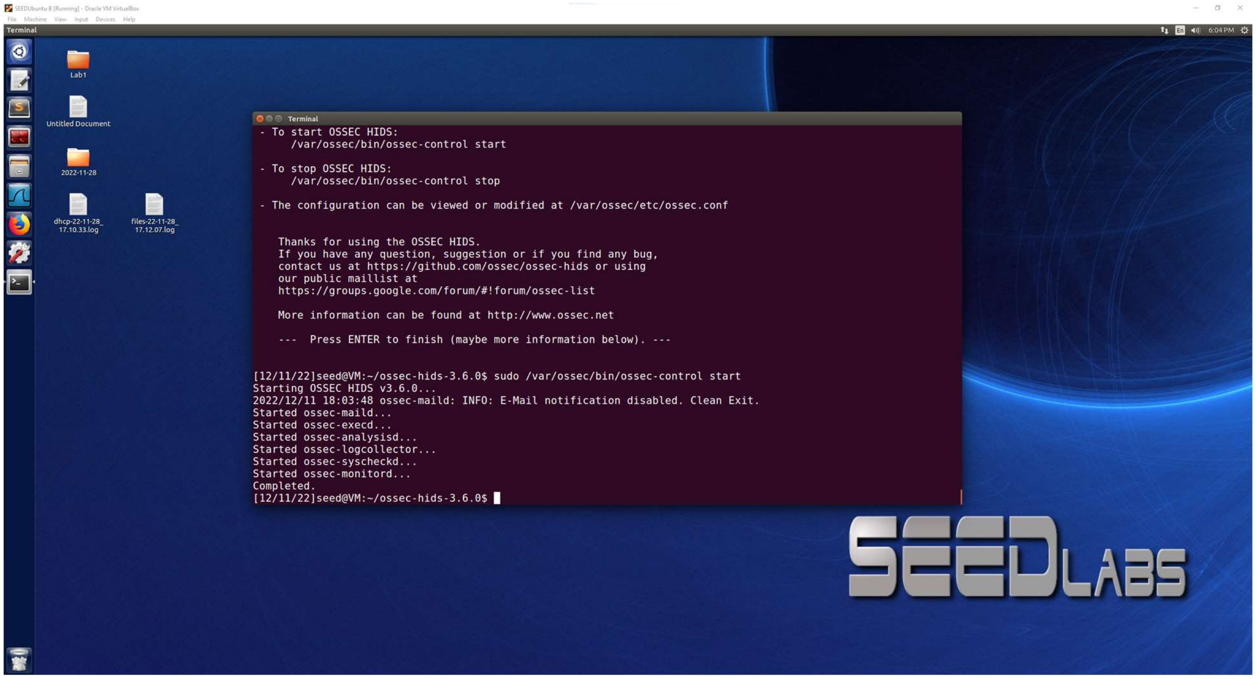
Lab 6-Part 2
Gunnar Yonker

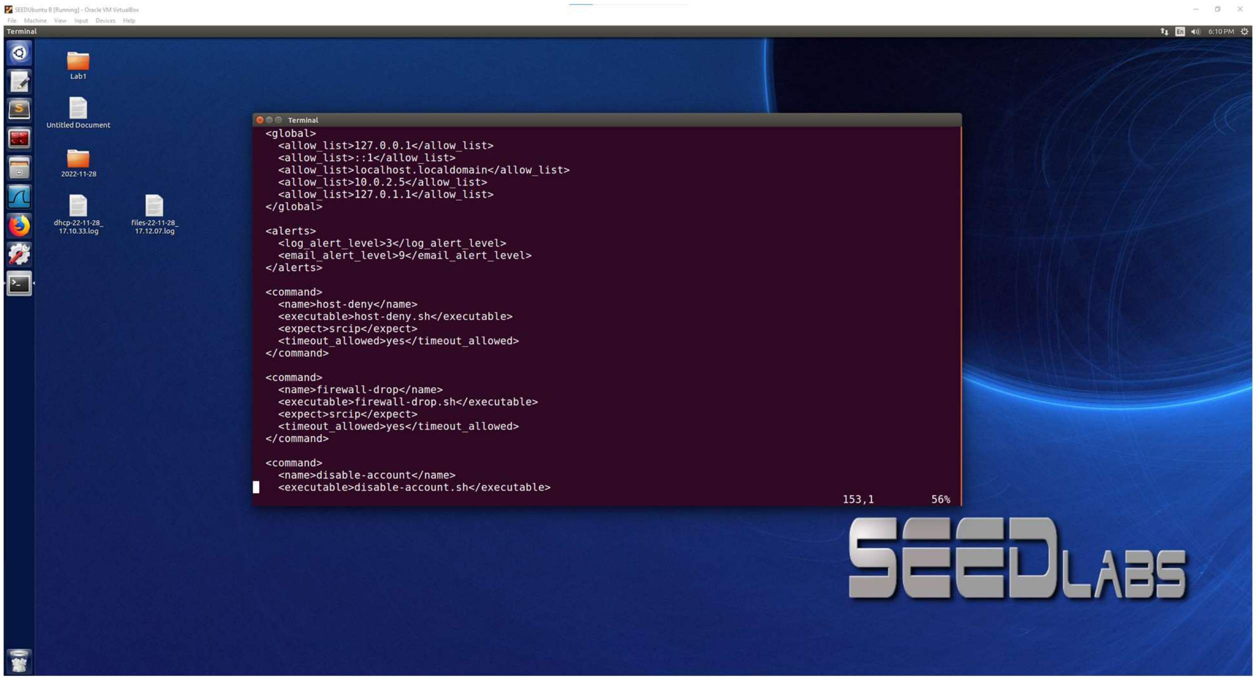
VM B(With OSSEC): 10.0.2.4

Screenshot showing that OSSEC was successfully installed and able to be started



```
 - To start OSSEC HIDS:
      /var/ossec/bin/ossec-control start

 - To stop OSSEC HIDS:
      /var/ossec/bin/ossec-control stop

 - The configuration can be viewed or modified at /var/ossec/etc/ossec.conf


    Thanks for using the OSSEC HIDS.
    If you have any question, suggestion or if you find any bug,
    contact us at https://github.com/ossec/ossec-hids or using
    our public maillist at
    https://groups.google.com/forum/#!forum/ossec-list

    More information can be found at http://www.ossec.net

    ---  Press ENTER to finish (maybe more information below). ---


[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.6.0...
2022/12/11 18:03:48 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ 
```

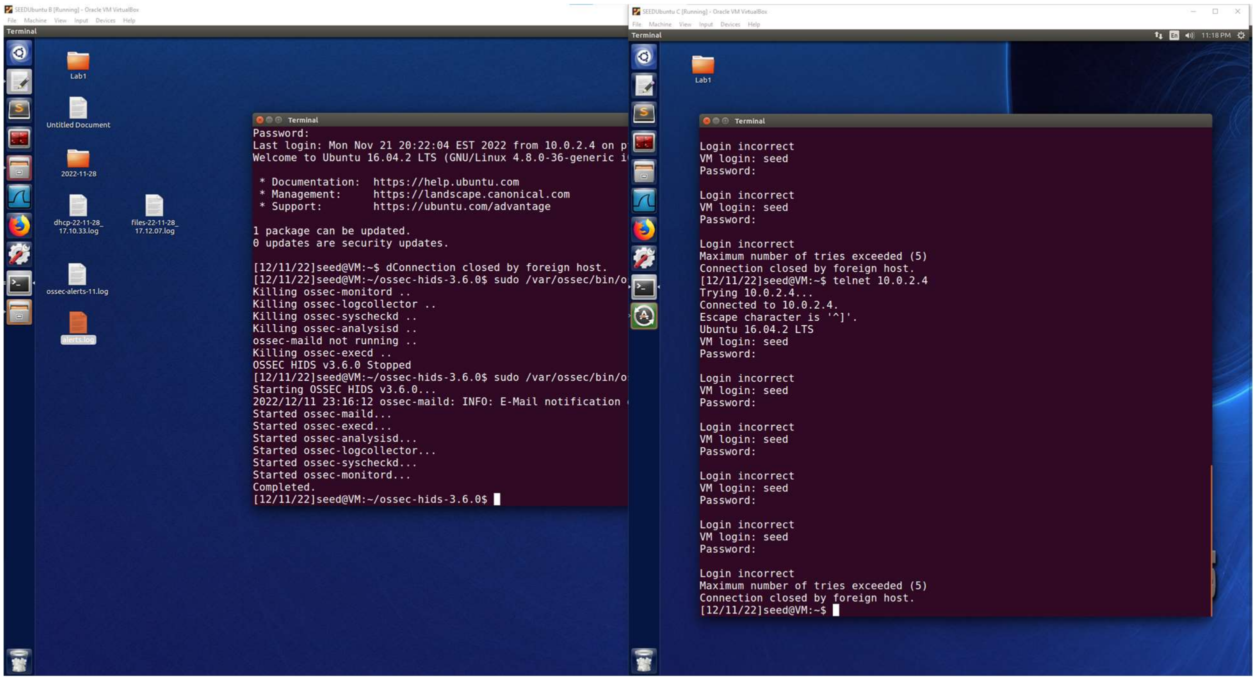
Severity Levels changed to 3 and 9



```
  <global>
    <allow_list>127.0.0.1</allow_list>
    <allow_list>::1</allow_list>
    <allow_list>localhost.localdomain</allow_list>
    <allow_list>10.0.2.5</allow_list>
    <allow_list>127.0.1.1</allow_list>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>9</email_alert_level>
  </alerts>

  <command>
    <name>host-deny</name>
    <executable>host-deny.sh</executable>
    <expect>srcip</expect>
    <timeout_allowed>yes</timeout_allowed>
  </command>

  <command>
    <name>firewall-drop</name>
    <executable>firewall-drop.sh</executable>
    <expect>srcip</expect>
    <timeout_allowed>yes</timeout_allowed>
  </command>

  <command>
    <name>disable-account</name>
    <executable>disable-account.sh</executable>
                                                                                 153,1         56%
```

Lab 6-Part 2
Gunnar Yonker

Password guessing attack, 10 attempts through telnet

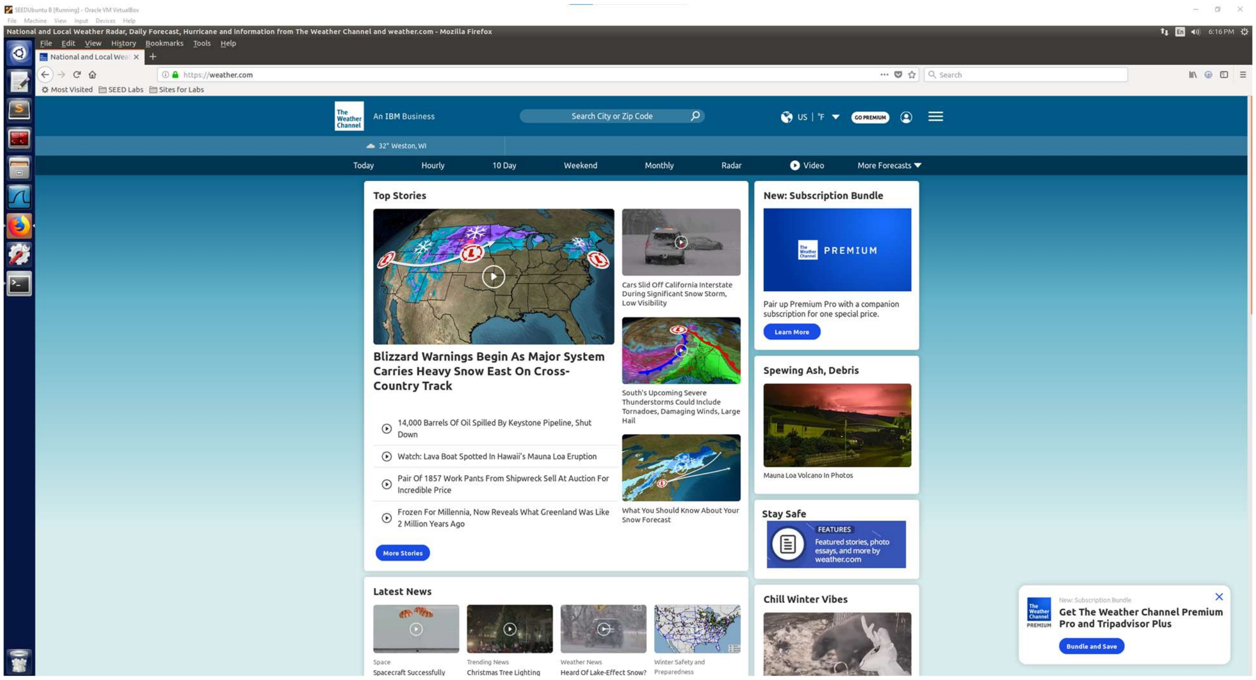


```
Password:
Last login: Mon Nov 21 20:22:04 EST 2022 from 10.0.2.4 on p
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i

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

1 package can be updated.
0 updates are security updates.

[12/11/22]seed@VM:~$ dConnection closed by foreign host.
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo /var/ossec/bin/o
Killing ossec-monitord ..
Killing ossec-logcollector ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
ossec-maild not running ..
Killing ossec-execd ..
OSSEC HIDS v3.6.0 Stopped
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo /var/ossec/bin/o
Starting OSSEC HIDS v3.6.0...
2022/12/11 23:16:12 ossec-maild: INFO: E-Mail notification 
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
[12/11/22]seed@VM:~/ossec-hids-3.6.0$
```

```
Login incorrect
VM login: seed
Password:

Login incorrect
VM login: seed
Password:

Login incorrect
Maximum number of tries exceeded (5)
Connection closed by foreign host.
[12/11/22]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:

Login incorrect
VM login: seed
Password:

Login incorrect
VM login: seed
Password:

Login incorrect
VM login: seed
Password:

Login incorrect
VM login: seed
Password:

Login incorrect
Maximum number of tries exceeded (5)
Connection closed by foreign host.
[12/11/22]seed@VM:~$
```

SEEDUbuntu B [Running] - Oracle VM VirtualBox
SEEDUbuntu C [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Lab1
Untitled Document
2022-11-28
dhcp-22-11-28_17.10.33.log
files-22-11-28_17.12.07.log
ossec-alerts-11.log
alerts.log
11:18 PM

Browsing a few https



National and Local Weather Radar, Daily Forecast, Hurricane and information from The Weather Channel and weather.com - Mozilla Firefox

https://weather.com

Top Stories

Blizzard Warnings Begin As Major System Carries Heavy Snow East On Cross-Country Track

14,000 Barrels Of Oil Spilled By Keystone Pipeline, Shut Down

Watch: Lava Boat Spotted In Hawaii's Mauna Loa Eruption

Pair Of 1857 Work Pants From Shipwreck Sell At Auction For Incredible Price

Frozen For Millennia, Now Reveals What Greenland Was Like 2 Million Years Ago

Cars Slid Off California Interstate During Significant Snow Storm, Low Visibility

South's Upcoming Severe Thunderstorms Could Include Tornadoes, Damaging Winds, Large Hail

What You Should Know About Your Snow Forecast

New: Subscription Bundle

Pair up Premium Pro with a companion subscription for one special price.

Spewing Ash, Debris

Mauna Loa Volcano In Photos

Stay Safe

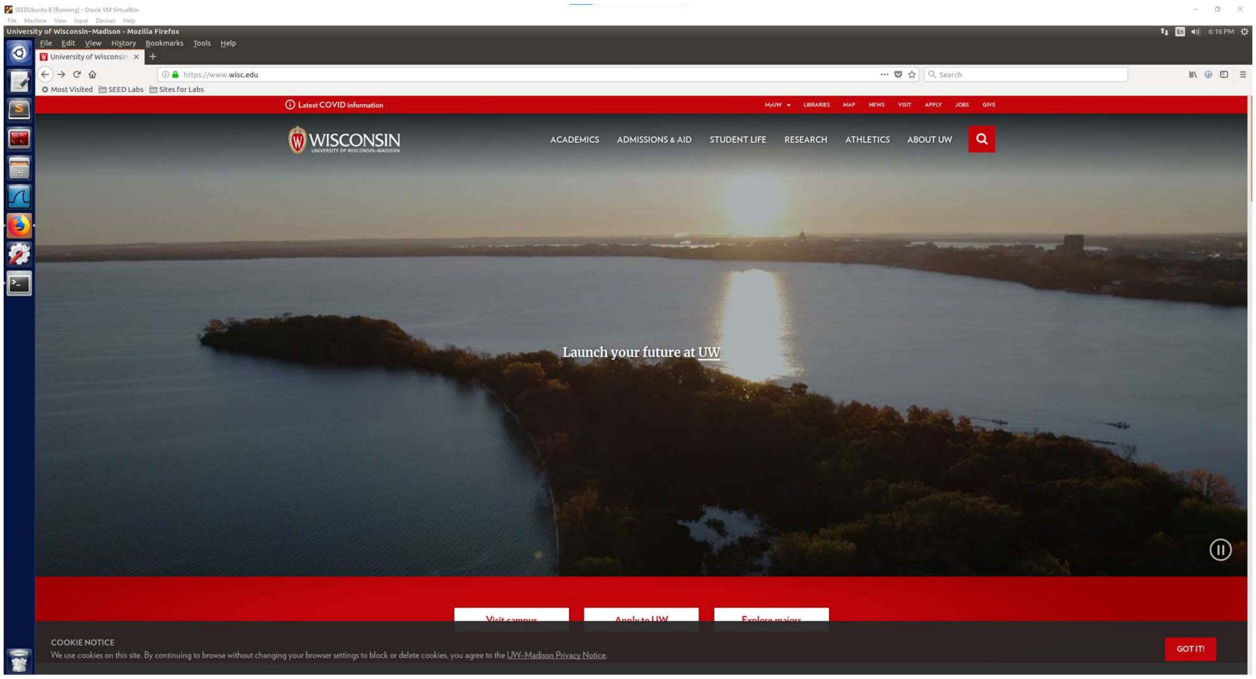
Featured stories, photo essays, and more by weather.com

Chill Winter Vibes

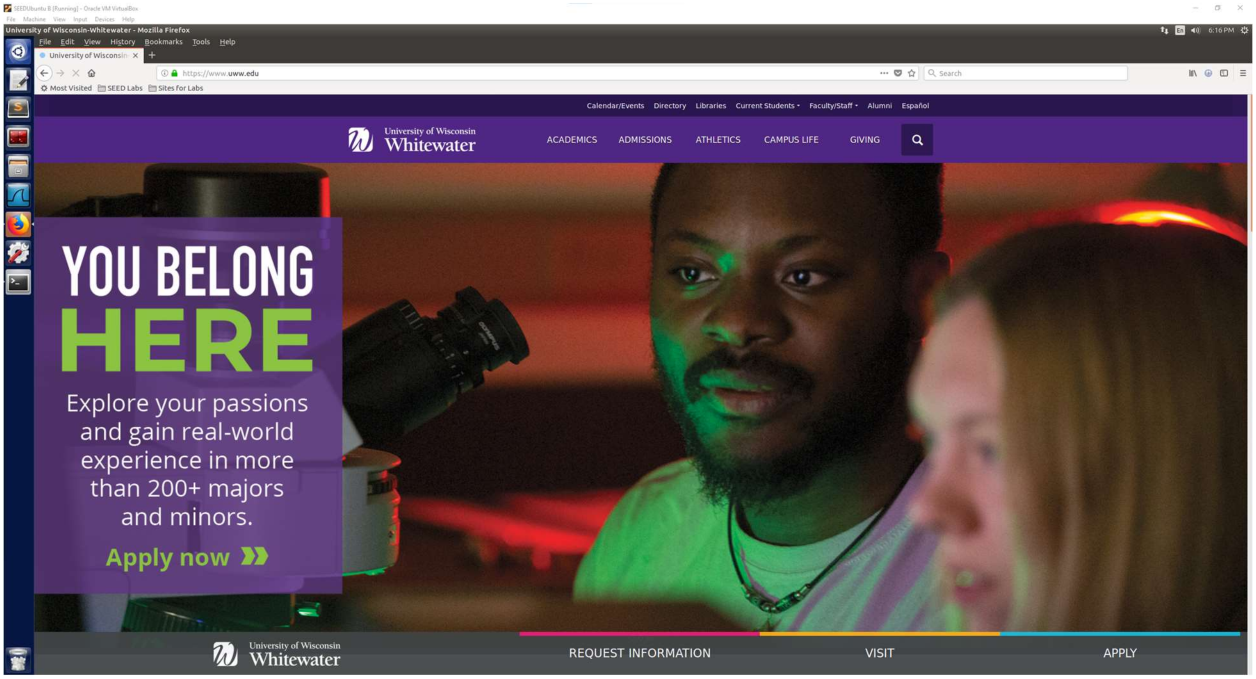
Latest News

Get The Weather Channel Premium Pro and Tripadvisor Plus

Lab 6-Part 2
Gunnar Yonker

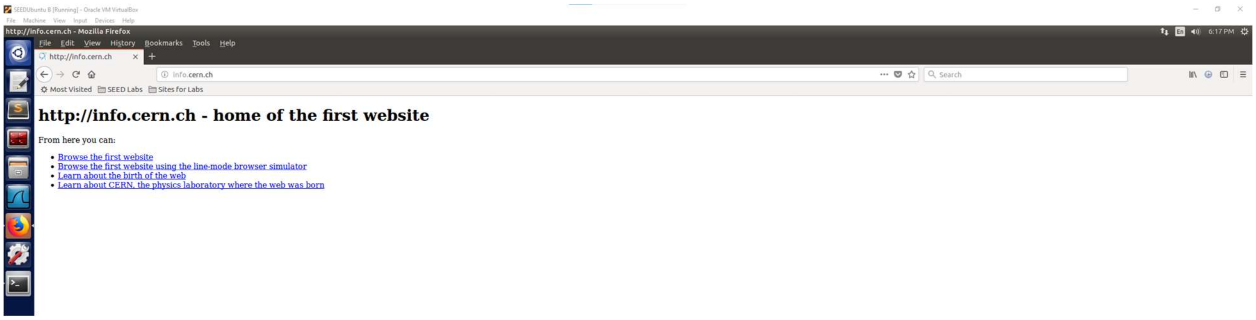


COOKIE NOTICE
We use cookies on this site. By continuing to browse without changing your browser settings to block or delete cookies, you agree to the UW–Madison Privacy Notice.



Lab 6-Part 2
Gunnar Yonker

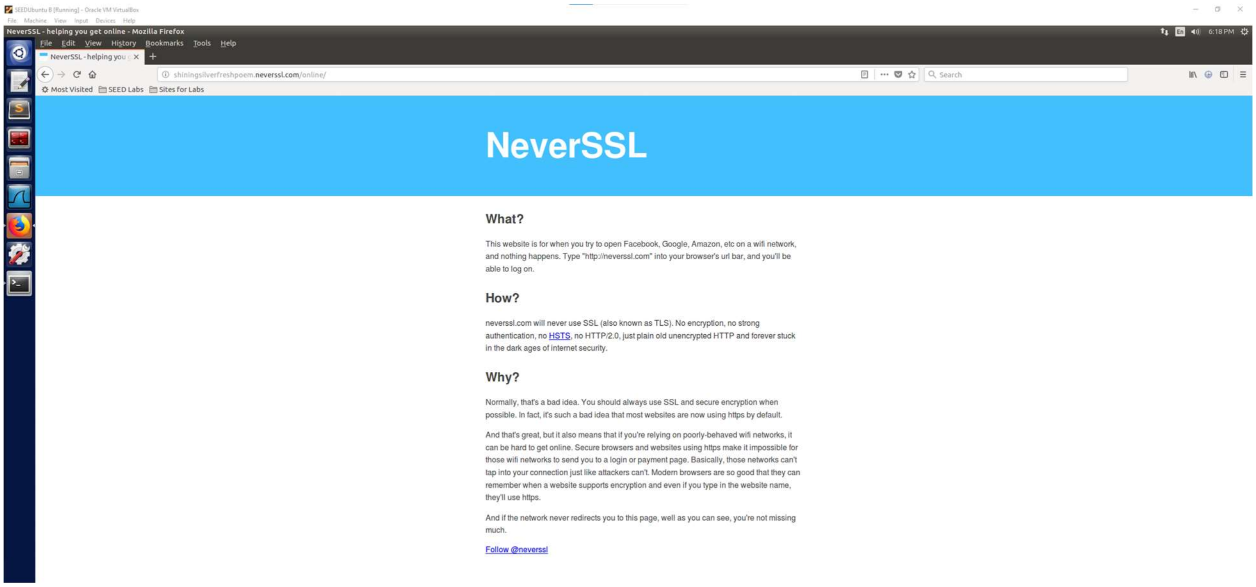
Browsing some http sites


SEEDUbuntu 8 [Running] - Oracle VM VirtualBox
http://info.cern.ch - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://info.cern.ch
info.cern.ch
Search
Most Visited
SEED Labs
Sites for Labs
6:17 PM

http://info.cern.ch - home of the first website

From here you can:

- Browse the first website
- Browse the first website using the line-mode browser simulator
- Learn about the birth of the web
- Learn about CERN, the physics laboratory where the web was born


SEEDUbuntu 8 [Running] - Oracle VM VirtualBox
NeverSSL - helping you get online - Mozilla Firefox
File Edit View History Bookmarks Tools Help
NeverSSL - helping you
shiningsilverfreshpoem.neverssl.com/online/
Search
Most Visited
SEED Labs
Sites for Labs
6:18 PM

NeverSSL

What?

This website is for when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's url bar, and you'll be able to log on.

How?

neverssl.com will never use SSL (also known as TLS). No encryption, no strong authentication, no HSTS, no HTTP/2.0, just plain old unencrypted HTTP and forever stuck in the dark ages of internet security.

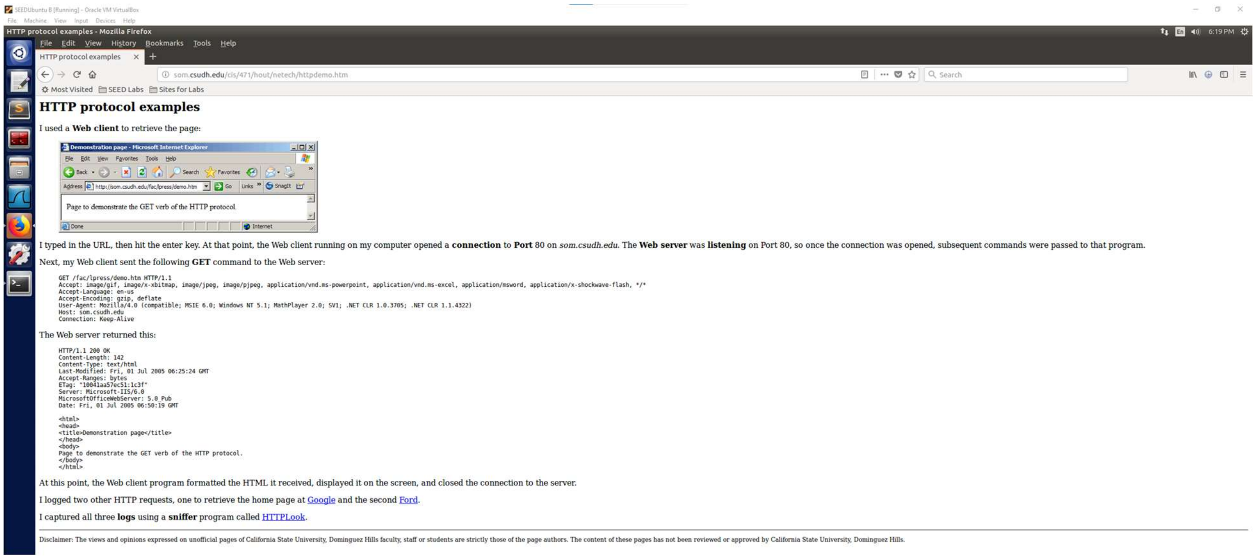
Why?

Normally, that's a bad idea. You should always use SSL and secure encryption when possible. In fact, it's such a bad idea that most websites are now using https by default.

And that's great, but it also means that if you're relying on poorly-behaved wifi networks, it can be hard to get online. Secure browsers and websites using https make it impossible for those wifi networks to send you to a login or payment page. Basically, those networks can't tap into your connection just like attackers can't. Modern browsers are so good that they can remember when a website supports encryption and even if you type in the website name, they'll use https.

And if the network never redirects you to this page, well as you can see, you're not missing much.

Follow @neverssl


SEEDUbuntu 8 [Running] - Oracle VM VirtualBox
HTTP protocol examples - Mozilla Firefox
File Edit View History Bookmarks Tools Help
HTTP protocol examples
som.csudh.edu/cis/471/hout/netech/httpdemo.htm
Search
Most Visited
SEED Labs
Sites for Labs
6:19 PM
Demonstration page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://som.csudh.edu/fac/lpress/demo.htm
Go
Links
SnagIt
Done
Internet

HTTP protocol examples

I used a **Web client** to retrieve the page:

Page to demonstrate the GET verb of the HTTP protocol.

I typed in the URL, then hit the enter key. At that point, the Web client running on my computer opened a **connection** to **Port** 80 on *som.csudh.edu*. The **Web server** was **listening** on Port 80, so once the connection was opened, subsequent commands were passed to that program.

Next, my Web client sent the following **GET** command to the Web server:

```
GET /fac/lpress/demo.htm HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, application/x-shockwave-flash, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; MathPlayer 2.0; SV1; .NET CLR 1.0.3705; .NET CLR 1.1.4322)
Host: som.csudh.edu
Connection: Keep-Alive
```

The Web server returned this:

```
HTTP/1.1 200 OK
Content-Length: 142
Content-Type: text/html
Last-Modified: Fri, 01 Jul 2005 06:25:24 GMT
Accept-Ranges: bytes
ETag: "10041aa57ec51:1c3f"
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
Date: Fri, 01 Jul 2005 06:50:19 GMT

<html>
<head>
<title>Demonstration page</title>
</head>
<body>
Page to demonstrate the GET verb of the HTTP protocol.
</body>
</html>
```

At this point, the Web client program formatted the HTML it received, displayed it on the screen, and closed the connection to the server.

I logged two other HTTP requests, one to retrieve the home page at Google and the second Ford.

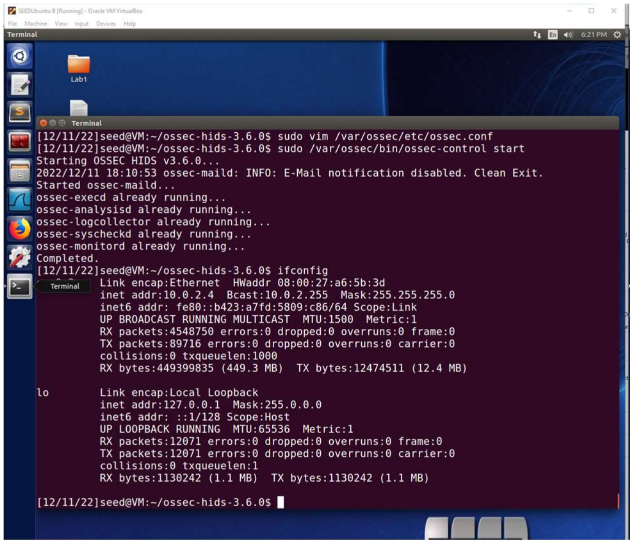
I captured all three **logs** using a **sniffer** program called HTTPLook.

Disclaimer: The views and opinions expressed on unofficial pages of California State University, Dominguez Hills faculty, staff or students are strictly those of the page authors. The content of these pages has not been reviewed or approved by California State University, Dominguez Hills.

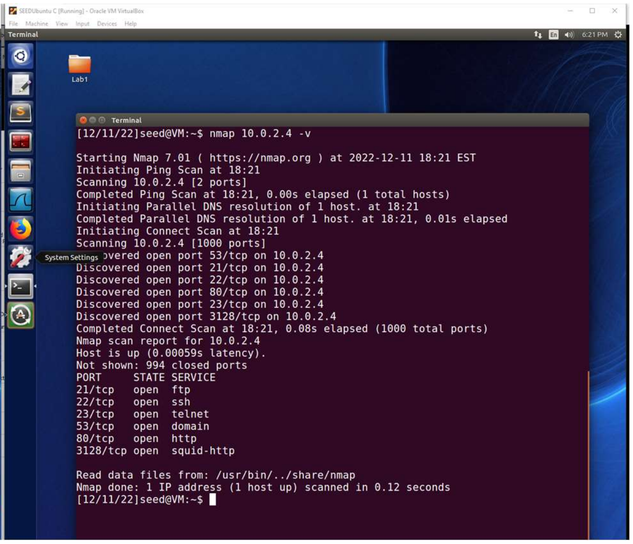
Lab 6-Part 2
Gunnar Yonker

Attack 1: nmap port scanning for open ports on OSSEC VM 10.0.2.4

nmap 10.0.2.4 -v


SEEDUbuntu B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
6:21 PM
Lab1
Terminal

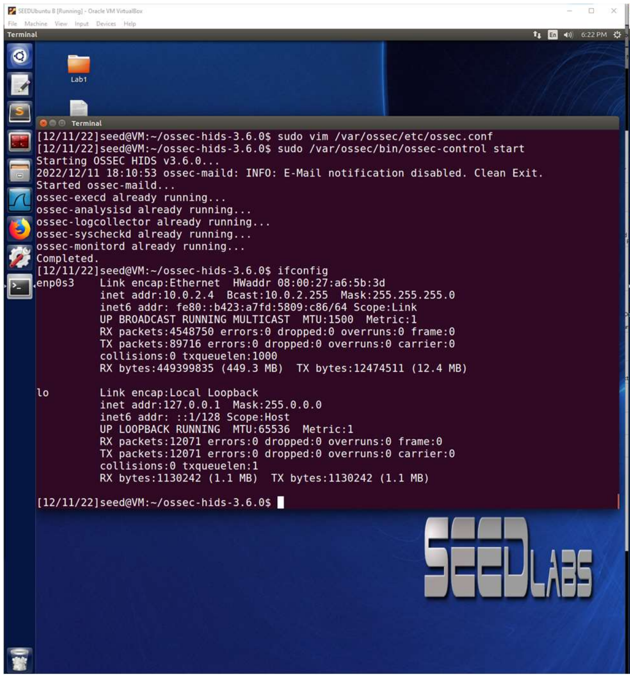
```
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo vim /var/ossec/etc/ossec.conf
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.6.0...
2022/12/11 18:10:53 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
ossec-execd already running...
ossec-analysisd already running...
ossec-logcollector already running...
ossec-syscheckd already running...
ossec-monitord already running...
Completed.
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ ifconfig
          Link encap:Ethernet  HWaddr 08:00:27:a6:5b:3d
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::b423:a7fd:5809:c86/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4548750 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89716 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:449399835 (449.3 MB)  TX bytes:12474511 (12.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12071 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12071 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1130242 (1.1 MB)  TX bytes:1130242 (1.1 MB)

[12/11/22]seed@VM:~/ossec-hids-3.6.0$
```


SEEDUbuntu C [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
6:21 PM
Lab1
Terminal
System Settings

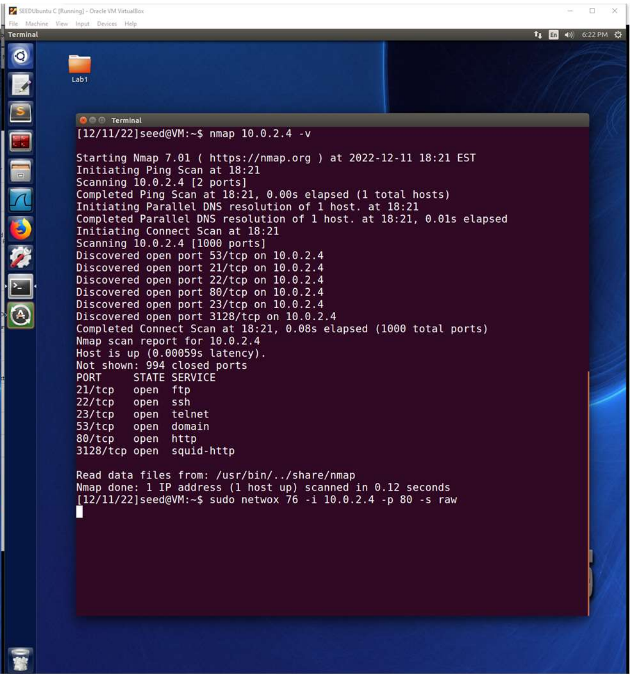
```
[12/11/22]seed@VM:~$ nmap 10.0.2.4 -v

Starting Nmap 7.01 ( https://nmap.org ) at 2022-12-11 18:21 EST
Initiating Ping Scan at 18:21
Scanning 10.0.2.4 [2 ports]
Completed Ping Scan at 18:21, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:21
Completed Parallel DNS resolution of 1 host. at 18:21, 0.01s elapsed
Initiating Connect Scan at 18:21
Scanning 10.0.2.4 [1000 ports]
   overed open port 53/tcp on 10.0.2.4
Discovered open port 21/tcp on 10.0.2.4
Discovered open port 22/tcp on 10.0.2.4
Discovered open port 80/tcp on 10.0.2.4
Discovered open port 23/tcp on 10.0.2.4
Discovered open port 3128/tcp on 10.0.2.4
Completed Connect Scan at 18:21, 0.08s elapsed (1000 total ports)
Nmap scan report for 10.0.2.4
Host is up (0.00059s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
3128/tcp open  squid-http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
[12/11/22]seed@VM:~$
```

Attack 2: SYN Flood Attack on OSSEC VM 10.0.2.4

sudo netwox 76 -i 10.0.2.4 -p 80 -s raw


SEEDUbuntu B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
6:22 PM
Lab1
SEEDLABS

```
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo vim /var/ossec/etc/ossec.conf
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.6.0...
2022/12/11 18:10:53 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
ossec-execd already running...
ossec-analysisd already running...
ossec-logcollector already running...
ossec-syscheckd already running...
ossec-monitord already running...
Completed.
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:a6:5b:3d
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::b423:a7fd:5809:c86/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4548750 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89716 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:449399835 (449.3 MB)  TX bytes:12474511 (12.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12071 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12071 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1130242 (1.1 MB)  TX bytes:1130242 (1.1 MB)

[12/11/22]seed@VM:~/ossec-hids-3.6.0$
```

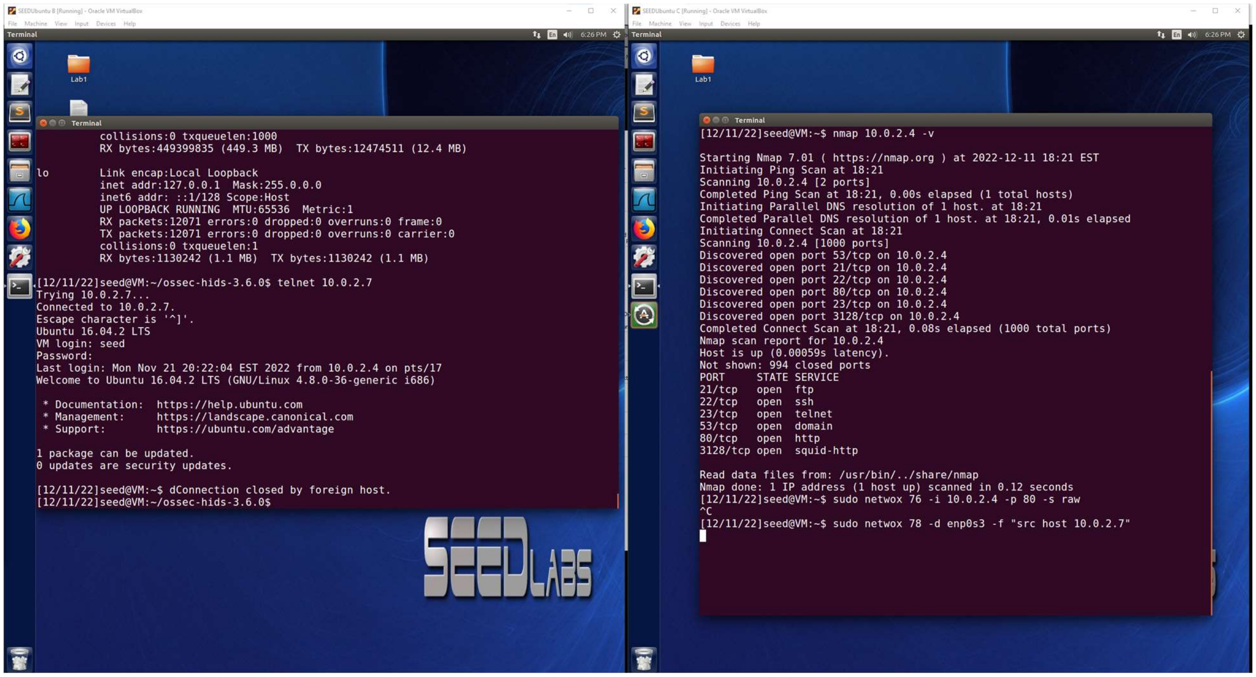

SEEDUbuntu C [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
6:21 PM
Lab1
Terminal

```
[12/11/22]seed@VM:~$ nmap 10.0.2.4 -v

Starting Nmap 7.01 ( https://nmap.org ) at 2022-12-11 18:21 EST
Initiating Ping Scan at 18:21
Scanning 10.0.2.4 [2 ports]
Completed Ping Scan at 18:21, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:21
Completed Parallel DNS resolution of 1 host. at 18:21, 0.01s elapsed
Initiating Connect Scan at 18:21
Scanning 10.0.2.4 [1000 ports]
Discovered open port 53/tcp on 10.0.2.4
Discovered open port 21/tcp on 10.0.2.4
Discovered open port 22/tcp on 10.0.2.4
Discovered open port 80/tcp on 10.0.2.4
Discovered open port 23/tcp on 10.0.2.4
Discovered open port 3128/tcp on 10.0.2.4
Completed Connect Scan at 18:21, 0.08s elapsed (1000 total ports)
Nmap scan report for 10.0.2.4
Host is up (0.00059s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
3128/tcp open  squid-http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
[12/11/22]seed@VM:~$ sudo netwox 76 -i 10.0.2.4 -p 80 -s raw
```

Lab 6-Part 2
Gunnar Yonker

Attack 3: TCP reset attack on OSSEC VM 10.0.2.4 when telnet to 10.0.2.7

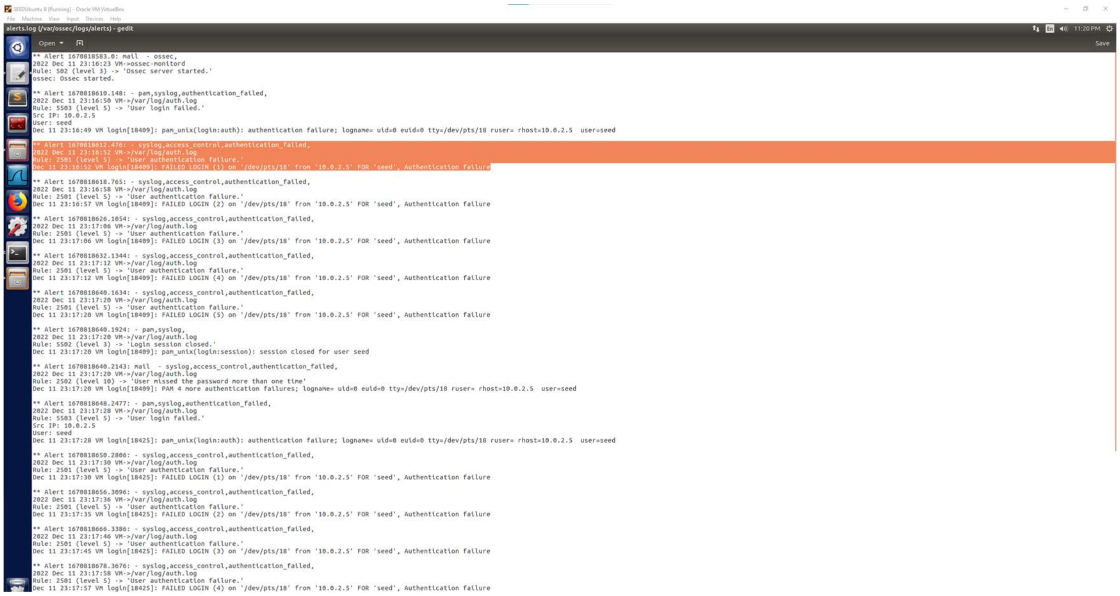
sudo netwox 78 -d enp0s3 -f “src host 10.0.2.7”



```
          collisions:0 txqueuelen:1000
          RX bytes:449399835 (449.3 MB)  TX bytes:12474511 (12.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12071 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12071 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1130242 (1.1 MB)  TX bytes:1130242 (1.1 MB)

[12/11/22]seed@VM:~/ossec-hids-3.6.0$ telnet 10.0.2.7
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Mon Nov 21 20:22:04 EST 2022 from 10.0.2.4 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

[12/11/22]seed@VM:~$ dConnection closed by foreign host.
[12/11/22]seed@VM:~/ossec-hids-3.6.0$
```

```
[12/11/22]seed@VM:~$ nmap 10.0.2.4 -v

Starting Nmap 7.01 ( https://nmap.org ) at 2022-12-11 18:21 EST
Initiating Ping Scan at 18:21
Scanning 10.0.2.4 [2 ports]
Completed Ping Scan at 18:21, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:21
Completed Parallel DNS resolution of 1 host. at 18:21, 0.01s elapsed
Initiating Connect Scan at 18:21
Scanning 10.0.2.4 [1000 ports]
Discovered open port 53/tcp on 10.0.2.4
Discovered open port 21/tcp on 10.0.2.4
Discovered open port 22/tcp on 10.0.2.4
Discovered open port 80/tcp on 10.0.2.4
Discovered open port 23/tcp on 10.0.2.4
Discovered open port 3128/tcp on 10.0.2.4
Completed Connect Scan at 18:21, 0.08s elapsed (1000 total ports)
Nmap scan report for 10.0.2.4
Host is up (0.00059s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
3128/tcp open  squid-http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
[12/11/22]seed@VM:~$ sudo netwox 76 -i 10.0.2.4 -p 80 -s raw
^C
[12/11/22]seed@VM:~$ sudo netwox 78 -d enp0s3 -f "src host 10.0.2.7"
```

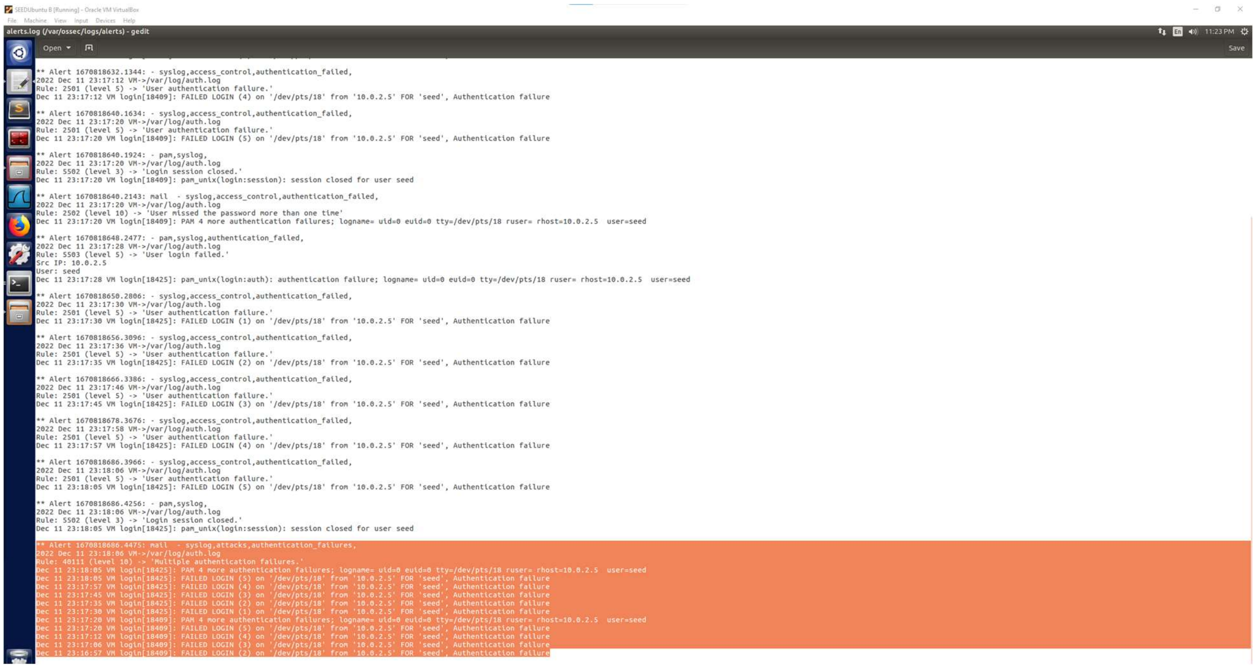
After stopping OSSEC and pulling up the alerts.log I was able to see the alerts for the incorrect password attempts. In the image below one of the attempts is highlighted where the Rule 2501 alert was issued labeled as “User authentication failure”, it also lists information such as the user that was trying to be accessed and then the attempt number that it was. After 5 attempts the connection session was closed and then re-opened for another 5 attempts. There is also information provided about the source IP address that was trying to access the user. This is a good informational log of the password attempt amounts, to what user, and where they came from.



```
** Alert 1670818583.0: mail  - ossec,
2022 Dec 11 23:16:23 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670818610.148: - pam,syslog,authentication_failed,
2022 Dec 11 23:16:50 VM->/var/log/auth.log
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: 10.0.2.5
User: seed
Dec 11 23:16:49 VM login[18409]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed

** Alert 1670818612.476: - syslog,access_control,authentication_failed,
2022 Dec 11 23:16:52 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:16:52 VM login[18409]: FAILED LOGIN (1) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818618.765: - syslog,access_control,authentication_failed,
2022 Dec 11 23:16:58 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:16:57 VM login[18409]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818626.1054: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:06 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:06 VM login[18409]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818632.1344: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:12 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:12 VM login[18409]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818640.1634: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:20 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:20 VM login[18409]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818640.1924: - pam,syslog,
2022 Dec 11 23:17:20 VM->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Dec 11 23:17:20 VM login[18409]: pam_unix(login:session): session closed for user seed

** Alert 1670818640.2143: mail  - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:20 VM->/var/log/auth.log
Rule: 2502 (level 10) -> 'User missed the password more than one time'
Dec 11 23:17:20 VM login[18409]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed

** Alert 1670818648.2477: - pam,syslog,authentication_failed,
2022 Dec 11 23:17:28 VM->/var/log/auth.log
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: 10.0.2.5
User: seed
Dec 11 23:17:28 VM login[18425]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed

** Alert 1670818650.2806: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:30 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:30 VM login[18425]: FAILED LOGIN (1) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818656.3096: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:36 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818666.3386: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:46 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818678.3676: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:58 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
```

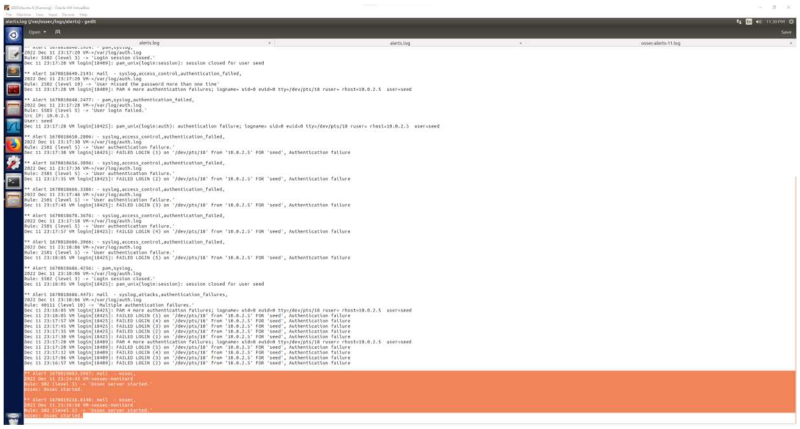
Lab 6-Part 2
Gunnar Yonker

After the alerts for each individual attempt there is also a log of Rule 40111 which is "Multiple authentication failures" which lists all of the attempts, from what IP address, and for what user they were trying to access. This compiles the attempts and would be a good indication of a brute password guessing attempt.


SEEDUbuntu B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
alerts.log (/var/ossec/logs/alerts) - gedit
Open
Save
11:23 PM

```
** Alert 1670818632.1344: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:12 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:12 VM login[18409]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818640.1634: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:20 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:20 VM login[18409]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818640.1924: - pam,syslog,
2022 Dec 11 23:17:20 VM->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Dec 11 23:17:20 VM login[18409]: pam_unix(login:session): session closed for user seed

** Alert 1670818640.2143: mail  - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:20 VM->/var/log/auth.log
Rule: 2502 (level 10) -> 'User missed the password more than one time'
Dec 11 23:17:20 VM login[18409]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed

** Alert 1670818648.2477: - pam,syslog,authentication_failed,
2022 Dec 11 23:17:28 VM->/var/log/auth.log
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: 10.0.2.5
User: seed
Dec 11 23:17:28 VM login[18425]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed

** Alert 1670818650.2806: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:30 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:30 VM login[18425]: FAILED LOGIN (1) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818656.3096: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:36 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818666.3386: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:46 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818678.3676: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:58 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818686.3966: - syslog,access_control,authentication_failed,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:18:05 VM login[18425]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818686.4256: - pam,syslog,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Dec 11 23:18:05 VM login[18425]: pam_unix(login:session): session closed for user seed

** Alert 1670818686.4475: mail  - syslog,attacks,authentication_failures,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 40111 (level 10) -> 'Multiple authentication failures.'
Dec 11 23:18:05 VM login[18425]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed
Dec 11 23:18:05 VM login[18425]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:30 VM login[18425]: FAILED LOGIN (1) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:20 VM login[18409]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed
Dec 11 23:17:20 VM login[18409]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:12 VM login[18409]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:06 VM login[18409]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:16:57 VM login[18409]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
```

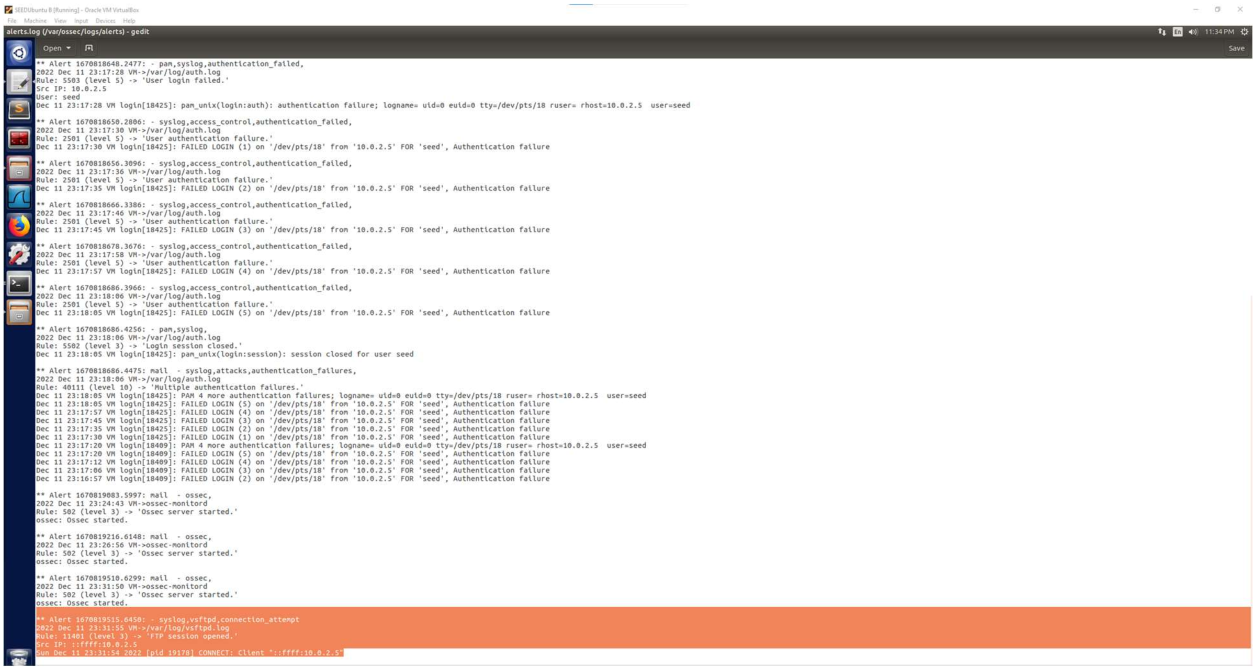
Next up was browsing the https and http websites. In the log file I did not see any alerts come up from the https browsing or the http browsing, I was not sure if this was an issue where nothing was being logged due to an error with the browsing or OSSEC not running, but after a second and third attempt of browsing the same websites and clicking on a few more links on the websites themselves there still was no updated information in the alerts.log file. The reasons for this that I can think of would be that there were no level 3 or higher alerts coming from the http or https websites, maybe the alerts would have been triggered at level 1 or 2 so they are not showing up. Or it is also possible that there are just simply no alerts being detected by OSSEC from the websites either due to configuration of OSSEC or that there is no malicious intent coming from the websites to be alerted to. Highlighted below is the second and third attempt of re-starting OSSEC and browsing through the websites to see if there was an issue the first try.


SEEDUbuntu B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
alerts.log (/var/ossec/logs/alerts) - gedit
Open
Save
alerts.log
alerts.log
ossec-alerts-11.log

```
2022 Dec 11 23:17:20 VM->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Dec 11 23:17:20 VM login[18409]: pam_unix(login:session): session closed for user seed

** Alert 1670818640.2143: mail  - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:20 VM->/var/log/auth.log
Rule: 2502 (level 10) -> 'User missed the password more than one time'
Dec 11 23:17:20 VM login[18409]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed

** Alert 1670818648.2477: - pam,syslog,authentication_failed,
2022 Dec 11 23:17:28 VM->/var/log/auth.log
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: 10.0.2.5
User: seed
Dec 11 23:17:28 VM login[18425]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed

** Alert 1670818650.2806: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:30 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:30 VM login[18425]: FAILED LOGIN (1) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818656.3096: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:36 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818666.3386: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:46 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818678.3676: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:58 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818686.3966: - syslog,access_control,authentication_failed,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:18:05 VM login[18425]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818686.4256: - pam,syslog,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Dec 11 23:18:05 VM login[18425]: pam_unix(login:session): session closed for user seed

** Alert 1670818686.4475: mail  - syslog,attacks,authentication_failures,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 40111 (level 10) -> 'Multiple authentication failures.'
Dec 11 23:18:05 VM login[18425]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed
Dec 11 23:18:05 VM login[18425]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:30 VM login[18425]: FAILED LOGIN (1) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:20 VM login[18409]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed
Dec 11 23:17:20 VM login[18409]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:12 VM login[18409]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:06 VM login[18409]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:16:57 VM login[18409]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670819083.5957: mail  - ossec,
2022 Dec 11 23:24:43 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819216.8148: mail  - ossec,
2022 Dec 11 23:26:56 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.
```

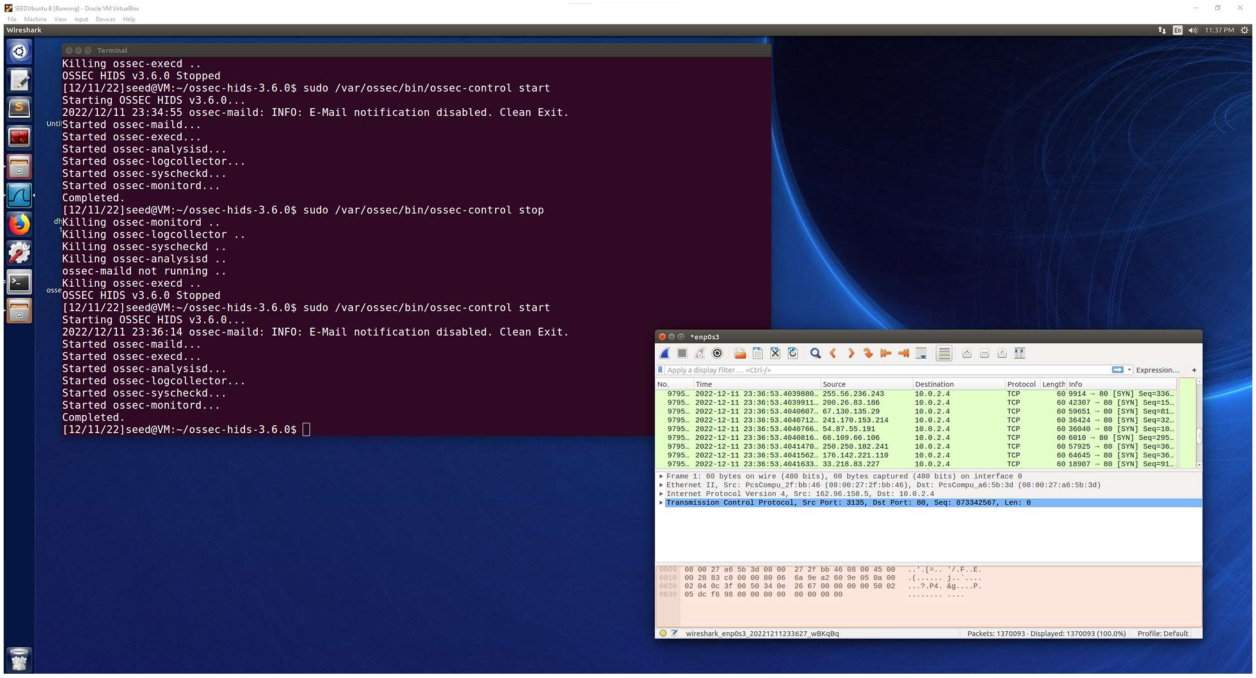
Lab 6-Part 2
Gunnar Yonker

Next was the nmap port scan while OSSEC was running. Looking at the log file there was a new addition of a level 3 alert Rule 11401 listed as a “FTP session opened”. The source IP is also shown here from the VM that ran the nmap scan on the OSSEC VM, from the logged information that is the only item that I can directly attribute to the port scanning attack is that the source of the attack was 10.0.2.5 and that it was a connection attempt.


SEEDUbuntu B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
alerts.log (/var/ossec/logs/alerts) - gedit
Open
11:34 PM
Save

```
** Alert 1670818648.2477: - pam,syslog,authentication_failed,
2022 Dec 11 23:17:28 VM->/var/log/auth.log
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: 10.0.2.5
User: seed
Dec 11 23:17:28 VM login[18425]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed

** Alert 1670818650.2806: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:30 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:30 VM login[18425]: FAILED LOGIN (1) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818656.3096: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:36 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818666.3386: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:46 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818678.3676: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:58 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818686.3966: - syslog,access_control,authentication_failed,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:18:05 VM login[18425]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818686.4256: - pam,syslog,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Dec 11 23:18:05 VM login[18425]: pam_unix(login:session): session closed for user seed

** Alert 1670818686.4475: mail  - syslog,attacks,authentication_failures,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 40111 (level 10) -> 'Multiple authentication failures.'
Dec 11 23:18:05 VM login[18425]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed
Dec 11 23:18:05 VM login[18425]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:30 VM login[18425]: FAILED LOGIN (1) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:20 VM login[18409]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed
Dec 11 23:17:20 VM login[18409]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:12 VM login[18409]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:06 VM login[18409]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:16:57 VM login[18409]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670819083.5997: mail  - ossec,
2022 Dec 11 23:24:43 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819216.6148: mail  - ossec,
2022 Dec 11 23:26:56 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819510.6299: mail  - ossec,
2022 Dec 11 23:31:50 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819515.6450: - syslog,vsftpd,connection_attempt
2022 Dec 11 23:31:55 VM->/var/log/vsftpd.log
Rule: 11401 (level 3) -> 'FTP session opened.'
Src IP: ::ffff:10.0.2.5
Sun Dec 11 23:31:54 2022 [pid 19178] CONNECT: Client "::ffff:10.0.2.5"
```

Next was the SYN Flood attack, to ensure that the attack was successful while OSSEC was running I also had Wireshark open as shown below to see that the SYN Flood attack was successful coming from spoofed IP address to port 80.

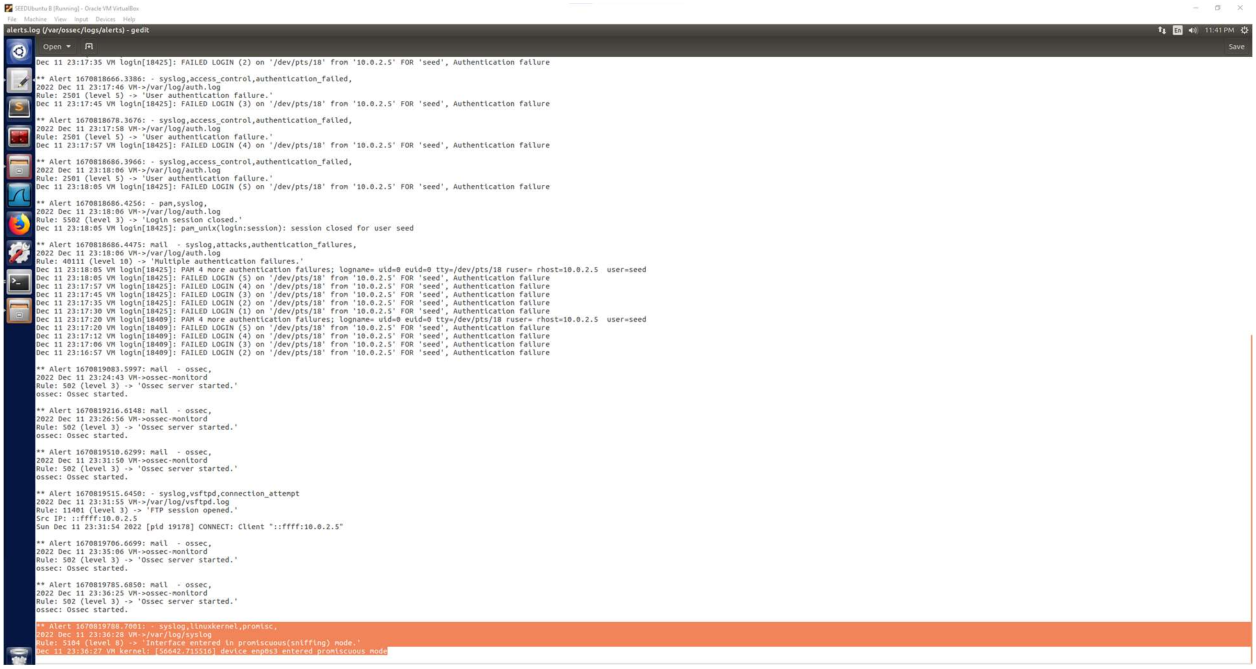

SEEDUbuntu B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark
11:37 PM
Terminal
*enp0s3
Apply a display filter … <Ctrl-/>
Expression…

```
Killing ossec-execd ..
OSSEC HIDS v3.6.0 Stopped
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.6.0...
2022/12/11 23:34:55 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo /var/ossec/bin/ossec-control stop
Killing ossec-monitord ..
Killing ossec-logcollector ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
ossec-maild not running ..
Killing ossec-execd ..
OSSEC HIDS v3.6.0 Stopped
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.6.0...
2022/12/11 23:36:14 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ 
```

```
No.    Time                          Source            Destination  Protocol  Length  Info
 9795… 2022-12-11 23:36:53.4039880… 255.56.236.243    10.0.2.4     TCP       60 9914 → 80 [SYN] Seq=336…
 9795… 2022-12-11 23:36:53.4039911… 200.26.83.186     10.0.2.4     TCP       60 42307 → 80 [SYN] Seq=15…
 9795… 2022-12-11 23:36:53.4040607… 67.130.135.29     10.0.2.4     TCP       60 59651 → 80 [SYN] Seq=81…
 9795… 2022-12-11 23:36:53.4040712… 241.170.153.214   10.0.2.4     TCP       60 36424 → 80 [SYN] Seq=32…
 9795… 2022-12-11 23:36:53.4040766… 54.87.55.191      10.0.2.4     TCP       60 36040 → 80 [SYN] Seq=10…
 9795… 2022-12-11 23:36:53.4040816… 66.109.66.106     10.0.2.4     TCP       60 6010 → 80 [SYN] Seq=295…
 9795… 2022-12-11 23:36:53.4041470… 250.250.182.241   10.0.2.4     TCP       60 57925 → 80 [SYN] Seq=36…
 9795… 2022-12-11 23:36:53.4041562… 176.142.221.110   10.0.2.4     TCP       60 64645 → 80 [SYN] Seq=36…
 9795… 2022-12-11 23:36:53.4041633… 33.218.83.227     10.0.2.4     TCP       60 18907 → 80 [SYN] Seq=91…

▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_2f:bb:46 (08:00:27:2f:bb:46), Dst: PcsCompu_a6:5b:3d (08:00:27:a6:5b:3d)
▸ Internet Protocol Version 4, Src: 162.96.158.5, Dst: 10.0.2.4
▸ Transmission Control Protocol, Src Port: 3135, Dst Port: 80, Seq: 873342567, Len: 0

0000  08 00 27 a6 5b 3d 08 00  27 2f bb 46 08 00 45 00   ..'.[=.. '/.F..E.
0010  00 28 83 c8 00 00 80 06  6a 9e a2 60 9e 05 0a 00   .(...... j..`....
0020  02 04 0c 3f 00 50 34 0e  26 67 00 00 00 00 50 02   ...?.P4. &g....P.
0030  05 dc f6 98 00 00 00 00  00 00 00 00               ........ ....

wireshark_enp0s3_20221211233627_wBKqBq    Packets: 1370093 · Displayed: 1370093 (100.0%)    Profile: Default
```

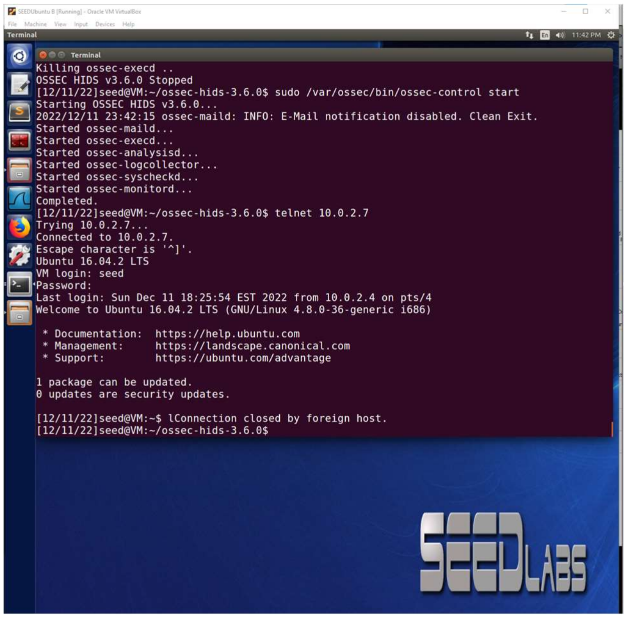
Lab 6-Part 2
Gunnar Yonker

In the alerts.log file the only new entry that I found was that of a level 8 alert with Rule 5104 labeled as "Interface entered in promiscuous(sniffing) mode". This alert I think would be attributed to the Wireshark program being opened and sniffing on enp0s3, which is a good bit of knowledge because the log would show if there was a sniffing program open on the user's system that the user may not know about in the event that there was an undetected intrusion, and an attacker was using this system to sniff packets on the subnet. Other than that, there was no additional alert showing that a SYN Flood attack was taking place, which Wireshark confirms that the attack was successful. I found it interesting that the SYN Flood was not detected, but that the Wireshark sniffing on enp0s3 was alerted at a very high level.

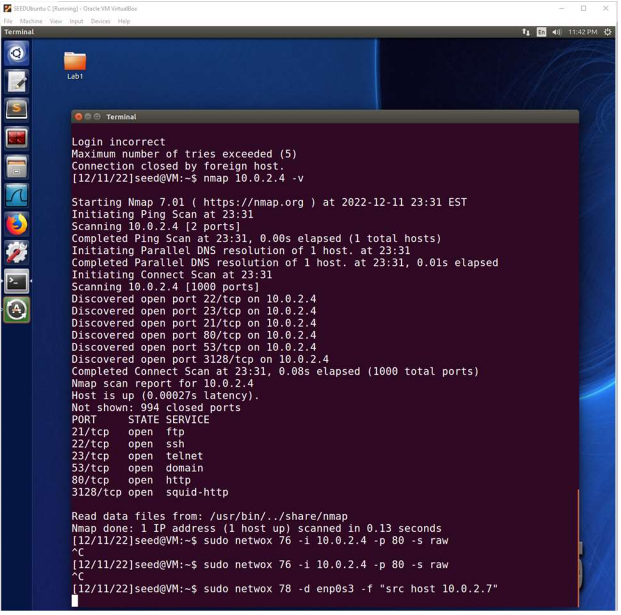

SEEDUbuntu B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
alerts.log (/var/ossec/logs/alerts) - gedit
Open
Save
11:41 PM

```
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818666.3386: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:46 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818678.3676: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:58 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818686.3966: - syslog,access_control,authentication_failed,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:18:05 VM login[18425]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818686.4256: - pam,syslog,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Dec 11 23:18:05 VM login[18425]: pam_unix(login:session): session closed for user seed

** Alert 1670818686.4475: mail  - syslog,attacks,authentication_failures,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 40111 (level 10) -> 'Multiple authentication failures.'
Dec 11 23:18:05 VM login[18425]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed
Dec 11 23:18:05 VM login[18425]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:30 VM login[18425]: FAILED LOGIN (1) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:20 VM login[18409]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed
Dec 11 23:17:20 VM login[18409]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:12 VM login[18409]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:06 VM login[18409]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:16:57 VM login[18409]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670819083.5997: mail  - ossec,
2022 Dec 11 23:24:43 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819216.6148: mail  - ossec,
2022 Dec 11 23:26:56 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819510.6299: mail  - ossec,
2022 Dec 11 23:31:50 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819515.6450: - syslog,vsftpd,connection_attempt
2022 Dec 11 23:31:55 VM->/var/log/vsftpd.log
Rule: 11401 (level 3) -> 'FTP session opened.'
Src IP: ::ffff:10.0.2.5
Sun Dec 11 23:31:54 2022 [pid 19178] CONNECT: Client "::ffff:10.0.2.5"

** Alert 1670819706.6699: mail  - ossec,
2022 Dec 11 23:35:06 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819785.6850: mail  - ossec,
2022 Dec 11 23:36:25 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819788.7001: - syslog,linuxkernel,promisc,
2022 Dec 11 23:36:28 VM->/var/log/syslog
Rule: 5104 (level 8) -> 'Interface entered in promiscuous(sniffing) mode.'
Dec 11 23:36:27 VM kernel: [56642.715516] device enp0s3 entered promiscuous mode
```

The third attack was a TCP reset attack on the OSSEC VM's telnet connection to 10.0.2.7, as seen below the attack was successful in closing the OSSEC VM's telnet connection.


SEEDUbuntu B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
11:42 PM
Terminal

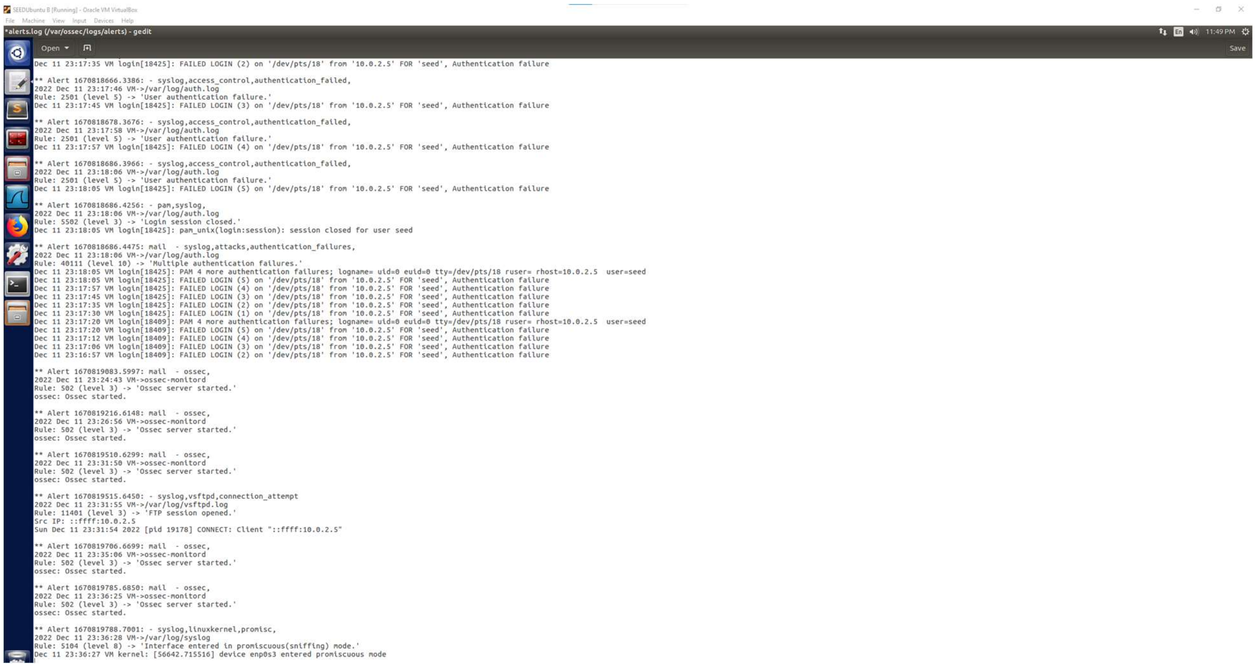
```
Killing ossec-execd ..
OSSEC HIDS v3.6.0 Stopped
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ sudo /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.6.0...
2022/12/11 23:42:15 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
[12/11/22]seed@VM:~/ossec-hids-3.6.0$ telnet 10.0.2.7
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Dec 11 18:25:54 EST 2022 from 10.0.2.4 on pts/4
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

[12/11/22]seed@VM:~$ lConnection closed by foreign host.
[12/11/22]seed@VM:~/ossec-hids-3.6.0$
```


SEEDUbuntu C [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
11:42 PM
Lab1
Terminal

```
Login incorrect
Maximum number of tries exceeded (5)
Connection closed by foreign host.
[12/11/22]seed@VM:~$ nmap 10.0.2.4 -v

Starting Nmap 7.01 ( https://nmap.org ) at 2022-12-11 23:31 EST
Initiating Ping Scan at 23:31
Scanning 10.0.2.4 [2 ports]
Completed Ping Scan at 23:31, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:31
Completed Parallel DNS resolution of 1 host. at 23:31, 0.01s elapsed
Initiating Connect Scan at 23:31
Scanning 10.0.2.4 [1000 ports]
Discovered open port 22/tcp on 10.0.2.4
Discovered open port 23/tcp on 10.0.2.4
Discovered open port 21/tcp on 10.0.2.4
Discovered open port 80/tcp on 10.0.2.4
Discovered open port 53/tcp on 10.0.2.4
Discovered open port 3128/tcp on 10.0.2.4
Completed Connect Scan at 23:31, 0.08s elapsed (1000 total ports)
Nmap scan report for 10.0.2.4
Host is up (0.00027s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
3128/tcp open  squid-http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
[12/11/22]seed@VM:~$ sudo netwox 76 -i 10.0.2.4 -p 80 -s raw
^C
[12/11/22]seed@VM:~$ sudo netwox 76 -i 10.0.2.4 -p 80 -s raw
^C
[12/11/22]seed@VM:~$ sudo netwox 78 -d enp0s3 -f "src host 10.0.2.7"
```

Lab 6-Part 2
Gunnar Yonker

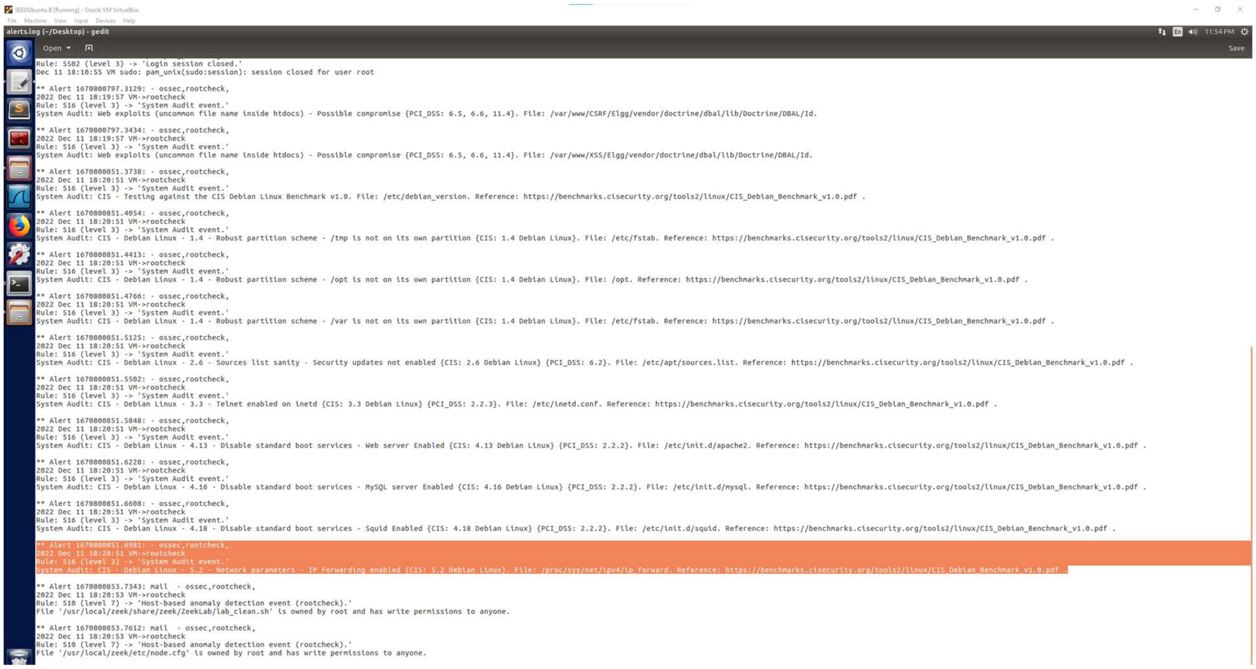
It appears that this attack, although successful was also not captured as an alert by OSSEC. There are no new alerts located in the log since the Wireshark alert. I think that it is possible that this could be considered lower than a 3 in severity which would cause this type of attack to not be logged with the current configurations of OSSEC on this VM. TCP Reset closed the telnet connection of the victim to the server but did not inflict an attack like a denial of service, the user would be able to telnet again into the server unless a TCP Reset attack was still taking place. The TCP Reset attack was successful as seen above, but it is not located in the log. The image below shows that there are no new logged alert entries.


SEEDUbuntu B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*alerts.log (/var/ossec/logs/alerts) - gedit
11:49 PM
Open
Save

```
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818666.3386: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:46 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818678.3676: - syslog,access_control,authentication_failed,
2022 Dec 11 23:17:58 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818686.3966: - syslog,access_control,authentication_failed,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Dec 11 23:18:05 VM login[18425]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670818686.4256: - pam,syslog,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Dec 11 23:18:05 VM login[18425]: pam_unix(login:session): session closed for user seed

** Alert 1670818686.4475: mail  - syslog,attacks,authentication_failures,
2022 Dec 11 23:18:06 VM->/var/log/auth.log
Rule: 40111 (level 10) -> 'Multiple authentication failures.'
Dec 11 23:18:05 VM login[18425]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed
Dec 11 23:18:05 VM login[18425]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:57 VM login[18425]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:45 VM login[18425]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:35 VM login[18425]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:30 VM login[18425]: FAILED LOGIN (1) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:20 VM login[18409]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=/dev/pts/18 ruser= rhost=10.0.2.5  user=seed
Dec 11 23:17:20 VM login[18409]: FAILED LOGIN (5) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:12 VM login[18409]: FAILED LOGIN (4) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:17:06 VM login[18409]: FAILED LOGIN (3) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure
Dec 11 23:16:57 VM login[18409]: FAILED LOGIN (2) on '/dev/pts/18' from '10.0.2.5' FOR 'seed', Authentication failure

** Alert 1670819083.5997: mail  - ossec,
2022 Dec 11 23:24:43 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819216.6148: mail  - ossec,
2022 Dec 11 23:26:56 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819510.6299: mail  - ossec,
2022 Dec 11 23:31:50 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819515.6450: - syslog,vsftpd,connection_attempt
2022 Dec 11 23:31:55 VM->/var/log/vsftpd.log
Rule: 11401 (level 3) -> 'FTP session opened.'
Src IP: ::ffff:10.0.2.5
Sun Dec 11 23:31:54 2022 [pid 19178] CONNECT: Client "::ffff:10.0.2.5"

** Alert 1670819706.6699: mail  - ossec,
2022 Dec 11 23:35:06 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819785.6850: mail  - ossec,
2022 Dec 11 23:36:25 VM->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1670819788.7001: - syslog,linuxkernel,promisc,
2022 Dec 11 23:36:28 VM->/var/log/syslog
Rule: 5104 (level 8) -> 'Interface entered in promiscuous(sniffing) mode.'
Dec 11 23:36:27 VM kernel: [56642.715516] device enp0s3 entered promiscuous mode
```

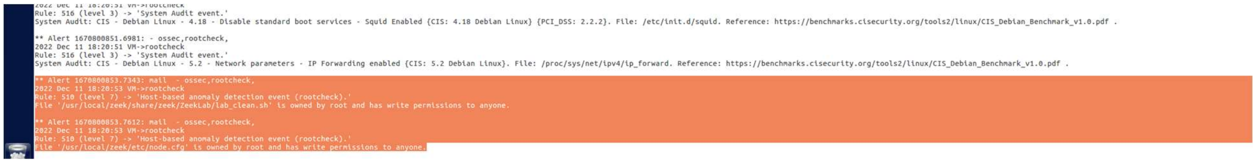
Lab 6-Part 2
Gunnar Yonker

I had left OSSEC running previously while I was at my indoor soccer game and wanted to point out something interesting I had found in the alerts.log file that does not attribute to the attacks or browsing, but that was interesting. There were a series of Rule 516 alerts labeled as “System Audit event”. These pertained to the rootcheck part of OSSEC which I remembered seeing during the setup video as being included in our local installation of OSSEC on this VM. There were a variety of system audit categories shown such as Web exploits with possible compromises, Robust partition schemes with directories not being on its own partition and Disable standard boot services. In the image below there is also a highlighted alert that shows that IP Forwarding is enabled which would trace back to a previous lab where for purposes of testing we had enabled IP forwarding and OSSEC was able to determine that it was still enabled and could be a possible vulnerability leading to abnormal events.


SEEDUbuntu B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
alerts.log (~/Desktop) - gedit
Open
Save
En
11:54 PM

```
Rule: 5502 (level 3) -> 'Login session closed.'
Dec 11 18:10:55 VM sudo: pam_unix(sudo:session): session closed for user root

** Alert 1670800797.3129: - ossec,rootcheck,
2022 Dec 11 18:19:57 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: Web exploits (uncommon file name inside htdocs) - Possible compromise {PCI_DSS: 6.5, 6.6, 11.4}. File: /var/www/CSRF/Elgg/vendor/doctrine/dbal/lib/Doctrine/DBAL/Id.

** Alert 1670800797.3434: - ossec,rootcheck,
2022 Dec 11 18:19:57 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: Web exploits (uncommon file name inside htdocs) - Possible compromise {PCI_DSS: 6.5, 6.6, 11.4}. File: /var/www/XSS/Elgg/vendor/doctrine/dbal/lib/Doctrine/DBAL/Id.

** Alert 1670800851.3738: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Testing against the CIS Debian Linux Benchmark v1.0. File: /etc/debian_version. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800851.4054: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 1.4 - Robust partition scheme - /tmp is not on its own partition {CIS: 1.4 Debian Linux}. File: /etc/fstab. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800851.4413: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 1.4 - Robust partition scheme - /opt is not on its own partition {CIS: 1.4 Debian Linux}. File: /opt. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800851.4766: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 1.4 - Robust partition scheme - /var is not on its own partition {CIS: 1.4 Debian Linux}. File: /etc/fstab. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800851.5125: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 2.6 - Sources list sanity - Security updates not enabled {CIS: 2.6 Debian Linux} {PCI_DSS: 6.2}. File: /etc/apt/sources.list. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800851.5502: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 3.3 - Telnet enabled on inetd {CIS: 3.3 Debian Linux} {PCI_DSS: 2.2.3}. File: /etc/inetd.conf. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800851.5848: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 4.13 - Disable standard boot services - Web server Enabled {CIS: 4.13 Debian Linux} {PCI_DSS: 2.2.2}. File: /etc/init.d/apache2. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800851.6228: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 4.16 - Disable standard boot services - MySQL server Enabled {CIS: 4.16 Debian Linux} {PCI_DSS: 2.2.2}. File: /etc/init.d/mysql. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800851.6608: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 4.18 - Disable standard boot services - Squid Enabled {CIS: 4.18 Debian Linux} {PCI_DSS: 2.2.2}. File: /etc/init.d/squid. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800851.6981: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 5.2 - Network parameters - IP Forwarding enabled {CIS: 5.2 Debian Linux}. File: /proc/sys/net/ipv4/ip_forward. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800853.7343: mail  - ossec,rootcheck,
2022 Dec 11 18:20:53 VM->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
File '/usr/local/zeek/share/zeek/ZeekLab/lab_clean.sh' is owned by root and has write permissions to anyone.

** Alert 1670800853.7612: mail  - ossec,rootcheck,
2022 Dec 11 18:20:53 VM->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
File '/usr/local/zeek/etc/node.cfg' is owned by root and has write permissions to anyone.
```

Also at the bottom of the above image there were two Rule 510 alerts labeled as “Host-based anomaly detection event” that pertained to two files in the zeek folder that is owned by root and has write permissions to anyone which OSSEC determined to be an anomaly and alerted it at a level 7.



```
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 4.18 - Disable standard boot services - Squid Enabled {CIS: 4.18 Debian Linux} {PCI_DSS: 2.2.2}. File: /etc/init.d/squid. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800851.6981: - ossec,rootcheck,
2022 Dec 11 18:20:51 VM->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 5.2 - Network parameters - IP Forwarding enabled {CIS: 5.2 Debian Linux}. File: /proc/sys/net/ipv4/ip_forward. Reference: https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .

** Alert 1670800853.7343: mail  - ossec,rootcheck,
2022 Dec 11 18:20:53 VM->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
File '/usr/local/zeek/share/zeek/ZeekLab/lab_clean.sh' is owned by root and has write permissions to anyone.

** Alert 1670800853.7612: mail  - ossec,rootcheck,
2022 Dec 11 18:20:53 VM->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
File '/usr/local/zeek/etc/node.cfg' is owned by root and has write permissions to anyone.
```

Lab 6-Part 2
Gunnar Yonker

My takeaway from this lab with OSSEC is that OSSEC was able to provide a lot of information especially on the brute password attempts in a clean log setup. However, I was surprised that an attack such as a SYN Flood attack was not logged in the alerts.log file which could be due to a user error if it should've been logged but I was able to determine that OSSEC was running, and that the SYN Flood attack was successful through the use of Wireshark. This also lead to a new discovery that Wireshark sniffing packets was detected and alerted through OSSEC which has its own use to know that a sniffing program was running. It was also interesting to see what the rootcheck part of OSSEC had detected and alerted about such as the IP Forwarding still being enabled on this VM and highlighting that as a possible vulnerability. I think that it would be interesting to learn more about the capabilities of OSSEC such as what level would be associated with specific more severe attacks and if OSSEC would be able to detect and log them.