### Text Description automatically generatedTask 8:

Figure 36 The rules was added into the local.rules file

NMAP PORT SCAN:

The plug-in used for this task is the detection plugins which is the flags detection in the snort rules (flags).

The Snort rule is alert tcp any any -> 192.168.56.101 any (msg: “NMAP PORT SCAN”;flags:S;sid:1000004;rev:2;). Flags: S has been added to detected the SYN in the packet when the packet is sent from the host machine to server from during the port scan. The rule has been added into local.rules file. The result is shown in figure 37.

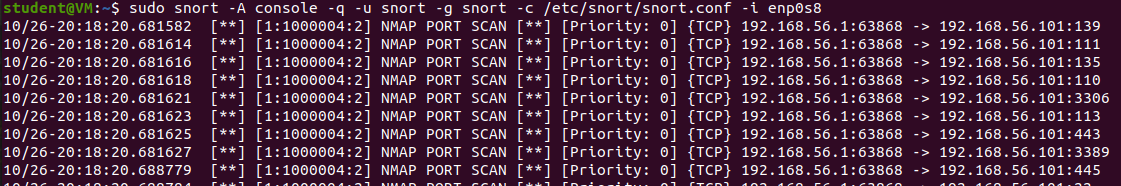


Figure 37 Result of PORT SCAN NMAP detection

NMAP IP SCAN:

The plug in used for nmap ip scan is itype which is part of detection plugin for the types of IMCP packet

The Snort rule is alert icmp any any -> 192.168.1.105 any (msg: "NMAP IP Scan"; itype:8; dsize:0;sid:10000004; rev: 1;). The itype is added with value 8. This is to detect the Echo Request from the ICMP packet (from the host discovery of NMAP). Dsize is also added to determine the unusual packet payload size (verify if the packet has 0 payload). According to figure 38, the IP Scan has detected successfully with the packet.

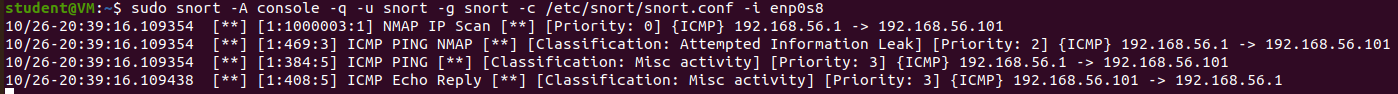


Figure 38 Result of Snort alert against nmap ip scan