Team lab 5: snort rules

Technology, Information Technology

Team Lab 5: Snort Rules Snort Sniffer Mode Meaning of command options snort –d –e -v –i 2 snort -v The snort command means thatthe sniffer mode will only print the TCP/ICMP/UDP headers and the IP headers for the user to see.

Snort -d -v

The Snort command instruct snort to display all the headers and the packet data being transported.

Snort -v -d -e

The command will show a lot of details that include TCP/ICMP/UDP headers, packet data being transported, and it also shows the data link layer or layer two headers.

Snort -v -d -e -i -2

The command means snort is displaying all the packets and headers from the -v-d-e option while listening on interface 2.

The screen-shot above shows two sections of the snort sniffer mode output. The first section of the output shows packets sent to the victim IP address(192: 168: 0. 11) from the attacker Ip address (192. 168. 0. 131).

04/16-17: 45: 00. 079555 0: 50: 56: 9E: 4: BF → 0: 50: 56: 9E: 6F: 1C type: 0x800 len: 0x4A

The line above is the first line of the output and displays the date and time the output was produced or when the packet was being sent from the attacker to the victim. The packets were captured on 16 April at around 17: 45 pm. The first line then shows the source and destination mac address of the attacker and victim. Type: 0x800 indicates that the connection is done over the IPv4 Internet protocol and define the length of the header that is being displayed.

The second line shows the source and destination IP address as 192. 168. 0. 11 and 192. 168. 0. 131 respectively. ICMP represents the header packet of the Internet control message protocol. TTL: 128 represents the time the packet is allowed to live, and the packet is allowed to travel through 128 loops before being dropped. ID: 74 represents theIPID for the source of the packet. IpLen: 20 represents the length of each IP address that is being used or being displayed by the snort. DgmLen: 60 defines the length of the captured packets. ID: 512 represents the destination IP ID. Seg: 1024 refers to the number of the maximum targets. ECHO refers to a packet request from the attacker being sent to the victim.

The next lines with the following contain the actual message being sent by the attacker.

61 62 63 …… 6F 70

71 72 73……… 68 69

The second section contains the output information where the victim has sent back packets in response to the request sent by the victim. The first line also contains the time, date details Mac addresses of the two machines and the Type: 0x800 indicates that the connection is over IPv4. The output then shows the IP addresses where the packet originates. The IP address is 192. 168. 0. 131, and the destination IP address is 192. 168. 0. 11. This means that the packet is a reply to the initial request that had been sent by the attacker. Therefore, the source this time is the victim, and the attacker is the destination of the packets.

The output information also contains the ID that is assigned when the packet is being transferred. The segment number seg: 1024 refers to the number of maximum targets. The packet also contains ECHO REPLY; that refers to the packet that is a reply to a request that had been sent by 192. 168. 0. 11 (attacker).

The next line represents the encoded message being sent as a reply to the packet request The message is decoded and contains alphabetical letters.

Stopping Snort will reveal that the there was a ping from 192. 168. 0. 1 to 192. 168. 0. 131.

Reference

The Snort Project, (2014). SNORT User Manual 2. 9. 7. Cisco.