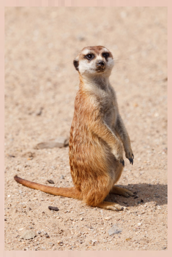
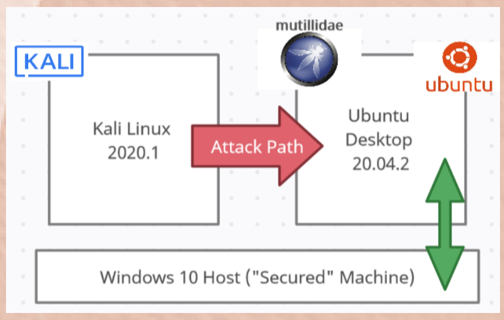


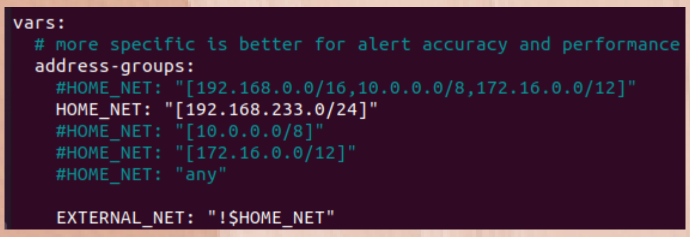
Suricata for Intrusion Detection & Prevention

Usage

- Can be configured as a ***network IDS and/or IPS.***
- Open Source Tool from OISF and competitor to Snort.
- Can perform signature-based malware detection (using ET rules or pcre).
- Can block web-based attacks (SQL Injection, XSS, Directory Traversal etc.).

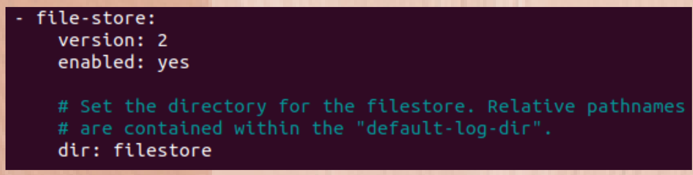


IPS & IDS Mode Configuration



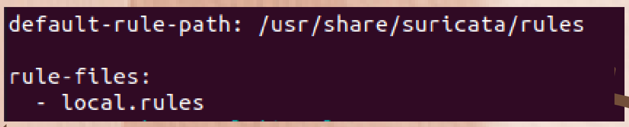
```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    #HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    HOME_NET: "[192.168.233.0/24]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
```

Compile Suricata from Source. Configure HOME_NET to be the IP subnet ID of the NAT Interface.



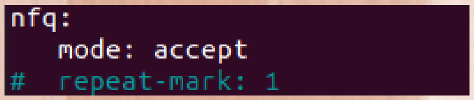
```
- file-store:
    version: 2
    enabled: yes

    # Set the directory for the filestore. Relative pathnames
    # are contained within the "default-log-dir".
    dir: filestore
```

Enable file-store to avoid any errors when running in IDS mode.



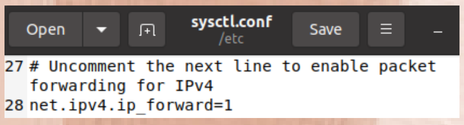
```
default-rule-path: /usr/share/suricata/rules

rule-files:
  - local.rules
```

Create local.rules under /usr/share/local/rules. Change the default path in suricata.yaml.



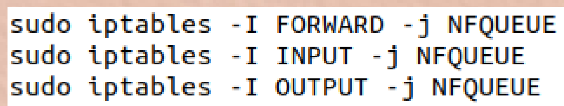
```
nfq:
    mode: accept
#   repeat-mark: 1
```

Enable nfq mode by specifying "accept" for IPS functionality



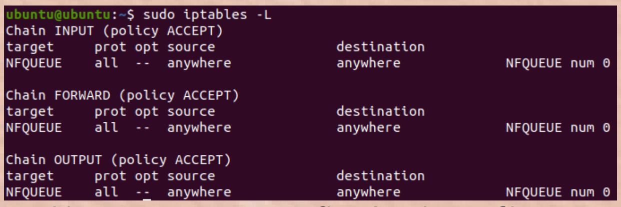
```
# Uncomment the next line to enable packet
 forwarding for IPv4
net.ipv4.ip_forward=1
```

Uncomment this line in /etc/sysctl.conf.



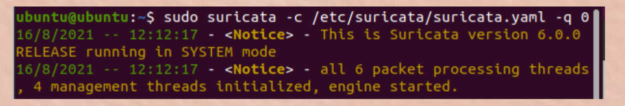
```
sudo iptables -I FORWARD -j NFQUEUE
sudo iptables -I INPUT -j NFQUEUE
sudo iptables -I OUTPUT -j NFQUEUE
```

Run the following commands to allow traffic to be processed by NFQueue.



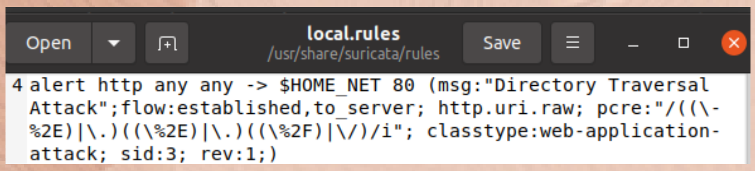
```
ubuntu@ubuntu:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
NFQUEUE    all  --  anywhere             anywhere             NFQUEUE num 0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
NFQUEUE    all  --  anywhere             anywhere             NFQUEUE num 0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
NFQUEUE    all  --  anywhere             anywhere             NFQUEUE num 0
```

We can now run Suricata after this is shown.



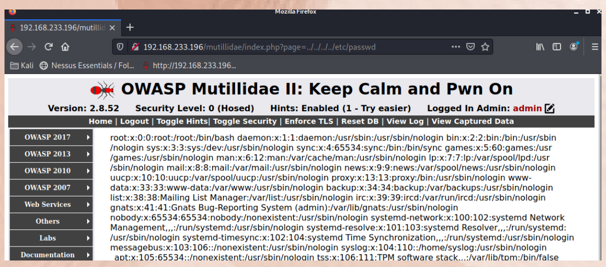
```
ubuntu@ubuntu:~$ sudo suricata -c /etc/suricata/suricata.yaml -q 0
16/8/2021 -- 12:12:17 - <Notice> - This is Suricata version 6.0.0
RELEASE running in SYSTEM mode
16/8/2021 -- 12:12:17 - <Notice> - all 6 packet processing threads
, 4 management threads initialized, engine started.
```

Test 1: Directory Attack (IDS mode)



```
alert http any any -> $HOME_NET 80 (msg:"Directory Traversal
Attack";flow:established,to_server; http.uri.raw; pcre:"/((\-
%2E)|\.)((\%2E)|\.)((\%2F)|\/)/i"; classtype:web-application-
attack; sid:3; rev:1;)
```

Use the following rule to generate an alert for "../" syntax used in directory traversal attacks.



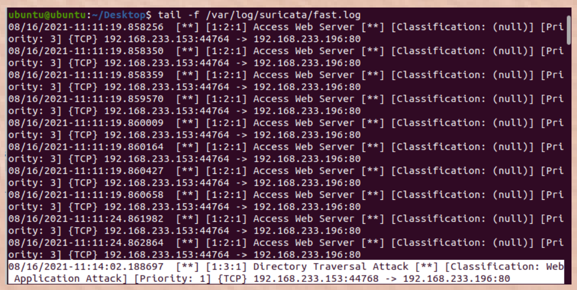
OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.52 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In Admin: admin

Home | Logout | Toggle Hints| Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin messagebus:x:103:106::/nonexistent:/usr/sbin/nologin syslog:x:104:110::/home/syslog:/usr/sbin/nologin apt:x:105:65534::/nonexistent:/usr/sbin/nologin tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false

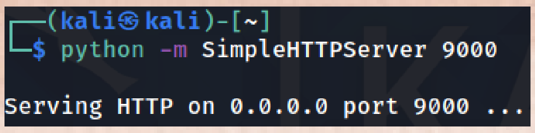
Use Kali Linux to conduct directory traversal by appending "*../../../../etc/passwd*" to the url.



```
ubuntu@ubuntu:~/Desktop$ tail -f /var/log/suricata/fast.log
08/16/2021-11:11:19.858256  [**] [1:2:1] Access Web Server [**] [Classification: (null)] [Pri
ority: 3] {TCP} 192.168.233.153:44764 -> 192.168.233.196:80
08/16/2021-11:11:19.858350  [**] [1:2:1] Access Web Server [**] [Classification: (null)] [Pri
ority: 3] {TCP} 192.168.233.153:44764 -> 192.168.233.196:80
08/16/2021-11:11:19.858359  [**] [1:2:1] Access Web Server [**] [Classification: (null)] [Pri
ority: 3] {TCP} 192.168.233.153:44764 -> 192.168.233.196:80
08/16/2021-11:11:19.859570  [**] [1:2:1] Access Web Server [**] [Classification: (null)] [Pri
ority: 3] {TCP} 192.168.233.153:44764 -> 192.168.233.196:80
08/16/2021-11:11:19.860009  [**] [1:2:1] Access Web Server [**] [Classification: (null)] [Pri
ority: 3] {TCP} 192.168.233.153:44764 -> 192.168.233.196:80
08/16/2021-11:11:19.860164  [**] [1:2:1] Access Web Server [**] [Classification: (null)] [Pri
ority: 3] {TCP} 192.168.233.153:44764 -> 192.168.233.196:80
08/16/2021-11:11:19.860427  [**] [1:2:1] Access Web Server [**] [Classification: (null)] [Pri
ority: 3] {TCP} 192.168.233.153:44764 -> 192.168.233.196:80
08/16/2021-11:11:19.860658  [**] [1:2:1] Access Web Server [**] [Classification: (null)] [Pri
ority: 3] {TCP} 192.168.233.153:44764 -> 192.168.233.196:80
08/16/2021-11:11:24.861982  [**] [1:2:1] Access Web Server [**] [Classification: (null)] [Pri
ority: 3] {TCP} 192.168.233.153:44764 -> 192.168.233.196:80
08/16/2021-11:11:24.862864  [**] [1:2:1] Access Web Server [**] [Classification: (null)] [Pri
ority: 3] {TCP} 192.168.233.153:44764 -> 192.168.233.196:80
08/16/2021-11:14:02.188697  [**] [1:3:1] Directory Traversal Attack [**] [Classification: Web
 Application Attack] [Priority: 1] {TCP} 192.168.233.153:44768 -> 192.168.233.196:80
```

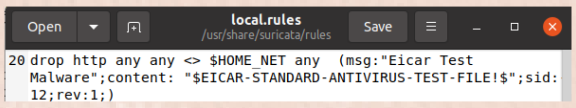
A log entry is created for the attack!

Test 2: EICAR Test Malware (IPS mode)



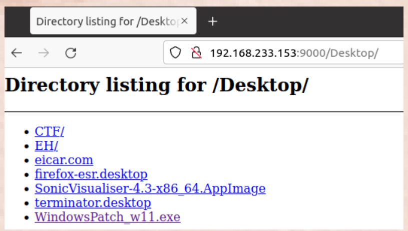
```
┌──(kali㉿kali)-[~]
└─$ python -m SimpleHTTPServer 9000

Serving HTTP on 0.0.0.0 port 9000 ...
```

Download eicar to Desktop and use python to host a simple HTTP server on Kali Linux.



```
drop http any any <> $HOME_NET any  (msg:"Eicar Test
Malware";content: "$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$";sid:
12;rev:1;)
```

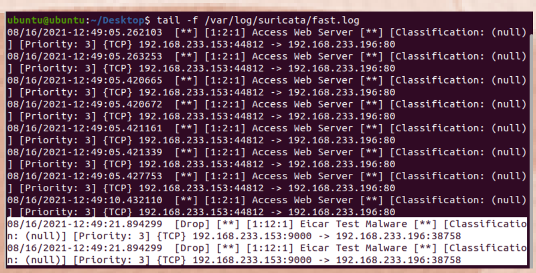
Create a drop rule specifying the signature of eicar (content can be found by opening eicar in a hex editor of choice).



Directory listing for /Desktop/

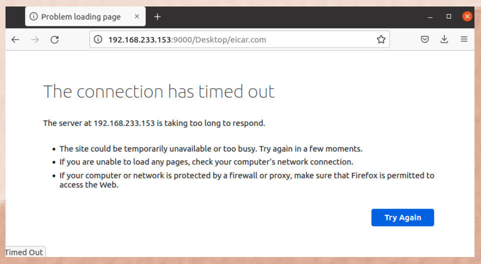
- CTF/
- EH/
- eicar.com
- firefox-esr.desktop
- SonicVisualiser-4.3-x86_64.AppImage
- terminator.desktop
- WindowsPatch_w11.exe

Navigate to the directory after enabling suricata and attempt to download the eicar file.



```
ubuntu@ubuntu:~/Desktop$ tail -f /var/log/suricata/fast.log
08/16/2021-12:49:05.262103  [**] [1:2:1] Access Web Server [**] [Classification: (null)
] [Priority: 3] {TCP} 192.168.233.153:44812 -> 192.168.233.196:80
08/16/2021-12:49:05.263253  [**] [1:2:1] Access Web Server [**] [Classification: (null)
] [Priority: 3] {TCP} 192.168.233.153:44812 -> 192.168.233.196:80
08/16/2021-12:49:05.420665  [**] [1:2:1] Access Web Server [**] [Classification: (null)
] [Priority: 3] {TCP} 192.168.233.153:44812 -> 192.168.233.196:80
08/16/2021-12:49:05.420672  [**] [1:2:1] Access Web Server [**] [Classification: (null)
] [Priority: 3] {TCP} 192.168.233.153:44812 -> 192.168.233.196:80
08/16/2021-12:49:05.421161  [**] [1:2:1] Access Web Server [**] [Classification: (null)
] [Priority: 3] {TCP} 192.168.233.153:44812 -> 192.168.233.196:80
08/16/2021-12:49:05.421339  [**] [1:2:1] Access Web Server [**] [Classification: (null)
] [Priority: 3] {TCP} 192.168.233.153:44812 -> 192.168.233.196:80
08/16/2021-12:49:05.427753  [**] [1:2:1] Access Web Server [**] [Classification: (null)
] [Priority: 3] {TCP} 192.168.233.153:44812 -> 192.168.233.196:80
08/16/2021-12:49:10.432110  [**] [1:2:1] Access Web Server [**] [Classification: (null)
] [Priority: 3] {TCP} 192.168.233.153:44812 -> 192.168.233.196:80
08/16/2021-12:49:21.894299  [Drop] [**] [1:12:1] Eicar Test Malware [**] [Classificatio
n: (null)] [Priority: 3] {TCP} 192.168.233.153:9000 -> 192.168.233.196:38758
08/16/2021-12:49:21.894299  [Drop] [**] [1:12:1] Eicar Test Malware [**] [Classificatio
n: (null)] [Priority: 3] {TCP} 192.168.233.153:9000 -> 192.168.233.196:38758
```

Drop Log Entries created; the source port being that of the http server (9000).



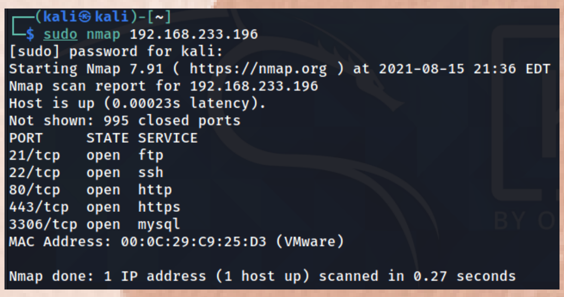
The connection has timed out

The server at 192.168.233.153 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

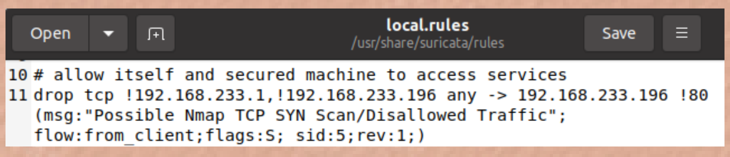
The fle cannot be downloaded and the browser times out.

Test 3: Nmap Partial "Masking" (IPS mode)



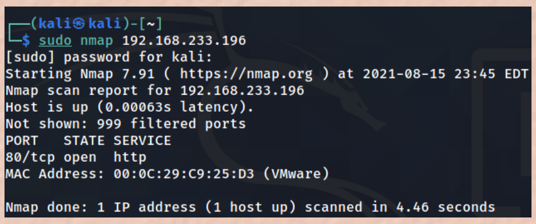
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.233.196
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-15 21:36 EDT
Nmap scan report for 192.168.233.196
Host is up (0.00023s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 00:0C:29:C9:25:D3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Perform an Nmap Scan before enabling Suricata.



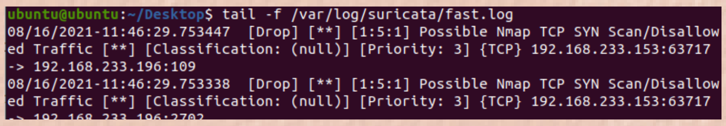
```
# allow itself and secured machine to access services
drop tcp !192.168.233.1,!192.168.233.196 any -> 192.168.233.196 !80
(msg:"Possible Nmap TCP SYN Scan/Disallowed Traffic";
flow:from_client;flags:S; sid:5;rev:1;)
```

Create a drop rule to deny access to tcp-based ports other than 80/tcp (except for the ubuntu box itself and the "secured" machine or WSL on the host).



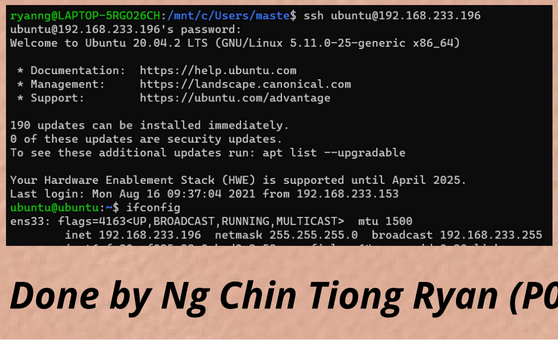
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.233.196
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-15 23:45 EDT
Nmap scan report for 192.168.233.196
Host is up (0.00063s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:C9:25:D3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
```

Perform another Nmap Scan after enabling suricata. Only port 80 will appear on the results.



```
ubuntu@ubuntu:~/Desktop$ tail -f /var/log/suricata/fast.log
08/16/2021-11:46:29.753447  [Drop] [**] [1:5:1] Possible Nmap TCP SYN Scan/Disallow
ed Traffic [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.233.153:63717
-> 192.168.233.196:109
08/16/2021-11:46:29.753338  [Drop] [**] [1:5:1] Possible Nmap TCP SYN Scan/Disallow
ed Traffic [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.233.153:63717
-> 192.168.233.196:2702
```

Log entries are created for the drop action.



```
ryanng@LAPTOP-5RGO26CH:/mnt/c/Users/maste$ ssh ubuntu@192.168.233.196
ubuntu@192.168.233.196's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.11.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

190 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Aug 16 09:37:04 2021 from 192.168.233.153
ubuntu@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.233.196  netmask 255.255.255.0  broadcast 192.168.233.255
```

SSH access/Nmap scan would still be allowed for the "secured" machine and no logs will be created when this action is performed.

-- Done by Ng Chin Tiong Ryan (P03) // S10196904C --