# ENPM685 – Security Tools for Information Security

Section: 0101

## Homework – 5

Name: Syed Mohammad Ibrahim

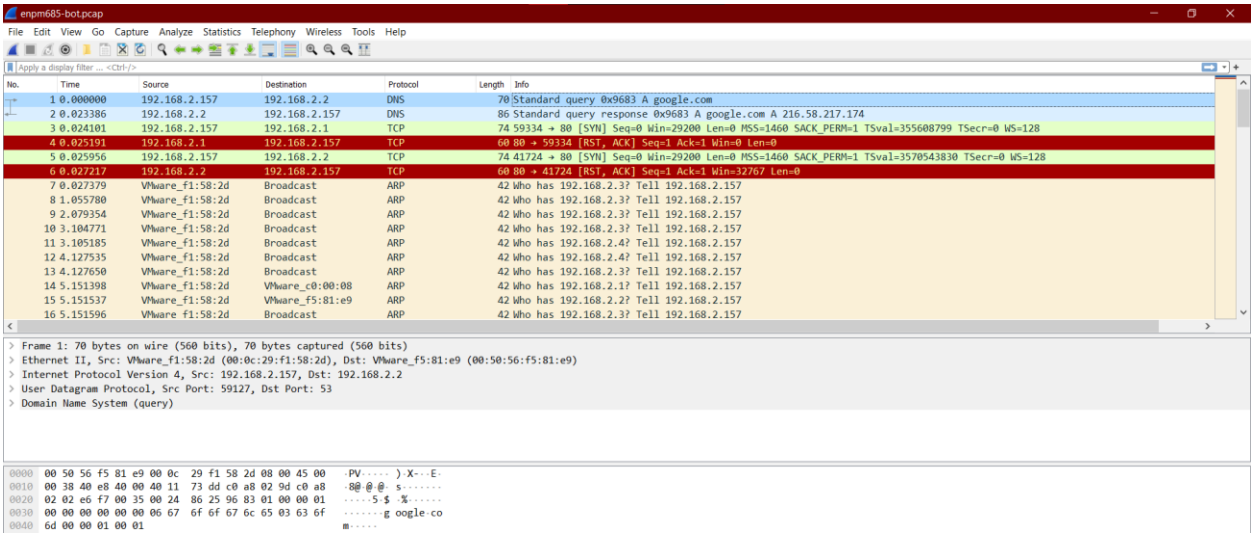
UID: *iamibi*

UID Number: 118428369

Email – *iamibi@umd.edu*

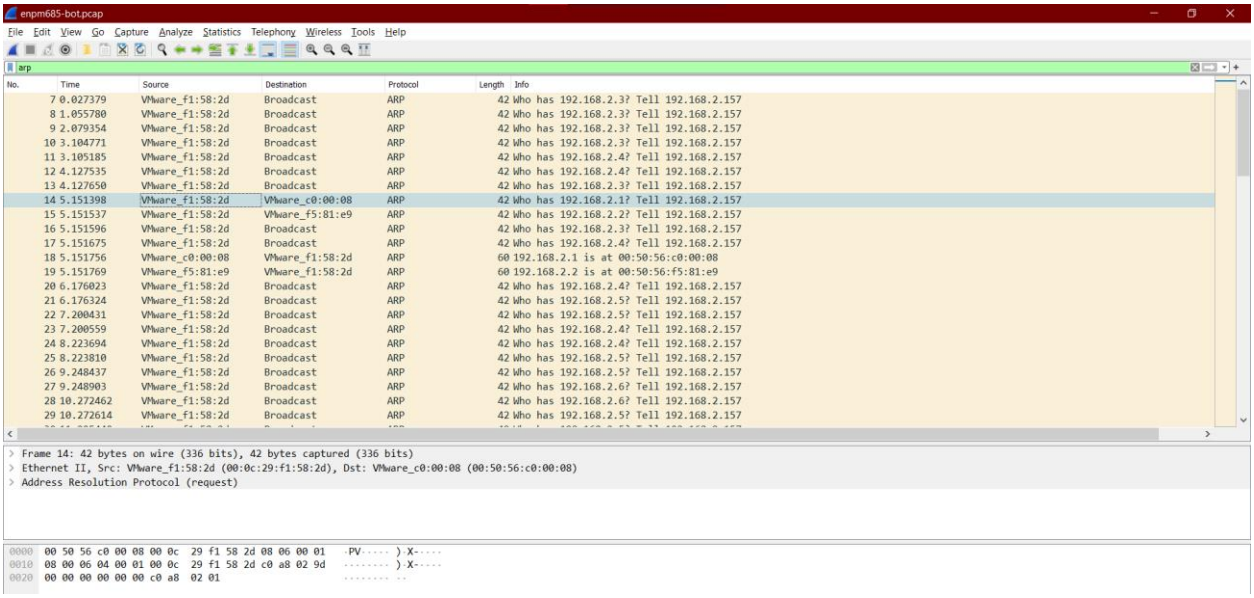
1. Reviewing the network traffic, what is the first thing that the executable does? Why do you think it is doing it?

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?

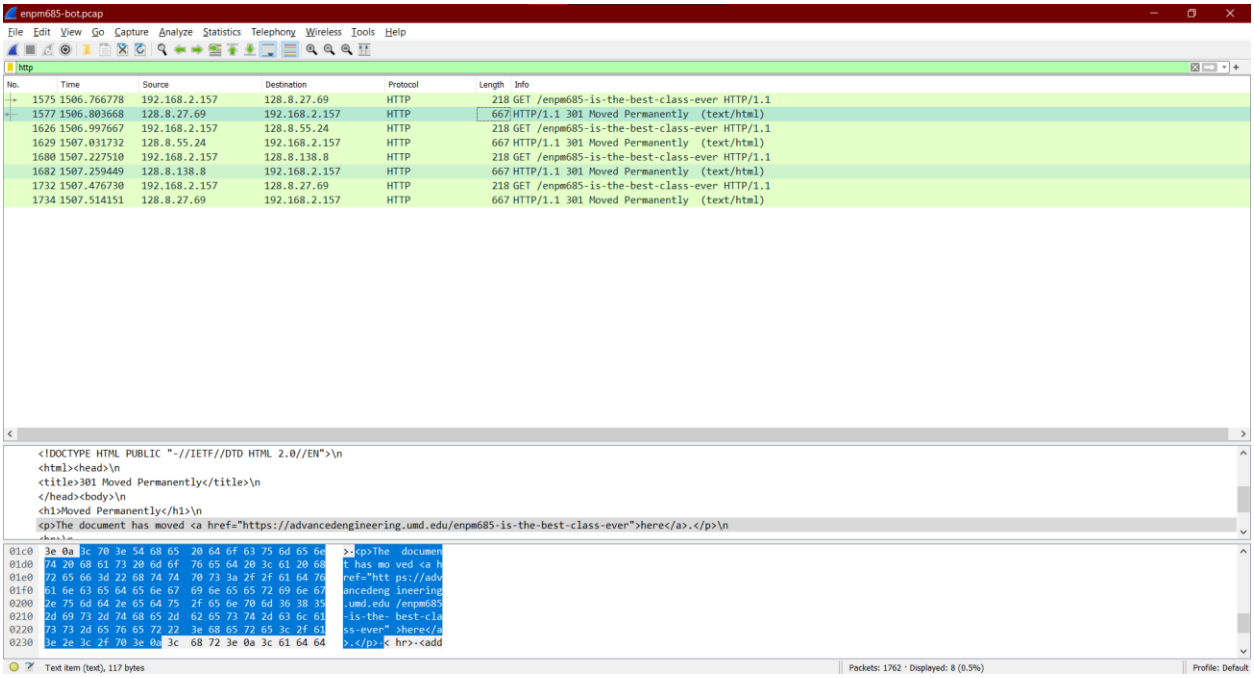
A. The large number of ARP queries are to check which system on the local network is available and is responding with their MAC address. If the executable is malicious, then it could be performing ARP spoofing, where a threat actor sends spoofed ARP response to any computer on the network to believe 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.




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.




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.