Traffic Analysis Investigative Report

For: CSIA 6250

Prepared by:

Joshua Hesch

2/7/2021

Table of Contents

Table of Figures

Executive Summary

The compromise that was investigated happened on November 21, 2015 at 9:03 AM MST. This compromise took place within the network that was compromised. The compromise started with the intruder performing scans looking for a way to get on the computer that was compromised. The compromise started on the computer with the IP address 10.0.7.54 running Linux. This was determined by looking at the time to live which was 64. This is consistent with Linux. The attack failed with the IP address 10.0.7.54.

The intruder was successful in the attack with IP address 10.0.7.50. The computer compromised had an IP address of 10.210.210.210 running Windows server 2003. The intruder transferred files onto the computer used to extract passwords. The files used to extract passwords in the compromise were pwdump2.exe and samdump.dll. The intruder was able to extract password hashes to the file l.txt. The intruder than exported the file to 10.0.7.50. The intruder deleted the files that were used in the compromise when the attack was finished.

It is the recommendation to use an internal firewall. Firewalls can lead the attacker to empty hosts and/or honey pots. This can make the attackers job a lot harder and provide a bigger window for them to be caught. Also, all ports that are not necessary should be closed. Finally, this attack could have been avoided using a patch from Microsoft, security bulletin MS03-039. It is recommended to keep all devices on the network updated.

Investigation Details

This investigation was conducted by examining pcap files in in Wireshark version 3.4.3. The files examined were hack_analysis.pcap and hack_analysis_b_capture.pcap. The files were examined on a Microsoft Surface laptop 3 running Windows 10 home. The following Wireshark filter was used to isolate the attack traffic 'not(tcp.port==80) and not(tcp.port==389) and not(udp.srcport==137 and udp.dstport==137) and not(arp)'.

The examination started with viewing hack_analysis.pcap in Wireshark. The attack started on November 21, 2015 at 9:03 AM MST. This was determined by looking at the first packet in the attack from 10.0.7.54 to 10.210.210.210. The intruder began performing a stealth port scan on 10.210.210.210 running Windows Server 2003. This was determined because open ports sequence was SYN, SYN/ACK, RST and closed port sequence was SYN, RST/ACK. Port Scan ran from packet number 20 – 2026. Port 21 was protected by tls-auth. The intruder failed to gain access to 10.210.210.210 via SMB protocol. The intruder began scanning ports from 10.0.7.50 to 10.210.210.210. Port scan ran from packet number 2193 – 4200. The intruder tried to gain access through LSASS vulnerability via buffer overrun. This vulnerability attack was not successful. The intruder gained entry to 10.210.210.210 via buffer overrun in RPCSS service. The intruder used trivial file transfer protocol to transfer pwdump2.exe to 10.210.210.210. The file is used to extract password hashes for user accounts. The above items were found by using the

analyze – follow feature in Wireshark and following each stream. This concluded examining the file hack_analysis.pcap.

The second file that was examined was hack_analysis_b_capture.pcap. This file was examined in Wireshark. The intruder transferred samdump.dll to assist in exporting the user passwords. The intruder extracted the password hashes to the file l.txt via pwdump2.exe. The intruder copied the file to 10.0.7.50 via trivial file transfer protocol. The intruder than deleted the following files pwdump2.exe, samdump.dll, and l.txt. The attack was concluded after the deletion of the files. The above items were found by using the analyze – follow feature in Wireshark and following each stream.

Conclusion

In conclusion, this attack was successful using the vulnerability located in Microsoft Security Bulletin MS03-039. This vulnerability was labeled as critical by Microsoft for Windows Server 2003. The skill level of the attack is believed to be a medium level on a scale of low, medium, and high. This determination was made because the attack was successful, however if the attacker had more experience than they would not have tried to use the LSASS vulnerability. This vulnerability is labeled as low for Windows Server 2003.

References

Chandel, R. (2017, August 20). *Understanding Nmap scan with wireshark.* Hacking Articles. https://www.hackingarticles.in/understanding-nmap-scan-wireshark/

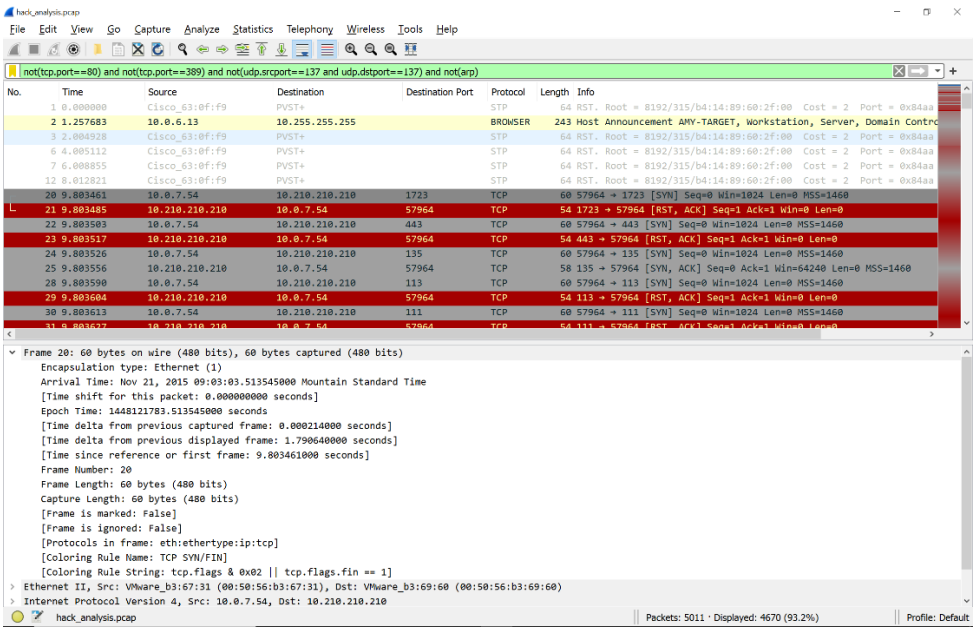
Microsoft. (2004, August 10). *Microsoft security bulletin MS04-011 – Critical.* https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2004/ms04-011?redirectedfrom=MSDN

Microsoft. (2003, September 10). *Microsoft security bulletin MS03-039- Critical*. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2003/ms03-039?redirectedfrom=MSDN

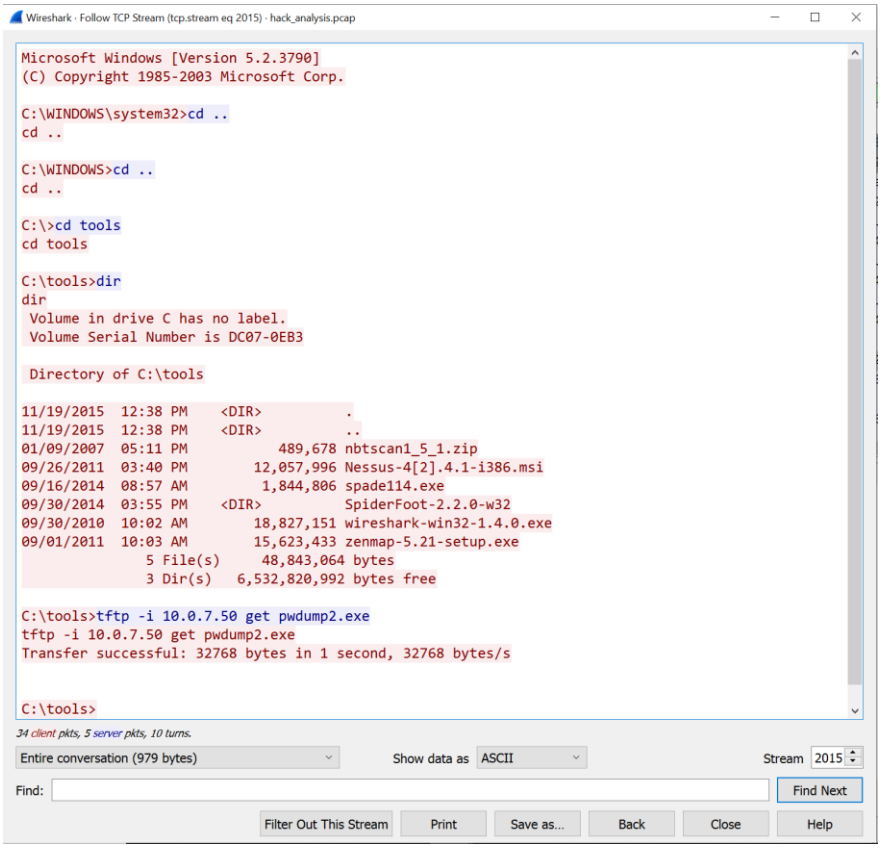
opadmin. (2019, May 9). *Everything you need to know about port scan attack.* Open Port. https://openport.net/everything-you-need-to-know-about-port-scan-attack/

Appendix

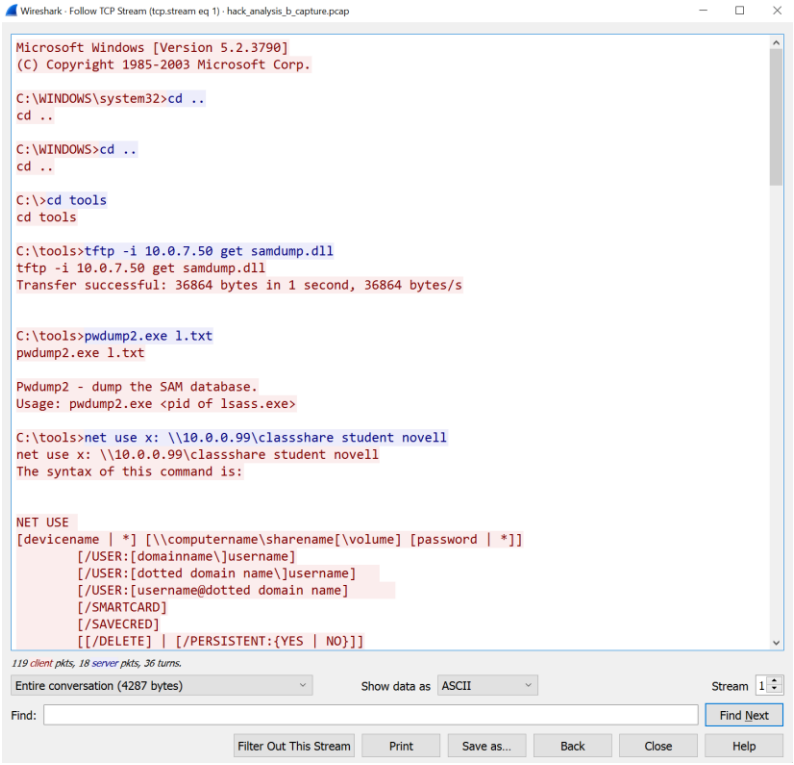
1 Start of Attack



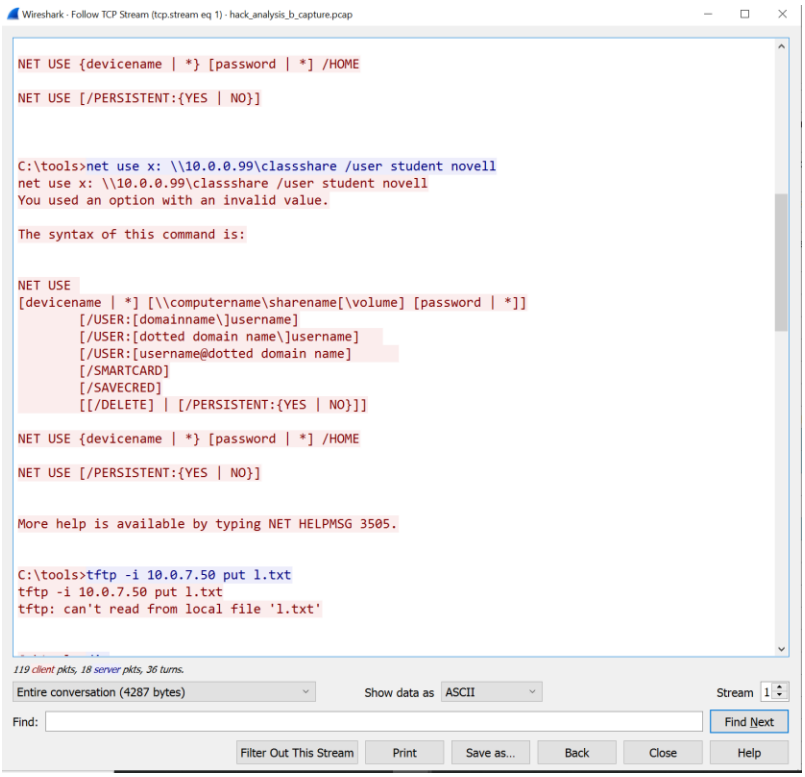
2 pwdump2



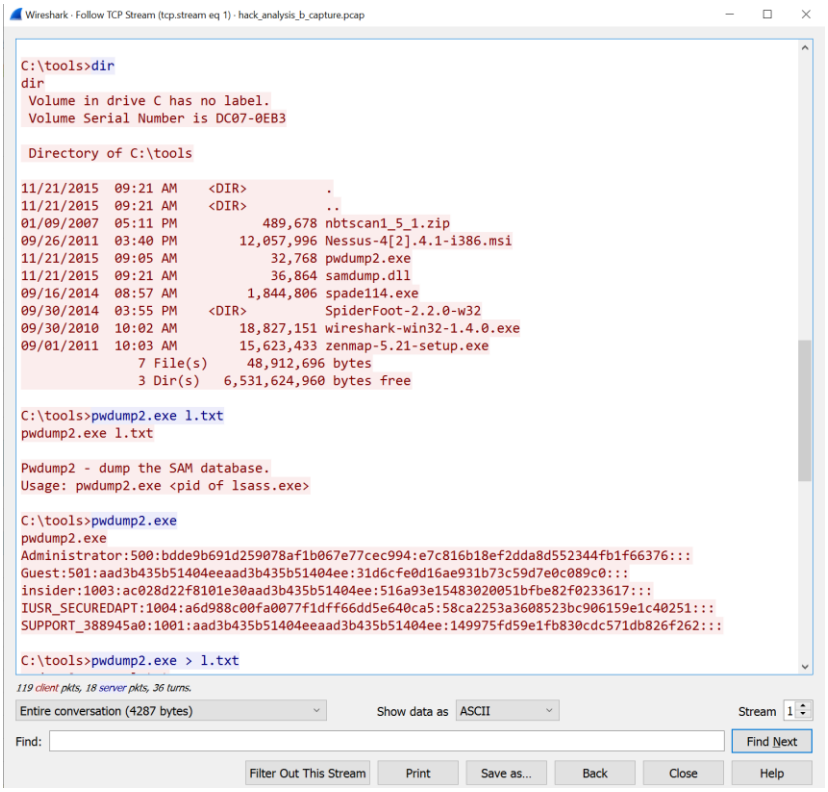
3 pwdump2, samdump, l.txt



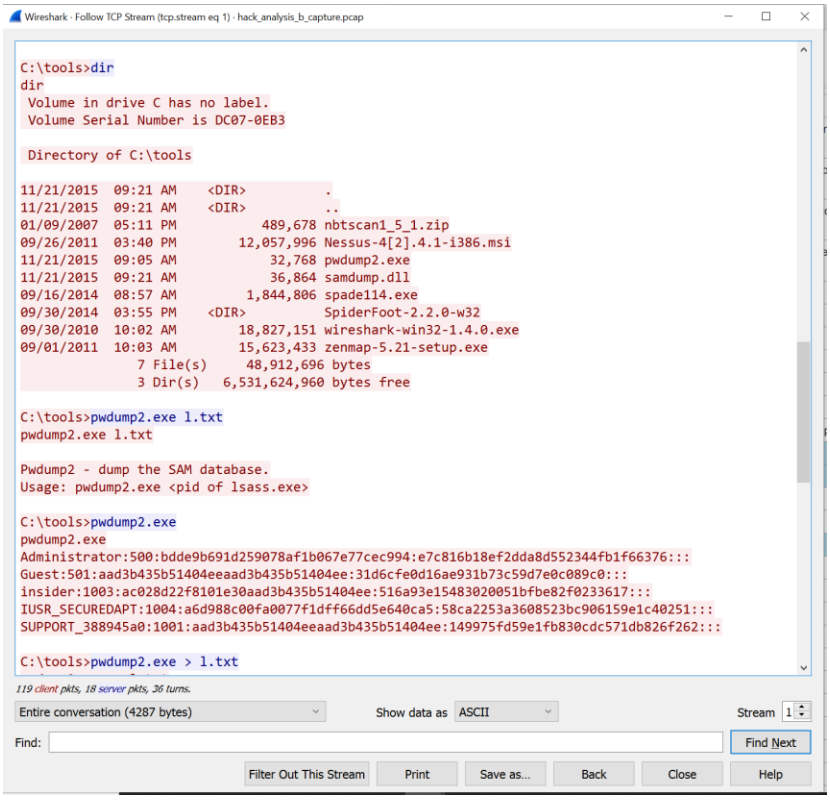
4pwdump2, samdump, l.txt



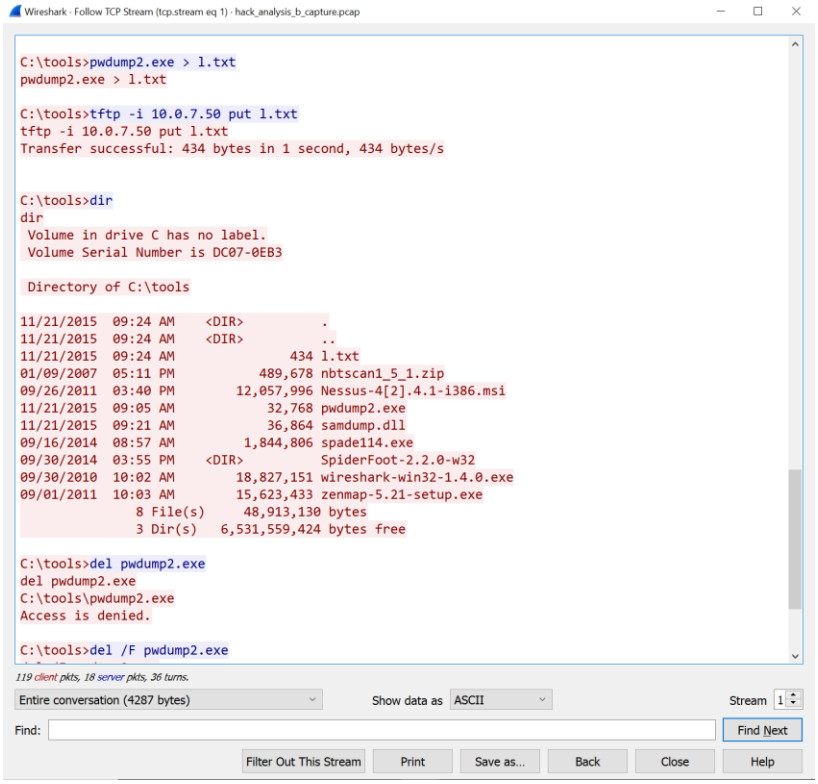
5 pwdump2, samdump, l.txt



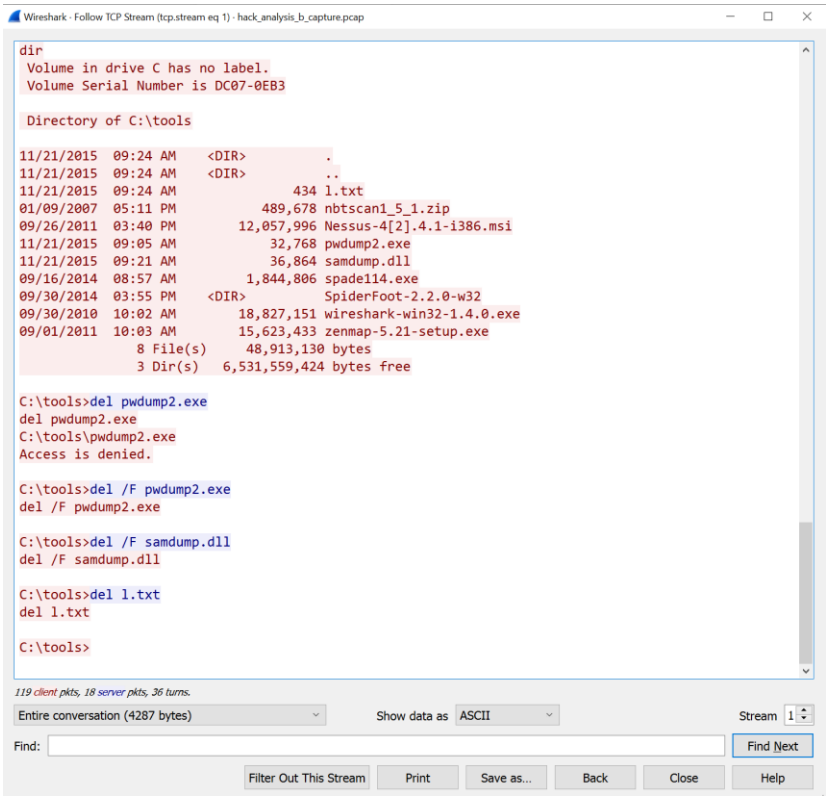
6 pwdump2, samdump, l.txt



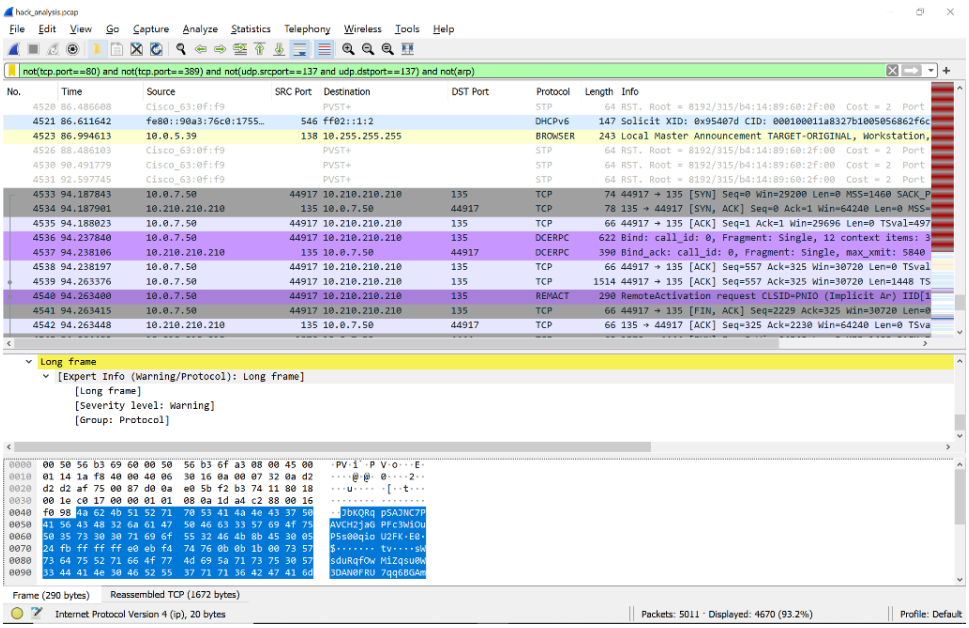
7 pwdump2, samdump, l.txt



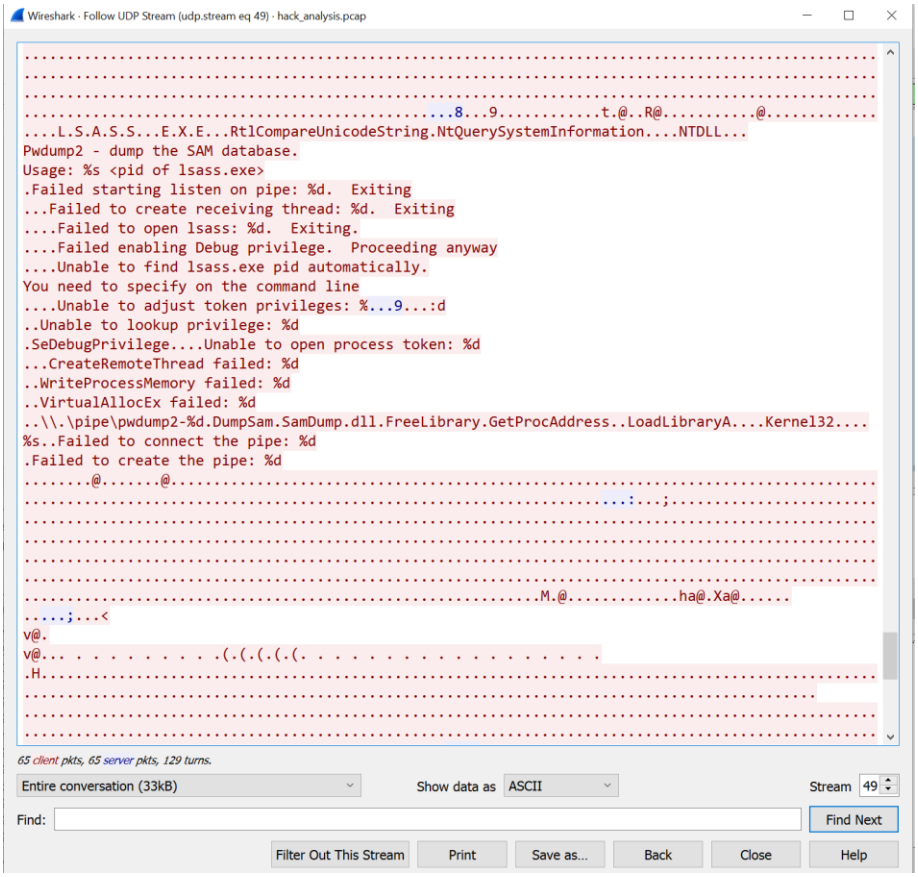
8 pwdump2, samdump, l.txt



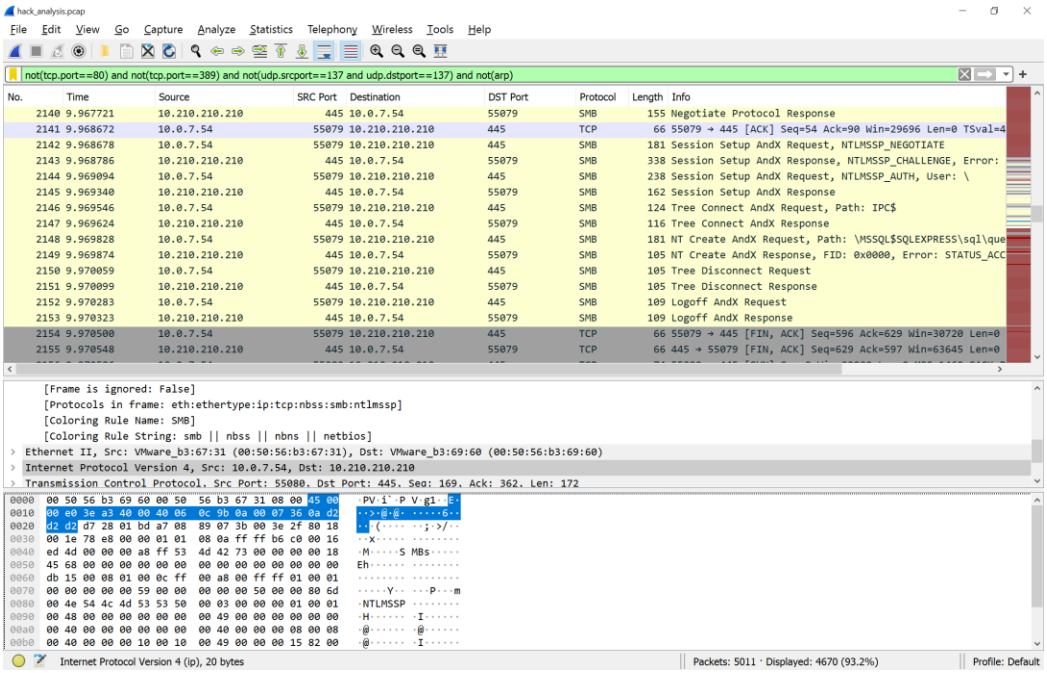
9 Buffer Overrun in RPCSS



10 Failed LSASS vulnerability



11 SMB Failed



12 10.0.7.50 Port Scan