



SEM 2 2022/2023 (A222)

MTN 3024
Network Security

ASSIGNMENT NO: 1

Name: Mohd Izzul Ikhwan Bin Mohd Yusof

Matric Number: D20201095609

Lecture Group: A

Lecturer: Dr. Okta Nurika



MTN3024 Network Security

Assignment 1 (Individual): Malware Traffic Analysis (10% of Coursemark)

Submission due date: 5 May 2023 at 23:00

CLO: CL01 – Understand theory and practice of network fundamentals from the defender's and attacker's perspectives

Question:

As a network forensic investigator, you have been asked to analyze a packet capture (pcap) file, which contains traces of communication that are suspected to contain malware transmission. You should do the following tasks as follows:

- a) What are the local hosts' IP addresses and MAC addresses?

Hint: Local hosts are the ones having private IP addresses. (10 marks)

Answer:

- Local host IP address = 172.16.1.16
- Local host MAC address = Dell_27:b0:f9 (00:1e:4f:27:b0:f9)

- b) What are the external hosts' IP addresses and MAC addresses? (10 marks)

Answer:

- External host IP address = 172.16.1.137
- External host MAC address = Baumulle_34:b4:fa (00:02:fb:34:b4:fa)

c) What is the IP address of the local DNS server? (Include screenshot). (7 marks)

Answer:

- Local DNS server IP address = 40.126.32.132

malware traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
9548	1468.722873	172.16.1.16	172.16.1.137	DNS	225	Standard query response 0xc953 A settings-win.dat
9194	1270.267138	172.16.1.16	172.16.1.137	DNS	160	Standard query response 0xc5cd No such name A wpa
7274	1190.904263	172.16.1.16	172.16.1.137	DNS	108	Standard query response 0xc5a9 A pcapworkshop-dc.
6995	995.046989	172.16.1.16	172.16.1.137	DNS	179	Standard query response 0xc4c1 A x1.c.lencr.org C
7391	1191.229726	172.16.1.16	172.16.1.137	DNS	201	Standard query response 0xc1aa SRV _ldap._tcp.Def
2989	131.207741	172.16.1.16	172.16.1.137	DNS	328	Standard query response 0xc11e A login.microsoft
6954	933.904668	172.16.1.16	172.16.1.137	DNS	226	Standard query response 0xc08b A v10.events.data.
288	1.486541	172.16.1.16	172.16.1.137	DNS	257	Standard query response 0xc06a A www.bing.com CNA
9865	1805.084960	172.16.1.16	172.16.1.137	DNS	230	Standard query response 0xbca5 A v10.events.data.
9593	1522.200422	172.16.1.16	172.16.1.137	DNS	92	Standard query response 0xb614 A dns.msftncsi.com
1250	4.456268	172.16.1.16	172.16.1.137	DNS	181	Standard query response 0xb2d2 A edge.microsoft.c
8945	1219.195394	172.16.1.16	172.16.1.137	DNS	160	Standard query response 0xb224 No such name A wpa

www.tm.ak.prd.aadg.trafficmanager.net: type A, class IN, addr 40.126.32.132

Name: www.tm.ak.prd.aadg.trafficmanager.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 142 (2 minutes, 22 seconds)

Data length: 4

Address: 40.126.32.132

[Request In: 2987]

[Time: 0.075755000 seconds]

Text item (text), 16 bytes

Packets: 9936 · Displayed: 156 (1.6%)

Profile: Default

d) What is the hostname of the local DNS server? (Include screenshot). (7 marks)

Answer:

- Host name = www.tm.ak.prd.aadg.trafficmanager.net

malware traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
9548	1468.722873	172.16.1.16	172.16.1.137	DNS	225	Standard query response 0xc953 A settings-win.dat
9194	1270.267138	172.16.1.16	172.16.1.137	DNS	160	Standard query response 0xc5cd No such name A wpa
7274	1190.904263	172.16.1.16	172.16.1.137	DNS	108	Standard query response 0xc5a9 A pcapworkshop-dc.
6995	995.046989	172.16.1.16	172.16.1.137	DNS	179	Standard query response 0xc4c1 A x1.c.lencr.org C
7391	1191.229726	172.16.1.16	172.16.1.137	DNS	201	Standard query response 0xc1aa SRV _ldap._tcp.Def
2989	131.207741	172.16.1.16	172.16.1.137	DNS	328	Standard query response 0xc11e A login.microsoft
6954	933.904668	172.16.1.16	172.16.1.137	DNS	226	Standard query response 0xc08b A v10.events.data.
288	1.486541	172.16.1.16	172.16.1.137	DNS	257	Standard query response 0xc06a A www.bing.com CNA
9865	1805.084960	172.16.1.16	172.16.1.137	DNS	230	Standard query response 0xbca5 A v10.events.data.
9593	1522.200422	172.16.1.16	172.16.1.137	DNS	92	Standard query response 0xb614 A dns.msftncsi.com
1250	4.456268	172.16.1.16	172.16.1.137	DNS	181	Standard query response 0xb2d2 A edge.microsoft.c
8945	1219.195394	172.16.1.16	172.16.1.137	DNS	160	Standard query response 0xb224 No such name A wpa

www.tm.ak.prd.aadg.trafficmanager.net: type A, class IN, addr 40.126.32.132

Name: www.tm.ak.prd.aadg.trafficmanager.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 142 (2 minutes, 22 seconds)

Data length: 4

Address: 40.126.32.132

[Request In: 2987]

[Time: 0.075755000 seconds]

Text item (text), 16 bytes

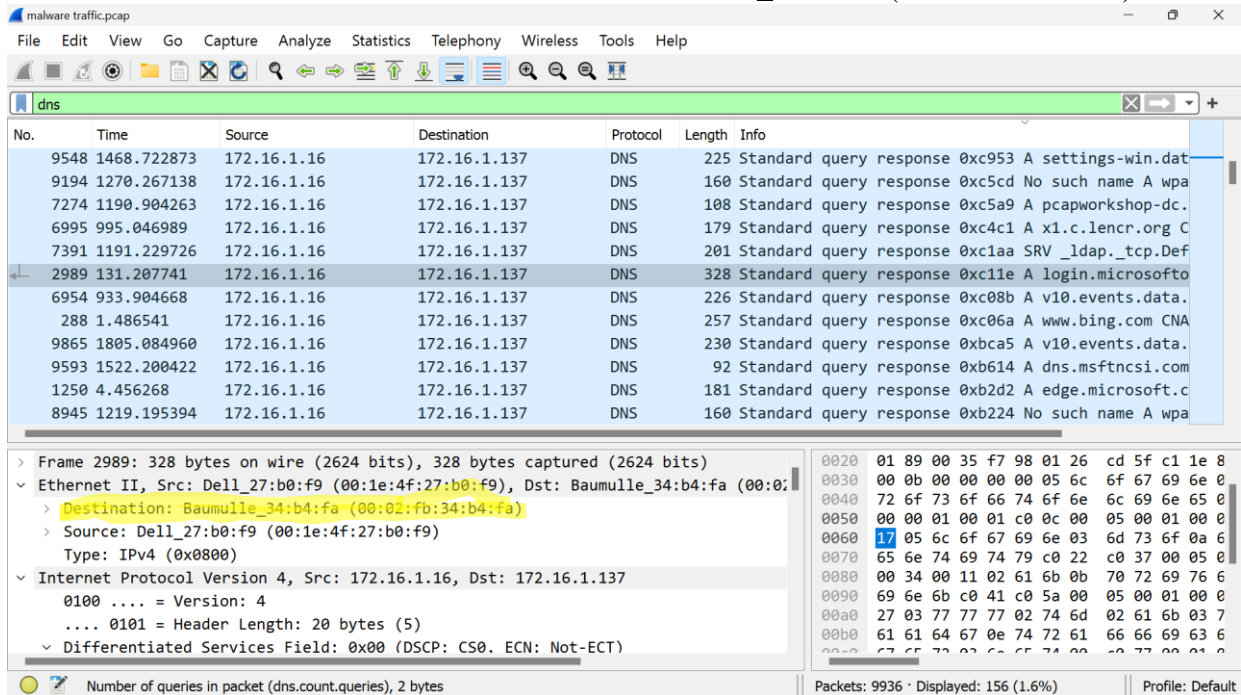
Packets: 9936 · Displayed: 156 (1.6%)

Profile: Default

e) What is the MAC address of the local DNS server? (Include screenshot). (7 marks)

Answer:

- Local DNS server MAC address = Baumulle_34:b4:fa (00:02:fb:34:b4:fa)



f) What is the SSL/TLS version between a local host and an external host? (5 marks)

Answer:

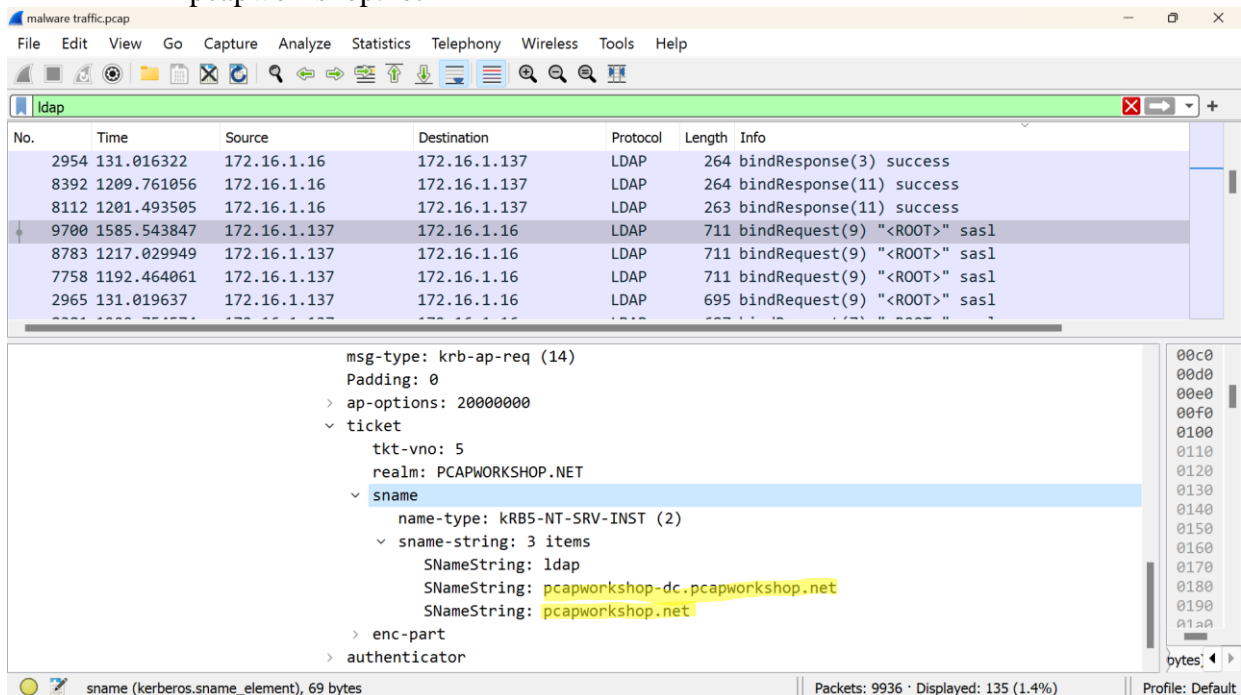
- SSL/TLS version for local host and external host = TLS 1.2 (0x0303)

g) What is the IP address of the local LDAP server? (Include screenshot). (7 marks)

h) What is the hostname of the local LDAP server? (Include screenshot). (7 marks)

Answer:

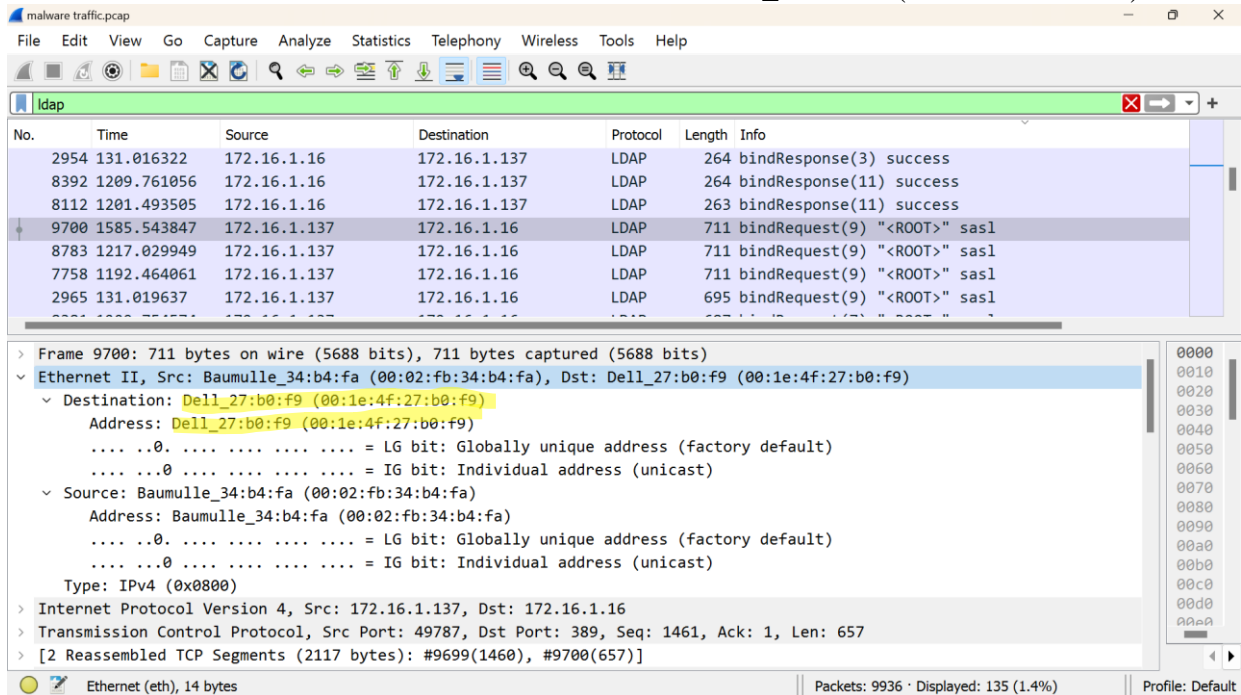
- Hostname for local LDAP server = pcapworkshop-dc.pcapworkshop.net // pcapworkshop.net



i) What is the MAC address of the local LDAP server? (Include screenshot). (7 marks)

Answer:

- Mac address of the local LDAP server = Dell_27:b0:f9 (00:1e:4f:27:b0:f9)



The screenshot shows a Wireshark packet capture of LDAP traffic. The packet list at the top shows several packets, with frame 9700 selected. The packet details pane shows the following information:

- Frame 9700: 711 bytes on wire (5688 bits), 711 bytes captured (5688 bits)
- Ethernet II, Src: Baumulle_34:b4:fa (00:02:fb:34:b4:fa), Dst: Dell_27:b0:f9 (00:1e:4f:27:b0:f9)
 - Destination: Dell_27:b0:f9 (00:1e:4f:27:b0:f9)
 - Address: Dell_27:b0:f9 (00:1e:4f:27:b0:f9)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Source: Baumulle_34:b4:fa (00:02:fb:34:b4:fa)
 - Address: Baumulle_34:b4:fa (00:02:fb:34:b4:fa)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.16.1.137, Dst: 172.16.1.16
- Transmission Control Protocol, Src Port: 49787, Dst Port: 389, Seq: 1461, Ack: 1, Len: 657
- [2 Reassembled TCP Segments (2117 bytes): #9699(1460), #9700(657)]

The packet bytes pane on the right shows the raw data of the packet, starting with 0000.

j) Find one HTTP connection between a local host and an external host and identify the IP addresses and port numbers of these two (2) hosts. (Include screenshot). (11 marks)

Answer:

- IP address & port number for local host for this HTTP = 172.16.1.137 // 59393
- IP address & port number for external host for this HTTP = 62.173.149.243 // 80

The screenshot displays a Wireshark packet capture of an HTTP connection. The packet list at the top shows several HTTP packets. The selected packet is a GET request for /stilak32.rar from 172.16.1.137 to 62.173.149.243. The packet details pane shows the TCP segment and the HTTP request. The packet bytes pane shows the raw data of the request.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
424911	0.000000	62.173.149.243	172.16.1.137	HTTP	871	HTTP/1.1 200 OK (application/x-rar-compressed)
279613	0.000000	62.173.149.243	172.16.1.137	HTTP	555	HTTP/1.1 200 OK (application/x-rar-compressed)
282227	0.000000	172.16.1.137	62.173.149.243	HTTP	232	GET /stilak64.rar HTTP/1.1
923498	0.000000	172.16.1.137	62.173.149.243	HTTP	232	GET /stilak32.rar HTTP/1.1
864989	0.000000	172.16.1.137	62.173.149.243	HTTP	230	GET /cook64.rar HTTP/1.1

Packet Details:

...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x680f [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.16.1.137
Destination Address: 62.173.149.243
Transmission Control Protocol, Src Port: 59393, Dst Port: 80, Seq: 179, Ack: 335784, Len: 178
Source Port: 59393
Destination Port: 80
[Stream index: 30]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 178]
Sequence Number: 179 (relative sequence number)
Sequence Number (raw): 323503800
[Next Sequence Number: 357 (relative sequence number)]

Packet Bytes:

```
GET /stilak32.rar HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
Host: 62.173.149.243
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 07 Mar 2023 02:07:20 GMT
Content-Type: application/x-rar-compressed
Content-Length: 335512
Last-Modified: Thu, 09 Feb 2023 21:25:34 GMT
Connection: keep-alive
ETag: "63e564ce-51e98"
Accept-Ranges: bytes
```


- k) Find one suspicious HTTP request that involved GET method. What is the requested file name? What are the IP address and port number of the host that transmitted this file? (Include screenshot). (11 marks)

Answer:

- Suspicious requested file name =
/drew/jBcVZ8UcDrrEW_2FFnbUN/XSkJ9jePxFRayUi9/fe72tvcL3iDN8Xi/B5Loj2rlckd1EIZgQM/ahgZg7Wpq/uYLcXDImxlRljA7bacS/rso8_2Bj6bDTVecKwa_/2FXNru1dMqBrglxg4F8Loq/njSjfHHGrQ5_2/BLHEMs_2/BjcqAbhuuvFRfNNp5i72uIv/uAmxeaidFU/e
- IP address of the host who transmitted this file = 46.8.19.86
- Port number of the host who transmitted this file = 80

The screenshot shows the Wireshark interface with a packet capture of malware traffic. The top pane displays a list of captured packets, with packet 589 selected. The middle pane shows the details of this packet, which is an HTTP GET request. The bottom pane shows the raw data of the packet.

No.	Source	Destination	Protocol	Length	Info
41884	172.16.1.137	173.254.32.85	HTTP	492	GET /mise/Cliente.zip HTTP/1.1
242641	172.16.1.137	62.173.138.138	HTTP	568	GET /drew/uyoXjOLPocMIEKrQlytVaWB/N_2Bjo4B1_/2BB8ggy1qo0bUbbK...
164731	172.16.1.137	62.173.140.94	HTTP	585	GET /drew/uxz9_2FZjFA21sXSRhF/dn7GeVjur_2BwkHo0TFsjm/_2BdLwdP...
589	172.16.1.137	46.8.19.86	HTTP	589	GET /drew/txYmhbQeS_2B/ZyS1I6NGQZ5/7yj1MeczMe_2B_/2FLQm5pa0gK...
259865	172.16.1.137	31.41.44.60	HTTP	591	GET /drew/qRV9mk9ZQT/WAZy2Izgfwv_2B/BQ048YfdQHKoe_2B_2Ff7/xb...
30607	172.16.1.137	46.8.19.233	HTTP	557	GET /drew/jBcVZ8UcDrrEW_2FFnbUN/XSkJ9jePxFRayUi9/fe72tvcL3iDN...
233457	172.16.1.137	62.173.140.76	HTTP	593	GET /drew/iHF4Eh26/Q3FNpetumnIfxyEIRI3Vfxp/SBEUGj9Z07/mCagQ3Y...

Protocol: TCP (6)
Header Checksum: 0x57b3 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.16.1.137
Destination Address: 46.8.19.86

Transmission Control Protocol, Src Port: 59430, Dst Port: 80, Seq: 530, Ack: 208, Len: 535
Source Port: 59430
Destination Port: 80
[Stream index: 51]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 535]
Sequence Number: 530 (relative sequence number)
Sequence Number (raw): 3008601453

HTTP User-Agent header (http.user_agent), 77 bytes

- 1) What is the URL of the suspicious requested file in the previous HTTP request? What is the HTTP version being used? Will the connection be closed after this file is transmitted? (Include screenshot). (11 marks)

Answer:

- URL of the suspicious requested file in the previous HTTP request = <http://46.8.19.86/drew/87Kol3wsW64/XzUI9sN5W8mEJo/Ry4an4JvksM8Ymx60M6o5/PQtzOD>
- HTTP version = HTTP/1.1
- Will the connection be closed after this file is transmitted? = Keep-Alive

The screenshot displays the Wireshark interface with a packet capture of an HTTP request. The top pane shows a list of packets, with packet 7051 selected. The middle pane shows the details of the selected packet, which is a Hypertext Transfer Protocol (HTTP) GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
3597	353.503095	172.16.1.137	62.173.140.103	HTTP	579	GET /drew/Q0EmvhsKdMeV_2B/h1ZqNxHPY3pA7HNxtL/9pXV
6988	970.280802	172.16.1.137	31.41.44.49	HTTP	568	GET /drew/LW7Yj7P8/aU1IMxI3vmot8f5MaoVHI4_/2FoM2M
9579	1479.207619	172.16.1.137	46.8.19.233	HTTP	561	GET /drew/KU4sSnNPgqF6dYVU/zMqg5LcUpXWHQk4/p13Tzr
9379	1419.205966	172.16.1.137	31.41.44.60	HTTP	566	GET /drew/ISHH0icNxxz6/Z8DngQGFVizm4L/FOC1M6PodyP1
9359	1358.961686	172.16.1.137	62.173.140.94	HTTP	583	GET /drew/Gs600gTSTNQmj5Wj0SbvjN/e3N2BAAt1DgtuW/sw
5645	421.025943	172.16.1.137	62.173.138.138	HTTP	663	GET /drew/At0eNEowDE_2Fx50b/NFBz3bCzAt61/AVGjZ99D
7051	1030.304592	172.16.1.137	46.8.19.86	HTTP	583	GET /drew/87Kol3wsW64/XzUI9sN5W8mEJo/Ry4an4JvksM8

Packet Details:

- Transmission Control Protocol, Src Port: 59430, Dst Port: 80, Seq: 1, Ack: 1, Len: 529
- Hypertext Transfer Protocol
 - [truncated]GET /drew/87Kol3wsW64/XzUI9sN5W8mEJo/Ry4an4JvksM8Ymx60M6o5/PQtzODdyH1TG1TtY/8vNIghEJJhKHPdL/gvYCYzkuSkLZDTI
 - [truncated]Expert Info (Chat/Sequence): GET /drew/87Kol3wsW64/XzUI9sN5W8mEJo/Ry4an4JvksM8Ymx60M6o5/PQtzODdyH1TG1T
 - Request Method: GET
 - Request URI [truncated]: /drew/87Kol3wsW64/XzUI9sN5W8mEJo/Ry4an4JvksM8Ymx60M6o5/PQtzODdyH1TG1TtY/8vNIghEJJhKHPdL/gv
 - Request Version: HTTP/1.1
 - User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)\r\n
 - Host: 46.8.19.86\r\n
 - Connection: Keep-Alive\r\n
 - Cache-Control: no-cache\r\n
 - \r\n
 - [Full request URI [truncated]: http://46.8.19.86/drew/87Kol3wsW64/XzUI9sN5W8mEJo/Ry4an4JvksM8Ymx60M6o5/PQtzODdyH1TG1T

Raw Data:

0030
0040
0050
0060
0070
0080
0090
00a0
00b0
00c0
00d0
00e0
00f0
0100
0110
0120

Copied http://46.8.19.86/drew/87Kol3wsW64/XzUI9sN5W8mEJo/Ry4an4JvksM8Ymx60M6o5/PQtzOD

Packets: 9936 · Displayed: 35 (0.4%)

Profile: Default



MTN3024 Network Security

Assessment Rubric for Assignment 1 (Individual)

CLO: CL01 – Understand theory and practice of network fundamentals from the defender's and attacker's perspectives

Malware Traffic Analysis (100 Marks)

Item	Level C (0-3 marks)	Level B (4-7 marks)	Level A (8-10 marks)	Mark
a.	Minimum local hosts discovery with neat presentation	Significant local hosts discovery with neat presentation	Complete local hosts discovery with neat presentation	
b.	Minimum external hosts discovery with neat presentation	Significant external hosts discovery with neat presentation	Complete external hosts discovery with neat presentation	
Item	Level C (0-3 marks)	Level B (3-5 marks)	Level A (5-7 marks)	
c.	Incorrect IP address of the local DNS server	Correct IP address of the local DNS server without neat presentation	Correct IP address of the local DNS server with neat presentation	
d.	Incorrect hostname of the local DNS server	Correct hostname of the local DNS server without neat presentation	Correct hostname of the local DNS server with neat presentation	
e.	Incorrect MAC address of the local DNS server	Correct MAC address of the local DNS server without neat presentation	Correct MAC address of the local DNS server with neat presentation	
Item	Level C (0 mark)	Level B (1-3 marks)	Level A (4-5 marks)	
f.	Incorrect SSL/TLS version	Incorrect SSL/TLS version without neat	Correct SSL/TLS version with neat	

		presentation	presentation	
	Level C (0-3 marks)	Level B (3-5 marks)	Level A (5-7 marks)	
g.	Incorrect IP address of the local LDAP server	Correct IP address of the local LDAP server without neat presentation	Correct IP address of the local LDAP server with neat presentation	
h.	Incorrect hostname of the local LDAP server	Correct hostname of the local LDAP server without neat presentation	Correct hostname of the local LDAP server with neat presentation	
i.	Incorrect MAC address of the local LDAP server	Correct MAC address of the local LDAP server without neat presentation	Correct MAC address of the local LDAP server with neat presentation	
	Level C (0-3 marks)	Level B (4-7 marks)	Level A (8-11 marks)	
j.	Incorrect IP addresses and port numbers	Correct IP addresses and port numbers without neat presentation	Correct IP addresses and port numbers with neat presentation	
k.	Incorrect filename, IP addresses, and port number	Correct filename, IP addresses, and port number without neat presentation	Correct filename, IP addresses, and port number with neat presentation	
l.	Incorrect URL, HTTP version, and connection status after transmission.	Correct URL, HTTP version, and connection status after transmission without neat presentation	Correct URL, HTTP version, and connection status after transmission with neat presentation	
Total Mark				
Grade marks Total mark/100 x 10%)				