NETVÆRKS- OG KOMMUNIKATIONSSIKKERHED

IDS rules

Agenda

- Before we begin
- IDS
- Hand-inn exercise

Before we begin

- Skoleprotokol
- Visit by Jesper B. Hansen (Siscon, Rådet for digital sikkerhed)
- Filling out survey from Kea

Security onion

Collection of tools built on top of Ubuntu distribution

IDS/IPS

- Snort
- Suricata

Analysis

- Squert
- ELSA
- Sguil

Logging

- Bro
- netsniff-ng

HIDS

- OSSEC

Security onlion services

- You can see the services running:
  `sudo service nsm status`

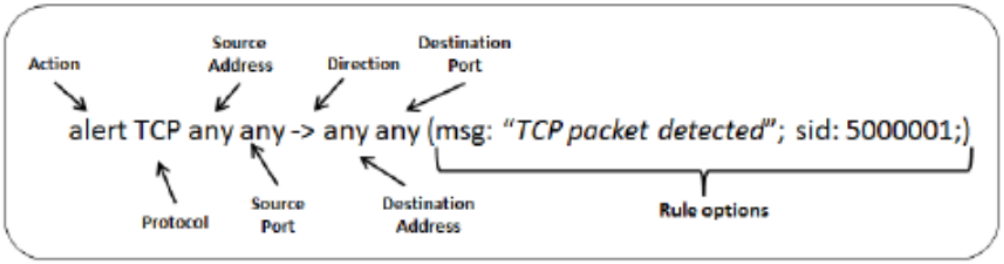
- To restart all services
  Sudo service nsm restart

- To restart a single sensor service for instance Snort after a config change:
  `sudo nsm_sensor_ps-restart --only-snort-alert`

Snort rules

- Several sources can be used for rules
- Most updated rules costs some money.
- ET
- GPL

Snort rules



- Address can also be $HOME_NET or $EXTERNAL_NET

Updating rules

- Rules can be written in

```
less etc/nsm/rules/local.rules
```

- The automatically downloaded rules are in

```
less etc/nsm/rules/downloaded.rules
```

- To update the rules to the most up to date, you can use

```
sudo rule-update
```

- It will create a copy of your old rules and place it in

```
ll etc/nsm/rules/backup/
```

Updating rules

- In some cases you would like to disable some alerts, and make sure that they will not be reapplied with the next rule-update request, you can disable them in
  `/etc/nsm/pulledpork/disablesid.conf`
- In our case we need to do that to the downloaded rule on line 5123, in downloaded.rules, because it crashes our snort.
- We find the sid of that rule, and then we add it to our disablesid.conf file
  `sudo nano /etc/nsm/pulledpork/disablesid.conf`
- At the bottom of that file we add
  `1:2002802`
- Then we update the rules again
  `sudo rule-update`
- If snort is not running
  `sudo nsm_sensor_ps-status --only-snort-alert`
- Then restart it
  `sudo nsm_sensor_ps-restart --only-snort-alert`

Creating custom rules

- Lets create a rule that will detect if someone is trying to retrieve something containing putty.exe (http://kallasoft.dk/putty.exe)
- Go to your local.rules and add the rule

```
sudo nano /etc/nsm/rules/local.rules
```

- Add the following to the file (its 1 line):

```
alert tcp any any -> any any (msg:"test"; uricontent:“putty.exe"; nocase;
sid:90005238; rev:1;)
```

- Then update the rules

```
sudo rule-update
```

- Now try to download the file http://kallasoft.dk/putty.exe from the kali linux

Detecting flooding

- We can also create rules to test for tcp flooding

```
alert tcp any any -> 192.168.65.1 any (msg:"TCP SYN
flood attack detected"; flags:S; threshold: type
threshold, track by_dst, count 20 , seconds 60;
classtype=denial-of-service;priority:5 ;sid: 5000001;
rev:1;)
```

- Then try to do the flooding from scapy.

Exercise 1

- Now try to create a rule that will trigger on someone doing ping on the internal network.
- Find the correct classification for the attack and put it on the rule. You can find all classifications in:

```
less /etc/nsm/rules/classification.config
```

Then set the class type in the rule

```
… classtype=xxx; …
```

Exercise 2

- You find that kallasoft webpage is considered malicious.
- Create a rules that will alert when someone from the internal network is trying to access it using http, https or ftp/ssh.

Blacklisting IP addresses

- First create a file inside the rules folder and call it preprocessor.rules

```
sudo nano /etc/nsm/rules/preprocessor.rules
```

- Then paste your alert rule in there (it should be 1 line) watch out for weird characters when you paste:

```
alert ( msg: “REPUTATION_EVENT_BLACKLIST"; sid: 1; gid: 136; rev: 1;metadata:
rule-type preproc ; classtype:bad-unknown; )
```

- Now enable the preprocessor.rules in the snort

```
sudo nano /etc/nsm/security-onion-eth0/snort.conf
```

- Search for preprocessor.rules (ctrl+w in nano) and remove the #

Blacklisting IP addresses

- Now add the ip address you want to block into your blacklist

```
sudo nano /etc/nsm/black_list.rules
```

- Just write the ip you want alarms on

```
8.8.8.8 # google ip
```

- Finally restart snort

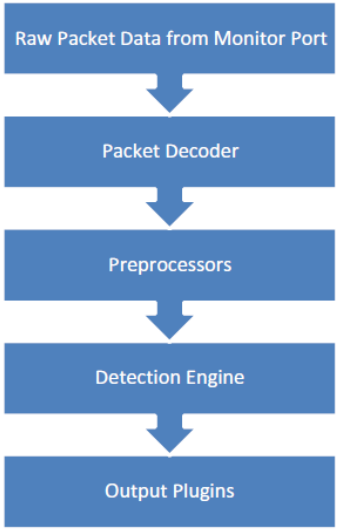
```
sudo nsm_sensor_ps-restart --only-snort-alert
```

Exercise 3

- Create a rule that will alert on your kali linux ip address
  - Hint: google for “scan_local”
- Are the other alerts for ICMP still showing up? Why?

Snort IDS architecture

- The preprocessor runs before the detection engine



Exercise 4

- Modify your ping alert so that it only alerts on a ttl higher that 60

Homework

- Write a rule that will detect if an ssh connection is successfully established from external network to the internal network!

- Create a rule that will alert when a http server locally replies with a "403" (forbidden) status code. The rule should only alert if this happens 3 times within 5 minutes.

Ps: a simple php file containing the following should throw the 403:

```php
<?php
    header("HTTP/1.1 403 Forbidden");
    exit;
?>
```

Hand-inn start-up

A midsize company requires a redesign of their network

Start with a clean slate, and create a network consisting of the following:

- 1 web server facing the www
- 1 web server for internal tools
- 2 database servers (for each webserver)
- 1 file server

- 1 sales team (~50 hosts) requiring internet access and access to local file server
- 1 technical support team (~10 hosts) requiring access to internal tools and web
- 1 development team (~10 hosts) they should have access to all systems, and have their own dev environment, consisting of a clone of the 5 servers above.
- Wifi setup for company access requiring only internet access

Hand-inn start-up

- Create a network diagram with all the components that you need (not vendor specific)
- Define the IPs for the subnets and devices
- Add the security devices you find necessary (firewalls, sensors, vpns)
- Write about your considerations (~ 1 page)

- Consider limited resources, and that we do not have all the storage in the world for storing full packet capture

- Preferably work in groups (2-3 persons)

References

Chapter on Squil and NSM

- http://ptgmedia.pearsoncmg.com/images/0321246772/samplechapter/bejtlich_chs.pdf

Snort rules infographic

- https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/116/original/Snort_rule_infographic.pdf?

Snort manual

- http://manual-snort-org.s3-website-us-east-1.amazonaws.com/