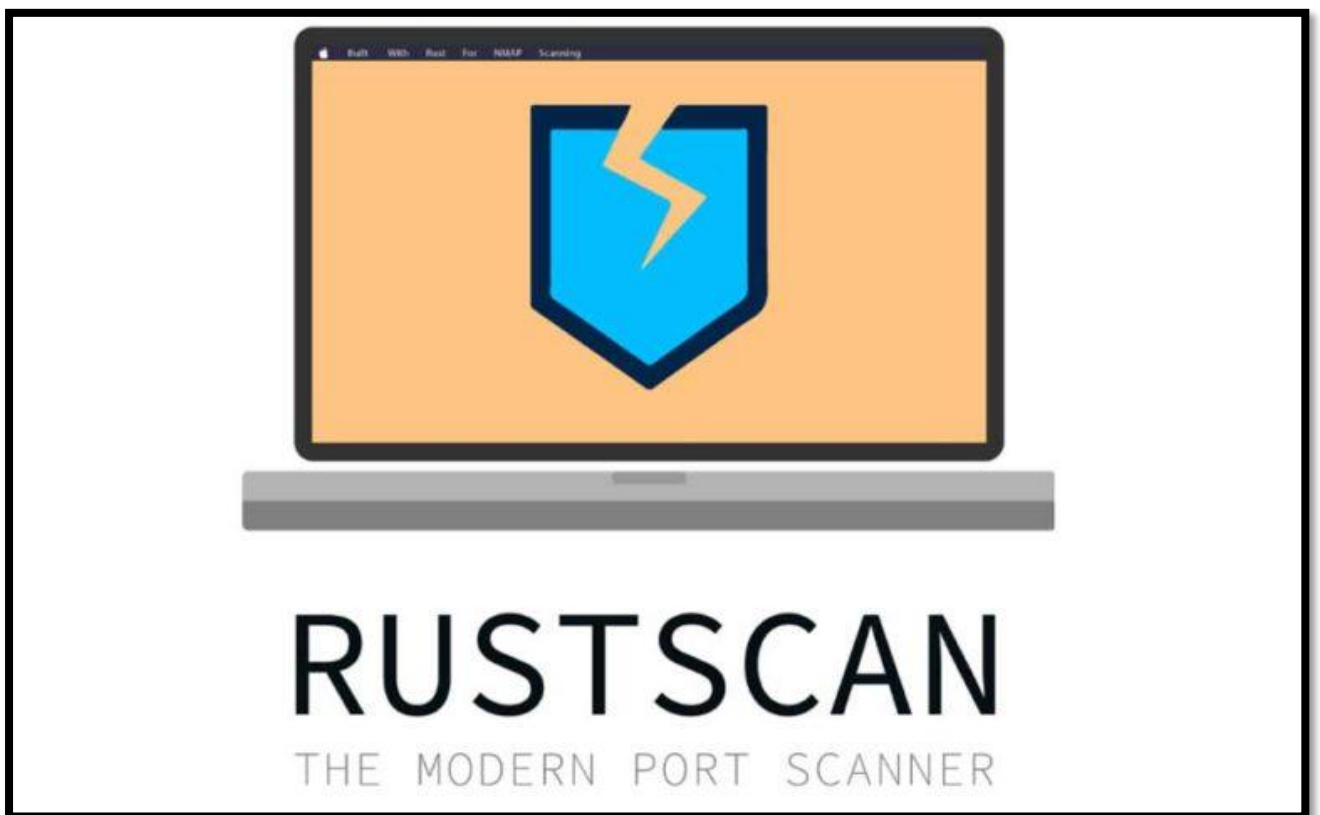


**Day 3 of Learning Cyber Security****Platform: Kali Linux****Name:** Ayesha Nadeem**Topic:** Rust Scan**Contact Me:** [ayeshanm8@gmail.com](mailto:ayeshanm8@gmail.com)**Date:** 3<sup>rd</sup> July, 2025

## RustScan: Fast Recon, Smarter Results

### Update and upgrade your Kali Linux system (optional)

Command 1:

```

File Actions Edit View Help

(ayeshanadeem@ayeshanadeem)-[~]
$ sudo apt update -y
[sudo] password for ayeshanadeem:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
40 packages can be upgraded. Run 'apt list --upgradable' to see

(ayeshanadeem@ayeshanadeem)-[~]
$ sudo apt upgrade -y
The following packages were automatically installed and are no longer needed:
  firebird3.0-common      libcephfs2      libgeos3.12
  firebird3.0-common-doc  libconfig++9v5  libgeos3.13
  fonts-liberation2       libconfig9      libgfapi0
  freerdp2-x11            libdaxctl1      libgfrpc0
  hydra-gtk               libdirectfb-1.7-7t64  libgfxdr0
  ibverbs-providers       libegl-dev      libgl1-mesa
  libarmadillo12          libflac12t64    libglapi-me
  libassuan0              libfmt9         libgles-dev
  libavfilter9            libfreerdp-client2-2t64  libgles1
  libbbfio1              libfreerdp2-2t64  libglusterf
  libboost-iostreams1.83.0  libgail-common  libglvnd-co
  libboost-thread1.83.0    libgail18t64    libglvnd-de
  libcapstone4            libgdal34t64    libgspell-1

Use 'sudo apt autoremove' to remove them.

Not upgrading:
  exiv2          libapache2-mod-php  libqt6multimedia6  libqt6multimedia6-dev
  gir1.2-nm-1.0  libnm0              libqt6qml6          libqt6qml6-dev
  imagemagick    libqt6core5compat6  libqt6qmlmodels6   libqt6qmlmodels6-dev
  kali-desktop-xfce  libqt6core6t64     libqt6quick6        libqt6quick6-dev

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 40

(ayeshanadeem@ayeshanadeem)-[~]

```

## Installation of Rust

### Command 2:

First install curl. It works behind the scene of rust scan in order to download required files.

```
(ayeshanadeem@ayeshanadeem)-[~]
$ sudo apt install curl -y
curl is already the newest version (8.12.1-3).
curl set to manually installed.
The following packages were automatically installed and are no longer req
  firebird3.0-common      libcephfs2      libgeos3.12.1t64  l
  firebird3.0-common-doc  libconfig++9v5  libgeos3.13.0     l
  fonts-liberation2      libconfig9      libgfapi0         l
  freerdp2-x11           libdaxctl1      libgfrpc0         l
  hydra-gtk              libdirectfb-1.7-7t64  libgfxdr0        l
  ibverbs-providers      libegl-dev      libgl1-mesa-dev   l
  libarmadillo12         libflac12t64    libglapi-mesa     l
  libassuan0             libfmt9         libgles-dev       l
  libavfilter9           libfreerdp-client2-2t64  libgles1         l
  libbfbio1              libfreerdp2-2t64  libglusterfs0     l
  libboost-iostreams1.83.0  libgail-common  libglvnd-core-dev l
  libboost-thread1.83.0   libgail18t64    libglvnd-dev      l
  libcapstone4           libgdal34t64    libgspell-1-2     l
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 40
```

### Command 3:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ curl --proto '=https' --tlsv1.2 -sSf https://sh.rustup.rs | sh
info: downloading installer
```

#### Welcome to Rust!

This will download and install the official compiler for the Rust programming language, and its package manager, Cargo.

Rustup metadata and toolchains will be installed into the Rustup home directory, located at:

```
/home/ayeshanadeem/.rustup
```

This can be modified with the RUSTUP\_HOME environment variable.

The Cargo home directory is located at:

```
/home/ayeshanadeem/.cargo
```

This can be modified with the CARGO\_HOME environment variable.

The **cargo**, **rustc**, **rustup** and other commands will be added to Cargo's bin directory, located at:

#### Rust is installed now. Great!

To get started you may need to restart your current shell. This would reload your **PATH** environment variable to include Cargo's bin directory (\$HOME/.cargo/bin).

To configure your current shell, you need to source the corresponding **env** file under \$HOME/.cargo.

This is usually done by running one of the following (note the leading DOT):

```
. "$HOME/.cargo/env"          # For sh/bash/zsh/ash/dash/pdksh
source "$HOME/.cargo/env.fish" # For fish
source "$HOME/.cargo/env.nu"   # For nushell
```

### Command 4:

Setting up environment

```
(ayeshanadeem@ayeshanadeem)-[~]
$ source $HOME/.cargo/env
```

```
(ayeshanadeem@ayeshanadeem)-[~]
$ rustup default stable
```

info: using existing install for 'stable-x86\_64-unknown-linux-gnu'

info: default toolchain set to 'stable-x86\_64-unknown-linux-gnu'

```
stable-x86_64-unknown-linux-gnu unchanged - rustc 1.85.0 (4d91de4e4 2025-02-17)
```

## Verify the installation

Command 5:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ rustscan --version
rustscan 2.1.1
```

## Download RustScan .deb package

Command 6:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ wget https://github.com/RustScan/RustScan/releases/download/2.2.2/rustscan_2.2.2_amd64.deb

--2025-03-15 13:09:44-- https://github.com/RustScan/RustScan/releases/download/2.2.2/rustscan_2.2.2_amd64.deb
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443 ... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/bee-san/RustScan/releases/download/2.2.2/rustscan_2.2.2_amd64.deb [following]
--2025-03-15 13:09:46-- https://github.com/bee-san/RustScan/releases/download/2.2.2/rustscan_2.2.2_amd64.deb
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/278933035/e7010509-0a95-4
Faws4_request&X-Amz-Date=20250315T170946Z&X-Amz-Expires=300&X-Amz-Signature=059aafd549d9bc3eaf4d3e4af9cd2a7fa9d9
_amd64.deb&response-content-type=application%2Foctet-stream [following]
--2025-03-15 13:09:46-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/278933035/
s-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250315T170946Z&X-Amz-Expires=300&X-Amz-Signature=059aafd549d9bc3eaf4d3
Drustscan_2.2.2_amd64.deb&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.109.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1506140 (1.4M) [application/octet-stream]
Saving to: 'rustscan_2.2.2_amd64.deb'

rustscan_2.2.2_amd64.deb                               100%[=====]
2025-03-15 13:09:50 (721 KB/s) - 'rustscan_2.2.2_amd64.deb' saved [1506140/1506140]
```

## Command 7:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ sudo dpkg -i rustscan_2.2.2_amd64.deb
Selecting previously unselected package rustscan.
(Reading database ... 448405 files and directories currently installed.)
Preparing to unpack rustscan_2.2.2_amd64.deb ...
Unpacking rustscan (2.2.2) ...
Setting up rustscan (2.2.2) ...
Processing triggers for kali-menu (2025.1.1) ...

(ayeshanadeem@ayeshanadeem)-[~]
```

## Command 8:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ sudo apt --fix-broken install
The following packages were automatically installed and are no longer required:
firebird3.0-common libcephfs2 libgeos3.12.1t64 libgtk2.0-0
firebird3.0-common-doc libconfig++9v5 libgeos3.13.0 libgtk2.0-l
fonts-liberation2 libconfig9 libgfsapi0 libgtk2.0-0
freerdp2-x11 libdaxctl1 libgfrpc0 libgtksourceview2.0-0
hydra-gtk libdirectfb-1.7-7t64 libgfxdr0 libgtksourceview2.0-0
ibverbs-providers libegl-dev libgl1-mesa-dev libgtksourceview2.0-0
libarmadillo12 libflac12t64 libglapi-mesa libgumbo2
libassuan0 libfmt9 libgles-dev libhdf5-100
libavfilter9 libfreerdp-client2-2t64 libgles1 libhdf5-hl
libbfio1 libfreerdp2-2t64 libglusterfs0 libibverbs0
libboost-iostreams1.83.0 libgail-common libglvnd-core-dev libimobilet
libboost-thread1.83.0 libgail18t64 libglvnd-dev libiniparser0
libcapstone4 libgdal34t64 libgspell-1-2 libjim0.82

Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 40

(ayeshanadeem@ayeshanadeem)-[~]
```



## Scanning and Vulnerability assessment

### Command 9:

## Scan a local host

```
(ayeshanadeem@ayeshanadeem)-[~]
$ rustscan -a 127.0.0.1 --range 1-65535
```

The Modern Day Port Scanner.

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

RustScan: Where '404 Not Found' meets '200 OK'.


```
[~] The config file is expected to be at "/home/ayeshanadeem/.rustscan.toml"  
[!] File limit is lower than default batch size. Consider upping with --ulimi  
[!] Your file limit is very small, which negatively impacts RustScan's speed.  
Open 127.0.0.1:22  
Open 127.0.0.1:35192  
[~] Starting Script(s)  
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-15 13:21 EDT  
Initiating SYN Stealth Scan at 13:21  
Scanning localhost (127.0.0.1) [2 ports]  
Discovered open port 22/tcp on 127.0.0.1  
Completed SYN Stealth Scan at 13:21, 0.01s elapsed (2 total ports)  
Nmap scan report for localhost (127.0.0.1)  
Host is up, received localhost-response (0.000055s latency).  
Scanned at 2025-03-15 13:21:05 EDT for 0s
```

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack ttl 64
35192/tcp	closed	unknown	reset ttl 64

Read data files from: /usr/share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds  
Raw packets sent: 2 (88B) | Rcvd: 5 (212B)

## Command 10:

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



```
The Modern Day Port Scanner.

: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :
-----
Open ports, closed hearts.

[~] The config file is expected to be at "/home/ayeshanadeem/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker imag
Open 162.159.135.42:443
Open 162.159.135.42:80
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
Open 162.159.135.42:2086
Open 162.159.135.42:2083
Open 162.159.135.42:2082
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-15 13:16 EDT
Initiating Ping Scan at 13:16
Scanning 162.159.135.42 [4 ports]
Completed Ping Scan at 13:16, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:16
Completed Parallel DNS resolution of 1 host. at 13:16, 13.01s elapsed
DNS resolution of 1 IPs took 13.01s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 13:16
Scanning 162.159.135.42 [10 ports]
Completed SYN Stealth Scan at 13:16, 0.02s elapsed (10 total ports)
Nmap scan report for 162.159.135.42
Host is up, received reset ttl 255 (0.0045s latency).
Scanned at 2025-03-15 13:16:00 UTC by ayeshanadeem

PORT      STATE      SERVICE    REASON
80/tcp    filtered  http       net-unreach from 10.0.2.2 ttl 255
443/tcp   filtered  https      net-unreach from 10.0.2.2 ttl 255
2052/tcp  filtered  clearvisn  net-unreach from 10.0.2.2 ttl 255
2053/tcp  filtered  knetd      net-unreach from 10.0.2.2 ttl 255
2082/tcp  filtered  infowave   net-unreach from 10.0.2.2 ttl 255
2083/tcp  filtered  radsec     net-unreach from 10.0.2.2 ttl 255
2086/tcp  filtered  gnet       net-unreach from 10.0.2.2 ttl 255
2087/tcp  filtered  eli        net-unreach from 10.0.2.2 ttl 255
2095/tcp  filtered  nbx-ser    net-unreach from 10.0.2.2 ttl 255
2096/tcp  filtered  nbx-dir    net-unreach from 10.0.2.2 ttl 255
```



Command 11:

```
(root@ayeshanadeem)~[/home/ayeshanadeem]
# rustscan -a 10.0.2.15 --range 1-65535
```

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

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

```
Nmap? More like slowmap.🐢
```

```
[~] The config file is expected to be at "/root/.rustscan.toml"
```

```
[~] File limit higher than batch size. Can increase speed by increasing batch size '-b 4900'.
```

```
Open 10.0.2.15:22
```

```
[~] Starting Script(s)
```

```
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-15 21:39 EDT
```

```
Initiating Parallel DNS resolution of 1 host.: 21:39
```

```
Completed Parallel DNS resolution of 1 host.. at 21:39, 13.00s elapsed
```

```
DNS resolution of 1 IPs took 13.01s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
```

```
Initiating SYN Stealth Scan at 21:39
```

```
Scanning 10.0.2.15 [1 port]
```

```
Discovered open port 22/tcp on 10.0.2.15
```

```
Completed SYN Stealth Scan at 21:39, 0.03s elapsed (1 total ports)
```

```
Nmap scan report for 10.0.2.15
```

```
Host is up, received localhost-response (0.00015s latency).
```

```
Scanned at 2025-03-15 21:39:16 EDT for 0s
```

```
PORT      STATE SERVICE REASON
```

```
22/tcp    open  ssh     syn-ack ttl 64
```

```
Read data files from: /usr/share/nmap
```

```
Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

```
Raw packets sent: 1 (44B) | Rcvd: 2 (88B)
```

## Command 12:

```
(root@ayeshanadeem) [/home/ayeshanadeem]
# rustscan -a 10.0.2.15 -- -sV

[0x00000000] [0x00000000] [0x00000000] [0x00000000]
[0x00000000] [0x00000000] [0x00000000] [0x00000000]

The Modern Day Port Scanner.

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

To scan or not to scan? That is the question.

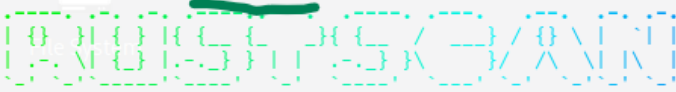
[~] The config file is expected to be at "/root/.rustscan.toml"
[~] File limit higher than batch size. Can increase speed by increasing batch size '-b 4900'.
Open 10.0.2.15:22
[~] Starting Script(s)
[>] Running script "nmap -vvv -p {{port}} {{ip}} -sV" on ip 10.0.2.15
Depending on the complexity of the script, results may take some time to appear.
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-15 21:43 EDT
NSE: Loaded 47 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 21:43
Completed Parallel DNS resolution of 1 host. at 21:43, 13.01s elapsed
DNS resolution of 1 IPs took 13.01s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 21:43
Scanning 10.0.2.15 [1 port]
Discovered open port 22/tcp on 10.0.2.15
Completed SYN Stealth Scan at 21:43, 0.02s elapsed (1 total ports)
Initiating Service scan at 21:43
Scanning 1 service on 10.0.2.15
Completed Service scan at 21:43, 0.05s elapsed (1 service on 1 host)
NSE: Script scanning 10.0.2.15.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 21:43
Completed NSE at 21:43, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 21:43
Completed NSE at 21:43, 0.00s elapsed
Nmap scan report for 10.0.2.15
Host is up, received localhost-response (0.00017s latency).
Scanned at 2025-03-15 21:43:41 EDT for 1s

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64    OpenSSH 9.9p2 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds
Raw packets sent: 1 (44B) | Rcvd: 2 (88B)
```

## Command 13:

```
(root@ayeshanadeem)-[/home/ayeshanadeem]
# rustscan -a 127.0.0.1 -p 21,22,3306 -- -sV
```



The Modern Day Port Scanner.

-----  
: <http://discord.skerritt.blog> :  
: <https://github.com/RustScan/RustScan> :  
-----

Port scanning: Making networking exciting since... whenever.

[~] The config file is expected to be at "/root/.rustscan.toml"  
[~] File limit higher than batch size. Can increase speed by increasing batch size '-b 4900'.  
Open 127.0.0.1:22  
[~] Starting Script(s)  
[>] Running script "nmap -vvv -p {{port}} {{ip}} -sV" on ip 127.0.0.1  
Depending on the complexity of the script, results may take some time to appear.  
[~] Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-15 21:47 EDT  
NSE: Loaded 47 scripts for scanning.  
Initiating SYN Stealth Scan at 21:47  
Scanning localhost (127.0.0.1) [1 port]  
Discovered open port 22/tcp on 127.0.0.1  
Completed SYN Stealth Scan at 21:47, 0.01s elapsed (1 total ports)  
Initiating Service scan at 21:47  
Scanning 1 service on localhost (127.0.0.1)  
Completed Service scan at 21:47, 0.02s elapsed (1 service on 1 host)  
NSE: Script scanning 127.0.0.1.  
NSE: Starting runlevel 1 (of 2) scan.  
Initiating NSE at 21:47  
Completed NSE at 21:47, 0.00s elapsed  
NSE: Starting runlevel 2 (of 2) scan.  
Initiating NSE at 21:47  
Completed NSE at 21:47, 0.00s elapsed  
Nmap scan report for localhost (127.0.0.1)  
Host is up, received localhost-response (0.000080s latency).  
Scanned at 2025-03-15 21:47:50 EDT for 0s

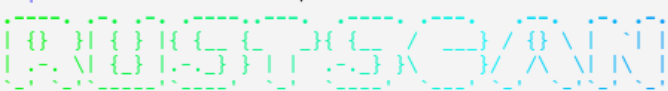
PORT	STATE	SERVICE	REASON	VERSION
22/tcp	open	ssh	syn-ack ttl 64	OpenSSH 9.9p2 Debian 1 (protocol 2.0)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Read data files from: /usr/share/nmap  
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds  
Raw packets sent: 1 (44B) | Rcvd: 2 (88B)

## Command 14:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ rustscan -a 10.0.2.14/22
```



The Modern Day Port Scanner.

-----  
: <http://discord.skerritt.blog> :  
: <https://github.com/RustScan/RustScan> :  
-----

To scan or not to scan? That is the question.

[~] The config file is expected to be at "/home/ayeshanadeem/.rustscan.toml"  
[~] File limit higher than batch size. Can increase speed by increasing batch size '-b 4900'.  
Open 10.0.2.15:22

### Command 15:

```
(ayeshanadeem@ayeshanadeem)~$ rustscan -a 10.0.2.15 -p 80,443,8080,22 -- -sV
```

```
[~] The Modern Day Port Scanner.
```

```
[~] http://discord.skerritt.blog :  
[~] https://github.com/RustScan/RustScan :  
[~] https://admin.tryhackme.com
```

```
[~] The config file is expected to be at "/home/ayeshanadeem/.rustscan.toml"  
[~] File limit higher than batch size. Can increase speed by increasing batch size '-b 4900'.  
Open 10.0.2.15:22  
[~] Starting Script(s)  
[>] Running script "nmap -vvv -p {{port}} {{ip}} -sV" on ip 10.0.2.15  
Depending on the complexity of the script, results may take some time to appear.  
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-15 22:23 EDT  
NSE: Loaded 47 scripts for scanning.  
Initiating Parallel DNS resolution of 1 host. at 22:23  
Completed Parallel DNS resolution of 1 host. at 22:23, 13.00s elapsed  
DNS resolution of 1 IPs took 13.00s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]  
Initiating SYN Stealth Scan at 22:23  
Scanning 10.0.2.15 [1 port]  
Discovered open port 22/tcp on 10.0.2.15  
Completed SYN Stealth Scan at 22:23, 0.02s elapsed (1 total ports)  
Initiating Service scan at 22:23  
Scanning 1 service on 10.0.2.15  
Completed Service scan at 22:23, 0.01s elapsed (1 service on 1 host)  
NSE: Script scanning 10.0.2.15.  
NSE: Starting runlevel 1 (of 2) scan.  
Initiating NSE at 22:23  
Completed NSE at 22:23, 0.00s elapsed  
NSE: Starting runlevel 2 (of 2) scan.  
Initiating NSE at 22:23  
Completed NSE at 22:23, 0.00s elapsed  
Nmap scan report for 10.0.2.15  
Host is up, received localhost-response (0.000088s latency).  
Scanned at 2025-03-15 22:23:40 EDT for 1s
```

PORT	STATE	SERVICE	REASON	VERSION
22/tcp	open	ssh	syn-ack ttl 64	OpenSSH 9.9p2 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel				

```
Read data files from: /usr/share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds  
Raw packets sent: 1 (44B) | Rcvd: 2 (88B)
```