**Experiment 9**

**Date of Performance :**  **Date of Submission:**

**SAP Id: 60004190057** **Name : Junaid Altaf Girkar**

**Div:** **A** **Batch : A4**

**Aim of Experiment**

Implementation of Network Intrusion Detection System using NMAP, SNORT and IPTABLE (CO6).

**Theory:**

**IPTables:**

iptables is a user-space utility program that allows a system administrator to configure the IP packet filter rules of the Linux kernel firewall, implemented as different Netfilter modules. The filters are organized in different tables, which contain chains of rules for how to treat network traffic packets. Different kernel modules and programs are currently used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

**NMAP:**

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks. Nmap can be used to monitor single hosts as well as vast networks that encompass hundreds of thousands of devices and multitudes of subnets.

| **C:\Users\junai>nmap 10.120.63.29 -O -sV -p 20-25 -Pn Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 00:35 India Standard Time Nmap scan report for 10.120.63.29 Host is up.  PORT STATE SERVICE VERSION 20/tcp filtered ftp-data 21/tcp filtered ftp 22/tcp filtered ssh 23/tcp filtered telnet 24/tcp filtered priv-mail 25/tcp filtered smtp Too many fingerprints match this host to give specific OS details  OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds** |
| --- |

| **C:\Users\junai>nmap 10.120.63.29 10.120.63.28 -sL Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 00:36 India Standard Time Nmap scan report for 10.120.63.29 Nmap scan report for 10.120.63.28 Nmap done: 2 IP addresses (0 hosts up) scanned in 0.10 seconds** |
| --- |

| **C:\Users\junai>nmap 10.120.63.29 -p 21,22,23,25,80 -Pn Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 00:37 India Standard Time Nmap scan report for 10.120.63.29 Host is up.  PORT STATE SERVICE 21/tcp filtered ftp 22/tcp filtered ssh 23/tcp filtered telnet 25/tcp filtered smtp 80/tcp filtered http  Nmap done: 1 IP address (1 host up) scanned in 3.39 seconds** |
| --- |

**SNORT:**

Snort is a free and open-source network intrusion prevention and detection system.

It uses a rule-based language combining signature, protocol, and anomaly inspection

methods to detect malicious activity such as denial-of-service (DoS) attacks, Buffer

overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

It is capable of performing real-time traffic analysis and packet logging on IP networks.

**IP Protocols supported by SNORT:**

As we know, IP is a unique address for every computer and is used for transferring data or packets over the internet from one network to the other network. Each packet contains a message, data, source, destination address, and much more. Snort supports three IP protocols for suspicious behavior:

● Transmission Control Protocol (TCP) Connects two different hosts and exchanges data between them. Examples include HTTP, SMTP, and FTP.

● User Datagram Protocol (UDP): Broadcasts messages over the internet. Examples include DNS traffic.

● Internet Control Message Protocol (ICMP): Sends network error messages in Windows. Examples include Ping and Traceroute.

**Snort Rules:**

Rules are a different methodology for performing detection, which bring the advantage of 0-day detection to the table. Developing a rule requires an acute understanding of how the vulnerability actually works. Snort generates alerts according to the rules defined in the configuration file. The Snort rule language is very flexible, and creation of new rules is relatively simple. Snort rules help in differentiating between normal internet activities and malicious activities

**ICMP Intrusion Detection:**

| **C:\Snort\bin>snort -c C:\Snort\etc\snort.conf -l C:\Snort\log -i2 -T Running in Test mode   --== Initializing Snort ==-- Initializing Output Plugins! Initializing Preprocessors! Initializing Plug-ins! Parsing Rules file "C:\Snort\etc\snort.conf" PortVar 'HTTP\_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ] PortVar 'SHELLCODE\_PORTS' defined : [ 0:79 81:65535 ] PortVar 'ORACLE\_PORTS' defined : [ 1024:65535 ] PortVar 'SSH\_PORTS' defined : [ 22 ] PortVar 'FTP\_PORTS' defined : [ 21 2100 3535 ] PortVar 'SIP\_PORTS' defined : [ 5060:5061 5600 ] PortVar 'FILE\_DATA\_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ] PortVar 'GTP\_PORTS' defined : [ 2123 2152 3386 ] Detection:  Search-Method = AC-Full-Q  Split Any/Any group = enabled  Search-Method-Optimizations = enabled  Maximum pattern length = 20** |
| --- |

**CONCLUSION**

Thus, we have successfully implemented a Network Intrusion Detection System using NMAP, SNORT and IPTables.