

ENPM685 – Security Tools for Information Security

Section: 0101

Homework – 5

Name: Syed Mohammad Ibrahim

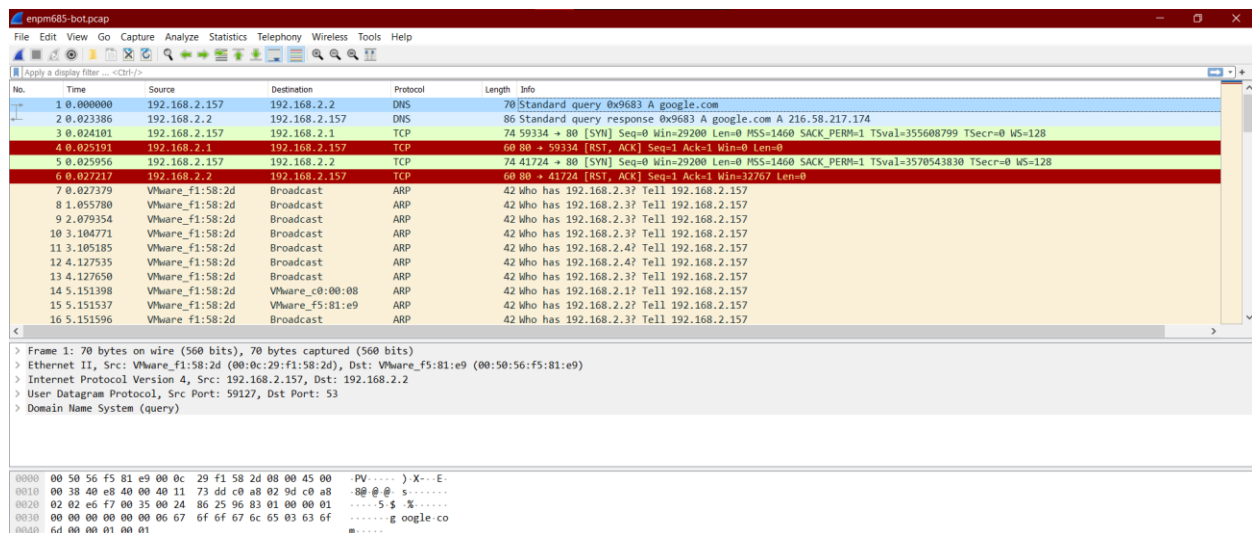
UID: *iamibi*

UID Number: 118428369

Email – iamibi@umd.edu

1. Reviewing the network traffic, what is the first thing that the executable does? Why do you think it is doing it?

A. The executable is trying to reach out to google.com. This could be to verify whether there is a network connectivity available or not.



2. There is a large number of ARP queries, why do you think that is? What might the executable be doing?

A. The large number of ARP queries are to check which system on the local network is available and is responding with their MAC address. If the executable is malicious, then it could be performing ARP spoofing, where a threat actor sends spoofed ARP response to any computer on the network to believe that certain IP address is associated with certain MAC address. However, this executable can be performing a legitimate scan required for its functionality and thus, could be non-malicious.

No.	Time	Source	Destination	Protocol	Length	Info
7	0.02379	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.157
8	1.055780	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.157
9	2.079354	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.157
10	3.104771	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.157
11	3.105185	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.4? Tell 192.168.2.157
12	4.127535	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.4? Tell 192.168.2.157
13	4.127650	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.157
14	5.151398	VMware_F1:58:2d	VMware_C0:00:08	ARP	42	Who has 192.168.2.1? Tell 192.168.2.157
15	5.151537	VMware_F1:58:2d	VMware_F5:81:e9	ARP	42	Who has 192.168.2.2? Tell 192.168.2.157
16	5.151596	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.3? Tell 192.168.2.157
17	5.151675	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.4? Tell 192.168.2.157
18	5.151756	VMware_C0:00:08	VMware_F1:58:2d	ARP	60	192.168.2.1 is at 00:50:56:c0:00:08
19	5.151769	VMware_F5:81:e9	VMware_F1:58:2d	ARP	60	192.168.2.2 is at 00:50:56:f5:81:e9
20	6.176023	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.4? Tell 192.168.2.157
21	6.176324	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.5? Tell 192.168.2.157
22	7.200431	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.5? Tell 192.168.2.157
23	7.200559	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.4? Tell 192.168.2.157
24	8.223694	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.4? Tell 192.168.2.157
25	8.223810	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.5? Tell 192.168.2.157
26	9.248437	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.5? Tell 192.168.2.157
27	9.248903	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.6? Tell 192.168.2.157
28	10.272462	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.6? Tell 192.168.2.157
29	10.272614	VMware_F1:58:2d	Broadcast	ARP	42	Who has 192.168.2.5? Tell 192.168.2.157

> Frame 14: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 > Ethernet II, Src: VMware_F1:58:2d (00:0c:29:f1:58:2d), Dst: VMware_C0:00:08 (00:50:56:c0:00:08)
 > Address Resolution Protocol (request)

```

0000  00 50 56 c0 00 00 0c 29 f1 58 2d 08 00 01  -PV.....)X-----
0010  08 00 06 04 00 01 00 0c 29 f1 58 2d c0 a8 02 9d  -.....)X-----
0020  00 00 00 00 00 c0 a8 02 01  -.....)
  
```

3. Does the executable make any call out to a command and control server? If so, what is the IP address, host name, and/or URL it calls out to? What kind of a response does it receive?

A. Yes, the executable makes a call to command-and-control server. The IP addresses of the server are 128.8.27.69, 128.8.55.24 and 128.8.138.8, hostname is **advancedengineering.umd.edu** and the URL is <http://advancedengineering.umd.edu/enpm685-is-the-best-class-ever>.

The response is HTTP/1.1 301 Moved Permanently. It contains additional message which says that the site has been moved to an HTTPS connection <https://advancedengineering.umd.edu/enpm685-is-the-best-class-ever>. However, any other information is not available because the further communication happens over HTTPS which makes it difficult to identify whether any data was transmitted as part of the GET query or not.

The image shows a Wireshark packet capture of a network traffic file named 'enpm685-bot.pcap'. The main display area shows a list of packets, with the selected packet (No. 1577) expanded to show its details and raw data. The packet list shows several HTTP GET requests to 'enpm685-is-the-best-class-ever' from various source IP addresses to 192.168.2.157. The selected packet (No. 1577) is an HTTP 301 Moved Permanently response from 192.168.2.157 to 128.8.27.69. The details pane shows the response structure, including the status line '301 Moved Permanently', the 'Location' header pointing to 'https://advancedengineering.umd.edu/enpm685-is-the-best-class-ever', and the body content which is an HTML document with a 301 Moved Permanently message.

No.	Time	Source	Destination	Protocol	Length	Info
1575	1506.766778	192.168.2.157	128.8.27.69	HTTP	218	GET /enpm685-is-the-best-class-ever HTTP/1.1
1577	1506.803668	128.8.27.69	192.168.2.157	HTTP	667	HTTP/1.1 301 Moved Permanently (text/html)
1626	1506.997667	192.168.2.157	128.8.55.24	HTTP	218	GET /enpm685-is-the-best-class-ever HTTP/1.1
1629	1507.031732	128.8.55.24	192.168.2.157	HTTP	667	HTTP/1.1 301 Moved Permanently (text/html)
1680	1507.227510	192.168.2.157	128.8.138.8	HTTP	218	GET /enpm685-is-the-best-class-ever HTTP/1.1
1682	1507.259449	128.8.138.8	192.168.2.157	HTTP	667	HTTP/1.1 301 Moved Permanently (text/html)
1732	1507.476730	192.168.2.157	128.8.27.69	HTTP	218	GET /enpm685-is-the-best-class-ever HTTP/1.1
1734	1507.514151	128.8.27.69	192.168.2.157	HTTP	667	HTTP/1.1 301 Moved Permanently (text/html)

```

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://advancedengineering.umd.edu/enpm685-is-the-best-class-ever">here</a>.</p>
</html>
  
```

4. After reviewing the packet capture of the network traffic generated by the executable and answering questions 1-3 what is your final determination – is the executable malicious? Provide a short write up on why or why not you believe the executable is malicious.

A. After analysis, it can be said that the executable might be displaying some erratic behavior considering just the network traffic. It is scanning the local network and getting any MAC address on it which could be a legitimate use-case considering the functionality of an application for monitor purpose. It could be malicious if the GET calls are transmitting any kind of sensitive information to the command-and-control server, but it is not identifiable from the given pcap file and further analysis is required.