Port Scanning

Varun Bindra
MS- Management Information System
Texas A&M University

Port scanning and some details about different port

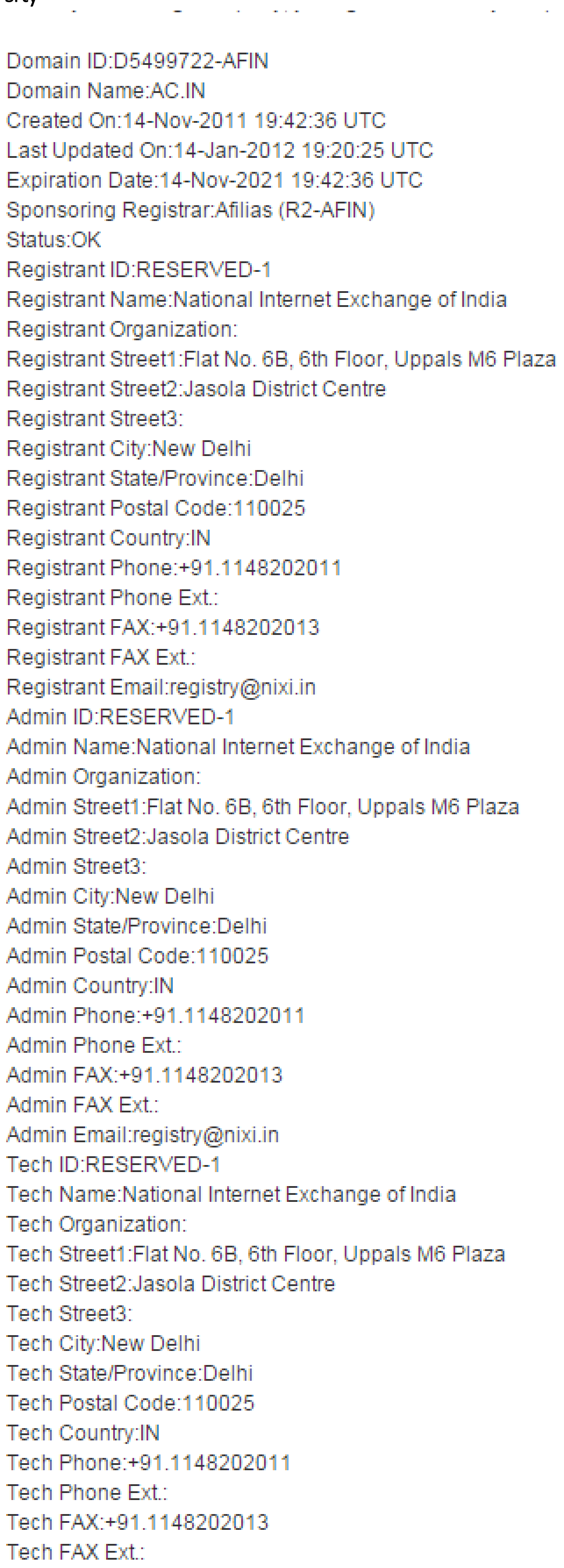
In this paper I will write some details about port scanning and will show how to scan ports using different commands. I will also explain about some ports like FTP, HTTP, mysql etc and how to find out which operating system is used on that port.

To scan I have taken different websites and their IP addresses.

Website name	URL	IP address
CH-Edge maker	http://ch-india.com	66.116.187.104
IIM Lucknow	**http://www.lkouniv.ac.in**	59.165.151.8
Lucknow University	**http://www.lkouniv.ac.in**	182.18.166.206

First I have find out administrative contacts for all the Universities and explained how can a hacker use their phone number and name for authentication purpose. Hacker can guess the password or make possible combination from name and phone number.

All the details about open ports are mention in this paper.

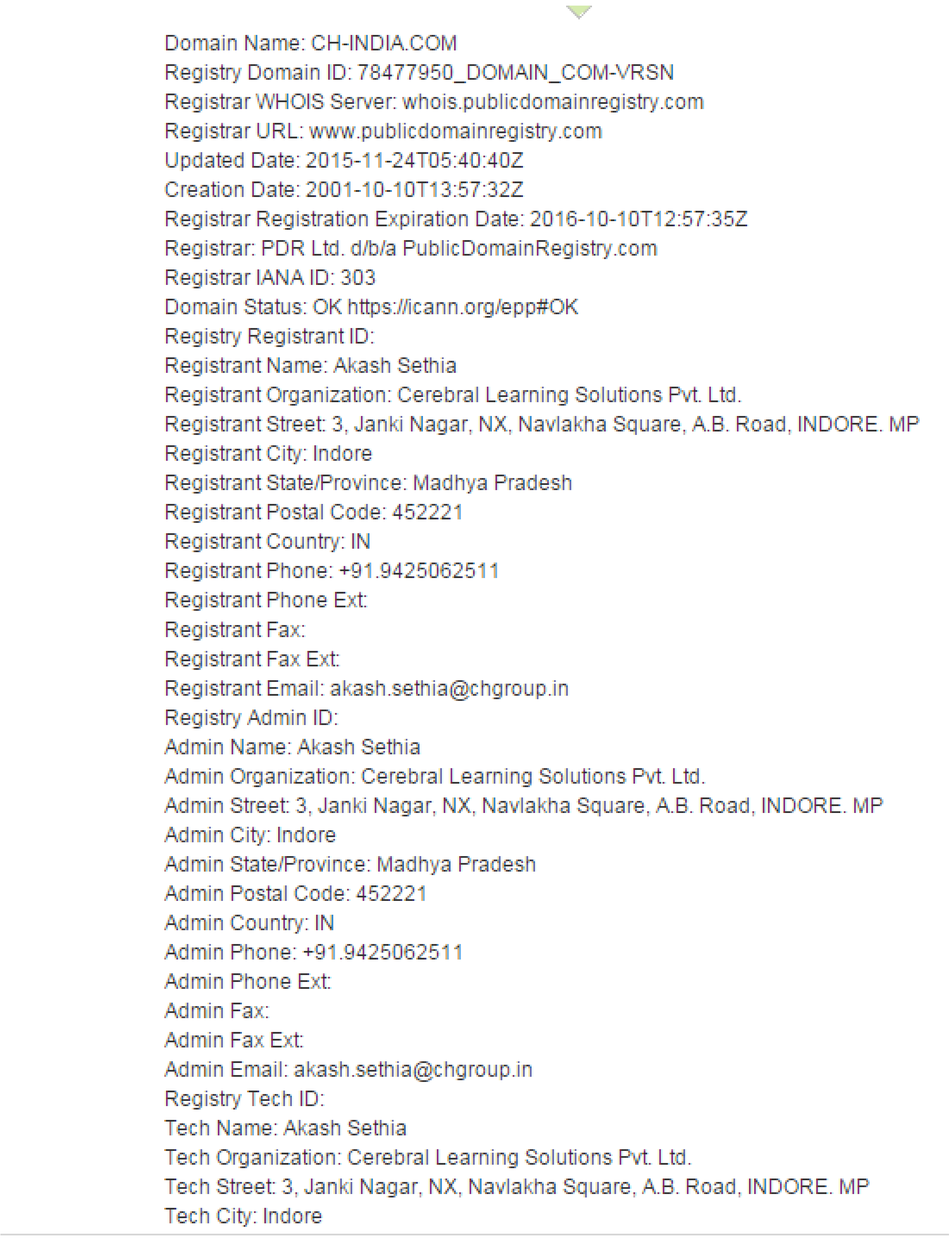


```
Domain ID:D5499722-AFIN
Domain Name:AC.IN
Created On:14-Nov-2011 19:42:36 UTC
Last Updated On:14-Jan-2012 19:20:25 UTC
Expiration Date:14-Nov-2021 19:42:36 UTC
Sponsoring Registrar:Afilias (R2-AFIN)
Status:OK
Registrant ID:RESERVED-1
Registrant Name:National Internet Exchange of India
Registrant Organization:
Registrant Street1:Flat No. 6B, 6th Floor, Uppals M6 Plaza
Registrant Street2:Jasola District Centre
Registrant Street3:
Registrant City:New Delhi
Registrant State/Province:Delhi
Registrant Postal Code:110025
Registrant Country:IN
Registrant Phone:+91.1148202011
Registrant Phone Ext.:
Registrant FAX:+91.1148202013
Registrant FAX Ext.:
Registrant Email:registry@nixi.in
Admin ID:RESERVED-1
Admin Name:National Internet Exchange of India
Admin Organization:
Admin Street1:Flat No. 6B, 6th Floor, Uppals M6 Plaza
Admin Street2:Jasola District Centre
Admin Street3:
Admin City:New Delhi
Admin State/Province:Delhi
Admin Postal Code:110025
Admin Country:IN
Admin Phone:+91.1148202011
Admin Phone Ext.:
Admin FAX:+91.1148202013
Admin FAX Ext.:
Admin Email:registry@nixi.in
Tech ID:RESERVED-1
Tech Name:National Internet Exchange of India
Tech Organization:
Tech Street1:Flat No. 6B, 6th Floor, Uppals M6 Plaza
Tech Street2:Jasola District Centre
Tech Street3:
Tech City:New Delhi
Tech State/Province:Delhi
Tech Postal Code:110025
Tech Country:IN
Tech Phone:+91.1148202011
Tech Phone Ext.:
Tech FAX:+91.1148202013
Tech FAX Ext.:
```

Varun Bindra
MS- Management Information System
Texas A&M University

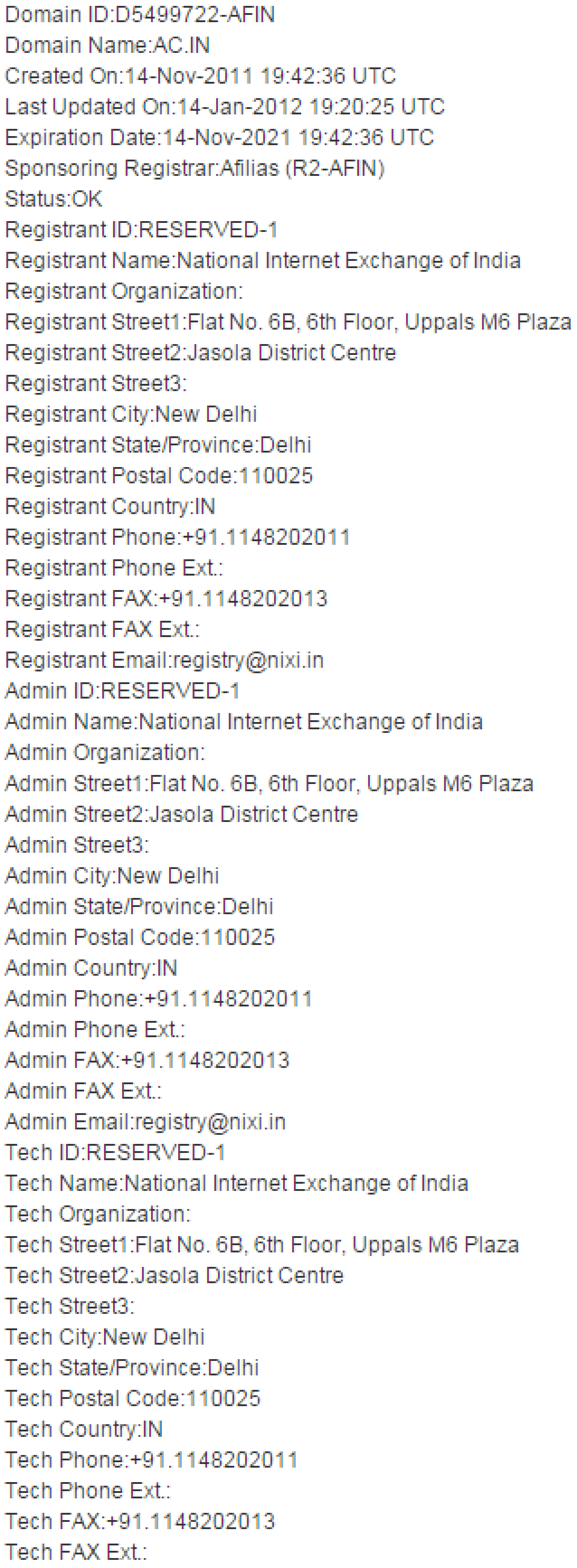
Port Scanning

Administrative contacts for Cerebral Heights:



```
Domain Name: CH-INDIA.COM
Registry Domain ID: 78477950_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2015-11-24T05:40:40Z
Creation Date: 2001-10-10T13:57:32Z
Registrar Registration Expiration Date: 2016-10-10T12:57:35Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: OK https://icann.org/epp#OK
Registry Registrant ID:
Registrant Name: Akash Sethia
Registrant Organization: Cerebral Learning Solutions Pvt. Ltd.
Registrant Street: 3, Janki Nagar, NX, Navlakha Square, A.B. Road, INDORE. MP
Registrant City: Indore
Registrant State/Province: Madhya Pradesh
Registrant Postal Code: 452221
Registrant Country: IN
Registrant Phone: +91.9425062511
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: akash.sethia@chgroup.in
Registry Admin ID:
Admin Name: Akash Sethia
Admin Organization: Cerebral Learning Solutions Pvt. Ltd.
Admin Street: 3, Janki Nagar, NX, Navlakha Square, A.B. Road, INDORE. MP
Admin City: Indore
Admin State/Province: Madhya Pradesh
Admin Postal Code: 452221
Admin Country: IN
Admin Phone: +91.9425062511
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: akash.sethia@chgroup.in
Registry Tech ID:
Tech Name: Akash Sethia
Tech Organization: Cerebral Learning Solutions Pvt. Ltd.
Tech Street: 3, Janki Nagar, NX, Navlakha Square, A.B. Road, INDORE. MP
Tech City: Indore
```

Administrative contacts for IIM Lucknow:



```
Domain ID:D5499722-AFIN
Domain Name:AC.IN
Created On:14-Nov-2011 19:42:36 UTC
Last Updated On:14-Jan-2012 19:20:25 UTC
Expiration Date:14-Nov-2021 19:42:36 UTC
Sponsoring Registrar:Afilias (R2-AFIN)
Status:OK
Registrant ID:RESERVED-1
Registrant Name:National Internet Exchange of India
Registrant Organization:
Registrant Street1:Flat No. 6B, 6th Floor, Uppals M6 Plaza
Registrant Street2:Jasola District Centre
Registrant Street3:
Registrant City:New Delhi
Registrant State/Province:Delhi
Registrant Postal Code:110025
Registrant Country:IN
Registrant Phone:+91.1148202011
Registrant Phone Ext.:
Registrant FAX:+91.1148202013
Registrant FAX Ext.:
Registrant Email:registry@nixi.in
Admin ID:RESERVED-1
Admin Name:National Internet Exchange of India
Admin Organization:
Admin Street1:Flat No. 6B, 6th Floor, Uppals M6 Plaza
Admin Street2:Jasola District Centre
Admin Street3:
Admin City:New Delhi
Admin State/Province:Delhi
Admin Postal Code:110025
Admin Country:IN
Admin Phone:+91.1148202011
Admin Phone Ext.:
Admin FAX:+91.1148202013
Admin FAX Ext.:
Admin Email:registry@nixi.in
Tech ID:RESERVED-1
Tech Name:National Internet Exchange of India
Tech Organization:
Tech Street1:Flat No. 6B, 6th Floor, Uppals M6 Plaza
Tech Street2:Jasola District Centre
Tech Street3:
Tech City:New Delhi
Tech State/Province:Delhi
Tech Postal Code:110025
Tech Country:IN
Tech Phone:+91.1148202011
Tech Phone Ext.:
Tech FAX:+91.1148202013
Tech FAX Ext.:
```

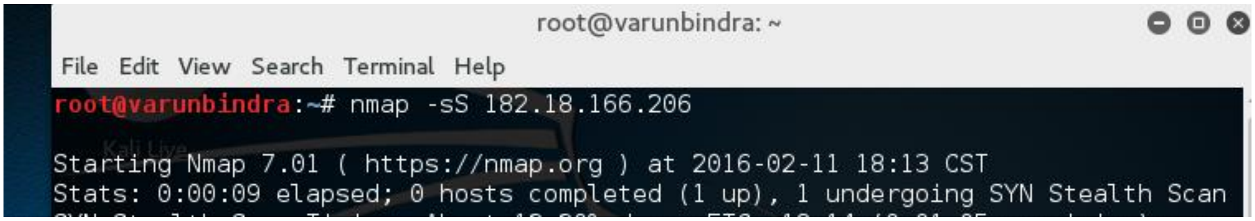
Varun Bindra
MS- Management Information System
Texas A&M University

Port Scanning

Administrative contacts are located in contact tab of website. A hacker can use their phone number and name for authentication purpose. Hacker can guess the password or make possible combination from name and phone number.

Port Scanning: 182.18.166.206

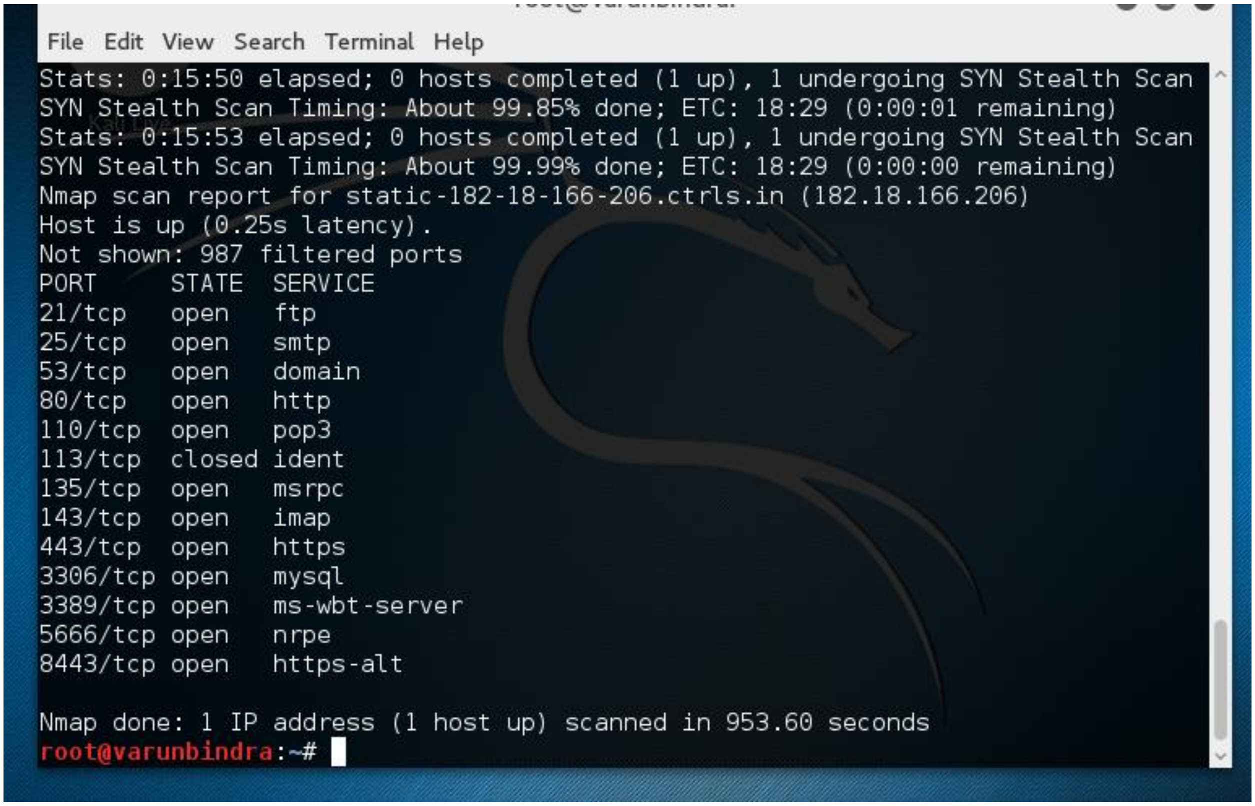
Command Used : - nmap –sS 182.12.166.206



```
root@varunbindra:~# nmap -sS 182.18.166.206

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-11 18:13 CST
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
```

Varun Bindra
MS- Management Information System
Texas A&M University

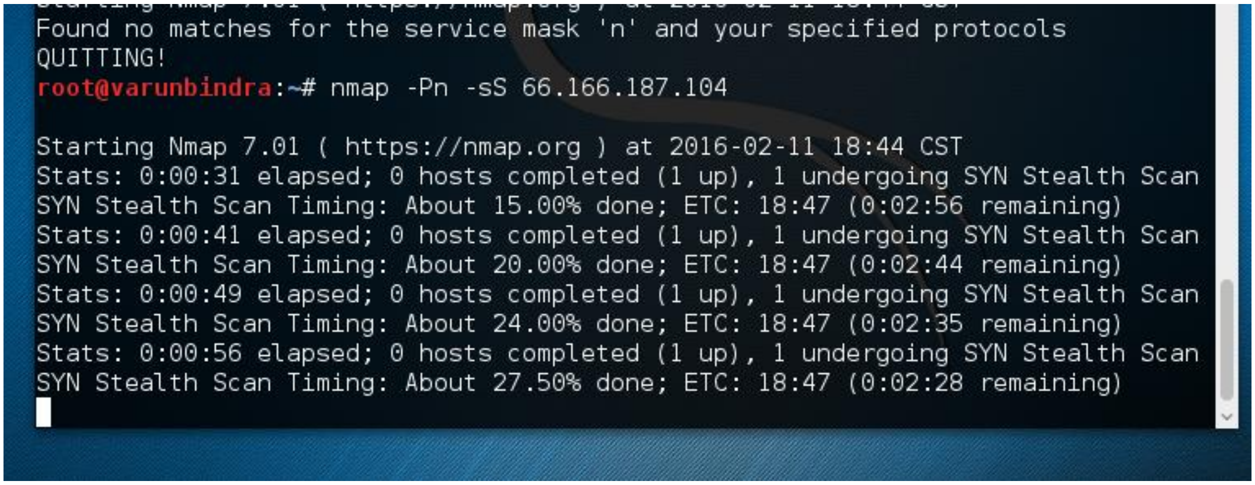
Port Scanning



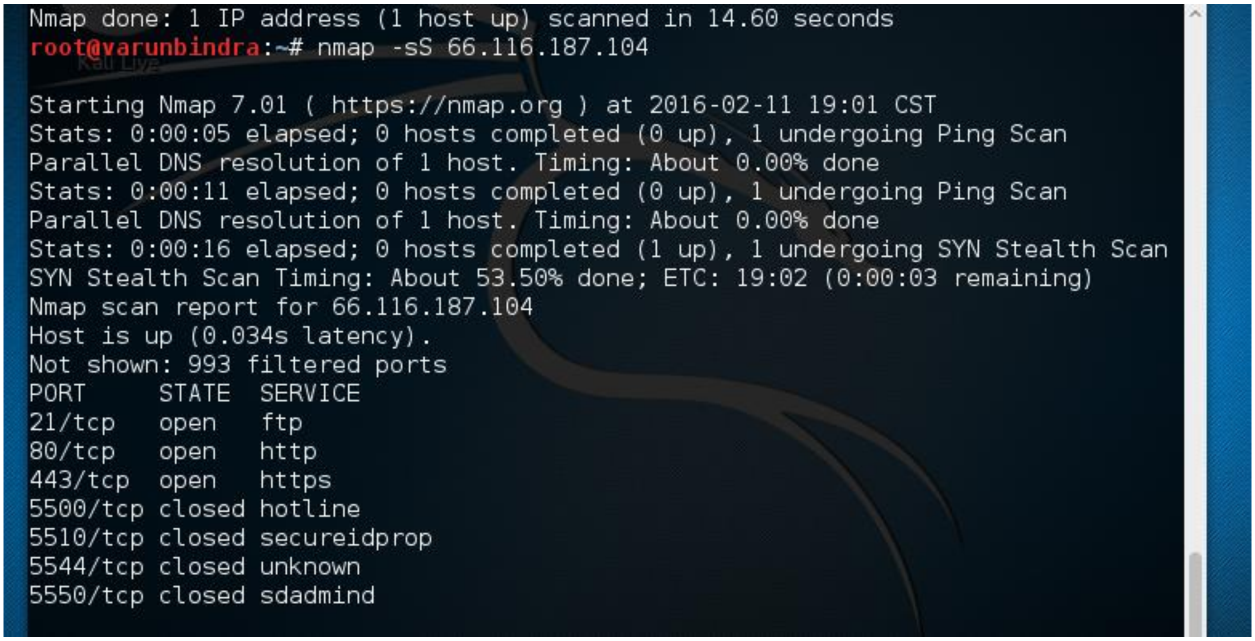
```
Stats: 0:15:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.85% done; ETC: 18:29 (0:00:01 remaining)
Stats: 0:15:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 18:29 (0:00:00 remaining)
Nmap scan report for static-182-18-166-206.ctrls.in (182.18.166.206)
Host is up (0.25s latency).
Not shown: 987 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
25/tcp   open   smtp
53/tcp   open   domain
80/tcp   open   http
110/tcp  open   pop3
113/tcp  closed ident
135/tcp  open   msrpc
143/tcp  open   imap
443/tcp  open   https
3306/tcp open   mysql
3389/tcp open   ms-wbt-server
5666/tcp open   nrpe
8443/tcp open   https-alt

Nmap done: 1 IP address (1 host up) scanned in 953.60 seconds
root@varunbindra:~#
```

Port Scanning: 66.116.187.104

Command Used : - nmap –sS 66.116.187.104



```
Found no matches for the service mask 'n' and your specified protocols
QUITTING!
root@varunbindra:~# nmap -Pn -sS 66.166.187.104

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-11 18:44 CST
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 15.00% done; ETC: 18:47 (0:02:56 remaining)
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.00% done; ETC: 18:47 (0:02:44 remaining)
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.00% done; ETC: 18:47 (0:02:35 remaining)
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.50% done; ETC: 18:47 (0:02:28 remaining)
```



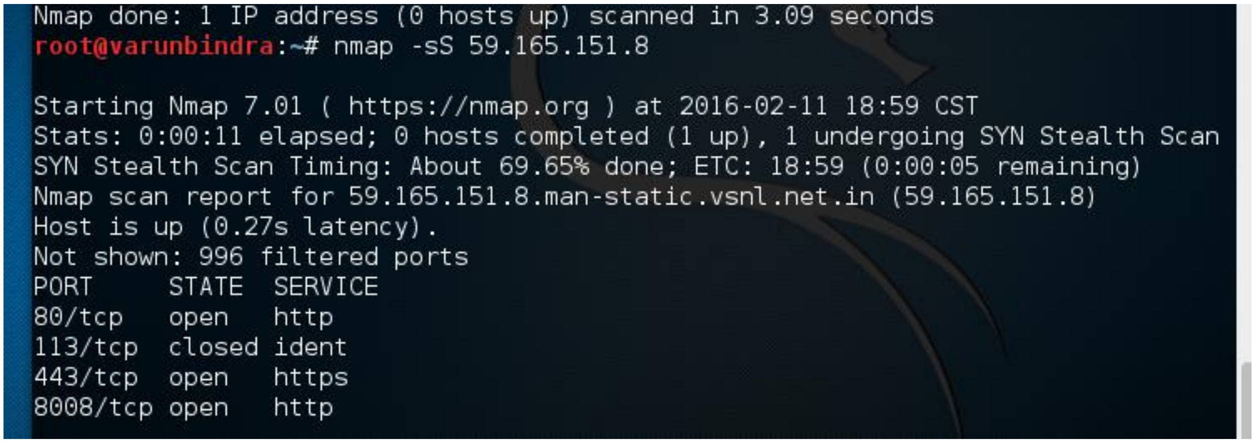
```
Nmap done: 1 IP address (1 host up) scanned in 14.60 seconds
root@varunbindra:~# nmap -sS 66.116.187.104

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-11 19:01 CST
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:11 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 53.50% done; ETC: 19:02 (0:00:03 remaining)
Nmap scan report for 66.116.187.104
Host is up (0.034s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
80/tcp   open   http
443/tcp  open   https
5500/tcp closed hotline
5510/tcp closed secureidprop
5544/tcp closed unknown
5550/tcp closed sdadmind
```

Port Scanning: 59.165.151.8

Command Used : - nmap –sS 59.165.151.8

Varun Bindra
MS- Management Information System
Texas A&M University

Port Scanning



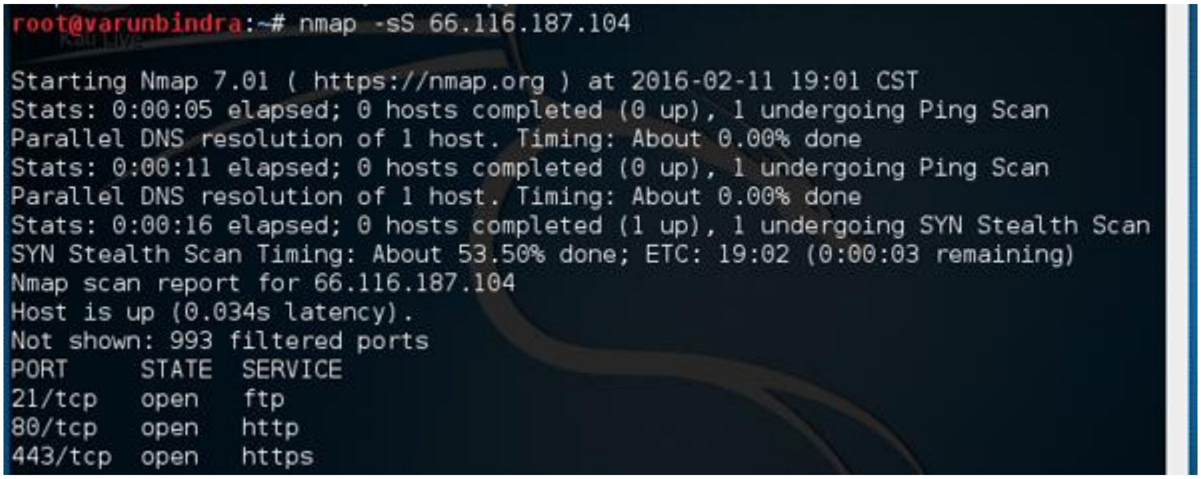
```
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
root@varunbindra:~# nmap -sS 59.165.151.8

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-11 18:59 CST
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.65% done; ETC: 18:59 (0:00:05 remaining)
Nmap scan report for 59.165.151.8.man-static.vsnl.net.in (59.165.151.8)
Host is up (0.27s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
8008/tcp open   http
```

We used nmap –sS command because this technique is often referred to as "half-open" scanning, because you don’t open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response.

Ports open for - 66.116.187.104

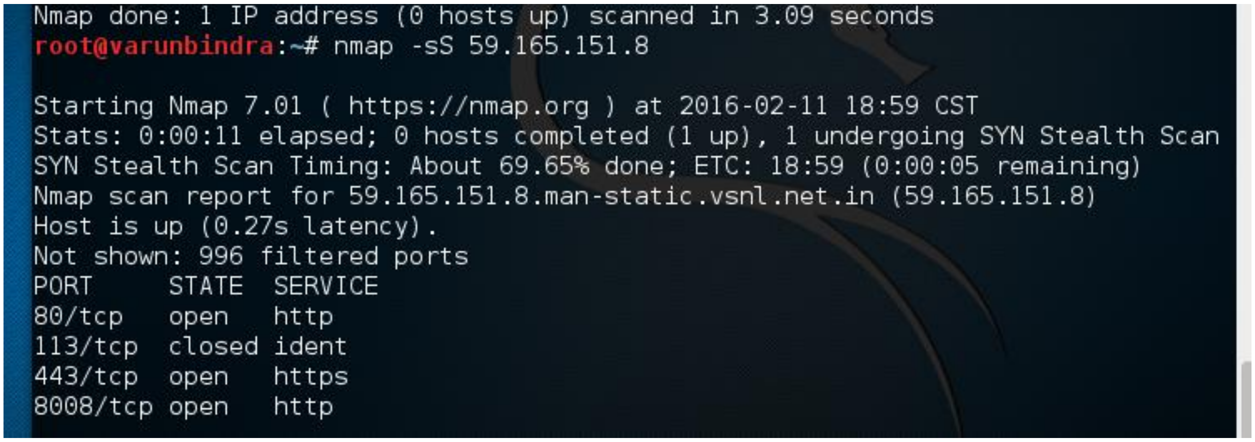
Varun Bindra
MS- Management Information System
Texas A&M University

Port Scanning



```
root@varunbindra:~# nmap -sS 66.116.187.104

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-11 19:01 CST
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:11 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 53.50% done; ETC: 19:02 (0:00:03 remaining)
Nmap scan report for 66.116.187.104
Host is up (0.034s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
80/tcp   open   http
443/tcp  open   https
```

Ports open for - 59.165.151.8

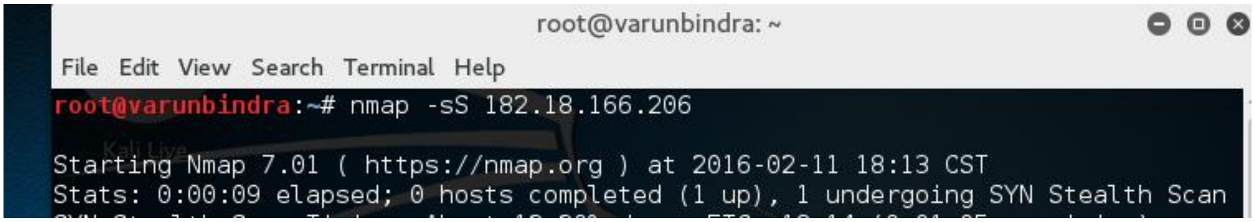


```
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
root@varunbindra:~# nmap -sS 59.165.151.8

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-11 18:59 CST
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.65% done; ETC: 18:59 (0:00:05 remaining)
Nmap scan report for 59.165.151.8.man-static.vsnl.net.in (59.165.151.8)
Host is up (0.27s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
8008/tcp open   http
```

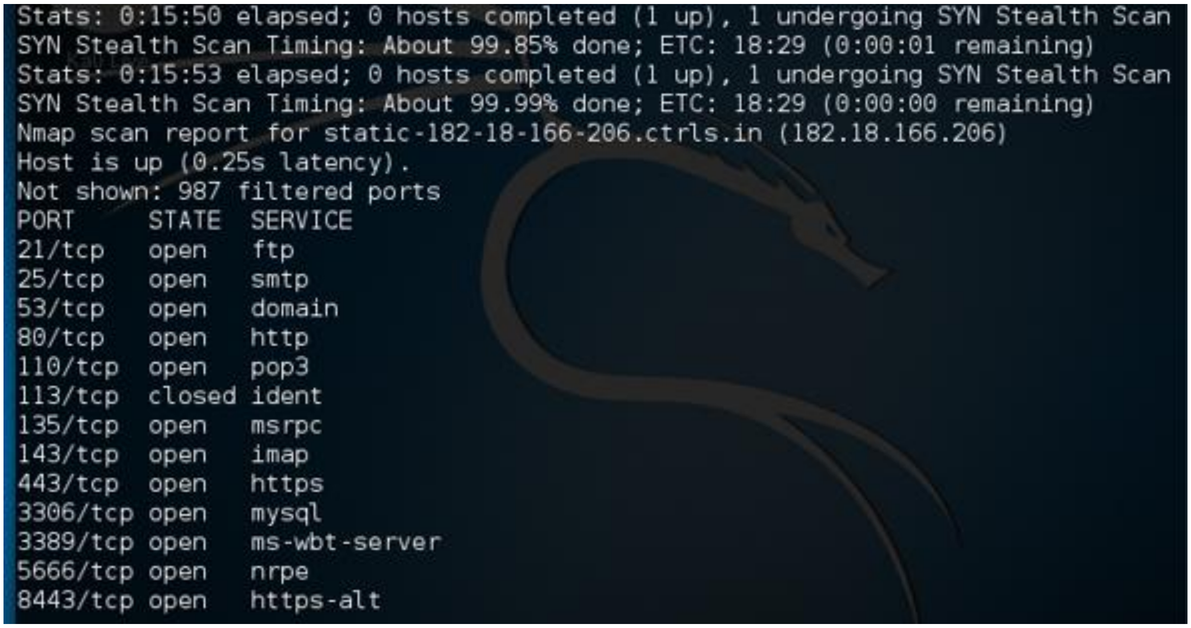
Ports open for - 182.18.166.206

Varun Bindra
MS- Management Information System
Texas A&M University

Port Scanning



```
root@varunbindra:~# nmap -sS 182.18.166.206

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-11 18:13 CST
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
```



```
Stats: 0:15:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.85% done; ETC: 18:29 (0:00:01 remaining)
Stats: 0:15:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 18:29 (0:00:00 remaining)
Nmap scan report for static-182-18-166-206.ctrls.in (182.18.166.206)
Host is up (0.25s latency).
Not shown: 987 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
25/tcp   open   smtp
53/tcp   open   domain
80/tcp   open   http
110/tcp  open   pop3
113/tcp  closed ident
135/tcp  open   msrpc
143/tcp  open   imap
443/tcp  open   https
3306/tcp open   mysql
3389/tcp open   ms-wbt-server
5666/tcp open   nrpe
8443/tcp open   https-alt
```

Open port for ip: 66.116.187.104 is FTP

FTP:

FTP is used in Web Servers for accessing the files remotely. Hackers identify the version of FTP application by using method called FTP banner grabbing. Banner grabbing is technique is used to extract information of individual. Banner grabbing can give you information about what type of operating system, web server. This can be a useful information for hackers and can proceed further to hack other important details.

Open port for ip: 59.165.151.8 is http

http: -

One of the common attack on http is session fixation attack in which force user session ID to an explicit value. The hacker can fix the session value according to his needs. After this the hacker will wait for the user to login to their system once. Once the user login to their systems and by using that he can extract valuable information.

Open port for ip: 182.18.166.206 is mysql

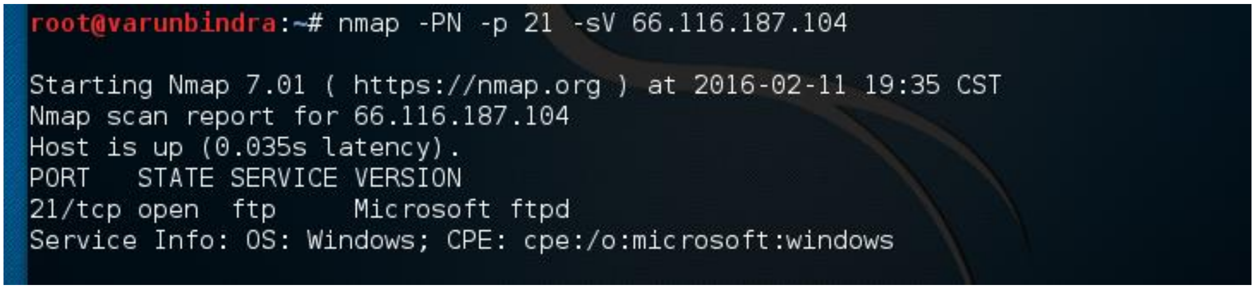
Hacker can attack to mysql through brute-force attack in which hacker look for the week password. It mounts against the services running on version 5.x. Hacker can find week password easily and he can extract valuable information through this attack.

Varun Bindra
MS- Management Information System
Texas A&M University

Port Scanning

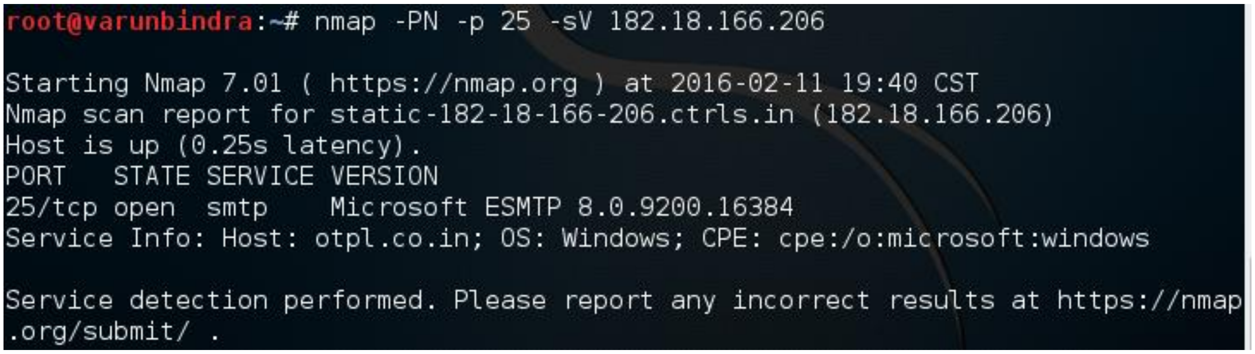
Method to find out which operating system is running on the host?

1) **For** 66.116.187.104 **: - nmap –PN –p 21 –sV** 66.116.187.104 **(Microsoft)**



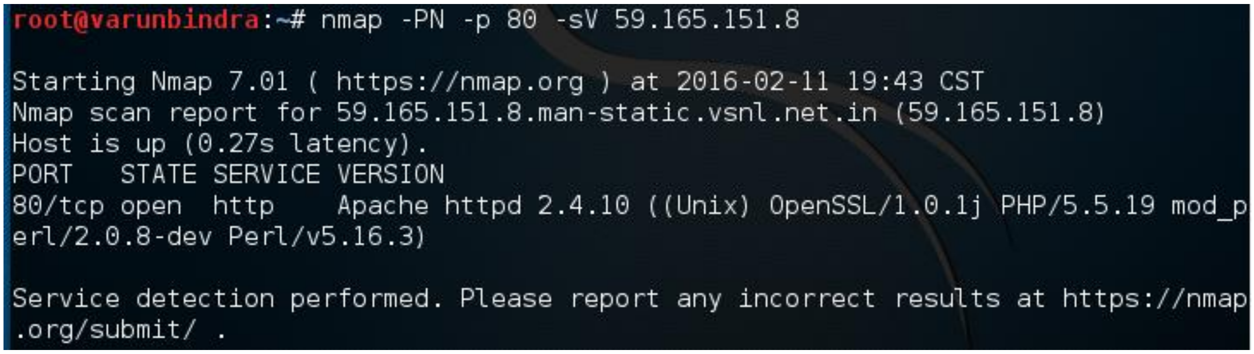
```
root@varunbindra:~# nmap -PN -p 21 -sV 66.116.187.104

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-11 19:35 CST
Nmap scan report for 66.116.187.104
Host is up (0.035s latency).
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

2) **For 182.18.166.206 : - nmap –PN –p 21 –sV 182.18.166.206 (Microsoft)**



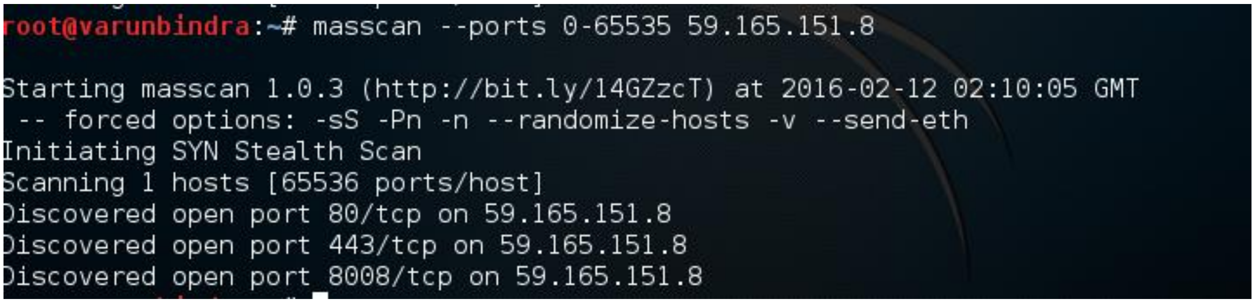
```
root@varunbindra:~# nmap -PN -p 25 -sV 182.18.166.206

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-11 19:40 CST
Nmap scan report for static-182-18-166-206.ctrls.in (182.18.166.206)
Host is up (0.25s latency).
PORT   STATE SERVICE VERSION
25/tcp open  smtp    Microsoft ESMTP 8.0.9200.16384
Service Info: Host: otpl.co.in; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
```

3) For 59.165.151.8 : - nmap –PN –p 21 –sV 59.165.151.8 (Apache)

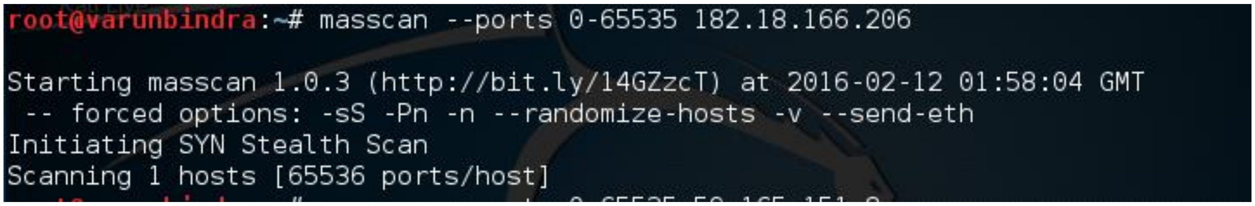


```
root@varunbindra:~# nmap -PN -p 80 -sV 59.165.151.8

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-11 19:43 CST
Nmap scan report for 59.165.151.8.man-static.vsnl.net.in (59.165.151.8)
Host is up (0.27s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.10 ((Unix) OpenSSL/1.0.1j PHP/5.5.19 mod_p
erl/2.0.8-dev Perl/v5.16.3)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
```

Using masscan on different ports



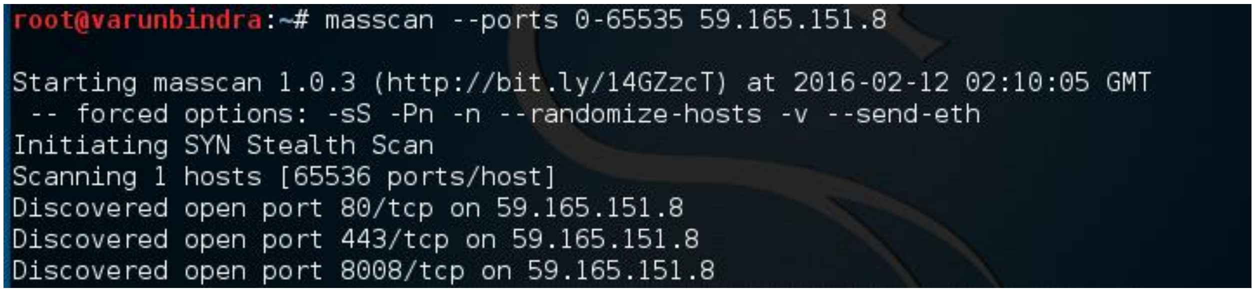
```
root@varunbindra:~# masscan --ports 0-65535 59.165.151.8

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2016-02-12 02:10:05 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
Discovered open port 80/tcp on 59.165.151.8
Discovered open port 443/tcp on 59.165.151.8
Discovered open port 8008/tcp on 59.165.151.8
```



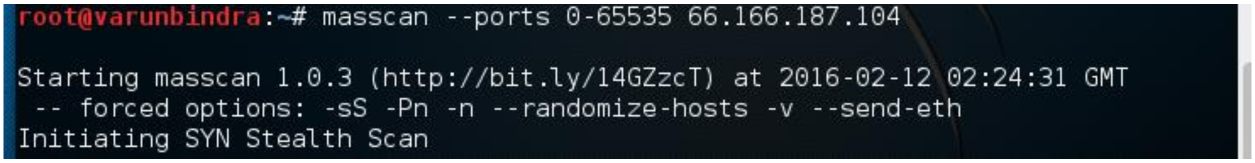
```
root@varunbindra:~# masscan --ports 0-65535 182.18.166.206

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2016-02-12 01:58:04 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
```

Varun Bindra
MS- Management Information System
Texas A&M University

Port Scanning

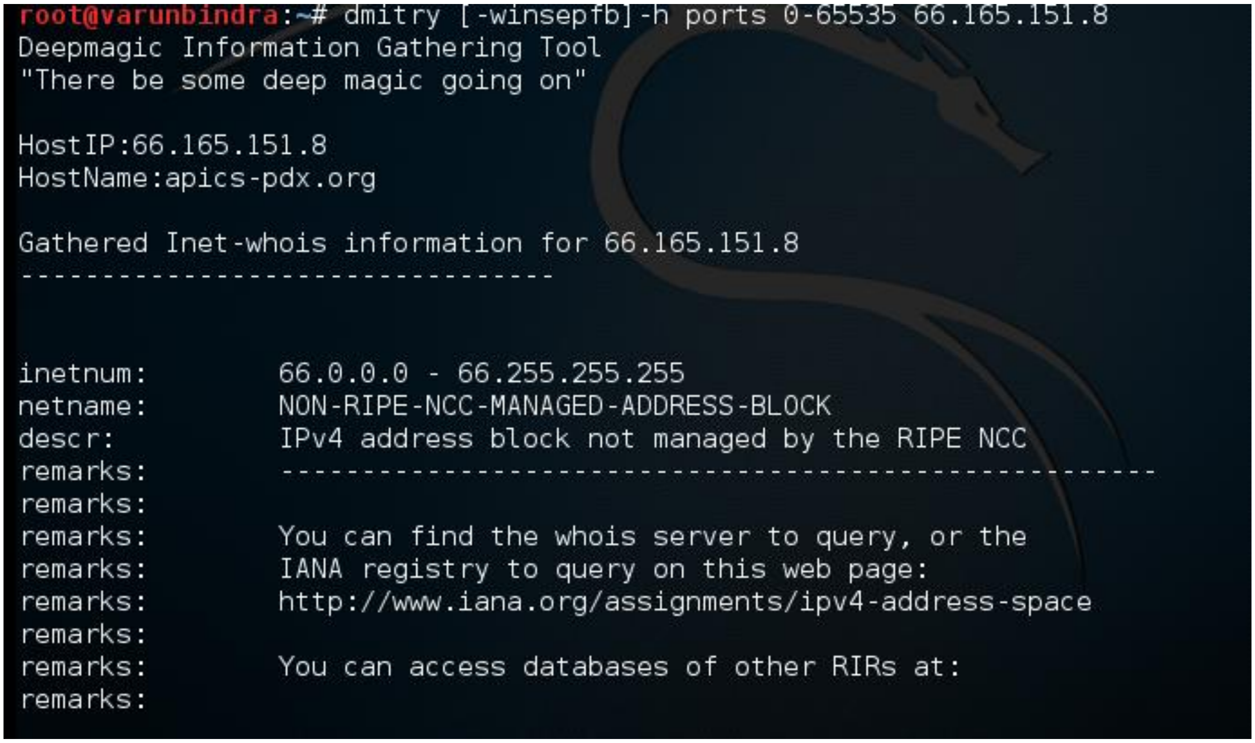


```
root@varunbindra:~# masscan --ports 0-65535 59.165.151.8

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2016-02-12 02:10:05 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
Discovered open port 80/tcp on 59.165.151.8
Discovered open port 443/tcp on 59.165.151.8
Discovered open port 8008/tcp on 59.165.151.8
```



```
root@varunbindra:~# masscan --ports 0-65535 66.166.187.104

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2016-02-12 02:24:31 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
```

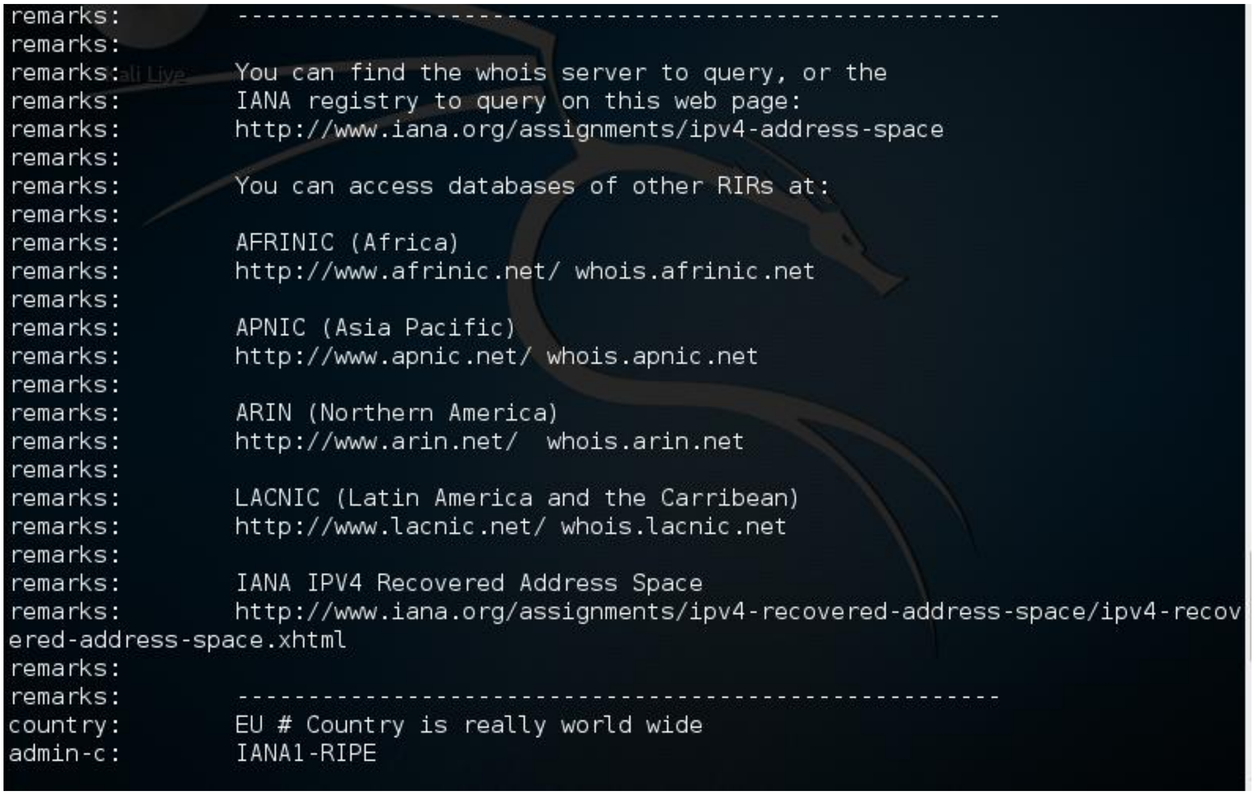
Using command : dmitry [-winsepfb] –h ports



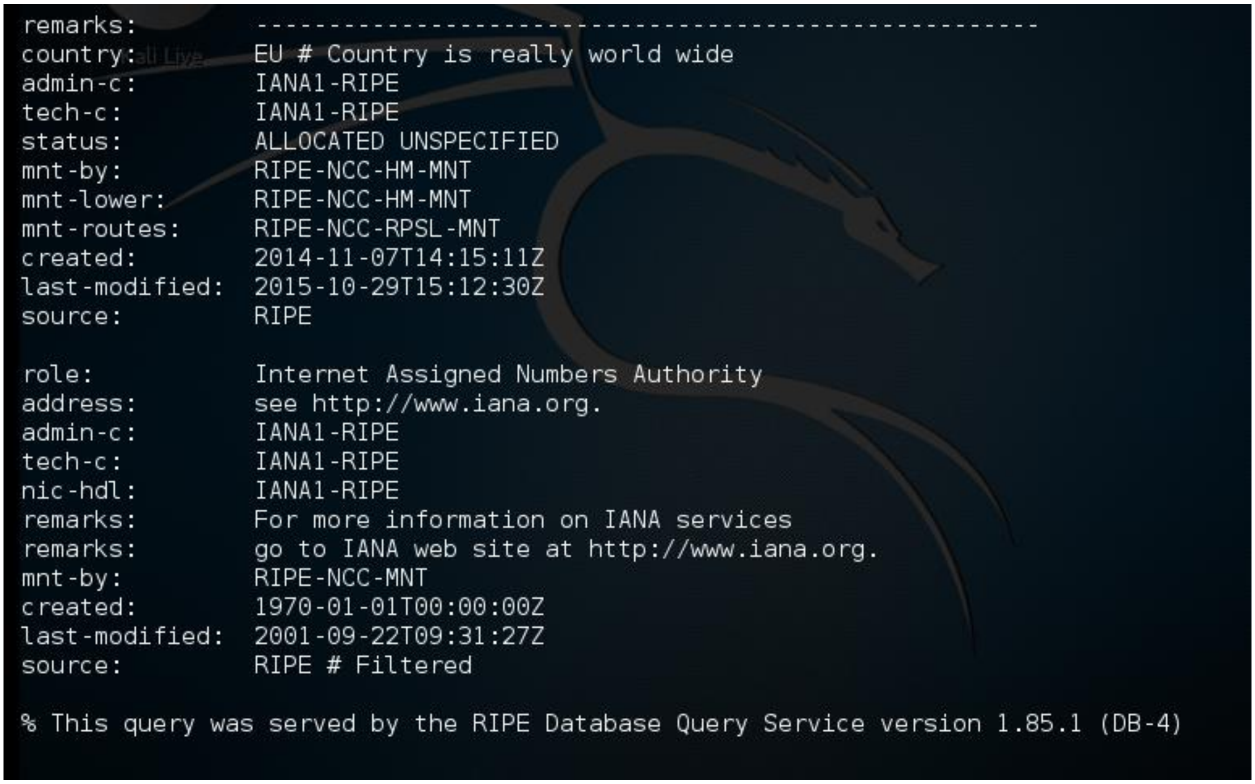
```
root@varunbindra:~# dmitry [-winsepfb]-h ports 0-65535 66.165.151.8
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:66.165.151.8
HostName:apics-pdx.org

Gathered Inet-whois information for 66.165.151.8
---------------------------------


inetnum:        66.0.0.0 - 66.255.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        You can find the whois server to query, or the
remarks:        IANA registry to query on this web page:
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:
remarks:        You can access databases of other RIRs at:
remarks:
```

Varun Bindra
MS- Management Information System
Texas A&M University

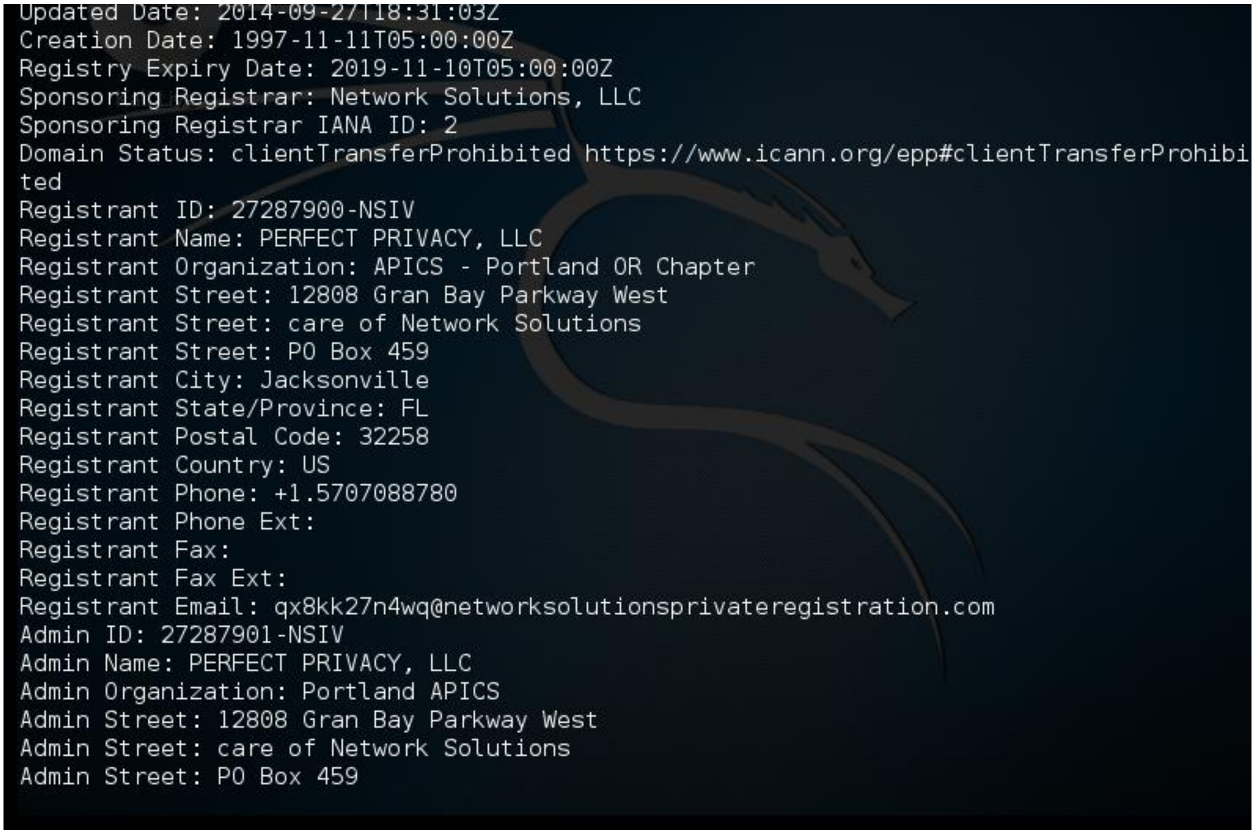
Port Scanning



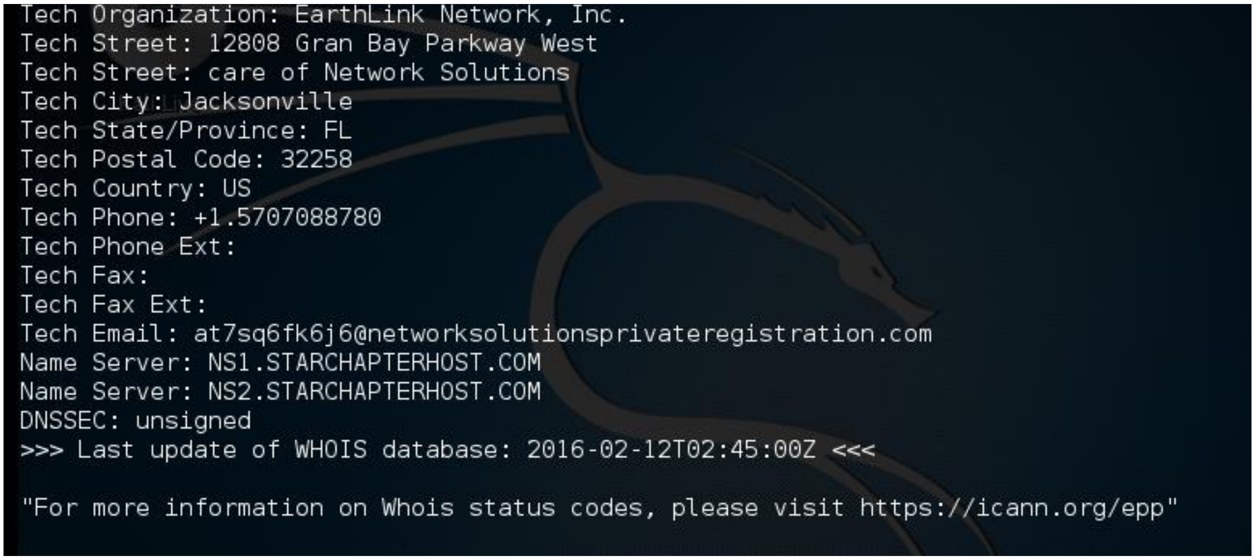
```
remarks:        ------------------------------------------------------
remarks:
remarks:        You can find the whois server to query, or the
remarks:        IANA registry to query on this web page:
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:
remarks:        You can access databases of other RIRs at:
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/  whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        IANA IPV4 Recovered Address Space
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space/ipv4-recov
ered-address-space.xhtml
remarks:
remarks:        ------------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
```



```
remarks:        ------------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
mnt-lower:      RIPE-NCC-HM-MNT
mnt-routes:     RIPE-NCC-RPSL-MNT
created:        2014-11-07T14:15:11Z
last-modified:  2015-10-29T15:12:30Z
source:         RIPE

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.85.1 (DB-4)
```



```
Updated Date: 2014-09-27T18:31:03Z
Creation Date: 1997-11-11T05:00:00Z
Registry Expiry Date: 2019-11-10T05:00:00Z
Sponsoring Registrar: Network Solutions, LLC
Sponsoring Registrar IANA ID: 2
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibi
ted
Registrant ID: 27287900-NSIV
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization: APICS - Portland OR Chapter
Registrant Street: 12808 Gran Bay Parkway West
Registrant Street: care of Network Solutions
Registrant Street: PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32258
Registrant Country: US
Registrant Phone: +1.5707088780
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: qx8kk27n4wq@networksolutionsprivateregistration.com
Admin ID: 27287901-NSIV
Admin Name: PERFECT PRIVACY, LLC
Admin Organization: Portland APICS
Admin Street: 12808 Gran Bay Parkway West
Admin Street: care of Network Solutions
Admin Street: PO Box 459
```

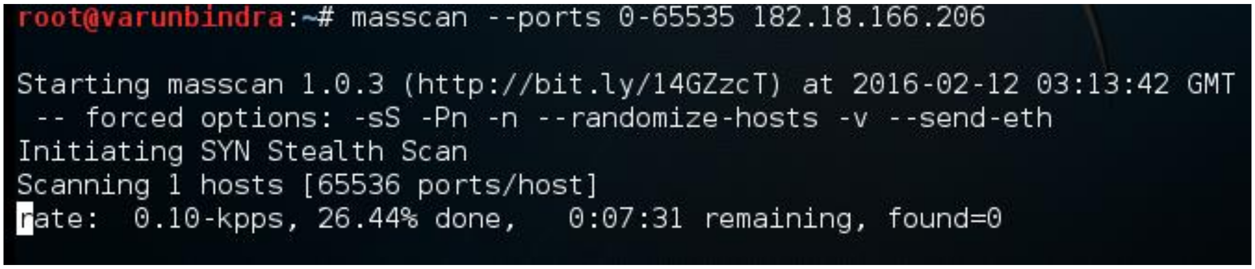


```
Tech Organization: EarthLink Network, Inc.
Tech Street: 12808 Gran Bay Parkway West
Tech Street: care of Network Solutions
Tech City: Jacksonville
Tech State/Province: FL
Tech Postal Code: 32258
Tech Country: US
Tech Phone: +1.5707088780
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: at7sq6fk6j6@networksolutionsprivateregistration.com
Name Server: NS1.STARCHAPTERHOST.COM
Name Server: NS2.STARCHAPTERHOST.COM
DNSSEC: unsigned
>>> Last update of WHOIS database: 2016-02-12T02:45:00Z <<<

"For more information on Whois status codes, please visit https://icann.org/epp"
```

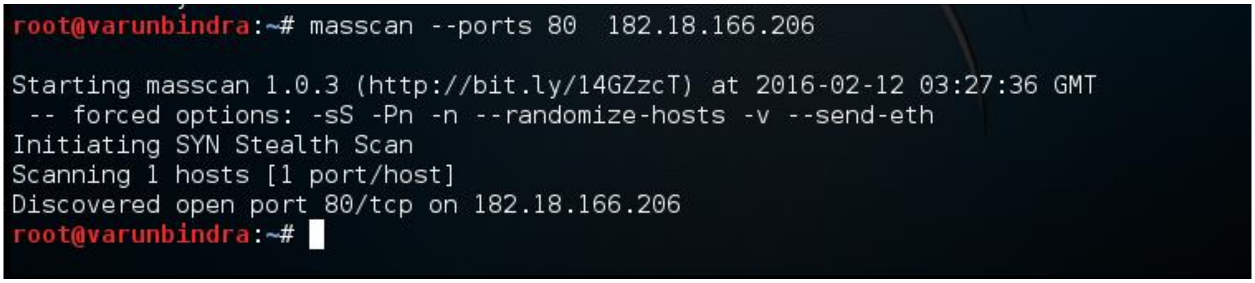
Msscan For Port : 182.18.166.206

Varun Bindra
MS- Management Information System
Texas A&M University

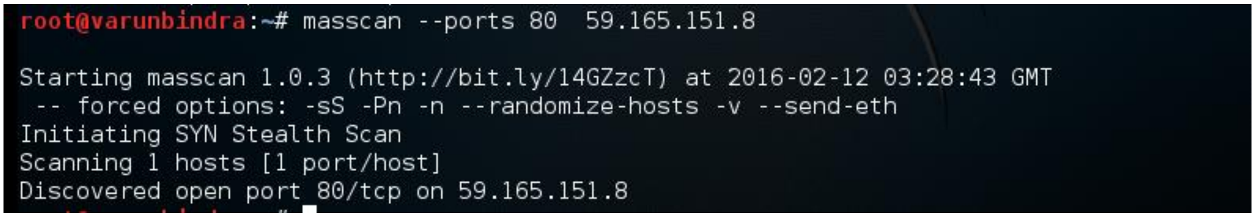
Port Scanning



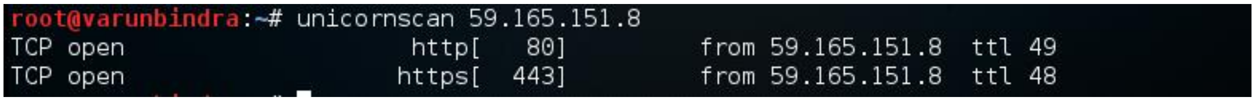
```
root@varunbindra:~# masscan --ports 0-65535 182.18.166.206

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2016-02-12 03:13:42 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
rate:  0.10-kpps, 26.44% done,   0:07:31 remaining, found=0
```



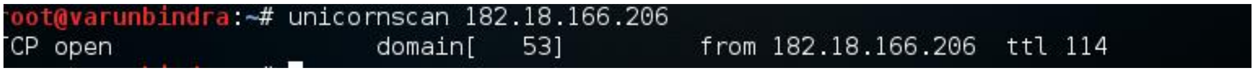
```
root@varunbindra:~# masscan --ports 80  182.18.166.206

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2016-02-12 03:27:36 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
Discovered open port 80/tcp on 182.18.166.206
root@varunbindra:~#
```



```
root@varunbindra:~# masscan --ports 80  59.165.151.8

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2016-02-12 03:28:43 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
Discovered open port 80/tcp on 59.165.151.8
```



```
root@varunbindra:~# unicornscan 59.165.151.8
TCP open                     http[   80]         from 59.165.151.8  ttl 49
TCP open                    https[  443]         from 59.165.151.8  ttl 48
```



```
oot@varunbindra:~# unicornscan 182.18.166.206
CP open                    domain[   53]         from 182.18.166.206  ttl 114
```