

## How to Install and Use RustScan on Kali Linux

### Introduction to RustScan

RustScan is a modern, fast, and efficient port scanner built using the Rust programming language. It is designed to be significantly faster than traditional port scanners by leveraging parallelism and optimizing system resources. RustScan can quickly identify open ports and seamlessly integrate with other tools like Nmap for advanced scanning and service detection.

Key features of RustScan include:

- Ultra-fast scanning using parallel execution.

- Ability to scan the entire 65,535 ports range efficiently.

- Easy integration with Nmap for detailed service enumeration.

- Supports both IPv4 and IPv6 addresses.

- Open-source and actively maintained by the community.

### ✔ 1. Update and Upgrade Your System

Ensure your system is up-to-date:

```
sudo apt update && sudo apt upgrade -y
```

### ✔ 2. Install Rust (If Not Installed)

If Rust is missing, install it:

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

Set Rust to your environment:

```
source $HOME/.cargo/env
```

```
rustup default stable
```

### ✔ 3. Download and Install RustScan (Deb Package Method)

This method works best for Kali Linux:

Download the .deb package:

**Wget**

```
https://github.com/RustScan/RustScan/releases/download/2.2.2/rustscan_2.2.2_amd64.  
deb
```

Made by Moez Javed  
Install the package:

```
sudo dpkg -i rustscan_2.2.2_amd64.deb
```

Fix dependencies if needed:

```
sudo apt --fix-broken install
```

## ✔ 4. Verify the Installation

Check if RustScan is successfully installed:

```
rustscan --version
```

## ✔ 5. Run a Test Scan

Example scan of a local IP address:

```
rustscan -a 192.168.100.84 --range 1-65535
```

```
(root@kali) ~# rustscan -a 192.168.100.84 --range 1-65535
RUSTSCAN
The Modern Day Port Scanner.
: http://discord.skerritt.blog
: https://github.com/RustScan/RustScan :
Scanning ports: The virtual equivalent of knocking on doors.
[-] The config file is expected to be at '/root/.rustscan.toml'
[-] File limit is lower than default batch size. Consider upping with --ulimit.
    t. 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 192.168.100.84:135
Open 192.168.100.84:135
Open 192.168.100.84:445
Open 192.168.100.84:5040
Open 192.168.100.84:49666
Open 192.168.100.84:49665
Open 192.168.100.84:49664
Open 192.168.100.84:49675
Open 192.168.100.84:49671
Open 192.168.100.84:49670
Open 192.168.100.84:49667
[-] Starting Script(s)
[-] Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-12 00:44 EDT
Initiating Ping Scan at 00:44
Scanning 192.168.100.84 [4 ports]
Completed Ping Scan at 00:44, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:44
Completed Parallel DNS resolution of 1 host. at 00:44, 0.04s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, S
F: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 00:44
Scanning 192.168.100.84 [11 ports]
Discovered open port 49667/tcp on 192.168.100.84
Discovered open port 5040/tcp on 192.168.100.84
Discovered open port 135/tcp on 192.168.100.84
Discovered open port 445/tcp on 192.168.100.84
Discovered open port 139/tcp on 192.168.100.84
Discovered open port 49671/tcp on 192.168.100.84
Discovered open port 49670/tcp on 192.168.100.84
Discovered open port 49675/tcp on 192.168.100.84
Discovered open port 49665/tcp on 192.168.100.84
Discovered open port 49664/tcp on 192.168.100.84
Discovered open port 49666/tcp on 192.168.100.84
Completed SYN Stealth Scan at 00:44, 0.05s elapsed (11 total ports)
```

```
rustscan -a cust.edu.pk --range 1-65535
```

Made by Moez Javed

```
root@kali: ~/home/moez
# rustscan -a cust.edu.pk --range 1-65535

RUSTSCAN

The Modern Day Port Scanner.

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

Open ports, closed hearts.

[-] 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'.
Open 162.159.135.42:80
Open 162.159.135.42:443
Open 162.159.135.42:2086
Open 162.159.135.42:2083
Open 162.159.135.42:2082
Open 162.159.135.42:2053
Open 162.159.135.42:2052
Open 162.159.135.42:2096
Open 162.159.135.42:2095
Open 162.159.135.42:2087
[-] Starting Script(s)
[-] Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-12 01:07 EDT
Initiating Ping Scan at 01:07
Scanning 162.159.135.42 [4 ports]
Completed Ping Scan at 01:07, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host: at 01:07
Completed Parallel DNS resolution of 1 host: at 01:07, 4.11s elapsed
DNS resolution of 1 IPs took 4.11s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating SYN Stealth Scan at 01:07
Scanning 162.159.135.42 [10 ports]
Discovered open port 443/tcp on 162.159.135.42
Discovered open port 2095/tcp on 162.159.135.42
Discovered open port 80/tcp on 162.159.135.42
Discovered open port 2086/tcp on 162.159.135.42
Discovered open port 2096/tcp on 162.159.135.42
Discovered open port 2082/tcp on 162.159.135.42
Discovered open port 2087/tcp on 162.159.135.42
Discovered open port 2052/tcp on 162.159.135.42
Discovered open port 2053/tcp on 162.159.135.42
Discovered open port 2083/tcp on 162.159.135.42
Completed SYN Stealth Scan at 01:07, 0.21s elapsed (10 total ports)
Nmap scan report for 162.159.135.42
Host is up, received reset ttl 255 (0.12s latency).
Scanned at 2025-03-12 01:07:51 EDT for 6s
```

## Tasks:

✓ RustScan Tasks:

Update and upgrade your Kali Linux system.

Install Rust and verify the installation.

Download and install RustScan using the .deb package.

Perform a full port scan on 127.0.0.1.

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

Save the scan results of 192.168.1.1 to a text file.

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

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

Perform a fast port scan on the subnet 192.168.1.0/24.

Find open web ports (80, 443, 8080) on 192.168.1.1.

**Report submission**, you are required to appear for a viva till Wednesday 11:00am  
**Venue:** B Block, 3rd Floor