Chan Ng Cashin
3/27/2024
HW09 - ECE 404

Description:

Flushed and deleted all previously defined rules in the filter, nat, raw, and mangle tables using -t, -F, and -X flags. -F flag is used to flush, -X flag is used to delete, and -t to specify table.

Used -A flag to update INPUT chain to accept only packets from f1.com. Used -p flag to specify that all protocols are to be accepted and -j to specify the ACCEPT target. Also used the -s flag to specify f1.com as the source.

Used MASQUERADE target to update nat table to change all outgoing packets to have the same IP as my machine.

To block scanning, I used the command line shown in Lecture 18. This line used the FORWARD chain to put a limit on the number of packets being scanned.

To block SYN-flooding I used a similar limit as the previous blocker to limit the number of packets being accepted.

For full loopback I again updated the INPUT chain using local host which is the lo interface. I also had to update the OUTPUT chain of the FILTER table. -i flag was used to specify the interface.

For port forwarding I updated PREROUTING chain in nat table to update the target rule between port 8888 and 25565 to DNAT. Then I updated FORWARD chain to accept packets to 25565 as the destination port.

Updated INPUT and OUTPUT chain in FILTER table to allow outgoing connections to engineering.purdue.edu.

Updated INPUT chain again to reject all packets that didn't follow the previously stated rules.

Output on next page

Firewall Output

```
channgcashin@channgcashin-Standard-PC-Q35-ICH9-2009:~/Documents/ECE404$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  cname.bitly.com      anywhere
ACCEPT     all  --  cname.bitly.com      anywhere
ACCEPT     all  --  anywhere             anywhere
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-unreachable
DROP       tcp  --  web-01-02-ha.ecn.purdue.edu  anywhere             tcp dpt:ssh
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,RST,ACK/SYN limit: avg 1/sec burst 5
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/SYN limit: avg 1/sec burst 5
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:25565

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             web-01-02-ha.ecn.purdue.edu  tcp spt:ssh
channgcashin@channgcashin-Standard-PC-Q35-ICH9-2009:~/Documents/ECE404$ sudo iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere             tcp dpt:8888 to::25565

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere
```