

MUHAMMAD HAMAD - PCAP ATTACK TRACE – OPTIONAL ASSIGNMENT

Q- Which systems (i.e. IP addresses) are involved?

Ans- Ip of attacker 98.114.205.102 and ip of victim 192.150.11.111

The screenshot shows the Wireshark interface with the file 'attack-trace.pcap' open. The packet list pane displays 17 packets. Packet 6 is selected, showing details for an Ethernet II frame, an Internet Protocol Version 4 packet, and a Transmission Control Protocol (TCP) segment. The TCP segment details show: Src Port: 445, Dst Port: 1828, Seq: 0, Ack: 1, Len: 0. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	98.114.205.102	192.150.11.111	TCP	62	1821 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM...
2	0.000464	192.150.11.111	98.114.205.102	TCP	62	445 → 1821 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460...
3	0.119058	98.114.205.102	192.150.11.111	TCP	60	1821 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.134175	98.114.205.102	192.150.11.111	TCP	60	1821 → 445 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
5	0.134550	98.114.205.102	192.150.11.111	TCP	62	1828 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM...
6	0.134878	192.150.11.111	98.114.205.102	TCP	62	445 → 1828 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460...
7	0.135193	192.150.11.111	98.114.205.102	TCP	54	445 → 1821 [ACK] Seq=1 Ack=2 Win=5840 Len=0
8	0.238169	192.150.11.111	98.114.205.102	TCP	54	445 → 1821 [FIN, ACK] Seq=1 Ack=2 Win=5840 Len=0
9	0.251859	98.114.205.102	192.150.11.111	TCP	60	1828 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	0.267724	98.114.205.102	192.150.11.111	SMB	191	Negotiate Protocol Request
11	0.267735	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=1 Ack=138 Win=6432 Len=0
12	0.354302	98.114.205.102	192.150.11.111	TCP	60	1821 → 445 [ACK] Seq=2 Ack=2 Win=64240 Len=0
13	0.487136	192.150.11.111	98.114.205.102	SMB	143	Negotiate Protocol Response
14	0.602288	98.114.205.102	192.150.11.111	SMB	222	Session Setup AndX Request, NTLMSSP_NEGOTIATE
15	0.602303	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=90 Ack=306 Win=7584 Len=0
16	0.723001	192.150.11.111	98.114.205.102	SMB	311	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: ST...
17	0.800000	98.114.205.102	192.150.11.111	SMB	222	Session Setup AndX Response, NTLMSSP_AUTH, Error: ST...

Q- What can you find out about the attacking host ?

Location of attacker is found from packet and operating system of attacker is windows 2000 that is found from packet number 14 native OS field

The screenshot shows the Wireshark interface with the file 'attack-trace.pcap' open. Packet 14 is selected, showing details for an Ethernet II frame, an Internet Protocol Version 4 packet, a Transmission Control Protocol (TCP) segment, and a NetBIOS Session Service message. The TCP segment details show: Src Port: 1828, Dst Port: 445, Seq: 138, Ack: 90, Len: 168. The NetBIOS Session Service message details show: Message Type: Session message (0x00), Length: 164. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
14	0.602288	98.114.205.102	192.150.11.111	SMB	222	Session Setup AndX Request, NTLMSSP_NEGOTIATE

Q- How many TCP sessions are contained in the dump file?

5 sessions

98.114.205.102:1821 -> 192.150.11.111:445
 98.114.205.102:1828 -> 192.150.11.111:445
 192.150.11.111:1957 <-98.114.205.102:1924
 192.150.11.111:36296 -> 98.114.205.102:8884
 98.114.205.102:2152 -> 192.150.11.111:1080

attack-trace.pcap

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	98.114.205.102	192.150.11.111	TCP	62	1821 -> 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2	0.009464	192.150.11.111	98.114.205.102	TCP	62	445 -> 1821 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	0.119058	98.114.205.102	192.150.11.111	TCP	60	1821 -> 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.134175	98.114.205.102	192.150.11.111	TCP	60	1821 -> 445 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
7	0.135193	192.150.11.111	98.114.205.102	TCP	54	445 -> 1821 [ACK] Seq=1 Ack=2 Win=5840 Len=0
8	0.238169	192.150.11.111	98.114.205.102	TCP	54	445 -> 1821 [FIN, ACK] Seq=1 Ack=2 Win=5840 Len=0
12	0.354302	98.114.205.102	192.150.11.111	TCP	60	1821 -> 445 [ACK] Seq=2 Ack=2 Win=64240 Len=0

▶ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
 ▶ Ethernet II, Src: Cisco_3b:56:01 (00:08:e2:3b:56:01), Dst: SuperMic_62:4e:4a (00:30:48:62:4e:4a)
 ▶ Internet Protocol Version 4, Src: 98.114.205.102, Dst: 192.150.11.111
 ▶ Transmission Control Protocol, Src Port: 1821, Dst Port: 445, Seq: 0, Len: 0

0000 00 30 48 62 4e 4a 00 08 e2 3b 56 01 00 00 45 00 ...V...HbNJ...E.
 0010 30 30 3f 40 00 71 06 02 4a 62 4e 4a 06 c0 96 ...e.e.9U...obr
 0020 30 6f 07 1d 01 bd 08 cb 80 66 00 00 00 70 02 ...f...P.
 0030 fa f0 fa 44 00 00 02 04 05 b4 01 01 04 02 ...D....

Internet Protocol Version 4 (ip), 20 bytes

Packets: 348 · Displayed: 7 (2.0%) · Load time: 0:0.116 · Profile: Default

attack-trace.pcap

tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Info
5	0.134550	98.114.205.102	192.150.11.111	TCP	62	1828 -> 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	0.134878	192.150.11.111	98.114.205.102	TCP	62	445 -> 1828 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	0.251859	98.114.205.102	192.150.11.111	TCP	60	1828 -> 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	0.267724	98.114.205.102	192.150.11.111	SMB	191	Negotiate Protocol Request
11	0.267735	192.150.11.111	98.114.205.102	TCP	54	445 -> 1828 [ACK] Seq=1 Ack=138 Win=6432 Len=0
13	0.487136	192.150.11.111	98.114.205.102	SMB	143	Negotiate Protocol Response
14	0.602288	98.114.205.102	192.150.11.111	SMB	222	Session Setup AndX Request, NTLMSSP_NEGOTIATE
15	0.602303	192.150.11.111	98.114.205.102	TCP	54	445 -> 1828 [ACK] Seq=90 Ack=306 Win=7504 Len=0
16	0.723001	192.150.11.111	98.114.205.102	SMB	311	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE...
17	0.840405	98.114.205.102	192.150.11.111	SMB	276	Session Setup AndX Request, NTLMSSP_AUTH, User: \
18	0.840419	192.150.11.111	98.114.205.102	TCP	54	445 -> 1828 [ACK] Seq=347 Ack=528 Win=8576 Len=0
19	0.957617	192.150.11.111	98.114.205.102	SMB	175	Session Setup AndX Response
20	1.073151	98.114.205.102	192.150.11.111	SMB	152	Tree Connect AndX Request, Path: \\192.150.11.111\ipc\$
21	1.073174	192.150.11.111	98.114.205.102	TCP	54	445 -> 1828 [ACK] Seq=468 Ack=626 Win=8576 Len=0
22	1.189374	192.150.11.111	98.114.205.102	SMB	114	Tree Connect AndX Response
23	1.307145	98.114.205.102	192.150.11.111	SMB	158	NT Create AndX Request, FID: 0x4000, Path: \lsarpc
24	1.307168	192.150.11.111	98.114.205.102	TCP	54	445 -> 1828 [ACK] Seq=528 Ack=730 Win=8576 Len=0
25	1.424860	192.150.11.111	98.114.205.102	SMB	193	NT Create AndX Response, FID: 0x4000
26	1.542389	98.114.205.102	192.150.11.111	DCERPC	214	Bind: call_id: 1, Fragment: Single, 1 context items: DSSETUP V0.0 ...
27	1.542401	192.150.11.111	98.114.205.102	TCP	54	445 -> 1828 [ACK] Seq=667 Ack=890 Win=9648 Len=0

▶ Frame 11: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
 ▶ Ethernet II, Src: SuperMic_62:4e:4a (00:30:48:62:4e:4a), Dst: Cisco_3b:56:01 (00:08:e2:3b:56:01)
 ▶ Internet Protocol Version 4, Src: 192.150.11.111, Dst: 98.114.205.102
 ▶ Transmission Control Protocol, Src Port: 445, Dst Port: 1828, Seq: 1, Ack: 138, Len: 0

0000 00 08 e2 3b 56 01 00 30 48 62 4e 4a 00 00 45 00 ...;V...HbNJ...E.
 0010 30 28 05 00 40 00 40 06 39 55 c0 06 0b 6f 62 72 (...e.e.9U...obr
 0020 ad 06 01 bd 07 24 5b d5 0e bf 08 cf f7 ac 50 10 ...f...\$[.P.
 0030 19 20 26 e5 00 00 ...&...

Internet Protocol Version 4 (ip), 20 bytes

Packets: 348 · Displayed: 31 (8.9%) · Load time: 0:0.94 · Profile: Default

tcp.stream eq 3

No.	Time	Source	Destination	Protocol	Length	Info
50	5.082620	192.150.11.111	98.114.205.102	TCP	74	36296 → 8884 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=...
52	5.201726	98.114.205.102	192.150.11.111	TCP	78	8884 → 36296 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 ...
53	5.201740	192.150.11.111	98.114.205.102	TCP	66	36296 → 8884 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=4055633911 TSe...
54	5.349393	98.114.205.102	192.150.11.111	TCP	87	8884 → 36296 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=21 TSval=438613 ...
55	5.349405	192.150.11.111	98.114.205.102	TCP	66	36296 → 8884 [ACK] Seq=1 Ack=22 Win=5888 Len=0 TSval=4055633948 TS...
56	5.349467	192.150.11.111	98.114.205.102	TCP	74	36296 → 8884 [PSH, ACK] Seq=1 Ack=22 Win=5888 Len=8 TSval=40556339...
57	5.474324	98.114.205.102	192.150.11.111	TCP	88	8884 → 36296 [PSH, ACK] Seq=22 Ack=9 Win=64232 Len=22 TSval=438614...
58	5.474373	192.150.11.111	98.114.205.102	TCP	74	36296 → 8884 [PSH, ACK] Seq=9 Ack=44 Win=5888 Len=8 TSval=40556339...
59	5.604502	98.114.205.102	192.150.11.111	TCP	86	8884 → 36296 [PSH, ACK] Seq=44 Ack=17 Win=64224 Len=20 TSval=43861...
60	5.604566	192.150.11.111	98.114.205.102	TCP	72	36296 → 8884 [PSH, ACK] Seq=17 Ack=64 Win=5888 Len=6 TSval=4055634...
61	5.736927	98.114.205.102	192.150.11.111	TCP	79	8884 → 36296 [PSH, ACK] Seq=64 Ack=23 Win=64218 Len=13 TSval=43861...
62	5.736981	192.150.11.111	98.114.205.102	TCP	74	36296 → 8884 [PSH, ACK] Seq=23 Ack=77 Win=5888 Len=8 TSval=4055634...
63	5.871853	98.114.205.102	192.150.11.111	TCP	85	8884 → 36296 [PSH, ACK] Seq=77 Ack=31 Win=64210 Len=19 TSval=43861...
64	5.871936	192.150.11.111	98.114.205.102	TCP	92	36296 → 8884 [PSH, ACK] Seq=31 Ack=96 Win=5888 Len=26 TSval=405563...
65	6.009400	98.114.205.102	192.150.11.111	TCP	95	8884 → 36296 [PSH, ACK] Seq=96 Ack=57 Win=64184 Len=29 TSval=43862...
66	6.009415	192.150.11.111	98.114.205.102	TCP	81	36296 → 8884 [PSH, ACK] Seq=57 Ack=125 Win=5888 Len=15 TSval=40556...
67	6.141826	98.114.205.102	192.150.11.111	TCP	106	8884 → 36296 [PSH, ACK] Seq=125 Ack=72 Win=64169 Len=40 TSval=4386...
68	6.179362	192.150.11.111	98.114.205.102	TCP	66	36296 → 8884 [ACK] Seq=72 Ack=165 Win=5888 Len=0 TSval=4055634156 ...
339	16.096872	192.150.11.111	98.114.205.102	TCP	72	36296 → 8884 [PSH, ACK] Seq=72 Ack=165 Win=5888 Len=6 TSval=405563...
340	16.097404	98.114.205.102	192.150.11.111	TCP	89	8884 → 36296 [PSH, ACK] Seq=165 Ack=72 Win=64169 Len=23 TSval=4387...

Frame 50: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 Ethernet II, Src: SuperMic_62:4e:4a (00:30:48:62:4e:4a), Dst: Cisco_3b:56:01 (00:08:e2:3b:56:01)
 Internet Protocol Version 4, Src: 192.150.11.111, Dst: 98.114.205.102
 Transmission Control Protocol, Src Port: 36296, Dst Port: 8884, Seq: 0, Len: 0

0000 00 08 e2 3b 56 01 00 30 48 62 4e 4a 08 00 45 00 ...;V..0 HbNJ..E.
 0010 00 3c 31 46 40 00 40 06 0d 98 c0 96 0b 6f 62 72 ...<1F0.0.obr
 0020 cd 66 8d c8 22 b4 5c 21 3e 9c 00 00 00 00 a0 02 ...f..".\! >.....
 0030 15 00 e8 00 00 00 02 04 05 b4 04 02 08 0a f1 bc
 0040 0f da 00 00 00 00 01 03 03 07
 Internet Protocol Version 4 (ip), 20 bytes

Packets: 348 · Displayed: 27 (7.8%) · Load time: 0:0.11 · Profile: Default

attack-trace.pcap

tcp.stream eq 4

No.	Time	Source	Destination	Protocol	Length	Info
68	6.142326	98.114.205.102	192.150.11.111	TCP	62	2152 → 1080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
69	6.142800	192.150.11.111	98.114.205.102	TCP	62	1080 → 2152 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK PE...
71	6.256763	98.114.205.102	192.150.11.111	TCP	60	2152 → 1080 [ACK] Seq=1 Ack=1 Win=64240 Len=0
72	6.273504	98.114.205.102	192.150.11.111	Socks	1078	Unknown
73	6.273515	192.150.11.111	98.114.205.102	TCP	54	1080 → 2152 [ACK] Seq=1 Ack=1025 Win=7168 Len=0
74	6.282623	98.114.205.102	192.150.11.111	Socks	1514	Unknown
75	6.282642	192.150.11.111	98.114.205.102	TCP	54	1080 → 2152 [ACK] Seq=1 Ack=2485 Win=10220 Len=0
76	6.284747	98.114.205.102	192.150.11.111	Socks	490	Unknown
77	6.284764	192.150.11.111	98.114.205.102	TCP	54	1080 → 2152 [ACK] Seq=1 Ack=2921 Win=13140 Len=0
78	6.395310	98.114.205.102	192.150.11.111	Socks	1514	Unknown
79	6.395327	192.150.11.111	98.114.205.102	TCP	54	1080 → 2152 [ACK] Seq=1 Ack=4381 Win=16060 Len=0
80	6.399808	98.114.205.102	192.150.11.111	Socks	1078	Unknown
81	6.399826	192.150.11.111	98.114.205.102	TCP	54	1080 → 2152 [ACK] Seq=1 Ack=5405 Win=18980 Len=0
82	6.406055	98.114.205.102	192.150.11.111	Socks	1514	Unknown
83	6.406071	192.150.11.111	98.114.205.102	TCP	54	1080 → 2152 [ACK] Seq=1 Ack=6865 Win=21900 Len=0
84	6.411801	98.114.205.102	192.150.11.111	Socks	1382	Unknown
85	6.411819	192.150.11.111	98.114.205.102	TCP	54	1080 → 2152 [ACK] Seq=1 Ack=8193 Win=24820 Len=0
86	6.507873	98.114.205.102	192.150.11.111	Socks	1514	Unknown
87	6.507891	192.150.11.111	98.114.205.102	TCP	54	1080 → 2152 [ACK] Seq=1 Ack=9653 Win=27740 Len=0
88	6.510371	98.114.205.102	192.150.11.111	Socks	622	Unknown

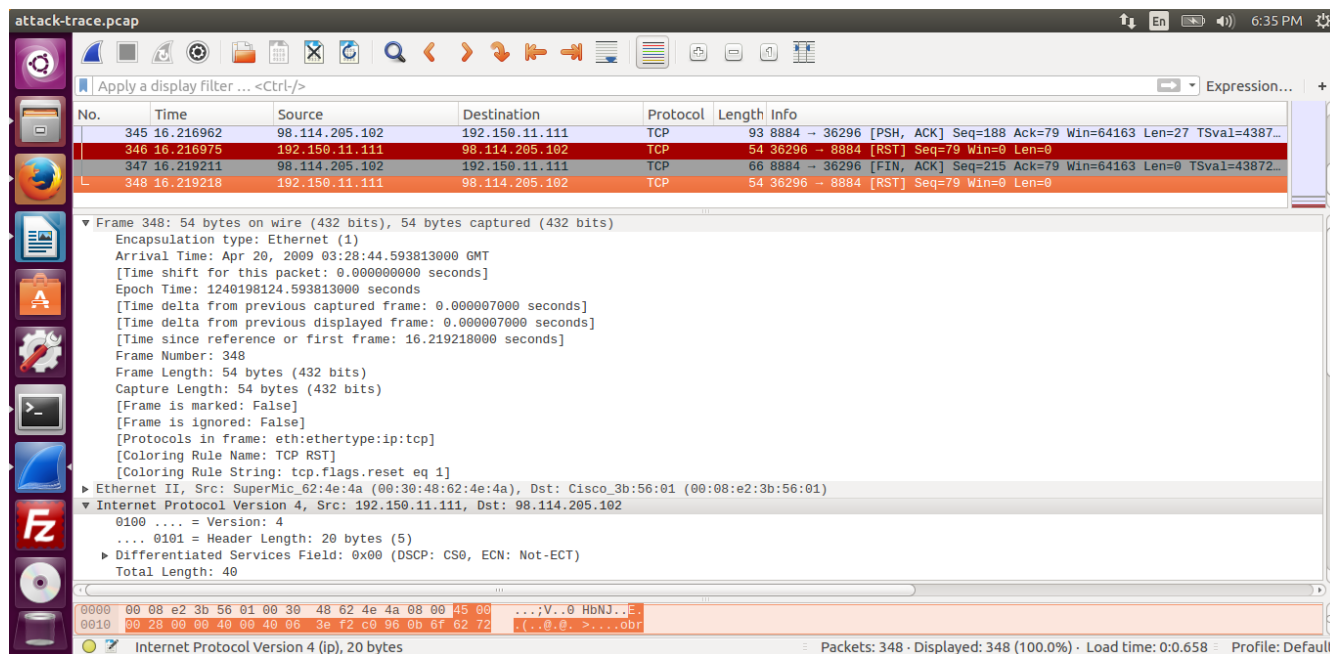
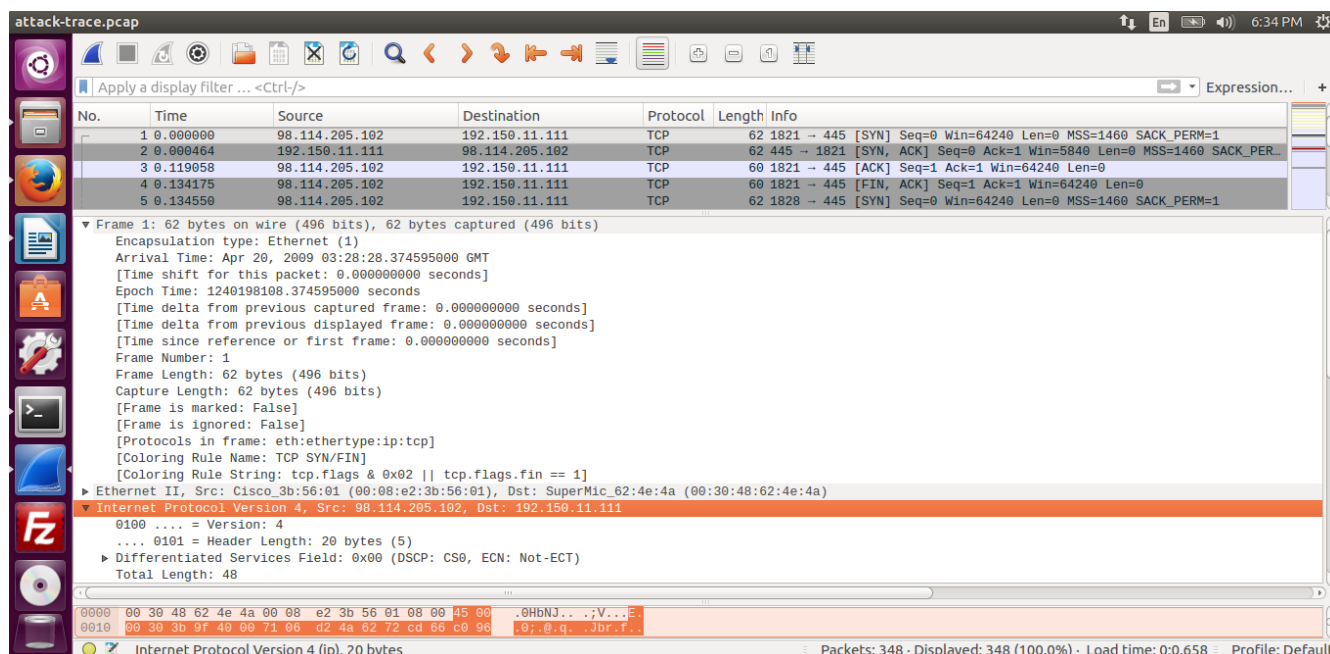
Frame 68: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
 Ethernet II, Src: Cisco_3b:56:01 (00:08:e2:3b:56:01), Dst: SuperMic_62:4e:4a (00:30:48:62:4e:4a)
 Internet Protocol Version 4, Src: 98.114.205.102, Dst: 192.150.11.111
 Transmission Control Protocol, Src Port: 2152, Dst Port: 1080, Seq: 0, Len: 0

0000 00 30 48 62 4e 4a 00 08 e2 3b 56 01 00 00 45 00 ...0HbNJ...;V...E.
 0010 00 30 3d 0c 40 00 71 06 00 20 62 72 cd 66 c0 96 ...0=0.0. :-Dr..E..
 0020 0b 6f 08 68 04 38 09 a4 a2 7f 00 00 00 00 70 02 ...d.h.8...-Dr..p..
 0030 fa f0 d3 8c 00 00 02 04 05 b4 01 01 04 02
 Internet Protocol Version 4 (ip), 20 bytes

Packets: 348 · Displayed: 271 (77.9%) · Load time: 0:0.15 · Profile: Default

Q- How long did it take to perform the attack?

16 seconds in total , can be checked by looking over time of first and last frame.



Q- Which operating system was targeted by the attack? And which service? Which vulnerability?

Ans- Windows XP is targeted that is victim's OS , the active directory feature provided by lsass accessed via lsarpc named pipe over TCP port 445 (445 corresponds to service "SMB over TCP") vulnerability was LSASS buffer overflow"

Wireshark

Wireshark - Follow TCP Stream (tcp.stream eq 1) - attack-trace

tcp.stream eq 1

No.	Time	Source
5	0.134550	98.114.205.102
6	0.134878	192.150.11.111
9	0.251859	98.114.205.102
10	0.267724	98.114.205.102
11	0.267735	192.150.11.111
13	0.487136	98.114.205.102
14	0.602288	192.150.11.111
15	0.602303	192.150.11.111
16	0.723001	192.150.11.111
17	0.840405	98.114.205.102
18	0.840419	98.114.205.102
19	0.957617	192.150.11.111
20	1.073151	98.114.205.102
21	1.073174	192.150.11.111
22	1.189374	192.150.11.111
23	1.307145	98.114.205.102
24	1.307168	192.150.11.111
25	1.424860	192.150.11.111
26	1.542389	98.114.205.102
27	1.542401	192.150.11.111
28	1.670219	192.150.11.111

[Protocols in frame: et
[Coloring Rule Name: SM
[Coloring Rule String:
Ethernet II, Src: Cisco_3b:56:01 (08:00:00:00:00:00), Dst: 08:00:00:00:00:00
Internet Protocol Version 4 (IP), Src: 98.114.205.102, Dst: 192.150.11.111

Packet 13. 11 client pkts, 9 server pkts, 15 turns. Click to select.

Entire conversation (5111 bytes) Show and save data as ASCII Stream 1

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

0000 00 30 48 62 4e 4a 00 08 e2 3b 56 01 08 00 45 00 ..0HbNJ...;V...E.
0010 00 d0 3b d8 40 00 71 06 d1 71 62 72 cd 66 c0 96 ...;@q...qbr.f..

Internet Protocol Version 4 (ip), 20 bytes Packets: 348 · Displayed: 31 (8.9%) · Load time: 0:0.84 · Profile: Default

Wireshark

Wireshark - Follow TCP Stream (tcp.stream eq 1) - attack-trace

tcp.stream eq 1

No.	Time	Source
5	0.134550	98.114.205.102
6	0.134878	192.150.11.111
9	0.251859	98.114.205.102
10	0.267724	98.114.205.102
11	0.267735	192.150.11.111
13	0.487136	98.114.205.102
14	0.602288	192.150.11.111
15	0.602303	192.150.11.111
16	0.723001	192.150.11.111
17	0.840405	98.114.205.102
18	0.840419	98.114.205.102
19	0.957617	192.150.11.111
20	1.073151	98.114.205.102
21	1.073174	192.150.11.111
22	1.189374	192.150.11.111
23	1.307145	98.114.205.102
24	1.307168	192.150.11.111
25	1.424860	192.150.11.111
26	1.542389	98.114.205.102
27	1.542401	192.150.11.111
28	1.670219	192.150.11.111

[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:
[Coloring Rule Name: SMB]
[Coloring Rule String: smb || nbss ||
Ethernet II, Src: Cisco_3b:56:01 (08:00:00:00:00:00), Dst: 08:00:00:00:00:00
Internet Protocol Version 4 (IP), Src: 98.114.205.102, Dst: 192.150.11.111

Packet 11. 11 client pkts, 9 server pkts, 15 turns. Click to select.

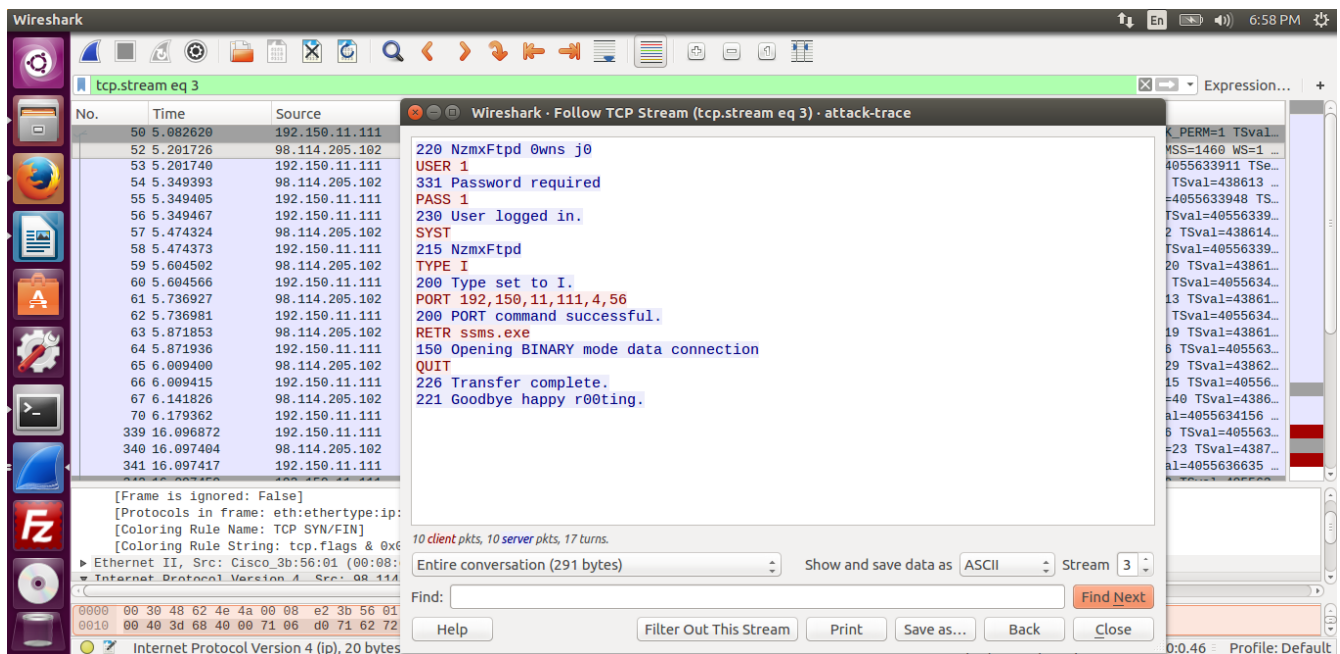
Entire conversation (5111 bytes) Show and save data as ASCII Stream 1

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

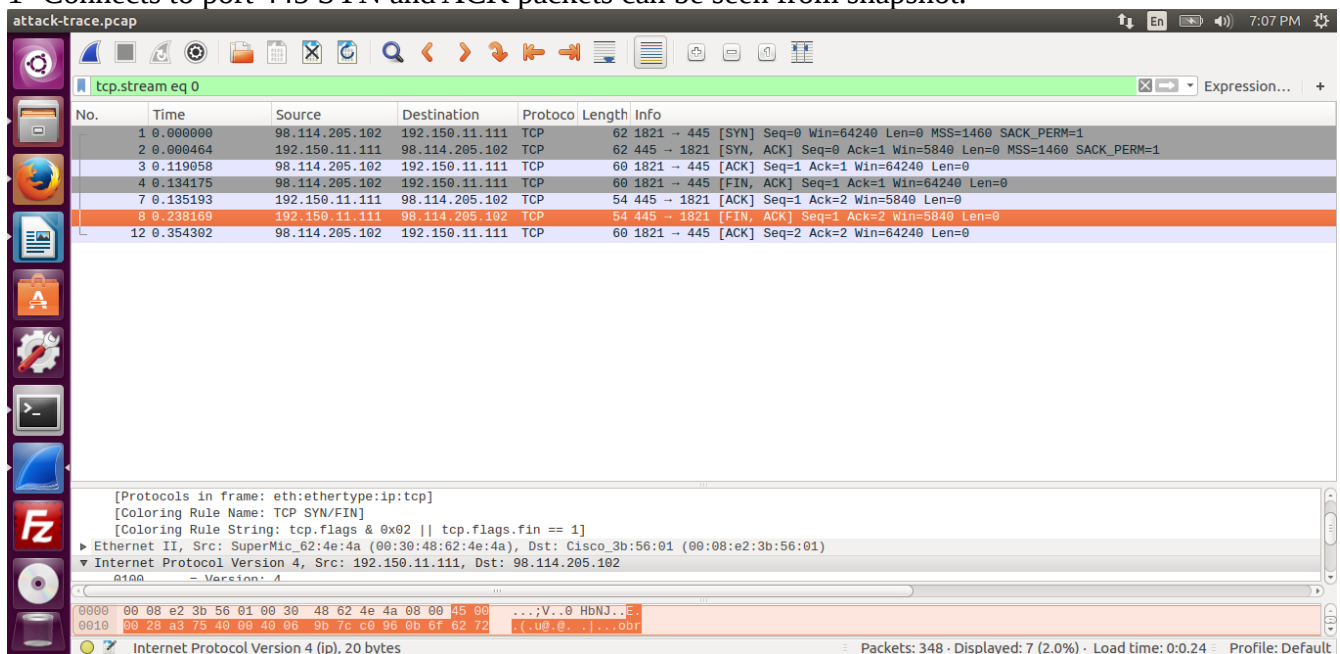
0000 00 30 48 62 4e 4a 00 08 e2 3b 56 01 08 00 45 00 ..0HbNJ...;V...E.
0010 00 90 3c 16 40 00 71 06 d1 73 62 72 cd 66 c0 96 ...;@q...qbr.f..

Internet Protocol Version 4 (ip), 20 bytes 0.116 Profile: Default

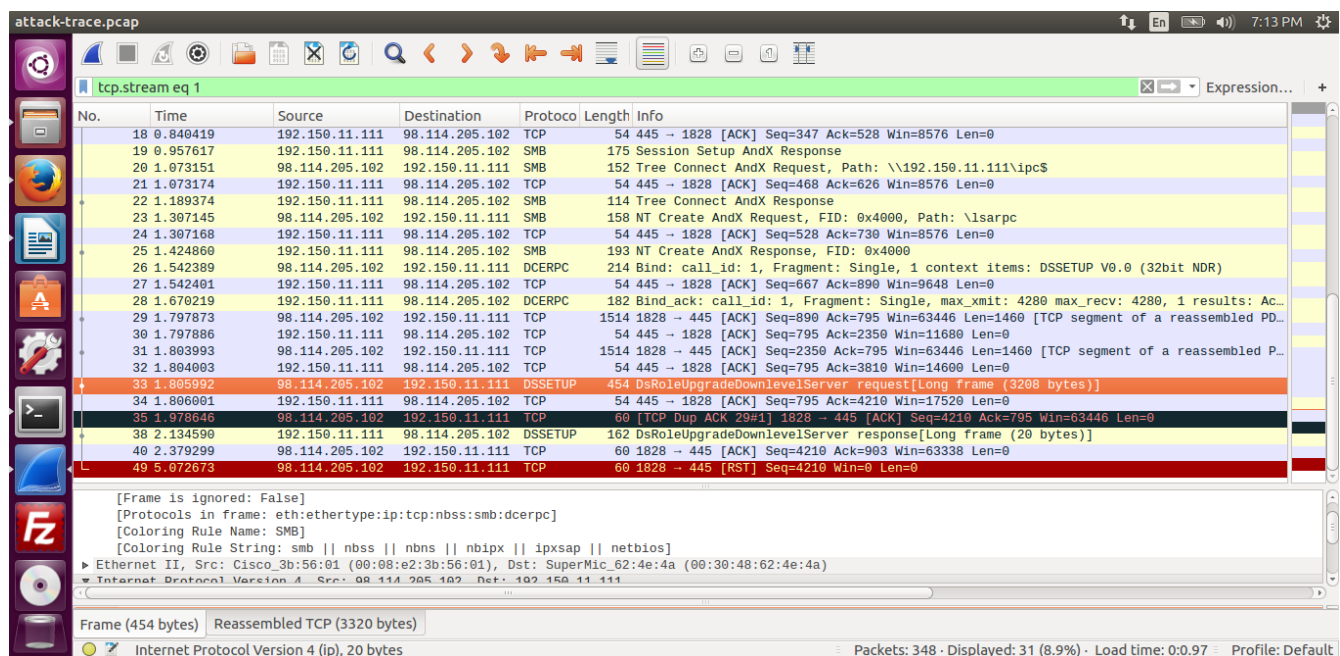


Q- Can you sketch an overview of the general actions performed by the attacker

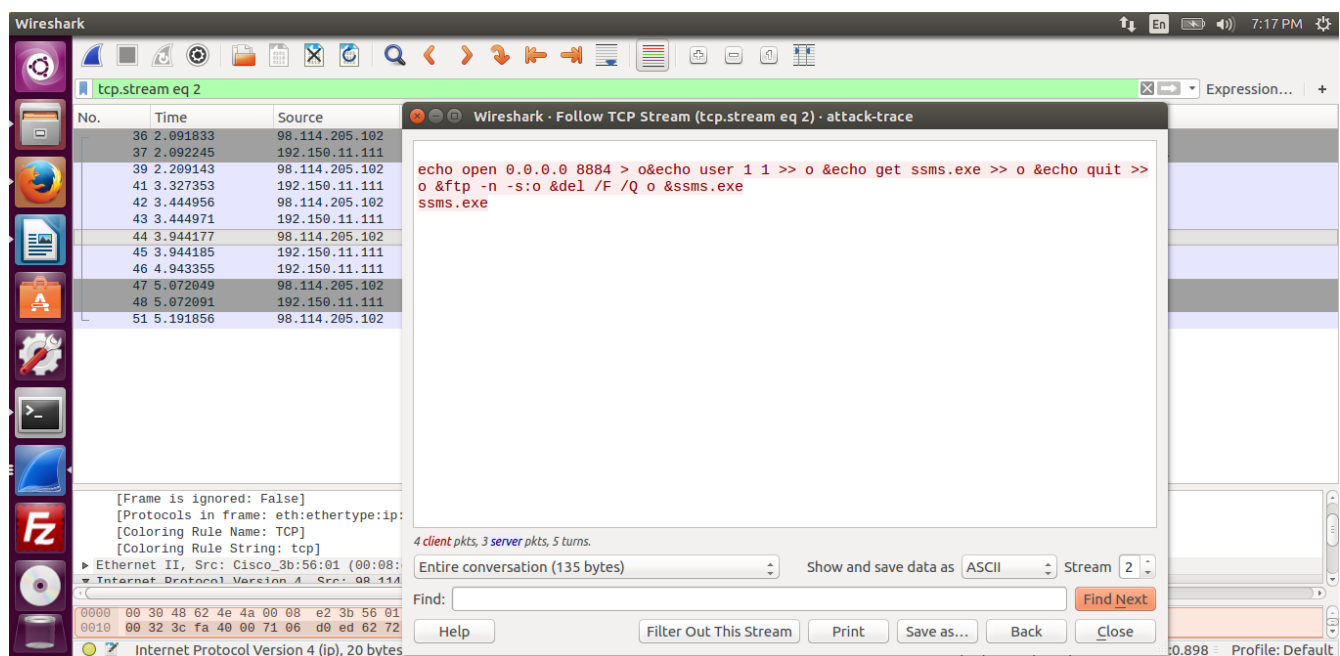
1- Connects to port 445 SYN and ACK packets can be seen from snapshot.



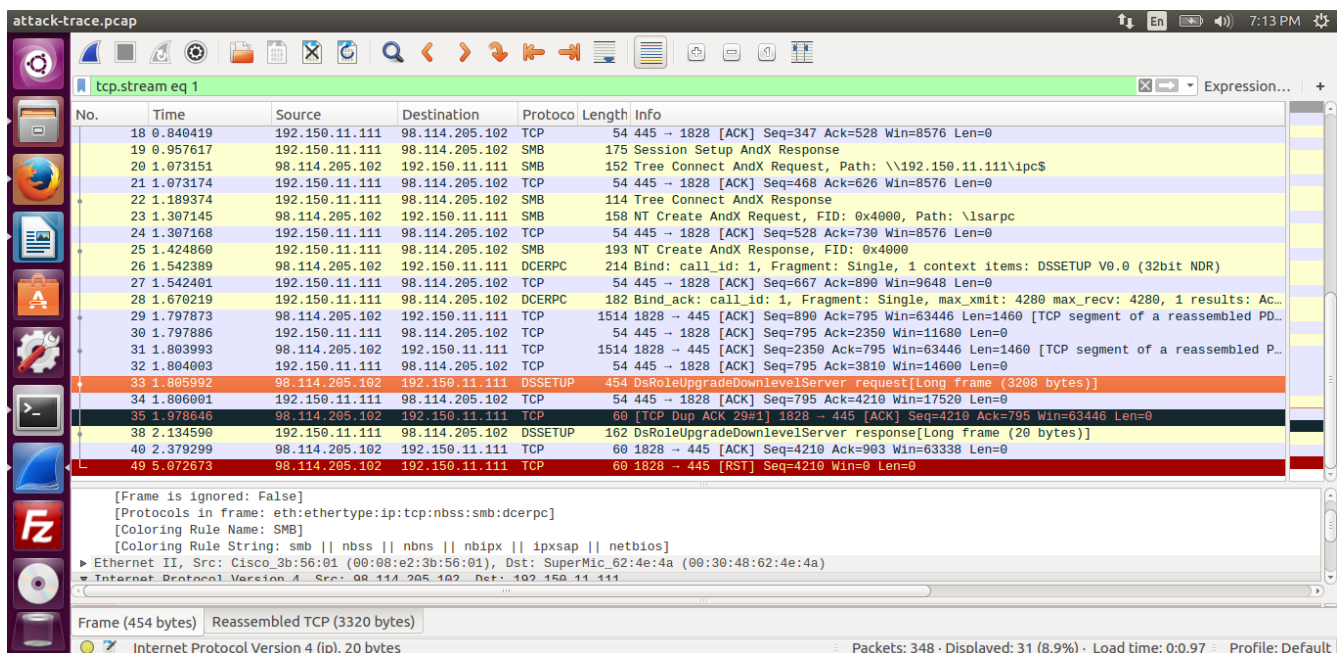
2- Establishes SMB session as null user over 445, connects to LSARPC named pipe and calls DeRoleUpgradeDownLevelServer() with a long szdomain name parameter containing a shell code of "bind shell", you can see long frame in snapshot



Now, the victim has a new tcp socket listening on port 1957, with a command shell bound to it. So the attacker will connect to this port, to send to the victim commands needed to download the malware

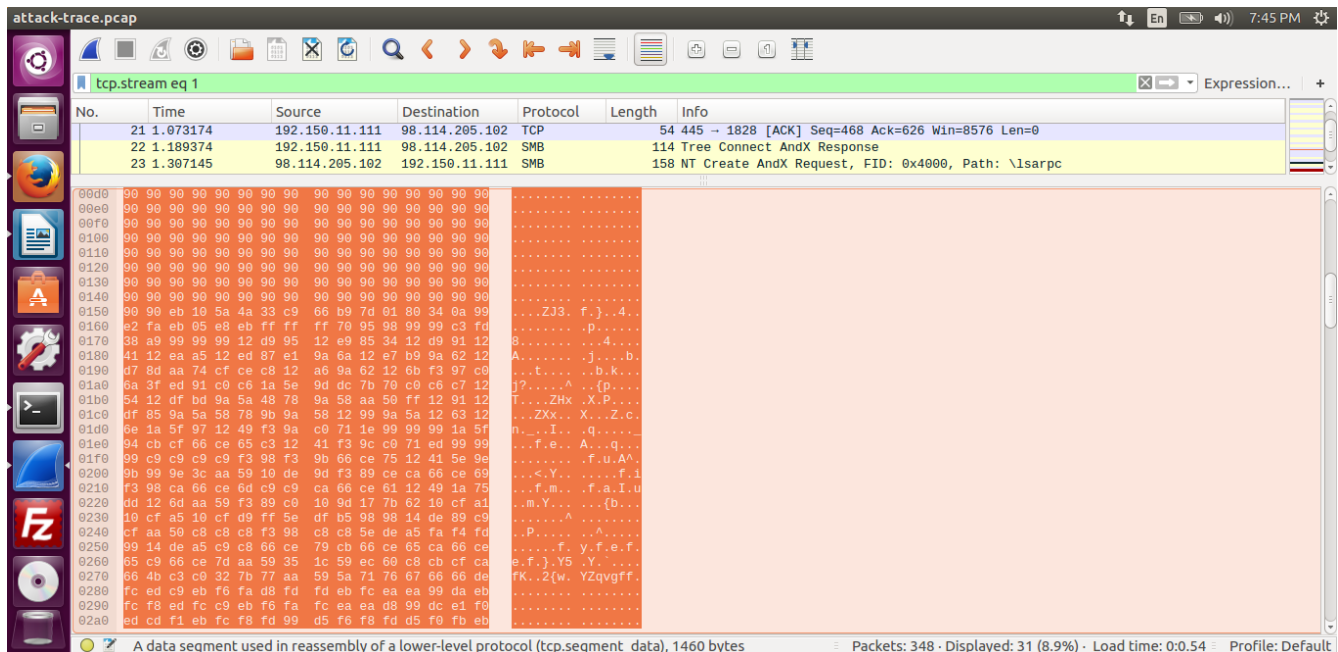


Then the victim will initiate an FTP connection to the attacker and will try to download a file name ssms.exe:



Q- What actions does the shellcode perform? Pls list the shellcode.

Ans- Shell code uses well-known methods to get functions' offsets and to build stack frames.



Q- Do you think a Honeypot was used to pose as a vulnerable victim? Why?

Ans . Yes because system reports itself as running a window operating system , which is a lie .

Q- Do you think this is a manual or an automated attack? Why?

Ans- The attacks seems automatic because 16 seconds are very minimal time for human attacker to perform an attack.

THE END