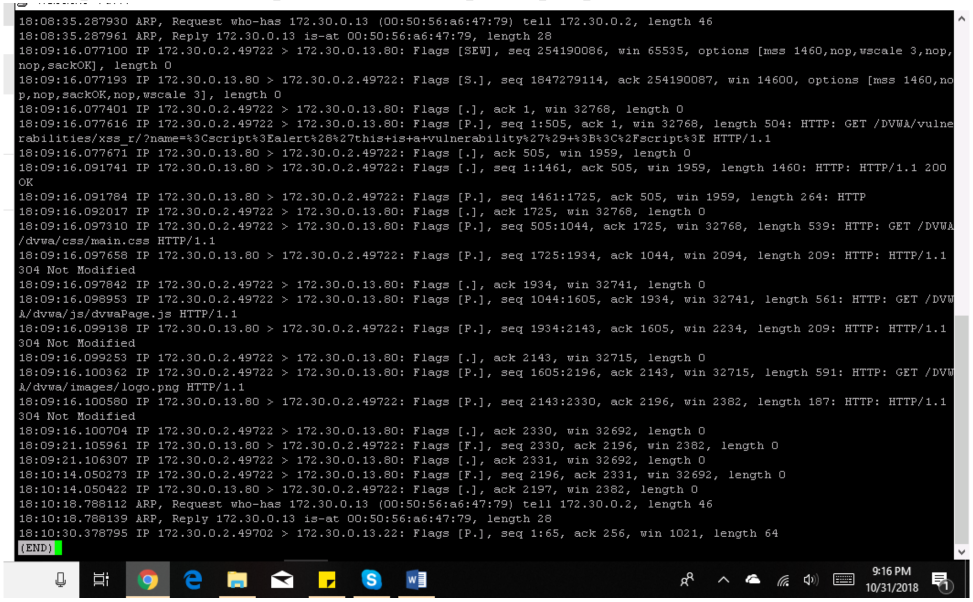
MARYMOUNT UNIVERSITY

Assignment: IT557; Monitoring, Auditing, and Penetration Testing
Assigned: Nov. 4, 2018
Instructor: Professor Ali Bicak
Student Name: George Boakye

LAB REPORT FILE (LAB7)

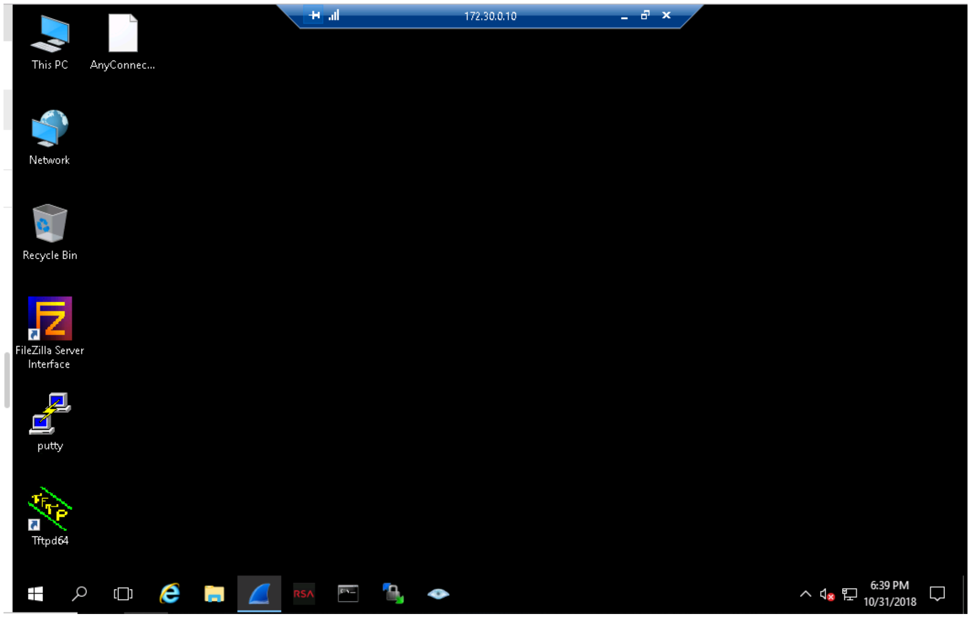
SECTION 1

Part 1: Step 25: Alert script within the tcpdumpcapturefile file (9th line from the top)

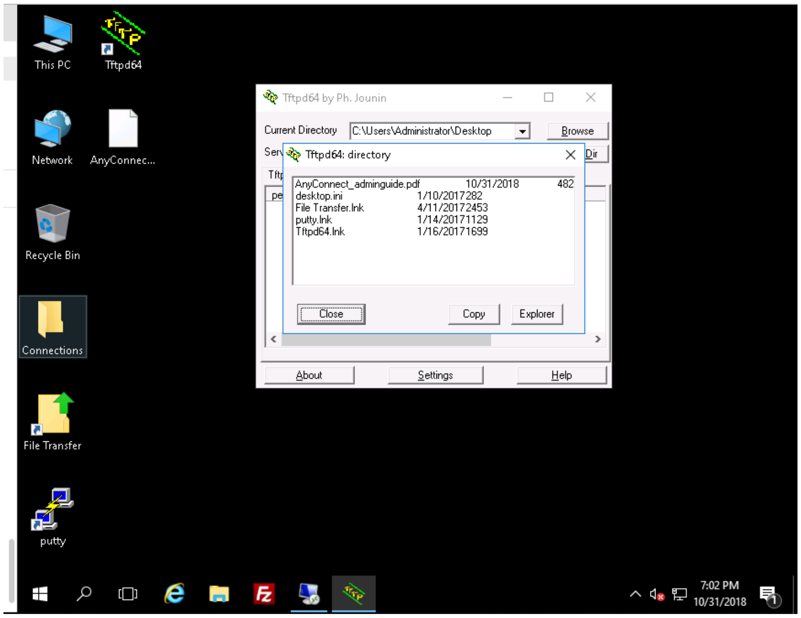


```
18:08:35.287930 ARP, Request who-has 172.30.0.13 (00:50:56:a6:47:79) tell 172.30.0.2, length 46
18:08:35.287961 ARP, Reply 172.30.0.13 is-at 00:50:56:a6:47:79, length 28
18:09:16.077100 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [SEW], seq 254190086, win 65535, options [mss 1460,nop,wscale 3,nop,
nop,sackOK], length 0
18:09:16.077193 IP 172.30.0.13.80 > 172.30.0.2.49722: Flags [S.], seq 1847279114, ack 254190087, win 14600, options [mss 1460,no
p,nop,sackOK,nop,wscale 3], length 0
18:09:16.077401 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [.], ack 1, win 32768, length 0
18:09:16.077616 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [P.], seq 1:505, ack 1, win 32768, length 504: HTTP: GET /DVWA/vulne
rabilities/xss_r/?name=%3Cscript%3Ealert%28%27this+is+a+vulnerability%27%29+%3B%3C%2Fscript%3E HTTP/1.1
18:09:16.077671 IP 172.30.0.13.80 > 172.30.0.2.49722: Flags [.], ack 505, win 1959, length 0
18:09:16.091741 IP 172.30.0.13.80 > 172.30.0.2.49722: Flags [.], seq 1:1461, ack 505, win 1959, length 1460: HTTP: HTTP/1.1 200
OK
18:09:16.091784 IP 172.30.0.13.80 > 172.30.0.2.49722: Flags [P.], seq 1461:1725, ack 505, win 1959, length 264: HTTP
18:09:16.092017 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [.], ack 1725, win 32768, length 0
18:09:16.097310 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [P.], seq 505:1044, ack 1725, win 32768, length 539: HTTP: GET /DVWA
/dvwa/css/main.css HTTP/1.1
18:09:16.097658 IP 172.30.0.13.80 > 172.30.0.2.49722: Flags [P.], seq 1725:1934, ack 1044, win 2094, length 209: HTTP: HTTP/1.1
304 Not Modified
18:09:16.097842 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [.], ack 1934, win 32741, length 0
18:09:16.098953 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [P.], seq 1044:1605, ack 1934, win 32741, length 561: HTTP: GET /DVW
A/dvwa/js/dvwaPage.js HTTP/1.1
18:09:16.099138 IP 172.30.0.13.80 > 172.30.0.2.49722: Flags [P.], seq 1934:2143, ack 1605, win 2234, length 209: HTTP: HTTP/1.1
304 Not Modified
18:09:16.099253 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [.], ack 2143, win 32715, length 0
18:09:16.100362 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [P.], seq 1605:2196, ack 2143, win 32715, length 591: HTTP: GET /DVW
A/dvwa/images/logo.png HTTP/1.1
18:09:16.100580 IP 172.30.0.13.80 > 172.30.0.2.49722: Flags [P.], seq 2143:2330, ack 2196, win 2382, length 187: HTTP: HTTP/1.1
304 Not Modified
18:09:16.100704 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [.], ack 2330, win 32692, length 0
18:09:21.105961 IP 172.30.0.13.80 > 172.30.0.2.49722: Flags [F.], seq 2330, ack 2196, win 2382, length 0
18:09:21.106307 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [.], ack 2331, win 32692, length 0
18:10:14.050273 IP 172.30.0.2.49722 > 172.30.0.13.80: Flags [F.], seq 2196, ack 2331, win 32692, length 0
18:10:14.050422 IP 172.30.0.13.80 > 172.30.0.2.49722: Flags [.], ack 2197, win 2382, length 0
18:10:18.788112 ARP, Request who-has 172.30.0.13 (00:50:56:a6:47:79) tell 172.30.0.2, length 46
18:10:18.788139 ARP, Reply 172.30.0.13 is-at 00:50:56:a6:47:79, length 28
18:10:30.378795 IP 172.30.0.2.49702 > 172.30.0.13.22: Flags [P.], seq 1:65, ack 256, win 1021, length 64
(END)
```

Part 3: Step 9: AnyConnect_adminguide.pdf file on TargetWindows02 Desktop



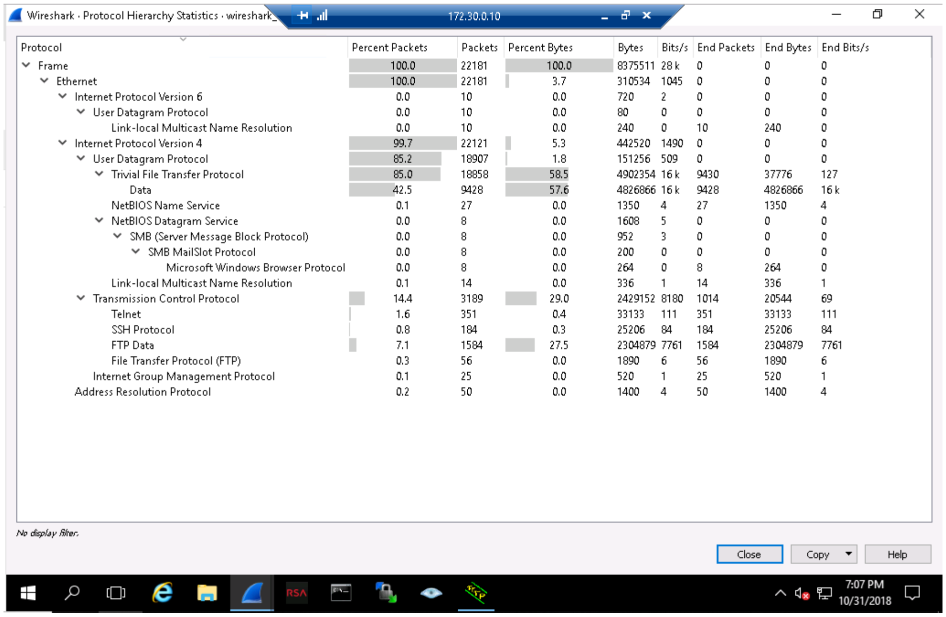
Part 3: Step 20: AnyConnect_adminguide.pdf transferred file in Tftpd64 Desktop directory



Current Directory C:\Users\Administrator\Desktop

```
AnyConnect_adminguide.pdf        10/31/2018        482
desktop.ini                 1/10/2017282
File Transfer.lnk           4/11/20172453
putty.lnk                   1/14/20171129
Tftpd64.lnk                 1/16/20171699
```

Part 4: Step 5: Protocol Statistics Hierarchy Window



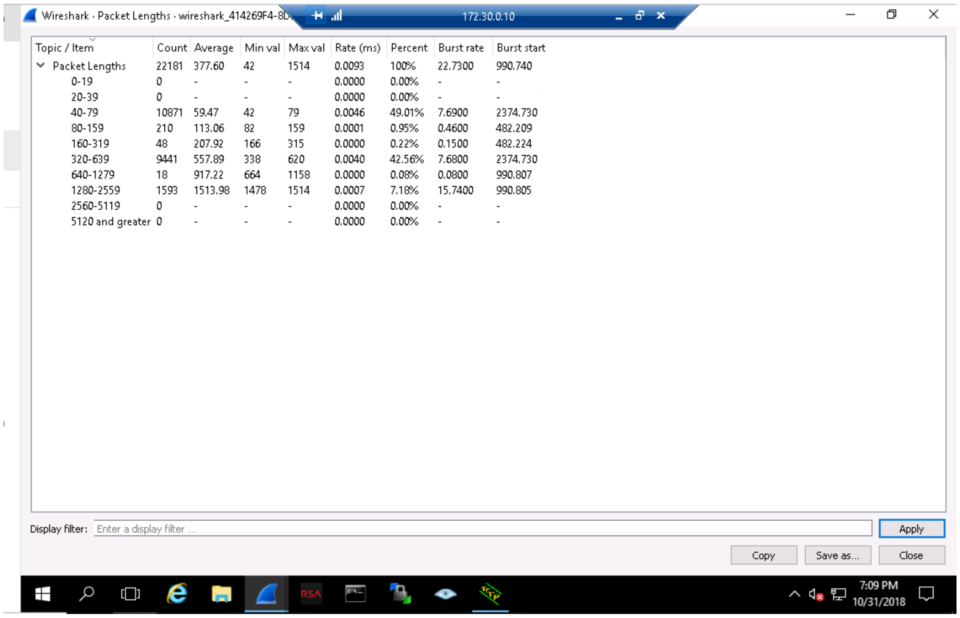
Wireshark · Protocol Hierarchy Statistics · wireshark_

172.30.0.10

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	22181	100.0	8375511	28 k	0	0	0
Ethernet	100.0	22181	3.7	310534	1045	0	0	0
Internet Protocol Version 6	0.0	10	0.0	720	2	0	0	0
User Datagram Protocol	0.0	10	0.0	80	0	0	0	0
Link-local Multicast Name Resolution	0.0	10	0.0	240	0	10	240	0
Internet Protocol Version 4	99.7	22121	5.3	442520	1490	0	0	0
User Datagram Protocol	85.2	18907	1.8	151256	509	0	0	0
Trivial File Transfer Protocol	85.0	18858	58.5	4902354	16 k	9430	37776	127
Data	42.5	9428	57.6	4826866	16 k	9428	4826866	16 k
NetBIOS Name Service	0.1	27	0.0	1350	4	27	1350	4
NetBIOS Datagram Service	0.0	8	0.0	1608	5	0	0	0
SMB (Server Message Block Protocol)	0.0	8	0.0	952	3	0	0	0
SMB MailSlot Protocol	0.0	8	0.0	200	0	0	0	0
Microsoft Windows Browser Protocol	0.0	8	0.0	264	0	8	264	0
Link-local Multicast Name Resolution	0.1	14	0.0	336	1	14	336	1
Transmission Control Protocol	14.4	3189	29.0	2429152	8180	1014	20544	69
Telnet	1.6	351	0.4	33133	111	351	33133	111
SSH Protocol	0.8	184	0.3	25206	84	184	25206	84
FTP Data	7.1	1584	27.5	2304879	7761	1584	2304879	7761
File Transfer Protocol (FTP)	0.3	56	0.0	1890	6	56	1890	6
Internet Group Management Protocol	0.1	25	0.0	520	1	25	520	1
Address Resolution Protocol	0.2	50	0.0	1400	4	50	1400	4

No display filter.

Part 4: Step 7: Packet Length Distribution Window



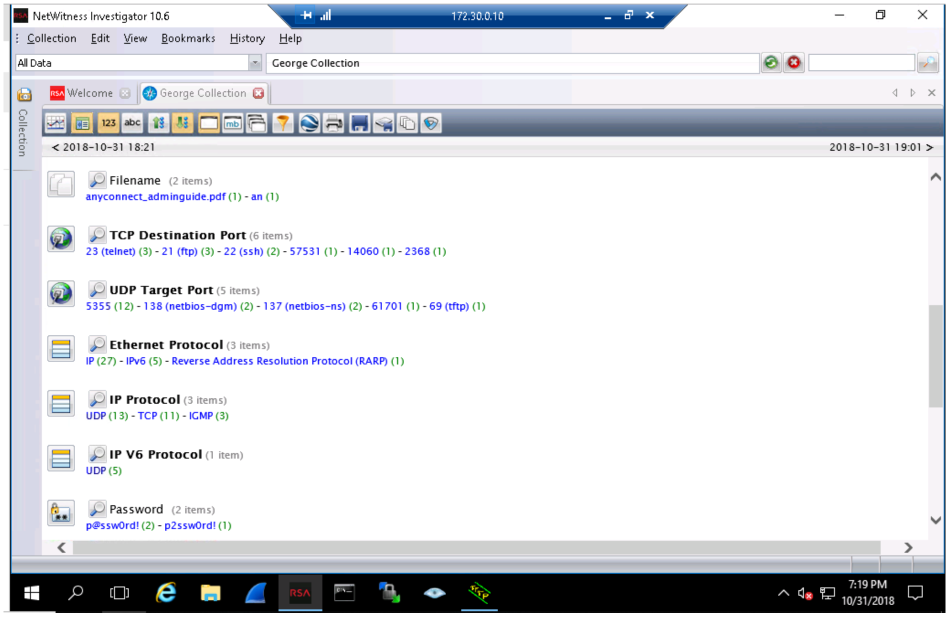
Wireshark · Packet Lengths · wireshark_414269F4-8D

172.30.0.10

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	22181	377.60	42	1514	0.0093	100%	22.7300	990.740
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	10871	59.47	42	79	0.0046	49.01%	7.6900	2374.730
80-159	210	113.06	82	159	0.0001	0.95%	0.4600	482.209
160-319	48	207.92	166	315	0.0000	0.22%	0.1500	482.224
320-639	9441	557.89	338	620	0.0040	42.56%	7.6800	2374.730
640-1279	18	917.22	664	1158	0.0000	0.08%	0.0800	990.807
1280-2559	1593	1513.98	1478	1514	0.0007	7.18%	15.7400	990.805
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Display filter: Enter a display filter ...

Part 5: Step 9: NetWitness showing Password(s)



< 2018-10-31 18:21 | 2018-10-31 19:01 >

Filename (2 items)
anyconnect_adminguide.pdf (1) - an (1)

TCP Destination Port (6 items)
23 (telnet) (3) - 21 (ftp) (3) - 22 (ssh) (2) - 57531 (1) - 14060 (1) - 2368 (1)

UDP Target Port (5 items)
5355 (12) - 138 (netbios-dgm) (2) - 137 (netbios-ns) (2) - 61701 (1) - 69 (tftp) (1)

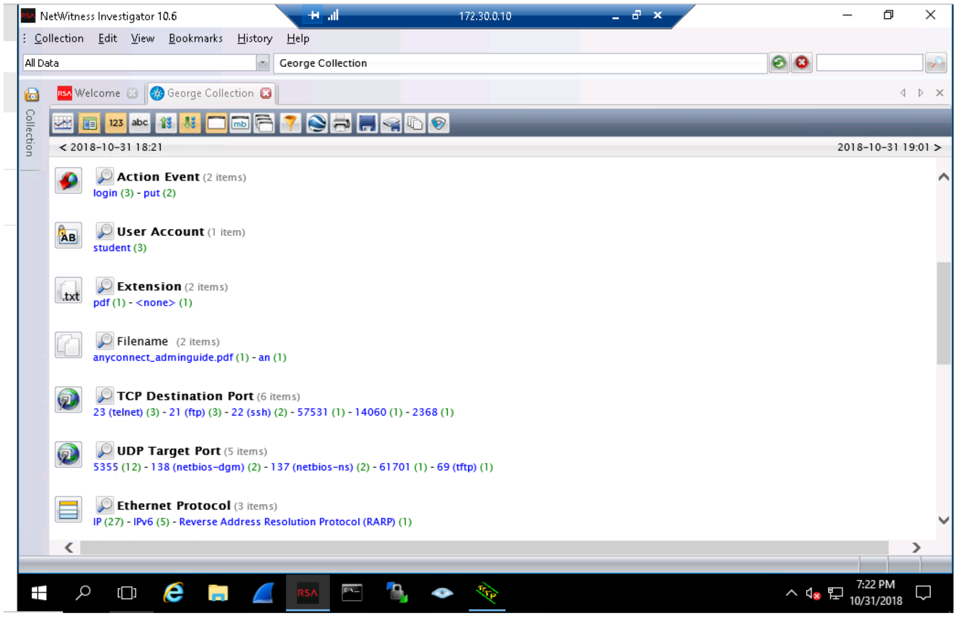
Ethernet Protocol (3 items)
IP (27) - IPv6 (5) - Reverse Address Resolution Protocol (RARP) (1)

IP Protocol (3 items)
UDP (13) - TCP (11) - ICMP (3)

IP V6 Protocol (1 item)
UDP (5)

Password (2 items)
p@ssw0rd! (2) - p2ssw0rd! (1)

Part 5: Step 10: NetWitness showing Filename (AnyConnect_adminguide.pdf)



< 2018-10-31 18:21 | 2018-10-31 19:01 >

Action Event (2 items)
login (3) - put (2)

User Account (1 item)
student (3)

Extension (2 items)
pdf (1) - <none> (1)

Filename (2 items)
anyconnect_adminguide.pdf (1) - an (1)

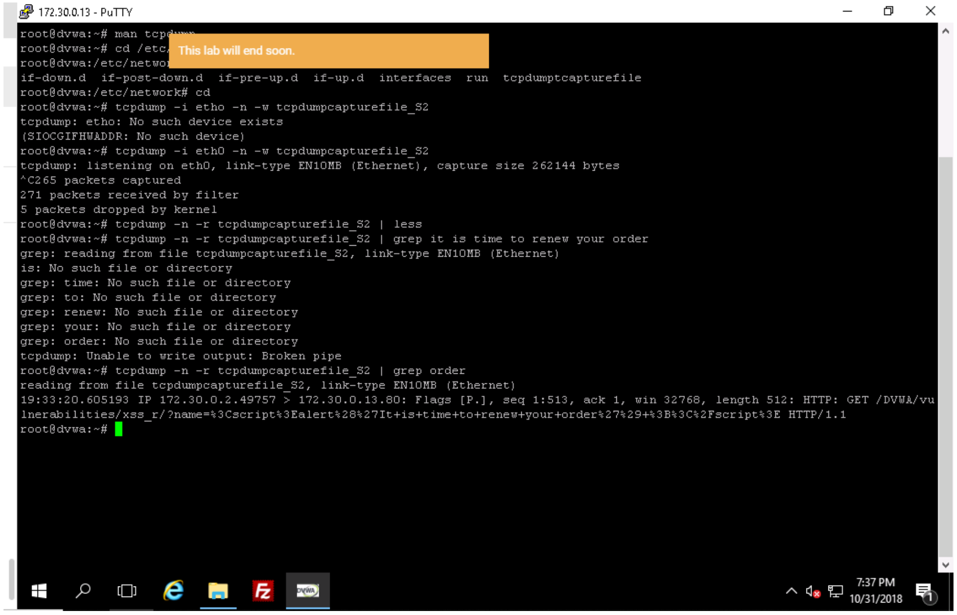
TCP Destination Port (6 items)
23 (telnet) (3) - 21 (ftp) (3) - 22 (ssh) (2) - 57531 (1) - 14060 (1) - 2368 (1)

UDP Target Port (5 items)
5355 (12) - 138 (netbios-dgm) (2) - 137 (netbios-ns) (2) - 61701 (1) - 69 (tftp) (1)

Ethernet Protocol (3 items)
IP (27) - IPv6 (5) - Reverse Address Resolution Protocol (RARP) (1)

SECTION 2

Part 1: Step 20: Grep command for alert message (5th line from bottom)

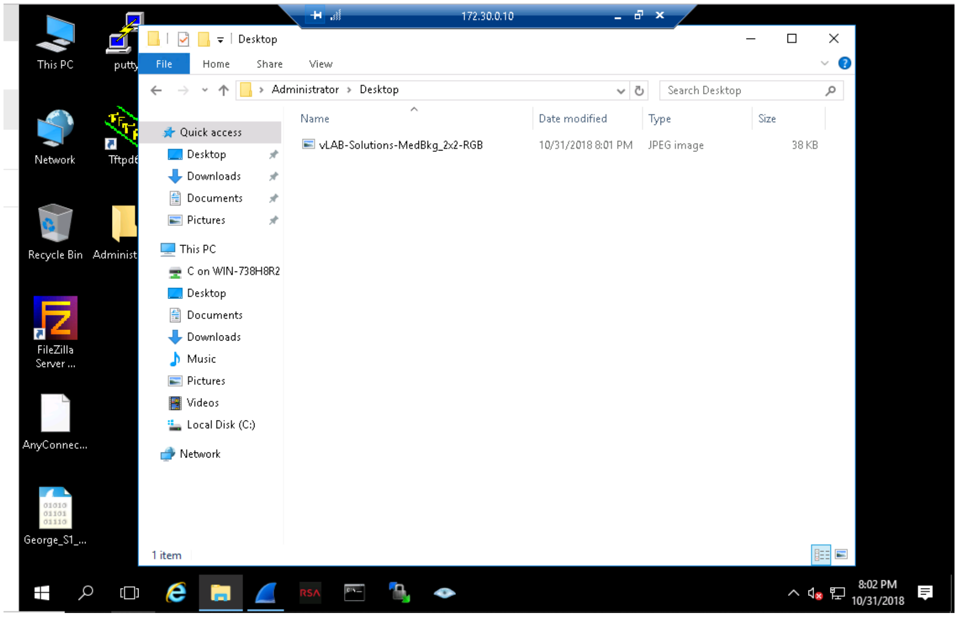


172.30.0.13 - PuTTY

```
root@dvwa:~# man tcpdump
root@dvwa:~# cd /etc/
root@dvwa:/etc/netwo
if-down.d  if-post-down.d  if-pre-up.d  if-up.d  interfaces  run  tcpdumptcapturefile
root@dvwa:/etc/network# cd
root@dvwa:~# tcpdump -i etho -n -w tcpdumpcapturefile_S2
tcpdump: etho: No such device exists
(SIOCGIFHWADDR: No such device)
root@dvwa:~# tcpdump -i eth0 -n -w tcpdumpcapturefile_S2
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C265 packets captured
271 packets received by filter
5 packets dropped by kernel
root@dvwa:~# tcpdump -n -r tcpdumpcapturefile_S2 | less
root@dvwa:~# tcpdump -n -r tcpdumpcapturefile_S2 | grep it is time to renew your order
grep: reading from file tcpdumpcapturefile_S2, link-type EN10MB (Ethernet)
is: No such file or directory
grep: time: No such file or directory
grep: to: No such file or directory
grep: renew: No such file or directory
grep: your: No such file or directory
grep: order: No such file or directory
tcpdump: Unable to write output: Broken pipe
root@dvwa:~# tcpdump -n -r tcpdumpcapturefile_S2 | grep order
reading from file tcpdumpcapturefile_S2, link-type EN10MB (Ethernet)
19:33:20.605193 IP 172.30.0.2.49757 > 172.30.0.13.80: Flags [P.], seq 1:513, ack 1, win 32768, length 512: HTTP: GET /DVWA/vu
lnerabilities/xss_r/?name=%3Cscript%3Ealert%28%27It+is+time+to+renew+your+order%27%29+%3B%3C%2Fscript%3E HTTP/1.1
root@dvwa:~#
```

This lab will end soon.

Part 3: Step 7: vLAB-Solutions-MedBkg_2x2-RGB file on TargetWindows02 Desktop



172.30.0.10

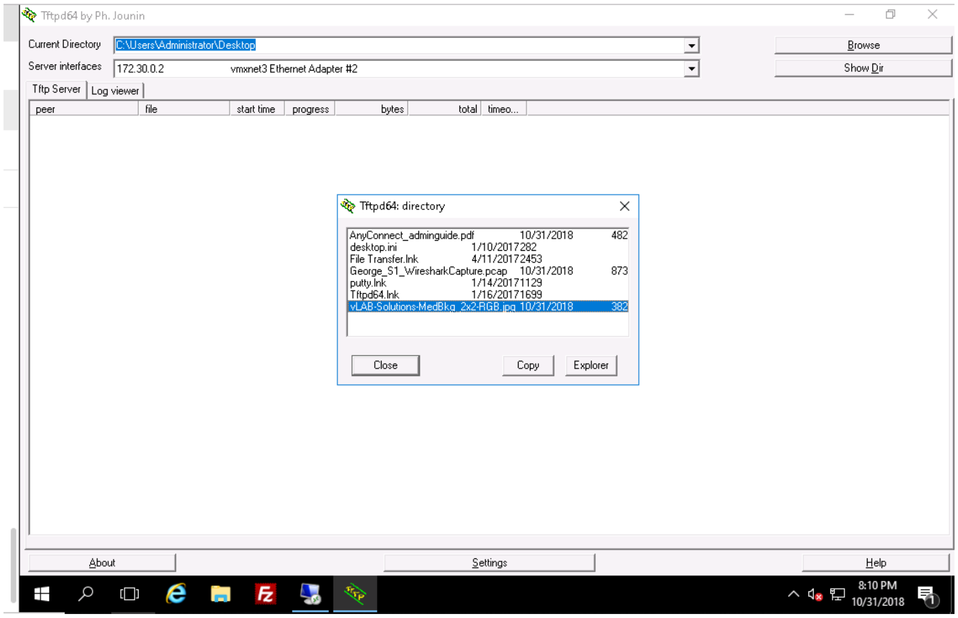
Desktop

Administrator › Desktop

```
Name                               Date modified        Type         Size
vLAB-Solutions-MedBkg_2x2-RGB      10/31/2018 8:01 PM   JPEG image   38 KB
```

1 item

Part 3: Step 7: vLAB-Solutions-MedBkg_2x2-RGB file in Tftpd64 Desktop directory



Tftpd64 by Ph. Jounin

Current Directory: C:\Users\Administrator\Desktop

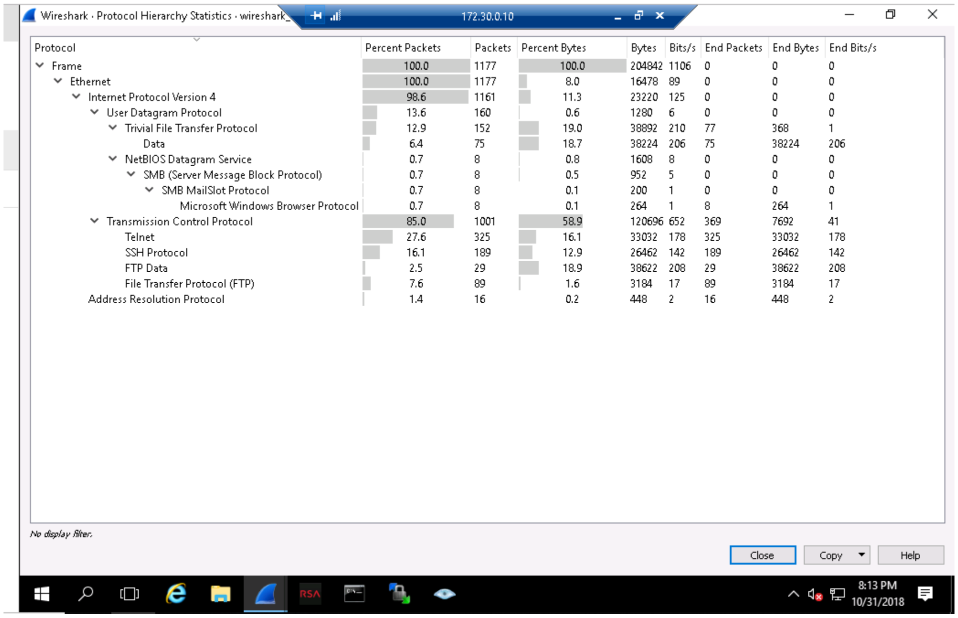
Server interfaces: 172.30.0.2 vmxnet3 Ethernet Adapter #2

peer	file	start time	progress	bytes	total	timeo...

Tftpd64: directory

```
AnyConnect_adminguide.pdf          10/31/2018      482
desktop.ini                 1/10/2017282
File Transfer.lnk           4/11/20172453
George_S1_WiresharkCapture.pcap    10/31/2018      873
putty.lnk                   1/14/20171129
Tftpd64.lnk                 1/16/20171699
vLAB-Solutions-MedBkg_2x2-RGB.jpg  10/31/2018      382
```

Part 4: Step 5: Protocol Statistics Hierarchy Window



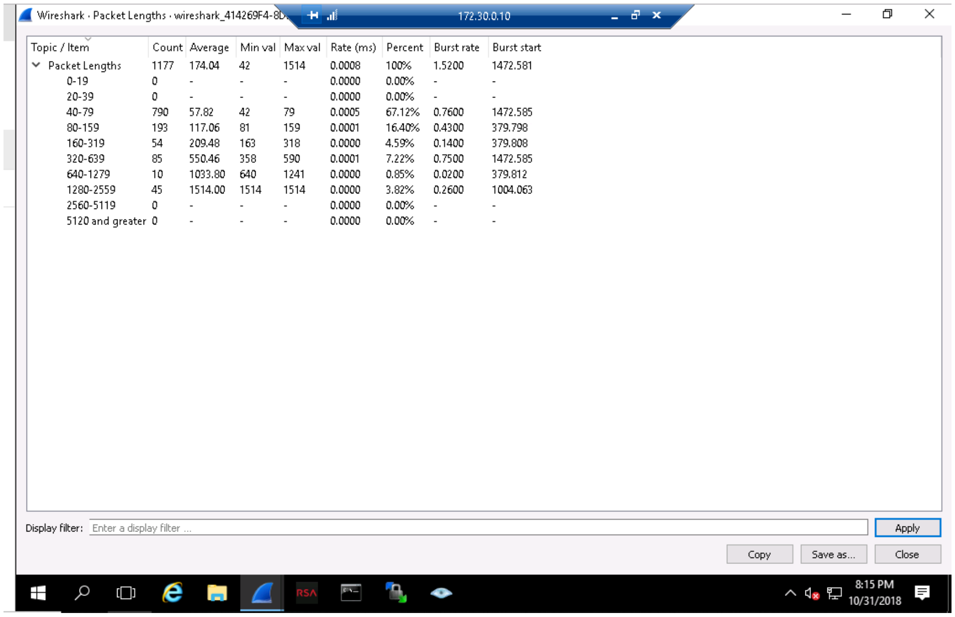
Wireshark · Protocol Hierarchy Statistics · wireshark_

172.30.0.10

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	1177	100.0	204842	1106	0	0	0
Ethernet	100.0	1177	8.0	16478	89	0	0	0
Internet Protocol Version 4	98.6	1161	11.3	23220	125	0	0	0
User Datagram Protocol	13.6	160	0.6	1280	6	0	0	0
Trivial File Transfer Protocol	12.9	152	19.0	38892	210	77	368	1
Data	6.4	75	18.7	38224	206	75	38224	206
NetBIOS Datagram Service	0.7	8	0.8	1608	8	0	0	0
SMB (Server Message Block Protocol)	0.7	8	0.5	952	5	0	0	0
SMB MailSlot Protocol	0.7	8	0.1	200	1	0	0	0
Microsoft Windows Browser Protocol	0.7	8	0.1	264	1	8	264	1
Transmission Control Protocol	85.0	1001	58.9	120696	652	369	7692	41
Telnet	27.6	325	16.1	33032	178	325	33032	178
SSH Protocol	16.1	189	12.9	26462	142	189	26462	142
FTP Data	2.5	29	18.9	38622	208	29	38622	208
File Transfer Protocol (FTP)	7.6	89	1.6	3184	17	89	3184	17
Address Resolution Protocol	1.4	16	0.2	448	2	16	448	2

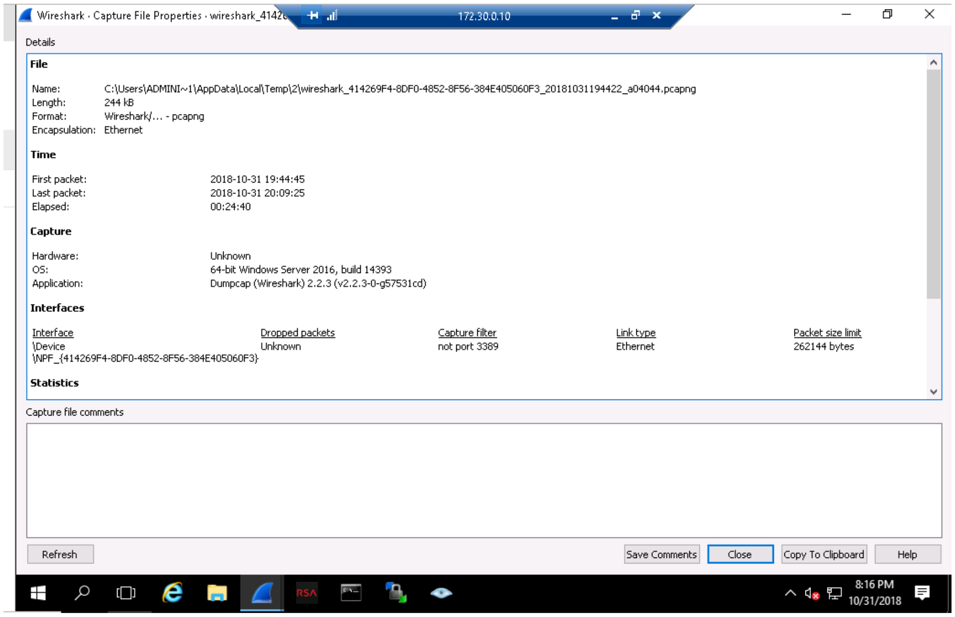
No display filter.

Part 4: Step 8: Packet length Distribution Window


Wireshark · Packet Lengths · wireshark_414269F4-8D...
172.30.0.10
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close
8:15 PM
10/31/2018

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	1177	174.04	42	1514	0.0008	100%	1.5200	1472.581
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	790	57.82	42	79	0.0005	67.12%	0.7600	1472.585
80-159	193	117.06	81	159	0.0001	16.40%	0.4300	379.798
160-319	54	209.48	163	318	0.0000	4.59%	0.1400	379.808
320-639	85	550.46	358	590	0.0001	7.22%	0.7500	1472.585
640-1279	10	1033.80	640	1241	0.0000	0.85%	0.0200	379.812
1280-2559	45	1514.00	1514	1514	0.0000	3.82%	0.2600	1004.063
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Part 4: Step 11: Capture File Properties Window



File

Name: C:\Users\ADMINI~1\AppData\Local\Temp\2\wireshark_414269F4-8DF0-4852-8F56-384E405060F3_20181031194422_a04044.pcapng
Length: 244 kB
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2018-10-31 19:44:45
Last packet: 2018-10-31 20:09:25
Elapsed: 00:24:40

Capture

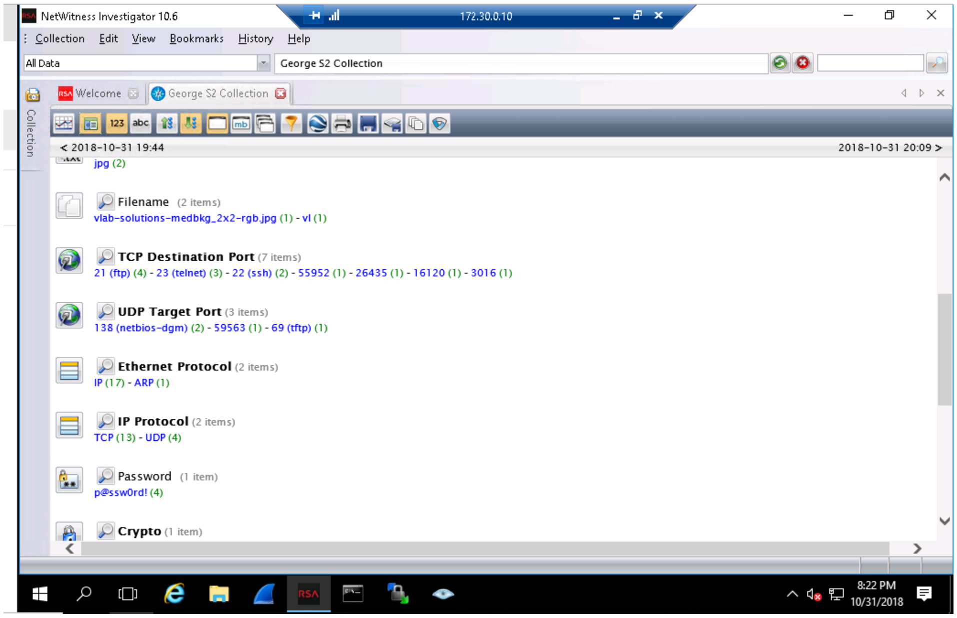
Hardware: Unknown
OS: 64-bit Windows Server 2016, build 14393
Application: Dumpcap (Wireshark) 2.2.3 (v2.2.3-0-g57531cd)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
\Device \NPF_{414269F4-8DF0-4852-8F56-384E405060F3}	Unknown	not port 3389	Ethernet	262144 bytes

Statistics

Part 5: Step 5: NetWitness showing Password



jpg (2)

Filename (2 items)
vlab-solutions-medbkg_2x2-rgb.jpg (1) - vl (1)

TCP Destination Port (7 items)
21 (ftp) (4) - 23 (telnet) (3) - 22 (ssh) (2) - 55952 (1) - 26435 (1) - 16120 (1) - 3016 (1)

UDP Target Port (3 items)
138 (netbios-dgm) (2) - 59563 (1) - 69 (tftp) (1)

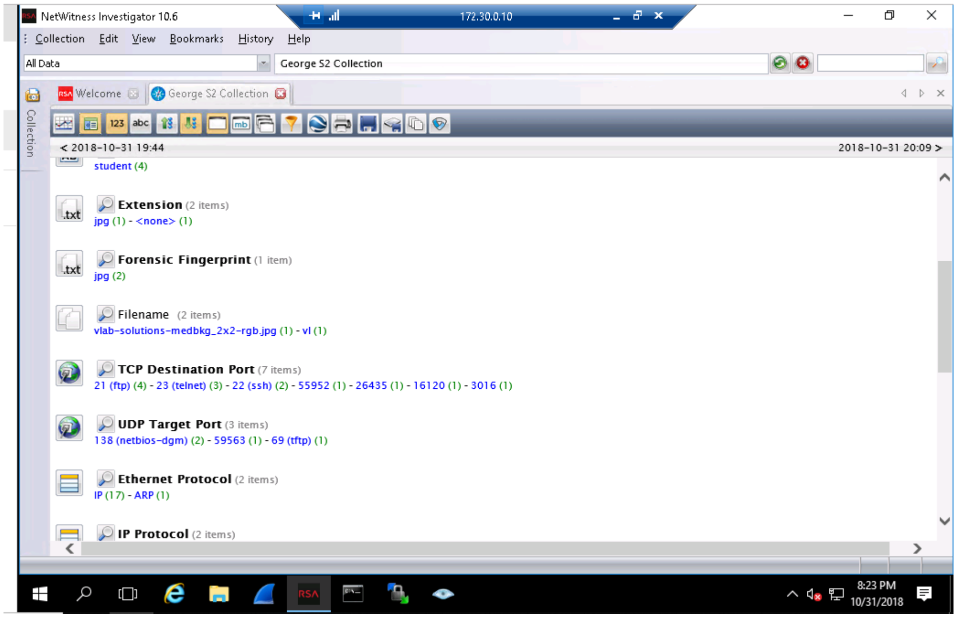
Ethernet Protocol (2 items)
IP (17) - ARP (1)

IP Protocol (2 items)
TCP (13) - UDP (4)

Password (1 item)
p@ssw0rd! (4)

Crypto (1 item)

Part 5: Step 6: NetWitness showing Filename (vLAB-Solutions-MedBkg_2x2-RGB)



student (4)

Extension (2 items)
jpg (1) - <none> (1)

Forensic Fingerprint (1 item)
jpg (2)

Filename (2 items)
vlab-solutions-medbkg_2x2-rgb.jpg (1) - vl (1)

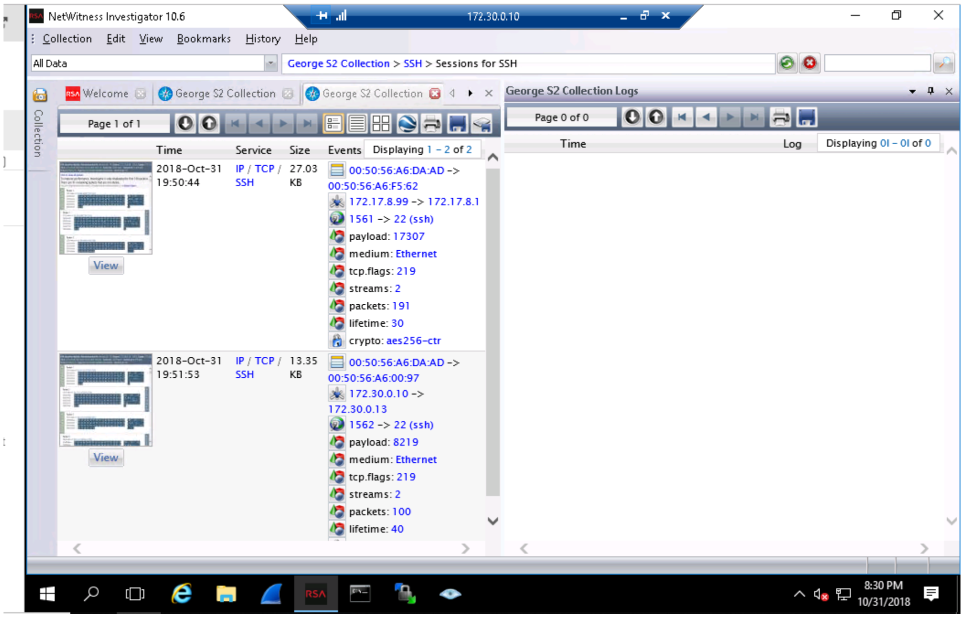
TCP Destination Port (7 items)
21 (ftp) (4) - 23 (telnet) (3) - 22 (ssh) (2) - 55952 (1) - 26435 (1) - 16120 (1) - 3016 (1)

UDP Target Port (3 items)
138 (netbios-dgm) (2) - 59563 (1) - 69 (tftp) (1)

Ethernet Protocol (2 items)
IP (17) - ARP (1)

IP Protocol (2 items)

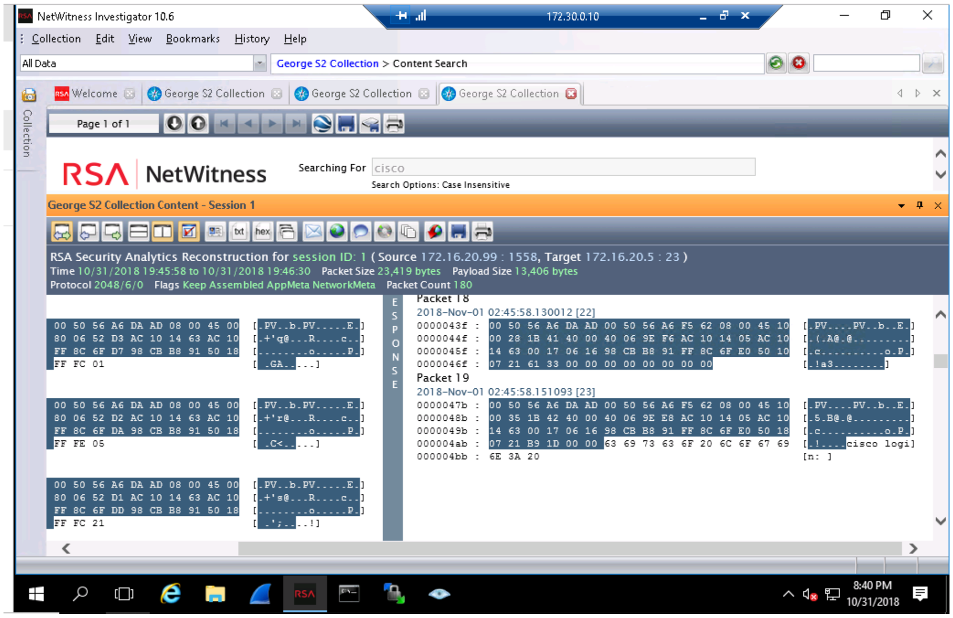
Part 5: Step 7: SSH Sessions and IP Addresses



Displaying 1 – 2 of 2

Time	Service	Size	Events
2018-Oct-31 19:50:44	IP / TCP / SSH	27.03 KB	00:50:56:A6:DA:AD -> 00:50:56:A6:F5:62 172.17.8.99 -> 172.17.8.1 1561 -> 22 (ssh) payload: 17307 medium: Ethernet tcp.flags: 219 streams: 2 packets: 191 lifetime: 30 crypto: aes256-ctr
2018-Oct-31 19:51:53	IP / TCP / SSH	13.35 KB	00:50:56:A6:DA:AD -> 00:50:56:A6:00:97 172.30.0.10 -> 172.30.0.13 1562 -> 22 (ssh) payload: 8219 medium: Ethernet tcp.flags: 219 streams: 2 packets: 100 lifetime: 40

Part 5: Step 11: cisco login capture



Searching For cisco
Search Options: Case Insensitive

George S2 Collection Content - Session 1

RSA Security Analytics Reconstruction for session ID: 1 (Source 172.16.20.99 : 1558, Target 172.16.20.5 : 23)
Time 10/31/2018 19:45:58 to 10/31/2018 19:46:30 Packet Size 23,419 bytes Payload Size 13,406 bytes
Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 180

```
00 50 56 A6 DA AD 08 00 45 00   [.PV..b.PV.....E.]
80 06 52 D3 AC 10 14 63 AC 10   [.+'q@...R....c..]
FF 8C 6F D7 98 CB B8 91 50 18   [.........o.....P.]
FF FC 01                        [ .GA.....]

00 50 56 A6 DA AD 08 00 45 00   [.PV..b.PV.....E.]
80 06 52 D2 AC 10 14 63 AC 10   [.+'r@...R....c..]
FF 8C 6F DA 98 CB B8 91 50 18   [.........o.....P.]
FF FE 05                        [ .C<.....]

00 50 56 A6 DA AD 08 00 45 00   [.PV..b.PV.....E.]
80 06 52 D1 AC 10 14 63 AC 10   [.+'s@...R....c..]
FF 8C 6F DD 98 CB B8 91 50 18   [.........o.....P.]
FF FC 21                        [ .';.....!]
```

```
Packet 18
2018-Nov-01 02:45:58.130012 [22]
0000043f : 00 50 56 A6 DA AD 00 50 56 A6 F5 62 08 00 45 10   [.PV....PV..b..E.]
0000044f : 00 28 1B 41 40 00 40 06 9E F6 AC 10 14 05 AC 10   [.(.A@.@.........]
0000045f : 14 63 00 17 06 16 98 CB B8 91 FF 8C 6F E0 50 10   [.c..........o.P.]
0000046f : 07 21 61 33 00 00 00 00 00 00 00 00               [.!a3........]
Packet 19
2018-Nov-01 02:45:58.151093 [23]
0000047b : 00 50 56 A6 DA AD 00 50 56 A6 F5 62 08 00 45 10   [.PV....PV..b..E.]
0000048b : 00 35 1B 42 40 00 40 06 9E E8 AC 10 14 05 AC 10   [.5.B@.@.........]
0000049b : 14 63 00 17 06 16 98 CB B8 91 FF 8C 6F E0 50 18   [.c..........o.P.]
000004ab : 07 21 B9 1D 00 00 63 69 73 63 6F 20 6C 6F 67 69   [.!....cisco logi]
000004bb : 6E 3A 20                                          [n: ]
```

SECTION 3

Part 1

Protocol filters help reduce the traffic based on functionality, or protocol. FTP relies on TCP to provide a connection-oriented method for transferring files. Filtering certain ports when capturing data such as FTP enables the network administrator to eliminate ports that are not needed at that instance. It gives an idea of the various protocol errors and misconfigurations that may exist on the network. The filtering provides a clear focus on what the administrator wants to see and analyzed for baselining purposes. Filtering gives a real view of how the network is truly being used.

Part 2

The ‘sudo tcpdump –i any port 20 -n’ will capture network traffic with FTP data packets. ‘any’ in the command just tells tcpdumpt to capture FTP packets on any of the infaces either eth0 or eth1. FTP uses ports 20 (Data)/21 (Control). Whichever FTP packet is desired is set in the filters. The ‘n’ part in the command only tells tcpdump to set IP addresses instead of domain names. The ‘n’ could be taken out per choice.

To view only the student account information in tcpdumpt, the directory must be changed to the specific student account housing the information to be viewed. For instance, if the student account is “dvwa”, the cd /dvwa should be used to switch to the student account. Then the ‘ls’ command to list the files within the dvwa account (Assuming file ‘lab7’ hosts the information).
The “sudo tcpdump –n –r lab7 | less” command enables viewing the information with scrolling using the up/down arrow keys.

Part 3

Understanding baseline traffic patterns is critical. Analyzing the data at the WAN – the point where network truly begins and examining internal traffic against that sent externally is crucial. By analyzing IP addresses, it helps to know which outside IP addresses are generally allowed to talk to a network and vice versa. For example, in detecting abnormal file access, a benchmark period building a histogram of file accesses will help to detect this suspicious activity.
A baseline could be created by configuring and specifying what protocols and IP addresses are left open for communication whiles closing all other unneeded ones. Any unauthorized connection from outside IP with packet sizes (Ethernet frames) and protocols is seen when analyzing the capture output.
For instance, the DVWA webserver could be configured to only allow http/https traffic since it’s a webserver. That way, any FTP activity detected on the network during analysis is a cause for suspicious activity.