Penetration Tools

CSC 154

Overview of Penetration Tools

- Linux tools
  - Gathering information of local systems
    - hostname/uname
    - ifconfig
    - who, last
    - ps
    - lsof
    - tcpdump
    - wireshark/etheral (also remote systems)
    - …
  - Gathering information of remote systems
    - ping
    - traceroute
    - finger (also local systems)
    - nslookup, dig
    - whois
    - arp, netstat (also local systems)
    - nmap
    - …
  - Collected tools
    - Metasploit
    - BackTrack/Kali Linux

- Window tools
  - Gathering information of local system
    - hostname
    - ipconfig
    - wireshark/etheral (also remote systems)
    - …
  - Gathering information of remote systems
    - ping
    - tracert
    - finger (also local system)
    - nslookup
    - arp, netstat (also local system)
    - nmap
    - …
  - Collected tools
    - Sam Spade

hostname(1)-Linux man page

- Show or set the system's host name
- Usage:
  - Gather/Manipulate:
    - host name
  - Example:
    - hostname
      - watermelon

Metasploitable - VMware Workstation

File Edit View VM Tabs Help

Home | Metasploitable

```
msfadmin@metasploitable:~/labs/p-buffer$ hostname
metasploitable
msfadmin@metasploitable:~/labs/p-buffer$ _
```

To direct input to this VM, click inside or press Ctrl+G.

uname(1)-Linu man page

- Print the information about the current system
- Usage:
  - Gather/Manipulate:
    - OS type and version
  - Example:
    - uname –a
      - SunOS hope 5.7 Generic_106541-08 sun4m sparc SUNW,SPARCstation-10

Metasploitable - VMware Workstation

File Edit View VM Tabs Help

Home | Metasploitable

```
msfadmin@metasploitable:~/labs/p-buffer$ hostname
metasploitable
msfadmin@metasploitable:~/labs/p-buffer$ uname -ar
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
msfadmin@metasploitable:~/labs/p-buffer$ _
```

To direct input to this VM, click inside or press Ctrl+G.

ifconfig(8)-Linux man page

- Configure a network interface
- Usage:
  - Gather/Manipulate:
    - IP address
    - HW address
  - Example:
    - ifconfig –a
      - run “ifconfig” on Linux or “ipconfig” on Windows for example result
    - ifconfig eth0 down

Metasploitable - VMware Workstation

File Edit View VM Tabs Help

Home | Metasploitable

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9a:f7:57
          inet6 addr: fe80::20c:29ff:fe9a:f757/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6256 (6.1 KB)  TX bytes:6624 (6.4 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:69793 (68.1 KB)  TX bytes:69793 (68.1 KB)

msfadmin@metasploitable:~$ _
```

To direct input to this VM, click inside or press Ctrl+G.

who(1)-Linux man page

- Displays who is logged on to the system
- Usage:
  - Gather/Mannipulate:
    - user logins
      - unusual: activities of inactive accounts
  - Example
    - who
    - who am I
      - Jack pts/3 2014-09-17 09:37(:0.0)

Metasploitable - VMware Workstation

File Edit View VM Tabs Help

Home | Metasploitable

```
msfadmin@metasploitable:~/labs/p-buffer$ who
msfadmin tty1         2015-10-05 17:05
msfadmin@metasploitable:~/labs/p-buffer$ _
```

To direct input to this VM, click inside or press Ctrl+G.

last(1)-Linux man page

- Show listing of last logged in users
- Usage:
  - Gather/Manipulate:
    - recent user logins
  - Example:
    - last -3

```
jack pts/1    137.138.255.237   Sun Sep  14 16:32   still logged in
lucy    pts/0       137.138.131.73     Sat Sep 13 17:58   still logged in
james pts/0       c48.193.173.92.e    Fri Sep 12 19:53 - 05:03 (09:09)
```

Metasploitable - VMware Workstation

File Edit View VM Tabs Help

Home | Metasploitable

```
msfadmin@metasploitable:~/labs/p-buffer$ who
msfadmin tty1         2015-10-05 17:05
msfadmin@metasploitable:~/labs/p-buffer$ last -3
msfadmin tty1                         Mon Oct  5 17:05   still logged in
msfadmin tty1                         Mon Oct  5 17:05 - 17:05  (00:00)
reboot   system boot  2.6.24-16-server Mon Oct  5 17:02 - 03:19  (10:16)

wtmp begins Mon May 17 21:45:07 2010
msfadmin@metasploitable:~/labs/p-buffer$ _
```

To direct input to this VM, click inside or press Ctrl+G.

ps(1)-Linux man page

- Report a snapshot of the current processes
- Usage:
  - Gather/Manipulate
    - Current processes
  - Example
    - ps aux
      - run “ps aux” in Linux to see an example result
      - ps aux|grep

Metasploitable - VMware Workstation

File Edit View VM Tabs Help

Home | Metasploitable

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3   2844  1696 ?        Ss   Oct05   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   Oct05   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   Oct05   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   Oct05   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   Oct05   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   Oct05   0:00 [migration/1]
root         7  0.0  0.0      0     0 ?        S<   Oct05   0:00 [ksoftirqd/1]
root         8  0.0  0.0      0     0 ?        S<   Oct05   0:00 [watchdog/1]
root         9  0.0  0.0      0     0 ?        S<   Oct05   0:00 [events/0]
root        10  0.0  0.0      0     0 ?        S<   Oct05   0:00 [events/1]
root        11  0.0  0.0      0     0 ?        S<   Oct05   0:00 [khelper]
root        46  0.0  0.0      0     0 ?        S<   Oct05   0:00 [kblockd/0]
root        47  0.0  0.0      0     0 ?        S<   Oct05   0:00 [kblockd/1]
root        50  0.0  0.0      0     0 ?        S<   Oct05   0:00 [kacpid]
root        51  0.0  0.0      0     0 ?        S<   Oct05   0:00 [kacpi_notify]
root       181  0.0  0.0      0     0 ?        S<   Oct05   0:00 [kseriod]
root       225  0.0  0.0      0     0 ?        S    Oct05   0:00 [pdflush]
root       226  0.0  0.0      0     0 ?        S    Oct05   0:00 [pdflush]
root       227  0.0  0.0      0     0 ?        S<   Oct05   0:00 [kswapd0]
root       269  0.0  0.0      0     0 ?        S<   Oct05   0:00 [aio/0]
root       270  0.0  0.0      0     0 ?        S<   Oct05   0:00 [aio/1]
root      1305  0.0  0.0      0     0 ?        S<   Oct05   0:00 [ksnapd]
root      1522  0.0  0.0      0     0 ?        S<   Oct05   0:00 [ata/0]
--More--
```

To direct input to this VM, click inside or press Ctrl+G.

lsof(8)-Linux man page

- List open files
- Usage:
  - Gather/Manipulate:
    - open files with process, device, port information
  - Example:
    - lsof
    - lsof –i
      - http://www.tecmint.com/10-lsof-command-examples-in-linux/

Metasploitable - VMware Workstation

File Edit View VM Tabs Help

Home | Metasploitable

```
COMMAND     PID     USER   FD      TYPE DEVICE    SIZE   NODE NAME
init          1     root  cwd   unknown                      /proc/1/cwd (readli
nk: Permission denied)
init          1     root  rtd   unknown                      /proc/1/root (readl
ink: Permission denied)
init          1     root  txt   unknown                      /proc/1/exe (readli
nk: Permission denied)
init          1     root NOFD                                /proc/1/fd (opendir
: Permission denied)
kthreadd      2     root  cwd   unknown                      /proc/2/cwd (readli
nk: Permission denied)
kthreadd      2     root  rtd   unknown                      /proc/2/root (readl
ink: Permission denied)
kthreadd      2     root  txt   unknown                      /proc/2/exe (readli
nk: Permission denied)
kthreadd      2     root NOFD                                /proc/2/fd (opendir
: Permission denied)
migration     3     root  cwd   unknown                      /proc/3/cwd (readli
nk: Permission denied)
migration     3     root  rtd   unknown                      /proc/3/root (readl
ink: Permission denied)
migration     3     root  txt   unknown                      /proc/3/exe (readli
nk: Permission denied)
migration     3     root NOFD                                /proc/3/fd (opendir
--More--
```

To direct input to this VM, click inside or press Ctrl+G.

tcpdump(8)-Linux man page

- Dump traffic on a network
- Usage:
  - Gather/Manipulate:
    - Raw network traffic
      - tcpdump will by default put NIC into promiscuous mode unless the -p option is specified.
  - Example:
    - tcpdump host watermelon
    - tcpdump –i eth1
      - http://www.thegeekstuff.com/2010/08/tcpdump-command-examples/

Metasploitable - VMware Workstation

File Edit View VM Tabs Help

Home | Metasploitable

```
msfadmin@metasploitable:~$ sudo tcpdump -i eth0
[sudo] password for msfadmin:
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes

0 packets captured
0 packets received by filter
0 packets dropped by kernel
msfadmin@metasploitable:~$ _
```

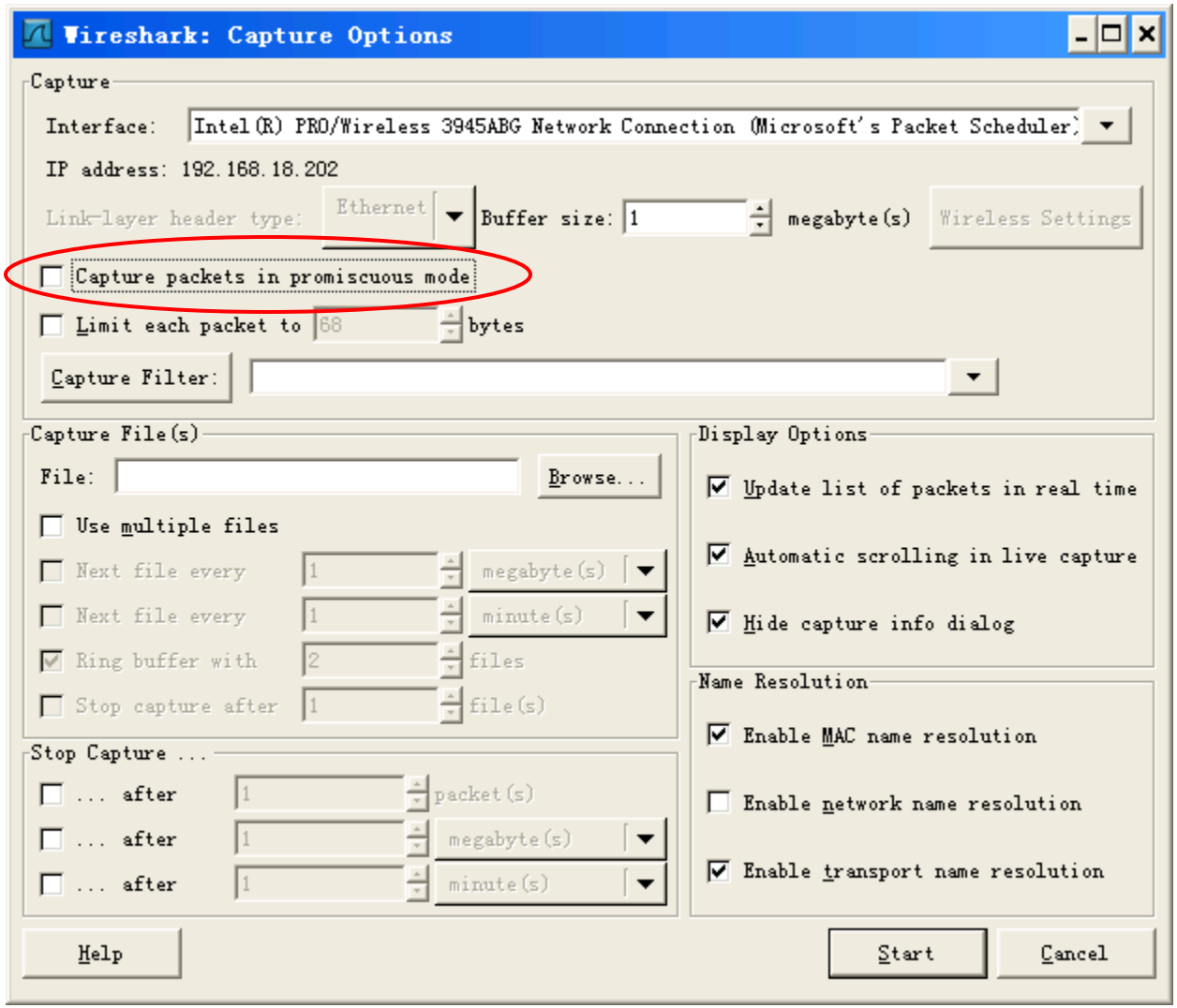
To direct input to this VM, click inside or press Ctrl+G.

My VM is isolated from Internet. Hence, no traffic.

wireshark(1)-Linux man page

- Interactively dump and analyze network traffic
- Usage:
  - Gather:
    - Network traffic packet information
      - source, dest, protocol, port, payload (on corresponding layers of OSI model)
      - trouble shooting vs. packet sniffering
  - Requirement for intercepting all traffic (not just own traffic):
    - connected to “hub”;
      - Users connected to “switches” can only see own traffic.
    - “promiscuous” mode supported by NIC, user privilege;

Wireshark Configuration



Wireshark Example

Capturing from NVIDIA nForce MCP Networking Adapter Driver: \Device\NPF_{2A44F669-393E-4495-AD0B-2BA0D26B7...

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.port == 80 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
23893	98.342195000	192.168.1.5	174.127.64.205	TCP	54	53246 > http [RST, ACK] Seq=368 Ack=
24329	103.913511000	192.168.1.5	174.127.64.205	TCP		Win=65535 Le
24331	103.924278000	192.168.1.5	23.67.253.162	TCP		Win=8192 Len
24332	103.931233000	192.168.1.5	174.127.64.205	TCP		Win=65535 Le
24333	103.957286000	174.127.64.205	192.168.1.5	TCP		Seq=0 Ack=1 W
24334	103.957455000	192.168.1.5	174.127.64.205	TCP		Ack=1 Win=65
24335	103.957678000	192.168.1.5	174.127.64.205	HTTP		show_mini&ver
24336	103.976274000	23.67.253.162	192.168.1.5	TCP		Seq=0 Ack=1 W
24337	103.976433000	192.168.1.5	23.67.253.162	TCP		Ack=1 Win=65
24338	103.976537000	192.168.1.5	23.67.253.162	HTTP		/redir/wured
24339	103.978424000	174.127.64.205	192.168.1.5	TCP		Seq=0 Ack=1 W
24340	103.978545000	192.168.1.5	174.127.64.205	TCP		Ack=1 Win=65
24341	103.978819000	192.168.1.5	174.127.64.205	HTTP		php?action=di
24342	103.990521000	23.67.253.162	192.168.1.5	TCP		Seq=0 Ack=1 W
24343	103.990604000	192.168.1.5	23.67.253.162	TCP		248 > http [A
24344	104.002726000	174.127.64.205	192.168.1.5	TCP		Ack=351 Win=
24345	104.010955000	174.127.64.205	192.168.1.5	HTTP		
24346	104.015822000	192.168.1.5	174.127.64.205	TCP		Seq=351 Ack=

Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit or Add Packet Comment...
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window

```
Identification: 0x6dc5 (28101)
⊞ Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
⊞ Header checksum: 0xdc04 [correct]
Source: 192.168.1.5 (192.168.1.5)
Destination: 174.127.64.205 (174.127.64.205)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
```

```
0000  c0 3f 0e 8d 39 df 00 21  97 41 a4 c7 08 00 45 00   .?..9..! .A....E.
0010  00 34 6d c5 40 00 80 06  dc 04 c0 a8 01 05 ae 7f   .4m.@... ........
0020  40 cd cf ff 00 50 95 9c  1b fd 00 00 00 00 80 02   @....P.. ........
0030  ff ff 3c 2d 00 00 02 04  05 b4 01 03 03 08 01 01   ..<-.... ........
0040  04 02                                              ..
```

Frame (frame), 66 bytes | Packets: 30284 Displayed: 11128 Marked: 1 | Profile: Default

Figure from www.snapfiles.com

ping(8)-Linux man page

- Send ICMP ECHO_REQUEST to network hosts
- Usage:
  - Gather/Manipulate:
    - system online? - Through response
    - how far away? - Based on RTT (Round Trip Time) given in summary statistics
    - what operating system? - Based on TTL (packet Time To Live) on each packet line
  - Example:
    - ping –c 5 www.google.com
      - http://www.thegeekstuff.com/2009/11/ping-tutorial-13-effective-ping-command-examples/

C:\Windows\System32\cmd.exe

```
C:\Windows\System32>ping google.com

Pinging google.com [216.58.195.78] with 32 bytes of data:
Reply from 216.58.195.78: bytes=32 time=5ms TTL=55
Reply from 216.58.195.78: bytes=32 time=5ms TTL=55
Reply from 216.58.195.78: bytes=32 time=6ms TTL=55

Ping statistics for 216.58.195.78:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 6ms, Average = 5ms
Control-C
^C
C:\Windows\System32>_
```

Screenshot taken based on Windows, as my Linux is metasploitable

traceroute(8)-Linux man page

- Print the route packets trace to network host
- Usage:
  - Gather/Manipulate:
    - physical location of machine
    - network information (gateway, other internal systems)
    - potential location of firewall
  - Example:
    - traceroute www.google.com

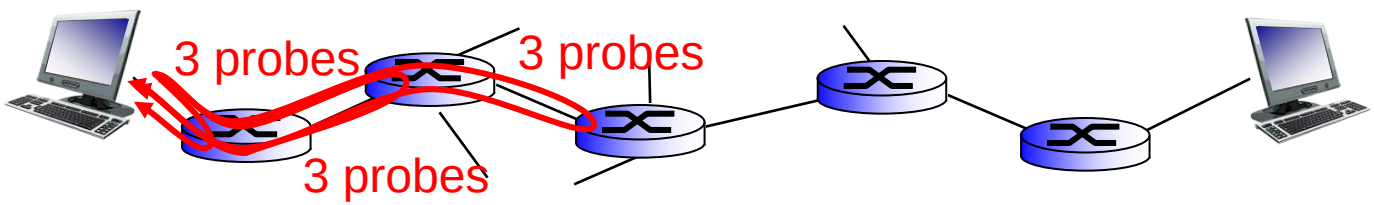


Figure from Jim Kurose, Keith Ross,
Computer Networking: A Top Down Approach, 6th edition

C:\Windows\System32\cmd.exe

```
C:\Windows\System32>traceroute baidu.com
'traceroute' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\System32>tracert baidu.com

Tracing route to baidu.com [123.125.114.144]
over a maximum of 30 hops:

  1     3 ms     5 ms     2 ms  10.118.127.254
  2     8 ms     2 ms     3 ms  130.86.1.252
  3     3 ms     2 ms     4 ms  sacstatertr-1-in.csus.edu [130.86.253.151]
  4     3 ms     2 ms     4 ms  dc-sac-dc2--sac-csu-cmf.cenic.net [137.164.41.20
1]
  5     5 ms     4 ms     4 ms  dc-oak-agg4--sac-dc1-10g.cenic.net [137.164.47.2
2]
  6     7 ms     6 ms     6 ms  dc-svl-agg4--oak-agg4-100ge.cenic.net [137.164.4
6.145]
  7     6 ms     6 ms     6 ms  10-1-1-91.ear1.SanJose1.Level3.net [4.15.122.45]

  8     7 ms     6 ms     7 ms  ae-3-18.edge1.SanJose3.Level3.net [4.69.209.173]

  9    37 ms     6 ms     8 ms  MCI-level3-20G.SanJose3.Level3.net [4.68.110.250
]
 10     *        *        *     Request timed out.
```

finger(1)-Linux man page

- Looks up and displays information about system users
- Usage:
  - Gather/Manipulate:
    - Usernames
      - Whether a user is currently logged in
  - Example:
    - finger localuser
    - finger @remotehost
    - finger remoteuser@remotehost
      - https://kb.iu.edu/d/aasp

```
finger skywalker@moe.cc.emory.edu

Luke Skywalker (skywalke) is not presently logged in.
Last seen at moe on Mon Jul 23 05:13:06 2001 from larry.cc.emory.edu
Mail forwarded to skywalke@mail.service.emory.edu.
Project: Save the galaxy!
Plan:
*Star-hopping Friday night with Han
*Appointment with Yoda Monday at 3:15pm
```

Picture from https://kb.iu.edu/d/aasp

nslookup(1)-Linux man page

- Query Internet name servers interactively
- Usage:
  - Gather/Manipulate:
    - Internet name server information
    - Find name for IP, or IP for name
  - Example:
    - nslookup www.google.com

```
Server:  ns4.csus.edu
Address:  130.86.251.251

Non-authoritative answer:
Name:    www.google.com
Addresses:  2607:f8b0:4010:801::1013
          74.125.239.52
          74.125.239.50
          74.125.239.48
          74.125.239.51
          74.125.239.49
```

dig(1)-Linux man page

- DNS lookup utility
- Usage:
  - Gather/Manipulate:
    - Name servers
    - Find name for IP, or IP for name
  - Example:
    - dig www.redhat.com
      - http://www.thegeekstuff.com/2012/02/dig-command-examples/

```
$ dig redhat.com

; <<>> DiG 9.7.3-RedHat-9.7.3-2.el6 <<>> redhat.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62863
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 3

;; QUESTION SECTION:
;redhat.com.                    IN      A

;; ANSWER SECTION:
redhat.com.             37      IN      A       209.132.183.81

;; AUTHORITY SECTION:
redhat.com.             73      IN      NS      ns4.redhat.com.
redhat.com.             73      IN      NS      ns3.redhat.com.
redhat.com.             73      IN      NS      ns2.redhat.com.
redhat.com.             73      IN      NS      ns1.redhat.com.

;; ADDITIONAL SECTION:
ns1.redhat.com.         73      IN      A       209.132.186.218
ns2.redhat.com.         73      IN      A       209.132.183.2
ns3.redhat.com.         73      IN      A       209.132.176.100

;; Query time: 13 msec
;; SERVER: 209.144.50.138#53(209.144.50.138)
;; WHEN: Thu Jan 12 10:09:49 2012
;; MSG SIZE  rcvd: 164
```

Picture from http://www.thegeekstuff.com/2012/02/dig-command-examples/

whois(1)-Linux man page

- Queries whois servers for Internet registration information
- Usage:
  - Gather/Manipulate:
    - Information used in registration (contact email, phone, location), which is good for social engineering
  - Example:
    - whois www.google.com
      - http://www.whois.net/

WHOIS LOOKUP

google.com is already registered*

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Aborting search 50 records found .....
Server Name: GOOGLE.COM.AFRICANBATS.ORG
Registrar: TUCOWS DOMAINS INC.
Whois Server: whois.tucows.com
Referral URL: http://www.tucowsdomains.com

Server Name: GOOGLE.COM.ANGRYPIRATES.COM
IP Address: 8.8.8.8
Registrar: NAME.COM, INC.
Whois Server: whois.name.com
Referral URL: http://www.name.com

Server Name: GOOGLE.COM.AR
Registrar: ENOM, INC.
Whois Server: whois.enom.com
Referral URL: http://www.enom.com

Server Name: GOOGLE.COM.AU
Registrar: PLANETDOMAIN PTY LTD.
Whois Server: whois.planetdomain.com
Referral URL: http://www.planetdomain.com

Server Name: GOOGLE.COM.BAISAD.COM
IP Address: 91.218.229.20
IP Address: 92.53.96.24
Registrar: REGISTRAR OF DOMAIN NAMES REG.RU LLC
Whois Server: whois.reg.com
Referral URL: http://www.reg.ru

Server Name: GOOGLE.COM.BEYONDWHOIS.COM
IP Address: 203.36.226.2
Registrar: INSTRA CORPORATION PTY, LTD.
Whois Server: whois.instra.net
Referral URL: http://www.instra.com

Picture from https://www.whois.net/

arp(8)-Linux man page

- Manipulates or displays the kernel's IPv4 network neighbor cache
- Usage:
  - Gather/Manipulate:
    - find neighbor systems
    - add entries to the table, delete one, or display the current content
  - Example:
    - arp –a

Internet Address	Physical Address	Type
130.86.69.254	00-10-db-ff-10-04	dynamic
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

netstat(8)-Linux man page

- Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships
- Usage:
  - Gather/Manipulate:
    - Find adjacent systems
    - Alive connection information, such as listening sockets
  - Example:
    - netstat –ln
      - http://www.thegeekstuff.com/2010/03/netstat-command-examples/

Metasploitable - VMware Workstation

File Edit View VM Tabs Help

Home | Metasploitable

```
msfadmin@metasploitable:~$ netstat -an | grep 22
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 127.0.0.1:42239         127.0.0.1:42239         ESTABLISHED
unix  2      [ ACC ]     STREAM     LISTENING     12297    /var/run/postgresql/.
s.PGSQL.5432
unix  2      [ ]         DGRAM                    12291
msfadmin@metasploitable:~$ _
```

To direct input to this VM, click inside or press Ctrl+G.

nmap(1)-Linux man page

- Network exploration tool and security/port scanner
- Usage:
  - Gather/Manipulate:
    - Network information: hosts, ports, OS, firewall
  - Example:
    - nmap -v scanme.nmap.org
      - http://nmap.org/book/man-examples.html

Metasploit and BackTrack/Kali Linux

- Metasploit
  - Penetration testing software
  - Cross-platform framework that aids you in developing and executing exploit code against a remote target machine
  - http://www.metasploit.com/

- BackTrack/Kali Linux
  - A security Linux distribution for penetration testing, with collected tools including Metasploit
  - http://www.backtrack-linux.org/
  - http://www.kali.org/
  - http://tools.kali.org/kali-metapackages

```
Session   Edit   View   Bookmarks   S

100666/rw-rw-rw-  1024    fil
100666/rw-rw-rw-  178     fil

meterpreter > cd My Documents
[-] stdapi_fs_chdir: Operation f
meterpreter > cd My\ Documents
meterpreter > ls

Listing: C:\Documents and Settin
================================

Mode              Size  Type  La
----              ----  ----  --
40555/r-xr-xr-x   0     dir   Mo
40777/rwxrwxrwx   0     dir   Mo
100666/rw-rw-rw-  28    fil   Mo
40555/r-xr-xr-x   0     dir   Mo
40555/r-xr-xr-x   0     dir   Mo
100666/rw-rw-rw-  79    fil   Mo

meterpreter > download Classifie
[*] downloading: ClassifiedDocum
[*] downloaded : ClassifiedDocum
meterpreter > getlwd
/opt/metasploit3/msf3
meterpreter >
```

```
root@bt: /opt/metasploit3/msf3 - Shell - Konsole
Session   Edit   View   Bookmarks   Settings   Help

root@bt:~# cd /opt/metasploit3/msf3/3
bash: cd: /opt/metasploit3/msf3/3: No such file or directory
root@bt:~# cd /opt/metasploit3/msf3/
root@bt:/opt/metasploit3/msf3# ls
ClassifiedDocument.txt  documentation  msfconsole  msfmachscan  ms
README                  external       msfd        msfopcode    ms
auto                    lib            msfelfscan  msfpayload   pl
autopwnage              modules        msfencode   msfpescan    sc
data                    msfcli         msfgui      msfrpc       te
root@bt:/opt/metasploit3/msf3# cat ClassifiedDocument.txt
Someone set us up the Bombe!root@bt:/opt/metasploit3/msf3#
```

back | track 4

- codename [pwnsauce]

Shell