**Day 45**

**Exploitation Analyst**

**Firewalls and TCP wrappers:**

**TCP Wrappers:**

**What are TCP Wrappers?**

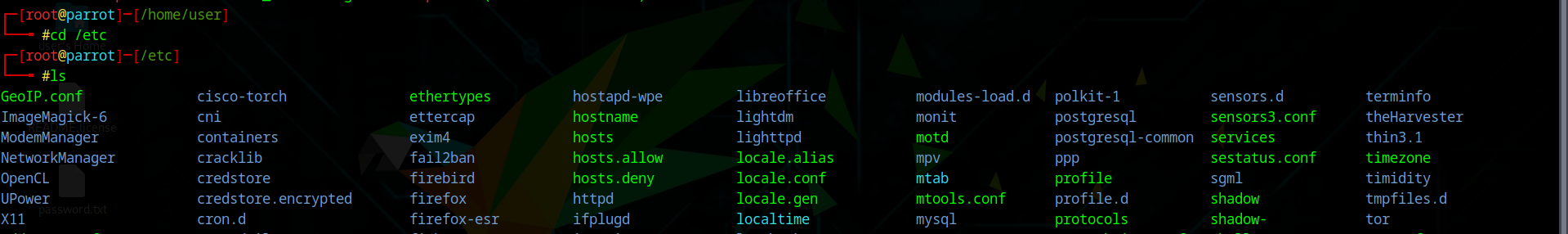
TCP Wrappers are an old security tool for Linux/Unix that control access to network services. They work by checking two config files — /etc/hosts.allow and /etc/hosts.deny — before letting a client connect.

* If a client’s IP matches hosts.allow, access is granted.
* If it matches hosts.deny, access is blocked.
* If no rule matches, the default is to allow.

They were commonly used to restrict services like SSH, FTP, or telnet. Today, they’re mostly replaced by firewalls (iptables/nftables) and Fail2ban, which are more powerful.

**TCP Wrappers work at the application layer, before the service fully accepts the connection, so it’s fast and simple.**

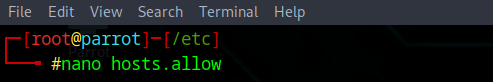
**Where are those two files?** In the /etc folder.

****

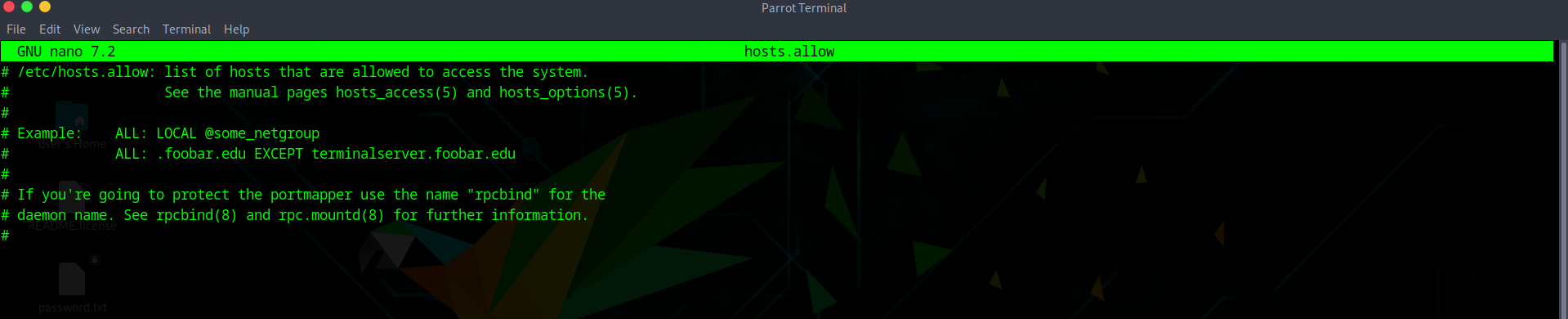
**Exploring TCP Wrappers:**

Steps:

Open the hosts.allow: Edit /etc/hosts.allow (allowed IPs)



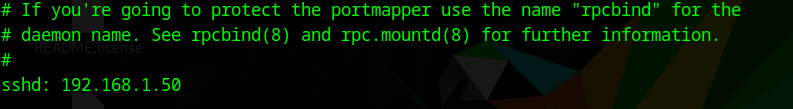
Following screen will appear:

****

This is the default content of /etc/hosts.allow, which is the configuration file used by TCP Wrappers to define which hosts or networks are allowed to access services on the system. It includes comments explaining syntax and giving examples, such as allowing all local connections (ALL: LOCAL) or permitting specific networks while excluding certain hosts. Essentially, it’s a template showing how to write rules that control access to daemons before connections are accepted.

Add a line:

sshd: 192.168.1.50

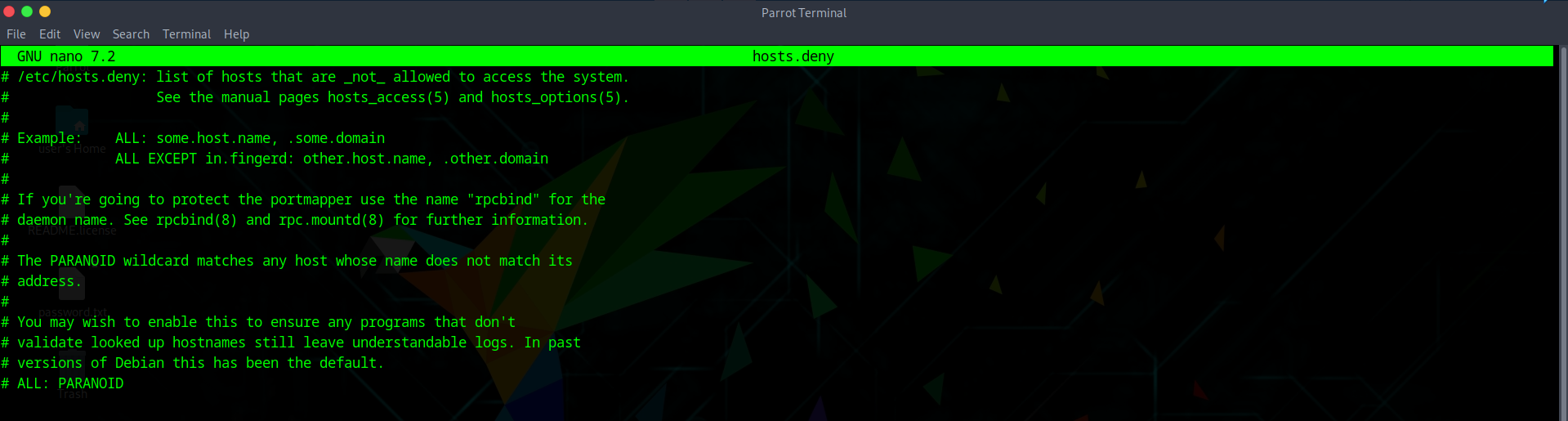


This allows SSH connections only from 192.168.1.50.

Edit /etc/hosts.deny (blocked IPs):

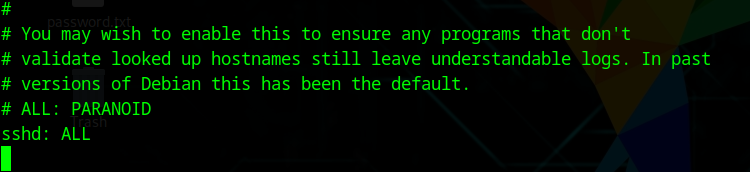


Following screen will appear:



Add a line:

sshd: ALL



This denies SSH connections from all other IPs not explicitly allowed.

--The End-