Christopher Bazyani

Practical Cyber Security

Unit 3

Packet Sniffing – ARP

**Finding your IP address and Gateway address**

Opening a command prompt as an administrator

Graphical user interface, application

Description automatically generated

Finding the Ethernet address of the main network interface of my computer with the ipconfig command



Finding the IP address of the local router or default gateway that my computer uses to reach the rest of the Internet using the netstat / route command.

Graphical user interface, text

Description automatically generated

Adding a filter of “arp” in Wireshark

Table

Description automatically generated

Using the “arp” command to clear the default gateway from the ARP cache. Using the command “arp –a” will show you the contents of the ARP cache as a check that I can run “arp”.

Going to command prompt and type arp -a

Calendar

Description automatically generated with medium confidence

Clearing this entry with the use of the arp command with different arguments like “arp –d” on Windows. Typing arp -d in the command prompt

Text

Description automatically generated

**Inspect the supplied ARP Trace**

Opening the trace.arp file provided in Wireshark

Graphical user interface, text, application

Description automatically generated

Setting a display filter for packets with the Ethernet address of my computer which is this case is 00:25:64:d5:10:8b

A picture containing text

Description automatically generated

Find and select an ARP request for the default gateway and examine its fields focusing on the Address Resolution Protocol for both the reply and request APR packets

Packet 2 (reply)

Graphical user interface, text, application

Description automatically generated

Packet 7 (request)

Text, letter

Description automatically generated

**Details of ARP over Ethernet**

**1. What opcode is used to indicate a request? What about a reply?**

Request opcode is 1 and the reply opcode is 2.





**2. What value is carried on a request for the unknown target MAC address?**

Target MAC address of the request is usually all zeros.



**3. What Ethernet Type value which indicates that ARP is the higher layer protocol?**

Ethernet Type value for ARP is 0x806.



**4. Is the ARP reply broadcast (like the ARP request) or not?**

ARP replies are usually not transmitted and are delivered directly to the target's Ethernet address.