

CMPE209 Network Security HomeWork1 Submission

Name : Prashanth Rajasekar
SJSUID : 011822460

1.

```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# date; whereis passwd
Sun Sep 9 23:13:42 EDT 2018
passwd: /usr/bin/passwd /etc/passwd /usr/share/man/man1/passwd.1.gz /usr/share/man
/man1/passwd.1ssl.gz /usr/share/man/man5/passwd.5.gz
root@kali:/etc# date; whereis shadow
Sun Sep 9 23:13:59 EDT 2018
shadow: /etc/shadow /usr/include/shadow.h /usr/share/man/man5/shadow.5.gz
root@kali:/etc#
```

Directory of shadow: /etc/shadow

Directory of passwd: /etc/passwd

Description:

Passwd file contains essential information required login like useraccount information. It's a text file containing system's accounts giving each account some information like user ID, group ID. We can read it, but should have necessary permissions to write it.

Shadow file contains the actual password which is encrypted.

2.

```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# date; dig ns
Sun Sep  9 23:21:00 EDT 2018
; <>> DiG 9.11.4-4-Debian <>> ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26427
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13
;; QUESTION SECTION:
.; IN NS
;; ANSWER SECTION:
.          5    IN  NS   h.root-servers.net.
.          5    IN  NS   i.root-servers.net.
.          5    IN  NS   j.root-servers.net.
.          5    IN  NS   k.root-servers.net.
.          5    IN  NS   l.root-servers.net.
.          5    IN  NS   m.root-servers.net.
.          5    IN  NS   a.root-servers.net.
.          5    IN  NS   b.root-servers.net.
.          5    IN  NS   c.root-servers.net.
.          5    IN  NS   d.root-servers.net.
.          5    IN  NS   e.root-servers.net.
.          5    IN  NS   f.root-servers.net.
.          5    IN  NS   g.root-servers.net.
```

```

;; ADDITIONAL SECTION:
a.root-servers.net.      5    IN      A          198.41.0.4
a.root-servers.net.      5    IN      AAAA        2001:503:ba3e::2:30
b.root-servers.net.      5    IN      A          199.9.14.201
b.root-servers.net.      5    IN      AAAA        2001:500:200::b
c.root-servers.net.      5    IN      A          192.33.4.12
c.root-servers.net.      5    IN      AAAA        2001:500:2::c
d.root-servers.net.      5    IN      A          199.7.91.13
d.root-servers.net.      5    IN      AAAA        2001:500:2d::d
e.root-servers.net.      5    IN      A          192.203.230.10
e.root-servers.net.      5    IN      AAAA        2001:500:a8::e
f.root-servers.net.      5    IN      A          192.5.5.241
g.root-servers.net.      5    IN      A          192.112.36.4
g.root-servers.net.      5    IN      AAAA        2001:500:12::d0d

;; Query time: 18 msec
;; SERVER: 192.168.203.2#53(192.168.203.2)
;; WHEN: Sun Sep 09 23:21:00 EDT 2018
;; MSG SIZE  rcvd: 508

root@kali:/etc#

```

There are 13 root name servers.

8 in USA, 3 in Europe, 2 in ASIA

PLACES	COUNTS
USA	8
Europe	3
ASIA	2



Ref :https://archive.icann.org/en/tlds/org/applications/uia/C17_5.html

3. google have 5 Mail Exchanger(MX) servers.

```
root@kali: /etc
File Edit View Search Terminal Help
mount-
root@kali:/etc# date; dig google.com MX
Sun Sep 9 23:32:16 EDT 2018

; <>> DiG 9.11.4-4-Debian <>> google.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58695
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 4
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;google.com.           IN      MX

;; ANSWER SECTION:
google.com.        5       IN      MX      10 aspmx.l.google.com.
google.com.        5       IN      MX      20 alt1.aspmx.l.google.com.
google.com.        5       IN      MX      40 alt3.aspmx.l.google.com.
google.com.        5       IN      MX      30 alt2.aspmx.l.google.com.
google.com.        5       IN      MX      50 alt4.aspmx.l.google.com.

;; ADDITIONAL SECTION:
aspmx.l.google.com. 5       IN      AAAA    2607:f8b0:400e:c03::1a
alt1.aspmx.l.google.com. 5   IN      AAAA    2607:f8b0:4001:c16::1a
alt4.aspmx.l.google.com. 5   IN      A       173.194.218.27

;; Query time: 17 msec
;; SERVER: 192.168.203.2#53(192.168.203.2)
;; WHEN: Sun Sep 09 23:32:16 EDT 2018
;; MSG SIZE rcvd: 219

root@kali:/etc#
```

query using Google's open DNS servers:

```
root@kali: /etc
File Edit View Search Terminal Help
mount-
root@kali:/etc# date; dig google.com MX
Sun Sep 9 23:32:16 EDT 2018

; <>> DiG 9.11.4-4-Debian <>> google.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58695
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 4
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;google.com.           IN      MX

;; ANSWER SECTION:
google.com.        5       IN      MX      10 aspmx.l.google.com.
google.com.        5       IN      MX      20 alt1.aspmx.l.google.com.
google.com.        5       IN      MX      40 alt3.aspmx.l.google.com.
google.com.        5       IN      MX      30 alt2.aspmx.l.google.com.
google.com.        5       IN      MX      50 alt4.aspmx.l.google.com.

;; ADDITIONAL SECTION:
aspmx.l.google.com. 5       IN      AAAA    2607:f8b0:400e:c03::1a
alt1.aspmx.l.google.com. 5   IN      AAAA    2607:f8b0:4001:c16::1a
alt4.aspmx.l.google.com. 5   IN      A       173.194.218.27
```

```
root@kali:/etc# date; dig @8.8.4.4 google.com MX
Sun Sep 9 23:43:17 EDT 2018
; <>> DiG 9.11.4-4-Debian <>> @8.8.4.4 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26702
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.           IN      MX
;; ANSWER SECTION:
google.com.          599     IN      MX      40 alt3.aspmx.l.google.com.
google.com.          599     IN      MX      50 alt4.aspmx.l.google.com.
google.com.          599     IN      MX      20 alt1.aspmx.l.google.com.
google.com.          599     IN      MX      10 aspmx.l.google.com.
google.com.          599     IN      MX      30 alt2.aspmx.l.google.com.

;; Query time: 152 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Sun Sep 09 23:43:17 EDT 2018
;; MSG SIZE rcvd: 147

root@kali:/etc#
```

4. Ways to find the authoritative name server:

- a. nslookup
- b. dig
- c. host
- d. whois

```
root@kali:/etc# date; dig ibasis.com ns
Sun Sep 9 23:47:29 EDT 2018
; <>> DiG 9.11.4-4-Debian <>> ibasis.com ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41424
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;ibasis.com.           IN      NS
;; ANSWER SECTION:
ibasis.com.          5       IN      NS      server1502.ivanet.net.
ibasis.com.          5       IN      NS      ns3.ibasis.net.
ibasis.com.          5       IN      NS      ns2.ibasis.net.
ibasis.com.          5       IN      NS      ns4.ibasis.net.
ibasis.com.          5       IN      NS      ns1.ibasis.net.

;; Query time: 108 msec
;; SERVER: 192.168.203.2#53(192.168.203.2)
;; WHEN: Sun Sep 09 23:47:29 EDT 2018
;; MSG SIZE rcvd: 153

root@kali:/etc#
```

```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# nslookup
> set querytype=ns
> ibasis.com
Server:      192.168.203.2
Address:     192.168.203.2#53

Non-authoritative answer:
ibasis.com      nameserver = ns3.ibasis.net.
ibasis.com      nameserver = ns2.ibasis.net.
ibasis.com      nameserver = server1502.ivanet.net.
ibasis.com      nameserver = ns4.ibasis.net.
ibasis.com      nameserver = ns1.ibasis.net.

Authoritative answers can be found from:
> 
```

```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# date; whois ibasis.com
Sun Sep  9 23:54:39 EDT 2018
Domain Name: IBASIS.COM
Registry Domain ID: 9796842_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-01-23T20:09:03Z
Creation Date: 1999-09-04T00:20:26Z
Registry Expiry Date: 2019-09-04T00:20:26Z
Registrar: Network Solutions, LLC.
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DALNS3.IBASIS.NET
Name Server: DALNS5.IBASIS.NET
Name Server: NS1.IBASIS.NET
Name Server: NS2.IBASIS.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-09-10T03:54:34Z <<<
```

```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# date; host -t ns ibasis.com
Mon Sep 10 00:00:22 EDT 2018
ibasis.com name server ns1.ibasis.net.
ibasis.com name server ns3.ibasis.net.
ibasis.com name server ns2.ibasis.net.
ibasis.com name server server1502.ivanet.net.
ibasis.com name server ns4.ibasis.net.
root@kali:/etc# 
```

Query using google's DNS servers

```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# date; nslookup
Mon Sep 10 00:05:27 EDT 2018
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=ns
> ibasis.com
Server:      8.8.8.8
Address:     8.8.8.8#53
ibasis.com
Non-authoritative answer:
ibasis.com      nameserver = server1502.ivanet.net.
ibasis.com      nameserver = ns3.ibasis.net.
ibasis.com      nameserver = ns4.ibasis.net.
ibasis.com      nameserver = ns2.ibasis.net.
ibasis.com      nameserver = ns1.ibasis.net.

Authoritative answers can be found from:
> |
```

5. dig stands for “Domain Information Groper” flexible tool for interrogating DNS name servers. Most DNS administrators use dig to troubleshoot DNS problems. other lookup tools tend to have less functionality than dig.

```
root@kali: /etc
File Edit View Search Terminal Help
mount-
shared-
block-
root@kali:/etc# dig www.lego.com +trace
;; Warning: Message parser reports malformed message packet.

; <>>> DiG 9.11.4-4-Debian <>>> www.lego.com +trace
;; global options: +cmd
.          5    IN   NS    j.root-servers.net.
start-vm-  5    IN   NS    k.root-servers.net.
tools.sh   5    IN   NS    l.root-servers.net.
.          5    IN   NS    m.root-servers.net.
.          5    IN   NS    a.root-servers.net.
.          5    IN   NS    b.root-servers.net.
.          5    IN   NS    c.root-servers.net.
.          5    IN   NS    d.root-servers.net.
.          5    IN   NS    e.root-servers.net.
.          5    IN   NS    f.root-servers.net.
.          5    IN   NS    g.root-servers.net.
.          5    IN   NS    h.root-servers.net.
.          5    IN   NS    i.root-servers.net.
;; Received 313 bytes from 192.168.203.2#53(192.168.203.2) in 22 ms

com.        172800  IN   NS    a.gtld-servers.net.
com.        172800  IN   NS    b.gtld-servers.net.
com.        172800  IN   NS    c.gtld-servers.net.
com.        172800  IN   NS    d.gtld-servers.net.
com.        172800  IN   NS    e.gtld-servers.net.
com.        172800  IN   NS    f.gtld-servers.net.
```

```
duers.sh      5      IN      NS      g.root-servers.net.  
.          5      IN      NS      h.root-servers.net.  
;          5      IN      NS      i.root-servers.net.  
;; Received 313 bytes from 192.168.203.2#53(192.168.203.2) in 22 ms  
  
com.vm-      172800  IN      NS      a.gtld-servers.net.  
com.vmsh.    172800  IN      NS      b.gtld-servers.net.  
com.         172800  IN      NS      c.gtld-servers.net.  
com.         172800  IN      NS      d.gtld-servers.net.  
com.         172800  IN      NS      e.gtld-servers.net.  
com.         172800  IN      NS      f.gtld-servers.net.  
com.         172800  IN      NS      g.gtld-servers.net.  
com.         172800  IN      NS      h.gtld-servers.net.  
com.         172800  IN      NS      i.gtld-servers.net.  
com.         172800  IN      NS      j.gtld-servers.net.  
com.         172800  IN      NS      k.gtld-servers.net.  
com.         172800  IN      NS      l.gtld-servers.net.  
com.         172800  IN      NS      m.gtld-servers.net.  
com.         86400   IN      DS      30909 8 2 E2D3C916F6DEEAC73294E826  
8FB5885044A833FC5459588F4A9184CF C41A5766  
com.         86400   IN      RRSIG   DS 8 1 86400 20180922170000 201809  
09160000 41656 . A4AyL4sd+jNxY0+ZA7El5MStWBzWIGfk5dNDKoLmVuhEZQpVWSxIG60F 0tIx2nhp  
0Xu0yxGK6cAGD+R4y5dPS3fAt50lWZFcC/IS6UCLB4DVfdV7 p0hdNlk7IqTKxBG77te3Ck/cQYnnG87B+  
iKxBVy2q06jbGxhh+Wge05y BFrUL5BkeuA31Vwd8tqP3v5z5h6DVXU+G8JojPQZdkDUuiEe4GwLfMvb A  
Yg2iToRLhjZA2f6D8ZUdJsFQIwhKmBz3ez26/eZUmxiaFSQxtjZ3Zl0 0dT4zl0K/AnDz40/3ER5duF/fe  
JyNRC1kcBXn5bXP2vth0NRwVFzVg/k chn5yA==  
;; Received 1172 bytes from 193.0.14.129#53(k.root-servers.net) in 100 ms  
  
lego.com.    172800  IN      NS      sdns23.ultradns.com.  
lego.com.    172800  IN      NS      sdns23.ultradns.net.  
lego.com.    172800  IN      NS      sdns23.ultradns.biz.  
lego.com.    172800  IN      NS      sdns23.ultradns.org.  
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0Q1GIN43N1ARRC90SM6  
QPQR81H5M9A NS SOA RRSIG DNSKEY NSEC3PARAM  
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 8 2 86400 2018091304441  
2 20180906033412 46475 com. fIY07slc/eSvGWCnDI+y2TLrKdtw9gh6YqU9wiZJGTJ9Dn/5Iiv1Mg  
Uo NUgphonp2p6LPEKls6S1GokL3N/qMv66VqDi02jINntemVeSG4Gmd0Ni 62aJA8p2Ch5eGkBq3yPjg9  
2pHdhNbK0fDZhENiU/Bdu25jCkVNOWtzA zS4=  
M5LA08S2ANLPRI3KL00NCECHV9A50VAK.com. 86400 IN NSEC3 1 1 0 - M5LBQKKATR1ECM09R2602  
H7I2U6FVL88 NS DS RRSIG  
M5LA08S2ANLPRI3KL00NCECHV9A50VAK.com. 86400 IN RRSIG NSEC3 8 2 86400 2018091504293  
5 20180908031935 46475 com. wq7ZhBnPxF6rlV47IcJ9idlJE9xsLM4YrTfietPe+tS2BTuufPnOn  
/R VOJtam3ap6bzjdD65CSL7lIEEQgh4PeLsxeuN68BURzTAcFvuAtsDaq4 GWBe73QoIZ3lRdTy83Rxks  
QvbhZeFWB0F6xgxKR5Bu9TOrSG/WA0t/dh QbY=  
;; Received 743 bytes from 192.12.94.30#53(e.gtld-servers.net) in 30 ms  
  
www.lego.com. 86400   IN      CNAME   lego.com.edgekey.net.  
;; Received 75 bytes from 156.154.140.23#53(sdns23.ultradns.com) in 43 ms  
  
root@kali:/etc#
```

6. Using connect scan

The terminal window shows the results of an Nmap scan on host 192.168.203.129. The output includes service versions for various ports, such as OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) and Apache httpd 2.2.8 ((Ubuntu) DAV/2). The Wireshark capture window below shows network traffic on interface eth0, with a list of captured frames and their details.

```
root@kali:/etc# date; nmap -sTV -p1-1600 -Pn 192.168.203.129
Mon Sep 10 00:20:12 EDT 2018
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-10 00:20 EDT
Nmap scan report for 192.168.203.129
Host is up (0.0024s latency).
Not shown: 1586 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
Service Info: Hosts: metasploitable.localdomain, localhost; OSs: Unix, Linux; CPE: cpe:/o:linux:linux kernel (request)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.70 seconds
root@kali:/etc#
```

File Edit View Search Terminal Help

root@kali:/etc# date; nmap -sTV -p1-1600 -Pn 192.168.203.129
Mon Sep 10 00:20:12 EDT 2018
Starting Nmap 7.70 (https://nmap.org) at 2018-09-10 00:20 EDT
Nmap scan report for 192.168.203.129
Host is up (0.0024s latency).
Not shown: 1586 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login login?
514/tcp open tcpwrapped
1099/tcp open rmiregistry GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
Service Info: Hosts: metasploitable.localdomain, localhost; OSs: Unix, Linux; CPE: cpe:/o:linux:linux kernel (request)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.70 seconds
root@kali:/etc#

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length
1241	9.343224307	192.168.203.129	192.168.203.133	TCP	480
1242	9.343225864	192.168.203.129	192.168.203.133	TCP	480
1243	9.343227496	192.168.203.129	192.168.203.133	TCP	480
1244	9.343229026	192.168.203.129	192.168.203.133	TCP	480
1245	9.343230419	192.168.203.129	192.168.203.133	TCP	480
1246	9.343231970	192.168.203.129	192.168.203.133	TCP	480
1247	9.343233630	192.168.203.129	192.168.203.133	TCP	480
1248	9.343235376	192.168.203.129	192.168.203.133	TCP	480
1249	9.343237153	192.168.203.129	192.168.203.133	TCP	480
1250	9.343238766	192.168.203.129	192.168.203.133	TCP	480
1251	9.343240331	192.168.203.129	192.168.203.133	TCP	480
1252	9.343241888	192.168.203.129	192.168.203.133	TCP	480
1253	9.343311374	192.168.203.133	192.168.203.129	TCP	480
1254	9.343323085	192.168.203.133	192.168.203.129	TCP	480

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 6
Ethernet II, Src: Vmware_24:f3:3f (00:0c:29:24:f3:3f), Dst: Vmware_c0:00:08 (00:0c:29:24:f3:3f)
Address Resolution Protocol (request)

0000 00 50 56 c0 00 08 00 0c 29 24 f3 3f 08 06 00 01 ·PV.....)\$..?.....
0010 08 00 06 04 00 01 00 0c 29 24 f3 3f c0 a8 cb 81)\$..?.....

wireshark_eth0_2...03_sV5gtz.pcapng Packets: 3702 · Displayed: 3702 (100.0%) Profile: Default

Using stealth scan

root@kali: /etc

File Edit View Search Terminal Help

```
root@kali:/etc# date; nmap -sS -p1-1600 -Pn 192.168.203.129
Mon Sep 10 00:31:26 EDT 2018
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-10 00:31 EDT
Nmap scan report for 192.168.203.129
Host is up (0.0042s latency).
Not shown: 1586 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
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
MAC Address: 00:0C:29:24:F3:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
root@kali:/etc#
```

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol
3203	0.221748910	192.168.203.129	192.168.203.133	TCP
3204	0.224693276	192.168.203.129	192.168.203.133	TCP
3205	0.224717441	192.168.203.129	192.168.203.133	TCP
3206	0.224720577	192.168.203.129	192.168.203.133	TCP
3207	0.224723617	192.168.203.129	192.168.203.133	TCP
3208	0.224726372	192.168.203.129	192.168.203.133	TCP
3209	0.224729414	192.168.203.129	192.168.203.133	TCP
3210	0.224732089	192.168.203.129	192.168.203.133	TCP
3211	0.224735769	192.168.203.129	192.168.203.133	TCP
3212	0.224738394	192.168.203.129	192.168.203.133	TCP
3213	0.224741125	192.168.203.129	192.168.203.133	TCP
3214	0.224746514	192.168.203.129	192.168.203.133	TCP
3215	0.224749244	192.168.203.129	192.168.203.133	TCP
3216	0.224752044	192.168.203.129	192.168.203.133	TCP
3217	0.224754804	192.168.203.129	192.168.203.133	TCP
3218	0.226206275	192.168.203.129	192.168.203.133	TCP

wireshark_eth...TDCPdo.pcapng · Packets: 3218 · Displayed: 3218 (100.0%) · Profile: Default

Using ACK Scan

The screenshot shows two windows side-by-side. The top window is a terminal window titled 'root@kali: /etc' with the command 'date; nmap -sA -p1-1600 -Pn 192.168.203.129' running. The output shows a scan report for host 192.168.203.129, which is up and has unfiltered ports 1-1600. The bottom window is Wireshark capturing traffic on interface 'eth0'. A list of 3204 TCP packets is shown, all originating from 192.168.203.129 to 192.168.203.133. The packet details pane shows the first frame is an ARP request for the destination IP. The bytes pane shows the captured hex and ASCII data for the first two bytes.

root@kali: /etc# date; nmap -sA -p1-1600 -Pn 192.168.203.129
Mon Sep 10 00:36:17 EDT 2018
Starting Nmap 7.70 (https://nmap.org) at 2018-09-10 00:36 EDT
Nmap scan report for 192.168.203.129
Host is up (0.0038s latency).
All 1600 scanned ports on 192.168.203.129 are unfiltered.
MAC Address: 00:0C:29:24:F3:3F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
root@kali: /etc#

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol
3193	0.254259927	192.168.203.129	192.168.203.133	TCP
3194	0.254262447	192.168.203.129	192.168.203.133	TCP
3195	0.254264947	192.168.203.129	192.168.203.133	TCP
3196	0.254267201	192.168.203.129	192.168.203.133	TCP
3197	0.254269787	192.168.203.129	192.168.203.133	TCP
3198	0.254272103	192.168.203.129	192.168.203.133	TCP
3199	0.254274476	192.168.203.129	192.168.203.133	TCP
3200	0.254276739	192.168.203.129	192.168.203.133	TCP
3201	0.254278996	192.168.203.129	192.168.203.133	TCP
3202	0.254281362	192.168.203.129	192.168.203.133	TCP
3203	0.254283752	192.168.203.129	192.168.203.133	TCP
3204	0.254286048	192.168.203.129	192.168.203.133	TCP

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface
Ethernet II, Src: VMware_85:ea:90 (00:0c:29:85:ea:90), Dst: Broadcast (ff:ff:
Address Resolution Protocol (request)

No.	Time	Source	Destination	Protocol
0000	ff ff ff ff ff ff 00 0c 29 85 ea 90 08 06 00 01			
0010	08 00 06 04 00 01 00 0c 29 85 ea 90 c0 a8 cb 85			

wireshark_eth...kODDJF.pcapng | Packets: 3204 · Displayed: 3204 (100.0%) | Profile: Default

Using Xmas scan

```
root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# date; nmap -sXV -p1-1600 -Pn 192.168.203.129
Mon Sep 10 00:39:44 EDT 2018
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-10 00:39 EDT
Nmap scan report for 192.168.203.129
Host is up (0.0035s latency).
Not shown: 1586 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec   netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
MAC Address: 00:0C:29:24:F3:3F (VMware), 42 bytes captured (336 bits) on interface
Service Info: Hosts: metasploitable.localdomain;5 localhost;sOSs: Unix,sLinux;fCPE
: cpe:/o:linux:linux_kernel:col (request)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.96 seconds
```

*eth0

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/> Expression... +
No. Time Source Destination Protocol
3166 1.372511330 192.168.203.129 192.168.203.133 TCP
3167 1.372512714 192.168.203.129 192.168.203.133 TCP
3168 1.372514044 192.168.203.129 192.168.203.133 TCP
3169 1.372515435 192.168.203.129 192.168.203.133 TCP
3170 1.372518015 192.168.203.129 192.168.203.133 TCP
3171 1.372519316 192.168.203.129 192.168.203.133 TCP
3172 1.372520687 192.168.203.129 192.168.203.133 TCP
3173 1.372522057 192.168.203.129 192.168.203.133 TCP
3174 1.372523387 192.168.203.129 192.168.203.133 TCP
3175 1.372524737 192.168.203.129 192.168.203.133 TCP
3176 1.372526070 192.168.203.129 192.168.203.133 TCP
3177 1.372527424 192.168.203.129 192.168.203.133 TCP
3178 1.372528774 192.168.203.129 192.168.203.133 TCP
3179 1.372530268 192.168.203.129 192.168.203.133 TCP
3180 1.372531061 192.168.203.129 192.168.203.133 TCP

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface
Ethernet II, Src: Vmware_85:ea:90 (00:0c:29:85:ea:90), Dst: Broadcast (ff:ff:ff)
Address Resolution Protocol (request)
```

wireshark_eth...TFR8CC.pcapng | Packets: 3667 · Displayed: 3667 (100.0%) | Profile: Default

7.

netstat -at : TCP

```
Eterm Font Background Terminal ? X
msfadmin@metasploitable:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address     State
tcp    0      0 *:exec                  *.*                LISTEN
tcp    0      0 *:50849                 *.*                LISTEN
tcp    0      0 *:login                 *.*                LISTEN
tcp    0      0 *:nfs                  *.*                LISTEN
tcp    0      0 *:shell                 *.*                LISTEN
tcp    0      0 *:8009                 *.*                LISTEN
tcp    0      0 *:8697                 *.*                LISTEN
tcp    0      0 *:mysql                 *.*                LISTEN
tcp    0      0 *:rmiregistry          *.*                LISTEN
tcp    0      0 *:ircd                 *.*                LISTEN
tcp    0      0 *:netbios-ssn          *.*                LISTEN
tcp    0      0 *:5900                 *.*                LISTEN
tcp    0      0 *:47982                *.*                LISTEN
tcp    0      0 *:sunrpc               *.*                LISTEN
tcp    0      0 *:x11                  *.*                LISTEN
tcp    0      0 *:www                  *.*                LISTEN
tcp    0      0 *:50769                *.*                LISTEN
tcp    0      0 *:8787                 *.*                LISTEN
tcp    0      0 *:8180                  *.*                LISTEN
tcp    0      0 *:tingreslock          *.*                LISTEN
tcp    0      0 *:ftp                  *.*                LISTEN
tcp    0      0 192.168.203.129:domain *.*                LISTEN
tcp    0      0 localhost:domain        *.*                LISTEN
tcp    0      0 *:telnet               *.*                LISTEN
tcp    0      0 *:postgresql           *.*                LISTEN
tcp    0      0 *:smtp                 *.*                LISTEN
tcp    0      0 localhost:953            *.*                LISTEN
tcp    0      0 *:52124                *.*                LISTEN
tcp    0      0 *:microsoft-ds          *.*                LISTEN
tcp    0      0 192.168.203:rmiregistry 192.168.203.133:60558 CLOSE_WAIT
tcp    0      0 192.168.203:rmiregistry 192.168.203.133:57260 CLOSE_WAIT
tcp    0      0 192.168.203:rmiregistry 192.168.203.133:60720 CLOSE_WAIT
tcp6   0      0 [::]:ffrox             [::]:*              LISTEN
tcp6   0      0 [::]:distcc            [::]:*              LISTEN
tcp6   0      0 [::]:domain             [::]:*              LISTEN
tcp6   0      0 [::]:ssh                [::]:*              LISTEN
```

netstat -au : UDP

```
Eterm Font Background Terminal ? X
msfadmin@metasploitable:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address     State
udp    0      0 *:nfs                  *.*                LISTEN
udp    0      0 *:57219                *.*                LISTEN
udp    0      0 192.168.203.:netbios-ns  *.*                LISTEN
udp    0      0 *:netbios-ns            *.*                LISTEN
udp    0      0 192.168.203:netbios-dgm *.*                LISTEN
udp    0      0 *:netbios-dgm          *.*                LISTEN
udp    0      0 *:795                  *.*                LISTEN
udp    0      0 localhost:snmp           *.*                LISTEN
udp    0      0 192.168.203.129:domain *.*                LISTEN
udp    0      0 localhost:domain        *.*                LISTEN
udp    0      0 *:41782                *.*                LISTEN
udp    0      0 localhost:41911          localhost:41911      ESTABLISHED
udp    0      0 *:bootpc               *.*                LISTEN
udp    0      0 *:tftp                 *.*                LISTEN
udp    0      0 *:46277                *.*                LISTEN
udp    0      0 *:41030                *.*                LISTEN
udp    0      0 *:sunrpc               *.*                LISTEN
udp6   0      0 [::]:48427             [::]:*              LISTEN
udp6   0      0 [::]:domain             [::]:*              LISTEN
```

8.

Scans Settings

test_scan [Back to My Scans](#)

Delete Configure Audit Trail Launch E:

Hosts 1 Vulnerabilities 51 History 1

Filter Search Hosts 1 Host (1 Selected) [Clear Selected Item](#)

<input checked="" type="checkbox"/> Host	Vulnerabilities
192.168.203.130	15 2 3 1 0 38

Scan Details

Name: test_scan
 Status: Completed
 Policy: Basic Network Scan
 Scanner: Local Scanner
 Start: Today at 1:09 AM
 End: Today at 1:12 AM
 Elapsed: 3 minutes

Vulnerabilities

Critical: 15, High: 2, Medium: 3, Low: 0, Info: 38

Scans Settings

<input type="checkbox"/> Sev	Name	Family	Count
CRITICAL	Microsoft Windows XP Unsupported Ins...	Windows	1
CRITICAL	MS03-026: Microsoft RPC Interface Buf...	Windows	1
CRITICAL	MS03-039: Microsoft RPC Interface Buf...	Windows	1
CRITICAL	MS03-043: Buffer Overrun in Messeng...	Windows	1
CRITICAL	MS04-007: ASN.1 Vulnerability Could ...	Windows	1
CRITICAL	MS04-011: Security Update for Microso...	Windows	1
CRITICAL	MS04-012: Cumulative Update for Micr...	Windows	1
CRITICAL	MS04-022: Microsoft Windows Task Sc...	Windows	1
CRITICAL	MS05-027: Vulnerability in SMB Could ...	Windows	1
CRITICAL	MS05-043: Vulnerability in Printer Spo...	Windows	1
CRITICAL	MS06-040: Vulnerability in Server Serv...	Windows	1
CRITICAL	MS08-067: Microsoft Windows Server ...	Windows	1

Scan Details

Name: test_scan
 Status: Completed
 Policy: Basic Network Scan
 Scanner: Local Scanner
 Start: Today at 1:09 AM
 End: Today at 1:12 AM
 Elapsed: 3 minutes

Vulnerabilities

Critical: 15, High: 2, Medium: 3, Low: 0, Info: 38

Scans				
Settings				
<input type="checkbox"/>	MEDIUM	Microsoft Windows SMB NULL Session...	Windows	1
<input type="checkbox"/>	MEDIUM	MS05-007: Vulnerability in Windows C...	Windows	1
<input type="checkbox"/>	MEDIUM	SMB Signing not required	Misc.	1
<input type="checkbox"/>	LOW	Multiple Ethernet Driver Frame Paddin...	Misc.	1
<input type="checkbox"/>	INFO	Nessus SYN scanner	Port scanners	5
<input type="checkbox"/>	INFO	DCE Services Enumeration	Windows	4
<input type="checkbox"/>	INFO	Microsoft Windows SMB Service Detect...	Windows	2
<input type="checkbox"/>	INFO	Common Platform Enumeration (CPE)	General	1
<input type="checkbox"/>	INFO	Device Type	General	1
<input type="checkbox"/>	INFO	Ethernet Card Manufacturer Detection	Misc.	1
<input type="checkbox"/>	INFO	Ethernet MAC Addresses	General	1
<input type="checkbox"/>	INFO	ICMP Timestamp Request Remote Dat...	General	1

Scans				
Settings				
<input type="checkbox"/>	INFO	Nessus Windows Scan Not Performed ...	Settings	1
<input type="checkbox"/>	INFO	NetBIOS Multiple IP Address Enumerat...	Windows	1
<input type="checkbox"/>	INFO	Network Time Protocol (NTP) Server D...	Service detection	1
<input type="checkbox"/>	INFO	No Credentials Provided	Settings	1
<input type="checkbox"/>	INFO	OS Identification	General	1
<input type="checkbox"/>	INFO	Patch Report	General	1
<input type="checkbox"/>	INFO	Server Message Block (SMB) Protocol ...	Misc.	1
<input type="checkbox"/>	INFO	Service Detection	Service detection	1
<input type="checkbox"/>	INFO	TCP/IP Timestamps Supported	General	1
<input type="checkbox"/>	INFO	Traceroute Information	General	1
<input type="checkbox"/>	INFO	UPnP Client Detection	Service detection	1
<input type="checkbox"/>	INFO	UPnP TCP Helper Detection	Windows	1
<input type="checkbox"/>	INFO	VMware Virtual Machine Detection	General	1