**Project Name:** Securing Debian Services Against Brute-Force Attacks Using Firewall Rules
**Author:** Akash R
**Date:** 21 August 2025

## 1. Objective

The goal of this project was to simulate a real-world penetration testing scenario by configuring a Debian firewall, allowing specific services, performing reconnaissance and attacks from Kali Linux, and then hardening the firewall and SSH services to prevent further attacks. This demonstrates both **security vulnerabilities** and **remediation techniques**.

## 2. Environment Setup

- **Target Machine:** Debian 13
  - Configured as a firewall
  - Services allowed: HTTP (80), HTTPS (443), SSH (22 initially, later hardened to 2222), ICMP (ping)
- **Attacker Machine:** Kali Linux
  - Used for scanning, enumeration, and brute-force testing
- **Tools Used:**
  - **iptables** → firewall configuration
  - **Nmap** → network reconnaissance
  - **Hydra** → SSH password brute-force testing
  - **SSH** → secure remote login

## 3. Steps Performed

### Step 1 — Firewall Setup

- Configured Debian as a firewall using iptables.

- Allowed inbound traffic only on required services:
- sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
- sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
- sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
- sudo iptables -A INPUT -p icmp -j ACCEPT
- Denied all other inbound traffic by default.

```
root@raj:~# iptables --version
iptables v1.8.11 (legacy)
root@raj:~# iptables -F
root@raj:~# iptables -X
root@raj:~# iptables -Z
root@raj:~# iptables -p INPUT ACCEPT
iptables v1.8.11 (legacy): unknown protocol "input" specified
Try `iptables -h' or 'iptables --help' for more information.
root@raj:~# iptables -P INPUT ACCEPT
root@raj:~# iptables -P OUTPUT ACCEPT
root@raj:~# iptables -P FORWARD ACCEPT
root@raj:~# ipdates -A INPUT -p tcp --dport 80 -j ACCEPT
-bash: ipdates: command not found
root@raj:~# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@raj:~# iptables -A INPUT -p tcp --dport 443 -j ACCEPT
root@raj:~# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
root@raj:~# iptables -A INPUT -p icmp -j ACCEPT
root@raj:~# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@raj:~# iptables -P INPUT DROP
root@raj:~# _
```

```
root@raj:~# iptables -L -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            ctstate RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 460 packets, 30820 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@raj:~#
```

**Step 2.1- checking connection**

**getting ip of Debain:( command : ip a )**

```
root@raj:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0b:4f:2a brd ff:ff:ff:ff:ff:ff
    altname enx0800270b4f2a
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 69518sec preferred_lft 58718sec
    inet6 fd00::a00:27ff:fe0b:4f2a/64 scope global dynamic mngtmpaddr proto kernel_ra
       valid_lft 82004sec preferred_lft 10004sec
    inet6 fd00::eb2e:6a7:6e18:d2fc/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 82004sec preferred_lft 10004sec
    inet6 fe80::d73d:9aae:8b87:a5ce/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:3f:dc:bc brd ff:ff:ff:ff:ff:ff
    altname enx0800273fdcbc
```

```
akashr@akash: ~
File  Actions  Edit  View  Help

┌──(akashr㉿akash)-[~]
└─$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=3.51 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=1.63 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=64 time=2.04 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=64 time=2.05 ms
64 bytes from 192.168.1.10: icmp_seq=5 ttl=64 time=1.29 ms
64 bytes from 192.168.1.10: icmp_seq=6 ttl=64 time=1.61 ms
64 bytes from 192.168.1.10: icmp_seq=7 ttl=64 time=1.47 ms
64 bytes from 192.168.1.10: icmp_seq=8 ttl=64 time=1.10 ms
64 bytes from 192.168.1.10: icmp_seq=9 ttl=64 time=1.49 ms
^C
--- 192.168.1.10 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8176ms
rtt min/avg/max/mdev = 1.095/1.798/3.514/0.673 ms
```

**Step 2.2 — Network Reconnaissance**

- From Kali, performed **Nmap scanning** on the Debian firewall:
- nmap 192.168.1.10
- nmap -sS 192.168.1.10
- Identified **open ports**: 22 (SSH), 80 (HTTP), 443 (HTTPS), ICMP allowed.

( **Using Apache**

sudo apt update

sudo apt install apache2 -y

sudo systemctl start apache2

sudo systemctl enable apache2

This automatically starts an HTTP server on **port 80**.
For HTTPS (443**), enable SSL:**

sudo apt install openssl -y

sudo a2enmod ssl

sudo systemctl restart apache2 )

command: nmap 192.168.1.10

```
┌──(akashr㉿akash)-[~]
└─$ nmap 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-21 13:51 IST
Nmap scan report for 192.168.1.10
Host is up (0.0013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:0B:4F:2A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.69 seconds
```

command: namp -sS 192.168.1.10

```
┌──(akashr㉿akash)-[~]
└─$ nmap -sS 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-21 14:01 IST
Nmap scan report for 192.168.1.10
Host is up (0.0013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:0B:4F:2A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.90 seconds
```

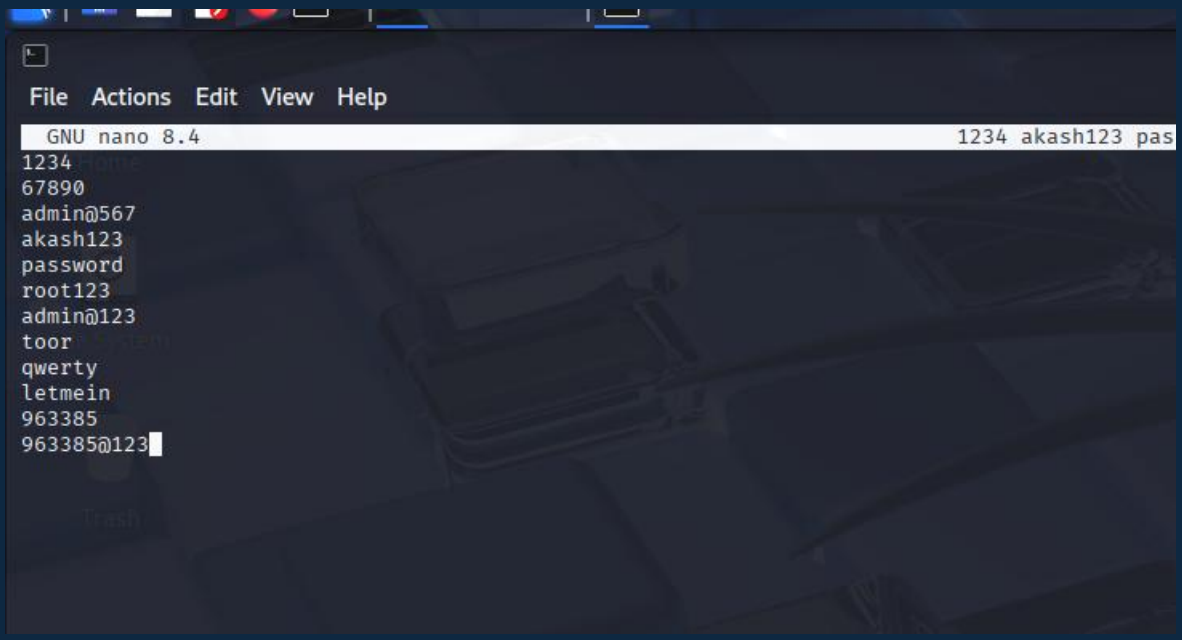
**Step 3 — Initial SSH Access**

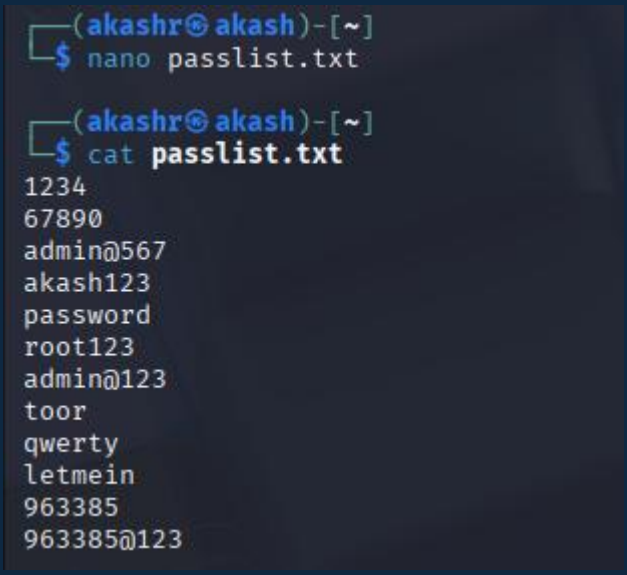
- Logged in manually via SSH:
- ssh akash@192.168.1.10
- Verified connectivity and proper user access.

```
└─$ ssh akash@192.168.1.10
akash@192.168.1.10's password:
Linux raj 6.12.38+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.38-1 (2025-07-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
akash@raj:~$
```

**Step 4 — Brute-Force Testing (Hydra Attack)**

- From Kali, launched Hydra to test SSH password security:
- hydra -l akash -P passlist.txt ssh://192.168.1.10
- Successfully obtained the password for user akash due to default SSH configuration and no login attempt restrictions.
- Logs on Debian showed multiple failed login attempts followed by one successful login.



```
┌──(akashr㉿akash)-[~]
└─$ hydra -l akash -P passlist.txt ssh://192.168.1.10

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-21 15:45:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: us
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:1/p:12), ~1 try per task
[DATA] attacking ssh://192.168.1.10:22/
[22][ssh] host: 192.168.1.10   login: akash   password: 963385
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-21 15:45:20
```

```
-- Boot b36145c98e0d4229b7934384fc9731eb --
Aug 21 08:11:16 raj systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Aug 21 08:11:16 raj sshd[713]: Server listening on 0.0.0.0 port 22.
Aug 21 08:11:16 raj sshd[713]: Server listening on :: port 22.
Aug 21 08:11:16 raj systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
-- Boot eadeed5ccd3e486bb19a7b6a293d9cc5 --
Aug 21 13:09:41 raj systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Aug 21 13:09:41 raj sshd[702]: Server listening on 0.0.0.0 port 22.
Aug 21 13:09:41 raj sshd[702]: Server listening on :: port 22.
Aug 21 13:09:41 raj systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Aug 21 14:02:30 raj sshd-session[1982]: Connection closed by 192.168.1.9 port 56322
Aug 21 14:38:15 raj sshd[702]: Timeout before authentication for connection from 192.168.1.9 to 192.168.1.10, pid = 2070
Aug 21 14:54:33 raj sshd[702]: Timeout before authentication for connection from 192.168.1.9 to 192.168.1.10, pid = 2108
Aug 21
Aug 21 15:13:53 raj sshd-session[2167]: Accepted password for akash from 192.168.1.9 port 42236 ssh2
Aug 21                                                                                  ) by akash(uid=0)
Aug 21 15:45:16 raj sshd-session[2258]: Received disconnect from 192.168.1.9 port 40072:11: Bye Bye [preauth]
Aug 21 15:45:16 raj sshd-session[2258]: Disconnected from authenticating user akash 192.168.1.9 port 40072 [preauth]
Aug 21 15:45:16 raj sshd[702]: drop connection #10 from [192.168.1.9]:40162 on [192.168.1.10]:22 Maxstartups
Aug 21 15:45:16 raj unix_chkpwd[2282]: password check failed for user (akash)
Aug 21 15:45:16 raj unix_chkpwd[2285]: password check failed for user (akash)
lines 1-49
```

### Step 5 — SSH Hardening and Firewall Strengthening

- Hardened SSH configuration on Debian:
  - Changed SSH port: 22 → 2222
  - Disabled root login: PermitRootLogin no
  - Limited login attempts: MaxAuthTries 3
- Updated firewall rules to allow new SSH port and block old one:
- sudo iptables -A INPUT -p tcp --dport 2222 -j ACCEPT
- sudo iptables -A INPUT -p tcp --dport 22 -j DROP
- Restarted SSH service and verified connectivity.

```
#Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no_
#StrictModes yes
#MaxAuthTries 3
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

**Step 6 — Second Brute-Force Attempt**

- Attempted Hydra attack on new SSH configuration:
- hydra -l akash -P passlist.txt ssh://192.168.1.10:2222
- Result: **Failed to connect** because:
  - SSH port had changed
  - MaxAuthTries limited attempts
  - Root login disabled
- Demonstrates the **effectiveness of hardening measures** against brute-force attacks.

**6. Key Takeaways**

- Always restrict **unused ports** on firewalls.
- Limit **SSH login attempts** and disable root login.
- Change default SSH port to reduce automated attacks.

- Regularly monitor **auth logs** to detect suspicious activity.
- Penetration testing helps identify weaknesses before attackers do.