

Name: Chaudhary Ehsan Rasheed

Reg. No: BCS223075

I had already updated my system a day prior so I didn't updated it again, moreover I installed RustScan using:

```
sudo apt install curl-y curl--proto '=https'--tlsv1.2-sf https://sh.rustup.rs | sh
```

Remaining tasks and their output are listed below:

*Perform a full port scan on 127.0.0.1:*

```
(kali@kali)~$ rustscan -b 1000 -a 127.0.0.1 --range 1-65535

RUSTSCAN
The Modern Day Port Scanner.

: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :

RustScan: Because guessing isn't hacking.

[~] The config file is expected to be at "/home/kali/.rustscan.toml"
[~] File limit higher than batch size. Can increase speed by increasing batch size '-b 924'.
Open 127.0.0.1:56794
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-16 13:10 EDT
Initiating SYN Stealth Scan at 13:10
Scanning localhost (127.0.0.1) [1 port]
Completed SYN Stealth Scan at 13:10, 0.02s elapsed (1 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response (0.00084s latency).
Scanned at 2025-03-16 13:10:30 EDT for 0s

PORT      STATE SERVICE REASON
56794/tcp  closed unknown reset ttl 64

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
Raw packets sent: 1 (44B) | Rcvd: 2 (84B)

(kali@kali)~$
```

*Scan the domain cust.edu.pk for open ports:*

```
(kali@kali)~$ rustscan -a cust.edu.pk --range 1-65535

RUSTSCAN
The Modern Day Port Scanner.

: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :

RustScan: Because guessing isn't hacking.

[~] The config file is expected to be at "/home/kali/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 162.159.135.42:80
Open 162.159.135.42:443
Open 162.159.135.42:8080
Open 162.159.135.42:8443
Open 162.159.135.42:8880
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-16 13:15 EDT
Initiating Ping Scan at 13:15
Scanning 162.159.135.42 [4 ports]
Completed Ping Scan at 13:15, 3.04s elapsed (1 total hosts)
Nmap scan report for 162.159.135.42 [host down, received no-response]
Read data files from: /usr/share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.19 seconds
Raw packets sent: 8 (304B) | Rcvd: 0 (0B)

(kali@kali)~$
```

*scan results of 192.168.1.1*

```
[kali@kali]~$ rustscan -a 192.168.1.1 --range 1-65535 -- -sV
```

```
The Modern Day Port Scanner.
```

```
: http://discord.skerritt.blog           :  
: https://github.com/RustScan/RustScan   :
```

```
Oday was here ♥
```

```
[~] The config file is expected to be at "/home/kali/.rustscan.toml"  
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers  
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.  
rustscan -a 192.168.1.1 --range 1-65535 -- -sV
```

```
Open 192.168.1.1:36645  
[~] Starting Script(s)  
[>] Running script "nmap -vvv -p {{port}} {{ip}} -sV" on ip 192.168.1.1  
Depending on the complexity of the script, results may take some time to appear.  
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-16 13:25 EDT  
NSE: Loaded 47 scripts for scanning.  
Initiating Ping Scan at 13:25  
Scanning 192.168.1.1 [4 ports]  
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan  
Ping Scan Timing: About 50.00% done; ETC: 13:25 (0:00:01 remaining)  
Completed Ping Scan at 13:25, 3.04s elapsed (1 total hosts)  
Nmap scan report for 192.168.1.1 [host down, received no-response]  
Read data files from: /usr/share/nmap  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.33 seconds  
Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```

*Use RustScan with Nmap to perform a service version scan on 192.168.1.1.*

```
(kali㉿kali)-[~]
$ sudo rustscan -a 192.168.1.100 -p 21,22,3306 -- -sV

[sudo] password for kali:
0day was here ♥

The Modern Day Port Scanner.

: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :

0day was here ♥

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the ulimit with '--ulimit 5000'.
[!] Looks like I didn't find any open ports for 192.168.1.100. This is usually caused by a high batch size.

*I used 4500 batch size, consider lowering it with 'rustscan -b <batch_size> -a <ip address>' or a comfortable number for your system.

Alternatively, increase the timeout if your ping is high. Rustscan -t 2000 for 2000 milliseconds (2s) timeout.
```

**Result:** [!] Looks like I didn't find any open ports for 192.168.1.1. This is usually caused by a high batch size.

Scan only ports 21, 22, and 3306 on a local IP.

```
(kali㉿kali)-[~]  
$ nmap -p 21,22,3306 192.168.1.100
```

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-17 07:56 EDT  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.88 seconds

Fast Scan:

```
(kali㉿kali)-[~]  
$ nmap -T4 -F 192.168.1.0/24
```

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-17 07:58 EDT  
Nmap scan report for 192.168.1.222  
Host is up (0.015s latency).  
Not shown: 99 filtered tcp ports (no-response)  
PORT STATE SERVICE  
80/tcp open http

Nmap done: 256 IP addresses (1 host up) scanned in 19.93 seconds

Find Open Web Ports on port 80,443,8080

```
(kali㉿kali)-[~]  
$ nmap -p 80,443,8080 192.168.1.0/24
```

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-17 08:01 EDT  
Nmap scan report for 192.168.1.222  
Host is up (0.077s latency).

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	filtered	https
8080/tcp	filtered	http-proxy

Nmap done: 256 IP addresses (1 host up) scanned in 79.52 seconds