Footprinting Lab

RUST SCAN

Robert Christopherson | Red-Team | 11.12.2022

Objective

Use open source and freely available tools to fingerprint a remote machine.

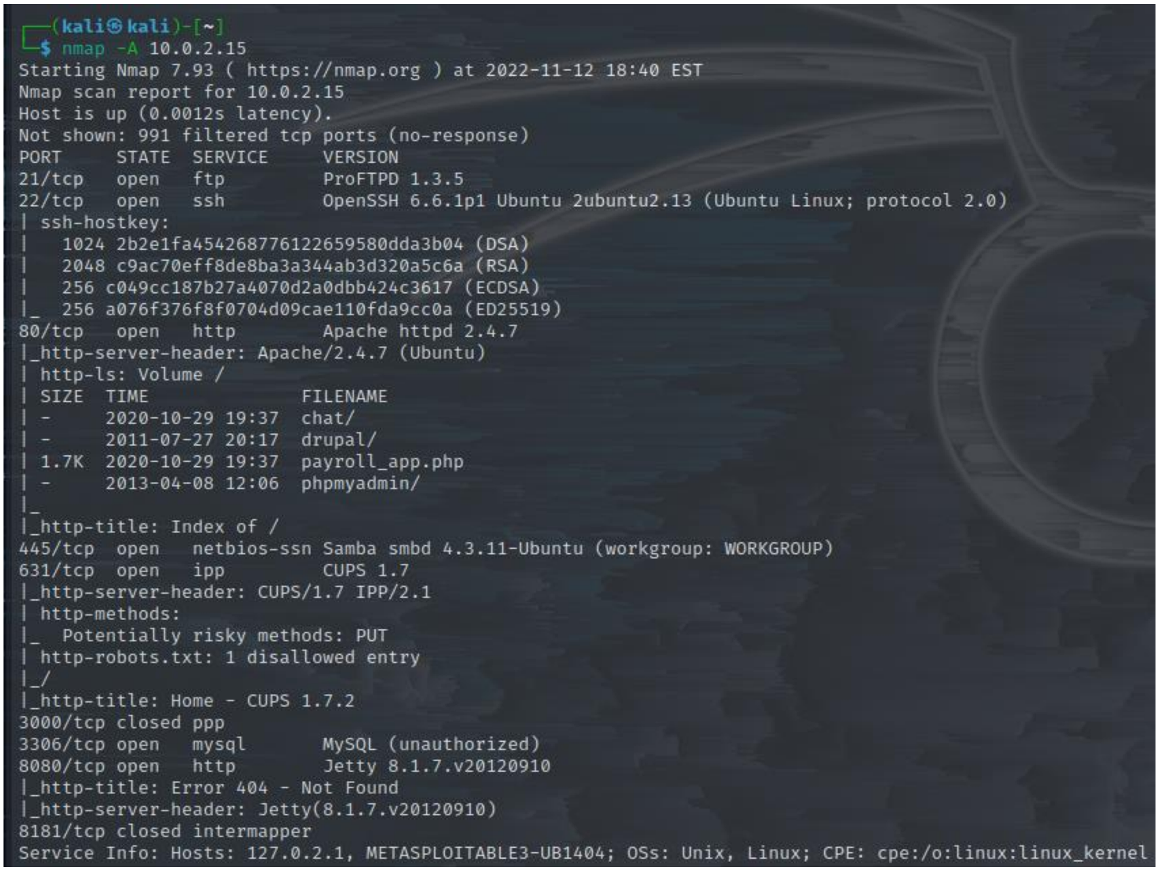
The attacker machine will be Kali Linux VM and the victim machine will be an Ubuntu VM

Method

Nmap Enumeration

- Nmap scan the device to view open ports and active services.
- We know the device IP since we set up the vulnerable machine in a VM

```
nmap -A 10.0.2.15
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-12 18:40 EST
Nmap scan report for 10.0.2.15
Host is up (0.0012s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b2e1fa454268776122659580dda3b04 (DSA)
|   2048 c9ac70eff8de8ba3a344ab3d320a5c6a (RSA)
|   256 c049cc187b27a4070d2a0dbb424c3617 (ECDSA)
|_  256 a076f376f8f0704d09cae110fda9cc0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-title: Index of /
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
|_http-server-header: CUPS/1.7 IPP/2.1
| http-methods:
|_  Potentially risky methods: PUT
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 1.7.2
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-title: Error 404 - Not Found
|_http-server-header: Jetty(8.1.7.v20120910)
8181/tcp closed intermapper
Service Info: Hosts: 127.0.2.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

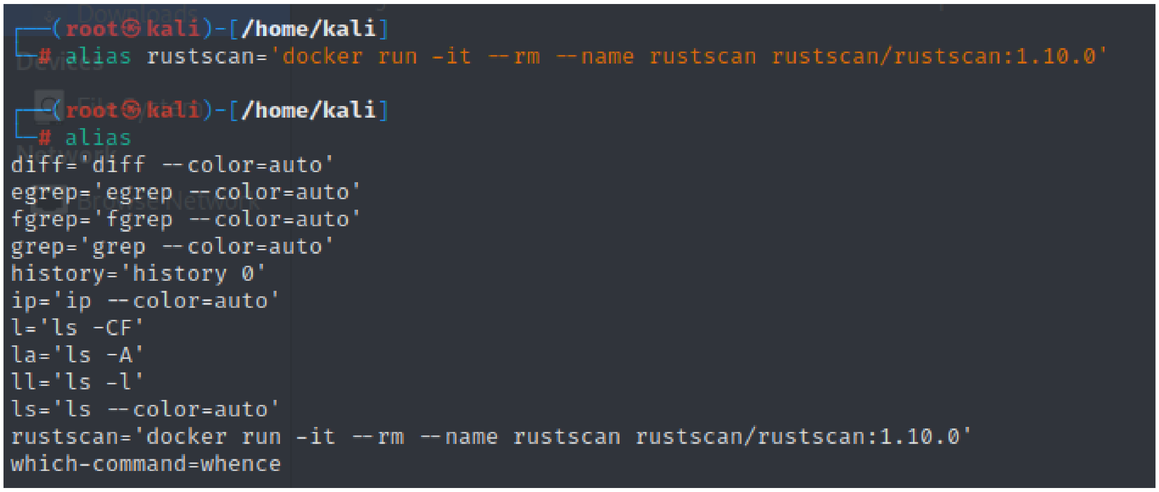
RustScan Setup

- https://github.com/RustScan/RustScan/wiki/Installation-Guide

- The recommended installation method uses docker so that’s what we will be doing.
    - To install Docker, follow their guide.
- Configure the docker setup to an alias in the terminal so that you can run a simple command to start RustScan easily.

```
alias rustscan='docker run -it --rm --name rustscan rustscan/rustscan:2.1.1'
```

- Running the “alias” command in our terminal, we can confirm the new alias has been generated. We can now start RustScan by simply using the “rustscan” command.



```
┌──(root㉿kali)-[/home/kali]
└─# alias rustscan='docker run -it --rm --name rustscan rustscan/rustscan:1.10.0'

┌──(root㉿kali)-[/home/kali]
└─# alias
diff='diff --color=auto'
egrep='egrep --color=auto'
fgrep='fgrep --color=auto'
grep='grep --color=auto'
history='history 0'
ip='ip --color=auto'
l='ls -CF'
la='ls -A'
ll='ls -l'
ls='ls --color=auto'
rustscan='docker run -it --rm --name rustscan rustscan/rustscan:1.10.0'
which-command=whence
```

RustScan Execution

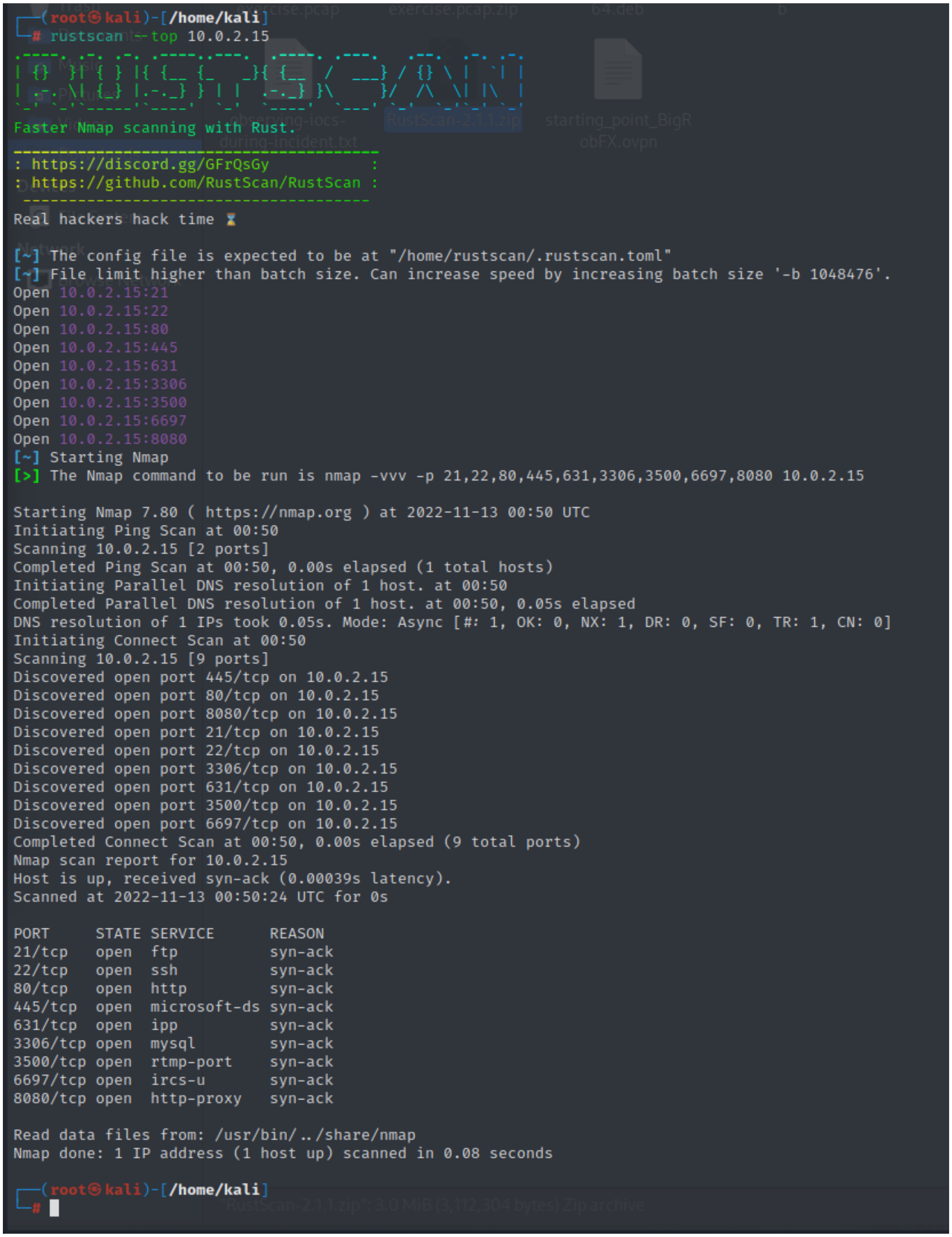
- Launch RustScan with our alias “rustscan” and any arguments including the IP address to be scanned.

```
rustscan --top 10.0.2.15
```

- RustScan will quickly enumerate open ports.
- RustScan will then run the following command via Nmap to further enumerate the open ports.

```
nmap -VVV -p 21,22,80,445,631,3306,3500,6697,8080 10.0.2.15
```

- We can then see the running services on the open ports and from there can do some further OSINT or research and ultimately exploit the services to gain access.
- Something to note: RustScan is known for its aggressive scanning behavior and is some real-world scenarios you might find yourself triggering safety measures and having your IP blocked or causing a server to crash.



```
┌──(root㉿kali)-[/home/kali]
└─# rustscan --top 10.0.2.15
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
Faster Nmap scanning with Rust.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Real hackers hack time ⏳

[~] The config file is expected to be at "/home/rustscan/.rustscan.toml"
[~] File limit higher than batch size. Can increase speed by increasing batch size '-b 1048476'.
Open 10.0.2.15:21
Open 10.0.2.15:22
Open 10.0.2.15:80
Open 10.0.2.15:445
Open 10.0.2.15:631
Open 10.0.2.15:3306
Open 10.0.2.15:3500
Open 10.0.2.15:6697
Open 10.0.2.15:8080
[~] Starting Nmap
[>] The Nmap command to be run is nmap -vvv -p 21,22,80,445,631,3306,3500,6697,8080 10.0.2.15

Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 00:50 UTC
Initiating Ping Scan at 00:50
Scanning 10.0.2.15 [2 ports]
Completed Ping Scan at 00:50, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:50
Completed Parallel DNS resolution of 1 host. at 00:50, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 00:50
Scanning 10.0.2.15 [9 ports]
Discovered open port 445/tcp on 10.0.2.15
Discovered open port 80/tcp on 10.0.2.15
Discovered open port 8080/tcp on 10.0.2.15
Discovered open port 21/tcp on 10.0.2.15
Discovered open port 22/tcp on 10.0.2.15
Discovered open port 3306/tcp on 10.0.2.15
Discovered open port 631/tcp on 10.0.2.15
Discovered open port 3500/tcp on 10.0.2.15
Discovered open port 6697/tcp on 10.0.2.15
Completed Connect Scan at 00:50, 0.00s elapsed (9 total ports)
Nmap scan report for 10.0.2.15
Host is up, received syn-ack (0.00039s latency).
Scanned at 2022-11-13 00:50:24 UTC for 0s

PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack
22/tcp   open  ssh          syn-ack
80/tcp   open  http         syn-ack
445/tcp  open  microsoft-ds syn-ack
631/tcp  open  ipp          syn-ack
3306/tcp open  mysql        syn-ack
3500/tcp open  rtmp-port    syn-ack
6697/tcp open  ircs-u       syn-ack
8080/tcp open  http-proxy   syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

┌──(root㉿kali)-[/home/kali]
└─# █
```