CIS294 Course Project

Background

You are a cybersecurity analyst that are tasked to an Apache web server log file and to analyze pcap file.

An Apache log file will consist HTTP requests made to the web server to the /logs/access.log file. An example is:

193.19.118.8 - - [30/Sep/2015:14:47:16 -0400] "GET /admin/ HTTP/1.0" 404 162 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:30.N) Gecko/20110302 Firefox/30.0"

Cybersecurity professionals often use Wireshark to break down packets of data being transferred across different networks. The user can search and filter for specific packets of data and analyze how they are transferred across their network. These packets can be used for analysis on a real-time or offline basis.

Required Equipment

- Kali Linux VM or online <u>https://bellard.org/jslinux/</u>
- Wireshark installed on Kali Linux, Windows 10 VM, or own PC

Instructions

- Download the CIS294CP Files.zip from iCampus Course Project to your PC Desktop.
- Unzip the file. There will be two files.
- The CIS294CP.txt is for Part 1 Log Analysis.
- The CIS294CP.pcapng file is for Part 2 PCAP Analysis.

Part 1 Log Analysis

Analyze the log file using terminal. Each correct answer/screenshot is worth 2.5 points each.

1. How many entries in the log?

10,000

2. Insert a screenshot showing the result.

3. How many different IP addresses reached the server?

```
1,753
```

4. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
_$ awk '{print $1}' CIS294CP.txt | sort | uniq -c | sort -rn | wc -l
1753
```

5. Which IP address reached the server the most?

```
66.249.73.135
```

6. Insert a screenshot showing the result.



7. How many times did the IP address with the most entries reached the server?

482 times

8. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
    grep '66.249.73.135' CIS294CP.txt | wc -l
482
```

9. How many HTTP 200 status code are listed?

```
9126
```

10.Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
    grep -w 'HTTP/1.*" 200' CIS294CP.txt | wc -l
9126
```

11. How many HTTP page not found code are in the log?

```
213
```

12.Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
    grep -w 'HTTP/1.*" 404' CIS294CP.txt | wc -l
213
```

13.Which IP address was accessing robots.txt files the most times?

```
208.115.111.72
```

14.Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
$ grep "robots.txt" CIS294CP.txt | awk '{print $1}' | sort | uniq -c | sort -rn
10 208.115.111.72
8 208.115.113.88
7 144.76.95.39
```

15.What was the most common article that was retrieved?

favicon.ico

16.Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]

-$ awk '{print $7}' CIS294CP.txt | sort | uniq -c | sort -rn | head

807 /favicon.ico

546 /style2.css

538 /reset.css

533 /images/jordan-80.png

516 /images/web/2009/banner.png

488 /blog/tags/puppet?flav=rss20

224 /projects/xdotool/

217 /?flav=rss20

197 /

180 /robots.txt
```

17.What is the second most common iPhone iOS version used?

iPhone iOS 7.0.4

18.Insert a screenshot showing the result.



19. How long did the log file last? In seconds

298,859 seconds

20.Insert a screenshot showing the result.

-(kali	<pre>leadileadileadileadileadileadileadileadi</pre>				
Ls awk	'Iprint \$4, \$5}' CIS29	94CP.txt	sort	uniq -c	head
2	[17/May/2015:10:05:00	+0000]			
3	[17/May/2015:10:05:03	+0000]			
1	[17/May/2015:10:05:04	+0000]			
1	[17/May/2015:10:05:06	+0000]			
1	[17/May/2015:10:05:07	+0000]			
1	[17/May/2015:10:05:08	+0000]			
1	[17/May/2015:10:05:10	+0000]			
2	[17/May/2015:10:05:11	+0000]			
1	[17/May/2015:10:05:12	+0000]			
1	[17/May/2015:10:05:13	+0000]			
r-(kali	<pre>limetable kali)-[~/Desktop]</pre>				
└─\$ awk	'{print \$4, \$5}' <u>CIS29</u>	94CP.txt	sort	uniq -c	tail
3	[20/May/2015:21:05:48	+0000]			
2	[20/May/2015:21:05:50	+0000]			
1	[20/May/2015:21:05:52	+0000]			
3	[20/May/2015:21:05:53	+0000]			
1	[20/May/2015:21:05:54	+0000]			
3	[20/May/2015:21:05:55	+0000]			
1	[20/May/2015:21:05:56	+0000]			
2	[20/May/2015:21:05:57	+0000]			
1	[20/May/2015:21:05:58	+0000]			
2	[20/May/2015:21:05:59	+0000]			

From: Sunday, May 17, 2015 at 10:05:00 am To: Wednesday, May 20, 2015 at 9:05:59 pm

Result: 3 days, 11 hours, 0 minutes and 59 seconds

The duration is 3 days, 11 hours, 0 minutes and 59 seconds

Or 3 days, 11 hours, 59 seconds

Alternative time units

3 days, 11 hours, 0 minutes and 59 seconds can be converted to one of these units:

- 298,859 seconds
- · 4980 minutes (rounded down)
- 83 hours
- · 3 days (rounded down)
- 0.95% of 2015

Part 1 Log Analysis Extra Credit

For extra ten points (5 points for each correct submission), answer and submit a screenshot for the following

1. Which IP address and on what date had the most entries?

75.97.9.59 had the most entries(197) in a single day which occurred on Monday, May 18, 2015 and was the 4th most reoccurring IP in the entire log with 273 total entries. 130.237.218.86 had the second most entries(183) in a single day on Wednesday, May 20, 2015 and was the 3rd most reoccurring IP total(357) in the entire log. 66.249.73.135 took third place for most entries in a single day with 180 entries on Monday, May 18, 2015 and reached the server 482 times total within the 3 days, 11 hours, and 59 seconds of the(entire) log file.

2. Insert a screenshot showing the result.

<pre>(kali@ kali)-[~/Desktop] grep "17/May/2015" CIS294CP.txt awk '{print \$1}' sort uniq -c sort -rn head 78 66.249.73.135 58 66.55.213.73 58 46.105.14.53 52 50.139.66.106 41 144.76.194.187 38 67.61.65.249 37 111.199.235.239 34 122.166.142.108 27 65.55.213.74 26 99.252.100.83</pre>
<pre>(kali@ kali)-[~/Desktop] grep "18/May/2015" CIS294CP.txt awk '{print \$1}' sort uniq -c sort -rn head 197 75.97.9.59 180 66.249.73.135 135 46.105.14.53 50 86.76.247.183 42 50.16.19.13 41 199.168.96.66 40 210.13.83.18 40 209.85.238.199 33 80.108.25.232 33 59.163.27.11</pre>
<pre>(kali@kali)-[~/Desktop] grep "19/May/2015" CIS294CP.txt awk '{print \$1}' sort uniq -c sort -rn head 174 130.237.218.86 104 66.249.73.135 87 46.105.14.53 67 75.97.9.59 50 14.160.65.22 43 93.17.51.134 39 183.179.22.186 39 115.112.233.75 38 24.11.96.184 35 193.244.33.47</pre>
<pre>(kali@ kali)-[~/Desktop] grep "20/May/2015" CIS294CP.txt awk '{print \$1}' sort uniq -c sort -rn head 183 130.237.218.86 120 66.249.73.135 84 46.105.14.53 37 89.107.177.18 37 184.66.149.103 34 204.62.56.3 34 200.31.173.106 33 38.99.236.50 32 68.180.224.225</pre>

CIS294 Course Project

Part 2 Pcap Analysis

Use the **CIS294CP.pcapng** file from the **CIS294CP Files** folder on your Windows 10 VM or the host PC that has Wireshark installed. Analyze the pcapng file. Each correct answer/screenshot is worth 2.5 points each.

1. How many ping requests were sent in the capture?

•

2. Insert a screenshot showing the result in Wireshark. licmp No. Time Source Destination Protocol Lengi Info 7 12, 196737607 10.0.2.15 ICMP 98 Echo (ping) reply 18.0.2.22 id=0x0841, seg=1/256, ttl=128 (request in 4) 8 13 209235817 10.0.2.22 ICMP 98 Echo (ping) request id=0x0841, seq=2/512, ttl=64 (reply in 9) 10.0.2.15 id=0x0841, seq=2/512, ttl=128 (request in 8) 9 13.209557789 ICMP 10.0.2.15 10.0.2.22 98 Echo (ping) reply 98 Echo (ping) request id=0x6841, seq=3/768, ttl=64 (reply in 11) 10 14.233249758 10.0.2.22 10.0.2.15 TOMP 11 14.233768129 10.0.2.15 ICMP 98 Echo (ping) reply id=0x6841, seq=3/768, ttl=128 (request in 10) 16.0.2.22 98 Echo (ping) request id=8x8841, seq=4/1824, ttl=64 (reply in 13) 12 15.248605631 10.0.2.22 10.0.2.15 ICMP 13 15.248936891 10.0.2.15 ICMP 98 Echo (ping) reply id=0x0841, seq=4/1024, ttl=128 (request in 12) 10.0.2.22 98 Echo (ping) request id=8x6841, seq=5/1280, ttl=64 (reply in 15) 14 16.273077068 10.0.2.22 ICMP 18.0.2.15 98 Echo (ping) reply 15 16.273407477 10.0.2.15 16.6.2.22 TEMP id=0x0841, seq=5/1280, ttl=128 (request in 14)

3. From what IP address did the ping request originate from?

ICMP

10.0.2.22

17 17 296626187 10.0.2.22

19 17.296904299 10.0.2.15

4. Insert a screenshot showing the result in Wireshark.

10.0.2.15

10.0.2.22

	Icmp									
No.	Time	Source	Destination	Protocol	Lengt Info					
	4 12.196178825	10.0.2.22	10.0.2.15	ICMP	98 Echo	(ping)	request	1d=8x8841,	seq=1/256,	ttl=64 (reply_in_7)
-	7 12.196737697	18.0.2.15	10.0.2.22	ICNP	98 Echo	(ping)	reply	1d=0x0841,	seq=1/256,	ttl=128 (request in 4)
	8 13.209235817	10.0.2.22	10.0.2.15	ICMP	98 Echo	(ping)	request	id=0x0841,	seq=2/512,	ttl=64 (reply in 9)
	9 13.209557789	18.0.2.15	10.0.2.22	ICMP	98 Echo	(ping)	reply	id=0x0841,	seq=2/512,	ttl=128 (request in 8)
	10 14.233249758	18.8.2.22	10.0.2.15	ICMP	98 Echo	(ping)	request	id=0x0841,	seq=3/768,	ttl=64 (reply in 11)
	11 14.233768129	10.0.2.15	10.0.2.22	ICMP	98 Echo	(ping)	reply	id=0x0841,	seq=3/768,	ttl=128 (request in 10)
	12 15.248605631	18.0.2.22	10.0.2.15	ICMP	98 Echo	(ping)	request	id=0x0841,	seq=4/1024	, ttl=64 (reply in 13)
	13 15,248936891	10.0.2.15	10.0.2.22	ICMP	98 Echo	(ping)	reply	id=0x0841,	seq=4/1024	, ttl=128 (request in 12)
	14 16,273077068	18.8.2.22	10.0.2.15	ICMP	98 Echo	(ping)	request	id=0x0841,	seq=5/1280	, ttl=64 (reply in 15)
	15 16.273407477	10.0.2.15	10.0.2.22	ICMP	98 Echo	(ping)	reply	1d=0x0B41,	seq=5/1280	, ttl=128 (request in 14)
	17 17.296626187	10.0.2.22	10.0.2.15	ICMP	98 Echo	(ping)	request	1d=0x0841,	seq=6/1536	, ttl=64 (reply in 19)
L	19 17.296904299	18.0.2.15	10.0.2.22	ICMP	98 Echo	(ping)	reply	id=0x0841,	seq=6/1536	, ttl=128 (request in 17)

98 Echo (ping) reply

98 Echo (ping) request id=8x9841, seq=6/1536, ttl=64 (reply in 19)

id=0x0841, seq=6/1536, ttl=128 (request in 17)

5. What is the IP address of the device associated with 08:00:27:4b:e3:60?

10.0.2.15

6. Insert a screenshot showing the result in Wireshark.



7. What version of Internet Group Management Protocol is in use?

IGMP Version 3

8. Insert a screenshot showing the result in Wireshark.

	gmp				
No:	Time	Source	Destination	Protocol	Lengt Info
	1 226.987679494	18.0.2.15	224.6.0.22	16MPv3	60 Membership Report / Leave group 224.0.0.252
	1_ 226.995032982 1_ 226.995788335	18.0.2.15	224.0.0.22	IGMPv3 IGMPv3	68 Membership Report / Join group 224.0.0.252 for any 60 Membership Report / Leave group 224.0.0.252
• •	rame 1108: 60 by thernet II, Src: nternet Protocol	tes on wire PcsCompu_4 Version 4.	(480 bits), b:e3:60 (08: Src: 10 0 2	60 byte: 00:27:4b ,15, Dst	s captured (480 bits) on interface eth0, id 0 :e3:60), Dst: IPv4mcast_16 (01:60:5e:00:00:16) : 224.0.0.22
	nternet Group Ma [IGMP Version; Type: Membershi Reserved: 00 Checksum: 0xfa0 [Checksum Statu Reserved: 0000 Num Group Record Sroup Record :	nagement Pr 3] p Report (0 11 [correct] is: Good] ds: 1 224.0.0.252	x22) Change To	Include	Mode:

- 9. What is the name of the host located at 10.0.2.22?
 - kali

10.Insert a screenshot showing the result in Wireshark.

	438 90.751235246	10.0.2.22	10.0.2.3	DHCP 347	DHCP R	lequest -	Transaction	1D 0xa823310c
	440 90.752764111	10.0.2.3	10.0.2.22	DHCP 596	DHCP A	CK -	Transaction	ID 0xa823310c
	1438 368.017532721	10.0.2.22	10.0.2.3	DHCP 347	2 DHCP R	Request -	Transaction	ID 0xa823310c
	1439 368,020489865	10.0.2.3	10.0.2.22	DHCP 596	DHCP A	- CK	Transaction	ID 0xa823310c
	1540 636.656977939	10.0.2.22	10.0.2.3	DHCP 343	2 DHCP R	lequest -	Transaction	ID 0xa823310c
	1541 636.659339563	10.0.2.3	10.0.2.22	DHCP 596	DHCP A	- CK	Transaction	ID 8xa823318c
	1583 893.665113499	10.0.2.22	10.0.2.3	DHCP 342	Z DHCP R	lequest -	Transaction	ID 0xa823310c
	1584 893.667053707	10.0.2.3	10.0.2.22	DHCP 590	DHCP A	CK -	Transaction	ID 0xa823310c
	1755.4785.8685667	18.8.2.22	10,0,2,3	DHCP 342	P. OHCP R	lequest -	Transaction	ID 8x22f8a847
11.	User Datagram Protoco Dynamic Host Configur Message type: Boot Hardware address le Hops: 0 Transaction ID: 0xa Seconds elapsed: 0 Bootp flags: 0x0000 Client IP address: Your (client) IP ad Next server IP addr Relay agent IP addr Client MAC address: Client MAC address: Client hardware add Server host name no Boot file name not Magic cookie: DHCP • Option: (12) Host N Length: 4 Host Name: kali	1, Src Port: 68, Ds ation Protocol (Req Request (1) sngth: 6 1823310c 8 (Unicast) 10.0.2.22 ddress: 0.0.0.0 ress: 0.0.0 ress: 0.0.0 ress: 0.0.0 ress: 0.0.0 ress: 0.0.0 ress: 0.0.0 ress: 0.0.0 ress: 0.0.0 ress: 0.0.0 ress: 0.0 ress: 0.0.0 ress: 0.0 ress: 0.0	t Port: 67 Jest) (08:00:27:7c:8e:8e) 000000000000000 t)					

What is the IP address of the DHCP server?

10.0.2.3

12.Insert a screenshot showing the result in Wireshark.

No.	Time	Source	Destination	Protocol	Length Info			
F	439 90.751235246	10.0.2.22	10.0.2.3	DHCP	342 DHCP Re	quest 🕞	Transaction	ID 0xa823310c
	440 90.752764111	10.0.2.3	10.0.2.22	DHCP	590 DHCP AC	ек –	Transaction	ID 0xa823318c
	1438 368.017532721	10.0.2.22	10.0.2.3	DHCP	342 DHCP Re	quest -	Transaction	ID 0xa823310c
	Frame 440: 590 bytes	on wire (4728 bits)	, 590 bytes captured	(4720 bit	s) on interfac	ce eth0,	id 0	
	Ethernet II, Src: Po	sCompu_c1:84:ca (08:	00:27:c1:84:ca), Dst:	PesCompu	_7c:8e:8e (68	:00:27:70	:8e:8e)	
	Internet Protocol Ve	rsion 4, Src: 10.0.2	.3. Dst: 10.0.2.22					
	User Datagram Protoc	ol, Src Port: 67, Ds	t Port: 68					
	Dynamic Host Configu	ration Protocol (ACK	a					
	Message type: Boot Hardware type: Eth Hardware address 1 Hops: 0 Transaction ID: 89 Seconds elapsed: 0 Bootp flags: 0x006 Client IP address Your (client) IP address Your (client) IP add Relay agent IP add Client MAC address Client hardware an Server host name no Magic cookie: DHCP Length: 4 DHCP Server Ide	t Reply (2) hernet (6x81) length: 6 xa823316c 90 (Unicast) : 10.0.2,22 address: 10.0.2,22 dress: 0.0.0.0 fress: 0.0.0.0 fress: 0.0.0.0 fress: 0.0.0.0 fress: 0.0.0.0 fress: 0.0.0.0 fress: 0.0.0.0 fress: 0.0.0 fress: 0.0 fress: 0.0.0 fress: 0.0.0 fress: 0.0.0 fress: 0.0 fress: 0 fress:	(08:00:27:7c:8e:8e) 0000000000000000 0.0.2.3)					
	+ Option: (53) DHCP	Message Type (ACK)						
	+ Option: (1) Subnet	Mask (255.255.255.8	0					
	+ Option: (3) Router							

13.What is the name of the host located at 10.0.2.15?

MSEDGEWIN10

14.Insert a screenshot showing the result in Wireshark.

	udp.stream eq 3								
No.	Time	Source	Destination	Protocol	Length Info				
	1115 226.996790320	0 10.0.2.15	224.0.0.251	MDNS	77 Standard	query 0x0			
-	1117 226.997224723	3 10.0.2.15	224.0.0.251	MDNS	115 Standard	query res			
	1122 226.997980351	1 10.0.2.15	224.0.0.251	MDNS	77 Standard	query 0x0			
	1124 226.998312572	2 10.0.2.15	224.0.0.251	MDNS	115 Standard	query res			
	1511 527.077121548	3 10.0.2.15	224.0.0.251	MDNS	77 Standard	query 0x0			
	1512 527.077327656	3 10.0.2.15	224.0.0.251	MDNS	115 Standard	query res			
	Frame 1117: 115 byte	es on wire (920	bits), 115 bytes captu	red (920 bits) on interface	eth0, id 0			
* 4	Ethernet II, Src: P	csCompu_4b:e3:6	0 (08:00:27:4b:e3:60),	Dst: IPv4mcas	t_fb (01:00:5e:	00:00:fb)			
	Internet Protocol V	ersion 4, Src:	10.0.2.15, Dst: 224.0.0	.251					
* 1	Jser Datagram Proto	col, Src Port:	5353, Dst Port: 5353						
* 1	Multicast Domain Na	me System (resp	onse)						
	Transaction ID: 0	x0000							
	Flags: 0x8400 Sta	ndard query res	ponse, No error						
	Questions: 0								
	Answer RRs: 2								
	Authority RRs: 0								
	Additional RRs: 0								
	- Answers								
	MSEDGEWIN10.loc	al: type AAAA,	class IN, addr fe80::c4	46:7390:ab3:ca	186				
	 MSEDGEWIN10.loc 	al: type A, cla	iss IN, addr 10.0.2.15						
	Name: MSEDGEV	/IN10.local							
	Type: A (Host	Address) (1)							
	.000 0000 000	00 0001 = Class:	IN (0x0001)						
	0	= Cache	flush: False						
	Time to live:	. 60 (1 minute)							
	Data length:	4							
	Address: 10.0	0.2.15							
	Request In: 1115								
	[Time: 0.00043440	3 seconds]							

15.What was the first command run by the attacker?

whoami

16.Insert a screenshot showing the result in Wireshark.

```
Wireshark · Follow TCP Stream (tcp.stream eq 5) · ClS294CP.pcapng
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\IEUser>whoami
whoami
msedgewin10\ieuser
```

17.What was the process ID of the SMB session?

18.Insert a screenshot showing the result in Wireshark.

```
C:\Users\IEUser>netstat -ano
netstat -ano
Active Connections
 Proto Local Address
                                Foreign Address
                                                       State
                                                                       PID
        0.0.0.0:135
 TCP
                                0.0.0.0:0
                                                       LISTENING
                                                                       872
TCP
        0.0.0.0:445
                                0.0.0.0:0
                                                       LISTENING
                                                                       4
  TCP
        0.0.0.0:3389
                                0.0.0.0:0
                                                       LISTENING
                                                                       552
```

19.What is the full pathway for balance sheet assets.xls file?

C:\Users\IEUser\Documents\balance sheet assets.xls

20.Insert a screenshot showing the result in Wireshark.

```
C:\Users\IEUser\Documents>dir
dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Documents
06/18/2020 07:50 AM <DIR> ..
06/18/2020 07:50 AM <DIR> ..
06/18/2020 07:38 AM 153,088 balance sheet 2017.xls
06/18/2020 07:43 AM 1,925,632 balance sheet assets.xls
06/18/2020 07:45 AM 203,776 five year summary financial data.xls
06/18/2020 07:39 AM 398,336 working capital analysis.xls
4 File(s) 2,680,832 bytes
2 Dir(s) 20,073,222,144 bytes free
```

C:\Users\IEUser\Documents>

Part 2 PCAP Analysis Extra Credit

For a potential 10 extra points (each correct answer or screenshot is worth 2.5 point each), look in CIS294CP.pcapng for the following:

1. What is the message hidden in the comments?

packet analysis is fun!!

2. Insert a screenshot showing the result in Wireshark.

10.0.2.22	TCF
:packet analysis is fi	
	10.0.2.22 packet analysis is fu

3. What type of CPU was used by the attacker? Provide the complete

make/model/type

Intel Core i7-9750H CPU @ 2.60GHz (with SSE4.2)

4. Insert a screenshot showing the result in Wireshark.

Time	
First packet:	2020-06-18 10:21:12
Last packet:	2020-06-18 12:20:36
Elapsed:	01:59:23
Capture	
Hardware:	Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (with SSE4.2)
OS:	Linux 5.2.0-kali2-amd64
Application:	Dumpcap (Wireshark) 3.0.3 (Git v3.0.3 packaged as 3.0.3-1)