# EXPERIMENT NO 07

CLASS: TE CMPN A PID: 182027

NAME: REBECCA DIAS ROLL NO. : 19

**Aim:**

a. Set up IPSEC under LINUX.

b. Set up Snort and study the logs.

**Theory:**

**a) What is IPSec?**

* In [computing](https://en.wikipedia.org/wiki/Computing), Internet Protocol Security (IPsec) is a secure network [protocol suite](https://en.wikipedia.org/wiki/Protocol_suite) that [authenticates](https://en.wikipedia.org/wiki/Authentication) and [encrypts](https://en.wikipedia.org/wiki/Encryption) the [packets](https://en.wikipedia.org/wiki/Packet_(information_technology)) of data to provide secure encrypted communication between two computers over an [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) network. It is used in [virtual private networks](https://en.wikipedia.org/wiki/Virtual_private_network) (VPNs).
* IPsec includes protocols for establishing [mutual authentication](https://en.wikipedia.org/wiki/Mutual_authentication) between agents at the beginning of a session and negotiation of [cryptographic keys](https://en.wikipedia.org/wiki/Key_(cryptography)) to use during the session.
* IPsec can protect data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).
* IPsec uses cryptographic security services to protect communications over [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) networks. It supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

**b) Uses of IPSec**

* **Key exchange:** [Keys](https://www.cloudflare.com/learning/ssl/what-is-a-cryptographic-key/) are necessary for encryption; a key is a string of random characters that can be used to "lock" (encrypt) and "unlock" (decrypt) messages. IPsec sets up keys with a key exchange between the connected devices, so that each device can decrypt the other device's messages.
* **Packet headers and trailers:** All data that is sent over a network is broken down into smaller pieces called packets. Packets contain both a payload, or the actual data being sent, and headers, or information about that data so that computers receiving the packets know what to do with them. IPsec adds several headers to data packets containing authentication and encryption information. IPsec also adds trailers, which go after each packet's payload instead of before.
* **Authentication:** IPsec provides authentication for each packet, like a stamp of authenticity on a collectible item. This ensures that packets are from a trusted source and not an attacker.
* **Encryption:** IPsec encrypts the payloads within each packet and each packet's IP header (unless transport mode is used instead of tunnel mode — see below). This keeps data sent over IPsec secure and private.
* **Transmission:** Encrypted IPsec packets travel across one or more networks to their destination using a transport protocol. At this stage, IPsec traffic differs from regular IP traffic in that it most often uses [UDP](https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/) as its transport protocol, rather than [TCP](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/). TCP, the Transmission Control Protocol, sets up dedicated connections between devices and ensures that all packets arrive. UDP, the User Datagram Protocol, does not set up these dedicated connections. IPsec uses UDP because this allows IPsec packets to get through [firewalls](https://www.cloudflare.com/learning/security/what-is-a-firewall/).
* **Decryption:** At the other end of the communication, the packets are decrypted, and applications (e.g. a browser) can now use the delivered data.

**c) Protocols used in IPSec**

In [networking](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/), a protocol is a specified way of formatting data so that any networked computer can interpret the data. IPsec is not one protocol, but a suite of protocols. The following protocols make up the IPsec suite:

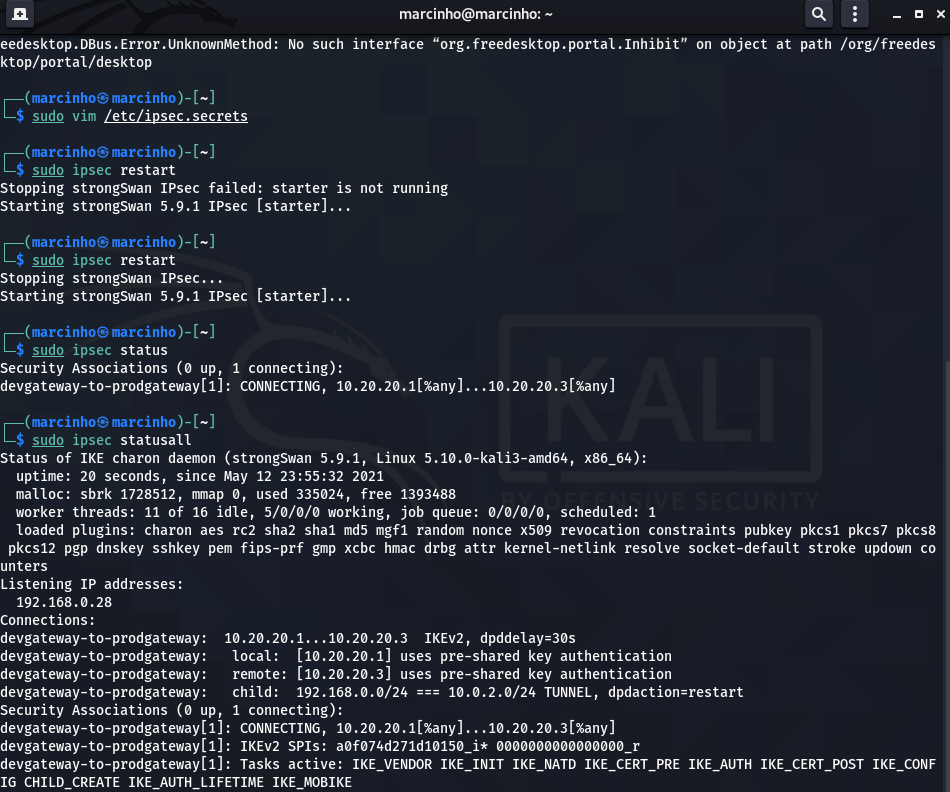
* **Authentication Header (AH)**: The AH protocol ensures that data packets are from a trusted source and that the data has not been tampered with, like a tamper-proof seal on a consumer product. These headers do not provide any encryption; they do not help conceal the data from attackers.
* **Encapsulating Security Protocol (ESP)**: ESP encrypts the IP header and the payload for each packet — unless transport mode is used, in which case it only encrypts the payload. ESP adds its own header and a trailer to each data packet.
* **Security Association (SA)**: SA refers to a number of protocols used for negotiating encryption keys and algorithms. One of the most common SA protocols is Internet Key Exchange (IKE).

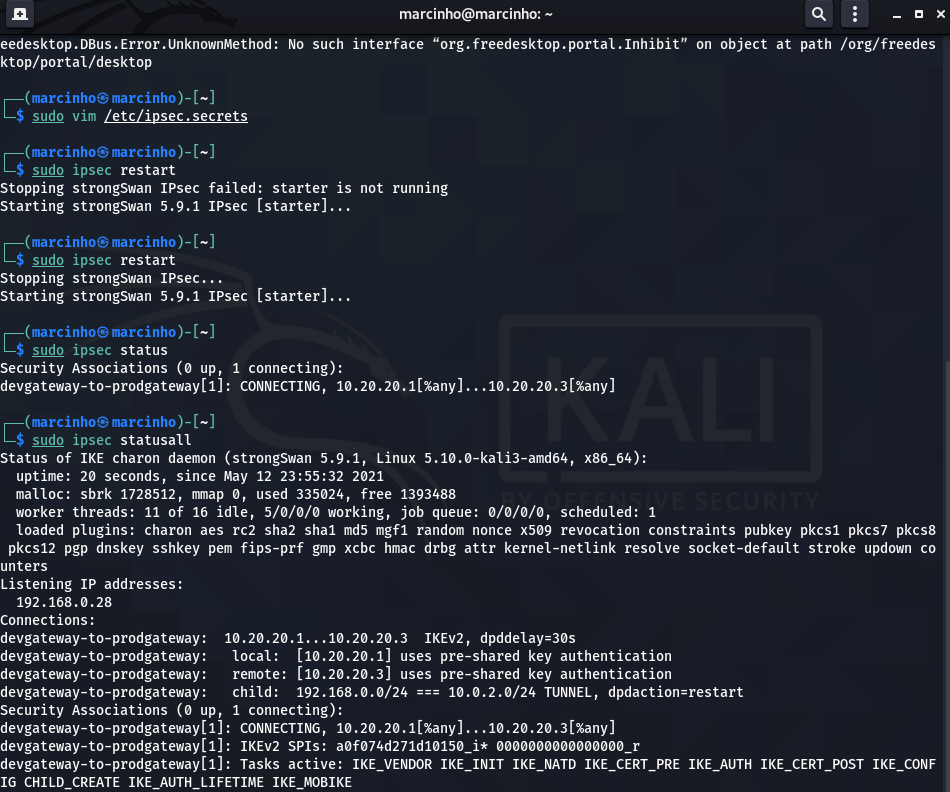
Finally, while the Internet Protocol (IP) is not part of the IPsec suite, IPsec runs directly on top of IP.

**d) Install IPSec in Linux and take screenshot of each step**









**e) What is IDS**

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a [security information and event management (SIEM)](https://en.wikipedia.org/wiki/Security_information_and_event_management) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

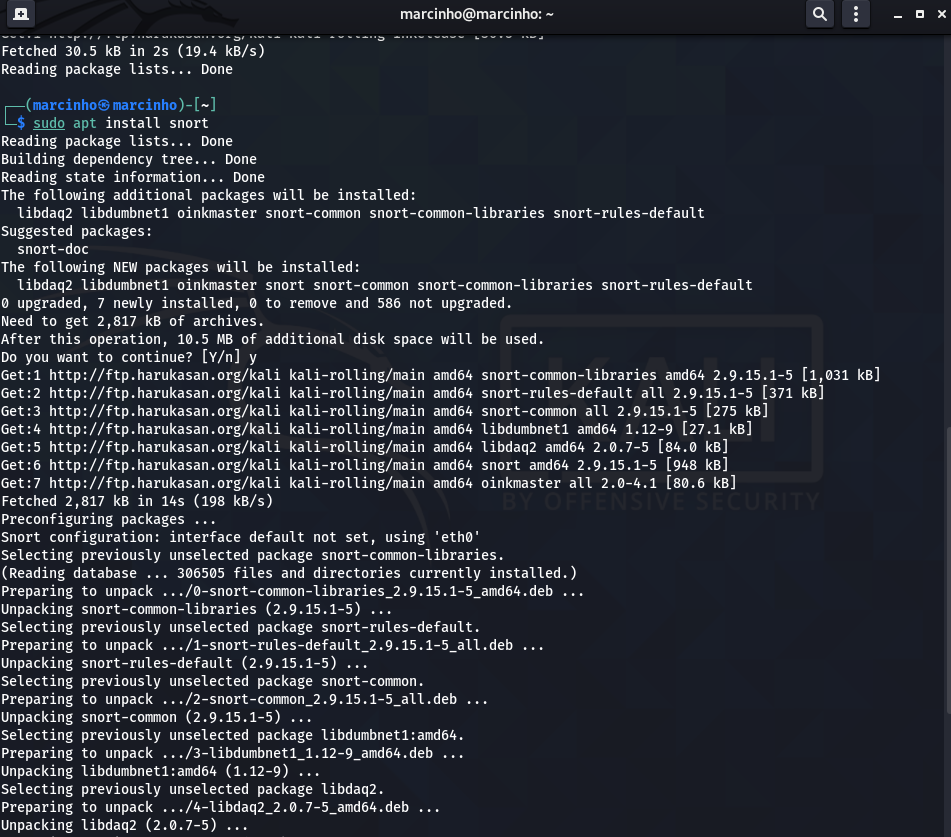
**f) What is SNORT tool**

* Snort is an [open source](https://whatis.techtarget.com/definition/open-source) network [intrusion detection](https://searchsecurity.techtarget.com/definition/intrusion-detection-system) system (NIDS) created by Martin Roesch. Snort is a [packet](https://searchnetworking.techtarget.com/definition/packet) [sniffer](https://searchnetworking.techtarget.com/definition/sniffer) that monitors network traffic in [real time](https://whatis.techtarget.com/definition/real-time), scrutinizing each [packet](https://searchnetworking.techtarget.com/definition/packet) closely to detect a dangerous [payload](https://searchsecurity.techtarget.com/definition/payload) or suspicious anomalies.
* Snort is based on *libpcap* (for library packet capture), a tool that is widely used in [TCP/IP](https://searchnetworking.techtarget.com/definition/TCP-IP) traffic [sniffer](https://searchnetworking.techtarget.com/definition/sniffer)s and analyzers. Through [protocol](https://searchnetworking.techtarget.com/definition/protocol) analysis and content searching and matching, Snort detects attack methods, including [denial of service](https://searchsecurity.techtarget.com/definition/denial-of-service), [buffer overflow](https://searchsecurity.techtarget.com/definition/buffer-overflow), [CGI](https://whatis.techtarget.com/definition/common-gateway-interface-CGI) attacks, [stealth](https://searchsecurity.techtarget.com/definition/stealth) [port](https://searchnetworking.techtarget.com/definition/port) scans, and SMB [probe](https://searchsecurity.techtarget.com/definition/probe)s. When suspicious behavior is detected, Snort sends a real-time alert to *syslog*, a separate 'alerts' file, or to a [pop-up](https://whatis.techtarget.com/definition/pop-up) window.

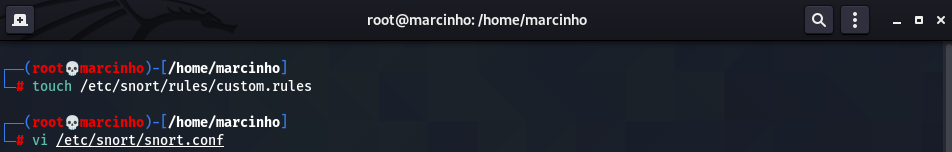
**g) Why it is used**

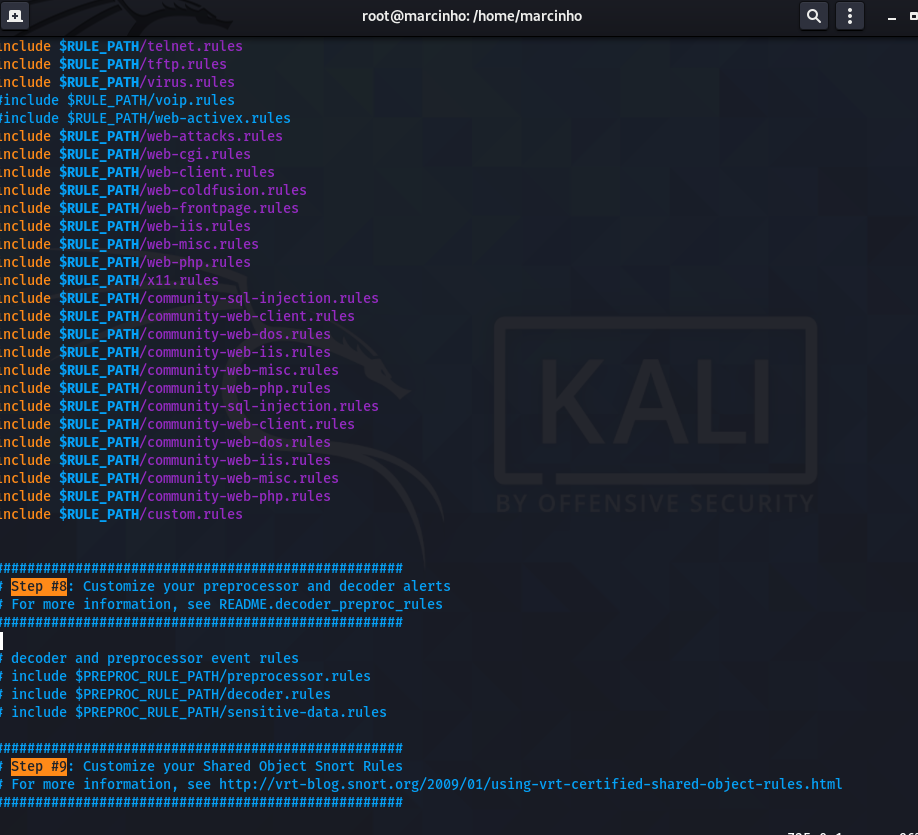
Snort performs protocol analysis, content searching and matching. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans.

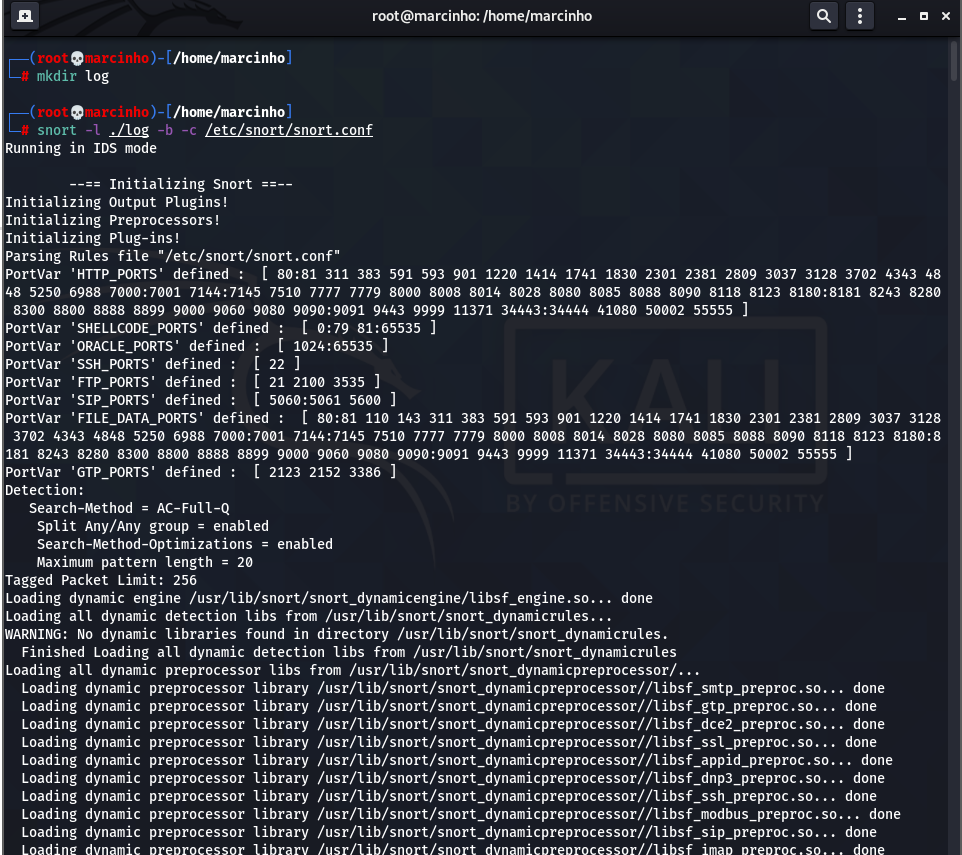
**h) Install SNORT on Linux and take screenshot of each step**

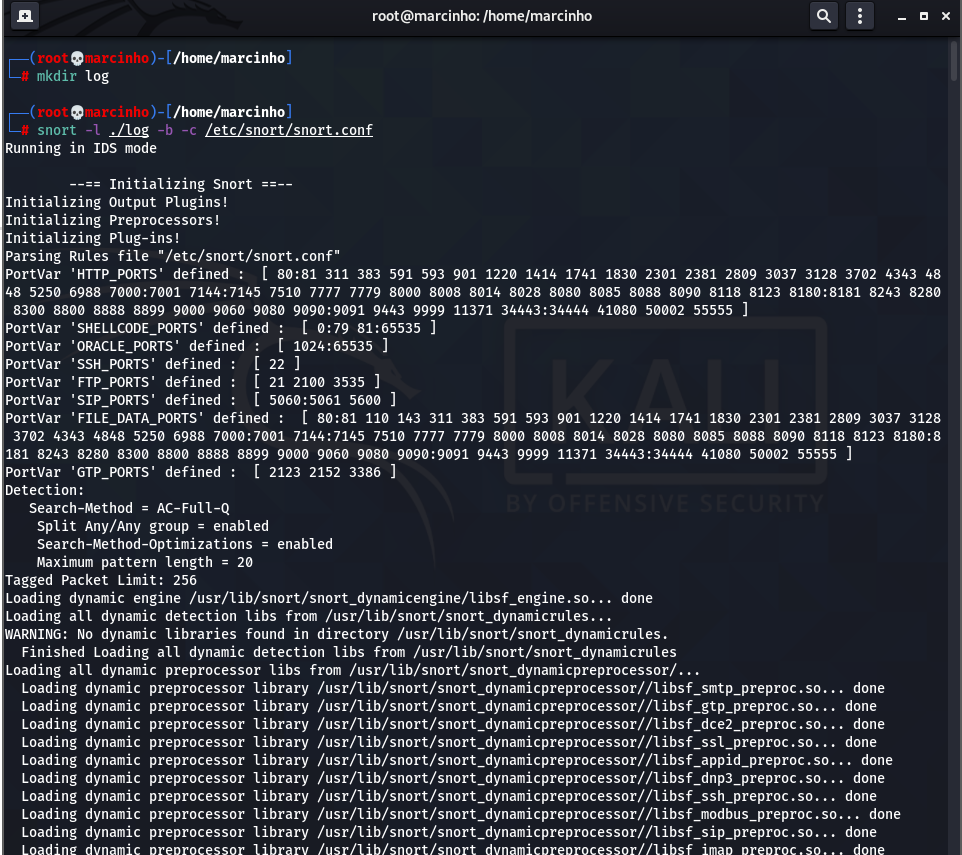


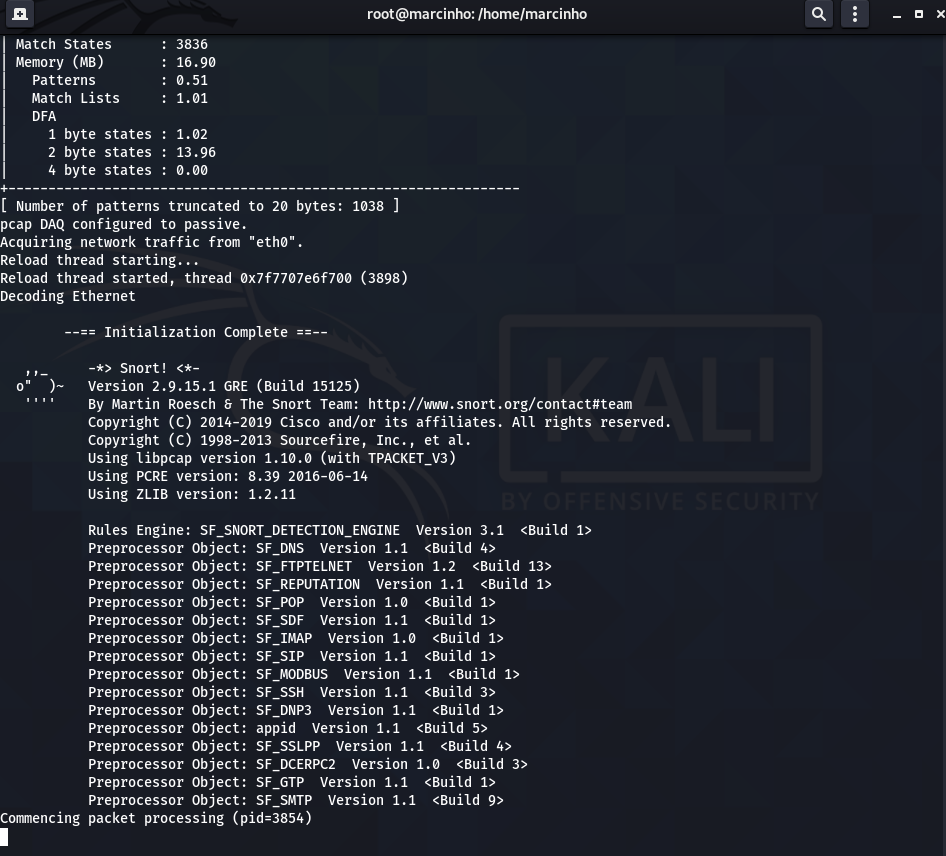


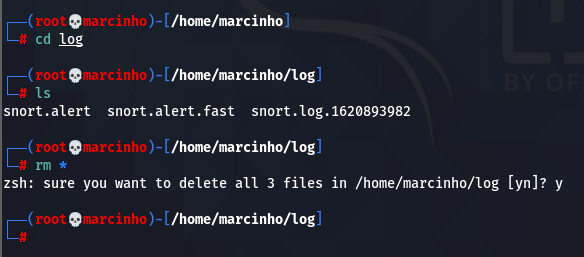


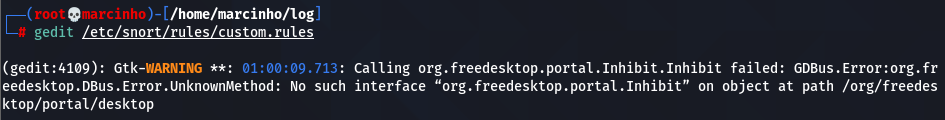


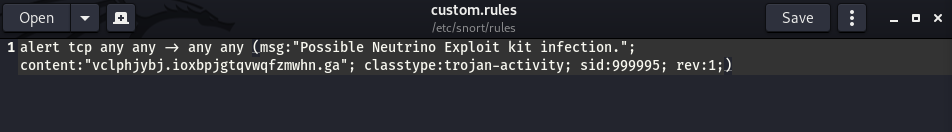


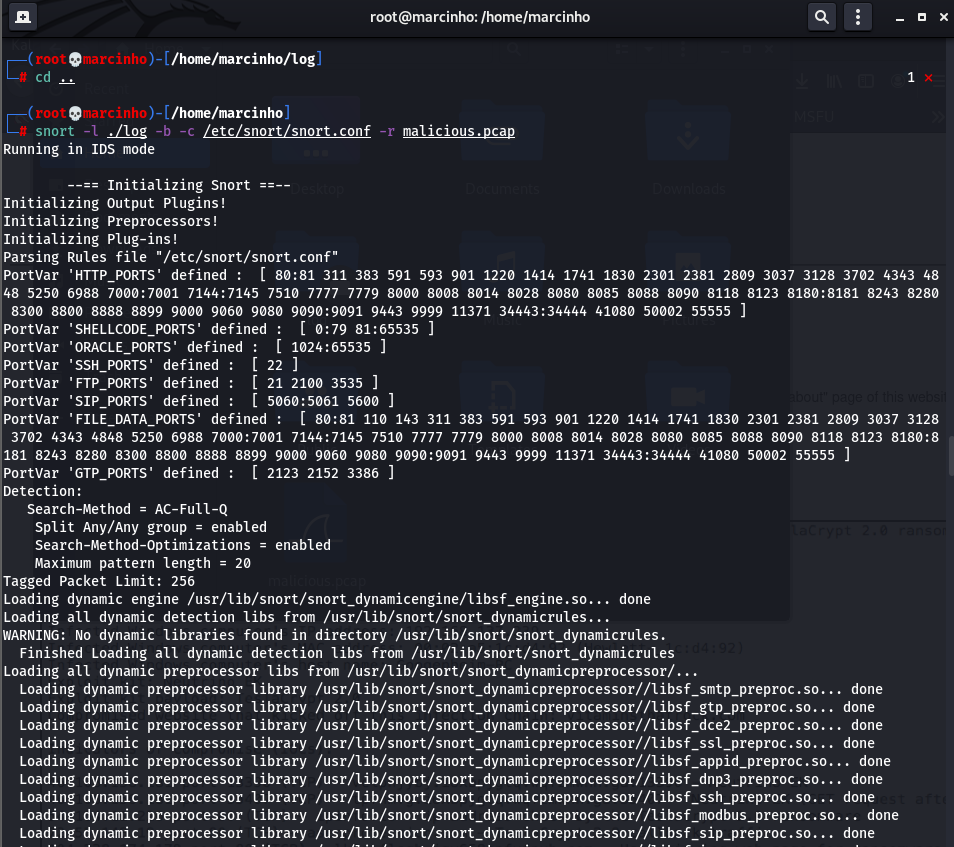


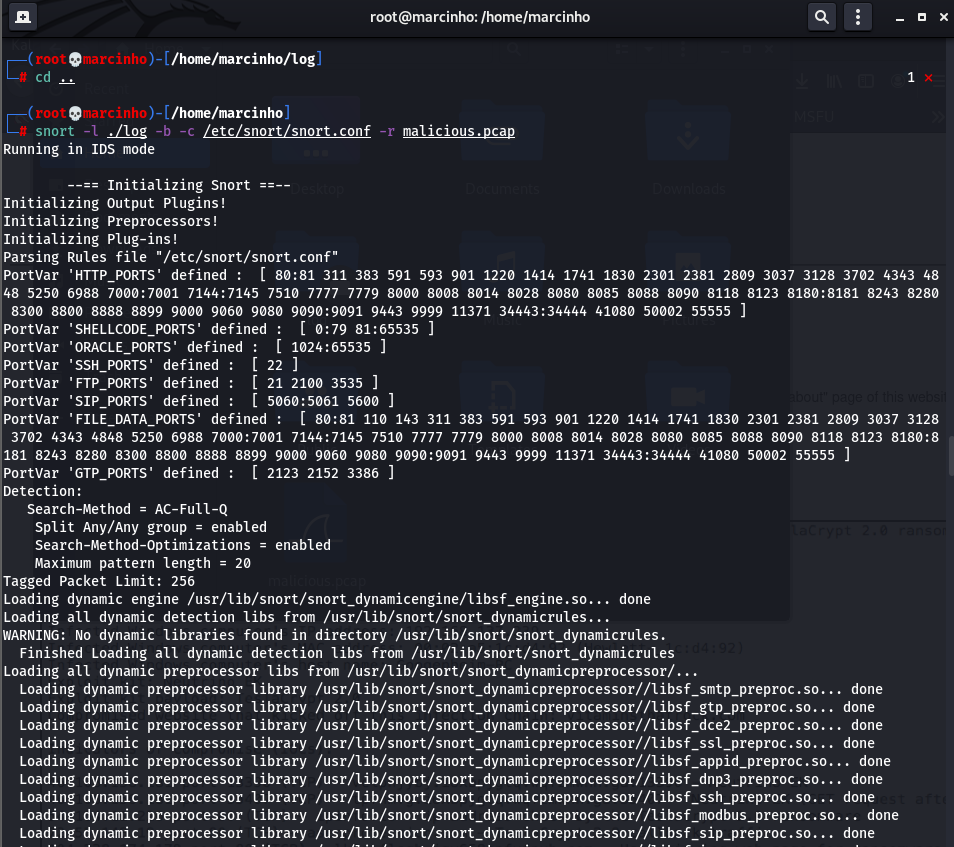




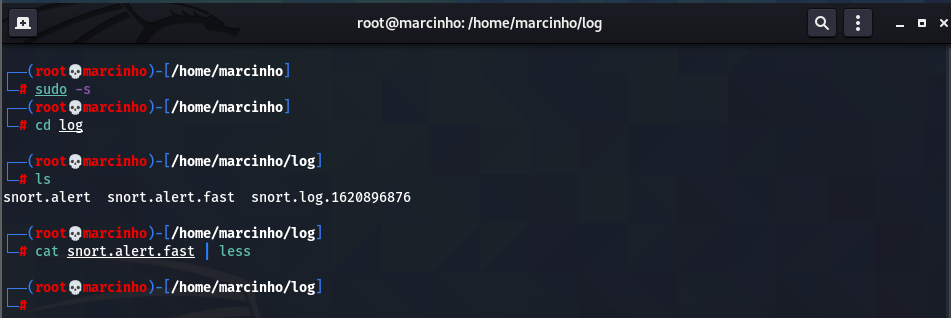


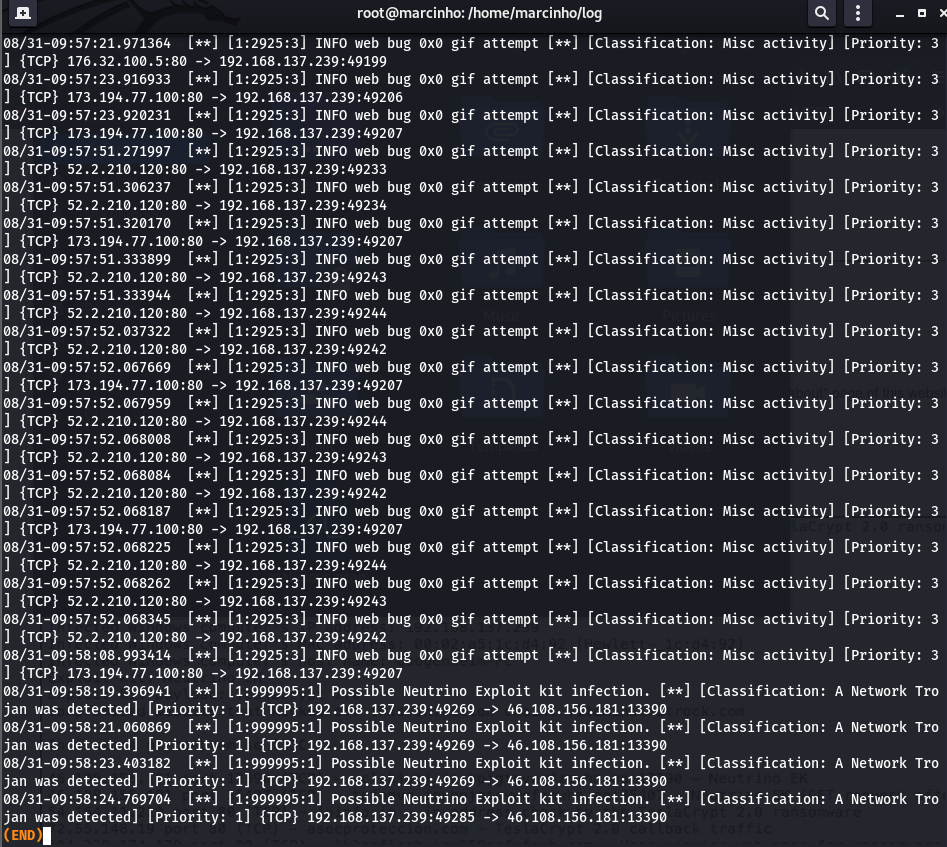


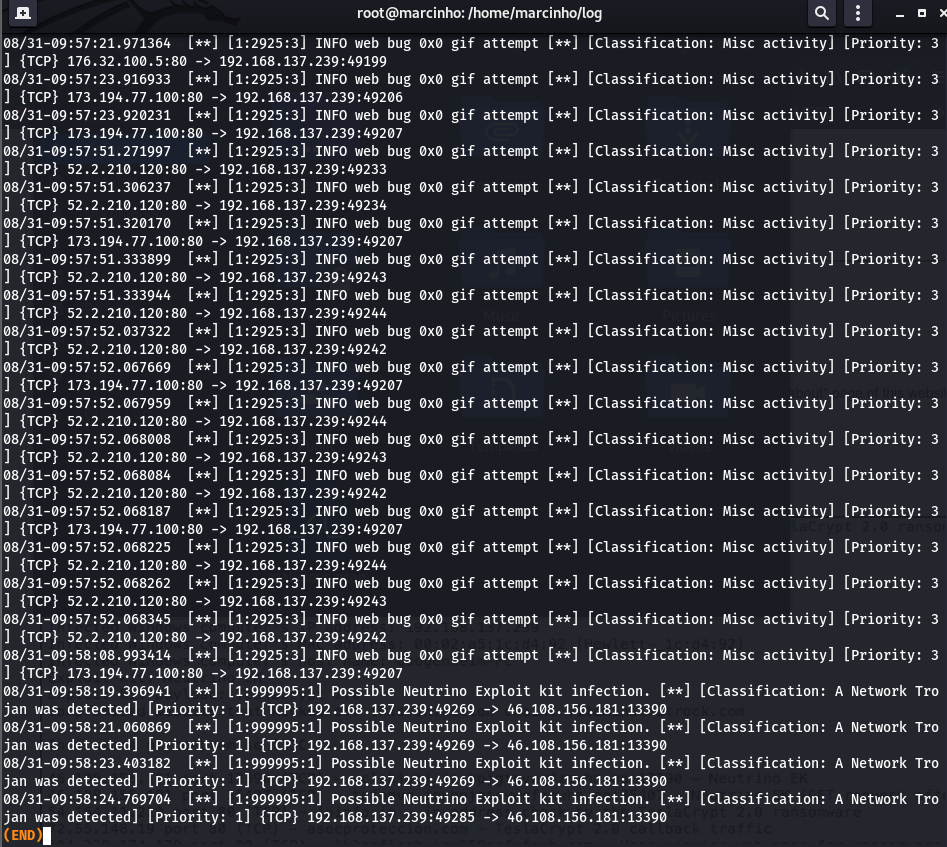


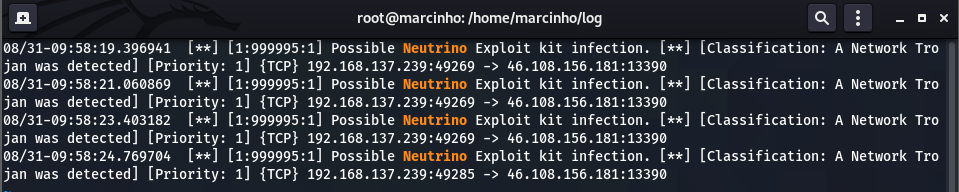


**i) Study logs of each step**









**Conclusion:**

In this experiment we learnt to install IPSEC and set up a VPN. We learnt about its components and all its features and set up a Site to Site IPSec VPN with Strongswan. We also learnt to install snort and use it to alert users about malicious packets and alert the user. We also learnt how to analyze the logs produced after running snort.