Date :

7A KEEPING SNORT UP TO DATE

Page No. : 22

Expt. No. : 7A

Aim

To Maintain snort IDS tool Detection capablity by adding Rules

Procedure

1) Open local.rules (located inside Snort rules directory)

2) Configure snort for the following rule actions

Alert : Generate an alert using selected alert method and log the packet.

Log: Log the packet.

Pass: Ignore the packet.

Activate: Alert and then turn on another dynamic rule

3) Once the rules are customized, according to above rule patterns Save the file.

Execute the Command

```
Snort -i <Interface Index> -c <Conf file path> -A Console
```

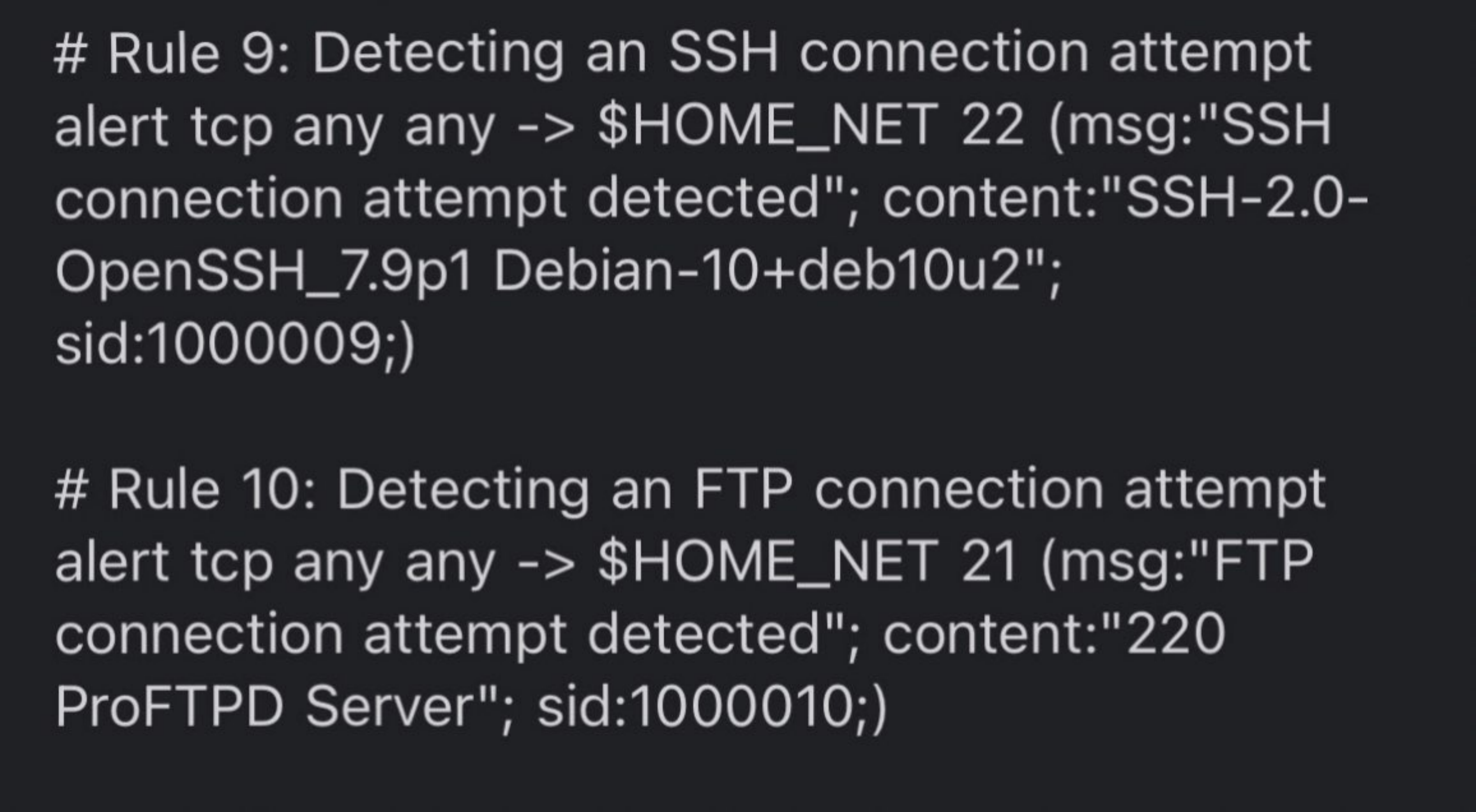
Result

Thus we have analysed & implemented Custom rules for maintaining Intrusion detection in Snort

Teacher's Signature:

23:30
5G 64
PAIDIPALLI SIRI

```
# Rule 1: Detect a port scan
alert tcp any any -> any 1:1024 (flags: S; msg:"Port
scan detected"; sid:1000001;)

# Rule 2: Detect a ping scan
alert icmp any any -> any any (icmp-type:8;
msg:"Ping sweep detected"; sid:1000002;)

# Rule 3: Detect a SYN flood attack
alert tcp any any -> $HOME_NET any (flags:S;
threshold: type both, track by_src, count 10,
seconds 60; msg:"SYN flood detected";
sid:1000003;)

# Rule 4: Detecting a buffer overflow attack
alert tcp any any -> $HOME_NET 80 (msg:"Buffer
overflow attack detected"; content:"|90 90 90
90|"; offset:0; depth:4; sid:1000004;)

# Rule 5: Detecting a SQL injection attack
alert tcp any any -> $HOME_NET 80 (msg:"SQL
injection attack detected"; content:"' or '1'='1";
sid:1000005;)

# Rule 6: Detecting a cross-site scripting attack
alert tcp any any -> $HOME_NET 80 (msg:"Cross-
site scripting attack detected"; content:"<script>";
sid:1000006;)

# Rule 7: Detecting a directory traversal attack
alert tcp any any -> $HOME_NET 80
(msg:"Directory traversal attack detected";
content:"../.."; sid:1000007;)

# Rule 8: Detecting a brute force attack
alert tcp any any -> $HOME_NET 22 (msg:"Brute
force attack detected"; content:"Failed password
for root from"; sid:1000008;)
```



```
# Rule 9: Detecting an SSH connection attempt
alert tcp any any -> $HOME_NET 22 (msg:"SSH
connection attempt detected"; content:"SSH-2.0-
OpenSSH_7.9p1 Debian-10+deb10u2";
sid:1000009;)

# Rule 10: Detecting an FTP connection attempt
alert tcp any any -> $HOME_NET 21 (msg:"FTP
connection attempt detected"; content:"220
ProFTPD Server"; sid:1000010;)
```

Date :

E7B Subtask Defeating Malware - Rootkit Hunter

Page No. : 23
Expt. No. : 7B

Aim

To detect Rootkit (stealth malware which hides and has privelage access) and manage it

Procedure

1) Download Rootkit tool from GMER.net

2) The tool displays process, modules, service files, registry, Rootkey, Malwares autostart, cmd of local host

3) Process menu, kill unwanted process if any exists.
Various system files exist like, .dll .sys and so on

4) Service menu displays entire service like autostart, enable, disable, sys etc

5) Registry contains HKEY of current & local user
Rootkey/Malwares scans the local drive selected

6) Autostart displays registry base autostart application
CMD allows the user to interact with Registry/Command Line utilities

Result

PTO →

Teacher's Signature: