Timbershade Post-Incident Report

|  |  |
| --- | --- |
| What activity is snort reporting on? | DHCP/NBNS traffic |
| What is the date and time of this alert? | January 28th, 2019 on 9:44 PM |
| What is the external IP address that snort is flagging for malicious activity? | 255.255.255.255 |
| What is the internal IP address that snort is flagging for malicious activity? | 172.17.8.109 |
| What is the source port of the activity? | 68 |
| What is the destination port of the activity? | 67 |
| What are the MAC Addresses of the computers involved? | 14:fe:b5:d4:15:ca (Dell\_d4:15:ca |
| What is the host name of the internal machine? | Dunn-Windows-PC |
| Can you confirm the date and time this issue occurred? | Yes |
| How can you confirm if the snort alert is accurate? | By running a TCP. |
| Can you safely verify whether or not malware was downloaded? | Yes |
| Would you categorize this alert as a False Positive or a True Positive? | False Positive |
| If this issue needs to be mitigated, what steps should be taken with the infected machine? | Filtering packets |
| What steps should be taken in regard to network security? | Default steps to network traffic blocking |
| Would you categorize this issue as a Web, Email or Network attack? | Network attack |

Narrative





