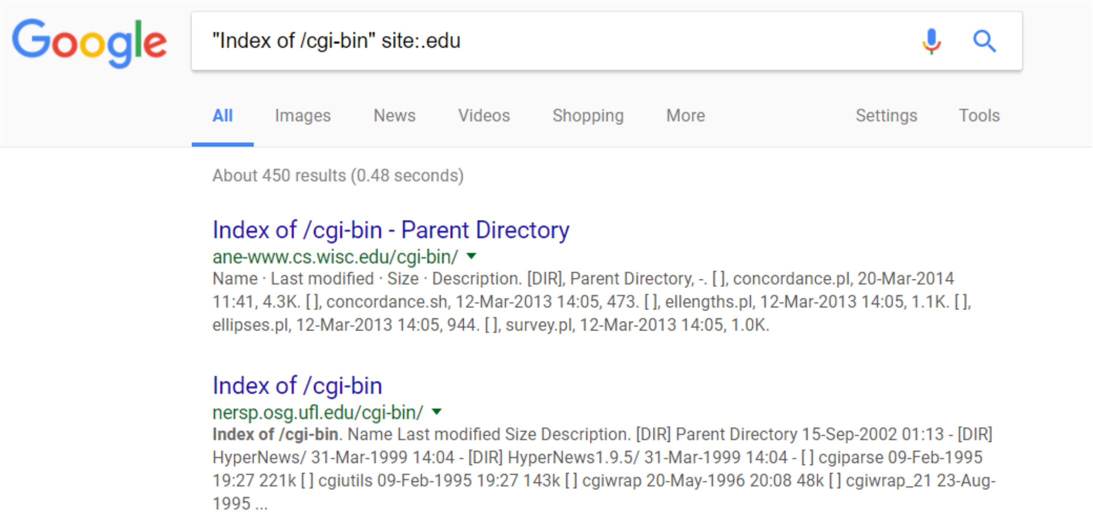


"Index of /secret"

About 196,000 results (0.41 seconds)

Index of /secret
gggggggggggggggggggggggggggggggg.com/secret/
Index of /secret. Name Last modified Size Description · Parent Directory - 0001.mov 20-Mar-2013 23:06 88M 1113_solo.zip 06-Sep-2013 20:57 298K 20110725_ooVoo3.pdf 25-Jul-2011 21:23 9.2M 20130204_v10_Bossa_T..> 24-Feb-2013 18:15 2.8M 37-51_Clicking.zip 03-Nov-2010 21:35 10M 37-51_Clicking_2.zip ...

Index of /secret/Event Videos - HackerX
https://hackerx.org/secret/Event%20Videos/
Index of /secret/Event Videos. Parent Directory · HackerX 4m Countdown.mp4 · datax.mp4 · desingerx.mp4 · hackerx.mp4 · hackerx_5m.mp4. Apache Server at hackerx.org Port 443.

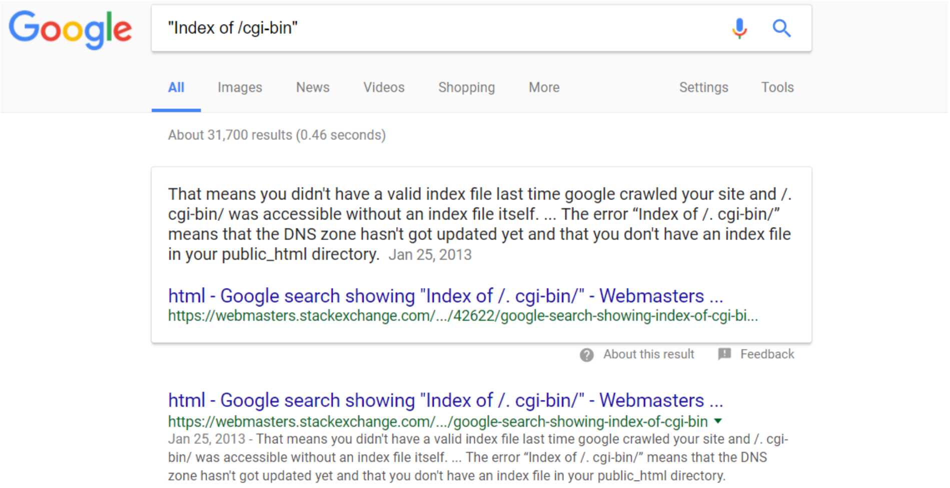


"Index of /cgi-bin" site:.edu

About 450 results (0.48 seconds)

Index of /cgi-bin - Parent Directory
ane-www.cs.wisc.edu/cgi-bin/
Name · Last modified · Size · Description. [DIR], Parent Directory, -. [ ], concordance.pl, 20-Mar-2014 11:41, 4.3K. [ ], concordance.sh, 12-Mar-2013 14:05, 473. [ ], ellengths.pl, 12-Mar-2013 14:05, 1.1K. [ ], ellipses.pl, 12-Mar-2013 14:05, 944. [ ], survey.pl, 12-Mar-2013 14:05, 1.0K.

Index of /cgi-bin
nersp.osg.ufl.edu/cgi-bin/
Index of /cgi-bin. Name Last modified Size Description. [DIR] Parent Directory 15-Sep-2002 01:13 - [DIR] HyperNews/ 31-Mar-1999 14:04 - [DIR] HyperNews1.9.5/ 31-Mar-1999 14:04 - [ ] cgiparse 09-Feb-1995 19:27 221k [ ] cgiutils 09-Feb-1995 19:27 143k [ ] cgiwrap 20-May-1996 20:08 48k [ ] cgiwrap_21 23-Aug-1995 ...



"Index of /cgi-bin"

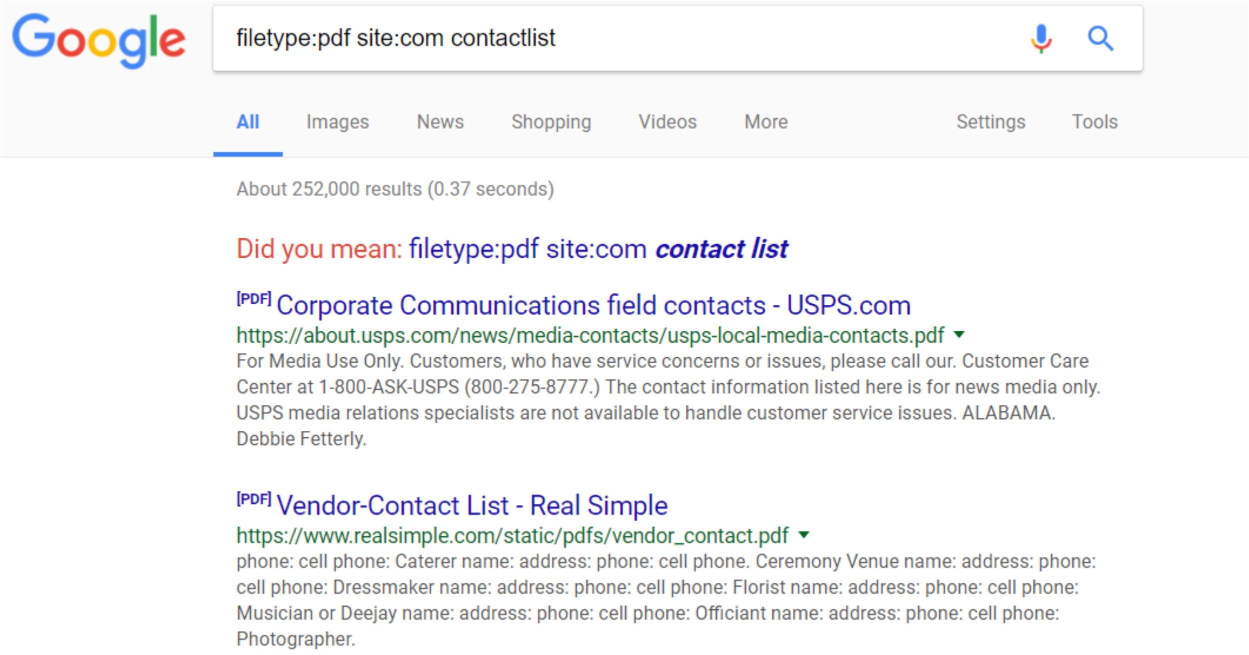
About 31,700 results (0.46 seconds)

That means you didn't have a valid index file last time google crawled your site and /. cgi-bin/ was accessible without an index file itself. ... The error “Index of /. cgi-bin/” means that the DNS zone hasn't got updated yet and that you don't have an index file in your public_html directory. Jan 25, 2013

html - Google search showing "Index of /. cgi-bin/" - Webmasters ...
https://webmasters.stackexchange.com/.../42622/google-search-showing-index-of-cgi-bi...

html - Google search showing "Index of /. cgi-bin/" - Webmasters ...
https://webmasters.stackexchange.com/.../google-search-showing-index-of-cgi-bin
Jan 25, 2013 - That means you didn't have a valid index file last time google crawled your site and /. cgi-bin/ was accessible without an index file itself. ... The error “Index of /. cgi-bin/” means that the DNS zone hasn't got updated yet and that you don't have an index file in your public_html directory.

4. Searching for particular file types



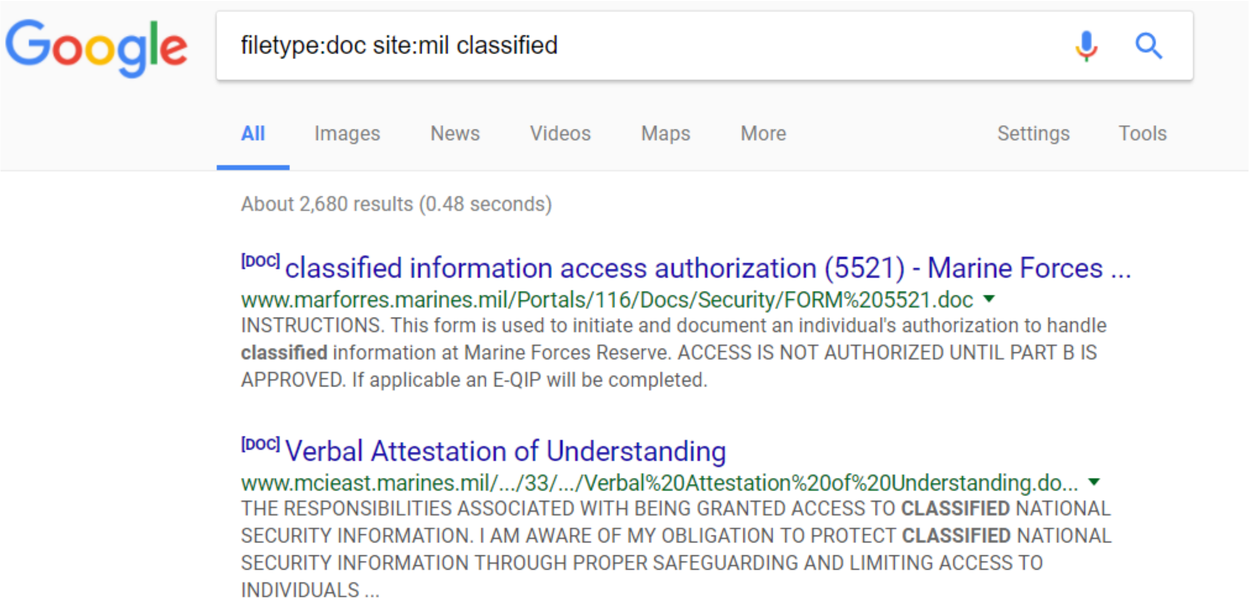
filetype:pdf site:com contactlist

About 252,000 results (0.37 seconds)

Did you mean: filetype:pdf site:com ***contact list***

[PDF] Corporate Communications field contacts - USPS.com
https://about.usps.com/news/media-contacts/usps-local-media-contacts.pdf
For Media Use Only. Customers, who have service concerns or issues, please call our. Customer Care Center at 1-800-ASK-USPS (800-275-8777.) The contact information listed here is for news media only. USPS media relations specialists are not available to handle customer service issues. ALABAMA. Debbie Fetterly.

[PDF] Vendor-Contact List - Real Simple
https://www.realsimple.com/static/pdfs/vendor_contact.pdf
phone: cell phone: Caterer name: address: phone: cell phone. Ceremony Venue name: address: phone: cell phone: Dressmaker name: address: phone: cell phone: Florist name: address: phone: cell phone: Musician or Deejay name: address: phone: cell phone: Officiant name: address: phone: cell phone: Photographer.



filetype:doc site:mil classified

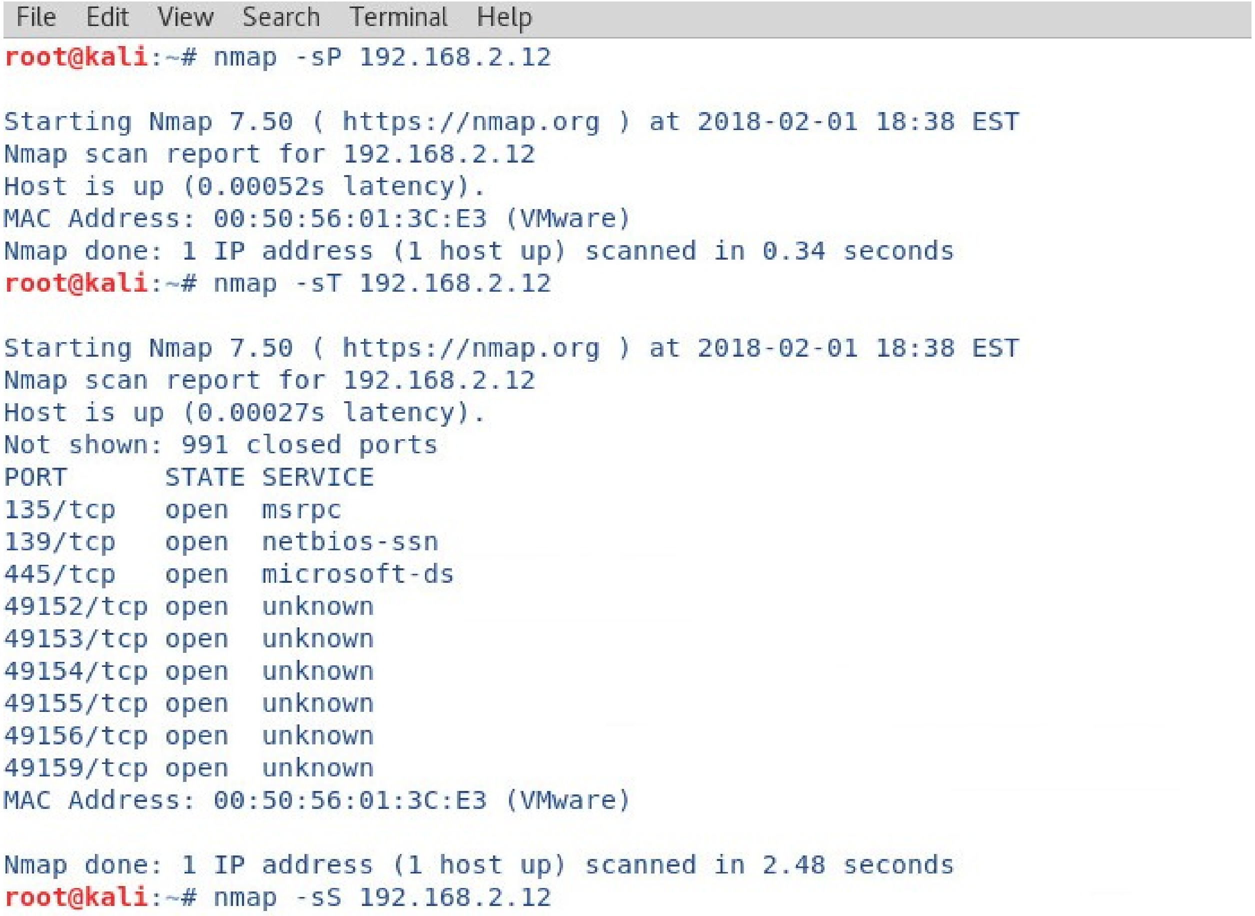
About 2,680 results (0.48 seconds)

[DOC] classified information access authorization (5521) - Marine Forces ...
www.marforres.marines.mil/Portals/116/Docs/Security/FORM%205521.doc
INSTRUCTIONS. This form is used to initiate and document an individual's authorization to handle **classified** information at Marine Forces Reserve. ACCESS IS NOT AUTHORIZED UNTIL PART B IS APPROVED. If applicable an E-QIP will be completed.

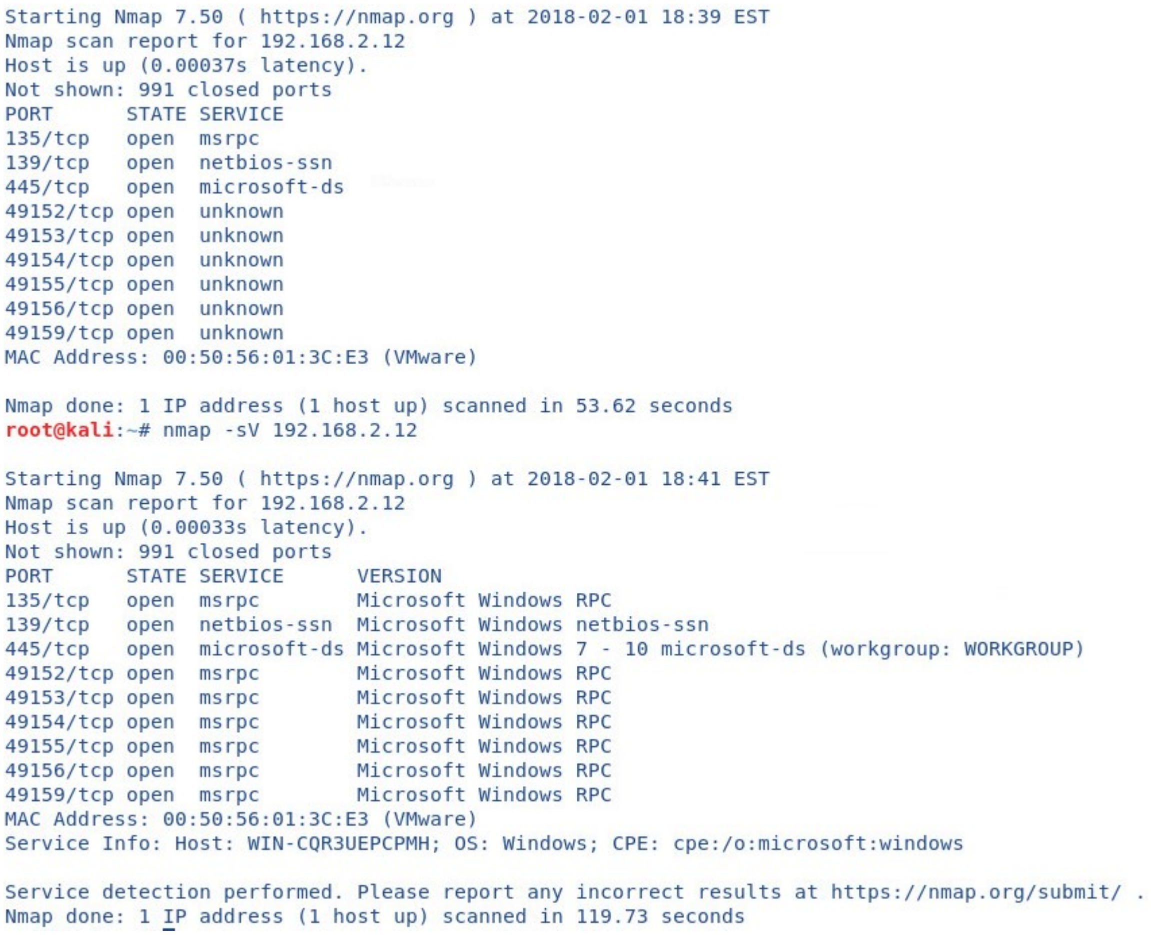
[DOC] Verbal Attestation of Understanding
www.mcieast.marines.mil/.../33/.../Verbal%20Attestation%20of%20Understanding.do...
THE RESPONSIBILITIES ASSOCIATED WITH BEING GRANTED ACCESS TO **CLASSIFIED** NATIONAL SECURITY INFORMATION. I AM AWARE OF MY OBLIGATION TO PROTECT **CLASSIFIED** NATIONAL SECURITY INFORMATION THROUGH PROPER SAFEGUARDING AND LIMITING ACCESS TO INDIVIDUALS ...

3.3 Active Reconnaissance

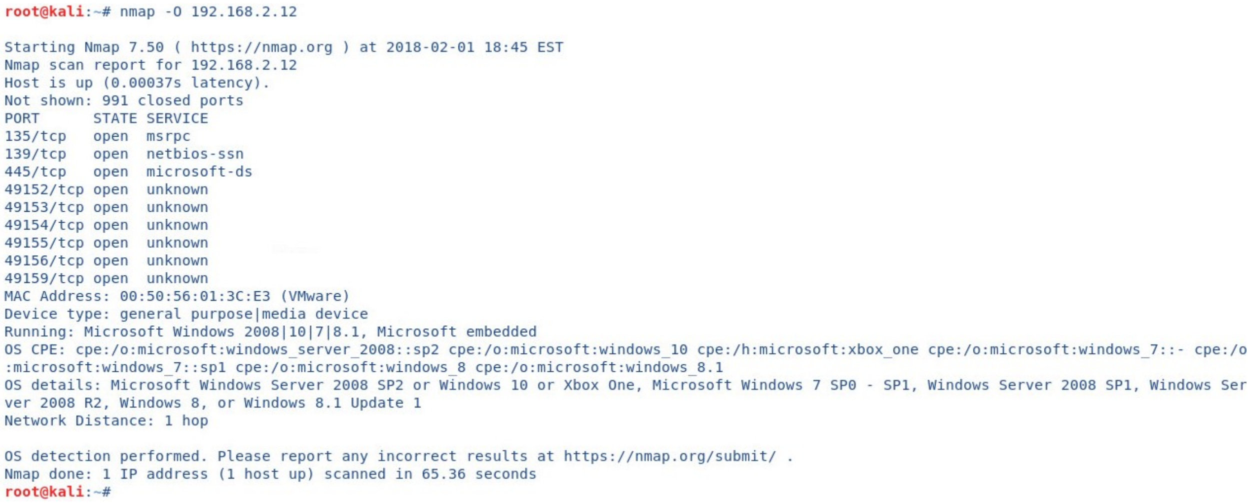
1. Open a bash shell and run the different commands against one of your Windows VMs



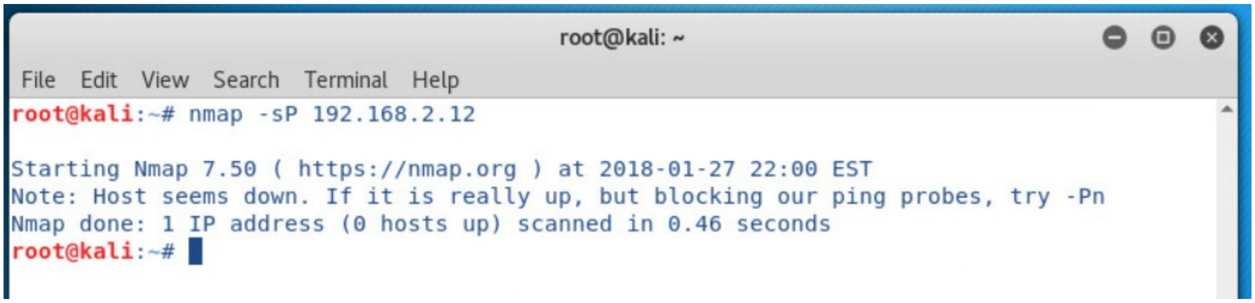
```
root@kali:~# nmap -sP 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-02-01 18:38 EST
Nmap scan report for 192.168.2.12
Host is up (0.00052s latency).
MAC Address: 00:50:56:01:3C:E3 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
root@kali:~# nmap -sT 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-02-01 18:38 EST
Nmap scan report for 192.168.2.12
Host is up (0.00027s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 00:50:56:01:3C:E3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.48 seconds
root@kali:~# nmap -sS 192.168.2.12
```



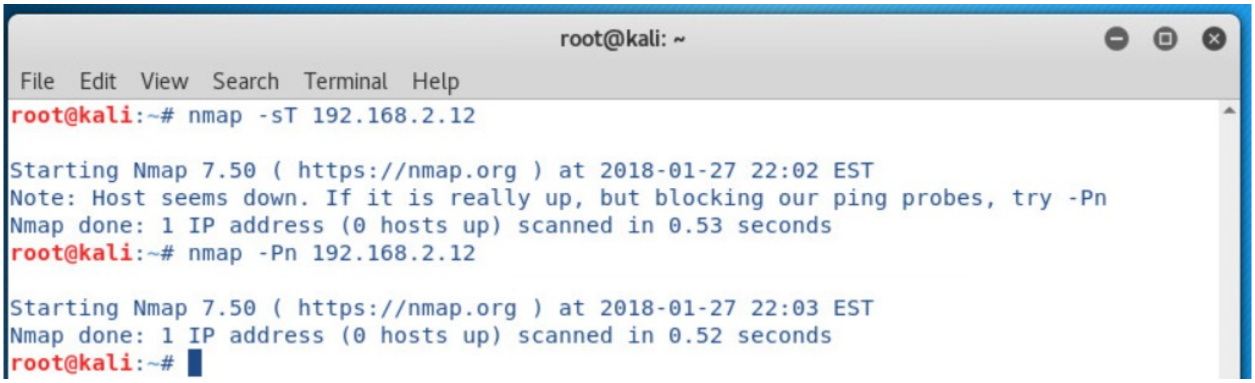
```
Starting Nmap 7.50 ( https://nmap.org ) at 2018-02-01 18:39 EST
Nmap scan report for 192.168.2.12
Host is up (0.00037s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 00:50:56:01:3C:E3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 53.62 seconds
root@kali:~# nmap -sV 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-02-01 18:41 EST
Nmap scan report for 192.168.2.12
Host is up (0.00033s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:50:56:01:3C:E3 (VMware)
Service Info: Host: WIN-CQR3UEPCPMH; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 119.73 seconds
```



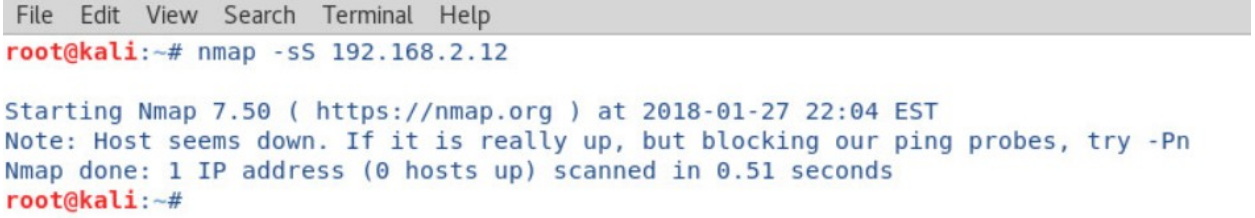
```
root@kali:~# nmap -O 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-02-01 18:45 EST
Nmap scan report for 192.168.2.12
Host is up (0.00037s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 00:50:56:01:3C:E3 (VMware)
Device type: general purpose|media device
Running: Microsoft Windows 2008|10|7|8.1, Microsoft embedded
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_10 cpe:/h:microsoft:xbox_one cpe:/o:microsoft:windows_7::- cpe:/o
:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One, Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Ser
ver 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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.36 seconds
root@kali:~#
```



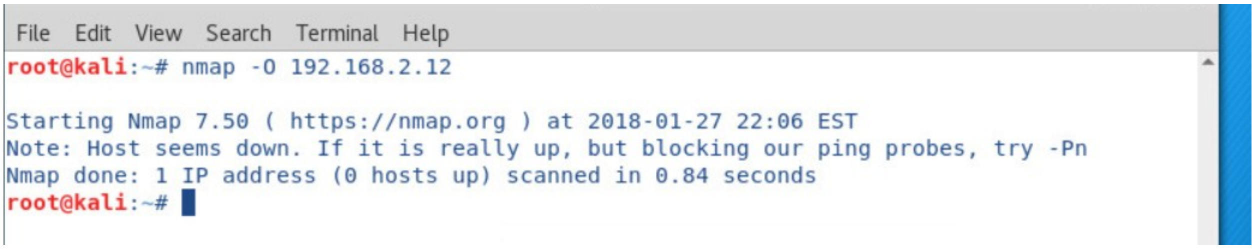
```
root@kali:~# nmap -sP 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-01-27 22:00 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.46 seconds
root@kali:~# 
```



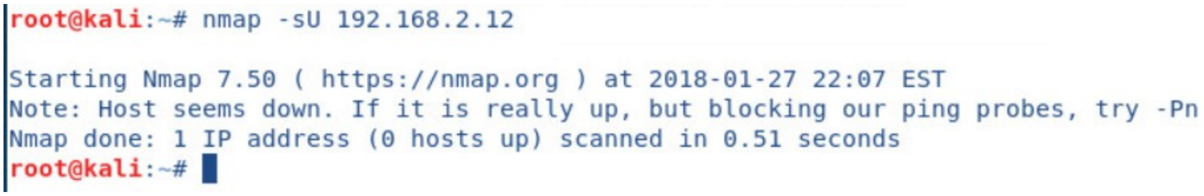
```
root@kali:~# nmap -sT 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-01-27 22:02 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.53 seconds
root@kali:~# nmap -Pn 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-01-27 22:03 EST
Nmap done: 1 IP address (0 hosts up) scanned in 0.52 seconds
root@kali:~# 
```



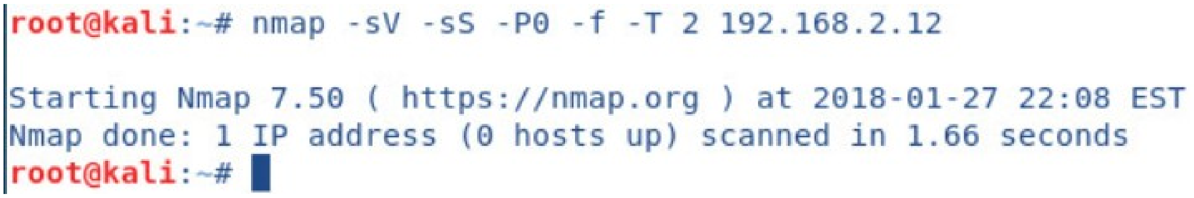
```
root@kali:~# nmap -sS 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-01-27 22:04 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.51 seconds
root@kali:~#
```



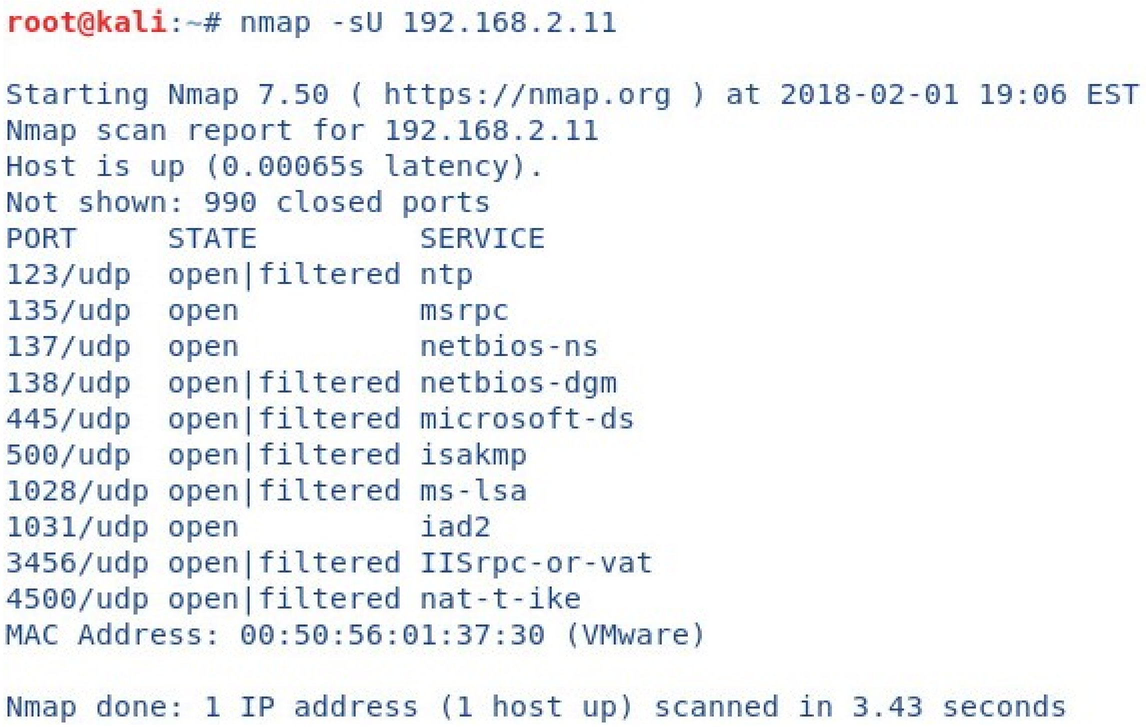
```
root@kali:~# nmap -O 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-01-27 22:06 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.84 seconds
root@kali:~# 
```



```
root@kali:~# nmap -sU 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-01-27 22:07 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.51 seconds
root@kali:~# 
```

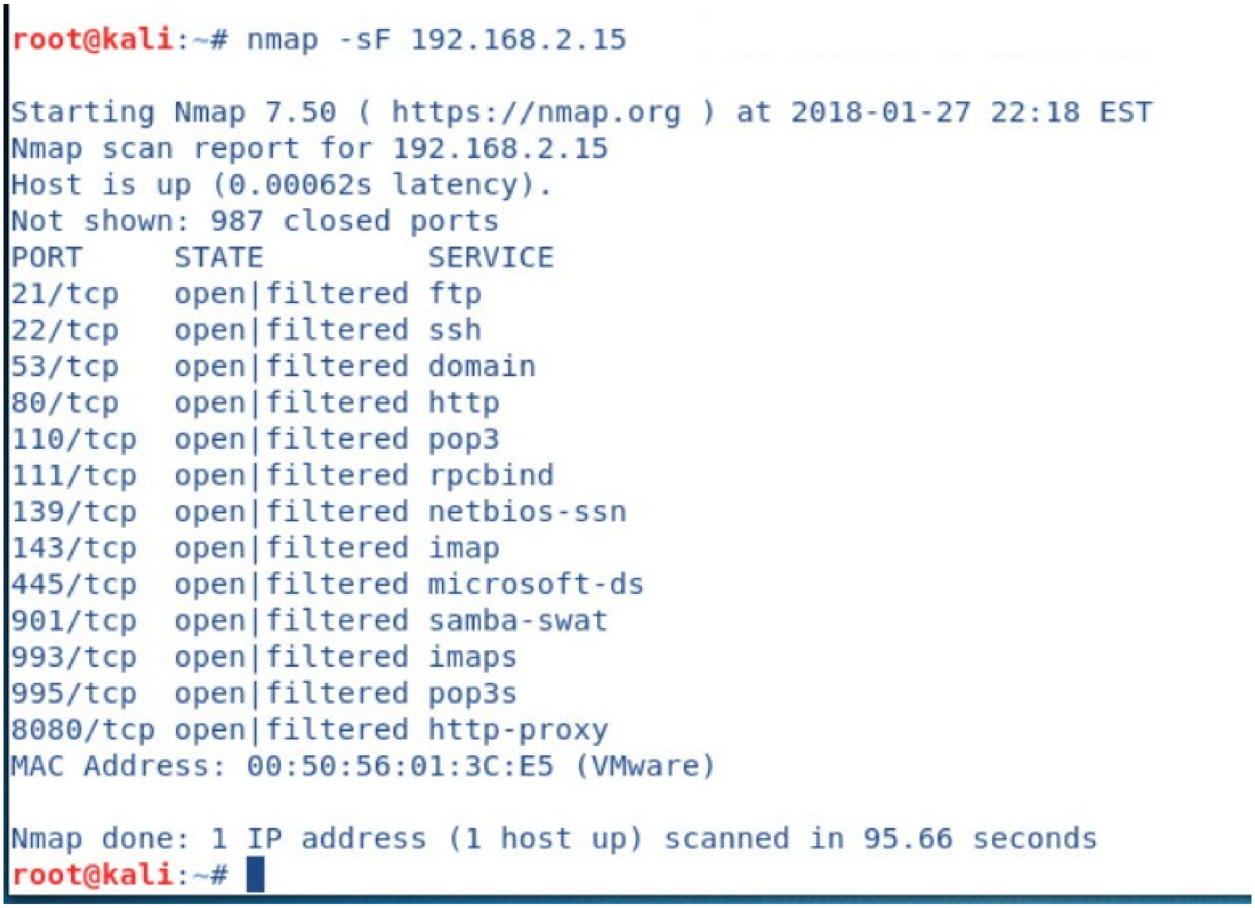


```
root@kali:~# nmap -sV -sS -P0 -f -T 2 192.168.2.12

Starting Nmap 7.50 ( https://nmap.org ) at 2018-01-27 22:08 EST
Nmap done: 1 IP address (0 hosts up) scanned in 1.66 seconds
root@kali:~# 
```

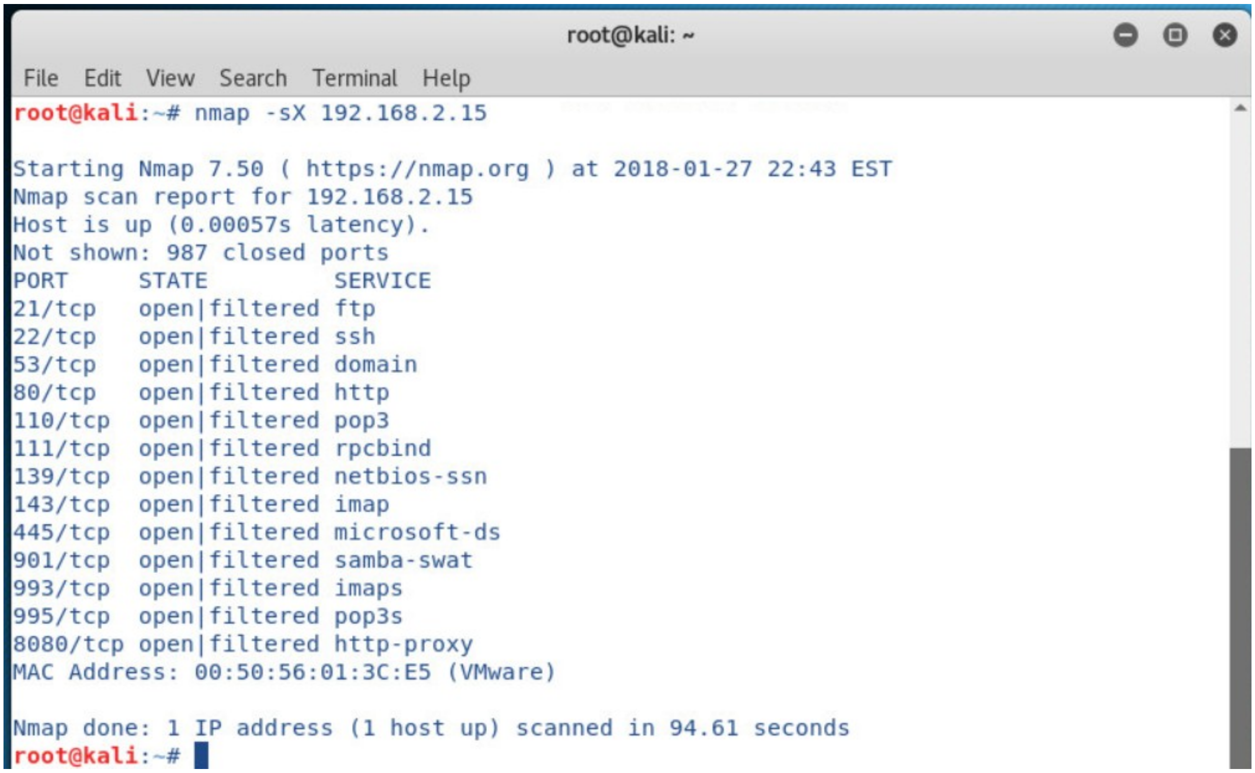


```
root@kali:~# nmap -sU 192.168.2.11

Starting Nmap 7.50 ( https://nmap.org ) at 2018-02-01 19:06 EST
Nmap scan report for 192.168.2.11
Host is up (0.00065s latency).
Not shown: 990 closed ports
PORT     STATE         SERVICE
123/udp  open|filtered ntp
135/udp  open          msrpc
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1028/udp open|filtered ms-lsa
1031/udp open          iad2
3456/udp open|filtered IISrpc-or-vat
4500/udp open|filtered nat-t-ike
MAC Address: 00:50:56:01:37:30 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.43 seconds
```

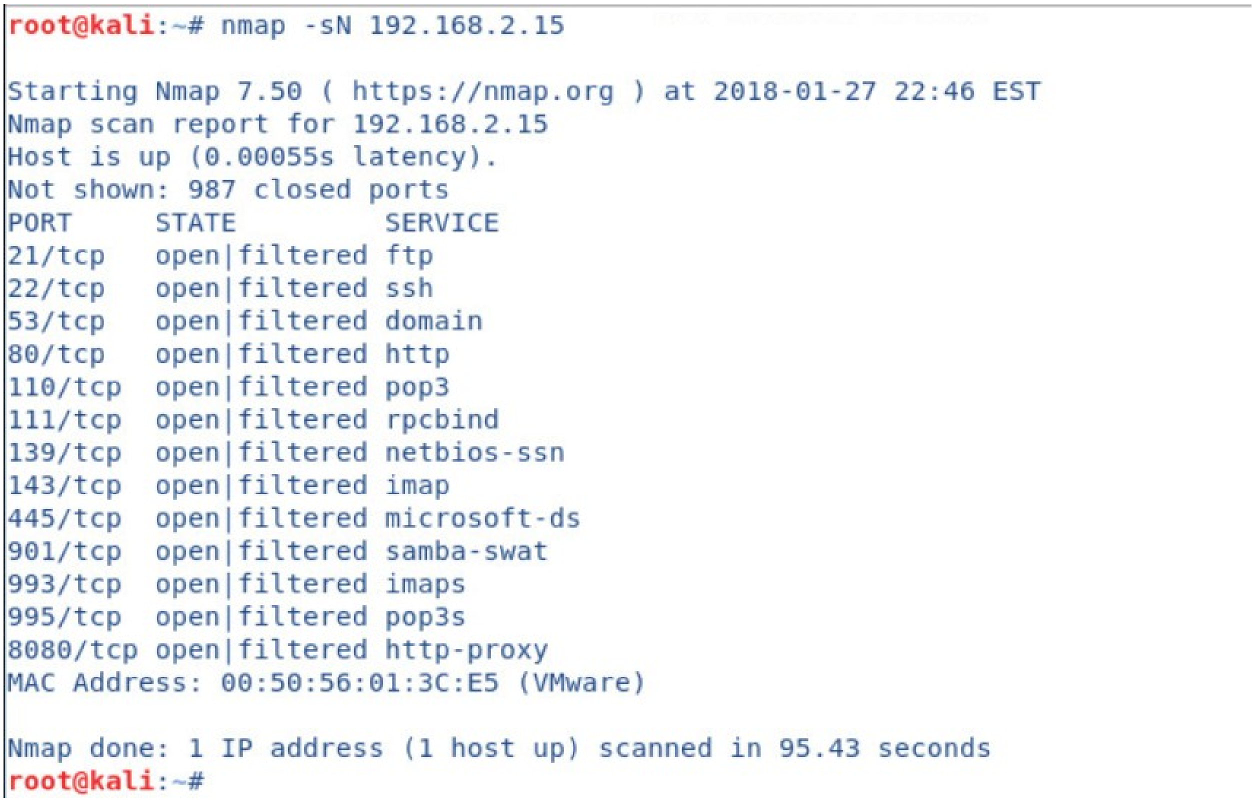
b. For the following scans, you will need to attack a UNIX box that has been setup by your instructor. Please record the IP address of the UNIX box here. 1. _192.168.2.15_



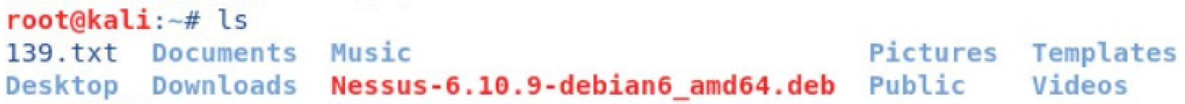
```
root@kali:~# nmap -sF 192.168.2.15

Starting Nmap 7.50 ( https://nmap.org ) at 2018-01-27 22:18 EST
Nmap scan report for 192.168.2.15
Host is up (0.00062s latency).
Not shown: 987 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
53/tcp   open|filtered domain
80/tcp   open|filtered http
110/tcp  open|filtered pop3
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
143/tcp  open|filtered imap
445/tcp  open|filtered microsoft-ds
901/tcp  open|filtered samba-swat
993/tcp  open|filtered imaps
995/tcp  open|filtered pop3s
8080/tcp open|filtered http-proxy
MAC Address: 00:50:56:01:3C:E5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 95.66 seconds
root@kali:~#
```



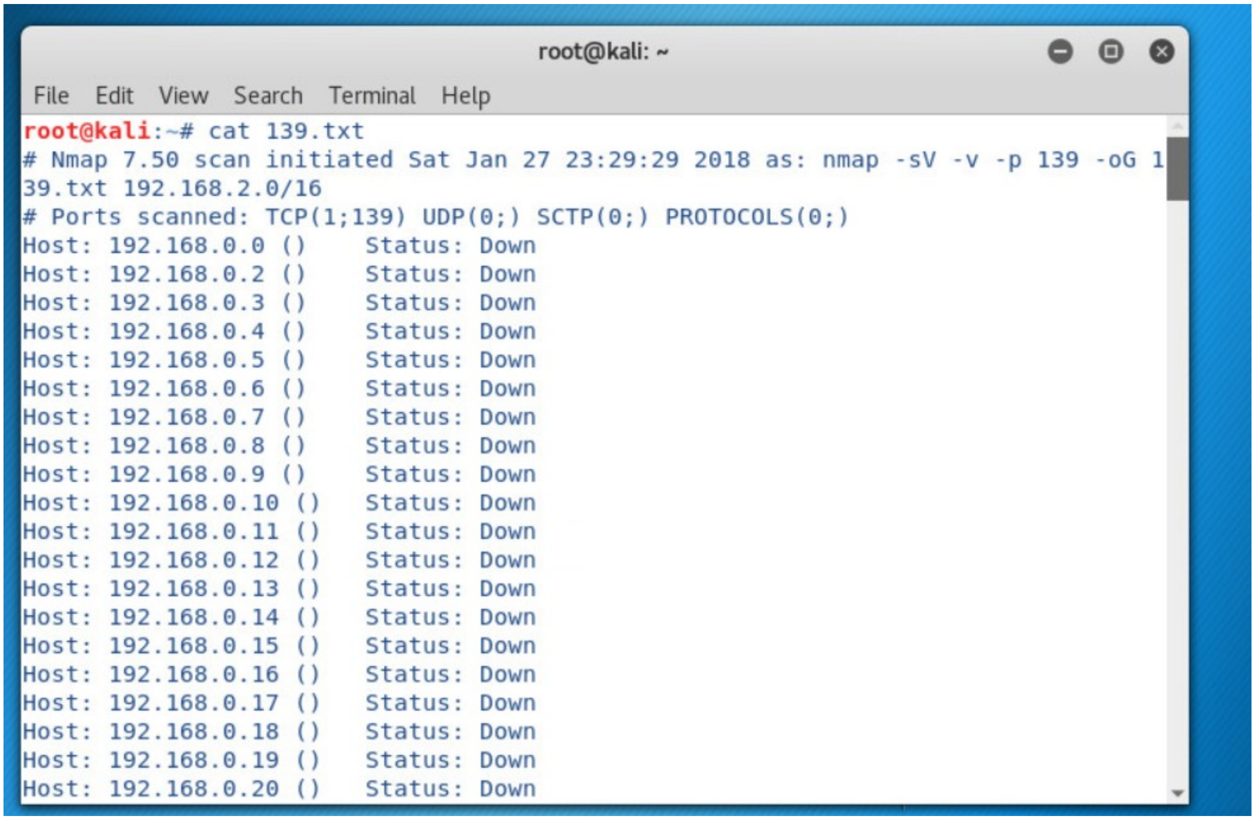
```
root@kali:~# nmap -sX 192.168.2.15

Starting Nmap 7.50 ( https://nmap.org ) at 2018-01-27 22:43 EST
Nmap scan report for 192.168.2.15
Host is up (0.00057s latency).
Not shown: 987 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
53/tcp   open|filtered domain
80/tcp   open|filtered http
110/tcp  open|filtered pop3
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
143/tcp  open|filtered imap
445/tcp  open|filtered microsoft-ds
901/tcp  open|filtered samba-swat
993/tcp  open|filtered imaps
995/tcp  open|filtered pop3s
8080/tcp open|filtered http-proxy
MAC Address: 00:50:56:01:3C:E5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 94.61 seconds
root@kali:~#
```



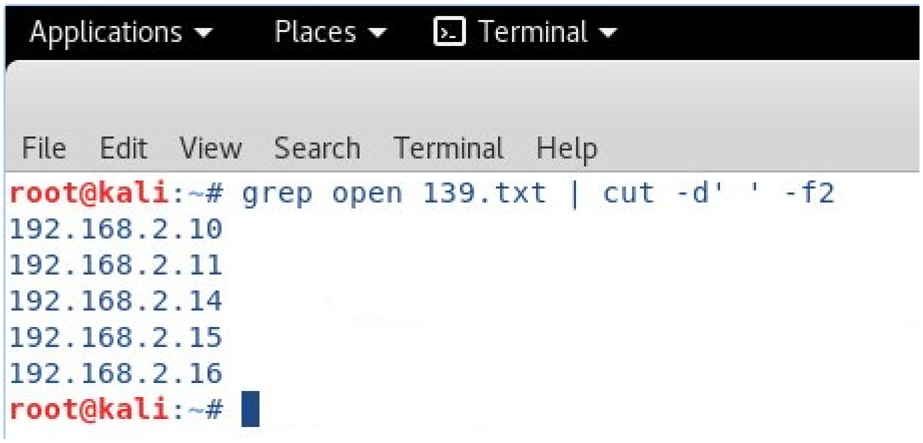
```
root@kali:~# nmap -sN 192.168.2.15

Starting Nmap 7.50 ( https://nmap.org ) at 2018-01-27 22:46 EST
Nmap scan report for 192.168.2.15
Host is up (0.00055s latency).
Not shown: 987 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
53/tcp   open|filtered domain
80/tcp   open|filtered http
110/tcp  open|filtered pop3
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
143/tcp  open|filtered imap
445/tcp  open|filtered microsoft-ds
901/tcp  open|filtered samba-swat
993/tcp  open|filtered imaps
995/tcp  open|filtered pop3s
8080/tcp open|filtered http-proxy
MAC Address: 00:50:56:01:3C:E5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 95.43 seconds
root@kali:~#
```



```
root@kali:~# ls
139.txt   Documents   Music                              Pictures   Templates
Desktop   Downloads   Nessus-6.10.9-debian6_amd64.deb   Public     Videos
```

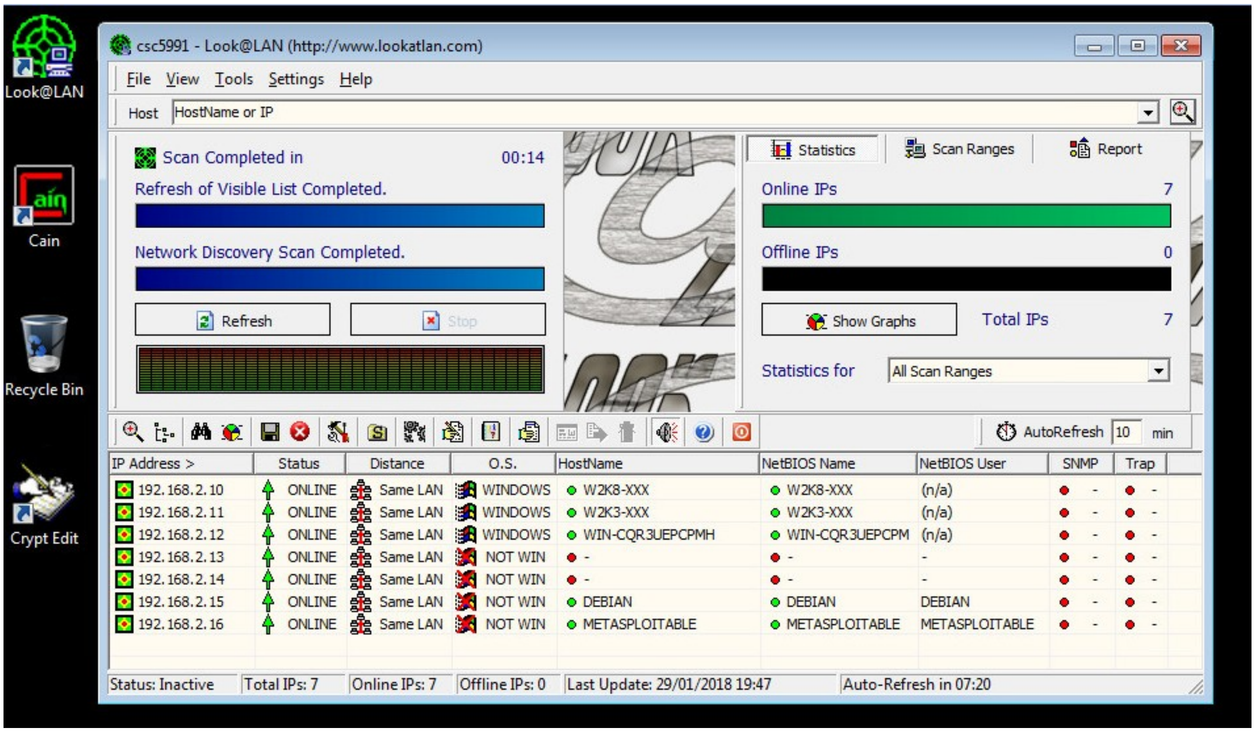


```
root@kali:~# cat 139.txt
# Nmap 7.50 scan initiated Sat Jan 27 23:29:29 2018 as: nmap -sV -v -p 139 -oG 1
39.txt 192.168.2.0/16
# Ports scanned: TCP(1;139) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 192.168.0.0 ()    Status: Down
Host: 192.168.0.2 ()    Status: Down
Host: 192.168.0.3 ()    Status: Down
Host: 192.168.0.4 ()    Status: Down
Host: 192.168.0.5 ()    Status: Down
Host: 192.168.0.6 ()    Status: Down
Host: 192.168.0.7 ()    Status: Down
Host: 192.168.0.8 ()    Status: Down
Host: 192.168.0.9 ()    Status: Down
Host: 192.168.0.10 ()   Status: Down
Host: 192.168.0.11 ()   Status: Down
Host: 192.168.0.12 ()   Status: Down
Host: 192.168.0.13 ()   Status: Down
Host: 192.168.0.14 ()   Status: Down
Host: 192.168.0.15 ()   Status: Down
Host: 192.168.0.16 ()   Status: Down
Host: 192.168.0.17 ()   Status: Down
Host: 192.168.0.18 ()   Status: Down
Host: 192.168.0.19 ()   Status: Down
Host: 192.168.0.20 ()   Status: Down
```



```
root@kali:~# grep open 139.txt | cut -d' ' -f2
192.168.2.10
192.168.2.11
192.168.2.14
192.168.2.15
192.168.2.16
root@kali:~# 
```

3.5 Look@LAN



Scan Completed in 00:14

Refresh of Visible List Completed.

Network Discovery Scan Completed.

Online IPs 7

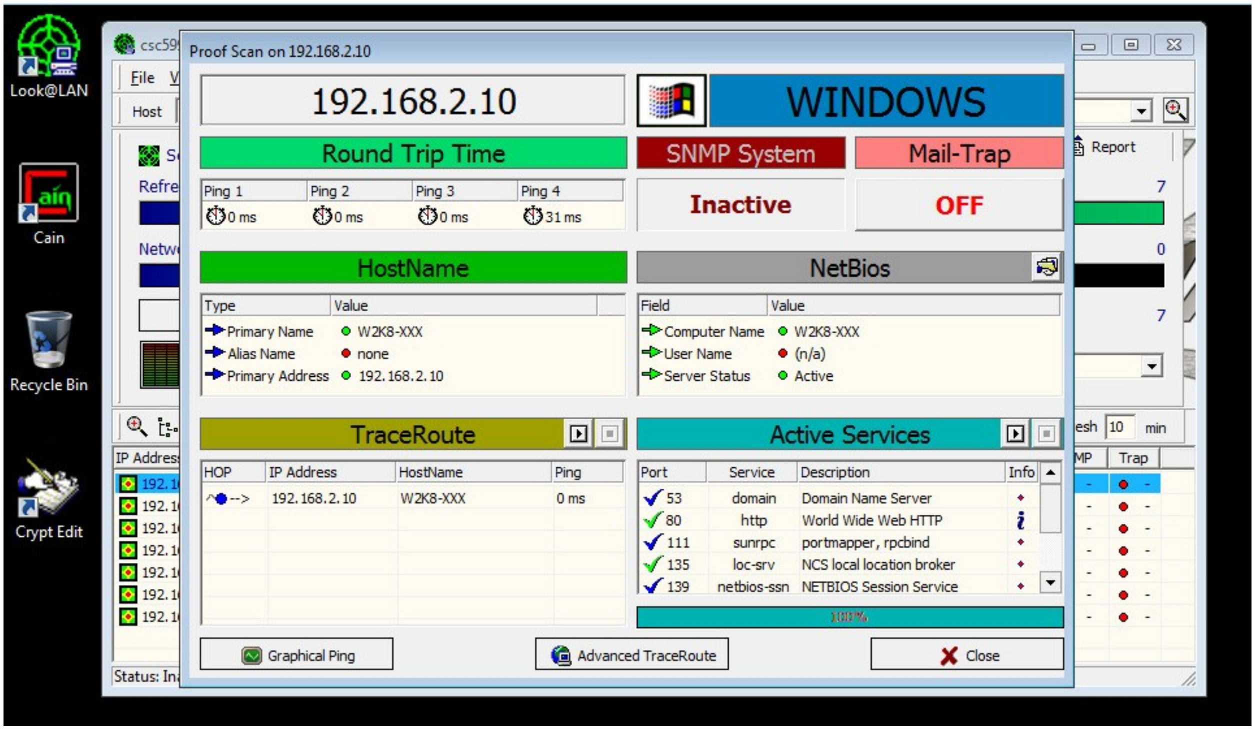
Offline IPs 0

Total IPs 7

Statistics for: All Scan Ranges

IP Address >	Status	Distance	O.S.	HostName	NetBIOS Name	NetBIOS User	SNMP	Trap
192.168.2.10	ONLINE	Same LAN	WINDOWS	W2K8-XXX	W2K8-XXX	(n/a)	● -	● -
192.168.2.11	ONLINE	Same LAN	WINDOWS	W2K3-XXX	W2K3-XXX	(n/a)	● -	● -
192.168.2.12	ONLINE	Same LAN	WINDOWS	WIN-CQR3UEPCPMH	WIN-CQR3UEPCPM	(n/a)	● -	● -
192.168.2.13	ONLINE	Same LAN	NOT WIN	-	-	-	● -	● -
192.168.2.14	ONLINE	Same LAN	NOT WIN	-	-	-	● -	● -
192.168.2.15	ONLINE	Same LAN	NOT WIN	DEBIAN	DEBIAN	DEBIAN	● -	● -
192.168.2.16	ONLINE	Same LAN	NOT WIN	METASPLOITABLE	METASPLOITABLE	METASPLOITABLE	● -	● -

Status: Inactive | Total IPs: 7 | Online IPs: 7 | Offline IPs: 0 | Last Update: 29/01/2018 19:47 | Auto-Refresh in 07:20



Proof Scan on 192.168.2.10

192.168.2.10 — WINDOWS

Round Trip Time

Ping 1	Ping 2	Ping 3	Ping 4
0 ms	0 ms	0 ms	31 ms

SNMP System: Inactive

Mail-Trap: OFF

HostName

Type	Value
Primary Name	W2K8-XXX
Alias Name	none
Primary Address	192.168.2.10

NetBios

Field	Value
Computer Name	W2K8-XXX
User Name	(n/a)
Server Status	Active

TraceRoute

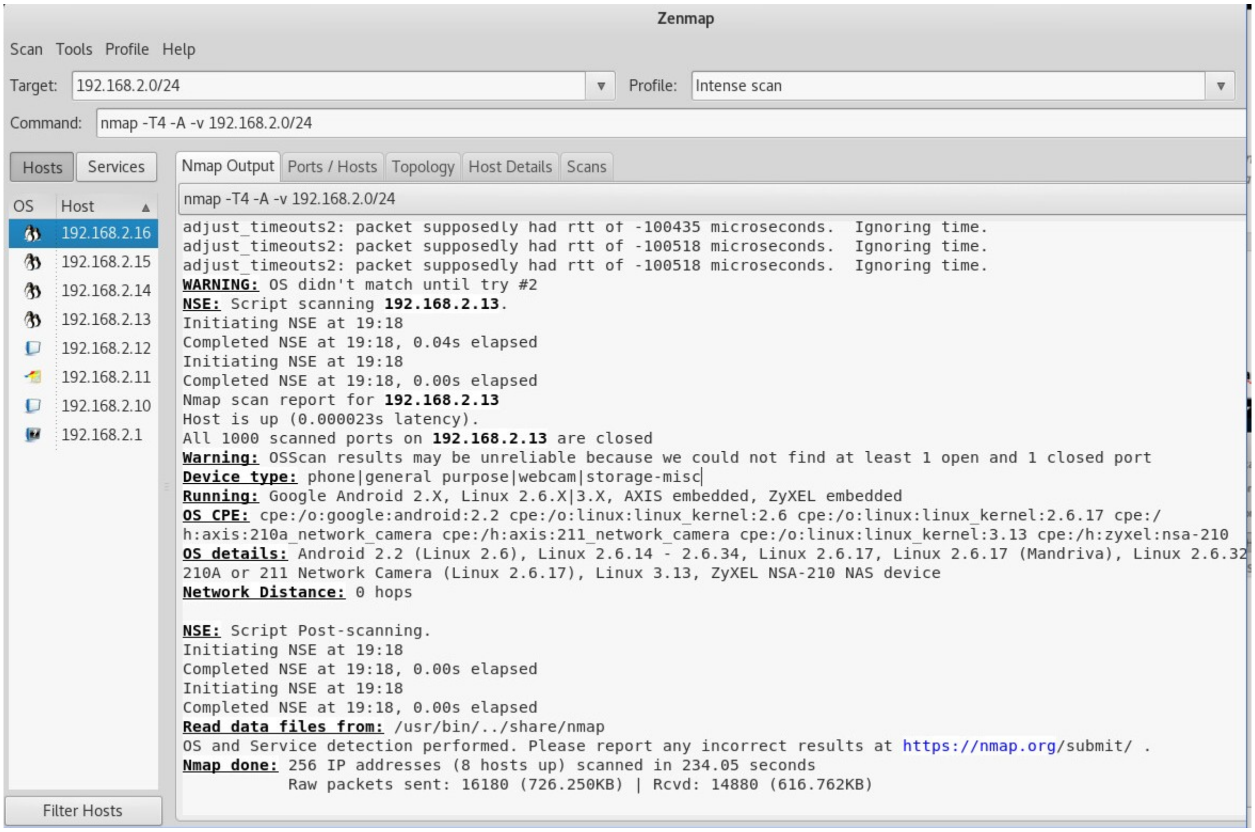
HOP	IP Address	HostName	Ping
-->	192.168.2.10	W2K8-XXX	0 ms

Active Services

Port	Service	Description	Info
✓ 53	domain	Domain Name Server	•
✓ 80	http	World Wide Web HTTP	i
✓ 111	sunrpc	portmapper, rpcbind	•
✓ 135	loc-srv	NCS local location broker	•
✓ 139	netbios-ssn	NETBIOS Session Service	•

100%

3.6 Zenmap



Target: 192.168.2.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.2.0/24

```
192.168.2.16
192.168.2.15
192.168.2.14
192.168.2.13
192.168.2.12
192.168.2.11
192.168.2.10
192.168.2.1
```

```
nmap -T4 -A -v 192.168.2.0/24
adjust_timeouts2: packet supposedly had rtt of -100435 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -100518 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -100518 microseconds.  Ignoring time.
WARNING: OS didn't match until try #2
NSE: Script scanning 192.168.2.13.
Initiating NSE at 19:18
Completed NSE at 19:18, 0.04s elapsed
Initiating NSE at 19:18
Completed NSE at 19:18, 0.00s elapsed
Nmap scan report for 192.168.2.13
Host is up (0.000023s latency).
All 1000 scanned ports on 192.168.2.13 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|general purpose|webcam|storage-misc
Running: Google Android 2.X, Linux 2.6.X|3.X, AXIS embedded, ZyXEL embedded
OS CPE: cpe:/o:google:android:2.2 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.6.17 cpe:/
h:axis:210a_network_camera cpe:/h:axis:211_network_camera cpe:/o:linux:linux_kernel:3.13 cpe:/h:zyxel:nsa-210
OS details: Android 2.2 (Linux 2.6), Linux 2.6.14 - 2.6.34, Linux 2.6.17, Linux 2.6.17 (Mandriva), Linux 2.6.32
210A or 211 Network Camera (Linux 2.6.17), Linux 3.13, ZyXEL NSA-210 NAS device
Network Distance: 0 hops

NSE: Script Post-scanning.
Initiating NSE at 19:18
Completed NSE at 19:18, 0.00s elapsed
Initiating NSE at 19:18
Completed NSE at 19:18, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (8 hosts up) scanned in 234.05 seconds
           Raw packets sent: 16180 (726.250KB) | Rcvd: 14880 (616.762KB)
```

3.7 Hping3

i. Take note of the following options: -c, -S, -p, -2 and -F
-c –count packet count

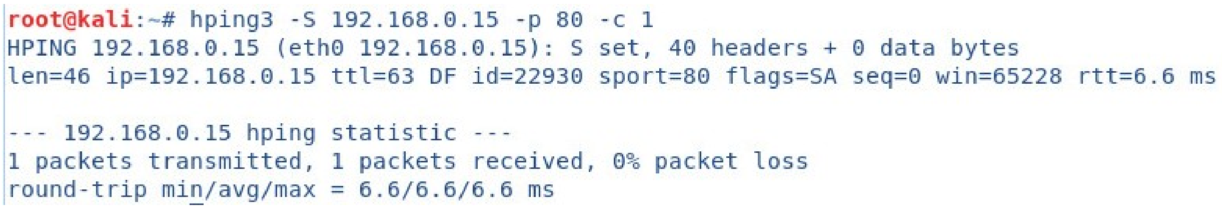
-S –baseport base source port

-p –destport [+][+] <port> destination port (default 0) ctrl+z inc/dec

-2 –udp UDP mode

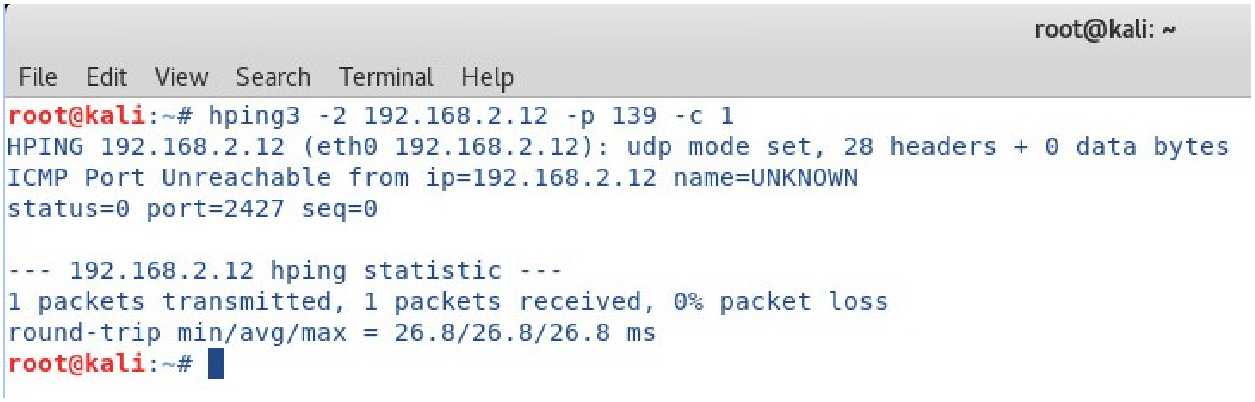
-F –fin Set FIN flag

b. Half-open SYN Scan



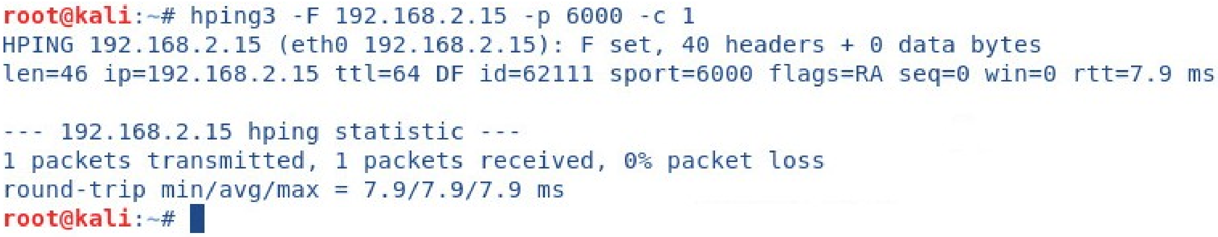
```
root@kali:~# hping3 -S 192.168.0.15 -p 80 -c 1
HPING 192.168.0.15 (eth0 192.168.0.15): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.15 ttl=63 DF id=22930 sport=80 flags=SA seq=0 win=65228 rtt=6.6 ms

--- 192.168.0.15 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 6.6/6.6/6.6 ms
```

c. UDP Scan (target windows computer)



```
root@kali:~# hping3 -2 192.168.2.12 -p 139 -c 1
HPING 192.168.2.12 (eth0 192.168.2.12): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.2.12 name=UNKNOWN
status=0 port=2427 seq=0

--- 192.168.2.12 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 26.8/26.8/26.8 ms
root@kali:~# 
```

d. FIN Scan (used against Debian)



```
root@kali:~# hping3 -F 192.168.2.15 -p 6000 -c 1
HPING 192.168.2.15 (eth0 192.168.2.15): F set, 40 headers + 0 data bytes
len=46 ip=192.168.2.15 ttl=64 DF id=62111 sport=6000 flags=RA seq=0 win=0 rtt=7.9 ms

--- 192.168.2.15 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.9/7.9/7.9 ms
root@kali:~# 
```

Vulnerabilities

No vulnerabilities discovered in this lab.