Cybersecurity (Security+) and P4 Programmable Switches

Lab 14: Intrusion Detection and Prevention using Suricata

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

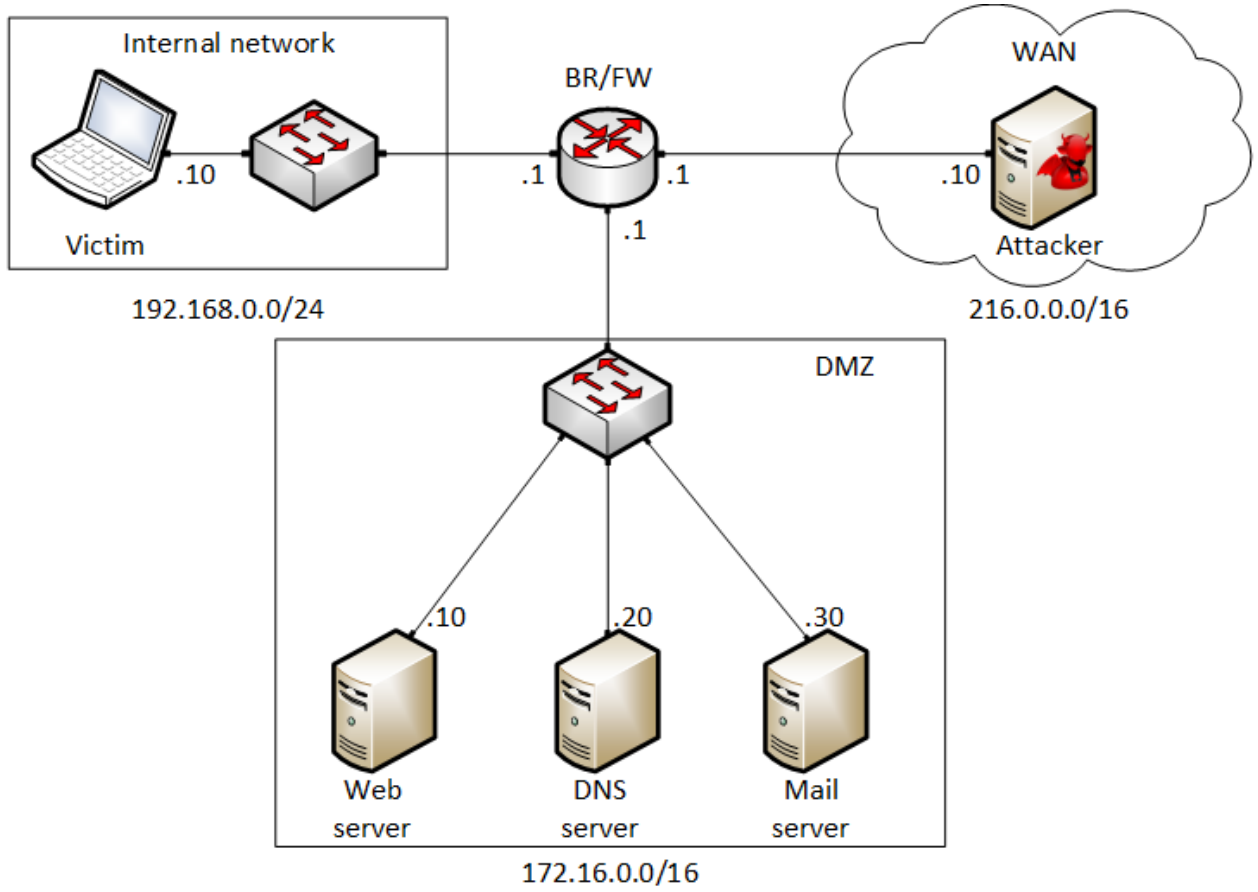
Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 21st, 2023

Lab 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

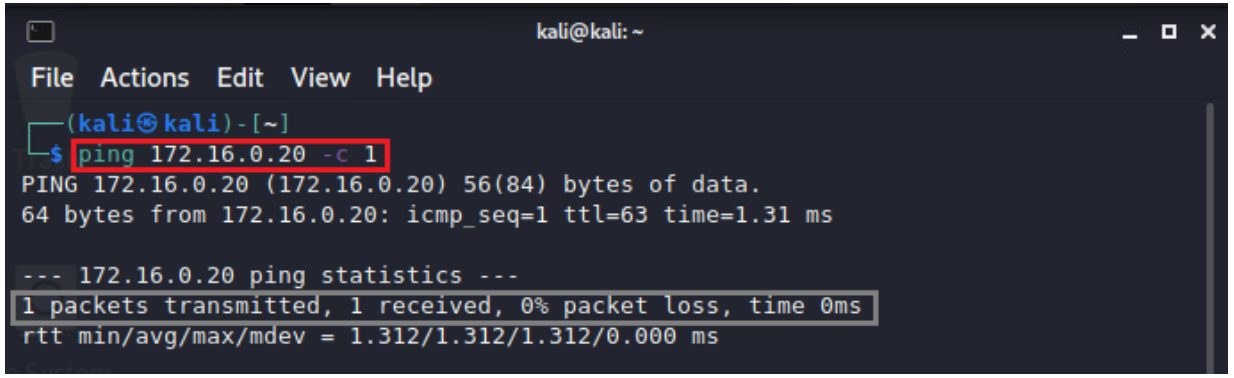
```
 GNU nano 2.3.1          File: /var/lib/suricata/rules/detect-icmp.rules          Modified

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

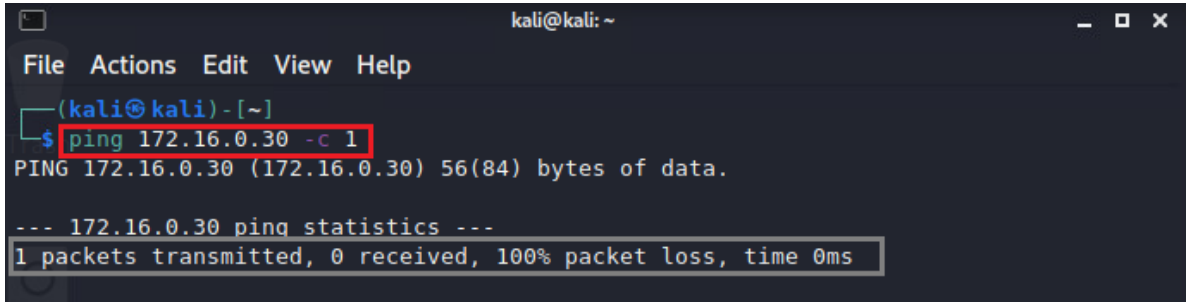
Adding a new rule to drop ICMP packets destined to the mail server

```
 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



Pinging the mail server



Suricata as IDS for TCP SYN Alerts

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

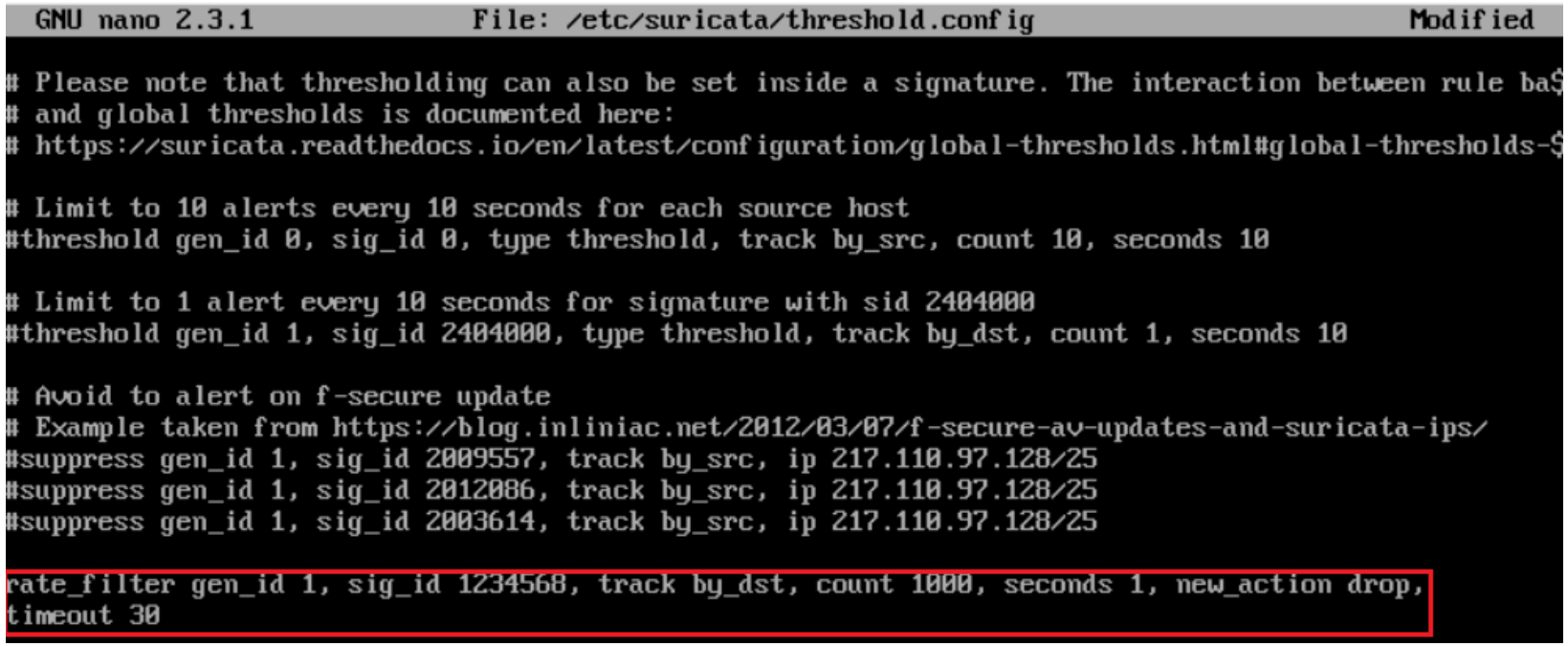
```
 GNU nano 2.3.1                File: /etc/suricata/suricata.yaml

    #
    # 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



Suricata as IPS for TCP SYN Flood Attack

Inspecting the network usage on the DNS server under TCP SYN flood attack

Inspecting the network usage on the mail server under TCP SYN flood attack