Solving playing detective pcap with Zeek – Sean Yarkoni

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

The challenge is:

1) The MAC address and IP address of the user's Windows computer

2) The host name of the user's Windows computer

3) The user's first and last name

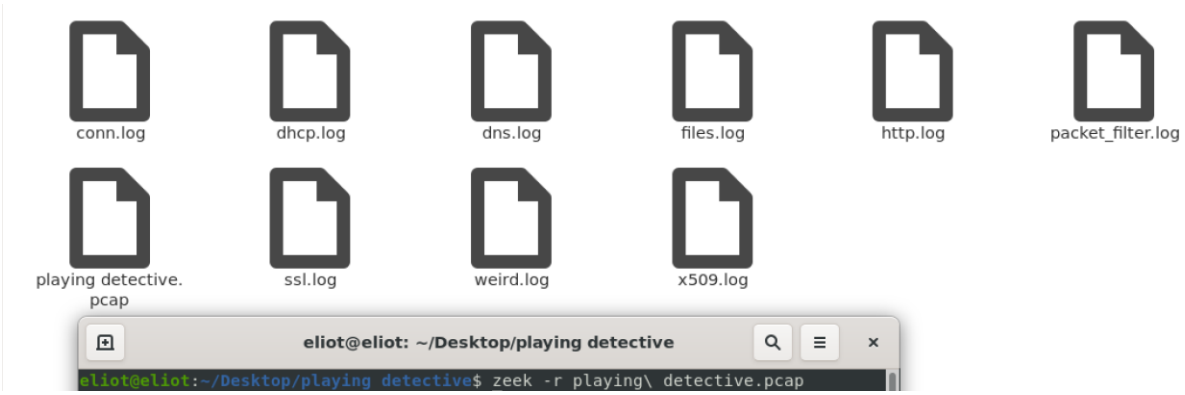
Pcap file working with:

https://malware-traffic-analysis.net/2016/04/16/index.html

2016-04-16-traffic-a
nalysis-exercise-PLAY

Solution:

In order for us to start we need Zeek to read the pcap file. For that will need to type: zeek -r playing\ detective.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



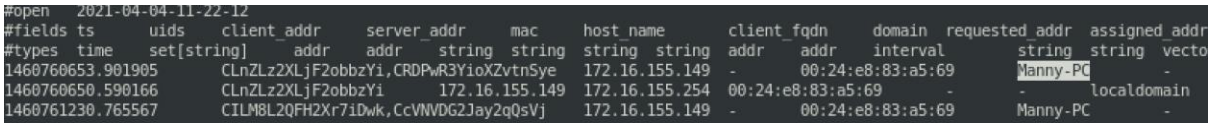
Now we can start solving the challenge

1) IP address are obtained from a DHCP server (router in hoses today) and in order for a DHCP server to give an IP address its need to know the MAC address of the computer connecting to the DHCP server, In order for us to find the IP address and the MAC address we can look at the DHCP file and see the user IP and MAC address, we can do this by typing: less -S dhcp.log

```
#open   2021-04-04-11-22-12
#fields ts      uids    client_addr     server_addr     mac     host_name       client_fqdn     domain  requested_addr  assigned_addr   lease_time
#types  time    set[string]     addr    addr    string  string  string  string  addr    addr    interval        string  string  vector[string]  inte
1460760653.901905       CLnZLz2XLjF2obbzYi,CRDPwR3YioXZvtnSye   172.16.155.149  -       00:24:e8:83:a5:69       Manny-PC        -       localdomain
1460760650.590166       CLnZLz2XLjF2obbzYi      172.16.155.149  172.16.155.254  00:24:e8:83:a5:69       -       -       localdomain     -       172.
1460761230.765567       CILM8L2QFH2Xr7iDwk,CcVNVDG2Jay2qQsVj    172.16.155.149  -       00:24:e8:83:a5:69       Manny-PC        -       localdomain
```

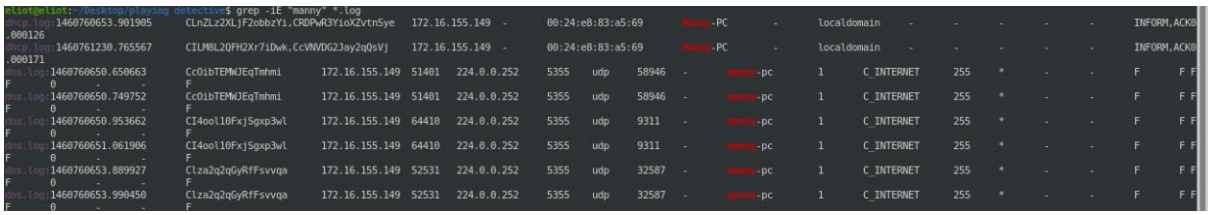
From here we can see that the IP address is 172.16.155.149 and the MAC address is 00:24:e8:83:a5:69 .

2) The user's host name of the Windows computer can be seen in the dhcp.log file under the name "host_name" and we can see it by typing: less -S dhcp.log



The user's host name of the Windows computer is: Manny-PC

3) For us to find the user's first and last name we can use what we already know and try to find his name with the information we already got, because we know the name of the PC can be his first or last name "Manny" we can try and grep that name with the command: grep -iE "manny" *.log and see the result:



Because Zeek without scripts won't read the payload in depth we will need to make a script that will help us, the only place that it might be relevant for us is the http.log, we will make a signature that will try and catch "manny" in the payload of an http transaction

We will need to create a directory and file that is a ".sig" in /zeek/scripts/base/protocols/ with the command:

sudo mkdir <name>

cd <name>

sudo touch <name>.sig

now we need to edit the file as sudo with "nano" or "vim" and add the string:

signature <name> {

ip-proto == tcp

dst-port == 80

http-request-body /.*(manny)/

event "<name>"

}

Then we need Zeek to read the pcap file with the string we just created with the command:

zeek -r playing\ detective.pcap -s /home/eliot/zeek/scripts/base/protocols/test/test.sig

then will see the file signetures.log add to the directory.

And now we can look if the new file has a log that contain information about the user's first and last name with the command: less -S signatures.log

Under the event_msg column we can see the string "http-request-body /.*(manny)/" finding was the email address of the user with the first and last name witch is "manny lehman"

How Zeek help us in the playing detective case?

1) We toke the playing\ detective.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

Dhcp.log is a file containing dynamic host configuration protocol leases.

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

Files.log is a file containing file analysis results.

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

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

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 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 1 and 2)

4) We experience with Zeek a very versatile signatures that we can make in order to get the information we are after, but in order to get that signature right and the information relevant, we need to know in which protocol and layer the information we want to get is supposed to be, when using signature, the user knowledge have a big role.