



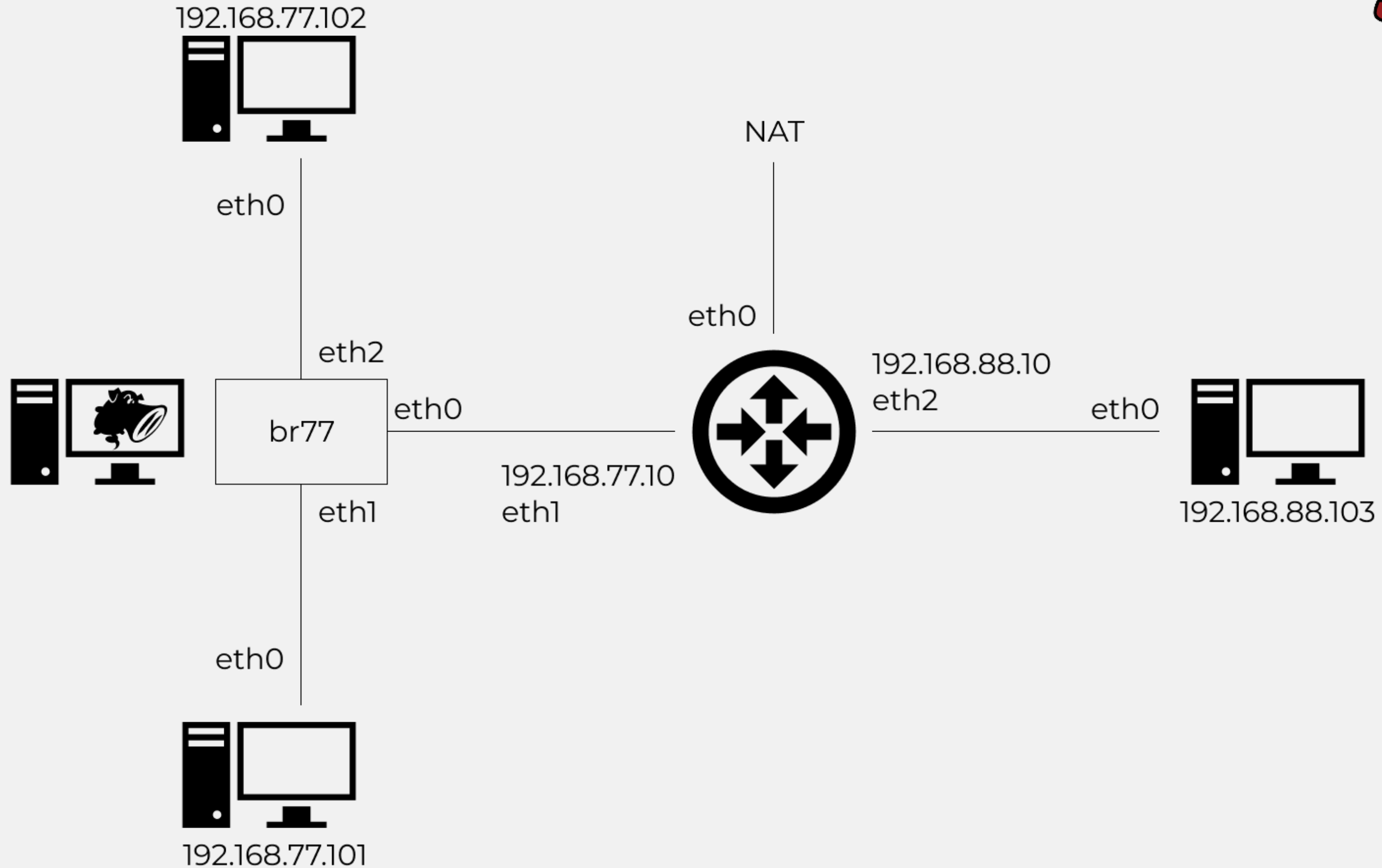
SNORT v3

Intrusion Detection & Prevention System

Edoardo Mich
Davide Moletta
Tefera Addis Sisay

Network Security Lab 22/23

Network setup



Rules syntax



```
action protocol IPaddr port# -> IPaddr port#  
      (options)
```

Rules syntax

SNORT actions



action protocol IPaddr port# -> IPaddr port#
(options)

Basic actions:

- Alert: generate an alert on the current packet
- Block: block the current packet and all the subsequent packets in this flow
- Drop: drop the current packet
- Log: log the current packet
- Pass: mark the current packet as passed

Active responses:

- React: send response to client and terminate session.
- Reject: terminate session with TCP reset or ICMP unreachable
- Rewrite: enables overwrite packet contents based on a "replace" option in the rules

Rules syntax

SNORT protocols



`action protocol IPaddr port# -> IPaddr port#`
`(options)`

Protocols:

- IP
- ICMP
- TCP
- UDP

Services:

- SSL
- HTTP
- SMTP

Rules syntax

IP addresses



`action protocol IPaddr port# -> IPaddr port#
(options)`

IP addresses on which the rule should be applied, can be defined in four ways:

- Numeric IP address: 192.168.77.101, 192.168.77.0/24
- Variable defined in the Snort config: \$HOME_NET
- The keyword any, meaning any IP address
- List of IP addresses: [192.168.77.0/24,10.1.1.0/24]

Rules syntax

Ports



`action protocol IPaddr port# -> IPaddr port#`
`(options)`

Ports on which snort will inspect and apply the rule, can be defined in five different ways:

- The keyword any, meaning any port
- Static port: 8080
- Variable defined in the Snort config: \$HTTP_PORTS
- Port ranges indicated with the range operator: 1:1024
- List of static ports: [1:1024,4444,5555]

Rules syntax

Direction operators



`action protocol IPaddr port# -> IPaddr port#`
`(options)`

The direction operator indicates the direction of the traffic that the rule should apply to.

There are two valid direction operators:

- `->`: The first IP is the source and the second is the destination
- `<>`: Both addresses are source and destination

Rules syntax

SNORT options



`action protocol IPaddr port# -> IPaddr port#
(options)`

All rule options are enclosed in parentheses after the end of the rule.

Each rule option is declared with its name followed by : and any option-specific criteria.

Each rule option is terminated with ;. Some examples of rule options are:

- msg: set a message to be displayed when the rule fires
- sid: set a numeric identifier to the rule
- priority: set a priority to the rule
- content: used to perform basic pattern matching against packet data

Directories

Where to find things



```
snort
├── binaries
├── confs
│   ├── snort_ids.lua
│   └── snort_ips_nfq.lua
├── dumps
│   ├── IDS_exercise
│   └── Qakbot.zip
├── enableNFQ.sh
└── rules
    └── snort3-community-rules
```

Aliases



```
snort3="snort --daq afpacket -A alert_full"
```

```
snort3_ips="snort --daq-dir /usr/local/lib/daq  
             -c /root/snort/confs/snort_ips_nfq.lua -Q -A alert_full"
```

```
snort3_pcap="snort --daq pcap -A alert_fast -k none"
```

```
snort3_qakbot="snort -c /usr/local/etc/snort/snort.lua -A alert_full  
              --lua \"alert_full = { file=true }\""
```

Exercise 1



Write a rule to detect ping from any IP to any IP

Run snort with the following command

```
snort3 -i br77 -R snort/rules/exercise01.rules
```

Exercise 1 solution



Write a rule to detect ping from any IP to any IP

```
alert icmp any any -> any any
(
    sid:1
)
```

Exercise 2



Write a rule to detect ping from .77.101 to .88.103
and write a message when the rule fires

Run snort with the following command

```
snort3 -i br77 -R snort/rules/exercise02.rules
```

Exercise 2 solution



Write a rule to detect ping from .77.101 to .88.103
and write a message when the rule fires

```
alert icmp 192.168.77.101 any -> 192.168.77.102 any  
(  
    sid:2;  
    msg:"ping from client 101 to client 102"  
)
```

Exercise 3



Write a rule to detect ping replies
from .77.101 to .77.102

Run snort with the following command

```
snort3 -i br77 -R snort/rules/exercise03.rules
```

Hint: use Wireshark to inspect the packets and
use the snort option itype: to write the rule

Exercise 3 solution



Write a rule to detect ping replies
from .77.101 to .77.102

```
alert icmp 192.168.77.101 any -> 192.168.77.102 any  
(  
    itype:0;  
    sid:3;  
    msg:"ping reply from client 101 to client 102"  
)
```

Exercise 4



Write a rule to detect TCP packets
from .77.101 to .88.103

Run snort with the following command

```
snort3 -i br77 -R snort/rules/exercise04.rules
```

Hint: every client machine has a python script that sends TCP packets to the specified IP address. Use python3 packet.py on client 101 and provide a valid IP to send the packet

Exercise 4 solution



Write a rule to detect TCP packets
from .77.101 to .88.103

```
alert tcp 192.168.77.101 any -> 192.168.88.103 any  
(  
    sid:4;  
    msg:"A TCP packet from client 101 to client 103"  
)
```

Exercise 5



Write a rule to detect TCP packets with
ACK flag from .77.101 to .88.103

Run snort with the following command

```
snort3 -i br77 -R snort/rules/exercise05.rules
```

Hint: use

client 103: nc -l -p 666

client 101: nc 192.168.88.103 666

Exercise 5 solution



Write a rule to detect TCP packets with
ACK flag from .77.101 to .88.103

```
alert tcp 192.168.77.101 any -> 192.168.88.103 any  
(  
  flags:*A;  
  sid:5;  
  msg:"ACK tcp packet from client 101 to client 103"  
)
```

Exercise 6



Write a rule to detect DNS requests from home network to anything but the company DNS server

Run snort with the following command

```
snort3 -i br77 -R snort/rules/exercise06.rules  
-c snort/confs/snort_ids.lua
```

Hint: remember that you can use variables instead of static IPs, check the configuration file snort_ids.lua to get further hints

Exercise 6 solution



Write a rule to detect DNS requests from home network to anything but the company DNS server

```
alert udp $HOME_NET any -> !$DNS_SERVER 53
(
  sid:6;
  msg:"DNS request to a not standard DNS server"
)
```

Exercise 7



Write a rule to detect HTTP requests with
unallowed user-agents from HOME_NET to .88.103

Run snort with the following command

```
snort3 -i br77 -R snort/rules/exercise07.rules  
      -c snort/confs/snort_ids.lua
```

Hint: the only user agent we want to accept is wget family

Exercise 7 solution



Write a rule to detect HTTP requests with
unallowed user-agents from HOME_NET to .88.103

```
alert http $HOME_NET any -> any any  
(  
  http_header:field user-agent;  
  content:! "wget", nocase;  
  sid:7;  
  msg:"Unallowed user-agent in HTTP request from HOME_NET"  
)
```

Exercise 8



Write a rule to detect SQLi on the pcap file

Run snort with the following command

```
snort3_pcap -c snort/confs/snort_ids.lua  
-r snort/dumps/sqlinj.pcap -R snort/rules/exercise08.rules
```

Exercise 8 solution



Write a rule to detect SQLi on the pcap file

```
alert http any any -> any 8080
(
  http_uri:query;
  content:"search=",nocase;
  pcre:"/(.*[\"\' ]\;)+.*"/;
  sid:8;
  msg:"SQLi command in search parameter"
)
```

Exercise 9



An example of Snort3 portscan module

Run snort with the following command

```
snort --daq afpacket -A alert_fast -i br77  
      -c /usr/local/etc/snort/snort.lua  
      --lua "port_scan = default_low_port_scan  
ips = {enable_builtin_rules = true, variables = default_variables}"
```

Hint: use the alias
snort3_portscan

Exercise 10



Write a rule to detect QAKbot on the pcap file

Run snort with the following command

```
snort3_qakbot -r snort/dumps/Qakbot/2023-05-24-obama264-  
Qakbot-infection.pcap -R snort/rules/exercise10.rules
```

Exercise 10 solution



Write a rule to detect QAKbot on the pcap file

You can find the rules in the file `secretpath/exercise10.rules`

IPS

Intrusion Prevention System



Run the following command to enable the IPS capabilities for snort

```
snort/enablenfq.sh
```


Exercise 11



Write a rule to block ping from any IP to any IP

Run snort with the following command

```
snort3_ips -R snort/rules/exercise11.rules
```


Exercise 11 solution



Write a rule to block ping from any IP to any IP

```
block icmp any any -> any any
(
    sid:11
)
```

Exercise 12



Write a rule to block TCP packets with
ACK flags from .77.101 to .88.103

Run snort with the following command

```
snort3_ips -R snort/rules/exercise12.rules
```

Exercise 12 solution



Write a rule to block TCP packets with
ACK flags from .77.101 to .88.103

```
block tcp 192.168.77.101 any -> 192.168.88.103 any  
(  
  flags:*A;  
  sid:12;  
  msg:"Blocked an ACK packet from client 101 to client 103"  
)
```

Exercise 13



Write a rule to drop DNS requests for unitn.it domains to not company DNS server.

Run snort with the following command

```
snort3_ips -R snort/rules/exercise13.rules
```

Hint: use Wireshark to inspect packets and use the snort option content:

Exercise 13 solution



Write a rule to drop DNS requests for untin.it domains to not company DNS server.

```
drop udp $HOME_NET any -> !$DNS_SERVER 53
(
  content:"|05 75 6e 69 74 6e 02 69 74 00|";
  sid:13;
  msg:"Blocked DNS request to a not standard DNS server"
)
```

Exercise 14



Write a rule to block SQLi on the pcap file

Run snort with the following command

```
snort3_pcap -r snort/dumps/sqlinj.pcap  
-R snort/rules/exercise14.rules
```

Exercise 14 solution



Write a rule to block SQLi on the pcap file

```
block http any any -> any 8080
(
  http_uri:query;
  content:"search=",nocase;
  pcre:"/(.*[\"\' ]\;)+.*(DROP|INSERT)+/";
  sid:14;
  msg:"Blocked SQL command in search parameter"
)
```

Thank you for your kind attention



Edoardo Mich
Davide Moletta
Tefera Addis Sisay

Network Security Lab 22/23