# Cybersecurity

**Activity 3.3.3 Analyzing Packet Fragmentation**

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

#4

|  |  |  |  |
| --- | --- | --- | --- |
| ip\_fragmentation | | | |
|  | Packet 1 | Packet 2 | Packet 3 |
| Identification | 0x7474 | 0x7474 | 0x7474 |
| Flags | 0x01 | 0x01 | 0x00 |
| Fragment Offset | 0 | 1480 | 2960 |

#10 Table

Description automatically generated with medium confidenceFind the first fragmented packet in the Packet List. You can scroll to do this or use the Find Packet tool. Packet 8

#11

|  |  |
| --- | --- |
| teardrop | |
| Identification | 0x00f2 |
| Fragment Offset | 0 |
| Flags | 0x01 |
| Data (Length in bytes) | 36 bytes |

#12

|  |  |
| --- | --- |
| teardrop | |
| Identification | 0x00f2 |
| Fragment Offset | 24 |
| Flags | 0x00 |
| Data (Length in bytes) | 20 bytes |

How can Wireshark data visualizations help you in your analysis? Spikes in graph mean lots of packet activity.

Conclusion

1. What assumptions does IPv4 packet fragmentation make that could result in system

vulnerabilities? The computer will continue reading the information.

1. What are the effects of a packet fragmentation (Teardrop) attack? Confusion in packet reading
2. How do you protect against a packet fragmentation exploit? Install malware detection methods, list of untrusted sources, or watch packet rate.