

Masato Anzai
Lab #4: nmap/iptables
N12725403

NMAP:

1. Ports open on 10.10.111.0/24: 63/tcp, 111/tcp
OS Details: Linux 2.6.9 - 2.6.24
Command Used: nmap -A 10.10.111.0/24

```
^ ~ | x root@bt: ~
File Edit View Terminal Help
root@bt:~# nmap -A 10.10.111.0/24

Starting Nmap 5.51 ( http://nmap.org ) at 2016-04-27 19:14 EDT
Nmap scan report for 10.10.111.1
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
63/tcp    open  domain  ISC BIND 9.5.1-P3
111/tcp   open  rpcbind 2 (rpc #100000)
MAC Address: 02:00:C2:66:02:02 (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.24
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  1.71 ms  10.10.111.1

Nmap scan report for 10.10.111.2
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
63/tcp    open  domain  ISC BIND 9.5.1-P3
111/tcp   open  rpcbind 2 (rpc #100000)
MAC Address: 02:00:C2:D6:0A:01 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).  
TCP/IP fingerprint:  
OS:SCAN(V=5.51%D=4/27%T=53%CT=1%CU=37357%PV=Y%DS=1%DC=D%G=Y%M=0200C2%TM=57  
OS:214803%P=i686-pc-linux-gnu)SEQ(SP=CF%GCD=1%ISR=D0%TI=Z%CI=Z%II=I%TS=9)OP  
OS:(O1=M5B4ST11NW5%02=M5B4ST11NW5%03=M5B4NT11NW5%04=M5B4ST11NW5%05=M5B4ST  
OS:11NW5%06=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)EC  
OS:N(R=Y%DF=Y%T=40%W=16D0%W=M5B4NNSNW%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S-%F=  
OS:AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=0%A=S+%F=AS%0=M5B4ST11NW5%RD  
OS:=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%  
OS:=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T7(R  
OS:=Y%DF=Y%T=40%W=0%Z=A=S+%F=AR%0=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%  
OS:RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
TRACEROUTE
HOP RTT      ADDRESS
1  1.69 ms  10.10.111.2

Nmap scan report for 10.10.111.111
Host is up (0.000068s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
111/tcp   open  rpcbind 2 (rpc #100000)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.19 - 2.6.36
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 63.82 seconds
root@bt:~#
```

2. Ports Open on 10.20.111.0/24: 53/tcp, 111/tcp

OS Details: Linux 2.6.9 - 2.6.24

Command Used: nmap -A 10.20.111.0/24

```
root@bt:~# nmap -A 10.20.111.0/24
Starting Nmap 5.51 ( http://nmap.org ) at 2016-04-27 19:17 EDT
Nmap scan report for 10.20.111.1
Host is up (0.0019s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain  ISC BIND 9.5.1-P3
111/tcp   open  rpcbind 2 (rpc #100000)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.24
Network Distance: 1 hop

TRACEROUTE (using port 1025/tcp)
HOP RTT      ADDRESS
1  1.67 ms  10.20.111.1

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 123.98 seconds
root@bt:~#
```

IPTABLES:

A)

Accepts all outgoing traffic at this point and can communicate with 10.10.111.0/24

```
router:~# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source                               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source                               destination
ACCEPT     icmp --  10.10.111.0/24                  10.20.111.0/24
ACCEPT     all   --  10.20.111.0/24                  10.10.111.0/24
```

B)

1) Internal Machine responds to ping from 10.10.111.0/24

```
router:~# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source                               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source                               destination
ACCEPT     icmp --  10.10.111.0/24                  10.20.111.0/24
ACCEPT     all   --  10.20.111.0/24                  10.10.111.0/24
```

Example Pings:

```
root@bt:~# ping 10.20.111.1
PING 10.20.111.1 (10.20.111.1) 56(84) bytes of data.
64 bytes from 10.20.111.1: icmp_seq=1 ttl=64 time=8.13 ms
From 10.10.111.1: icmp_seq=2 Redirect Host(New nexthop: 10.10.
64 bytes from 10.20.111.1: icmp_seq=2 ttl=64 time=2.81 ms
64 bytes from 10.20.111.1: icmp_seq=3 ttl=64 time=1.98 ms
64 bytes from 10.20.111.1: icmp_seq=4 ttl=64 time=1.67 ms
64 bytes from 10.20.111.1: icmp_seq=5 ttl=64 time=1.52 ms
64 bytes from 10.20.111.1: icmp_seq=6 ttl=64 time=2.15 ms
64 bytes from 10.20.111.1: icmp_seq=7 ttl=64 time=1.52 ms
64 bytes from 10.20.111.1: icmp_seq=8 ttl=64 time=1.43 ms
64 bytes from 10.20.111.1: icmp_seq=9 ttl=64 time=1.88 ms
64 bytes from 10.20.111.1: icmp_seq=10 ttl=64 time=2.22 ms
64 bytes from 10.20.111.1: icmp_seq=11 ttl=64 time=2.09 ms
```

```
C:\Documents and Settings\poly>ping 10.20.111.1

Pinging 10.20.111.1 with 32 bytes of data:

Reply from 10.20.111.1: bytes=32 time=9ms TTL=64
Reply from 10.20.111.1: bytes=32 time=3ms TTL=64
Reply from 10.20.111.1: bytes=32 time=3ms TTL=64

Ping statistics for 10.20.111.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 9ms, Average = 5ms
Control-C
```

2) Block incoming HTTP and SSH requests

Command: iptables -A INPUT -p tcp -s 10.10.111.0/24 —source-port 1024:65535 -d 10.20.111.0/24 —destination-port 80 -j REJECT

iptables -A INPUT -p tcp -s 10.10.111.0/24 —source-port 1024:65535 -d 10.20.111.0/24 —destination-port 80 -j REJECT

```
router:~# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source          destination
1    REJECT     tcp  --  10.10.111.0/24    10.20.111.0/24    tcp spts:1024:
65535 dpt:www reject-with icmp-port-unreachable
2    REJECT     tcp  --  10.10.111.0/24    10.20.111.0/24    tcp spts:1024:
65535 dpt:ssh reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
num  target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination
1    ACCEPT     icmp --  10.10.111.0/24    10.20.111.0/24
2    ACCEPT     all  --  10.20.111.0/24    10.10.111.0/24
```

3) Internal machine accepts telnet connection:

Code:

```
router:~# iptables -A INPUT -m mac --mac-source 02:00:c2:4a:00:01 -p tcp -d 10.20.111.0/24 --destination-port 23 -j ACCEPT
```

IPTABLE:

```
router:~# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source          destination
1    REJECT     tcp  --  10.10.111.0/24   10.20.111.0/24      tcp spts:1024
65535 dpt:www reject-with icmp-port-unreachable
2    REJECT     tcp  --  10.10.111.0/24   10.20.111.0/24      tcp spts:1024
65535 dpt:ssh reject-with icmp-port-unreachable
3    ACCEPT     tcp  --  anywhere        10.20.111.0/24      MAC 02:00:c2:4a:00:01 tcp dpt:telnet

Chain FORWARD (policy ACCEPT)
num  target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination
1    ACCEPT     icmp --  10.10.111.0/24   10.20.111.0/24
2    ACCEPT     all   --  10.20.111.0/24   10.10.111.0/24
```

TELNET:

```
root@bt:~# telnet 10.20.111.0
Trying 10.20.111.0...
```