SNORT v3

Network Security Laboratory Project Cheatsheet

Group 4: Edoardo Mich, Davide Moletta, Tefera Addis Sisay

University of Trento

June 4, 2023

1 Aliases

Alias used to run snort in IDS mode

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

Alias to run snort in IPS mode

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

Alias to run snort on .pcap files in IDS mode

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

Alias to run snort on qakbot .pcap file

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

Alias to run snort in portscan mode

```
snort3_portscan="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}""
```

2 Useful commands

Command to run Snort in IDS mode

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

Command to run Snort in IPS mode

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

Command to run Snort in IDS mode giving a specific configuration file

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

Command to run Snort in IDS mode giving a specific configuration file and a .pcap file

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

Command to run Snort for the Qakbot exercise

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

Command to start tcpdump on a specifc interface

```
tcpdump -ni eth0
```

Command for NetCat

```
#On client 103
nc -lp 666
#On client 101 (alerted)
nc 192.168.88.103 666
#On client 102
nc 192.168.88.103 666
```

Command to run a basic python server and connect to it via wget/curl

```
#On client 103
python3 -m http.server 666
#On client 101/102
wget 192.168.88.103:666
#On client 101/102 (alerted)
curl 192.168.88.103:666
```

Command for Nmap

```
#On client 101
nmap -nsS 192.168.77.102
nmap -nsT 192.168.77.102
nmap -nsU 192.168.77.102
```

Command for nslookup

```
nslookup google.com 192.168.88.103
```

3 Useful Snort options

The sid rule option is used to set a numeric identifier to a Snort rule.

```
action protocol IPaddress port# -> IPaddress port#
(
    sid: num
)
```

The msg rule option is used to set a string that Snort will print once the rule fires.

```
action protocol IPaddress port# -> IPaddress port#
(
    msg: "A message"
)
```

The itype rule option is used to compare a packet's ICMP type to a specified integer value. It is a non-payload detection option.

```
action icmp IPaddress port# -> IPaddress port#
(
     itype: num
)
```

The flags rule option is used to check if flag bits are set in a TCP header. Additionally, one of the following modifiers can be added:

1. **+** match the specified flags plus any others,
2. ***** match if any of the specified flags are set,
3. **!** match if the specified flags are not set.

```
action tcp IPaddr port# -> IPaddr port#
(
    flags:[+*!] F || S || R || P || A || U || C || E || 0
)
```

The http_header rule option allows to look for content matches in HTTP header (we can specify in which field using http_header: flied fieldName).

```
action http IPaddr port# -> IPaddr port#
(
   http_header:field fieldName
)
```

The content rule option is used to perform pattern matching against packet data.

```
action protocol IPaddr port# -> IPaddr port#
(
   content:[!]"content_string", nocase //used to be case insensitive
   content:"|hexvalues|" //to match against HexValues instead of strings

)
```

The http_uri rule option allows to look for content matches in HTTP uri.

```
action http IPaddr port# -> IPaddr port#
(
   http_uri:path || query || fragment || host || port || scheme
)
```

The pcre rule option is used to match Perl compatible regular expression strings against packet data.

```
action protocol IPaddr port# -> IPaddr port#
(
   pcre:[!]"/pcre_string/[flag]" //use pcrepattern sintax for regex
)
```