**LESSON 3 – NETWORK SECURITY**

**ACTIVITY 3.3.1 – ANALYZING ADDRESS RESOLUTION**

**Vocabulary:**

|  |  |
| --- | --- |
| Packet switched |  |
| MAC Address |  |
| ARP |  |
| ARP Poisoning |  |

**ANALYZING ARP TRAFFIC**

4. Expand the Frame entry in the Packet Details pane. Record some of the packet details. You will compare data in this packet with data in the other packet.

|  |
| --- |
| **arp\_resolution: Packet 1: Frame details** |
| Arrival Time: |  |
| Frame Length: |  |
| Protocols in Frame: |  |

5. Expand the Ethernet II entry in the Packet Details pane. Record the values for the following items:

|  |
| --- |
| **arp\_resolution: Packet 1: Ethernet details** |
| Source Address: |  |
| Destination Address: |  |

6. Expand the Address Resolution Protocol entry in the Packet Details pane. Record the values for the following items:

|  |
| --- |
| **arp\_resolution: Packet 1: Address Resolution Protocol details** |
| Protocol Type: |  |
| Opcode: |  |
| Sender (source) MAC Address: |  |
| Sender (source) IP Address: |  |
| Target (Destination) MAC Address: |  |
| Target (Destination) IP Address: |  |

**DETAILS OF AN ARP REPLY PACKET**

12. Once again, the Packet Details pane tells us more about the packet. If necessary, expand the Frame element in the Packet Details pane.

|  |
| --- |
| **arp\_resolution: Packet 2: Frame details** |
| Arrival Time: |  |
| Frame Length: |  |
| Protocols in Frame: |  |

14. If necessary, expand the Ethernet entry. Record the details.

|  |
| --- |
| **arp\_resolution: Packet 2: Ethernet details** |
| Source Address: |  |
| Destination Address: |  |

15. If necessary, expand the Address Resolution Protocol element in the Packet Details pane. Record the details.

|  |
| --- |
| **arp\_resolution: Packet 2: Address Resolution Protocol details** |
| Protocol Type: |  |
| Opcode: |  |
| Sender (source) MAC Address: |  |
| Sender (source) IP Address: |  |
| Target (Destination) MAC Address: |  |
| Target (Destination) IP Address: |  |

**GRATUITOUS ARP**

**PLTW COMPUTER SCIENCE NOTEBOOK**

Why might a malicious user fake or spoof an ARP broadcast packet?

|  |
| --- |
|  |

**ARP POISONING ATTACK**

29. Find the first ARP packet. (You can use an arp filter to simplify this.) In the Info column, “Who has 172.16.0.017? Tell 172.16.0.1” appears to be a broadcast message from your router. Record the following information using your new custom columns.

**THE FIRST ARP PACKET 54**

|  |
| --- |
| **arp\_poison** |
| Source: |  |
| Src MAC: |  |
| Destination |  |
| Dest MAC |  |

30. In the Packet Details pane, expand the Address Resolution Protocol element and record the following information. You only need to record the ASCII version of the MAC address (if provided).

|  |
| --- |
| **arp\_poison: ARP request** |
| Opcode: |  |
| Sender MAC Address: |  |
| Sender IP Address: |  |
| Target MAC Address: |  |
| Target IP Address: |  |

33. Find the ARP reply to this request. Record the following information in Packet Details.

**THE REPLY ARP PACKET 55.**

|  |
| --- |
| **arp\_poison: ARP request** |
| Opcode: |  |
| Sender MAC Address: |  |
| Sender IP Address: |  |
| Target MAC Address: |  |
| Target IP Address: |  |

34. Record the packet numbers for the ARP request and ARP reply.

|  |
| --- |
|  |

36. Scroll through the Packet List, looking for changes in communication patterns near the packets with the ARP poison attempt. Try to see a glitch or an anomaly (something unexpected).

|  |
| --- |
|  |

37. In the last packet before the glitch (the ARP messages) and in the first packet after the glitch, use Packet Details to record the information below and compare a valid (good) packet with your suspicious (bad) packet.

**THE LAST “GOOD” PACKET IS AT PACKET 52.**

|  |
| --- |
| **arp\_poison: good** |
| Source: |  |
| Src MAC: |  |
| Destination |  |
| Dest MAC |  |

**THE FIRST “BAD” PACKET IS AT PACKET 57.**

|  |
| --- |
| **arp\_poison: bad** |
| Source: |  |
| Src MAC: |  |
| Destination |  |
| Dest MAC |  |

**PLTW COMPUTER SCIENCE NOTEBOOK**

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

|  |
| --- |
|  |

**CONCLUSION**

What assumptions does ARP make that could result in system vulnerabilities?

|  |
| --- |
|  |

What are the effects of an ARP poisoning attack?

|  |
| --- |
|  |

How do you protect against an ARP poisoning exploit?

|  |
| --- |
|  |