1. **Detection**: Describe the type of traffic you analyzed, including whether or not it was an attack.
2. **Response**: Describe how you concluded this was normal or malicious/attack traffic.
3. **Recovery**: Describe how the exploit could affect the system, specifically the function of each host/network node.
4. **Identify**: List the hosts involved (IP address, MAC address), date/time of the incident, and note the attacker and victim if applicable.
5. **Protect**: If malicious, provide your recommended mitigation.
6. **Lesson** Learned: Discuss new insights into your analysis process.

|  |  |
| --- | --- |
| **File 1** | |
| **Detection** | This traffic is suspicious ARP traffic, specifically, it appears to be an attempt of ARP poisoning |
| **Response** | ICMP traffic is normal but 10.2.0.4 becomes unreachable. Lots of ARP traffic indicated ARP poisoning. Hosts have same MAC address. |
| **Recovery** | ARP attack corrupts cache/tables |
| **Identify** | 10.2.0.1, 10.2.0.2, 10.2.0.3, 10.2.0.5 – one is an attacker and rest were attacked. 10.2.0.3 is the attacker |
| **Protect** | Create a static ARP entry on the server for permanent entry |
| **Lesson** | Learned in depth knowledge on ARP packet reading |

|  |  |
| --- | --- |
| **File 2** | |
| **Detection** | IPv4 and TCP are normal |
| **Response** | Fragmented IP with a response immediately after with the same sources |
| **Recovery** | N/A |
| **Identify** | N/A |
| **Protect** | N/A |
| **Lesson** | There is nothing unusual about the packet which indicates there is no issue with host send and response |

|  |  |
| --- | --- |
| **File 3** | |
| **Detection** | TCP and ICMP have normal traffic |
| **Response** | There is no spamming of traffic from ICMP |
| **Recovery** | N/A |
| **Identify** | N/A |
| **Protect** | N/A |
| **Lesson** | Spikes on the I/O Graph does not mean a smurf attack |

|  |  |
| --- | --- |
| **File 4** | |
| **Detection** | ARP and ICMP is normal |
| **Response** | Since there is no overload of ARP or ICMP packets there is no issue |
| **Recovery** | N/A |
| **Identify** | N/A |
| **Protect** | N/A |
| **Lesson** | Spikes on the I/O Graph does not mean a smurf attack |

|  |  |
| --- | --- |
| **File 5** | |
| **Detection** | Lots of ICMP packets are flooded into the host |
| **Response** | ICMP traffic is not normal rate and much faster |
| **Recovery** | It spoofs the source address that hosts reply to it |
| **Identify** | 192.168.253.254, 192.168.255.255, 10.2.0.3, 10.2.0.1 –others were victims and attackers are 192.168.253.254 and 192.168.255.255 |
| **Protect** | Configure firewall to drop ICMP packets |
| **Lesson** | Lots of packets can be sent in a matter of seconds |