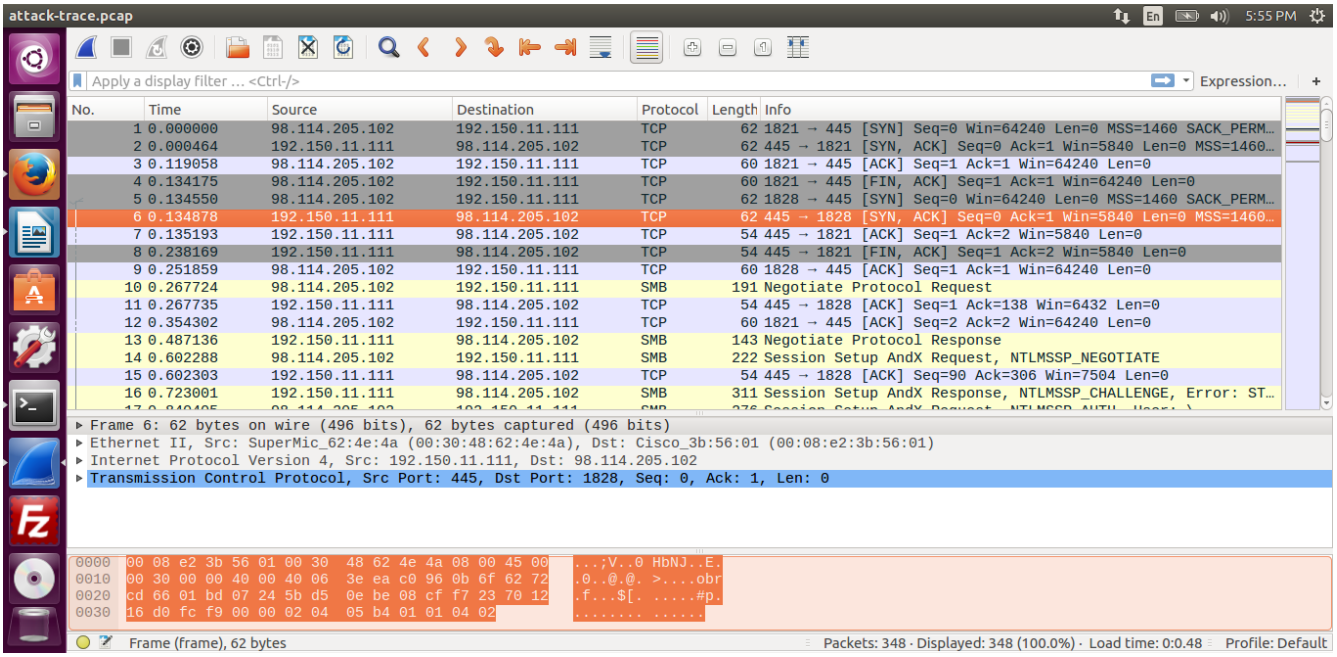
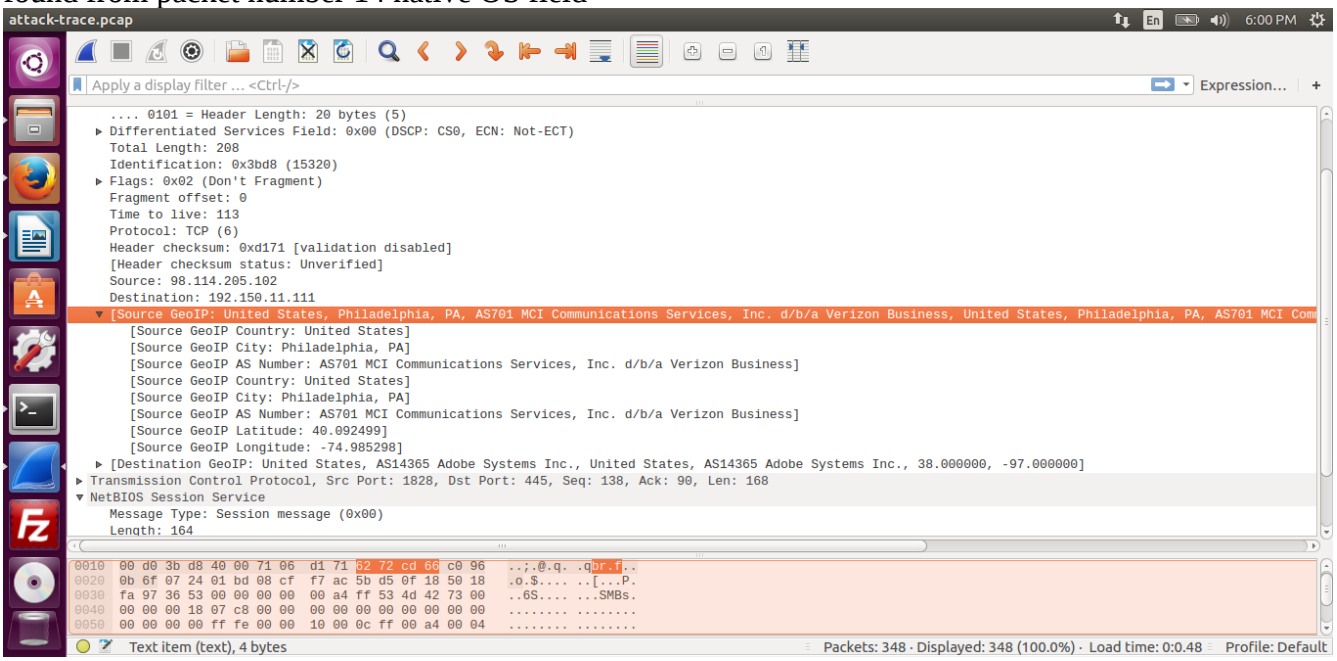
Q- Which systems (i.e. IP addresses) are involved?
Ans- Ip of attacker 98.114.205.102 and ip of victim 192.150.11.111



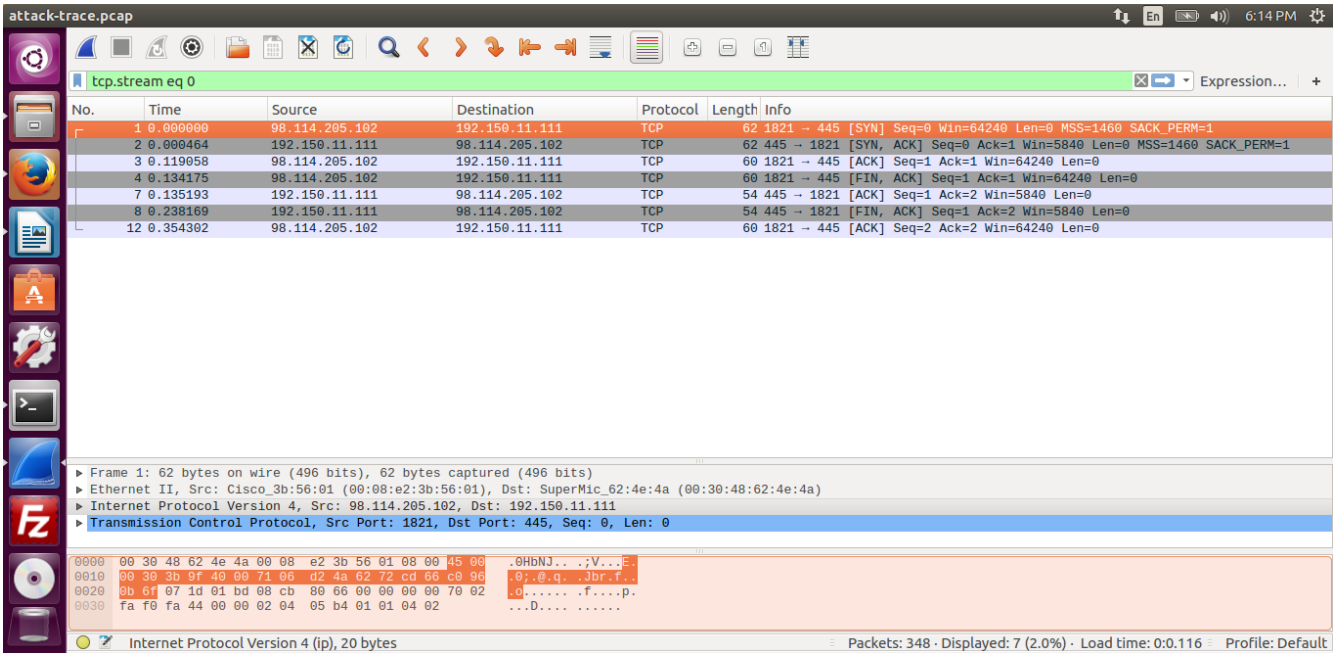
Q- What can you find out about the attacking host ?
Location of attacker is found from packet and operating system of attacker is windows 2000 that is found from packet number 14 native OS field

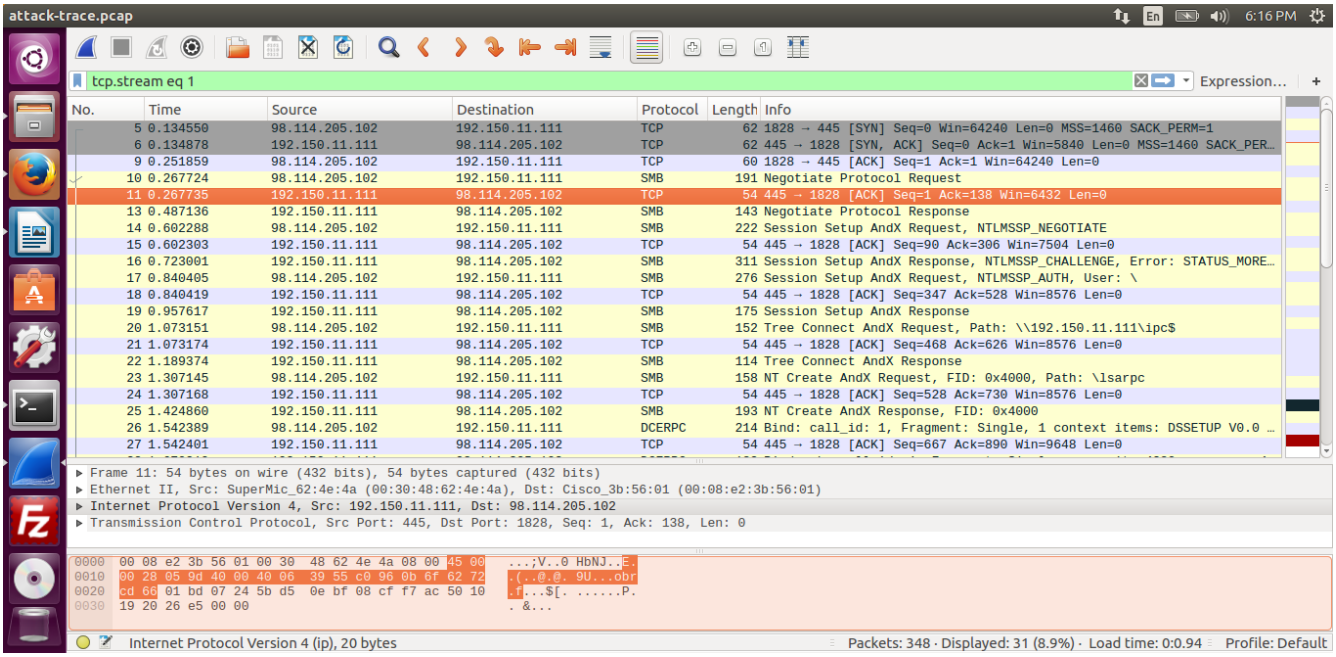


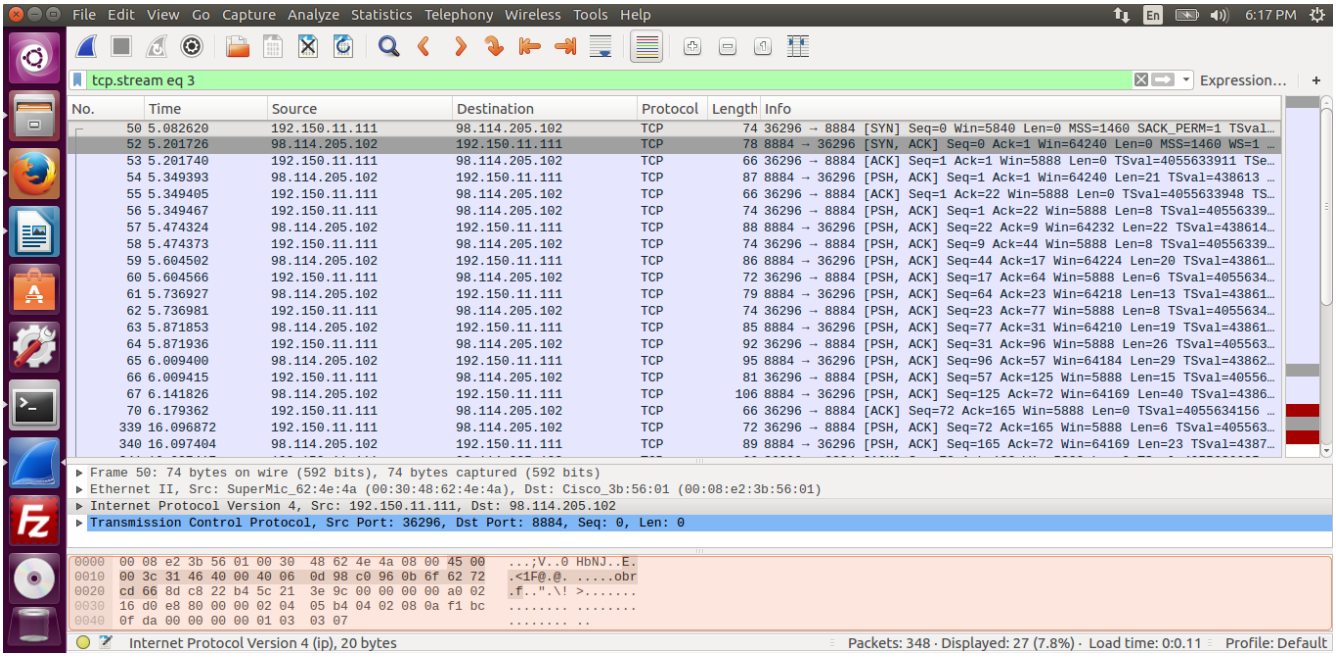
Q- How many TCP sessions are contained in the dump file?

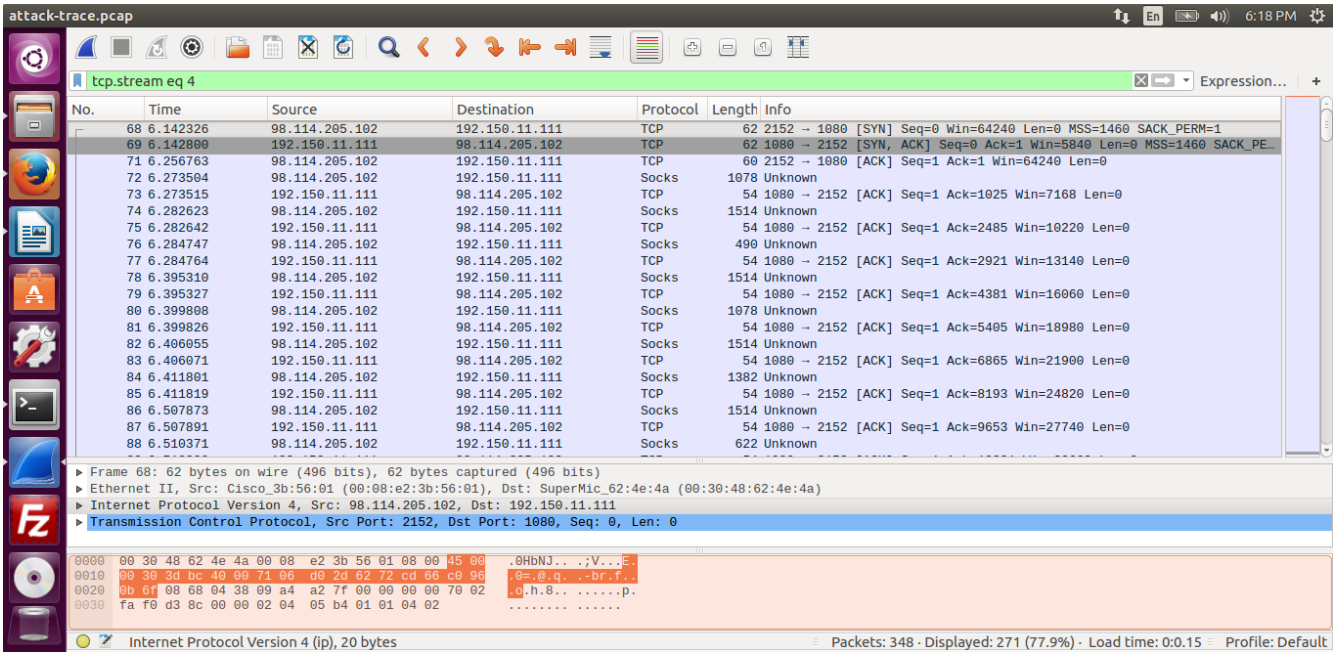
5 sessions

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



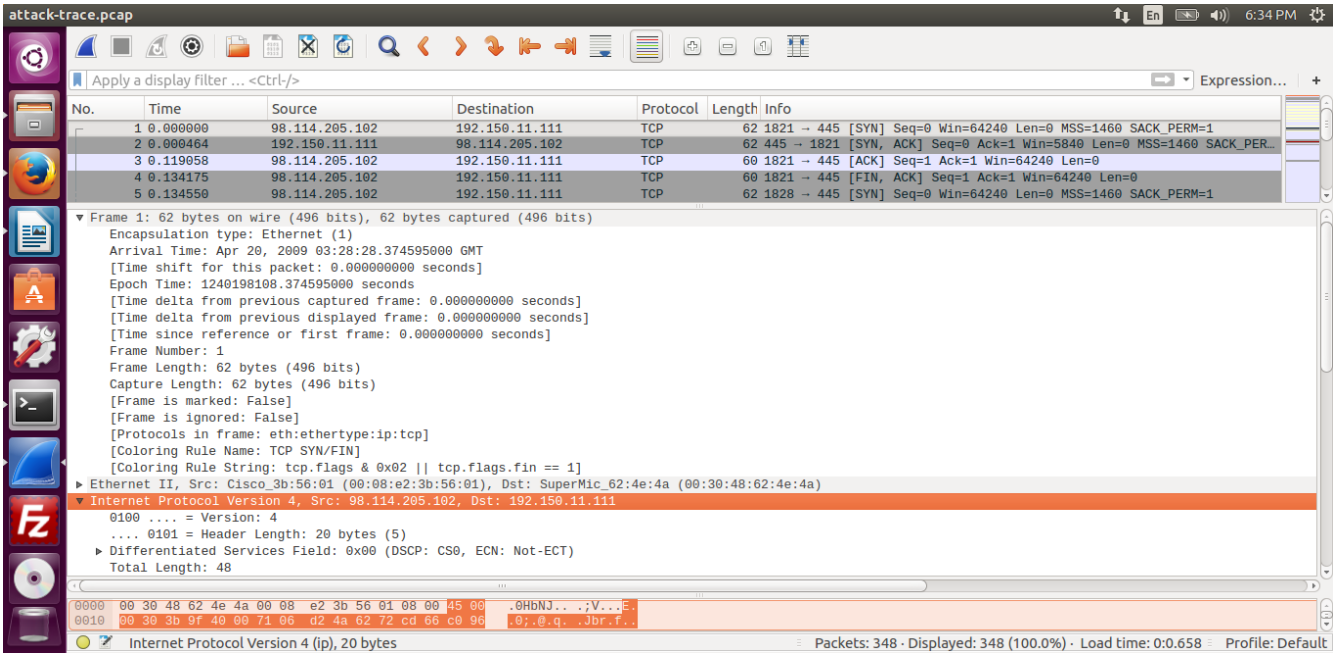


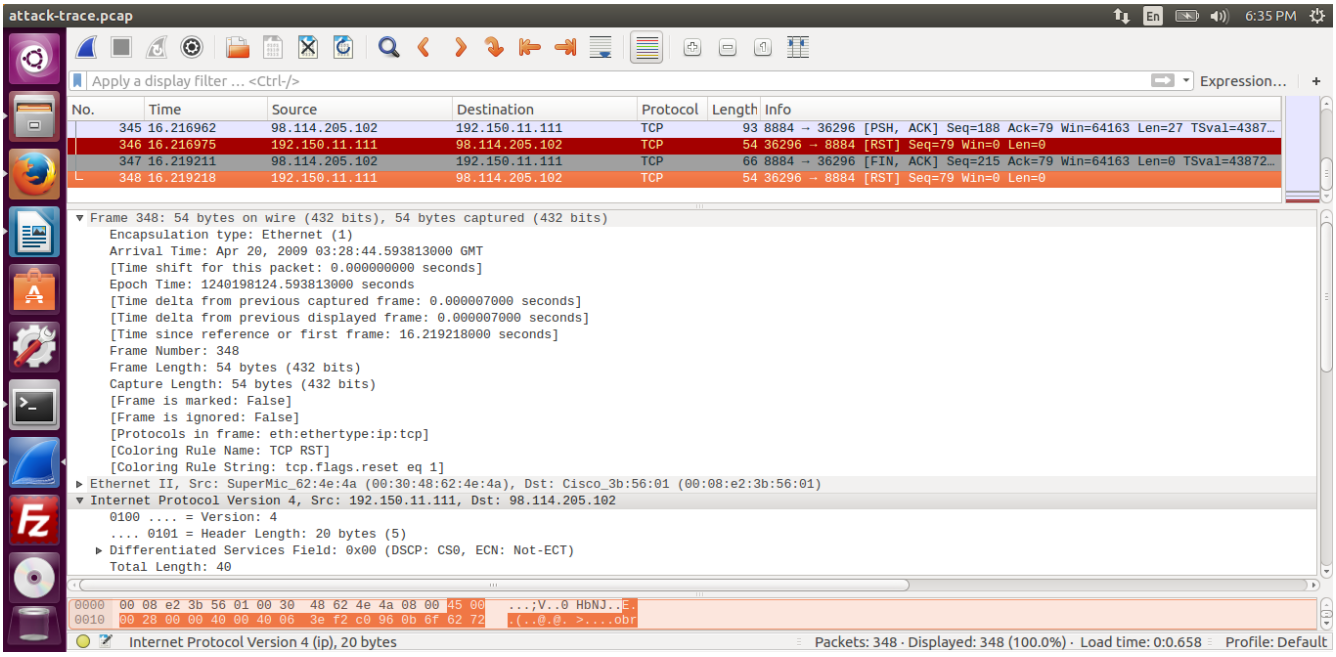




Q- How long did it take to perform the attack?

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

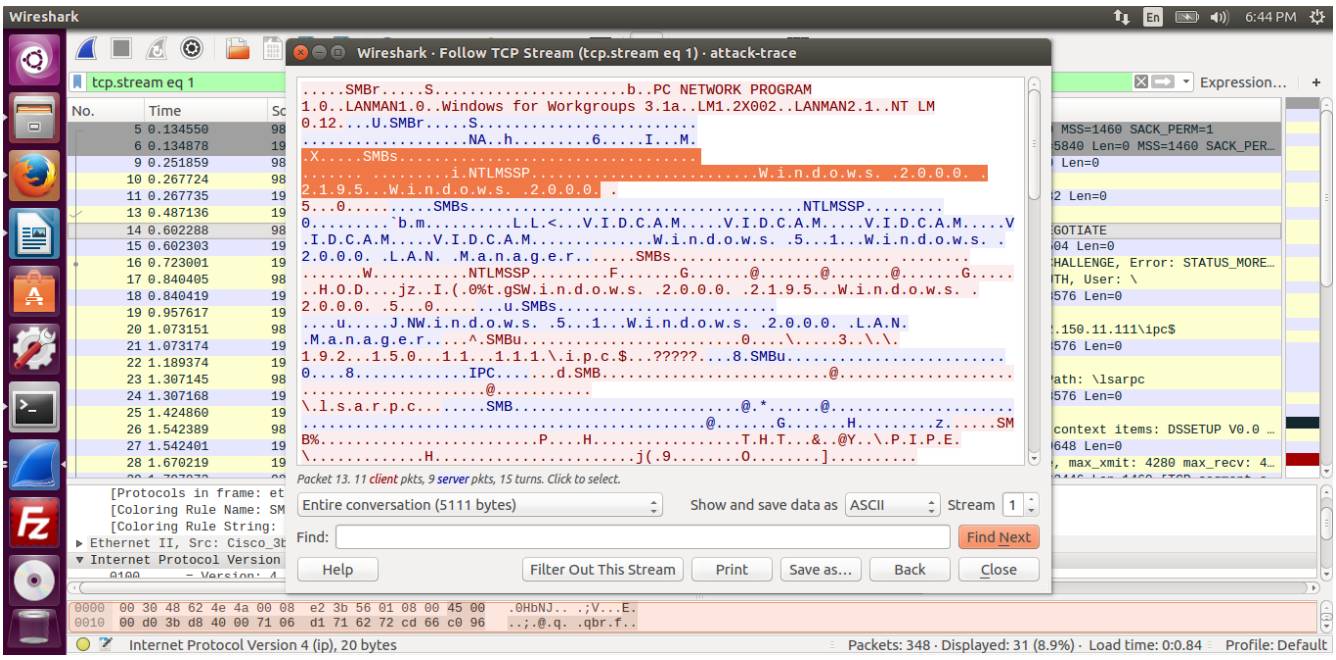


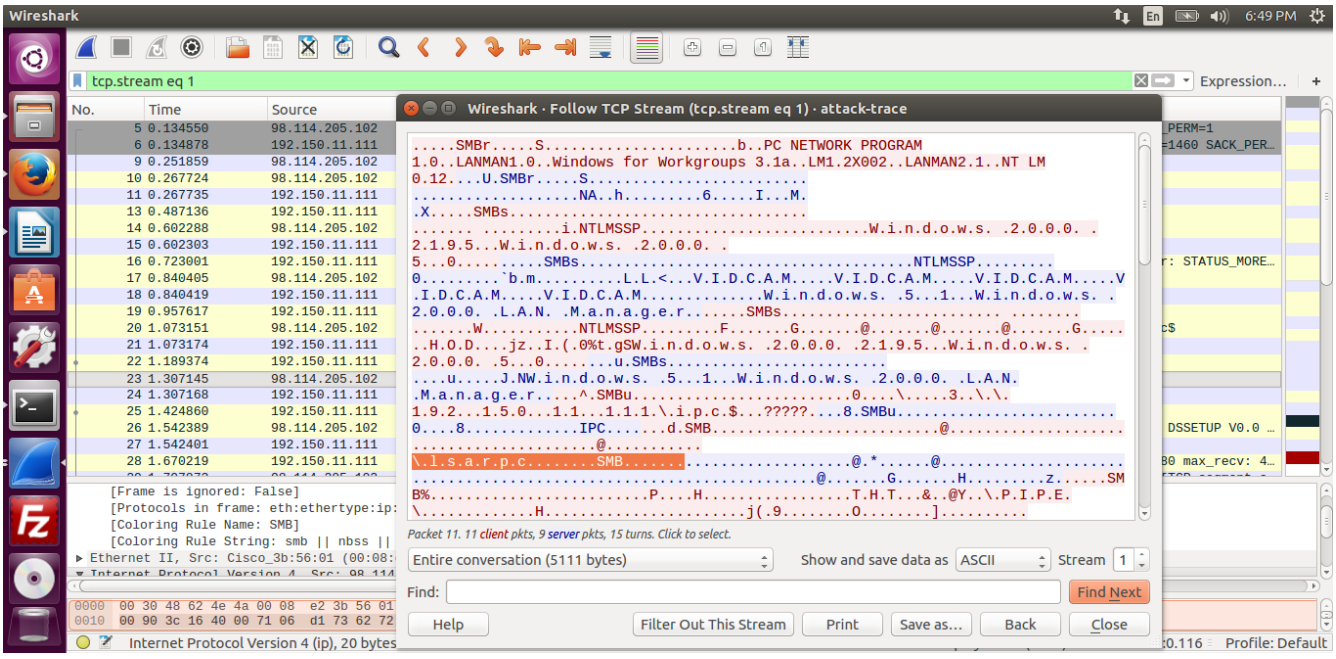


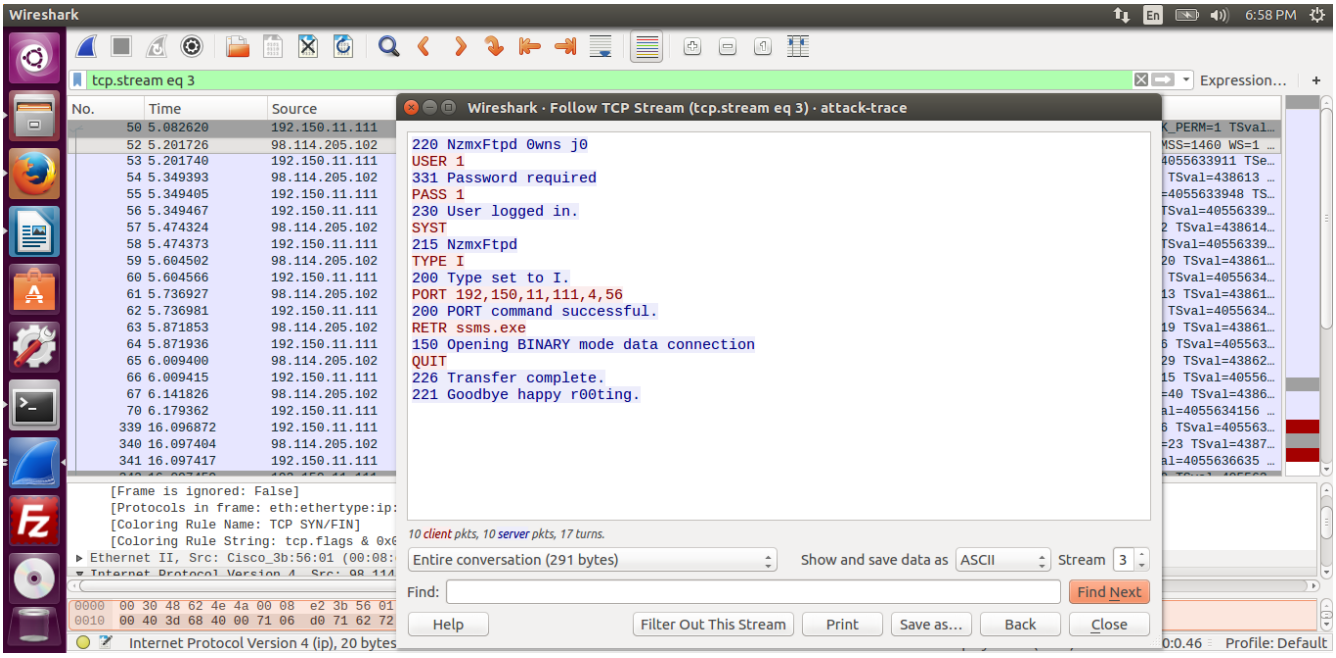
Q- Which operating system was targeted by the attack? And which service? Which vulnerability?

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"

.

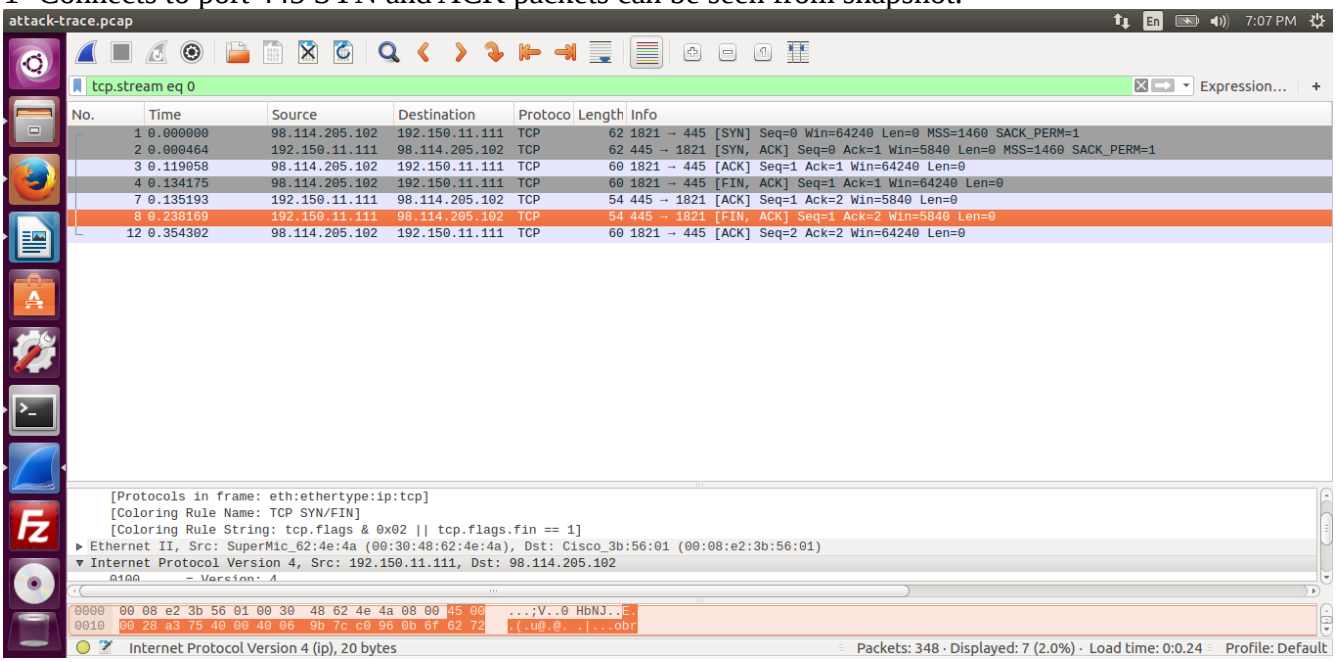

Wireshark
6:44 PM
Wireshark · Follow TCP Stream (tcp.stream eq 1) · attack-trace
tcp.stream eq 1
Expression…
No.
Time
Packet 13. 11 client pkts, 9 server pkts, 15 turns. Click to select.
Entire conversation (5111 bytes)
Show and save data as
ASCII
Stream
Find:
Find Next
Help
Filter Out This Stream
Print
Save as…
Back
Close
Internet Protocol Version 4 (ip), 20 bytes
Packets: 348 · Displayed: 31 (8.9%) · Load time: 0:0.84
Profile: Default


Wireshark
6:49 PM
Wireshark · Follow TCP Stream (tcp.stream eq 1) · attack-trace
tcp.stream eq 1
Expression…
No.
Time
Source
Packet 11. 11 client pkts, 9 server pkts, 15 turns. Click to select.
Entire conversation (5111 bytes)
Show and save data as
ASCII
Stream
Find:
Find Next
Help
Filter Out This Stream
Print
Save as…
Back
Close
Internet Protocol Version 4 (ip), 20 bytes
Profile: Default

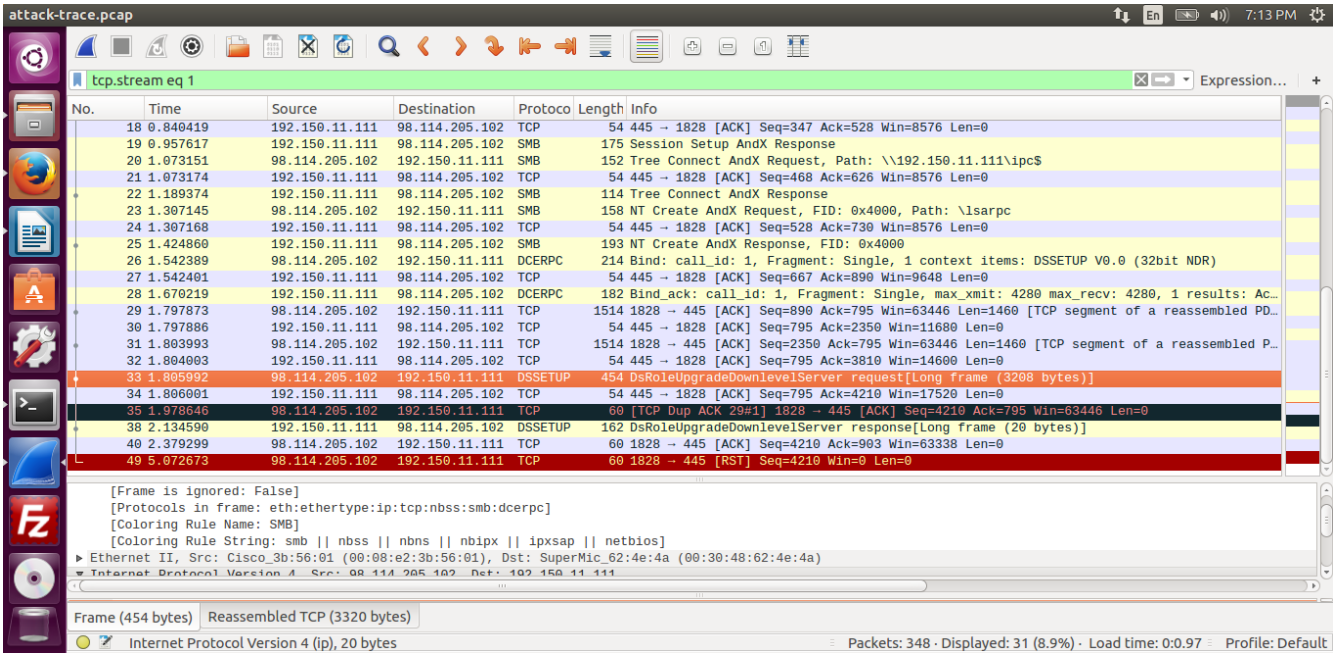


Q- Can you sketch an overview of the general actions performed by the attacker

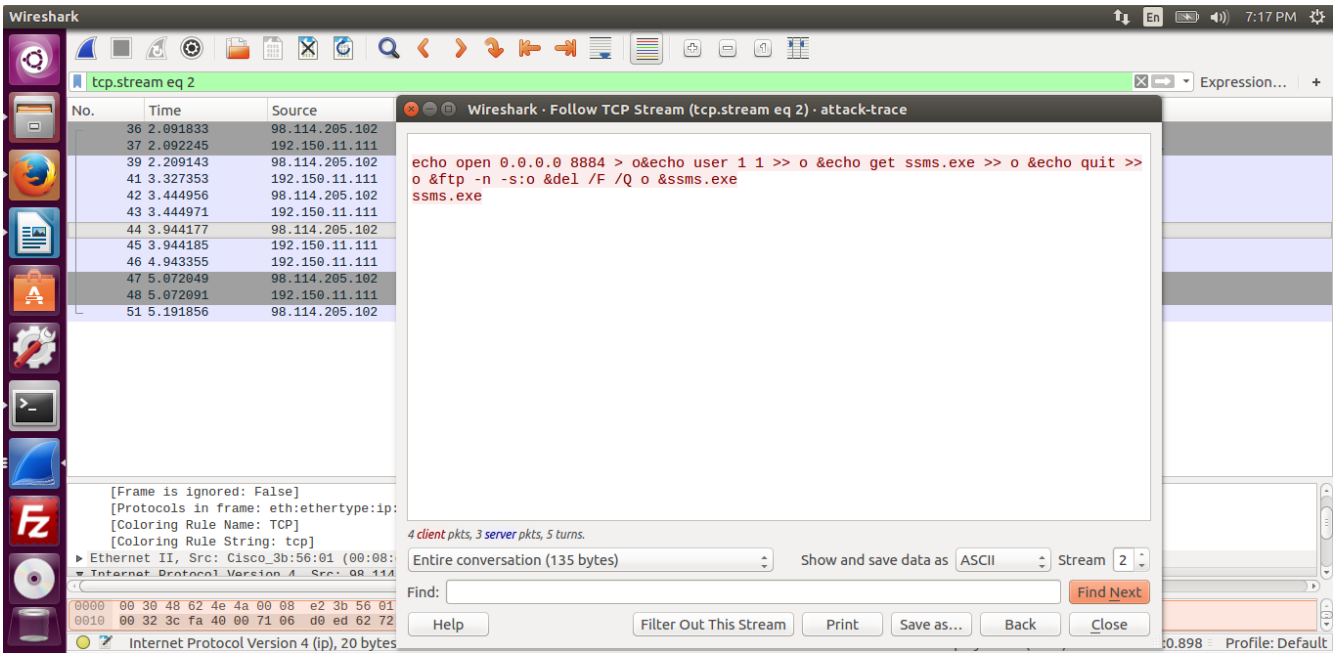
1- Connects to port 445 SYN and ACK packets can be seen from snapshot.



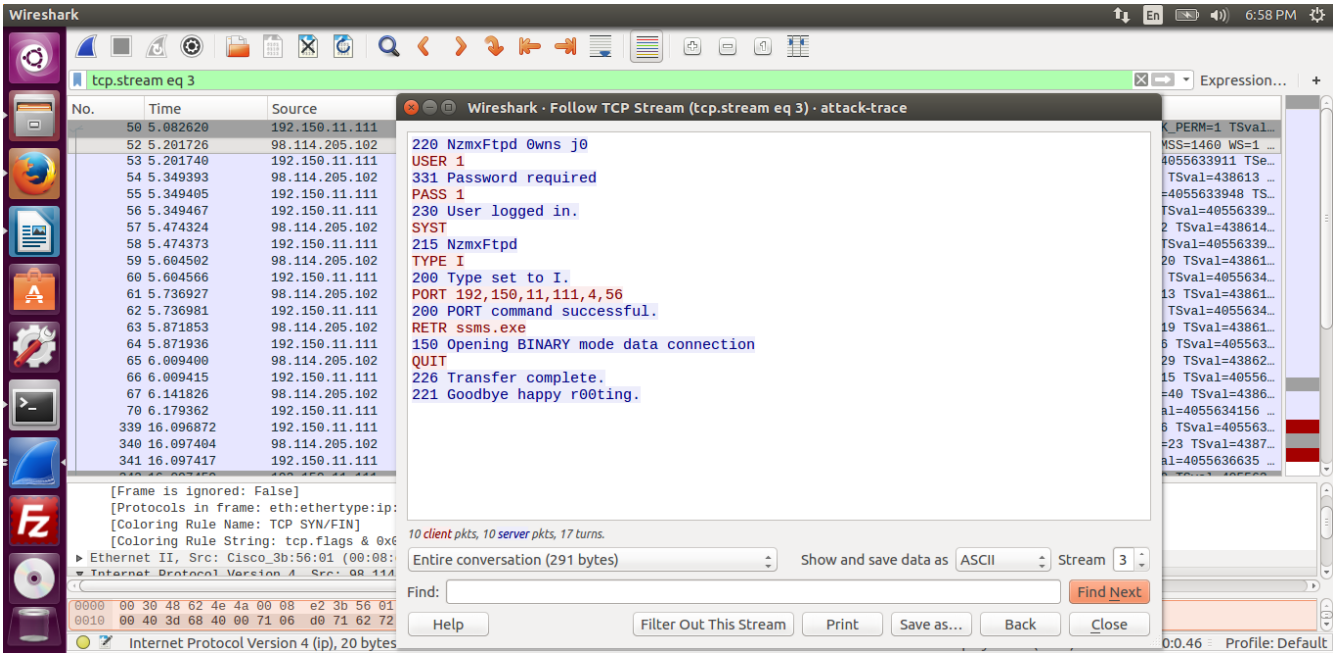
2-Establishes SMB session as null user over 445 , connects to LSARPC named pipe and calls DeRoleUpgradeDownLevelServer() with a long szdomain name parameter containing a shell code of “bind shell” , you can see long frame in snapshot



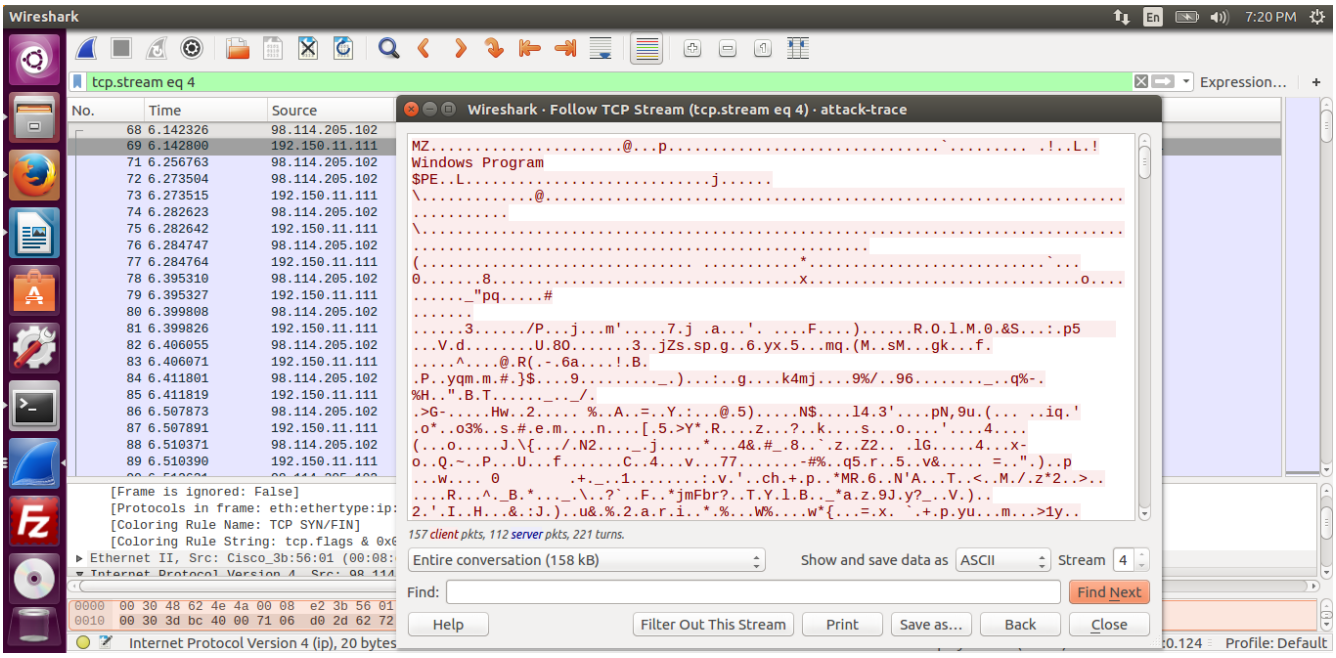
Now, the victim has a new tcp socket listening on port 1957, with a command shell bound to it.So the attacker will connect to this port, to send to the victim commands needed to download the malware



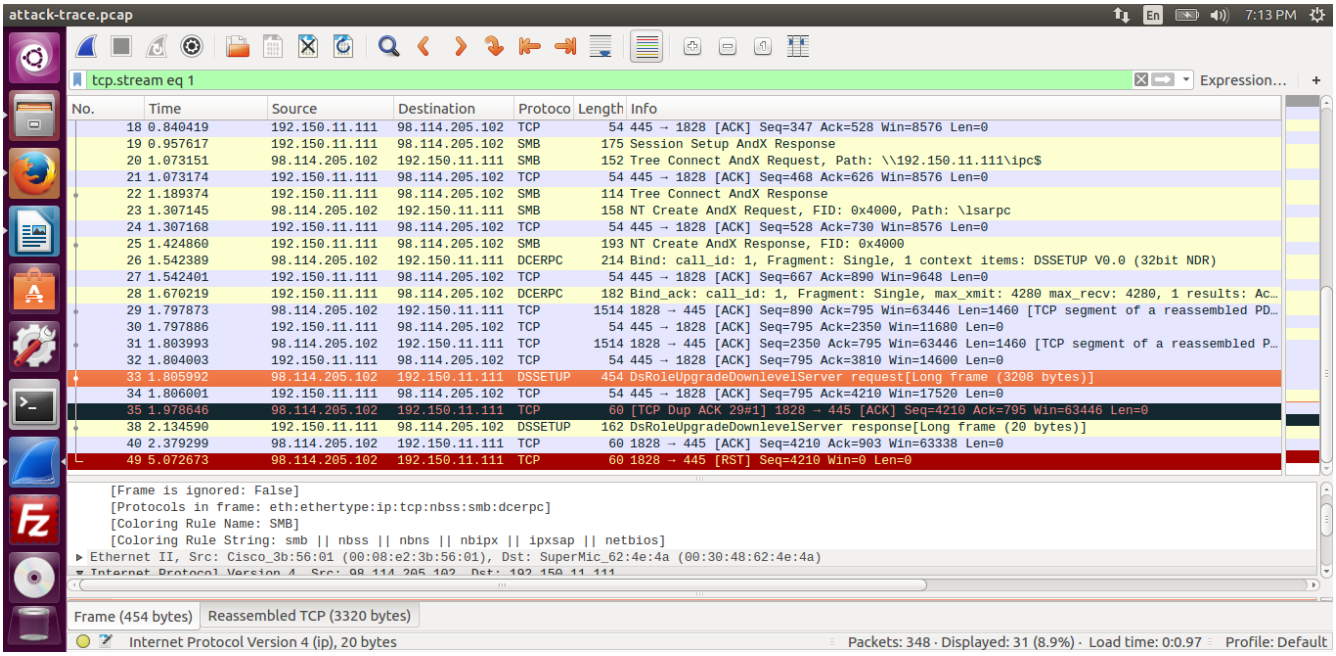
Then the victim will initiate an FTP connection to the attacker and will try to download a file name ssms.exe:



Then attacking hosts will then connect back to the victim on the annouced tcp port (PORT command) The malware is retrieved, and executed on the victim , Portable executeable file is being downloaded as shown ..

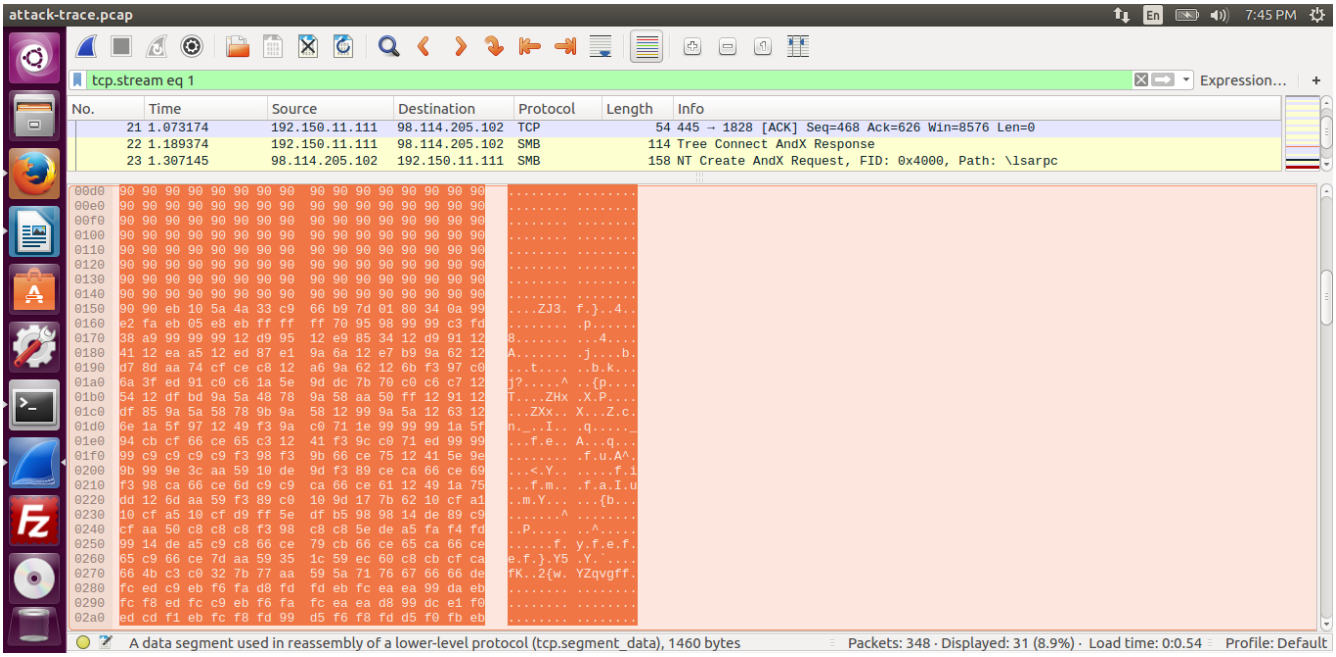


Q- What specific vulnerability was attacked?
Ans-
The MS04-11 vulnerability was attacked and exploited.This vulnerability exploit a lack of array boundary checking in a LSASS function (Operation: DsRoleUpgradeDownlevel Server) which lead to a buffer overflow and could be use to execute code remotely.



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