



# Cybersecurity (Security+) and P4 Programmable Switches

## Lab 14: Intrusion Detection and Prevention using Suricata

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

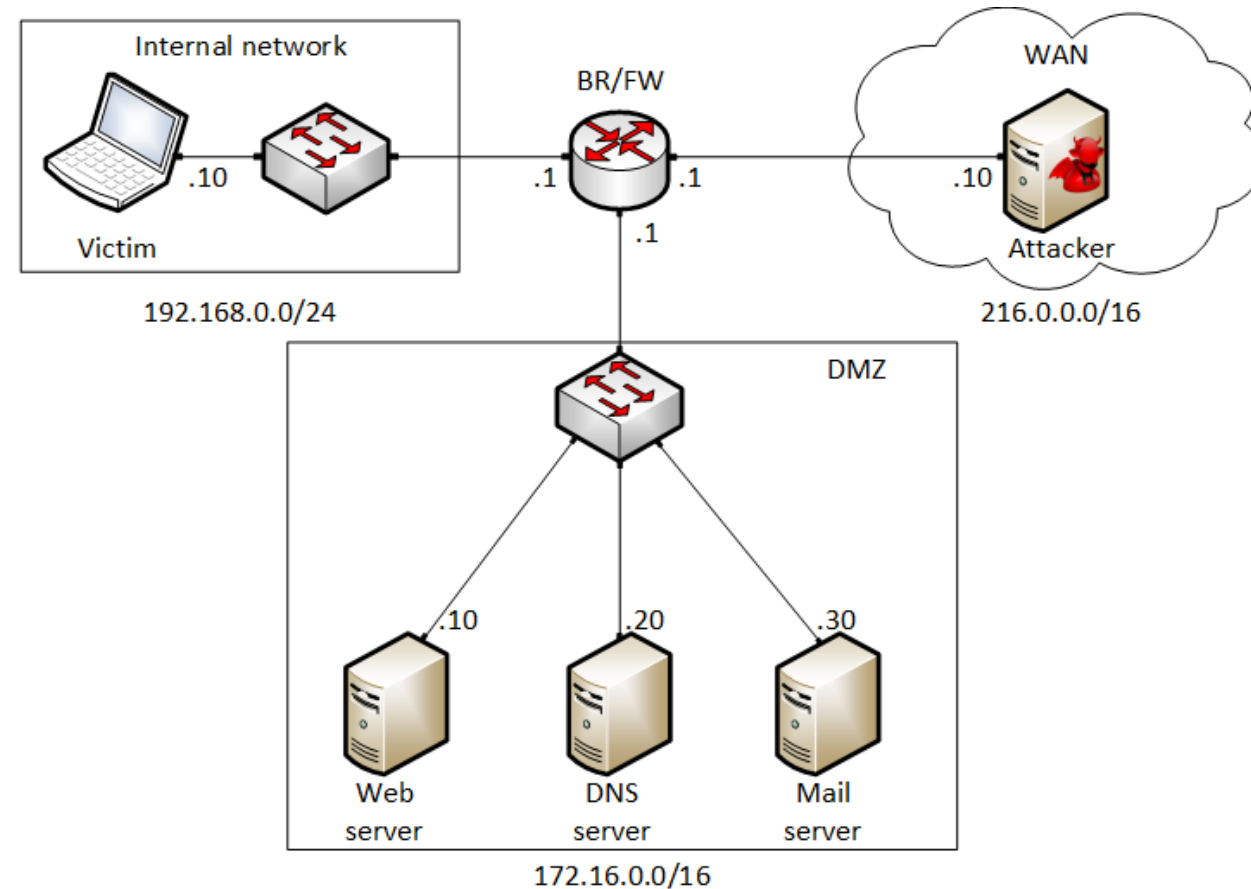
Western Academy Support and Training Center (WASTC)  
University of South Carolina (USC)  
Energy Sciences Network (ESnet)

June 21<sup>st</sup>, 2023

# Lab 14: Intrusion Detection and Prevention using Suricata

# Attack Scenario

- Using the BR/FW as a *Suricata* IDS to send alerts upon matching ICMP packets destined to the DNS server
- Using the BR/FW as *Suricata* IPS to drop ICMP packets destined to the mail server
- Using the BR/FW as a *Suricata* IDS to send alerts upon matching TCP SYN packets destined to the DNS server
- Using the BR/FW as a *Suricata* IPS to prevent SYN flood attack against the DNS server



# Suricata as IDS for ICMP Alerts

Adding a new custom rule file to *Suricata* configuration file

```
GNU nano 2.3.1 File: /etc/suricata/suricata.yaml

# The most common hashmode commands are: hash2tuple, hash2tuplesorted,
# hash5tuple, hash5tuplesorted and roundrobin.
#
# See Napatech NTPL documentation other hashmodes and details on their use.
#
# This parameter has no effect if auto-config is disabled.
#
hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
# - suricata.rules
- detect-icmp.rules
```

Adding a new rule to alert ICMP packets destined to the DNS server

```
GNU nano 2.3.1 File: /var/lib/suricata/rules/detect-icmp.rules Modified

alert icmp any any -> 172.16.0.20 any (msg:"ICMP detected to the DNS server"; sid:123456; rev:1;)
```

# Suricata as IPS for ICMP Drops

Adding a new rule to drop ICMP packets destined to the mail server

```
GNU nano 2.3.1 File: /var/lib/suricata/rules/detect-icmp.rules Modified
alert icmp any any -> 172.16.0.20 any (msg:"ICMP detected to the DNS server"; sid:123456; rev:1;)
drop icmp any any -> 172.16.0.30 any (msg:"ICMP to 172.16.0.30 is dropped"; sid:1234567; rev:1;)
```

Pinging the DNS server

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ ping 172.16.0.20 -c 1
PING 172.16.0.20 (172.16.0.20) 56(84) bytes of data:
64 bytes from 172.16.0.20: icmp_seq=1 ttl=63 time=1.31 ms

--- 172.16.0.20 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.312/1.312/1.312/0.000 ms
```

Pinging the mail server

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ ping 172.16.0.30 -c 1
PING 172.16.0.30 (172.16.0.30) 56(84) bytes of data:

--- 172.16.0.30 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

# Suricata as IDS for TCP SYN Alerts

Adding a new custom rule file to *Suricata* configuration file

```
GNU nano 2.3.1      File: /etc/suricata/suricata.yaml
#
# See Napatech NTPL documentation other hashmodes and details on their use.
#
# This parameter has no effect if auto-config is disabled.
#
hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
# - suricata.rules
- detect-icmp.rules
- detect-SYN-Flood.rules
```

Adding a new rule to alert TCP SYN packets destined to the DNS server

```
GNU nano 2.3.1      File: /var/lib/suricata/rules/detect-SYN-Flood.rules
alert tcp any any -> 172.16.0.20 any (flags:S; sid:1234568; rev:1;)
```

# Suricata as IPS for TCP SYN Flood Attack

---

Adding a new rule to limit the rate of TCP SYN packets destined to the DNS server

```
GNU nano 2.3.1          File: /etc/suricata/threshold.config          Modified
# Please note that thresholding can also be set inside a signature. The interaction between rule ba$
# and global thresholds is documented here:
# https://suricata.readthedocs.io/en/latest/configuration/global-thresholds.html#global-thresholds-$
# Limit to 10 alerts every 10 seconds for each source host
#threshold gen_id 0, sig_id 0, type threshold, track by_src, count 10, seconds 10
# Limit to 1 alert every 10 seconds for signature with sid 2404000
#threshold gen_id 1, sig_id 2404000, type threshold, track by_dst, count 1, seconds 10
# Avoid to alert on f-secure update
# Example taken from https://blog.inliniac.net/2012/03/07/f-secure-av-updates-and-suricata-ips/
#suppress gen_id 1, sig_id 2009557, track by_src, ip 217.110.97.128/25
#suppress gen_id 1, sig_id 2012086, track by_src, ip 217.110.97.128/25
#suppress gen_id 1, sig_id 2003614, track by_src, ip 217.110.97.128/25
rate_filter gen_id 1, sig_id 1234568, track by_dst, count 1000, seconds 1, new_action drop,
timeout 30
```

