NETWORK ATTACK REPORT

Tyler Dao

SECU73010 – NETWORK SECURITY

Contents

System Configuration

Devices

- CCVM2025: Target Server
- Parrot OS VM: Attacker
- OPNSense: VPN Server

Network Configuration

LAN: 192.168.1.0/24

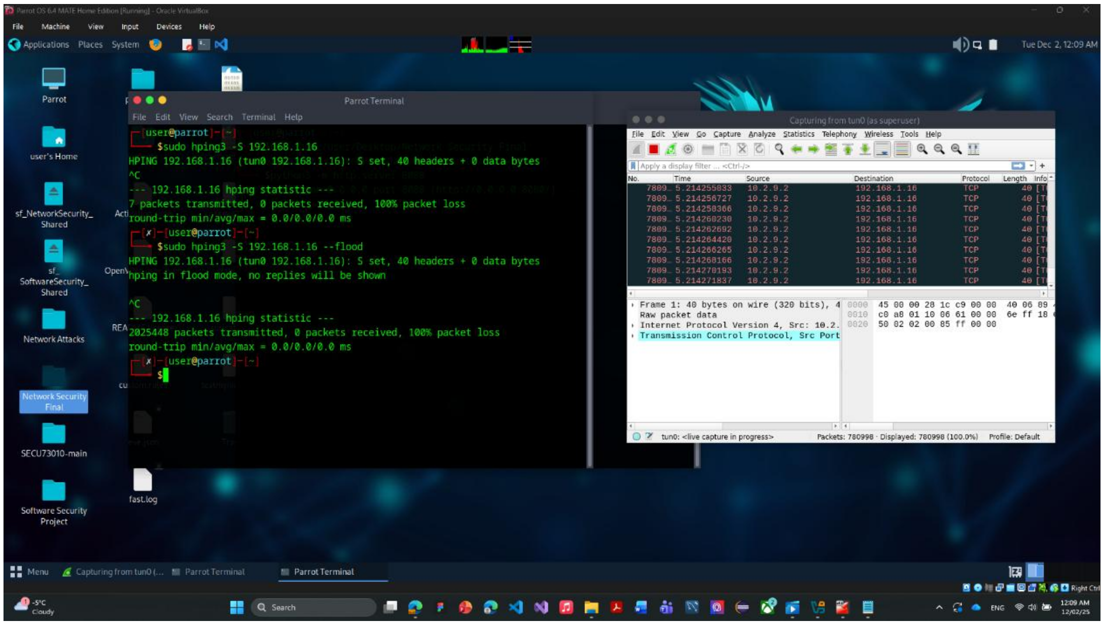
- CCVM2025: 192.168.1.16
- Parrot OS VM:
  - Adapter 1 (Bridged): 10.10.113.135
  - VPN Connection to OPNSense server: 10.2.9.2
- OPNSense:
  - LAN Gateway: 192.168.1.1
  - VPN Server: 10.2.9.0/24

Suricata service on OPNSense server acts like an IDS to monitor any suspicious content going to the LAN network.

Network attack scenarios

DoS attack

Attacker uses hping 3 to send high amount of TPC SYN packets to target server on port 80 to disrupt it. The characteristic of this attack is a high amount of TCP SYN packet will be sent from one or multiple sources to one IP address. Suricata rule can be written to track if there are to many TCP SYN packets in the traffic to a specific destination.



```
┌─[user@parrot]─[~]
└──╼ $sudo hping3 -S 192.168.1.16
HPING 192.168.1.16 (tun0 192.168.1.16): S set, 40 headers + 0 data bytes
^C
--- 192.168.1.16 hping statistic ---
7 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo hping3 -S 192.168.1.16 --flood
HPING 192.168.1.16 (tun0 192.168.1.16): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

^C
--- 192.168.1.16 hping statistic ---
2025448 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
┌─[✗]─[user@parrot]─[~]
└──╼ $
```

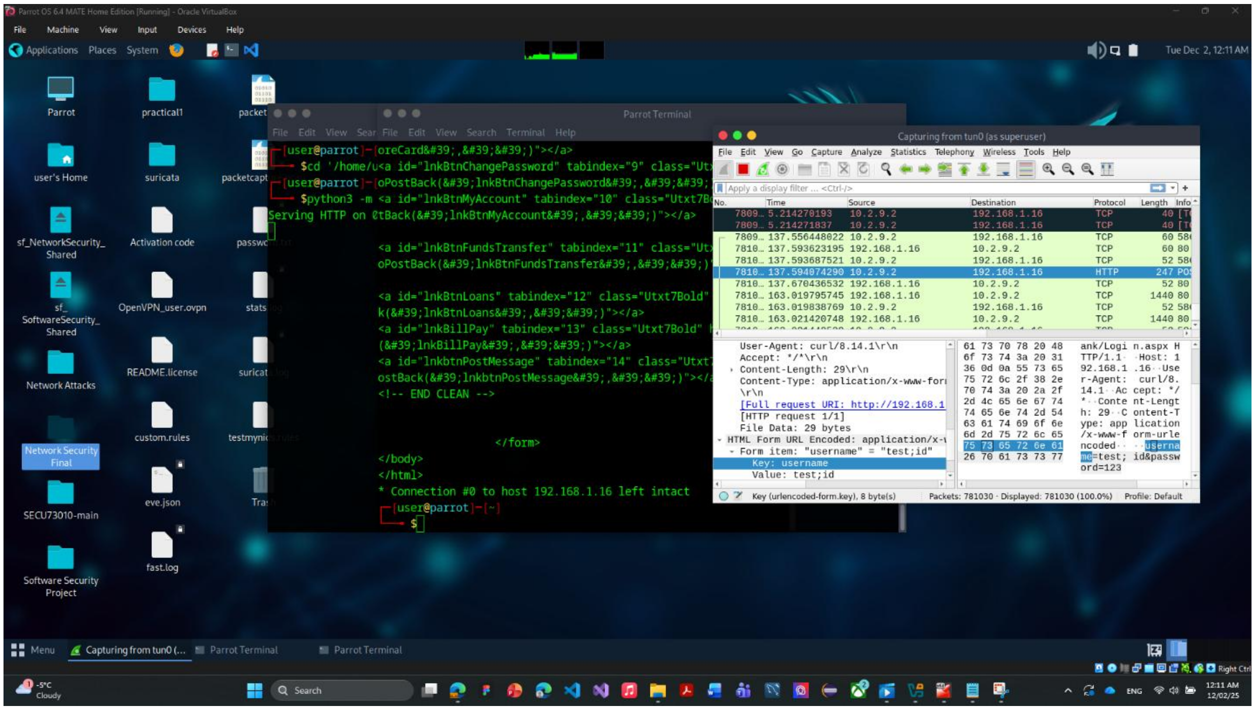
```
No.      Time          Source      Destination    Protocol  Length  Info
7809…  5.214255833   10.2.9.2    192.168.1.16   TCP       40  [T
7809…  5.214256727   10.2.9.2    192.168.1.16   TCP       40  [T
7809…  5.214258366   10.2.9.2    192.168.1.16   TCP       40  [T
7809…  5.214260230   10.2.9.2    192.168.1.16   TCP       40  [T
7809…  5.214262692   10.2.9.2    192.168.1.16   TCP       40  [T
7809…  5.214264420   10.2.9.2    192.168.1.16   TCP       40  [T
7809…  5.214266265   10.2.9.2    192.168.1.16   TCP       40  [T
7809…  5.214268166   10.2.9.2    192.168.1.16   TCP       40  [T
7809…  5.214270193   10.2.9.2    192.168.1.16   TCP       40  [T
7809…  5.214271837   10.2.9.2    192.168.1.16   TCP       40  [T

› Frame 1: 40 bytes on wire (320 bits), 4     0000  45 00 00 28 1c c9 00 00  40 06 89
  Raw packet data                             0010  c0 a8 01 10 06 61 00 00  6e ff 18
› Internet Protocol Version 4, Src: 10.2.     0020  50 02 02 00 85 ff 00 00
› Transmission Control Protocol, Src Port

tun0: <live capture in progress>    Packets: 780998 · Displayed: 780998 (100.0%)    Profile: Default
```

Parrot Terminal
File Edit View Search Terminal Help
Capturing from tun0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Parrot
user's Home
sf_NetworkSecurity_Shared
sf_SoftwareSecurity_Shared
Network Attacks
Network Security Final
SECU73010-main
Software Security Project
fast.log
Menu
Capturing from tun0 (…
Parrot Terminal
Parrot Terminal
Tue Dec 2, 12:09 AM

In the scenario, ~2 millions TCP packets were sent to target server within 10 seconds.

Command Attack

In this attack, if the server does not sanitize the input properly, the attacker uses HTTP packet to insert malicious system command such as “cat”,” “id”, “bash”, etc. to get the information about server system. Suricata rule can be written to detect a pattern with characters that are usually used in the system command such as “;”, “||”, “&&”, and some malicious key words such “cat”, “id”, “bash”.



```
┌─[user@parrot]─[oreCard&#39;,&#39;&#39;)"></a>
└──╼ $cd '/home/u<a id="lnkBtnChangePassword" tabindex="9" class="Ut
┌─[user@parrot]─[oPostBack(&#39;lnkBtnChangePassword&#39;,&#39;&#39;
└──╼ $python3 -m <a id="lnkBtnMyAccount" tabindex="10" class="Utxt7B
Serving HTTP on @tBack(&#39;lnkBtnMyAccount&#39;,&#39;&#39;)"></a>

                 <a id="lnkBtnFundsTransfer" tabindex="11" class="Ut
                 oPostBack(&#39;lnkBtnFundsTransfer&#39;,&#39;&#39;)

                 <a id="lnkBtnLoans" tabindex="12" class="Utxt7Bold"
                 k(&#39;lnkBtnLoans&#39;,&#39;&#39;)"></a>
                 <a id="lnkBillPay" tabindex="13" class="Utxt7Bold"
                 (&#39;lnkBillPay&#39;,&#39;&#39;)"></a>
                 <a id="lnkbtnPostMessage" tabindex="14" class="Utxt
                 ostBack(&#39;lnkbtnPostMessage&#39;,&#39;&#39;)"></a
                 <!-- END CLEAN -->


                              </form>
                 </body>
                 </html>
                 * Connection #0 to host 192.168.1.16 left intact
                 ┌─[user@parrot]─[~]
                 └──╼ $
```

Capturing from tun0 (as superuser)

```
No.     Time            Source          Destination     Protocol  Length Info
7809…  5.214270193     10.2.9.2        192.168.1.16    TCP         40 [T
7809…  5.214271837     10.2.9.2        192.168.1.16    TCP         40 [T
7809…  137.556448022   10.2.9.2        192.168.1.16    TCP         60 58
7810…  137.593623195   192.168.1.16    10.2.9.2        TCP         60 80
7810…  137.593687521   10.2.9.2        192.168.1.16    TCP         52 58
7810…  137.594074290   10.2.9.2        192.168.1.16    HTTP       247 PO
7810…  137.670436532   192.168.1.16    10.2.9.2        TCP         52 80
7810…  163.019795745   192.168.1.16    10.2.9.2        TCP       1440 80
7810…  163.019838769   10.2.9.2        192.168.1.16    TCP         52 58
7810…  163.021420748   192.168.1.16    10.2.9.2        TCP       1440 80
```

```
    User-Agent: curl/8.14.1\r\n
    Accept: */*\r\n
  › Content-Length: 29\r\n
    Content-Type: application/x-www-for
    \r\n
    [Full request URI: http://192.168.1
    [HTTP request 1/1]
    File Data: 29 bytes
⌄ HTML Form URL Encoded: application/x-
  ⌄ Form item: "username" = "test;id"
      Key: username
      Value: test;id
```

```
61 73 70 78 20 48   ank/Logi n.aspx H
6f 73 74 3a 20 31   TTP/1.1· ·Host: 1
36 0d 0a 55 73 65   92.168.1 .16··Use
75 72 6c 2f 38 2e   r-Agent:  curl/8.
70 74 3a 20 2a 2f   14.1··Ac cept: */
2d 4c 65 6e 67 74   *··Conte nt-Lengt
74 65 6e 74 2d 54   h: 29··C ontent-T
63 61 74 69 6f 6e   ype: app lication
6d 2d 75 72 6c 65   /x-www-f orm-urle
75 73 65 72 6e 61   ncoded··  ··userna
26 70 61 73 73 77   me=test; id&passw
                    ord=123
```

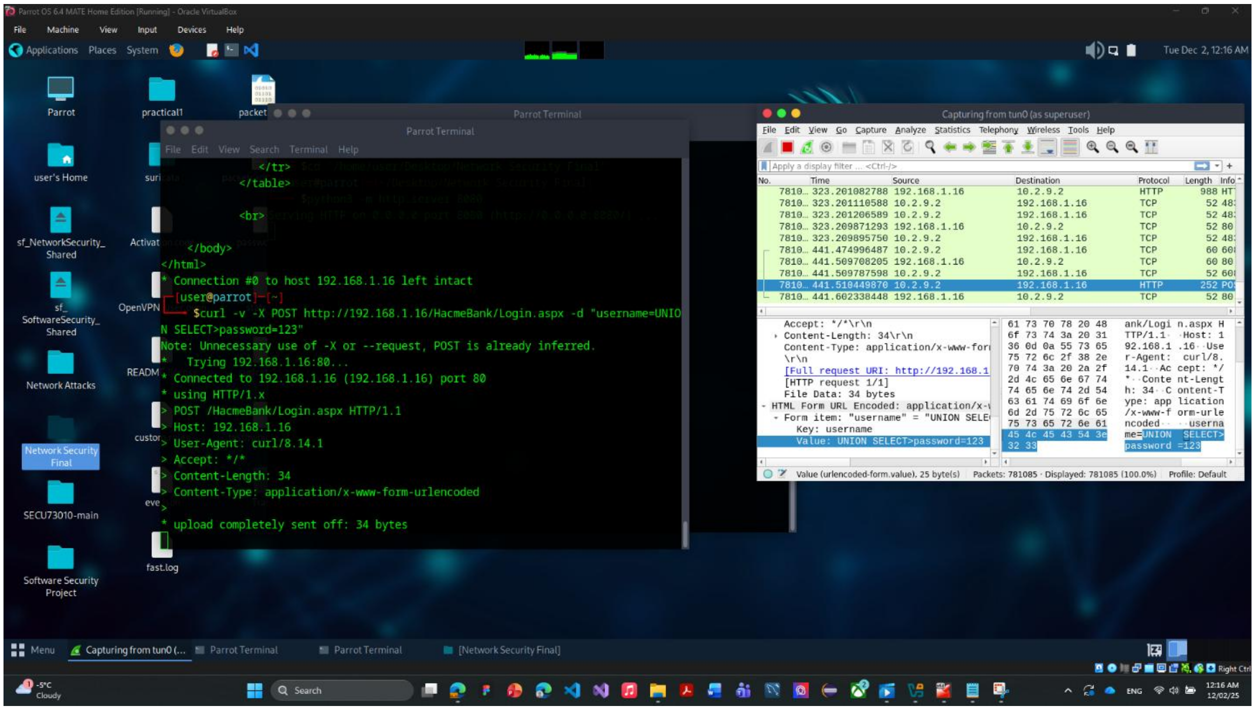
Key (urlencoded-form.key), 8 byte(s)   Packets: 781030 · Displayed: 781030 (100.0%)   Profile: Default

Parrot OS 6.4 MATE Home Edition [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System
Tue Dec 2, 12:11 AM
Parrot
practical1
packet
user's Home
suricata
packetcapt
sf_NetworkSecurity_Shared
Activation code
passwo
sf_SoftwareSecurity_Shared
OpenVPN_user.ovpn
stats
Network Attacks
README.license
suricat
custom.rules
testmyni
Network Security Final
eve.json
Tras
SECU73010-main
fast.log
Software Security Project
Parrot Terminal
File Edit View Search Terminal Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Menu
Capturing from tun0 (…
Parrot Terminal
Parrot Terminal
Right Ctrl
-5°C
Cloudy
Search
ENG
12:11 AM
12/02/25

In the scenario, I have inserted "; id &&" in the username field in HTTP body to send to server, the command is to get the identity of users and groups in server.

SQL injection attack

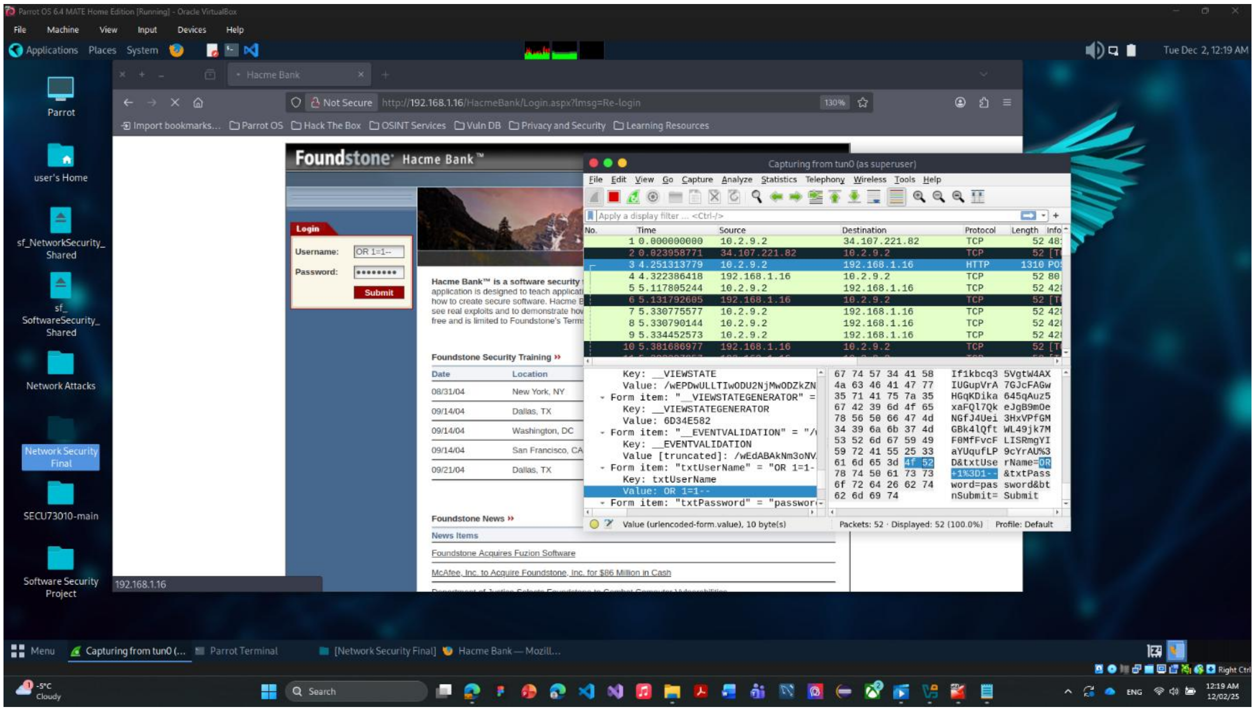
In this attack, if the server does not sanitize user's input properly, the attacker can insert malicious queries into the input field to be sent with HTTP packet to get information on the database such as "OR 1=1--" or "UNION SELECT users FROM users" to get users information from the database.


Capturing from tun0 (as superuser)
Parrot Terminal
File Edit View Search Terminal Help

```
        </tr>
      </table>

      <br>

   </body>
</html>
* Connection #0 to host 192.168.1.16 left intact
┌─[user@parrot]─[~]
└──╼ $curl -v -X POST http://192.168.1.16/HacmeBank/Login.aspx -d "username=UNIO
N SELECT>password=123"
Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 192.168.1.16:80...
* Connected to 192.168.1.16 (192.168.1.16) port 80
* using HTTP/1.x
> POST /HacmeBank/Login.aspx HTTP/1.1
> Host: 192.168.1.16
> User-Agent: curl/8.14.1
> Accept: */*
> Content-Length: 34
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 34 bytes
```

```
No.    Time          Source         Destination    Protocol Length Info
7810…  323.201082788 192.168.1.16   10.2.9.2       HTTP     988 HT
7810…  323.201110588 10.2.9.2       192.168.1.16   TCP      52 48
7810…  323.201206589 10.2.9.2       192.168.1.16   TCP      52 48
7810…  323.209871293 192.168.1.16   10.2.9.2       TCP      52 80
7810…  323.209895750 10.2.9.2       192.168.1.16   TCP      52 48
7810…  441.474996487 10.2.9.2       192.168.1.16   TCP      60 60
7810…  441.509708205 192.168.1.16   10.2.9.2       TCP      60 80
7810…  441.509787598 10.2.9.2       192.168.1.16   TCP      52 60
7810…  441.510449870 10.2.9.2       192.168.1.16   HTTP     252 PO
7810…  441.602338448 192.168.1.16   10.2.9.2       TCP      52 80

  Accept: */*\r\n
 › Content-Length: 34\r\n
  Content-Type: application/x-www-for
  \r\n
  [Full request URI: http://192.168.1
  [HTTP request 1/1]
  File Data: 34 bytes
⌄ HTML Form URL Encoded: application/x-
 ⌄ Form item: "username" = "UNION SELE
    Key: username
    Value: UNION SELECT>password=123

61 73 70 78 20 48   ank/Logi n.aspx H
6f 73 74 3a 20 31   TTP/1.1· ·Host: 1
36 0d 0a 55 73 65   92.168.1 .16··Use
75 72 6c 2f 38 2e   r-Agent:  curl/8.
70 74 3a 20 2a 2f   14.1··Ac cept: */
2d 4c 65 6e 67 74   *··Conte nt-Lengt
74 65 6e 74 2d 54   h: 34··C ontent-T
63 61 74 69 6f 6e   ype: app lication
6d 2d 75 72 6c 65   /x-www-f orm-urle
75 73 65 72 6e 61   ncoded··  ··userna
45 4c 45 43 54 3e   me=UNION  SELECT>
32 33               password =123

Value (urlencoded-form.value), 25 byte(s)   Packets: 781085 · Displayed: 781085 (100.0%)   Profile: Default
```

In this demo, I used command curl on the terminal to send a POST request to server with the body contains "username=UNION SELECT". Suricata rule shall be able to detect "UNION" or "SELECT" in the network traffic.

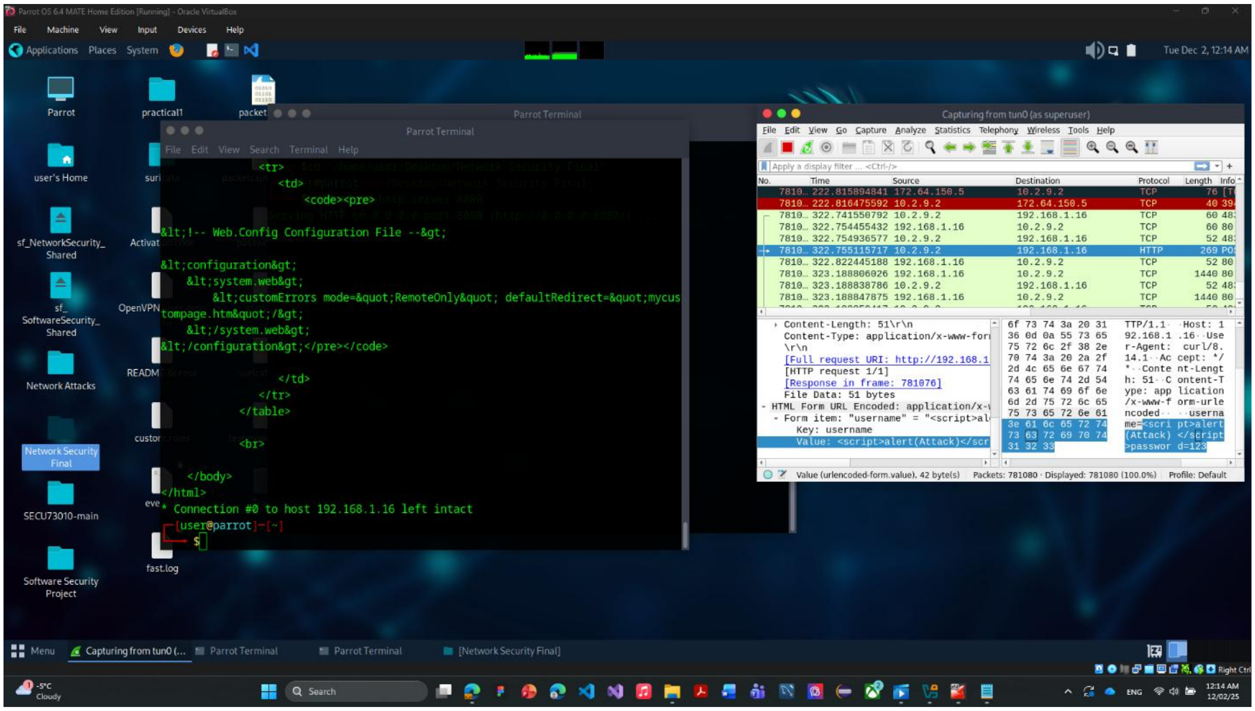

Hacme Bank
Not Secure http://192.168.1.16/HacmeBank/Login.aspx?lmsg=Re-login
Foundstone Hacme Bank
Login
Username: OR 1=1--
Password: ••••••••
Submit
Capturing from tun0 (as superuser)

```
No. Time          Source         Destination    Protocol Length Info
  1 0.000000000   10.2.9.2       34.107.221.82  TCP      52 48
  2 0.023958771   34.107.221.82  10.2.9.2       TCP      52 [T
  3 4.251313779   10.2.9.2       192.168.1.16   HTTP     1310 PO
  4 4.322386418   192.168.1.16   10.2.9.2       TCP      52 80
  5 5.117805244   10.2.9.2       192.168.1.16   TCP      52 42
  6 5.131792605   192.168.1.16   10.2.9.2       TCP      52 [T
  7 5.330775577   10.2.9.2       192.168.1.16   TCP      52 42
  8 5.330790144   10.2.9.2       192.168.1.16   TCP      52 42
  9 5.334452573   10.2.9.2       192.168.1.16   TCP      52 42
 10 5.381686977   192.168.1.16   10.2.9.2       TCP      52 [T

    Key: __VIEWSTATE
    Value: /wEPDwULLTIwODU2NjMwODZkZN
 ⌄ Form item: "__VIEWSTATEGENERATOR" =
    Key: __VIEWSTATEGENERATOR
    Value: 6D34E582
 ⌄ Form item: "__EVENTVALIDATION" = "/
    Key: __EVENTVALIDATION
    Value [truncated]: /wEdABAkNm3oNV
 ⌄ Form item: "txtUserName" = "OR 1=1-
    Key: txtUserName
    Value: OR 1=1--
 ⌄ Form item: "txtPassword" = "passwor

67 74 57 34 41 58   If1kbcq3 5VgtW4AX
4a 63 46 41 47 77   IUGupVrA 7GJcFAGw
35 71 41 75 7a 35   HGqKDika 645qAuz5
67 42 39 6d 4f 65   xaFQl7Qk eJgB9mOe
78 56 50 66 47 4d   NGfJ4Uei 3HxVPfGM
34 39 6a 6b 37 4d   GBk4lQft WL49jk7M
53 52 6d 67 59 49   F0MfFvcF LISRmgYI
59 72 41 55 25 33   aYUqufLP 9cYrAU%3
61 6d 65 3d 4f 52   D&txtUse rName=OR
78 74 50 61 73 73   +1%3D1-- &txtPass
6f 72 64 26 62 74   word=pas sword&bt
62 6d 69 74         nSubmit= Submit

Value (urlencoded-form.value), 10 byte(s)   Packets: 52 · Displayed: 52 (100.0%)   Profile: Default
```

In this scenario, I used the website Hacme Bank website running on server, I typed "OR 1=1--" in username field and when I clicked submit, an HTTP packet was sent to the server and “txtUserName=OR+1%3D1--” is included in the packet. To detect this, Suricata rule shall be able to detect “OR+1%3D1--”, which is the encoded of “OR 1=1--” in the network traffic.

Cross-site attack

In this attack, the attacker can insert a script into the request to bypass the website’s security methods to steal sensitive information such as cookies, session ID.



```
            <tr>
              <td>
                <code><pre>

&lt;!-- Web.Config Configuration File --&gt;

&lt;configuration&gt;
    &lt;system.web&gt;
        &lt;customErrors mode=&quot;RemoteOnly&quot; defaultRedirect=&quot;mycus
tompage.htm&quot;/&gt;
    &lt;/system.web&gt;
&lt;/configuration&gt;</pre></code>

              </td>
            </tr>
          </table>

          <br>

    </body>
</html>
* Connection #0 to host 192.168.1.16 left intact
┌─[user@parrot]─[~]
└──── $
```

```
No.     Time          Source         Destination    Protocol Length Info
7810… 222.815894841 172.64.150.5   10.2.9.2       TCP        76 [T
7810… 222.816475592 10.2.9.2       172.64.150.5   TCP        40 39
7810… 322.741550792 10.2.9.2       192.168.1.16   TCP        60 48
7810… 322.754455432 192.168.1.16   10.2.9.2       TCP        60 80
7810… 322.754936577 10.2.9.2       192.168.1.16   TCP        52 48
7810… 322.755115717 10.2.9.2       192.168.1.16   HTTP      269 PO
7810… 322.822445188 192.168.1.16   10.2.9.2       TCP        52 80
7810… 323.188806026 192.168.1.16   10.2.9.2       TCP      1440 80
7810… 323.188838786 10.2.9.2       192.168.1.16   TCP        52 48
7810… 323.188847875 192.168.1.16   10.2.9.2       TCP      1440 80
```

```
  › Content-Length: 51\r\n
    Content-Type: application/x-www-for
    \r\n
    [Full request URI: http://192.168.1
    [HTTP request 1/1]
    [Response in frame: 781076]
    File Data: 51 bytes
› HTML Form URL Encoded: application/x-
  › Form item: "username" = "<script>al
      Key: username
      Value: <script>alert(Attack)</scr
```

```
6f 73 74 3a 20 31   TTP/1.1· ·Host: 1
36 0d 0a 55 73 65   92.168.1 .16· ·Use
75 72 6c 2f 38 2e   r-Agent:  curl/8.
70 74 3a 20 2a 2f   14.1· ·Ac cept: */
2d 4c 65 6e 67 74   *· ·Conte nt-Lengt
74 65 6e 74 2d 54   h: 51· ·C ontent-T
63 61 74 69 6f 6e   ype: app lication
6d 2d 75 72 6c 65   /x-www-f orm-urle
75 73 65 72 6e 61   ncoded· · · ·userna
3e 61 6c 65 72 74   me=<scri pt>alert
73 63 72 69 70 74   (Attack) </script
31 32 33            >passwor d=123
```

Value (urlencoded-form.value), 42 byte(s) · Packets: 781080 · Displayed: 781080 (100.0%) · Profile: Default

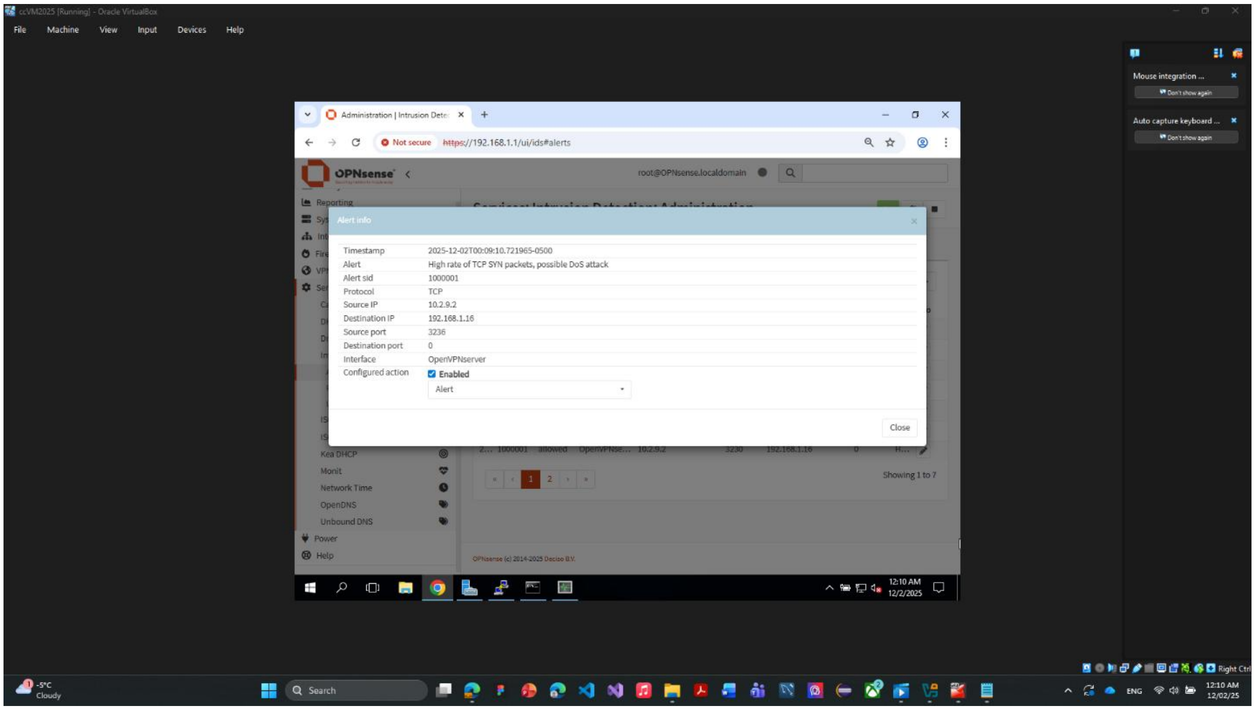
I used the command curl to send a POST request to server with username is “<script>alert(“Attack”)</script>”, in real attack, the attacker can use it to get information if it was stored in the browser’s session storage. TO detect this, Suricata shall look for the “<script>” tag in user’s request.

Suricata rules and alerts

Dos attack

alert tcp any any -> $HOME_NET any (msg:"High rate of TCP SYN packets, possible DoS attack"; flags:S; flow:stateless; threshold: type limit, track by_src, count 200, seconds 1; classtype:bad-unknown; sid:1000001; rev:2;)

- This rule will monitor TCP packets from any network to the home net (192.168.1.0/24), flag:S tells it to just count the SYS packet, flow:stateless means each packet will be individual, Suricata does not have to know the context of it, threshold: type limit, track by_src, count 200, seconds 1 means the alert will be triggered of there are more than 200 packets come from the same IP address in 1 second.

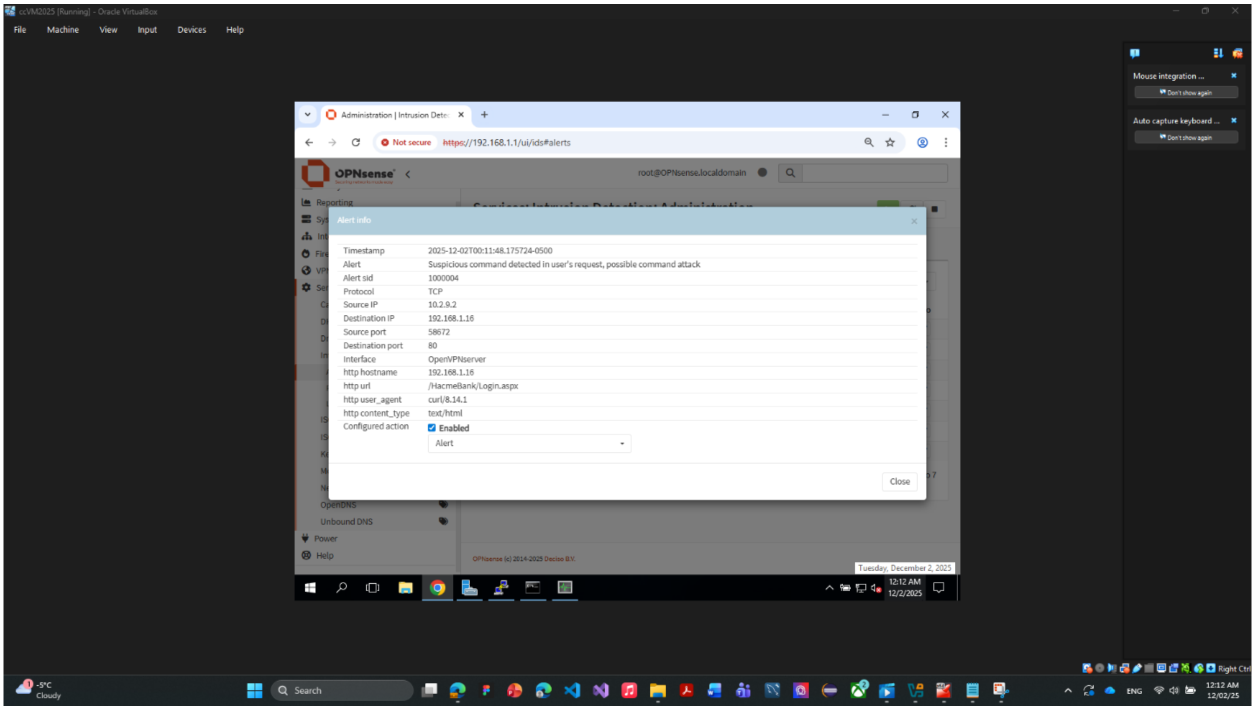


Timestamp	2025-12-02T00:09:10.721965-0500
Alert	High rate of TCP SYN packets, possible DoS attack
Alert sid	1000001
Protocol	TCP
Source IP	10.2.9.2
Destination IP	192.168.1.16
Source port	3236
Destination port	0
Interface	OpenVPNserver
Configured action	☑ Enabled Alert

Command attack

alert http any any -> any any (msg:"Suspicious command detected in user's request, possible command attack"; http.request_body; pcre:"/(\;|\|\||\&\&)\s(id|cat|curl|uname|nc|bash|sh)\b/i"; classtype:bad-unknown; sid:1000004; rev:3;)*

- This rule will monitor HTTP packet from any network to any network, as long as it goes through the firewall. http.request_body tells the rule to look at the HTTP body, pcre:"/(\;|\|\||\&\&)\s*(id|cat|curl|uname|nc|bash|sh)\b/i" tells the rule to not check by content, but check by the pattern, if the content contains a semicolon, or 2 slashes, or 2 ampersands, followed by at least a space, then one of these key words “id”, “cat”, “curl”, “uname”, “nc”, “bash”, “sh”, \b means check if the word is exactly matched with the keyword, for example, if the word is “curlXYZ” then it is not a match, /i means case insensitive.


ccVM2025 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Administration | Intrusion Detec
Not secure
https://192.168.1.1/ui/ids#alerts
OPNsense
root@OPNsense.localdomain
Reporting
OpenDNS
Unbound DNS
Power
Help
Alert info
Close
OPNsense (c) 2014-2025 Deciso B.V.
Tuesday, December 2, 2025
12:12 AM
12/2/2025
Mouse integration ...
Auto capture keyboard ...
Don't show again
-5°C
Cloudy
Search
Right Ctrl
12:12 AM
12/02/25

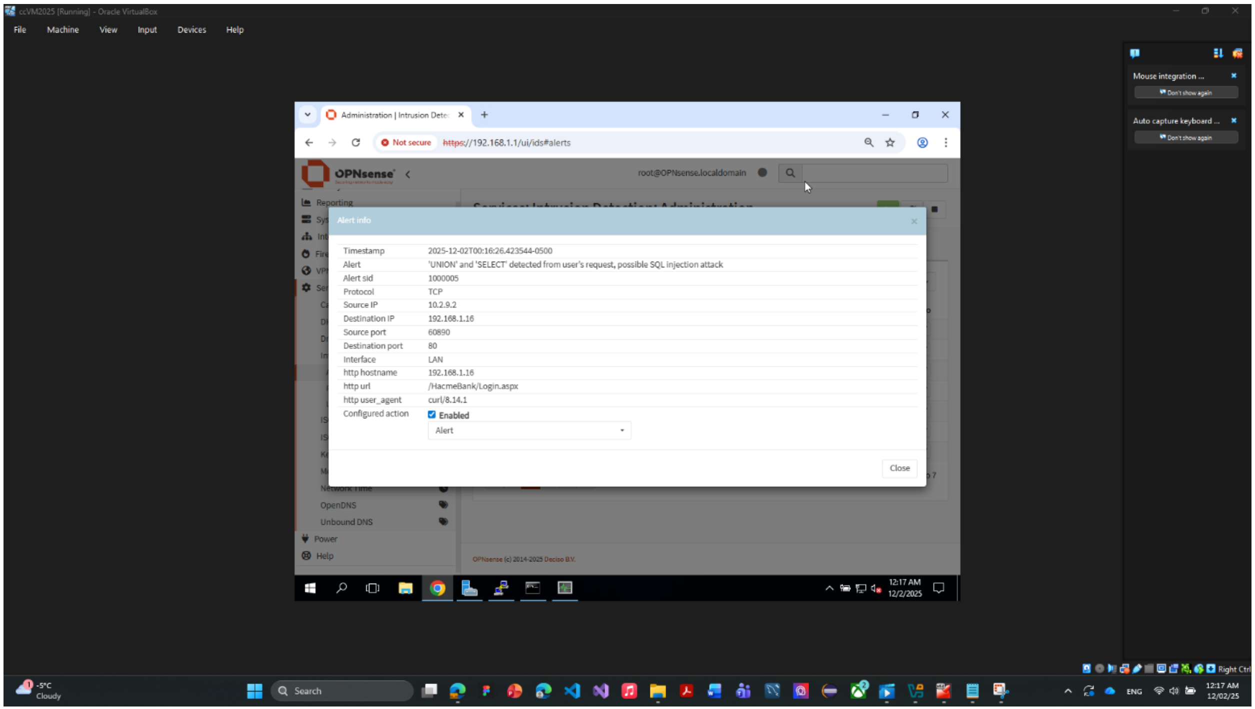
Timestamp	2025-12-02T00:11:48.175724-0500
Alert	Suspicious command detected in user's request, possible command attack
Alert sid	1000004
Protocol	TCP
Source IP	10.2.9.2
Destination IP	192.168.1.16
Source port	58672
Destination port	80
Interface	OpenVPNserver
http hostname	192.168.1.16
http url	/HacmeBank/Login.aspx
http user_agent	curl/8.14.1
http content_type	text/html
Configured action	☑ Enabled Alert

SQL injection attack

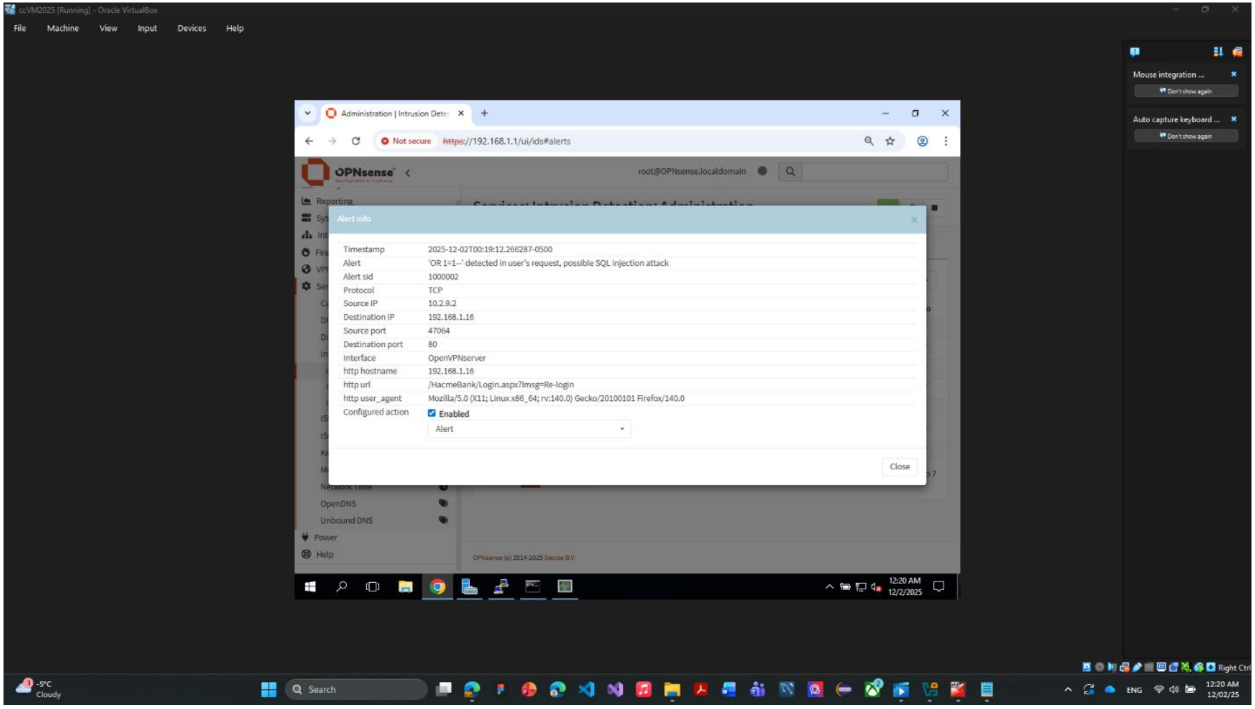
alert tcp any any -> any any (msg:"'UNION' and 'SELECT' detected from user's request, possible SQL injection attack";http.request_body; content:"UNION"; content:"SELECT"; classtype:bad-unknown; sid:1000005; rev:3;)

alert http any any -> any any (msg:"'OR 1=1--' detected in user's request, possible SQL injection attack"; http.request_body; content:"OR+1%3D1--"; classtype:bad-unknown; sid:1000002; rev:3;)

- These 2 rules do the same thing, they all look at the HTTP request body, one rule looks for the encoded “OR 1=1--”, another rule looks for “UNION” or “SELECT” in the payload.



Timestamp	2025-12-02T00:16:26.423544-0500
Alert	'UNION' and 'SELECT' detected from user's request, possible SQL injection attack
Alert sid	1000005
Protocol	TCP
Source IP	10.2.9.2
Destination IP	192.168.1.16
Source port	60890
Destination port	80
Interface	LAN
http hostname	192.168.1.16
http url	/HacmeBank/Login.aspx
http user_agent	curl/8.14.1
Configured action	☑ Enabled Alert

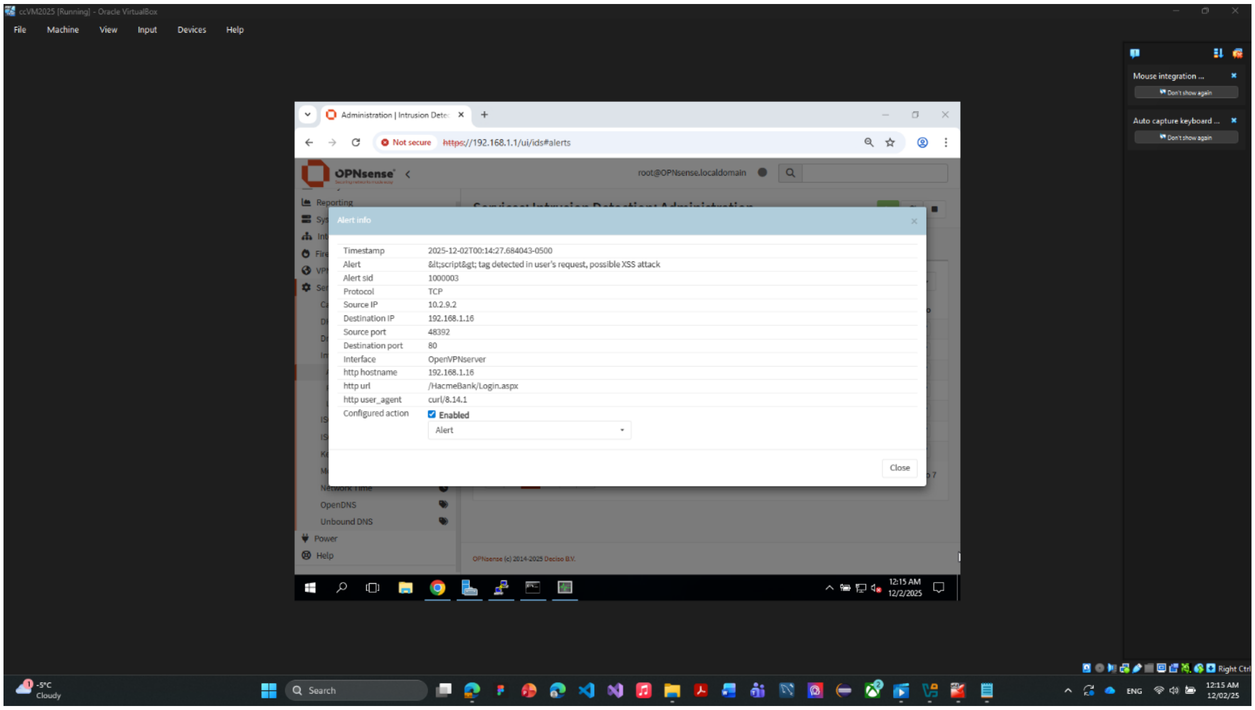


Timestamp	2025-12-02T00:19:12.266287-0500
Alert	'OR 1=1--' detected in user's request, possible SQL injection attack
Alert sid	1000002
Protocol	TCP
Source IP	10.2.9.2
Destination IP	192.168.1.16
Source port	47064
Destination port	80
Interface	OpenVPNserver
http hostname	192.168.1.16
http url	/HacmeBank/Login.aspx?lmsg=Re-login
http user_agent	Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Configured action	☑ Enabled Alert

Cross-site attack

alert tcp any any -> any any (msg:"<script> tag detected in user's request, possible XSS attack"; http.request_body; content:"<script>"; classtype:bad-unknown; sid:1000003; rev:3;)

- This rule looks for "<script>" in the HTTP request body, if there is a script tag in the request body, it will be triggered.



ccVM2025 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Administration | Intrusion Detec
Not secure
https://192.168.1.1/ui/ids#alerts
OPNsense
root@OPNsense.localdomain
Reporting
OpenDNS
Unbound DNS
Power
Help
OPNsense (c) 2014-2025 Deciso B.V.
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
12:15 AM
12/2/2025
-5°C
Cloudy
Search
ENG
12:15 AM
12/02/25

Alert info

Timestamp	2025-12-02T00:14:27.684043-0500
Alert	<script> tag detected in user's request, possible XSS attack
Alert sid	1000003
Protocol	TCP
Source IP	10.2.9.2
Destination IP	192.168.1.16
Source port	48392
Destination port	80
Interface	OpenVPNserver
http hostname	192.168.1.16
http url	/HacmeBank/Login.aspx
http user_agent	curl/8.14.1
Configured action	☑ Enabled Alert

Close