Cybersecurity (Security+) and P4 Programmable Switches

Overview Cybersecurity Labs

Ali AlSabeh, Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

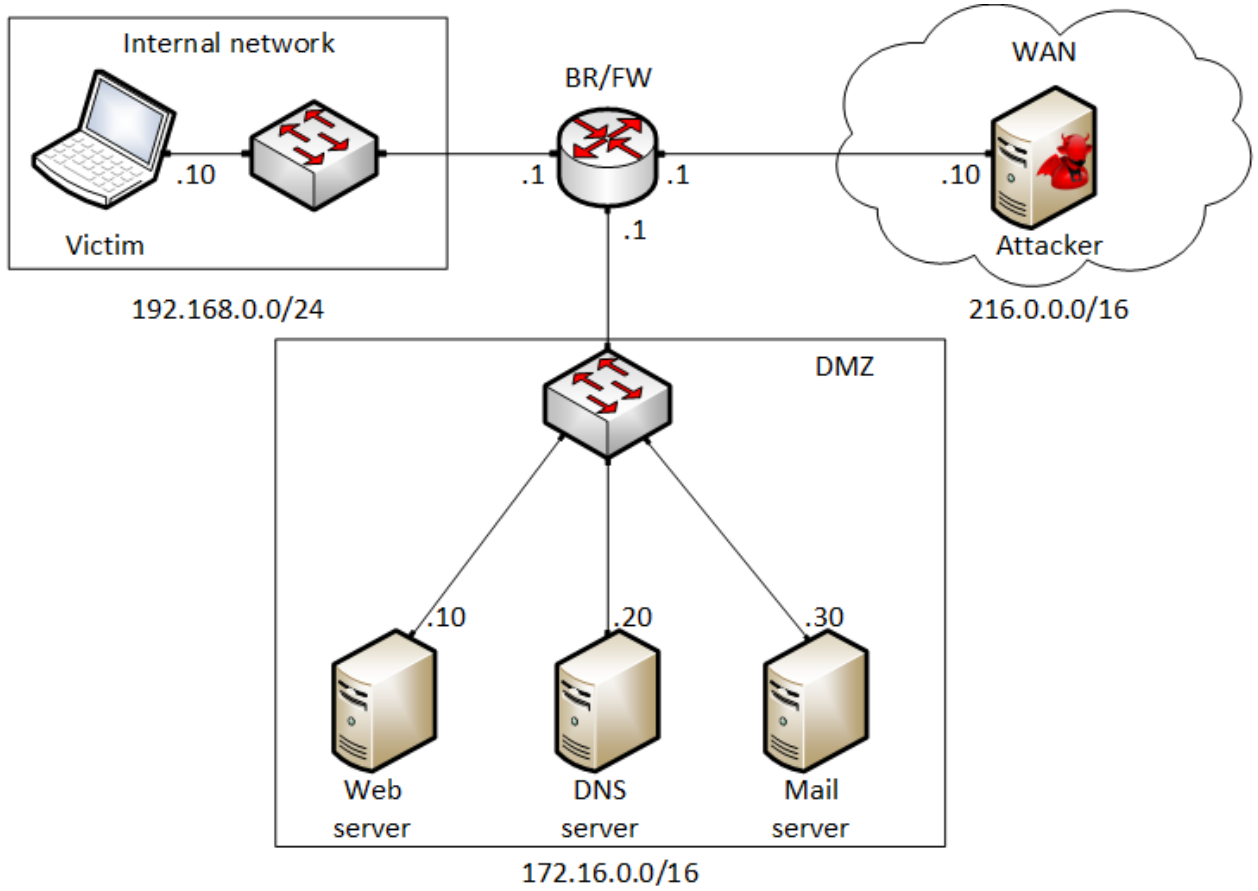
Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 21st, 2023

Lab 12: Configuring a Stateful Packet Filter using iptables

Attack Scenario

- Allow packets originating from the internal network to reach the WAN
- Deny packets originating from the WAN towards the internal network
- Allow packets originating from the internal network or the external network to reach the DMZ network (but not vice versa) as follows
  - The web server can only be reached on ports 80 (HTTP) or port 443 (HTTPS)
  - The DNS server can only be reached on port 53 (DNS)
  - The mail server can only be reached on port 25 (SMTP)



Configuring iptables

Displaying empty iptables rules

```
[root@BR-FW ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 6 packets, 501 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Allowing packets originating from the internal network to reach the WAN

```
[root@BR-FW ~]# iptables -I FORWARD -s 192.168.0.0/24 -d 216.0.0.0/16 -j ACCEPT
[root@BR-FW ~]# _
```

Allowing packets originating from the WAN to reach the internal network

```
[root@BR-FW ~]# iptables -A FORWARD -s 216.0.0.0/16 -d 192.168.0.0/24 -j ACCEPT
[root@BR-FW ~]# _
```

Configuring iptables

Displaying new iptables rules

```
[root@BR-FW ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 25 packets, 1725 bytes)
 pkts bytes target     prot opt in     out     source               destination
    8   480 ACCEPT     all  --  *      *       192.168.0.0/24       216.0.0.0/16
    0     0 ACCEPT     all  --  *      *       216.0.0.0/16         192.168.0.0/24

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Pinging the WAN from the internal network

```
Select Command Prompt

C:\Users\admin>ping 216.0.0.10

Pinging 216.0.0.10 with 32 bytes of data:
Reply from 216.0.0.10: bytes=32 time=1ms TTL=63
Reply from 216.0.0.10: bytes=32 time<1ms TTL=63
Reply from 216.0.0.10: bytes=32 time<1ms TTL=63
Reply from 216.0.0.10: bytes=32 time<1ms TTL=63

Ping statistics for 216.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Pinging the internal network from the WAN

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ping 192.168.0.10 -c 1                                        1 ×
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=127 time=0.912 ms

--- 192.168.0.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.912/0.912/0.912/0.000 ms
```

Configuring iptables

Deleting a rule from the FORWARD chain (by its index)

```
[root@BR-FW ~]# iptables -D FORWARD 2
[root@BR-FW ~]# _
```

Allowing external traffic **replying** to internal traffic

```
[root@BR-FW ~]# iptables -A FORWARD -s 216.0.0.0/16 -d 192.168.0.0/24 -j ACCEPT -m state --state REL
ATED,ESTABLISHED
[root@BR-FW ~]# _
```

Displaying new iptables rules

```
[root@BR-FW ~]# iptables -nvL --line-numbers
Chain INPUT (policy ACCEPT 1 packets, 229 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       13   804 ACCEPT     all  --  *      *       192.168.0.0/24       216.0.0.0/16
2        0     0 ACCEPT     all  --  *      *       216.0.0.0/16         192.168.0.0/24       state
RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
```

Configuring iptables

Allowing **specific** traffic coming from the internal network or the WAN to the web

```
[root@BR-FW ~]# iptables -I FORWARD -s 192.168.0.0/24,216.0.0.0/16 -d 172.16.0.10 -p tcp --match mul
tiport --dports 80,443 -j ACCEPT
[root@BR-FW ~]#
```

Allowing **specific** traffic coming from the web server to the internal network or the WAN and related to an established session

```
[root@BR-FW ~]# iptables -I FORWARD 3 -s 172.16.0.10 -d 192.16.0.0/24,216.0.0.0/16 -p tcp --match mu
ltiport --sports 80,443 -j ACCEPT -m state --state RELATED,ESTABLISHED
[root@BR-FW ~]# _
```