# Cybersecurity

# **Activity 3.3.1 Analyzing Address Resolution**

Copy and paste screenshots and/or answer questions from the activity.

#4

|  |  |
| --- | --- |
| **arp\_resolution: Packet 1: Frame details** | |
| Arrival Time | December 10, 11:59pm |
| Frame Length | 42 bytes |
| Protocols in Frame | eth:ethertype:arp |

#5

|  |  |
| --- | --- |
| **arp\_resolution: Packet 1: Ethernet details** | |
| Source Address | 00:16:ce:6e:8b:24 |
| Destination Address | ff:ff:ff:ff:ff:ff |

What is the format of these two addresses? A MAC address

What makes the destination a broadcast address? ff:ff:ff:ff:ff:ff

#6

|  |  |
| --- | --- |
| **arp\_resolution: Packet 1: Address Resolution Protocol Details** | |
| Protocol Type | IPv4 (0x0800) |
| Opcode | request (1) |
| Sender (source) MAC Address | 00:16:ce:6e:8b:24 |
| Sender (source) IP Address | 192.168.0.114 |
| Target (destination) MAC Address | 00:00:00:00:00:00 |
| Target (destination) IP Address | 192.168.0.1 |

#12

|  |  |
| --- | --- |
| **arp\_resolution: Packet 2: Frame details** | |
| Arrival Time | December 10, 11:59pm |
| Frame Length | 46 bytes |
| Protocols in Frame | eth:ethertype:arp |

#14

|  |  |
| --- | --- |
| **arp\_resolution: Packet 2: Ethernet details** | |
| Source Address | 00:13:46:0b:22:ba |
| Destination Address | 00:16:ce:6e:8b:24 |

#15

|  |  |
| --- | --- |
| **arp\_resolution: Packet 2: Address Resolution Protocol Details** | |
| Protocol Type | IPv4 (0x0800) |
| Opcode | reply (2) |
| Sender (source) MAC Address | 00:13:46:0b:22:ba |
| Sender (source) IP Address | 192.168.0.1 |
| Target (destination) MAC Address | 00:16:ce:6e:8b:24 |
| Target (destination) MAC Address | 192.168.0.114 |

* 1. Comparing the request and reply packets, how are the opcodes related?

The reply (2) represents the answer to the request (1) sent out.

* 1. What is the Sender MAC address value and where else does it appear in Wireshark?

**D-Link\_0b:22:ba**and  **00:13:46:0b:22:ba and it also appears Source Value under Ethernet II**

* 1. Consider a situation where the Sender MAC address doesn’t match that of the host sending the reply. What might that indicate?

Getting the wrong answer to the question being broadcasted.

#29

|  |  |
| --- | --- |
| **arp\_poison** | |
| Source | Hewlett\_bf:91:ee |
| Src MAC | Hewlett\_bf:91:ee |
| Destination | Dell\_c0:56:f0 |
| Dest MAC | Dell\_c0:56:f0 |

#30

|  |  |
| --- | --- |
| **arp\_poison: Details values** | |
| Opcode | request (1) |
| Sender MAC Address | Hewlett\_bf:91:ee (00:25:b3:bf:91:ee) |
| Sender IP Address | 172.16.0.1 |
| Target MAC Address | 00:00:00\_00:00:00 |
| Target MAC Address | 172.16.0.107 |

#31 Compare what you know about your router (IP and MAC address) to the packet data. What appears strange about this ARP broadcast message?

The MAC address as reported is incorrect. It appears that Hewlett\_bf:91:ee is acting like the 172.16.0.1 router

#32 Explore differences between the legitimate ARP broadcast and the one that is an ARP poison. What are some additional clues that indicate a message has been poisoned?

Reports the target MAC is the broadcast (00:00:00:00:00:00) but this conflicts with the Dest MAC address and it is not a broadcast but rather a unicast message to spoof the address

#33

|  |  |
| --- | --- |
| **arp\_poison: Reply values** | |
| Opcode | Repy (2) |
| Sender MAC Address | Dell\_c0:56:f0 |
| Sender IP Address | 172.16.0.107 |
| Target MAC Address | Hewlett\_bf:91:ee |
| Target MAC Address | 172.16.0.1 |

#34

Record the packet numbers for the ARP request and ARP reply. You will reference these packets in the next section.

ARP request: 54

ARP reply: 55

#37

|  |  |
| --- | --- |
| **arp\_poison: good packet** | |
| Source | 12.153.20.41 |
| Src MAC | Cisco\_31:07:33 |
| Destination | 172.16.0.107 |
| Dest MAC | Dell\_c0:56:f0 |

|  |  |
| --- | --- |
| **arp\_poison: bad packet** | |
| Source | Hewlett\_bf:91:ee |
| Src MAC | Hewlett\_bf:91:ee |
| Destination | Dell\_c0:56:f0 |
| Dest MAC | Dell\_c0:56:f0 |

Describe the change in the communication pattern. What do you suppose this change might indicate about the attempted attack?

Instead of a communication between dell and cisco there is only communication between dell and Hewlett indicating that there is someone taking new control over the packet.