NETWORK & MULTIMEDIA LAB

INTRUSION DETECTION SYSTEM

Spring 2021

Recall: Network Security Basics

- **Protection:**
  - You should configure your systems and networks as correctly as possible

- **Detection:** Intrusion Detection System
  - You must be able to identify when the configuration has changed or when some network traffic indicates a problem
    - Host-based IDS (HIDS)
    - Network-based IDS (NIDS)

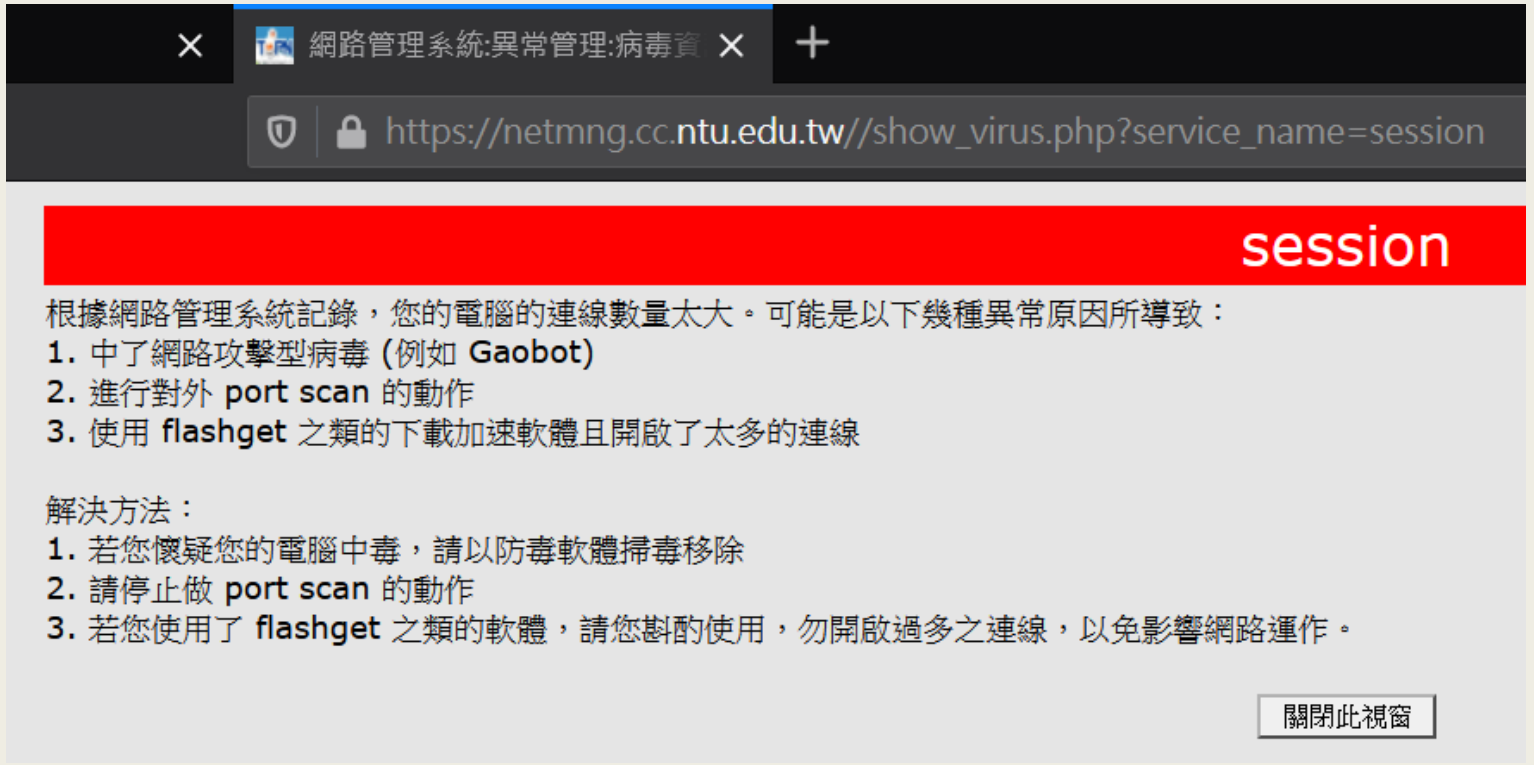
- **Reaction:** Intrusion Prevention System
  - After identifying problems quickly, you must respond to them and return to a safe state as rapidly as possible

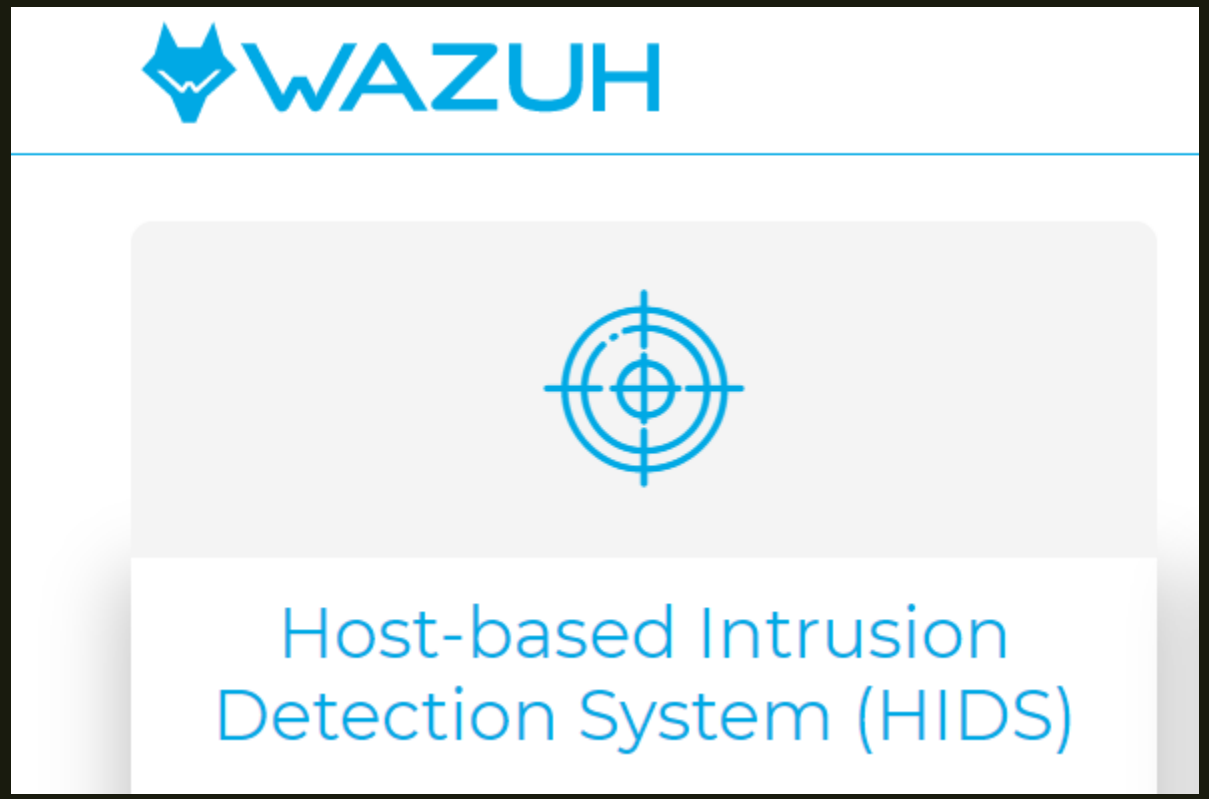
Security Products

	Network-based	Host-based
Detection	NIDS	HIDS
Prevention	IPS	Anti-Virus

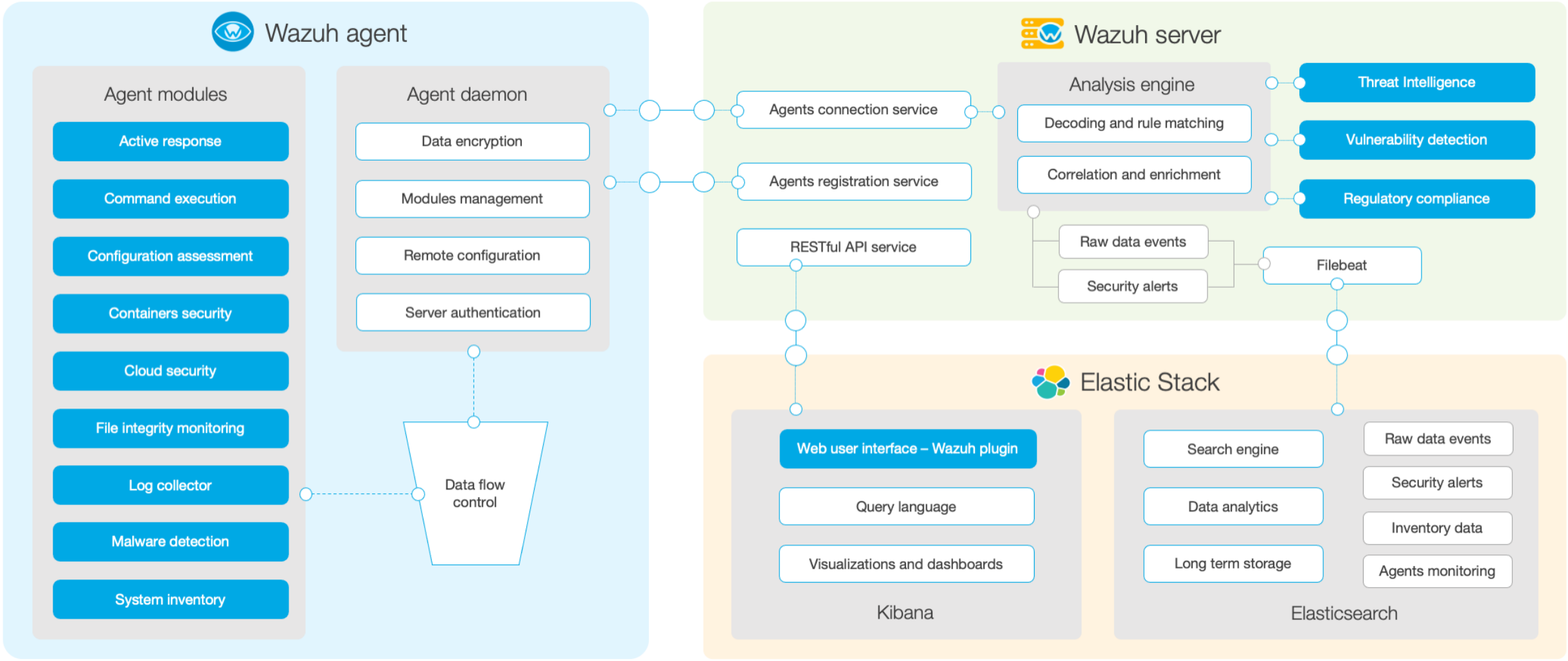
Detection approaches

- Signature-Based
- Statistical anomaly

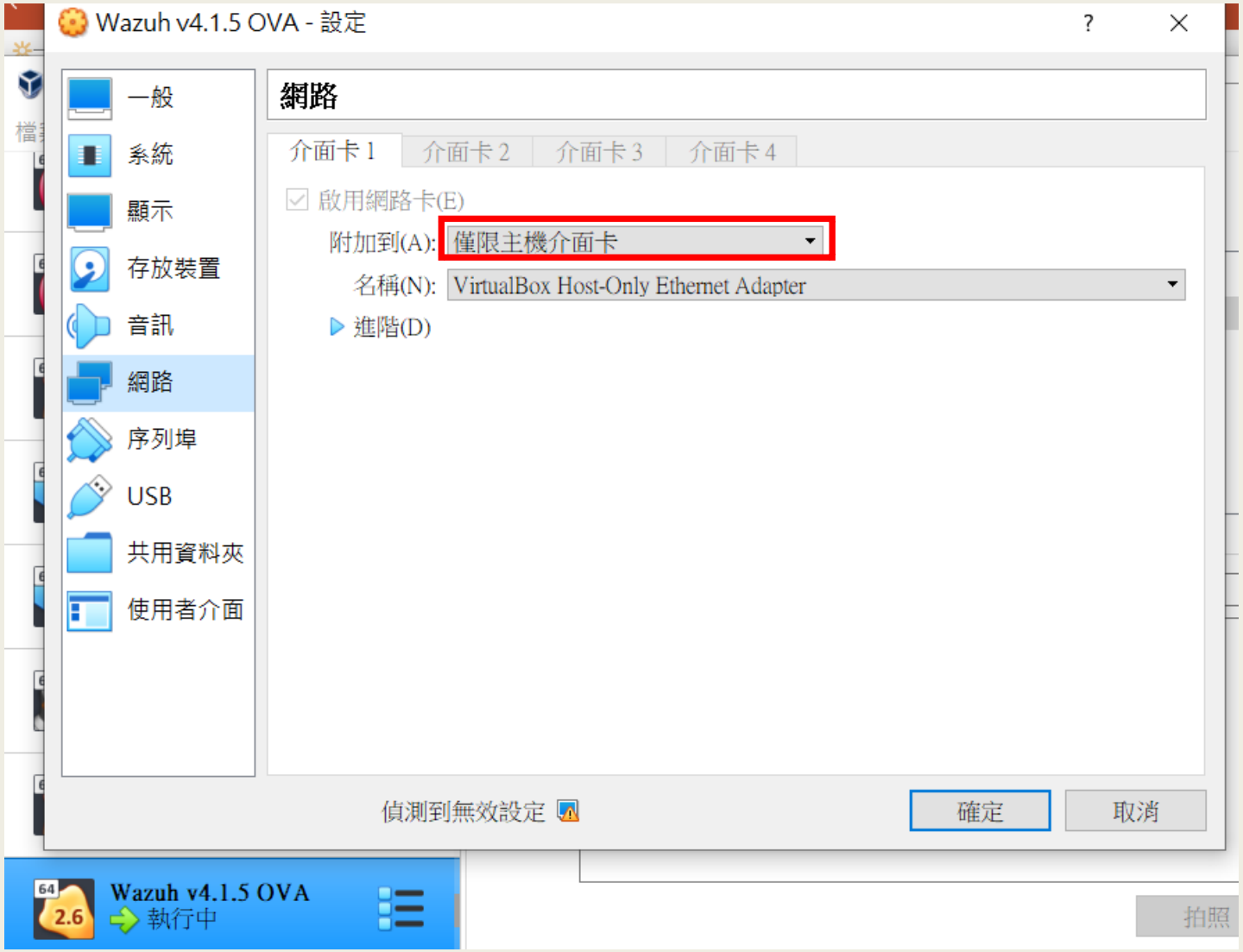



WAZUH
Host-based Intrusion Detection System (HIDS)

- The Wazuh architecture is based on agents, running on the monitored endpoints, that forward security data to a central server.



Wazuh


Wazuh v4.1.5 OVA - 設定
一般
系統
顯示
存放裝置
音訊
網路
序列埠
USB
共用資料夾
使用者介面
網路
介面卡 1
介面卡 2
介面卡 3
介面卡 4
啟用網路卡(E)
附加到(A): 僅限主機介面卡
名稱(N): VirtualBox Host-Only Ethernet Adapter
進階(D)
偵測到無效設定
確定
取消
Wazuh v4.1.5 OVA
執行中
拍照

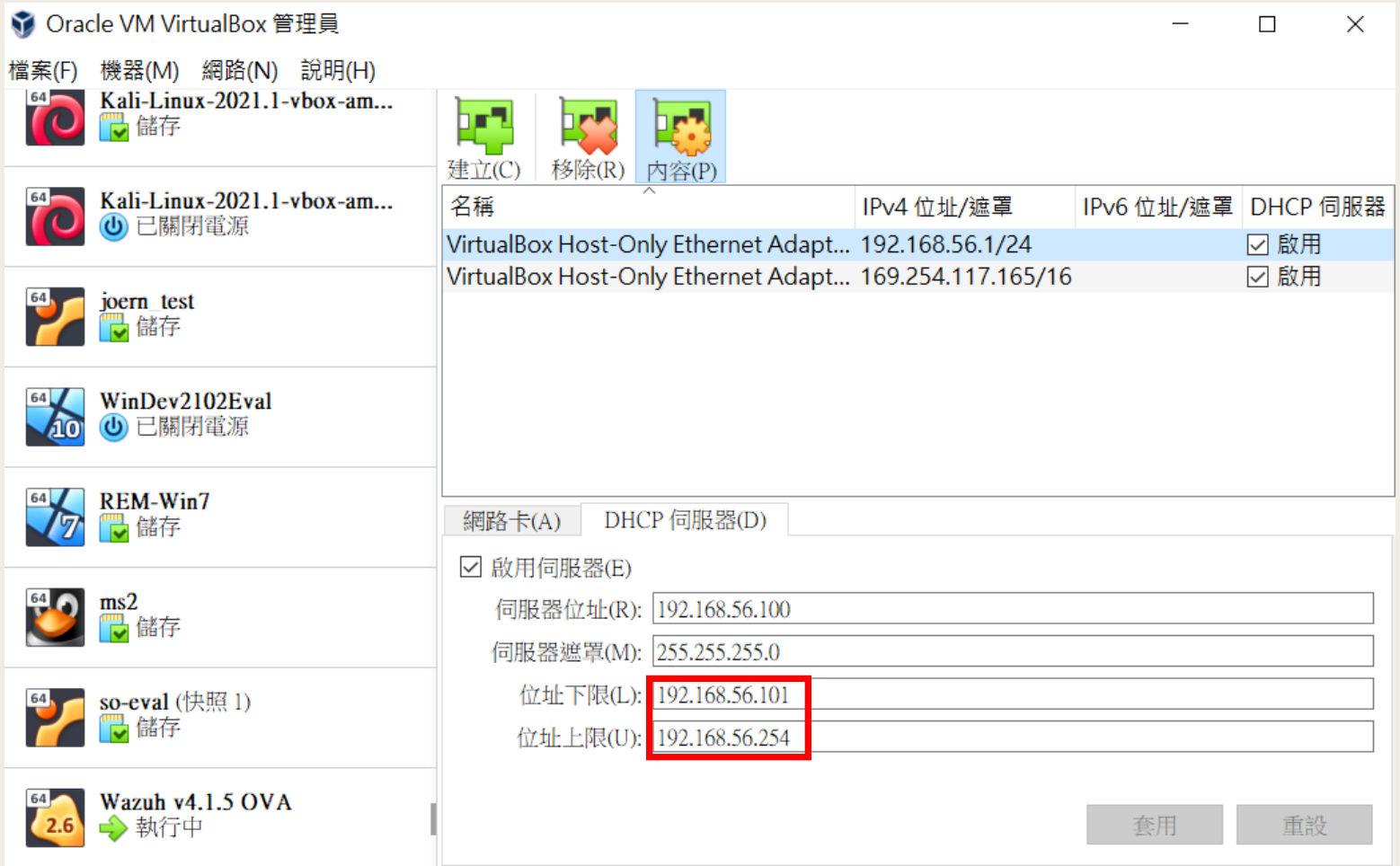
Wazuh

- VM
  - Username: root
  - Password: wazuh

- Web interface
  - Username: admin
  - Password: admin

Wazuh – Set a static IP

1. Determine IP
   - 192.168.56.99 (out of DHCP range - 192.168.56.2-99)



Wazuh – Set a static IP

2. Configuration
   - *vi /etc/sysconfig/network-scripts/ifcfg-eth0*

```
# Automatically generated by the vm import process
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
TYPE=Ethernet
NM_CONTROLLED=no
IPADDR="192.168.56.99"
NETMASK="255.255.255.0"
```

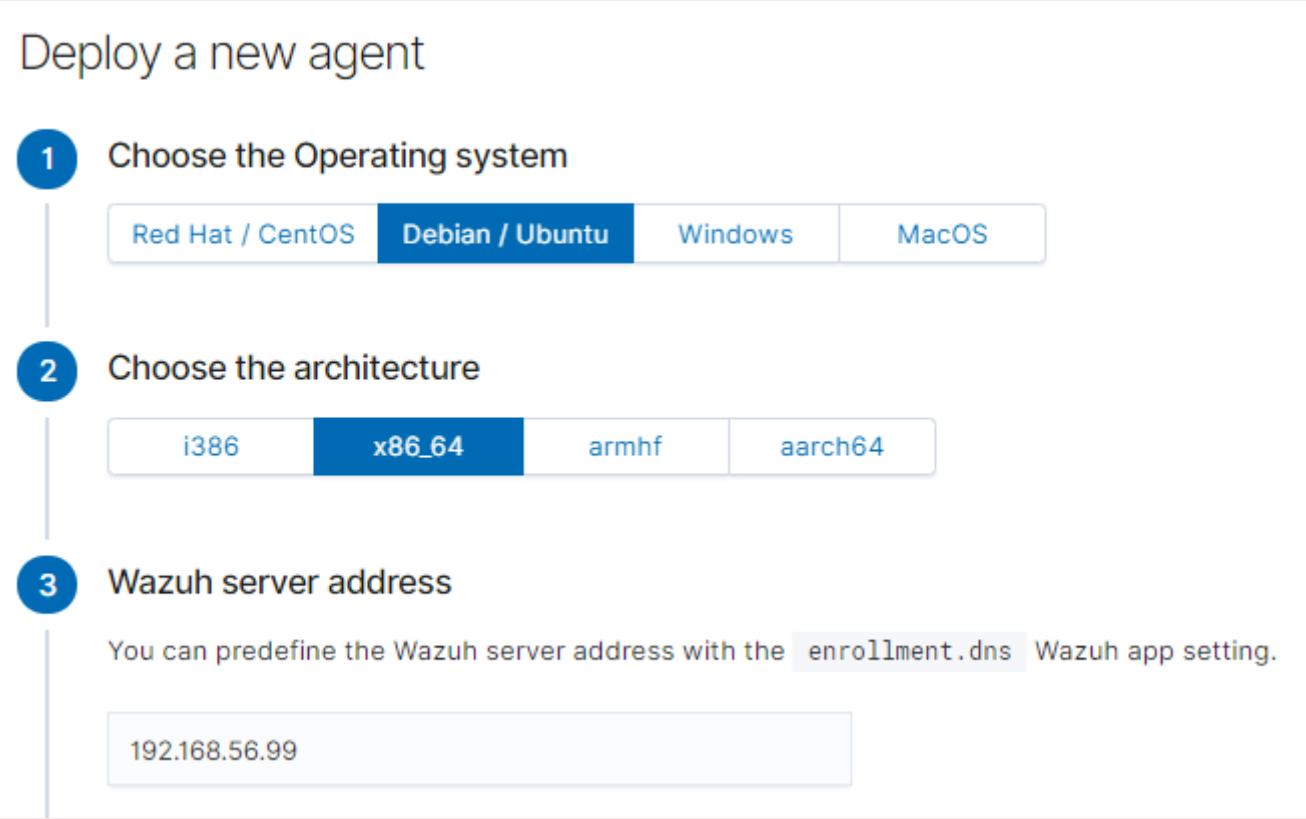
Wazuh – Set a static IP

3. Restart service
   - *service network restart*
4. Check IP
   - *ip addr*

```
[root@manager ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
0
    link/ether 08:00:27:4c:3a:ff brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.99/24 brd 192.168.56.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe4c:3aff/64 scope link
       valid_lft forever preferred_lft forever
[root@manager ~]#
```

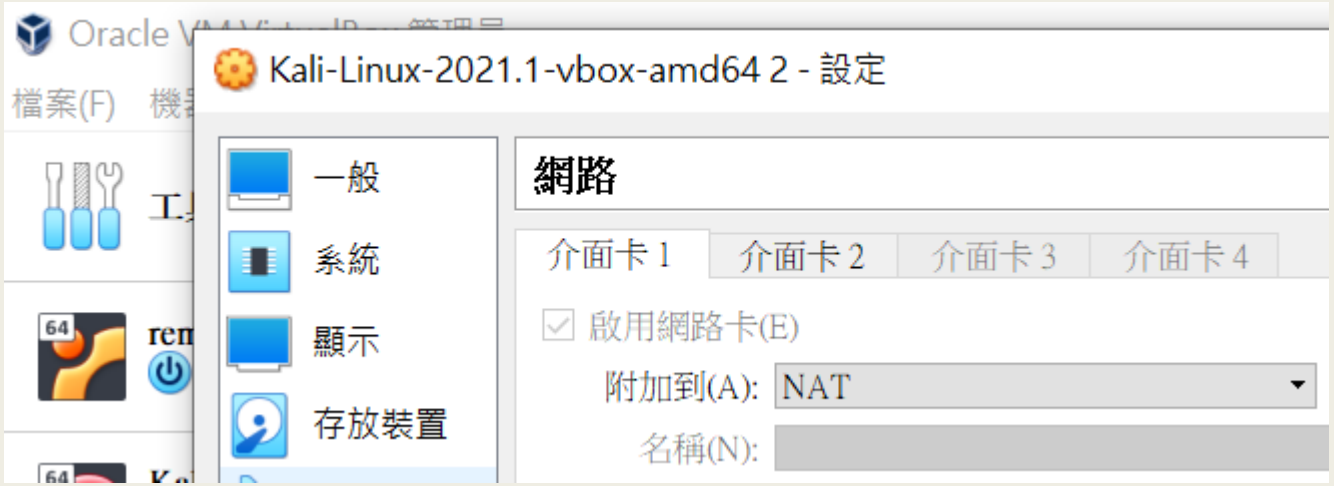
Wazuh – Deploy a new agent on Kali

- Select Debian/Ubuntu

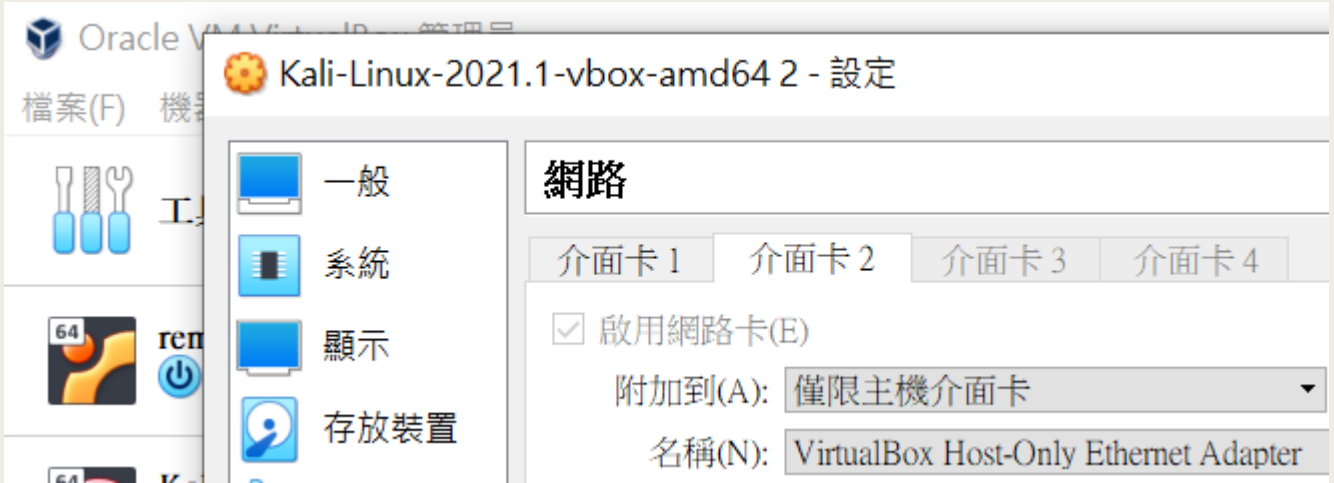


Wazuh – Deploy a new agent

- For downloading Agent



- For connecting to Server



Wazuh - Elastic

https://192.168.56.99/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,valu

Elastic

WAZUH / Agents

STATUS

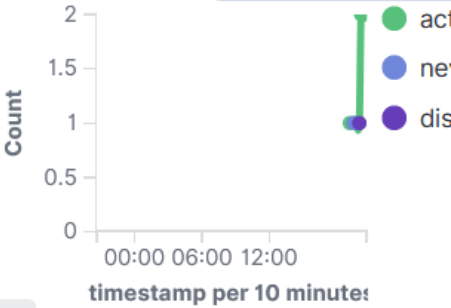
DETAILS

Active	Disconnected	Never connected	Agents coverage
2	1	0	66.67%

Last registered agent: kali

Most active agent: LAPTOP-FVTV10HK

EVOLUTION



Filter or search agent

Agents (3)

Deploy new agent

ID	Name	IP	Group(s)	OS	Cluster node	Versi...	Registration date	Last keep alive	Status
010	WinDev2102Eval	10.0.3.15	default	Microsoft Window...	node01	v4.1.5	May 17, 2021...	May 17, 2021...	disconnected
011	LAPTOP-FVTV10HK	192.168.0.17	default	Microsoft Window...	node01	v4.1.5	May 17, 2021...	May 17, 2021...	active
012	kali	10.0.2.15	default	Kali GNU/Linux 202...	node01	v4.1.5	May 17, 2021...	May 17, 2021...	active

Agent's Information

WAZUH / Agents / LAPTOP-FVTV10HK / Inventory data

LAPTOP-FVTV10HK

Cores: **16** Memory: **23981.59 MB** Arch: **x86_64** OS: **Microsoft Windows 10 Enterprise 10.0.19041** CPU: **AMD Ryzen 7 4800HS with Radeon Graphics** Last scan: **May 19, 2021 @ 23:**

Network interfaces

Name	MAC	State	MTU	Type
Npcap Loopback Adapter	02:00:4C:4F:4F:50	up	65536	ethernet
VirtualBox Host-Only Network	0A:00:27:00:00:0D	up	1500	ethernet
VirtualBox Host-Only Network #2	0A:00:27:00:00:17	up	1500	ethernet
	C8:E2:65:FF:32:60	down	1500	wireless

Network ports

Process	Local IP	Local port	State	Protocol
svchost.exe	0.0.0.0	49666	listening	tcp
svchost.exe	0.0.0.0	49667	listening	tcp
spoolsv.exe	0.0.0.0	49668	listening	tcp
services.exe	0.0.0.0	49674	listening	tcp
PRTG Server.exe	127.0.0.1	80	listening	tcp
Dropbox.exe	127.0.0.1	843	listening	tcp

Network settings

Interface	Address
Npcap Loopback Adapter	169.254.108.226

Packages (193)

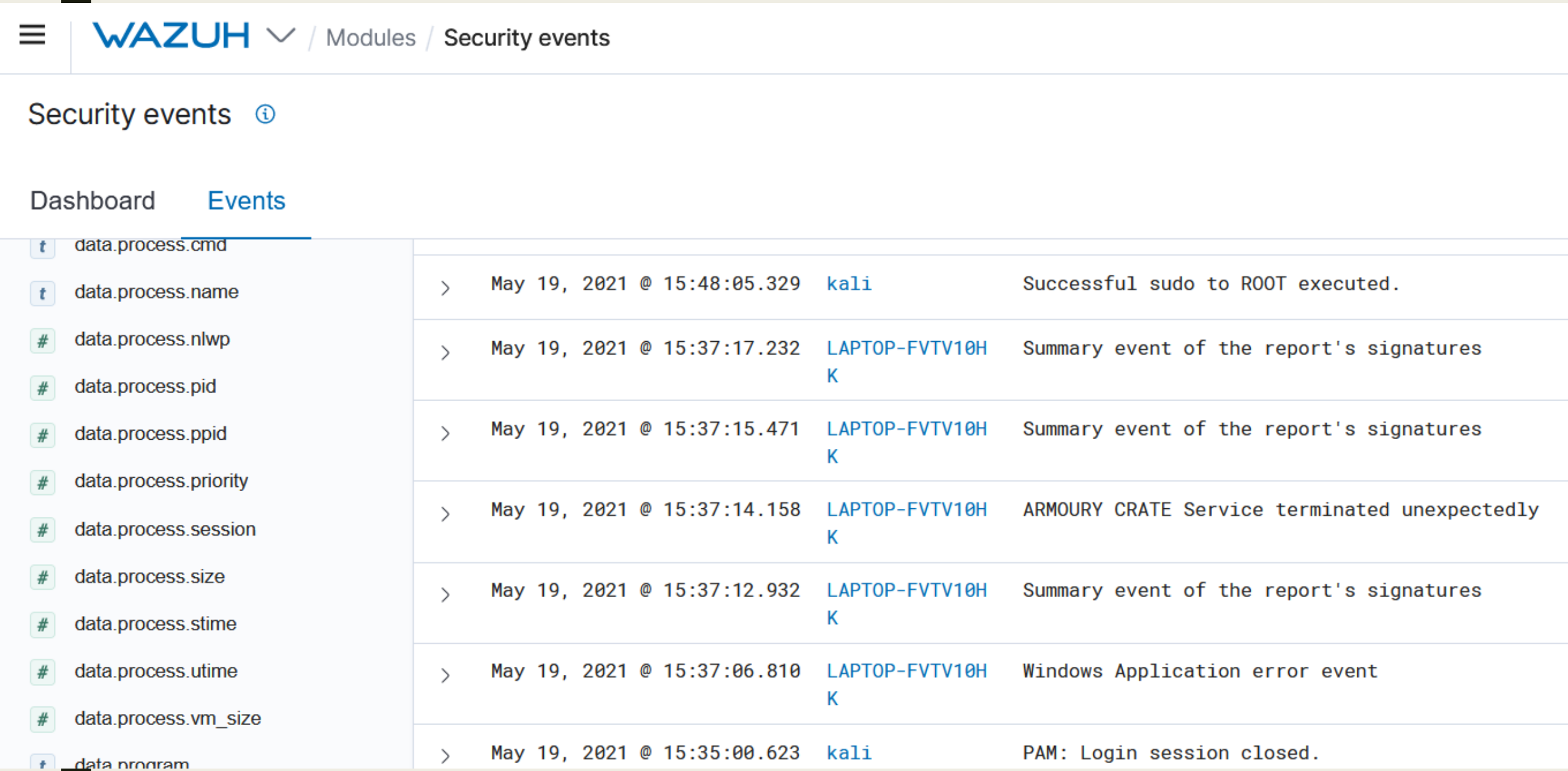
Filter packages...

Name
010 Editor 10.0.2 (64-bit)

Processes (336)

Filter processes...

Name	PID	Parent PID
OfficeClickToRun.exe	5184	1104


WAZUH
Modules
Security events
Security events
Dashboard
Events
data.process.cmd
data.process.name
data.process.nlwp
data.process.pid
data.process.ppid
data.process.priority
data.process.session
data.process.size
data.process.stime
data.process.utime
data.process.vm_size
data.program
May 19, 2021 @ 15:48:05.329 kali Successful sudo to ROOT executed.
May 19, 2021 @ 15:37:17.232 LAPTOP-FVTV10HK Summary event of the report's signatures
May 19, 2021 @ 15:37:15.471 LAPTOP-FVTV10HK Summary event of the report's signatures
May 19, 2021 @ 15:37:14.158 LAPTOP-FVTV10HK ARMOURY CRATE Service terminated unexpectedly
May 19, 2021 @ 15:37:12.932 LAPTOP-FVTV10HK Summary event of the report's signatures
May 19, 2021 @ 15:37:06.810 LAPTOP-FVTV10HK Windows Application error event
May 19, 2021 @ 15:35:00.623 kali PAM: Login session closed.

SURICATA

Open Source IDS / IPS / NSM engine

Suricata – Install on Kali

 # apt -y install epel-release wget jq

 # curl -O https://copr.fedorainfracloud.org/coprs/jasonish/suricata-stable/repo/epel-7/jasonish-suricata-stable-epel-7.repo

 # apt -y install suricata

 # wget https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.tar.gz

 # tar zxvf emerging.rules.tar.gz

 # rm /etc/suricata/rules/ -f*

 # mv rules/.rules /etc/suricata/rules/*

 # rm -f /etc/suricata/suricata.yaml

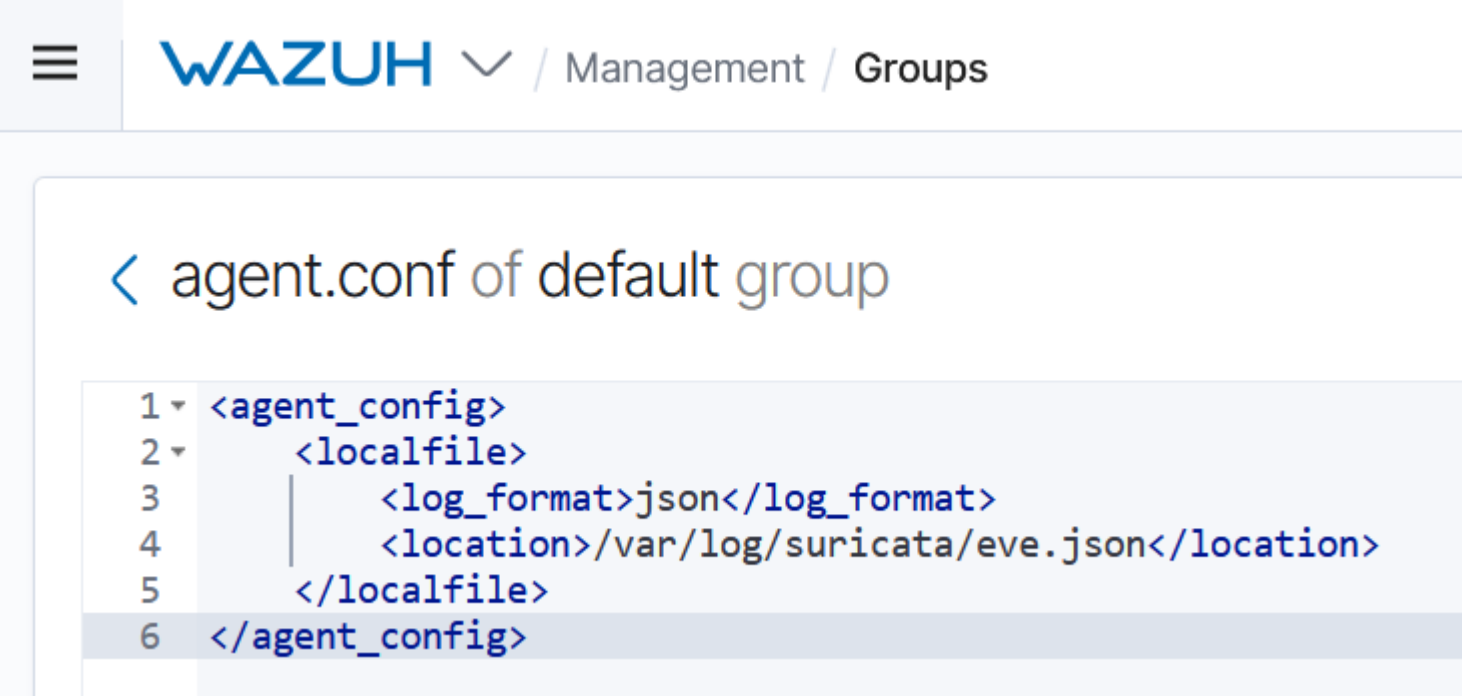
 # sudo wget -O /etc/suricata/suricata.yaml http://www.branchnetconsulting.com/wazuh/suricata.yaml

 # systemctl daemon-reload

 # systemctl enable suricata

 # systemctl start suricata

Configure Wazuh – get log from Suricata

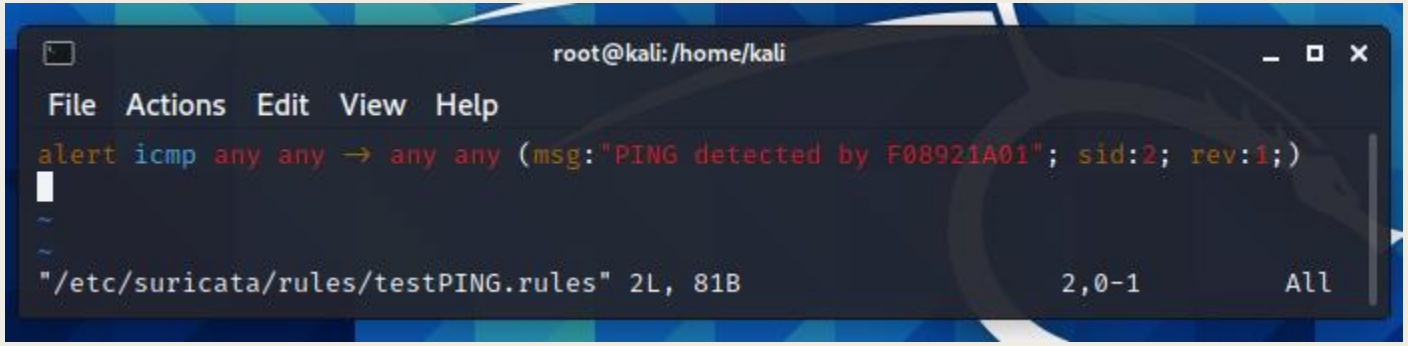



```
<agent_config>
        <localfile>
                <log_format>json</log_format>
                <location>/var/log/suricata/eve.json</location>
        </localfile>
</agent_config>
```

Suricata – Add a custom rule

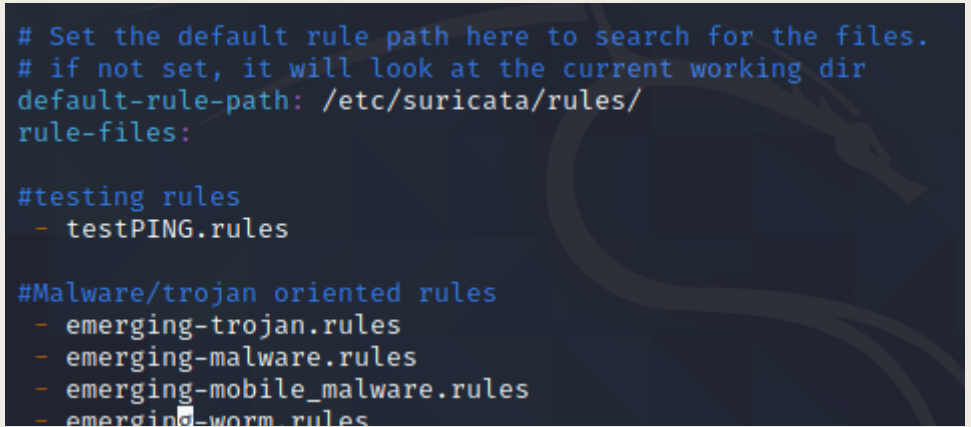
- Add a rule file

  # *echo "alert icmp any any -> any any (msg:"PING detected by F08921A01"; sid:2; rev:1;)" > /etc/suricata/rules/testPING.rules*



- Configuration

  # *vim /etc/suricata/suricata.yaml*



Suricata – Add a custom rule

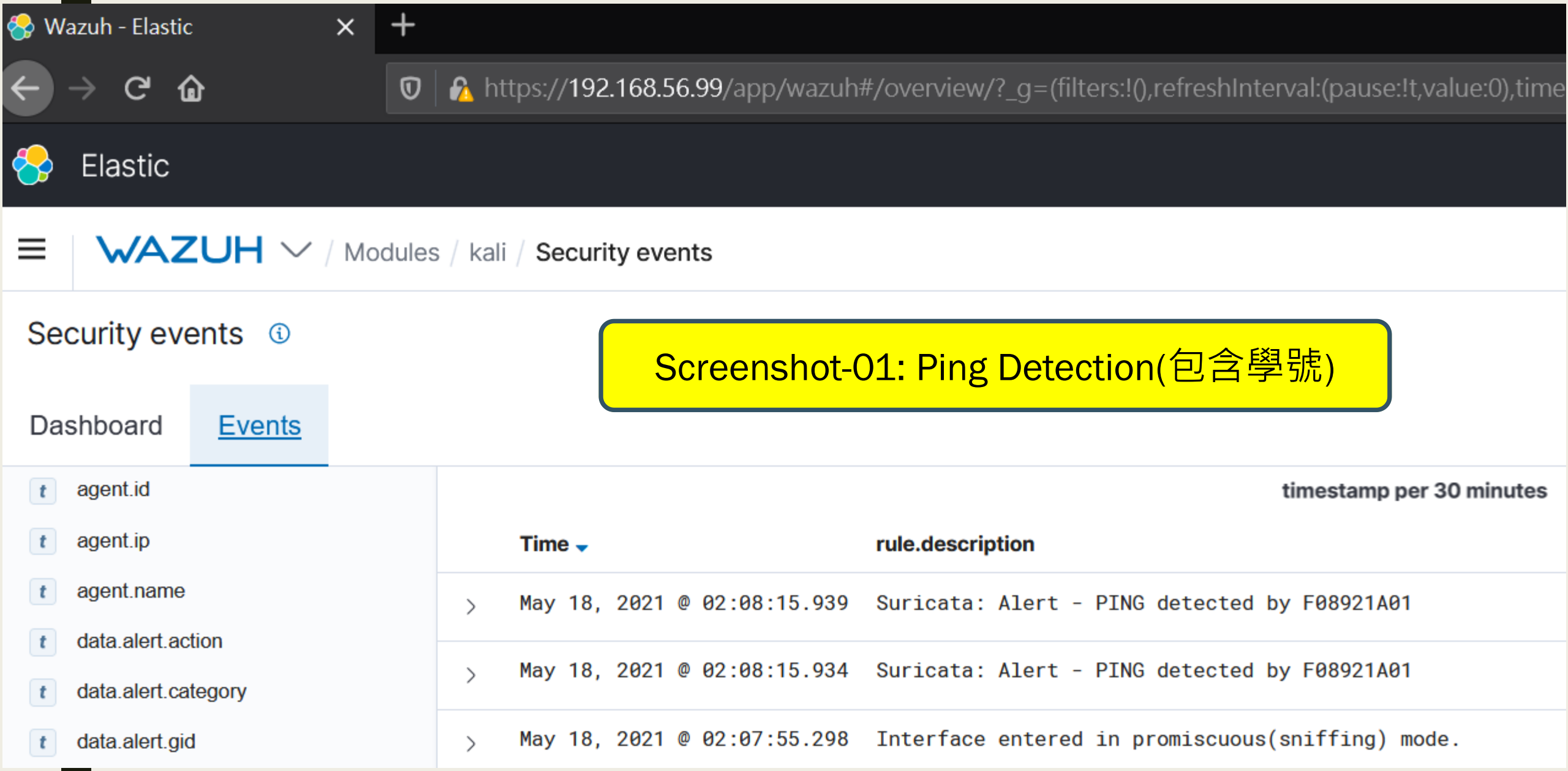
- Restart
  - # *systemctl daemon-reload*
  - # *systemctl enable suricata*
  - # *systemctl start suricata*

Ping Detection

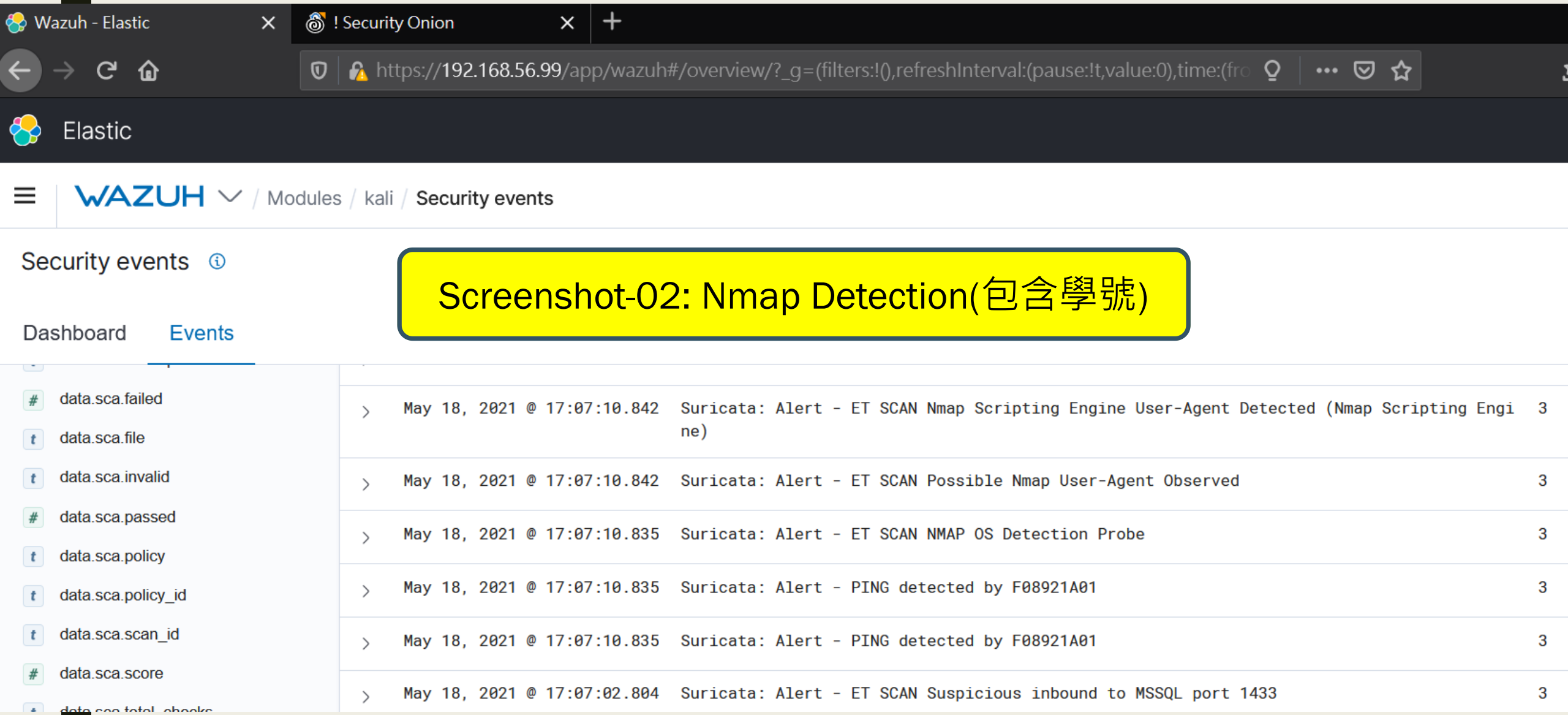
```
C:\Users\yun>ping 192.168.56.111

Ping 192.168.56.111 (使用 32 位元組的資料):
要求等候逾時。
回覆自 192.168.56.111: 位元組=32 時間<1ms TTL=64
回覆自 192.168.56.111: 位元組=32 時間<1ms TTL=64
```

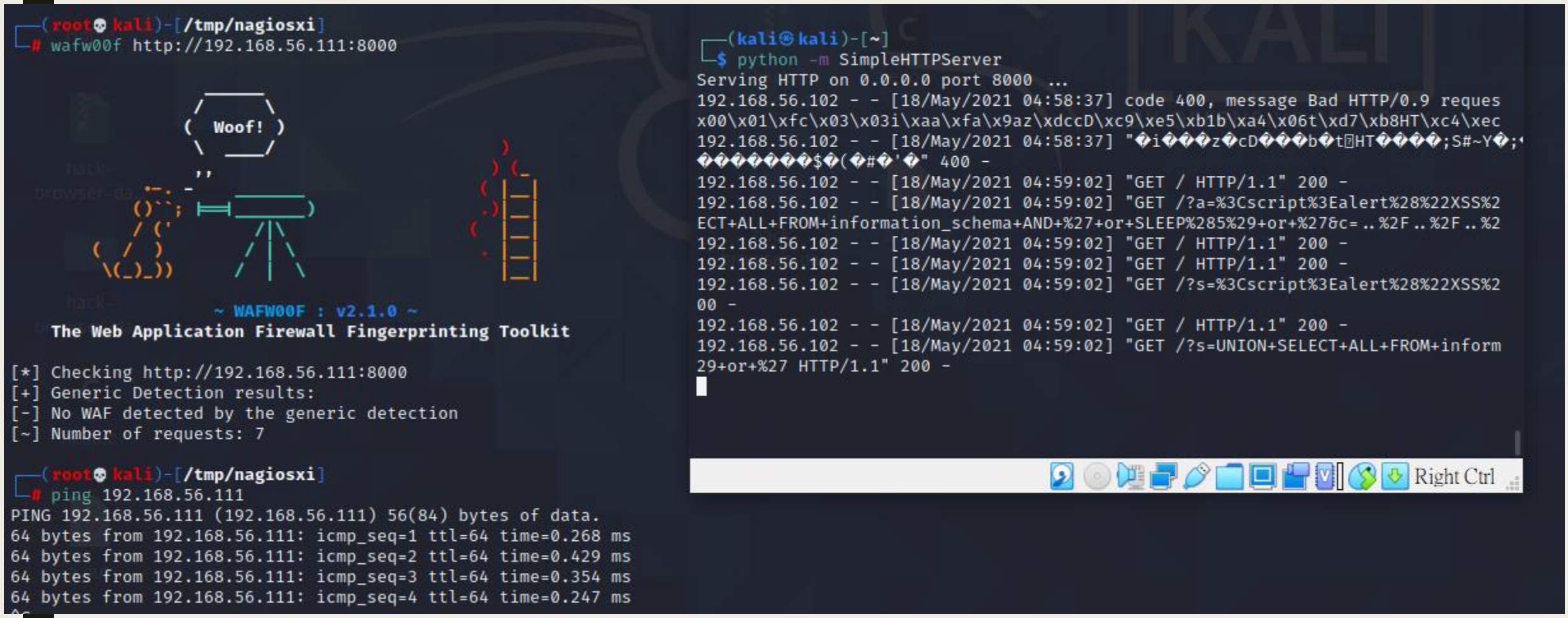
```
┌──(root💀kali)-[/home/kali]
└─# cat /var/log/suricata/eve.json | tail -n 2
{"timestamp":"2021-05-17T14:08:11.838969-0400","flow_id":463816488635705,"in_iface":"eth1","event_type":"alert","src_ip":"192.168.56.1","src_port":0,"dest_ip":"192.168.56.111",
rt":{"action":"allowed","gid":1,"signature_id":2,"rev":1,"signature":"PING detected by F08921A01","category":"","severity":3},"flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes
.838969-0400"}}
{"timestamp":"2021-05-17T14:08:11.839000-0400","flow_id":463816488635705,"in_iface":"eth1","event_type":"alert","src_ip":"192.168.56.111","src_port":0,"dest_ip":"192.168.56.1",
rt":{"action":"allowed","gid":1,"signature_id":2,"rev":1,"signature":"PING detected by F08921A01","category":"","severity":3},"flow":{"pkts_toserver":1,"pkts_toclient":1,"bytes
1.838969-0400"}}
```

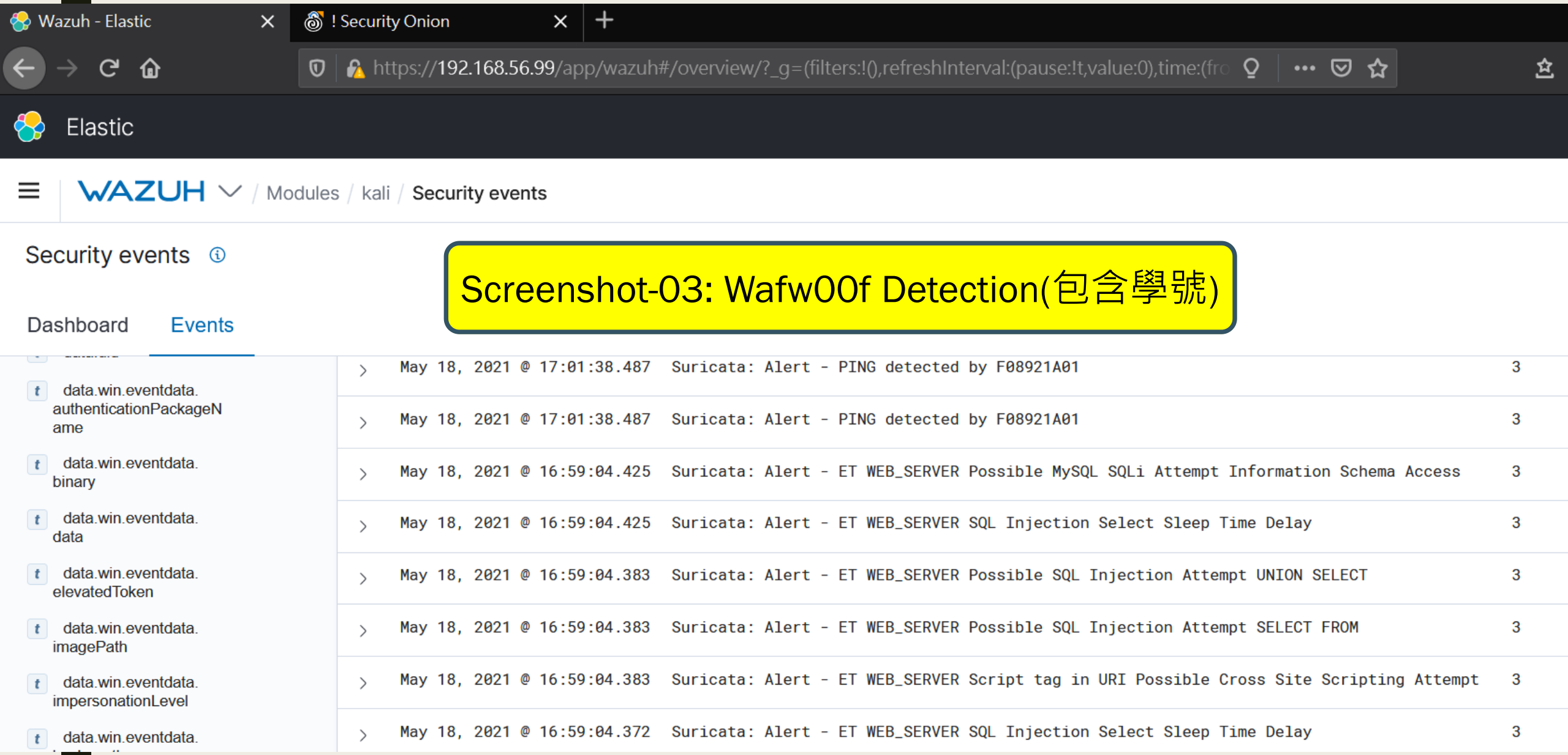

Wazuh - Elastic
https://192.168.56.99/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time
Elastic
WAZUH
Modules
kali
Security events
Security events
Screenshot-01: Ping Detection(包含學號)
Dashboard
Events
agent.id
agent.ip
agent.name
data.alert.action
data.alert.category
data.alert.gid
timestamp per 30 minutes
Time
rule.description
May 18, 2021 @ 02:08:15.939 Suricata: Alert - PING detected by F08921A01
May 18, 2021 @ 02:08:15.934 Suricata: Alert - PING detected by F08921A01
May 18, 2021 @ 02:07:55.298 Interface entered in promiscuous(sniffing) mode.

nmap 192.168.56.111 -A

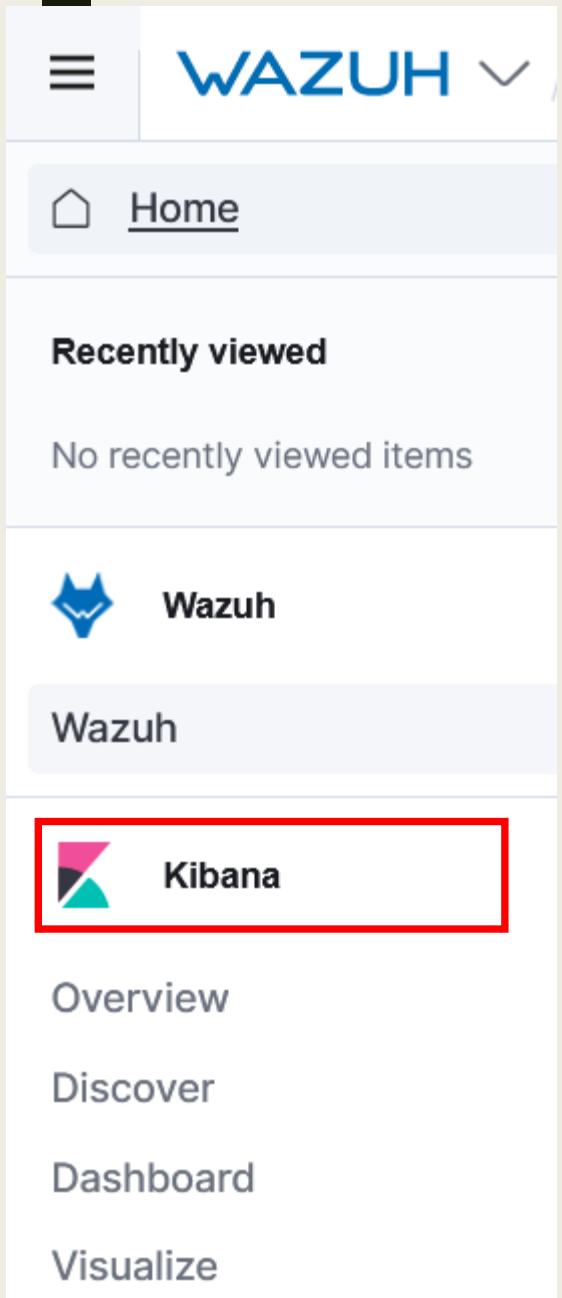


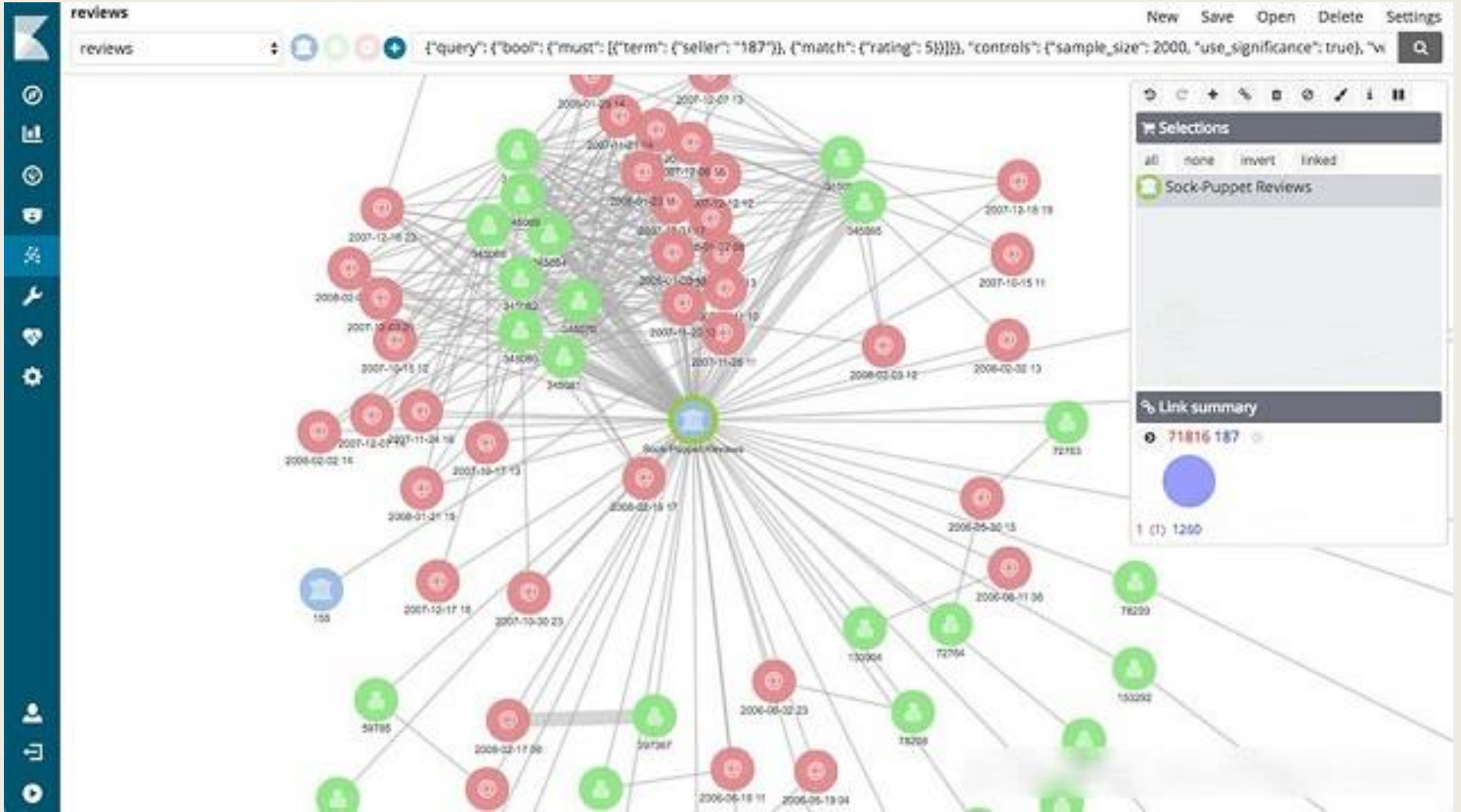
Wafw00f Detection



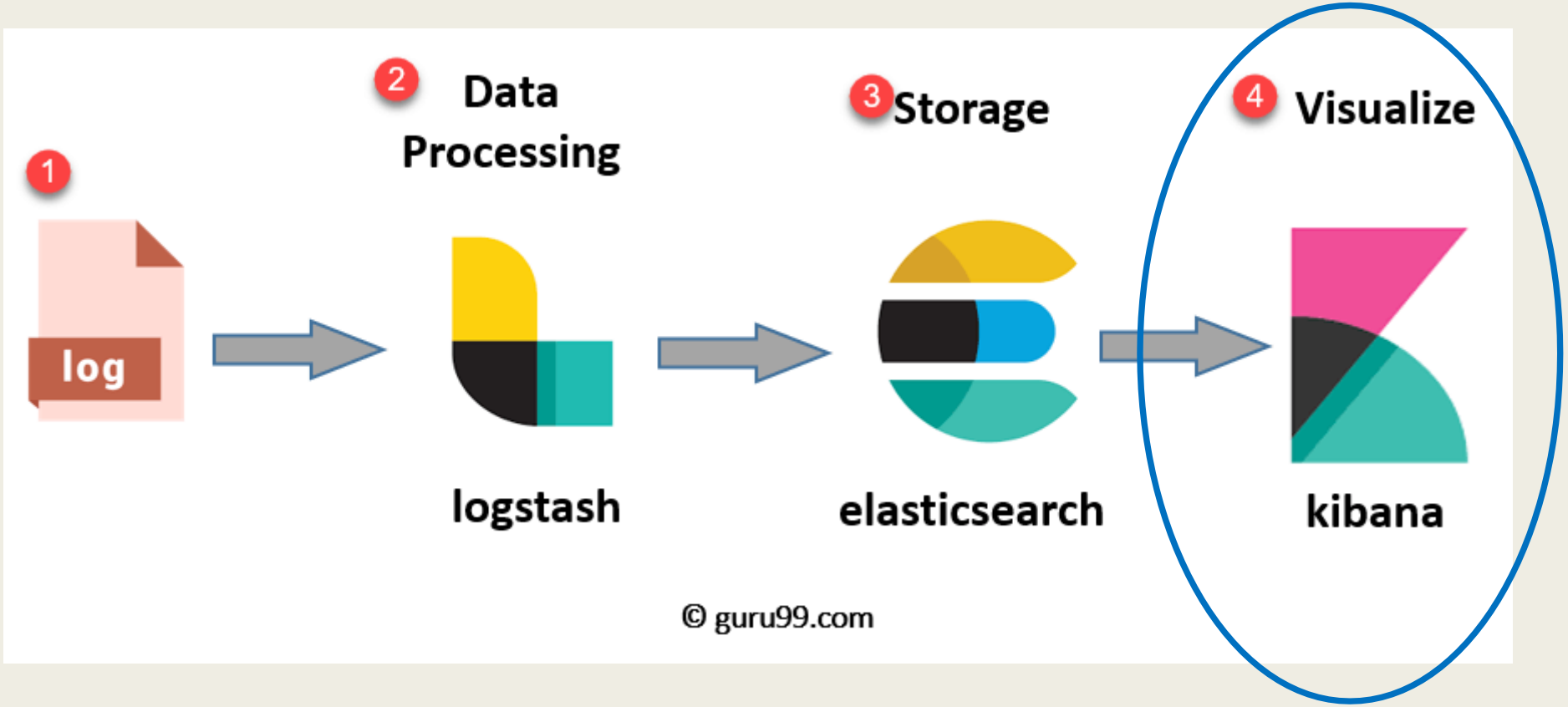

Wazuh - Elastic
! Security Onion
https://192.168.56.99/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(fro
Elastic
WAZUH
Modules / kali / Security events
Security events
Dashboard
Events
Screenshot-03: Wafw00f Detection(包含學號)
data.win.eventdata.authenticationPackageName
data.win.eventdata.binary
data.win.eventdata.data
data.win.eventdata.elevatedToken
data.win.eventdata.imagePath
data.win.eventdata.impersonationLevel
data.win.eventdata.
May 18, 2021 @ 17:01:38.487 Suricata: Alert - PING detected by F08921A01 3
May 18, 2021 @ 17:01:38.487 Suricata: Alert - PING detected by F08921A01 3
May 18, 2021 @ 16:59:04.425 Suricata: Alert - ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access 3
May 18, 2021 @ 16:59:04.425 Suricata: Alert - ET WEB_SERVER SQL Injection Select Sleep Time Delay 3
May 18, 2021 @ 16:59:04.383 Suricata: Alert - ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT 3
May 18, 2021 @ 16:59:04.383 Suricata: Alert - ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM 3
May 18, 2021 @ 16:59:04.383 Suricata: Alert - ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt 3
May 18, 2021 @ 16:59:04.372 Suricata: Alert - ET WEB_SERVER SQL Injection Select Sleep Time Delay 3

Kibana - Data visualization dashboard software for Elasticsearch



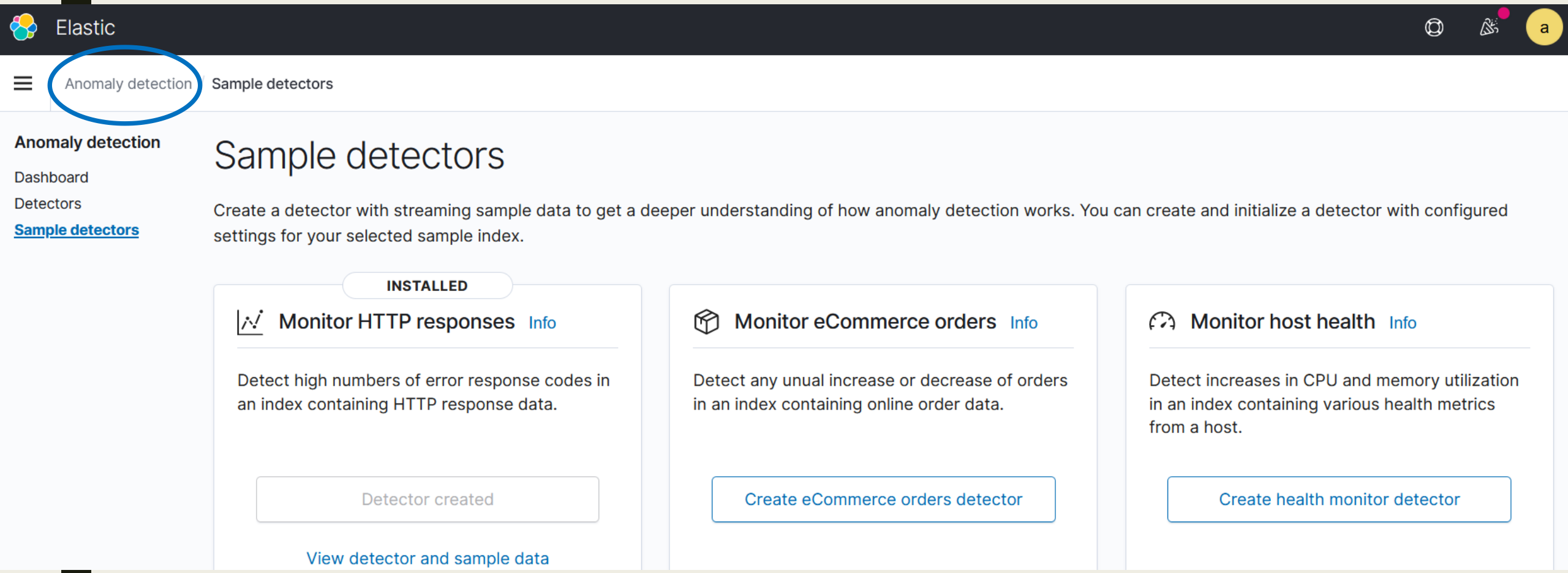


ELK Stack Tutorial: What is Kibana, Logstash & Elasticsearch?



Blue team final project

Blue team final project



Security – Paper 題目實做或延伸

2019 IEEE Symposium on Security and Privacy

HOLMES: Real-time APT Detection through Correlation of Suspicious Information Flows

進階持續性威脅
(Advanced Persistent Threat, APT)

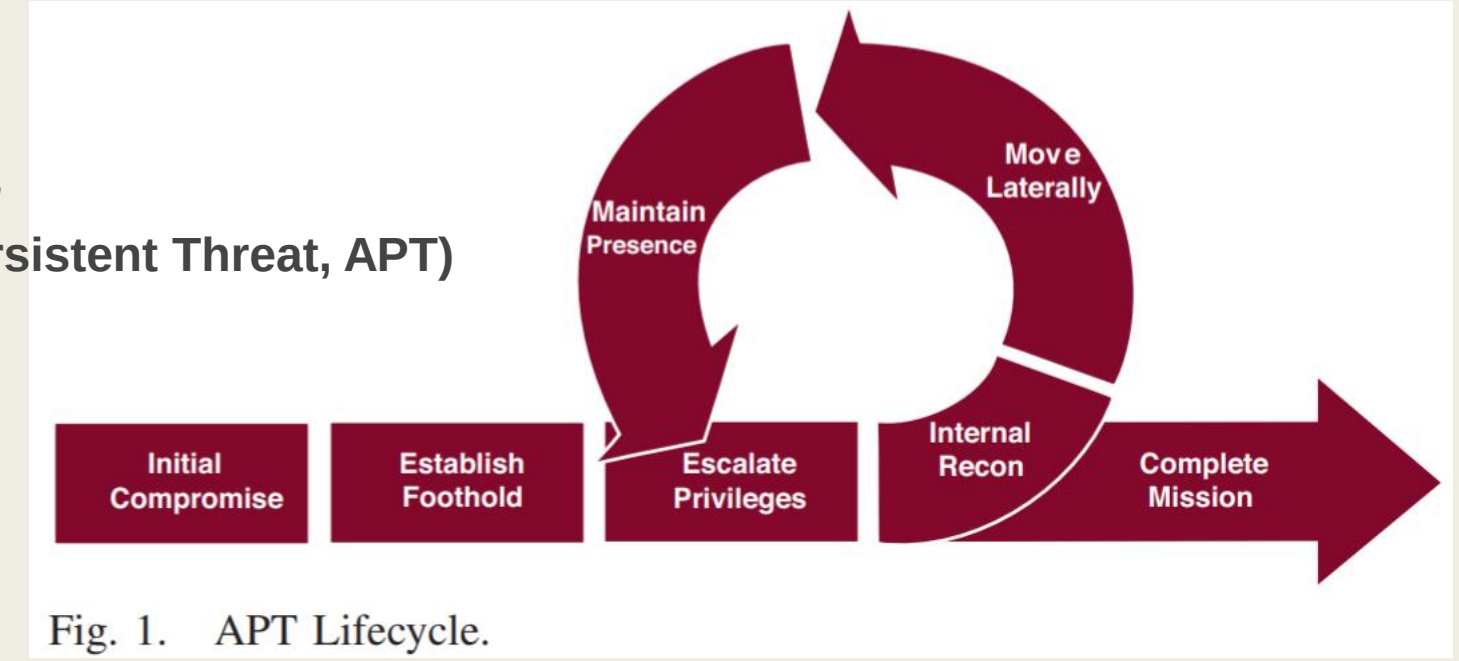


Fig. 1. APT Lifecycle.

APT Detection

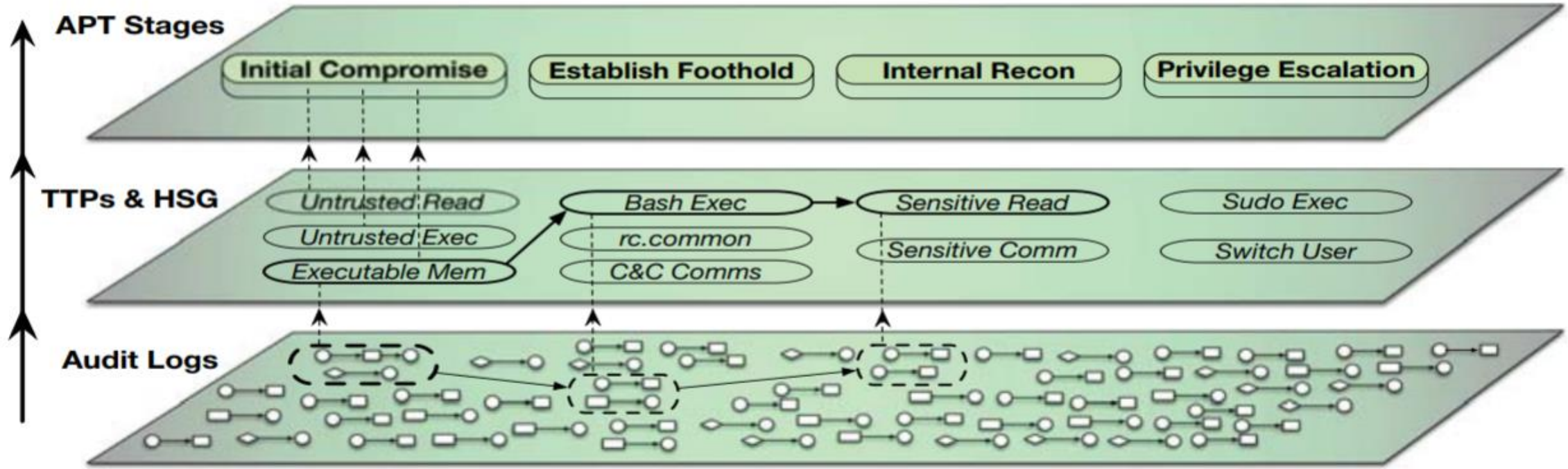


Fig. 3. HOLMES Approach: From Audit Records to High-Level APT Stages

APT Detection

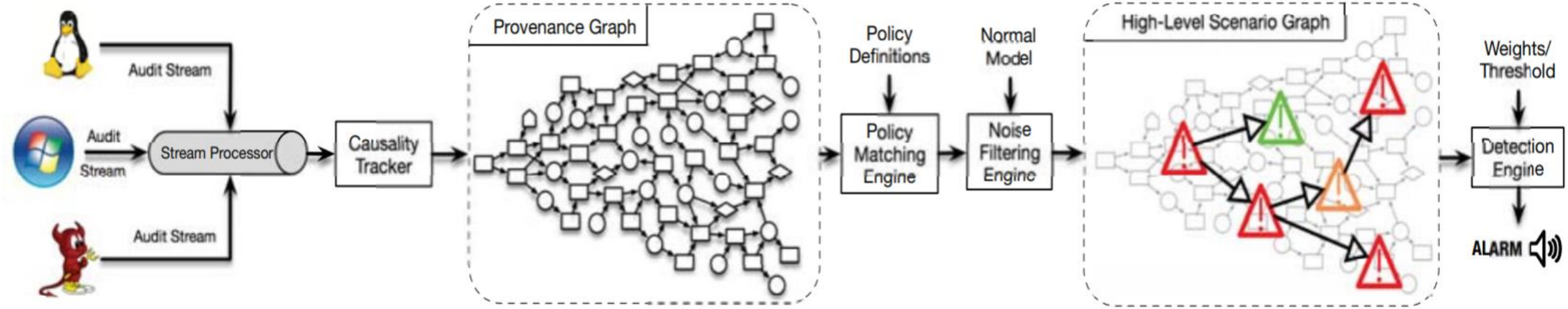
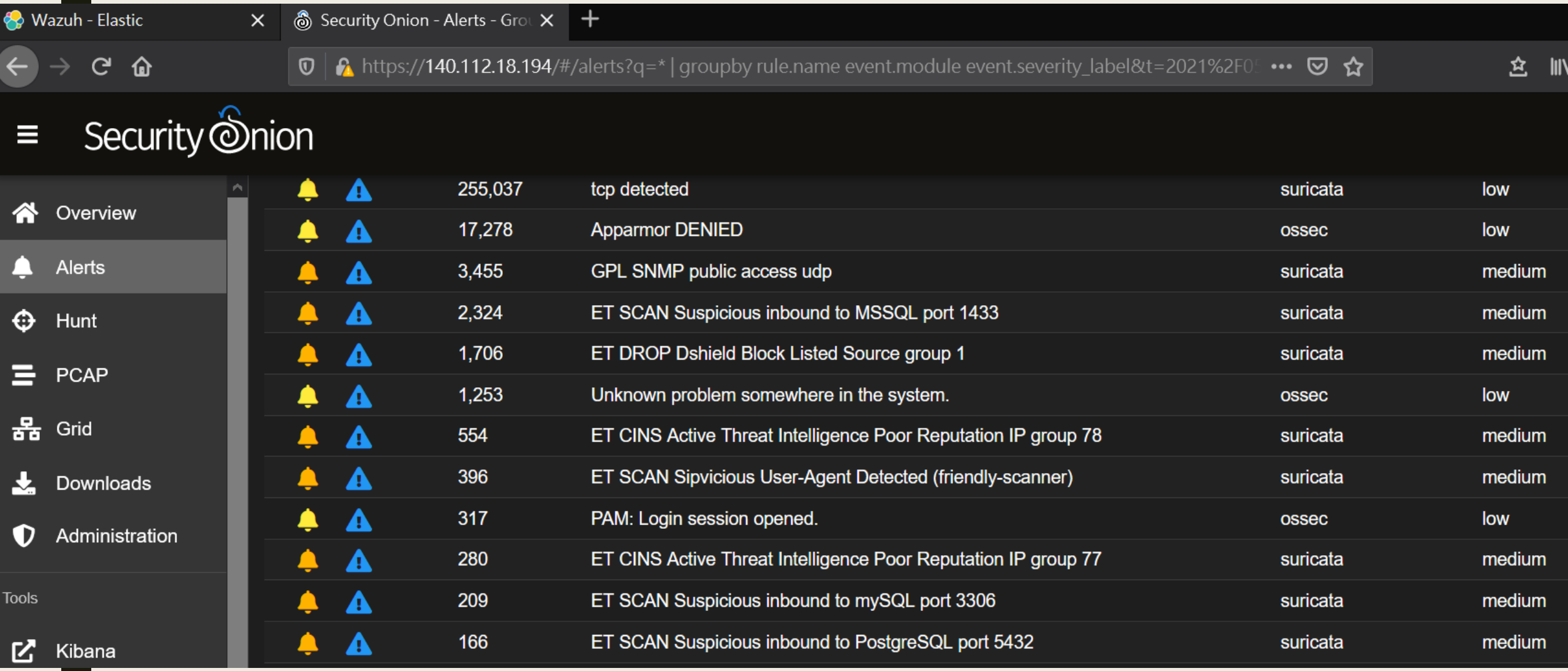


Fig. 6. HOLMES Architecture.

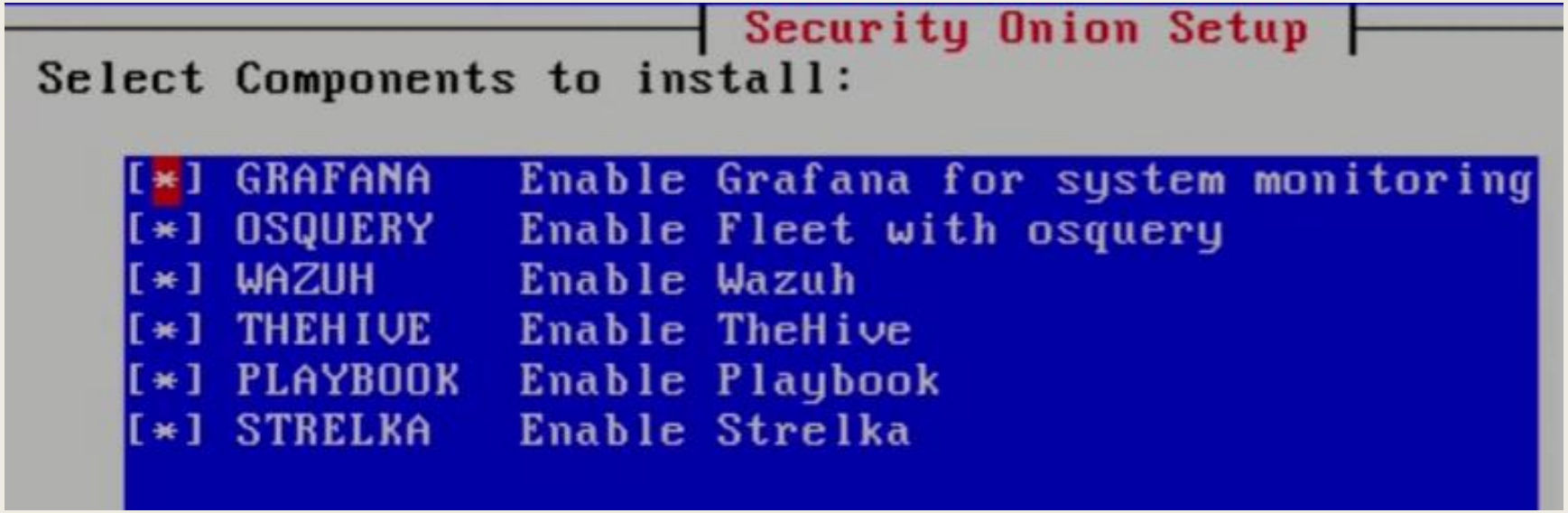
- Host audit data
  - Linux auditd
  - BSD dtrace
  - Windows ETW (Event Tracing for Windows)
- Evaluated HOLMES on data generated by DARPA Transparent Computing program
  - https://github.com/darpa-i2o/Transparent-Computing

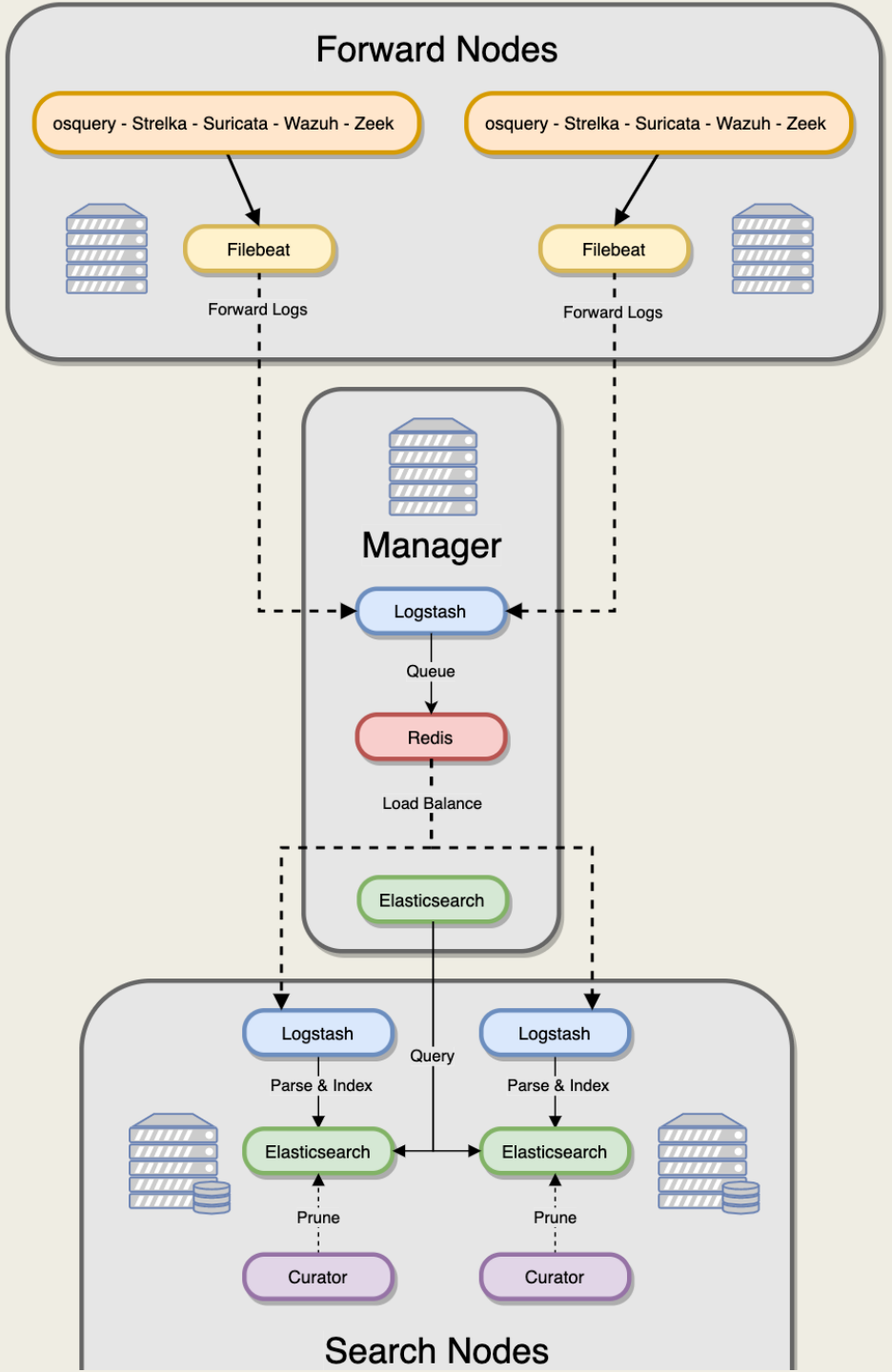

Security Onion

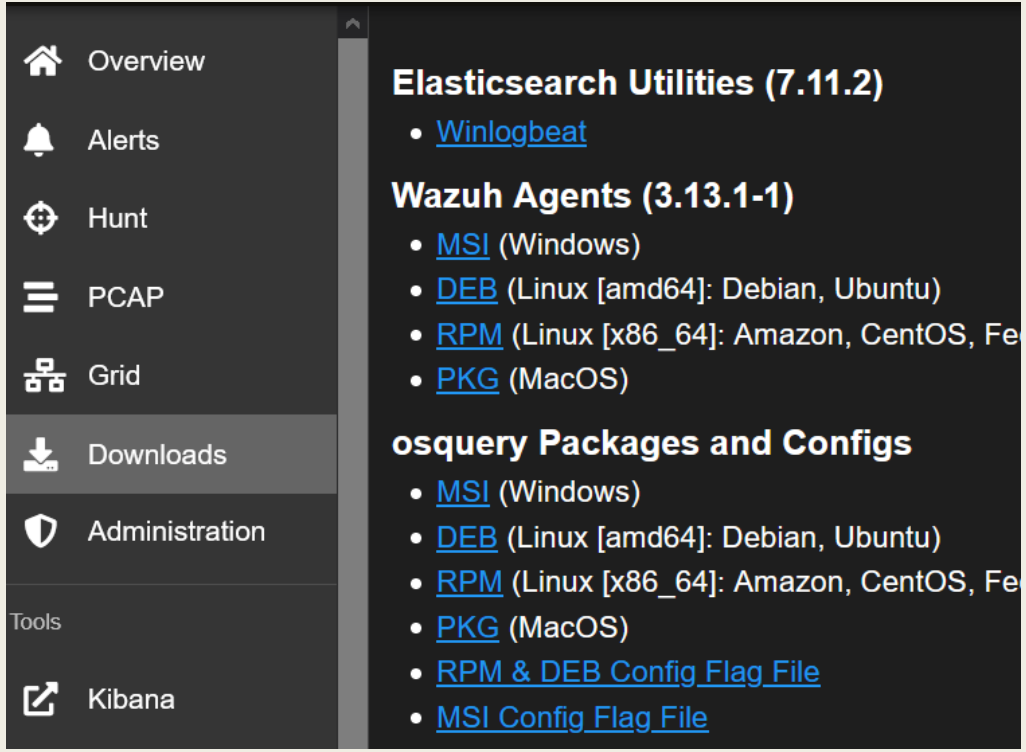
Security Onion – Alerts



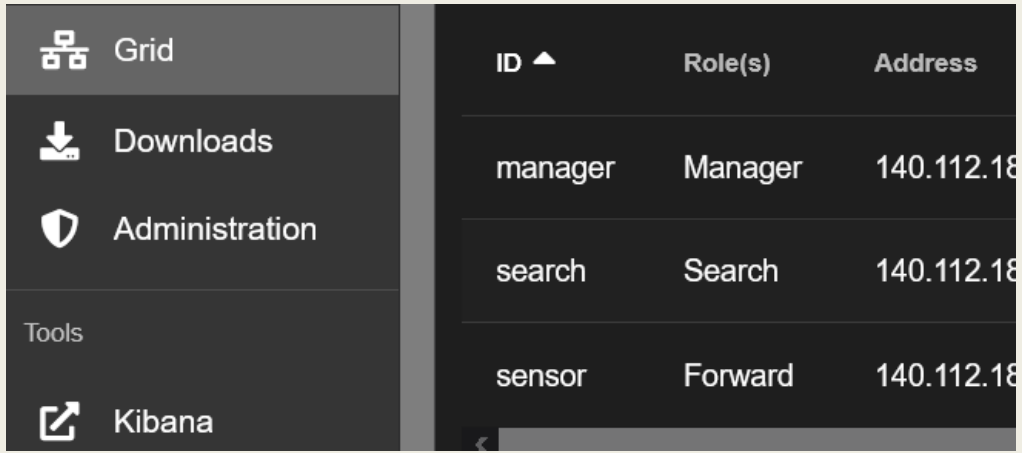
Security “Onion”



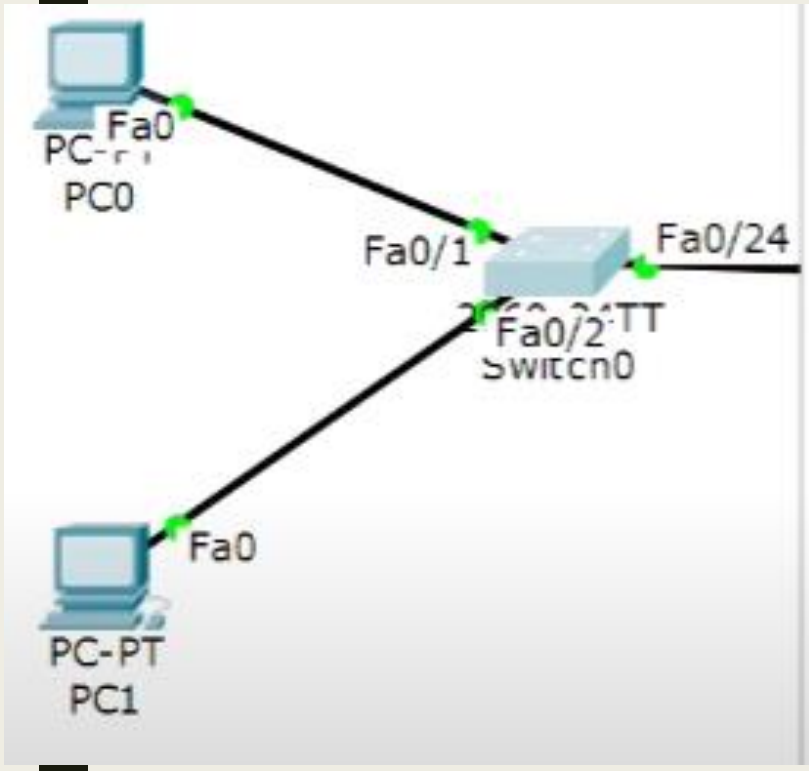




Agent： Install on every host
NIDS： Install on sensors (with Port Mirroring)



Port Mirroring




```
Switch(config)#monitor session 1 destination interface f0/24
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
show
Switch#show mo
Switch#show monitor
Session 1
---------
Type                      : Local Session
Description               : -
Source Ports              :
    Both                  : Fa0/1,Fa0/2
Destination Ports         : Fa0/24
    Encapsulation         : Native
          Ingress         : Disabled
```

HW

- Upload pdf

Screenshot-01: Ping Detection(包含學號)

Screenshot-02: Nmap Detection(包含學號)

Screenshot-03: Wafw00f Detection(包含學號)