Network Security Lab (CY-331)

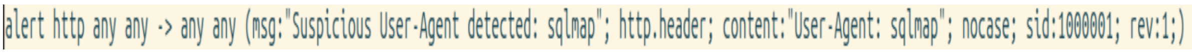
Suricata Lab

Name: Rooshan Riaz

Reg No: 2022506

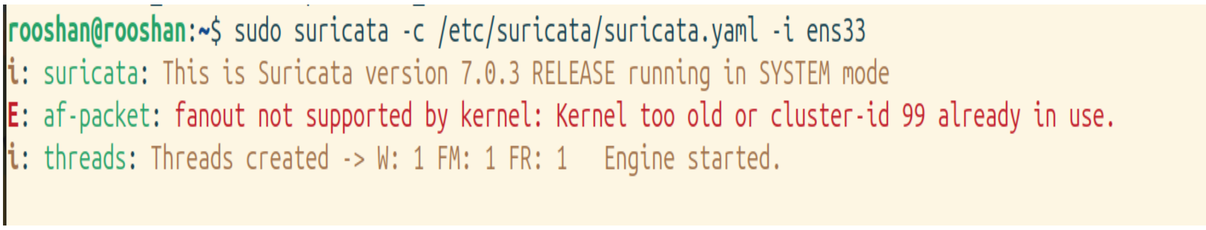
Task 1:

Adding rule to detect the sqlmap User-Agent string



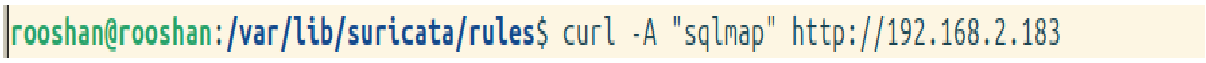
```
alert http any any -> any any (msg:"Suspicious User-Agent detected: sqlmap"; http.header; content:"User-Agent: sqlmap"; nocase; sid:1000001; rev:1;)
```

After saving the rule, reloading Suricata to apply it



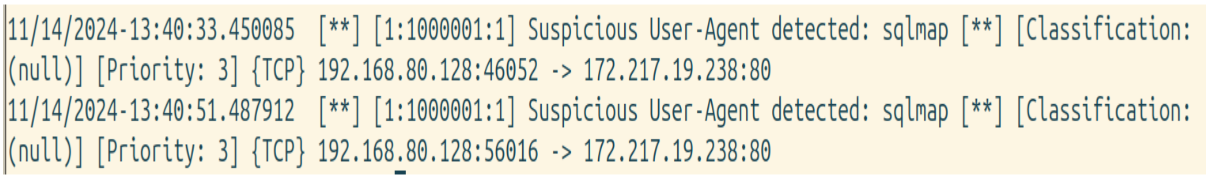
```
rooshan@rooshan:~$ sudo suricata -c /etc/suricata/suricata.yaml -i ens33
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
E: af-packet: fanout not supported by kernel: Kernel too old or cluster-id 99 already in use.
i: threads: Threads created -> W: 1 FM: 1 FR: 1   Engine started.
```

Using curl to simulate HTTP requests with the "sqlmap" User-Agent string



```
rooshan@rooshan:/var/lib/suricata/rules$ curl -A "sqlmap" http://192.168.2.183
```

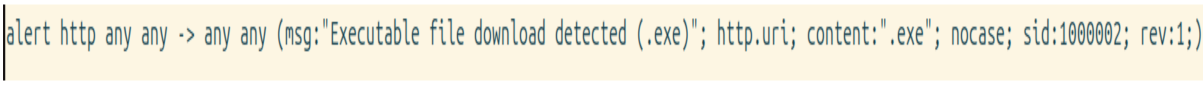
Checking Suricata's alert log to confirm the detection



```
11/14/2024-13:40:33.450085  [**] [1:1000001:1] Suspicious User-Agent detected: sqlmap [**] [Classification:
(null)] [Priority: 3] {TCP} 192.168.80.128:46052 -> 172.217.19.238:80
11/14/2024-13:40:51.487912  [**] [1:1000001:1] Suspicious User-Agent detected: sqlmap [**] [Classification:
(null)] [Priority: 3] {TCP} 192.168.80.128:56016 -> 172.217.19.238:80
```

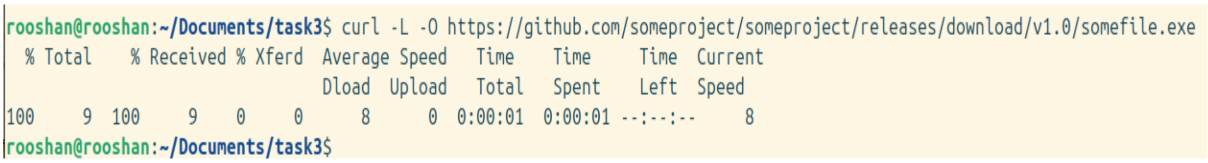
Task 2:

Adding the rule to detect .exe file downloads



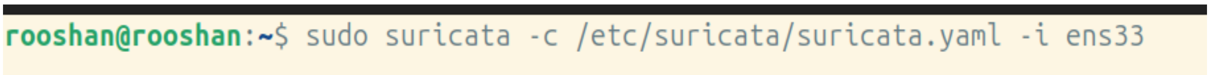
```
alert http any any -> any any (msg:"Executable file download detected (.exe)"; http.uri; content:".exe"; nocase; sid:1000002; rev:1;)
```

Downloading a .exe file using curl



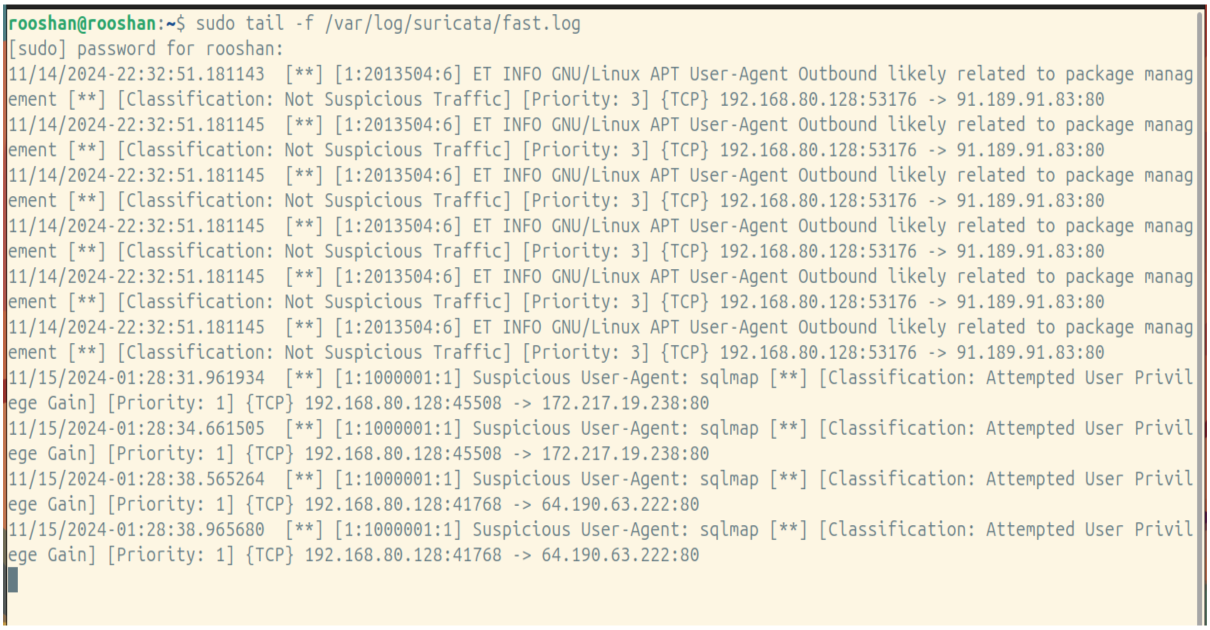
```
rooshan@rooshan:~/Documents/task3$ curl -L -O https://github.com/someproject/someproject/releases/download/v1.0/somefile.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100     9  100     9    0     0      8      0  0:00:01  0:00:01 --:--:--     8
rooshan@rooshan:~/Documents/task3$
```

Loading suricata to apply the rule



```
rooshan@rooshan:~$ sudo suricata -c /etc/suricata/suricata.yaml -i ens33
```

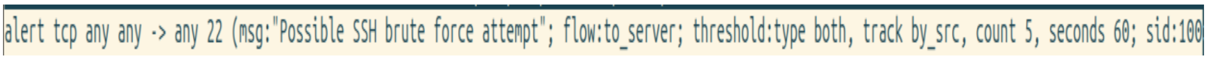
Logs



```
rooshan@rooshan:~$ sudo tail -f /var/log/suricata/fast.log
[sudo] password for rooshan:
11/14/2024-22:32:51.181143  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/14/2024-22:32:51.181145  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/14/2024-22:32:51.181145  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/14/2024-22:32:51.181145  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/14/2024-22:32:51.181145  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/14/2024-22:32:51.181145  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/15/2024-01:28:31.961934  [**] [1:1000001:1] Suspicious User-Agent: sqlmap [**] [Classification: Attempted User Privil
ege Gain] [Priority: 1] {TCP} 192.168.80.128:45508 -> 172.217.19.238:80
11/15/2024-01:28:34.661505  [**] [1:1000001:1] Suspicious User-Agent: sqlmap [**] [Classification: Attempted User Privil
ege Gain] [Priority: 1] {TCP} 192.168.80.128:45508 -> 172.217.19.238:80
11/15/2024-01:28:38.565264  [**] [1:1000001:1] Suspicious User-Agent: sqlmap [**] [Classification: Attempted User Privil
ege Gain] [Priority: 1] {TCP} 192.168.80.128:41768 -> 64.190.63.222:80
11/15/2024-01:28:38.965680  [**] [1:1000001:1] Suspicious User-Agent: sqlmap [**] [Classification: Attempted User Privil
ege Gain] [Priority: 1] {TCP} 192.168.80.128:41768 -> 64.190.63.222:80
```

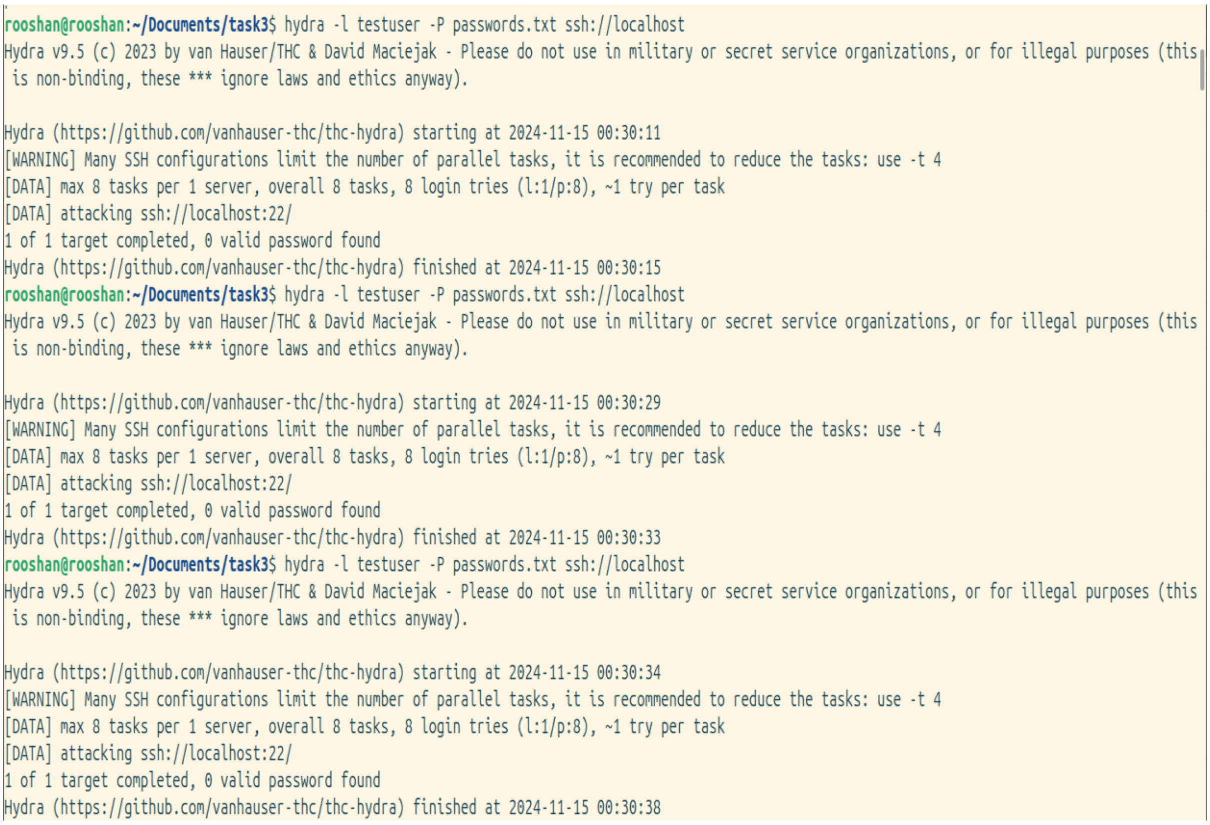
Task 3:

Adding the rule



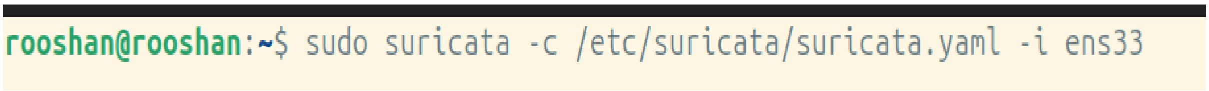
```
alert tcp any any -> any 22 (msg:"Possible SSH brute force attempt"; flow:to_server; threshold:type both, track by_src, count 5, seconds 60; sid:100
```

Using hydra to connect with ssh



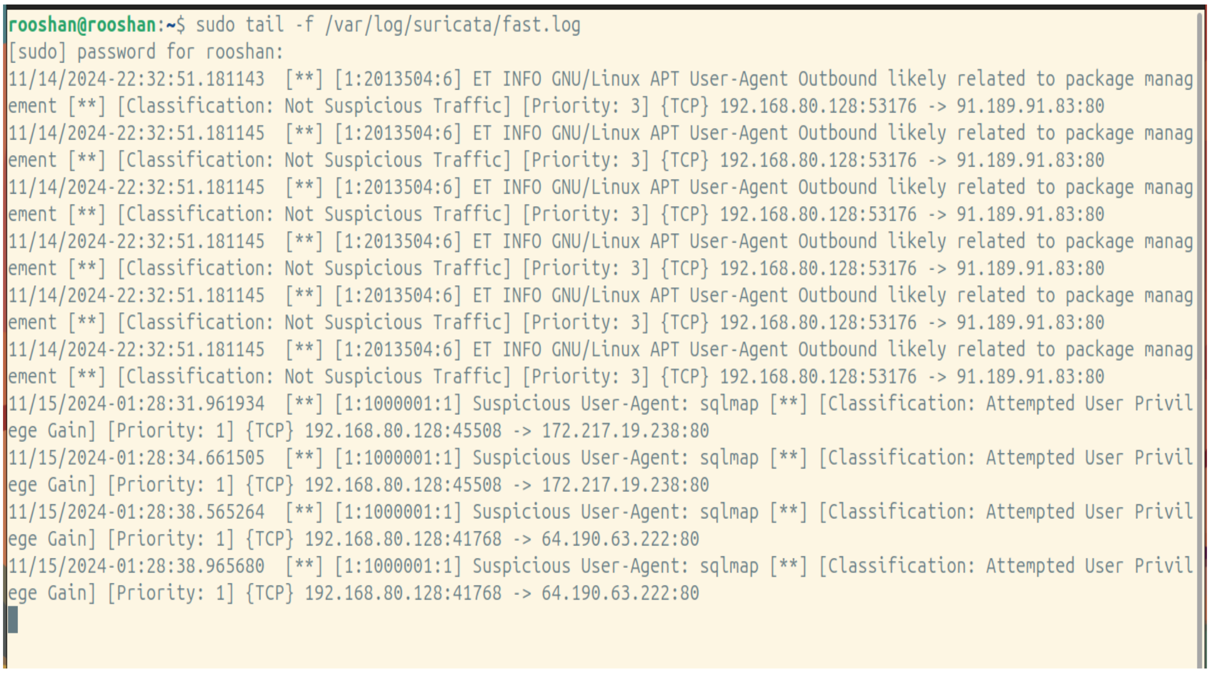
```
rooshan@rooshan:~/Documents/task3$ hydra -l testuser -P passwords.txt ssh://localhost
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this
 is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-15 00:30:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 try per task
[DATA] attacking ssh://localhost:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-15 00:30:15
rooshan@rooshan:~/Documents/task3$ hydra -l testuser -P passwords.txt ssh://localhost
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this
 is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-15 00:30:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 try per task
[DATA] attacking ssh://localhost:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-15 00:30:33
rooshan@rooshan:~/Documents/task3$ hydra -l testuser -P passwords.txt ssh://localhost
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this
 is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-15 00:30:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 try per task
[DATA] attacking ssh://localhost:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-15 00:30:38
```

Loading suricata to apply the rule



```
rooshan@rooshan:~$ sudo suricata -c /etc/suricata/suricata.yaml -i ens33
```

Logs



```
rooshan@rooshan:~$ sudo tail -f /var/log/suricata/fast.log
[sudo] password for rooshan:
11/14/2024-22:32:51.181143  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/14/2024-22:32:51.181145  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/14/2024-22:32:51.181145  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/14/2024-22:32:51.181145  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/14/2024-22:32:51.181145  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/14/2024-22:32:51.181145  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.80.128:53176 -> 91.189.91.83:80
11/15/2024-01:28:31.961934  [**] [1:1000001:1] Suspicious User-Agent: sqlmap [**] [Classification: Attempted User Privil
ege Gain] [Priority: 1] {TCP} 192.168.80.128:45508 -> 172.217.19.238:80
11/15/2024-01:28:34.661505  [**] [1:1000001:1] Suspicious User-Agent: sqlmap [**] [Classification: Attempted User Privil
ege Gain] [Priority: 1] {TCP} 192.168.80.128:45508 -> 172.217.19.238:80
11/15/2024-01:28:38.565264  [**] [1:1000001:1] Suspicious User-Agent: sqlmap [**] [Classification: Attempted User Privil
ege Gain] [Priority: 1] {TCP} 192.168.80.128:41768 -> 64.190.63.222:80
11/15/2024-01:28:38.965680  [**] [1:1000001:1] Suspicious User-Agent: sqlmap [**] [Classification: Attempted User Privil
ege Gain] [Priority: 1] {TCP} 192.168.80.128:41768 -> 64.190.63.222:80
```