Solving nitroba pcap with Zeek – Sean Yarkoni

Solving the challenge nitroba with Zeek on Ubuntu-20.04.2-live-server-amd64.

The challenges are:

1) Map out the Nitroba dorm room network.

2) Find who sent email to lilytuckrige@yahoo.com

2.A) Look for a TCP flow that includes the hostile message

2.B) Find information that can tie that message to a particular web browser.

3) Identify the other TCP connections that belong to the attacker

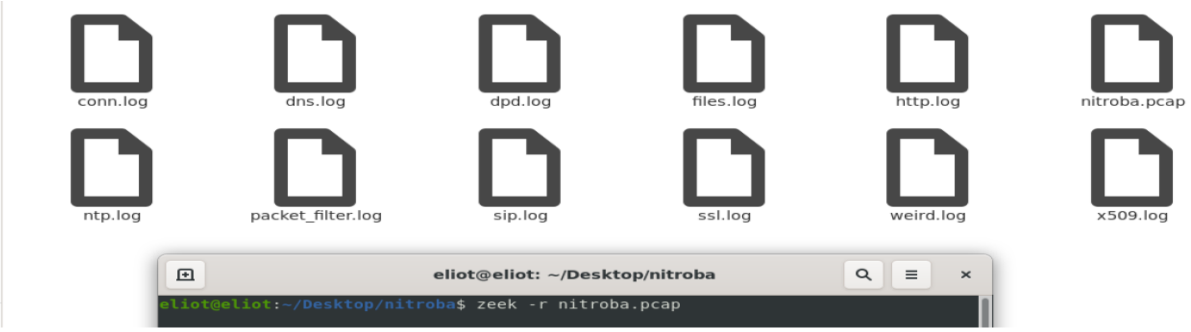
4) Find information in one of those TCP connections that IDs the attacker.

Pcap file working with:

nitroba.pcap

Solution:

In order for us to start we need Zeek to read the PCAP file. For that will need to type: zeek -r nitroba.pcap -> This command will tell Zeek to read the file and create different Log files that Zeek can create using the information that can be found in the PCAP.



```
eliot@eliot:~/Desktop/nitroba$ zeek -r nitroba.pcap
```

Now we can start solving the challenge.

1) Mapping the Nitroba dorm room network will be done with the conn.log file that show every connection made in the PCAP file.

-The commands will create a text file with every source and destination IP that we can work with in the next step.

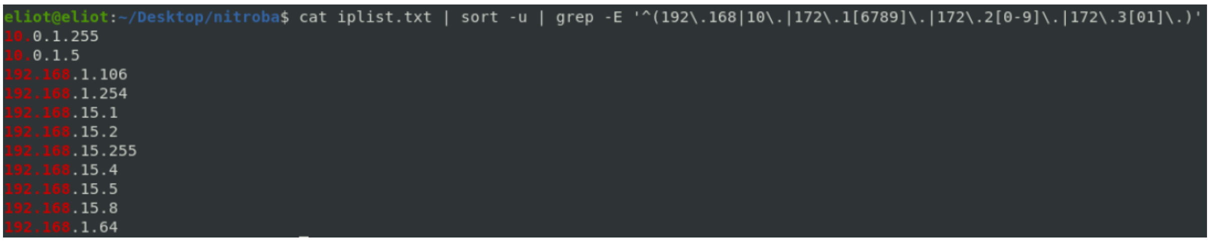
less -S conn.log | /usr/local/zeek/bin/zeek-cut id.orig_h > iplist.txt

less -S conn.log | /usr/local/zeek/bin/zeek-cut id.resp_h >> iplist.txt

-Now we have a file with every source and destination IP that we need to sort and grep in order to have only the IPs inside the dorm room.

cat iplist.txt | sort -u | grep -E '^(192\.168|10\.|172\.1[6789]\.|172\.2[0-9]\.|172\.3[01]\.)'

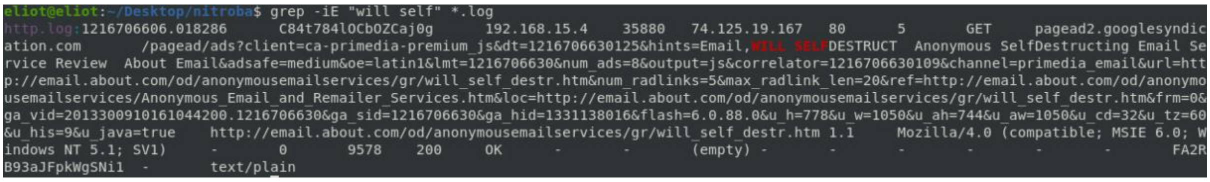
The list of IPs in the dorm room network is:



```
eliot@eliot:~/Desktop/nitroba$ cat iplist.txt | sort -u | grep -E '^(192\.168|10\.|172\.1[6789]\.|172\.2[0-9]\.|172\.3[01]\.)'
10.0.1.255
10.0.1.5
192.168.1.106
192.168.1.254
192.168.15.1
192.168.15.2
192.168.15.255
192.168.15.4
192.168.15.5
192.168.15.8
192.168.1.64
```

2.A) TCP flow that includes the hostile message can be found with the command:

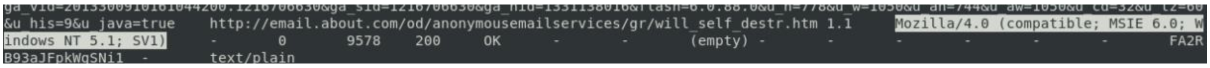
grep -iE "will self" *.log



```
eliot@eliot:~/Desktop/nitroba$ grep -iE "will self" *.log
http.log:1216706606.018286      C84t784lOCbOZCaj0g      192.168.15.4    35880   74.125.19.167   80      5       GET     pagead2.googlesyndic
ation.com       /pagead/ads?client=ca-primedia-premium_js&dt=1216706630125&hints=Email,WILL SELFDESTRUCT  Anonymous SelfDestructing Email Se
rvice Review  About Email&adsafe=medium&oe=latin1&lmt=1216706630&num_ads=8&output=js&correlator=1216706630109&channel=primedia_email&url=htt
p://email.about.com/od/anonymousemailservices/gr/will_self_destr.htm&num_radlinks=5&max_radlink_len=20&ref=http://email.about.com/od/anonymo
usemailservices/Anonymous_Email_and_Remailer_Services.htm&loc=http://email.about.com/od/anonymousemailservices/gr/will_self_destr.htm&frm=0&
ga_vid=2013300910161044200.1216706630&ga_sid=1216706630&ga_hid=1331138016&flash=6.0.88.0&u_h=778&u_w=1050&u_ah=744&u_aw=1050&u_cd=32&u_tz=60
&u_his=9&u_java=true    http://email.about.com/od/anonymousemailservices/gr/will_self_destr.htm 1.1     Mozilla/4.0 (compatible; MSIE 6.0; W
indows NT 5.1; SV1)     -       0       9578    200     OK      -       -       (empty) -       -       -       -       -       -       FA2R
B93aJFpkWgSNi1  -       text/plain
```

2.B) A particular web browser that can be tie to that message can be found with the last command: grep -iE "will self" *.log and can be seen in the previous photo at the end.

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)



```
ga_vid=2013300910161044200.1216706630&ga_sid=1216706630&ga_hid=1331138016&flash=6.0.88.0&u_h=778&u_w=1050&u_ah=744&u_aw=1050&u_cd=32&u_tz=60
&u_his=9&u_java=true    http://email.about.com/od/anonymousemailservices/gr/will_self_destr.htm 1.1     Mozilla/4.0 (compatible; MSIE 6.0; W
indows NT 5.1; SV1)     -       0       9578    200     OK      -       -       (empty) -       -       -       -       -       -       FA2R
B93aJFpkWgSNi1  -       text/plain
```

3) The other TCP connections that belong to the attacker can be seen by typing:

cat *.log | grep -iE "Windows NT"

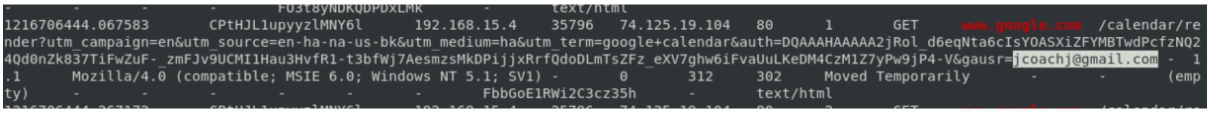
*Note: Windows NT- is the shortest way to find the user agent that belong to the attacker.

The result of that output I will save with the command: (in order to ID the attacker)

cat *.log | grep -iE "Windows NT" > attacker.txt

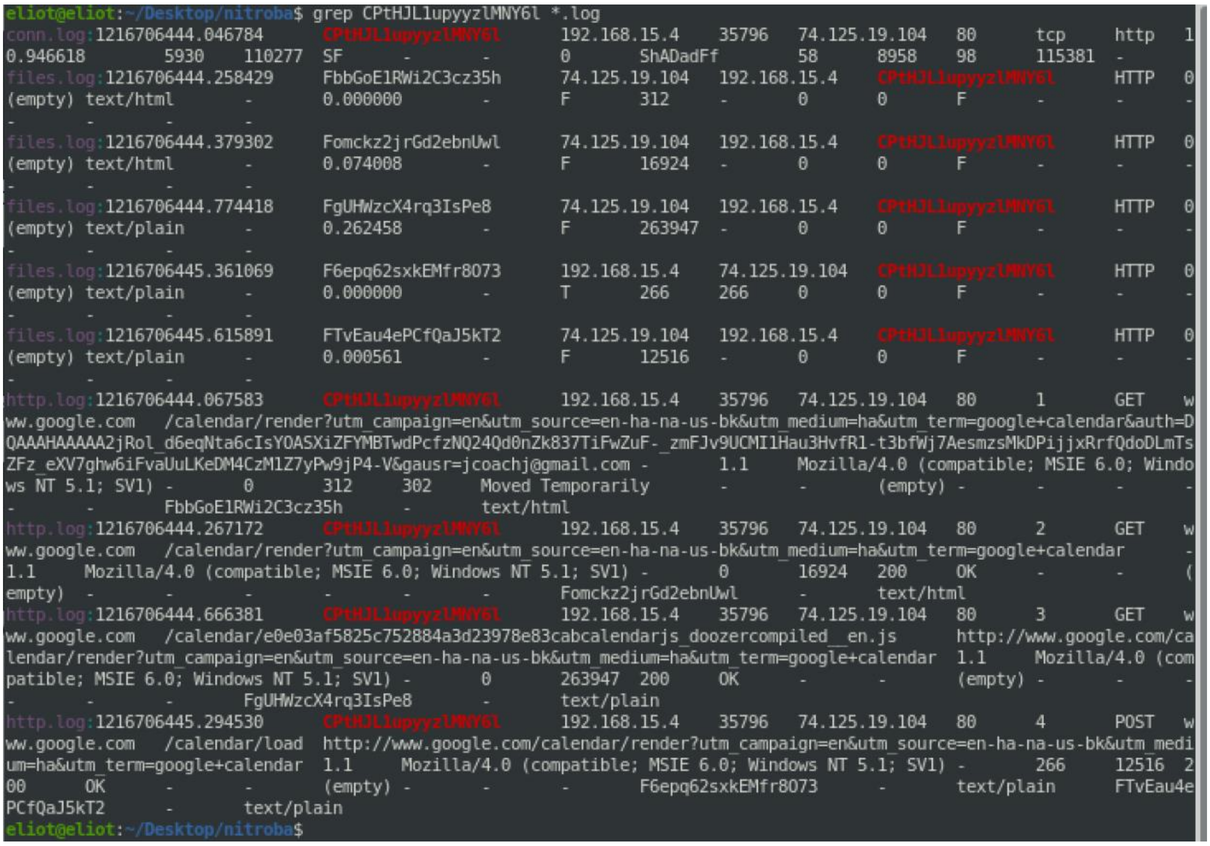
4) Information in one of those TCP connections that IDs the attacker can be found by searching through the file or by trying to see where it is possible that the attacker made a mistake because the attacker is using "www.google.com" a lot by typing: cat attacker.txt | grep -iE "www.google.com"   we can sort throw less packets but have higher possibility to find the attacker mistake.

The attacker can be found in the 1216706444.067583 packet and his email address is: jcoachj@gmail.com



```
-       -       -       -       FU3t8yNDKQDPDxLMK       -       text/html
1216706444.067583       CPtHJL1upyyzlMNY6l      192.168.15.4    35796   74.125.19.104   80      1       GET     www.google.com  /calendar/re
nder?utm_campaign=en&utm_source=en-ha-na-us-bk&utm_medium=ha&utm_term=google+calendar&auth=DQAAAHAAAAA2jRol_d6eqNta6cIsYOASXiZFYMBTwdPcfzNQ2
4Qd0nZk837TiFwZuF-_zmFJv9UCMI1Hau3HvfR1-t3bfWj7AesmzsMkDPijjxRrfQdoDLmTsZFz_eXV7ghw6iFvaUuLKeDM4CzM1Z7yPw9jP4-V&gausr=jcoachj@gmail.com -   1
.1      Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) -       0       312     302     Moved Temporarily       -       -       (emp
ty)     -       -       -       -       -       -       FbbGoE1RWi2C3cz35h      -       text/html
1216706444.267172       CPtHJL1upyyzlMNY6l      192.168.15.4    35796   74.125.19.104   80      2       GET     www.google.com  /calendar/re
```

Also, with zeek it is possible to find every connection that is related to the same packet by using the string zeek gives to the same connection in this case the string is: CPtHJL1upyyzlMNY6l and by typing the command: grep CPtHJL1upyyzlMNY6l *.log we can see other related information on the same packets string.



```
eliot@eliot:~/Desktop/nitroba$ grep CPtHJL1upyyzlMNY6l *.log
conn.log:1216706444.046784      CPtHJL1upyyzlMNY6l      192.168.15.4    35796   74.125.19.104   80      tcp     http    1
0.946618        5930    110277  SF      -       -       0       ShADadFf        58      8958    98      115381  -
files.log:1216706444.258429     FbbGoE1RWi2C3cz35h      74.125.19.104   192.168.15.4    CPtHJL1upyyzlMNY6l      HTTP    0
(empty) text/html       -       0.000000        -       F       312     -       0       0       F       -       -       -
-       -       -       -
files.log:1216706444.379302     Fomckz2jrGd2ebnUwl      74.125.19.104   192.168.15.4    CPtHJL1upyyzlMNY6l      HTTP    0
(empty) text/html       -       0.074008        -       F       16924   -       0       0       F       -       -       -
-       -       -       -
files.log:1216706444.774418     FgUHWzcX4rq3IsPe8       74.125.19.104   192.168.15.4    CPtHJL1upyyzlMNY6l      HTTP    0
(empty) text/plain      -       0.262458        -       F       263947  -       0       0       F       -       -       -
-       -       -       -
files.log:1216706445.361069     F6epq62sxkEMfr8073      192.168.15.4    74.125.19.104   CPtHJL1upyyzlMNY6l      HTTP    0
(empty) text/plain      -       0.000000        -       T       266     266     0       0       F       -       -       -
-       -       -       -
files.log:1216706445.615891     FTvEau4ePCfQaJ5kT2      74.125.19.104   192.168.15.4    CPtHJL1upyyzlMNY6l      HTTP    0
(empty) text/plain      -       0.000561        -       F       12516   -       0       0       F       -       -       -
-       -       -       -
http.log:1216706444.067583      CPtHJL1upyyzlMNY6l      192.168.15.4    35796   74.125.19.104   80      1       GET     w
ww.google.com   /calendar/render?utm_campaign=en&utm_source=en-ha-na-us-bk&utm_medium=ha&utm_term=google+calendar&auth=D
QAAAHAAAAA2jRol_d6eqNta6cIsYOASXiZFYMBTwdPcfzNQ24Qd0nZk837TiFwZuF-_zmFJv9UCMI1Hau3HvfR1-t3bfWj7AesmzsMkDPijjxRrfQdoDLmTs
ZFz_eXV7ghw6iFvaUuLKeDM4CzM1Z7yPw9jP4-V&gausr=jcoachj@gmail.com -       1.1     Mozilla/4.0 (compatible; MSIE 6.0; Windo
ws NT 5.1; SV1) -       0       312     302     Moved Temporarily       -       -       (empty) -       -       -       -
-       -       FbbGoE1RWi2C3cz35h      -       text/html
http.log:1216706444.267172      CPtHJL1upyyzlMNY6l      192.168.15.4    35796   74.125.19.104   80      2       GET     w
ww.google.com   /calendar/render?utm_campaign=en&utm_source=en-ha-na-us-bk&utm_medium=ha&utm_term=google+calendar      -
1.1     Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) -       0       16924   200     OK      -       -       (
empty)  -       -       -       -       -       -       Fomckz2jrGd2ebnUwl      -       text/html
http.log:1216706444.666381      CPtHJL1upyyzlMNY6l      192.168.15.4    35796   74.125.19.104   80      3       GET     w
ww.google.com   /calendar/e0e03af5825c752884a3d23978e83cabcalendarjs_doozercompiled__en.js      http://www.google.com/ca
lendar/render?utm_campaign=en&utm_source=en-ha-na-us-bk&utm_medium=ha&utm_term=google+calendar  1.1     Mozilla/4.0 (com
patible; MSIE 6.0; Windows NT 5.1; SV1) -       0       263947  200     OK      -       -       (empty) -       -       -
-       -       -       FgUHWzcX4rq3IsPe8       -       text/plain
http.log:1216706445.294530      CPtHJL1upyyzlMNY6l      192.168.15.4    35796   74.125.19.104   80      4       POST    w
ww.google.com   /calendar/load  http://www.google.com/calendar/render?utm_campaign=en&utm_source=en-ha-na-us-bk&utm_medi
um=ha&utm_term=google+calendar  1.1     Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) -       266     12516   2
00      OK      -       -       (empty) -       -       -       F6epq62sxkEMfr8073      -       text/plain      FTvEau4e
PCfQaJ5kT2      -       text/plain
eliot@eliot:~/Desktop/nitroba$
```

How Zeek help us in the Nitroba case?

1) We toke the nitroba.pcap file and run it throw Zeek to get a sorted Log files of the traffic captured in the pcap file by category.

2) We looked at all the files and figure what they contain before getting in to work.

Conn.log is a file containing TCP/UDP/ICMP connections.

Dns.log is a file containing domain name system activity.

Dpd.log is a file containing dynamic protocol detection failures.

Files.log is a file containing file analysis results.

Http.log is a file containing hypertext transfer protocol requests and replies.

Ntp.log is a file containing network time protocol.

Packet_filter.log is a file containing list of packet filters that were applied.

Sip.log is a file containing session initiation protocol

Ssl.log is a file containing SSL/TLS handshake info.

Weird.log is a file containing session initiation protocol.

x509.log is a file containing X.509 certificate info.

3) We used a tool called Zeek-cut in order to cut from the log file the columns that we were interested with instead of using complicated regex to get the same solution.

4) We saw that the log files Zeek generate show us rich related information that can be found in each packet wan Zeek read the pcap file with his "out of the box" settings, each file is sorted in a way that it is easy to read and understand in order for us to find what we need easily. (for example: challenge 2.b)

5) We saw that Zeek give's packets a string that we can copy and grep to find related information connected to the packet from different log files and it will be easier to us to "dig" through a suspicions or interesting connection.