

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.

```
[root@parrot ~]# cd /etc
[root@parrot ~]# cd /etc
[root@parrot ~]# ls
GeoIP.conf  cisco-torch  ethtypes     hostapd-wpe  libreoffice  modules-load.d  polkit-1  sensors.d  terminfo
ImageMagick-6  cni          ettercap     hostname     lightdm      monit           postgresql  sensors3.conf  theHarvester
ModemManager  containers   exim4        hosts        lighttpd     motd            postgresql-common  services      thin3.1
NetworkManager  cracklib    fail2ban     hosts.allow  locale.alias  mpv             ppp        sestatus.conf  timezone
OpenCL         credstore   firebird     hosts.deny   locale.conf  mtab            profile    sgml          timidity
UPower        credstore.encrypted  firefox      httpd        locale.gen   mtools.conf     profile.d  shadow       tmpfiles.d
VLL           cron.d      firefox-esr  ifplugd      localtime   mysql            protocols  shadow-      tor
```

Exploring TCP Wrappers:

Steps:

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

```
File Edit View Search Terminal Help
[root@parrot ~]# nano /etc/hosts.allow
#nano hosts.allow
```

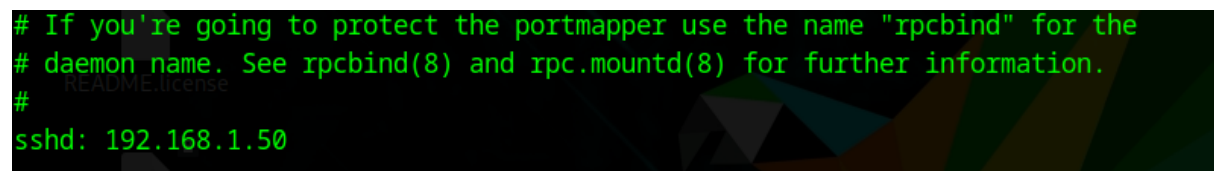
Following screen will appear:

```
GNU nano 7.2 hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:
# ALL: LOCAL @some_netgroup
# ALL: .foofoo.edu EXCEPT terminalserver.foofoo.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
```

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:

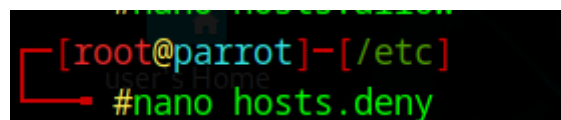
```
sshd: 192.168.1.50
```



```
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
sshd: 192.168.1.50
```

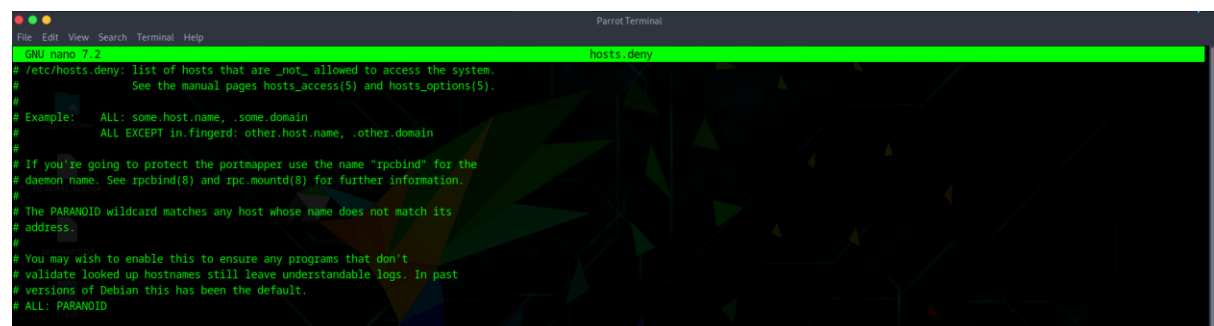
This allows SSH connections only from 192.168.1.50.

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



```
[root@parrot]-[/etc]
#nano hosts.deny
```

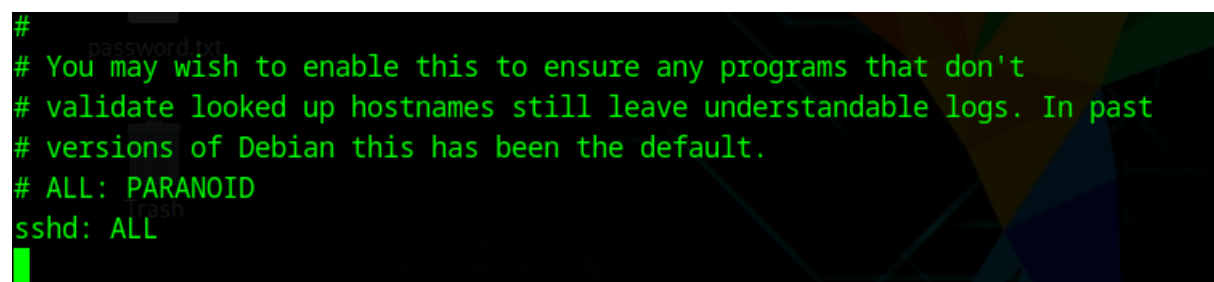
Following screen will appear:



```
GNU nano 7.2 hosts.deny
/etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:  ALL: some.host.name, .some.domain
#          ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
```

Add a line:

```
sshd: ALL
```



```
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
sshd: ALL
```

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

--The End--