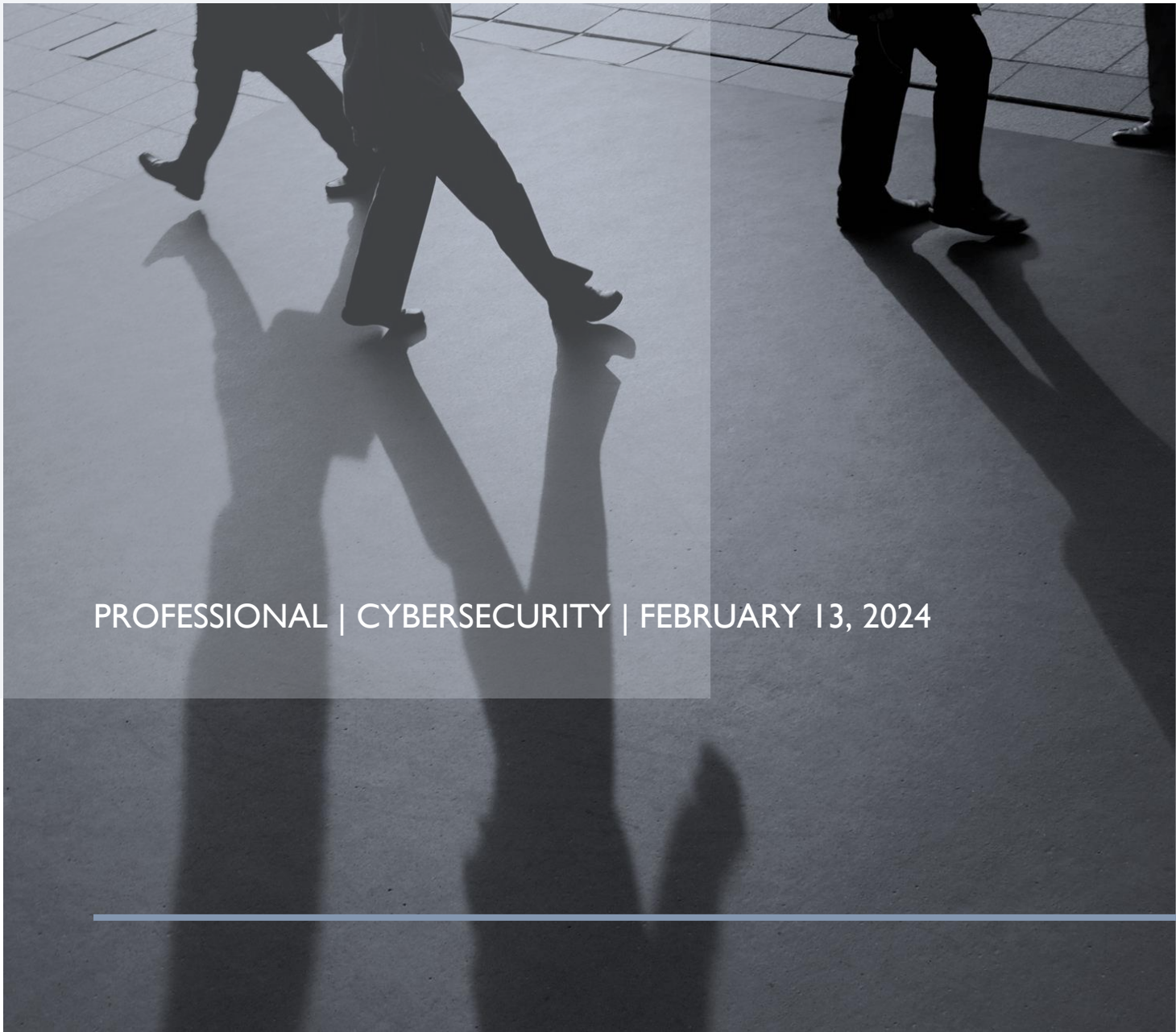
FOOTPRINTING

BY JAMES ROBERSON



PROFESSIONAL | CYBERSECURITY | FEBRUARY 13, 2024

WHAT HAPPENED?

As agreed, I can access all ports but for only one specific IP. All ports are scanned using the network mapper and the output is saved into a text file. Once completing the Nmap tool, you also wanted me to run multiple tools against your network. In this case, I decided with Rustscan; a highly powerful, fast tool. Much like Nmap except Rustscan can scan all ports within a matter of seconds (developers of Rustscan are very proud of this). They have full support for scripting engines, meaning we can pip Nmap scripts together with the alias of our Rustscan (unless you've opted-in to type out each command each time). It also uses basic math as adaptive learning to keep the experience fast and concise.

- Scanned all ports using Network Mapper. Check.
- Studied and researched a new tool despite Nmap. Check.
- Used that new tool to run similar Nmap scans. Check and check.

After running my Nmap scripts, as shown in Figure 1, I went on to discover those same ports but with a new tool, Rustscan. To install Rustscan, I navigated to the README page of Rustscan's GitHub and made my way to installation. Here, I began looking for a way to get Rustscan onto my Linux machine. One way that recommended was Docker. So I went, installed docker (Figure 2), and attempted to pull request the ready image from Rustscan's releases page in Figures 3 and 4. However, I kept running into denied permissions. What could be the issue? Upon further research, I found that sometimes the path for the docker image isn't configured with the permissions I need. Instead of going through the fixes in Figure 4, I decided to download an older released version, 2.0.1; it's a Debian file. Since it's Debian I simply navigated to the download's directory, de-packaged the file and ran it in Figure 6.

I ran a script for all ports against my target machine and yielded the results of Figures 7 and 8. Rustscan returned the number of ports running, which ports are running, the version of service they're running, and even the syn-ack responses. In summary, Rustscan is an extremely robust tool due to the fact it can run on any operating system while continuing to be as fast as it is. Nmap is a go to tool, built into Kali for ethical penetration testing, yes, but Rustscan is preferred because of the various scripts that it can run as well as its ability to pip those scripts to Nmap scripts for a more narrow, deeper, direct scan.

PROOF:

```
┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ nmap -p- -A 10.0.2.9 -oN Metasploitable3AllPorts.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 20:55 CST
Nmap scan report for 10.0.2.9
Host is up (0.0061s latency).
Not shown: 65511 closed tcp ports (conn-refused)
PORT     STATE SERVICE            VERSION
21/tcp   open  ftp                Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
22/tcp   open  ssh                OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 fd:08:98:ca:3c:e8:c1:3c:ea:dd:09:1a:2e:89:a5:1f (RSA)
|_  521 7e:57:81:8e:f6:3c:1d:cf:eb:7d:ba:d1:12:31:b5:a8 (ECDSA)
80/tcp   open  http               Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds       Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
3306/tcp open  mysql              MySQL 5.5.20-log
| mysql-info:
|   Protocol: 10
|   Version: 5.5.20-log
|   Thread ID: 8
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, FoundRows, ODBCClient, LongColumnFlag, LongPassword, Speaks41ProtocolNew, InteractiveClient, IgnoreSpaceBeforeParenthesis, ConnectWithDa
wDatabaseTableColumn, SupportsLoadDataLocal, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatements
|   Status: Autocommit
|   Salt: E!sC5|78Sz,iO0@pd'0
|_  Auth Plugin Name: mysql_native_password
3389/tcp open  ssl/ms-wbt-server?
|_ssl-date: 2024-02-13T03:01:02+00:00; +1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: VAGRANT-2008R2
|   NetBIOS_Domain_Name: VAGRANT-2008R2
|   NetBIOS_Computer_Name: VAGRANT-2008R2
|   DNS_Domain_Name: vagrant-2008R2
|   DNS_Computer_Name: vagrant-2008R2
|   Product_Version: 6.1.7601
|_  System_Time: 2024-02-13T03:00:47+00:00
| ssl-cert: Subject: commonName=vagrant-2008R2
| Not valid before: 2024-02-05T01:43:38
|_Not valid after:  2024-08-06T01:43:38
5985/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8009/tcp open  ajp13              Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8020/tcp open  http               Apache httpd
|_http-title: 503 Service Unavailable
|_http-server-header: Apache
8027/tcp open  papachi-p2p-srv?
8282/tcp open  http               Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
```

```
┌──(bitman㉿KaliII)-[~]
└─$ echo james
james

┌──(bitman㉿KaliII)-[~]
└─$
```

Figure 1.

```
bitman@KaliII: ~/Desktop
File  Actions  Edit  View  Help
ll_ports_scan  backdoor.py  deep_scan  EternalBlue  RED_HAWK  routersploit  sherlock  tools  version_output

┌──(bitman㉿KaliII)-[~/Desktop]
└─$ sudo apt install docker.io
[sudo] password for bitman:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  bluez-firmware cython3 debtags debugedit dh-elpa-helper firmware-atheros firmware-brcm80211 firmware-intel-sound firmware-iwlwifi firmware-libertas firmware-realtek firmware-sof-signed firmware-ti-connec
  gir1.2-javascriptcoregtk-4.0 gir1.2-libxfce4ui-2.0 gir1.2-libxfce4util-1.0 gir1.2-soup-2.4 gir1.2-webkit2-4.0 gobject-introspection gobject-introspection-bin kali-debtags kali-linux-firmware king-phisher
  libblockdev-fs2 libblockdev-loop2 libblockdev-part-err2 libblockdev-part2 libblockdev-swap2 libblockdev-utils2 libblockdev2 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libcfitsio9 libcurl3-nss lib
  libgupnp-igd-1.0-4 libjavascriptcoregtk-4.0-18 libjim0.81 libllvm15:i386 libllvm16:i386 libmagickcore-6.q16-6 libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libmount-dev libmpdec3 libnfs13 libobjc-12-
  libpoppler123 libprotobuf23 libpython3.10 libpython3.10-minimal libpython3.10-stdlib librtlsdr0 libselinux1-dev libsepol-dev libsoup-gnome2.4-1 libspatialite7 libsuperlu5 libtexluajit2 libtiff5 libucl1 l
  libzxingcore1 lua-lpeg nss-plugin-pem perl-modules-5.36 php8.1-mysql pwgen python-pastedeploy-tpl python3-advancedhttpserver python3-backcall python3-boltons python3-cairo-dev python3-commonmark python3-
  python3-geojson python3-graphene python3-graphene-sqlalchemy python3-graphql-core python3-graphql-relay python3-icalendar python3-maxminddb python3-pickleshare python3-requests-toolbelt python3-rfc3986 p
  python3-unicodecsv ruby3.0 ruby3.0-dev ruby3.0-doc tftp uuid-dev
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  cgroupfs-mount containerd libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl libproc-processtable-perl libsort-naturally-perl needrestart runc tini
Suggested packages:
  containernetworking-plugins docker-doc aufs-tools btrfs-progs debootstrap rinse rootlesskit xfsprogs zfs-fuse | zfsutils-linux
Recommended packages:
  criu
The following NEW packages will be installed:
  cgroupfs-mount containerd docker.io libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl libproc-processtable-perl libsort-naturally-perl needrestart runc tini
0 upgraded, 12 newly installed, 0 to remove and 47 not upgraded.
Need to get 67.8 MB of archives.
After this operation, 272 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 runc amd64 1.1.12+ds1-1 [2,757 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 containerd amd64 1.6.24~ds1-1 [26.9 MB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 docker.io amd64 20.10.25+dfsg1-2+b3 [37.0 MB]
Get:5 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 cgroupfs-mount all 1.4 [6,276 B]
Get:10 http://http.kali.org/kali kali-rolling/main amd64 libproc-processtable-perl amd64 0.636-1+b1 [42.2 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 tini amd64 0.19.0-1 [255 kB]
Get:7 http://http.kali.org/kali kali-rolling/main amd64 libintl-xs-perl amd64 1.33-1+b1 [15.5 kB]
Get:12 http://kali.download/kali kali-rolling/main amd64 needrestart all 3.6-7 [59.7 kB]
Get:6 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 libintl-perl all 1.33-1 [720 kB]
Get:8 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 libmodule-find-perl all 0.16-2 [10.6 kB]
Get:9 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 libmodule-scandeps-perl all 1.35-1 [43.7 kB]
Get:11 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 libsort-naturally-perl all 1.03-4 [13.1 kB]
Fetched 67.8 MB in 10s (7,126 kB/s)
Selecting previously unselected package runc.
(Reading database ... 435432 files and directories currently installed.)
Preparing to unpack .../00-runc_1.1.12+ds1-1_amd64.deb ...
Unpacking runc (1.1.12+ds1-1) ...
Selecting previously unselected package containerd.
Preparing to unpack .../01-containerd_1.6.24~ds1-1_amd64.deb ...
Unpacking containerd (1.6.24~ds1-1) ...
Selecting previously unselected package tini.
Preparing to unpack .../02-tini_0.19.0-1_amd64.deb ...
Unpacking tini (0.19.0-1) ...
Selecting previously unselected package docker.io.
Preparing to unpack .../03-docker.io_20.10.25+dfsg1-2+b3_amd64.deb ...
Unpacking docker.io (20.10.25+dfsg1-2+b3) ...
Selecting previously unselected package cgroupfs-mount.
Preparing to unpack .../04-cgroupfs-mount_1.4_all.deb ...
```

Figure 2.

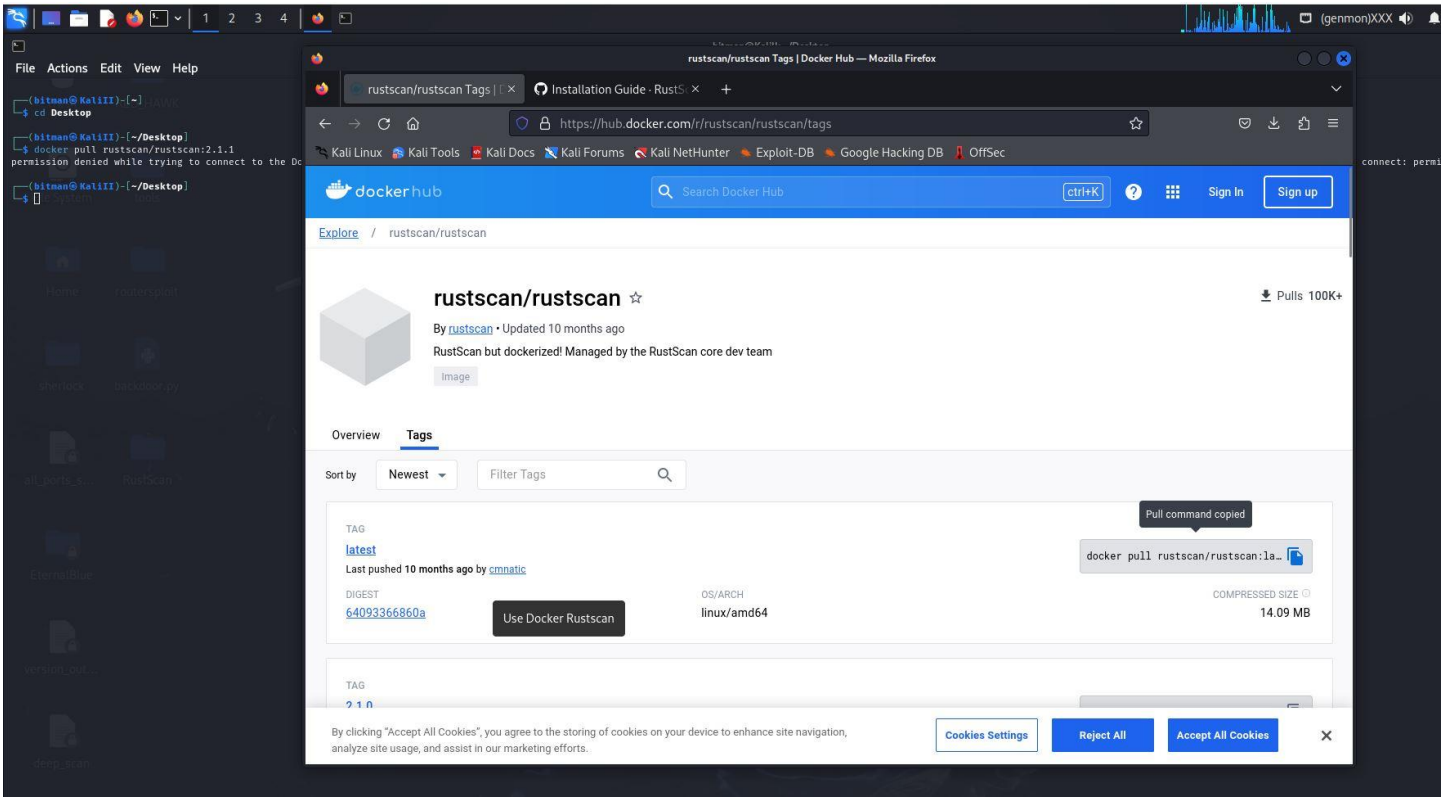


Figure 3.

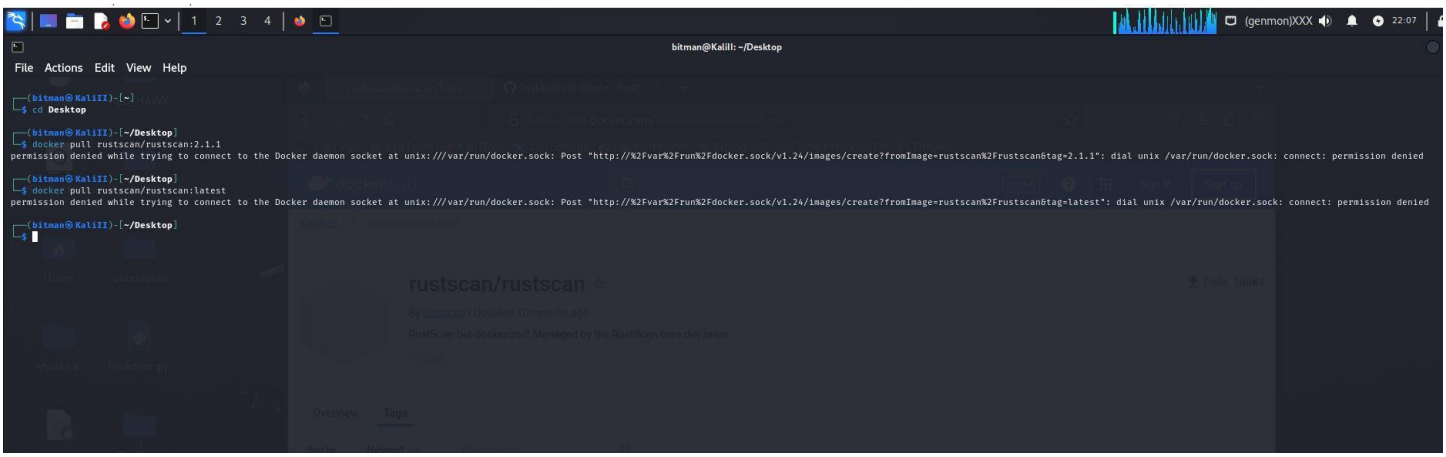


Figure 4.

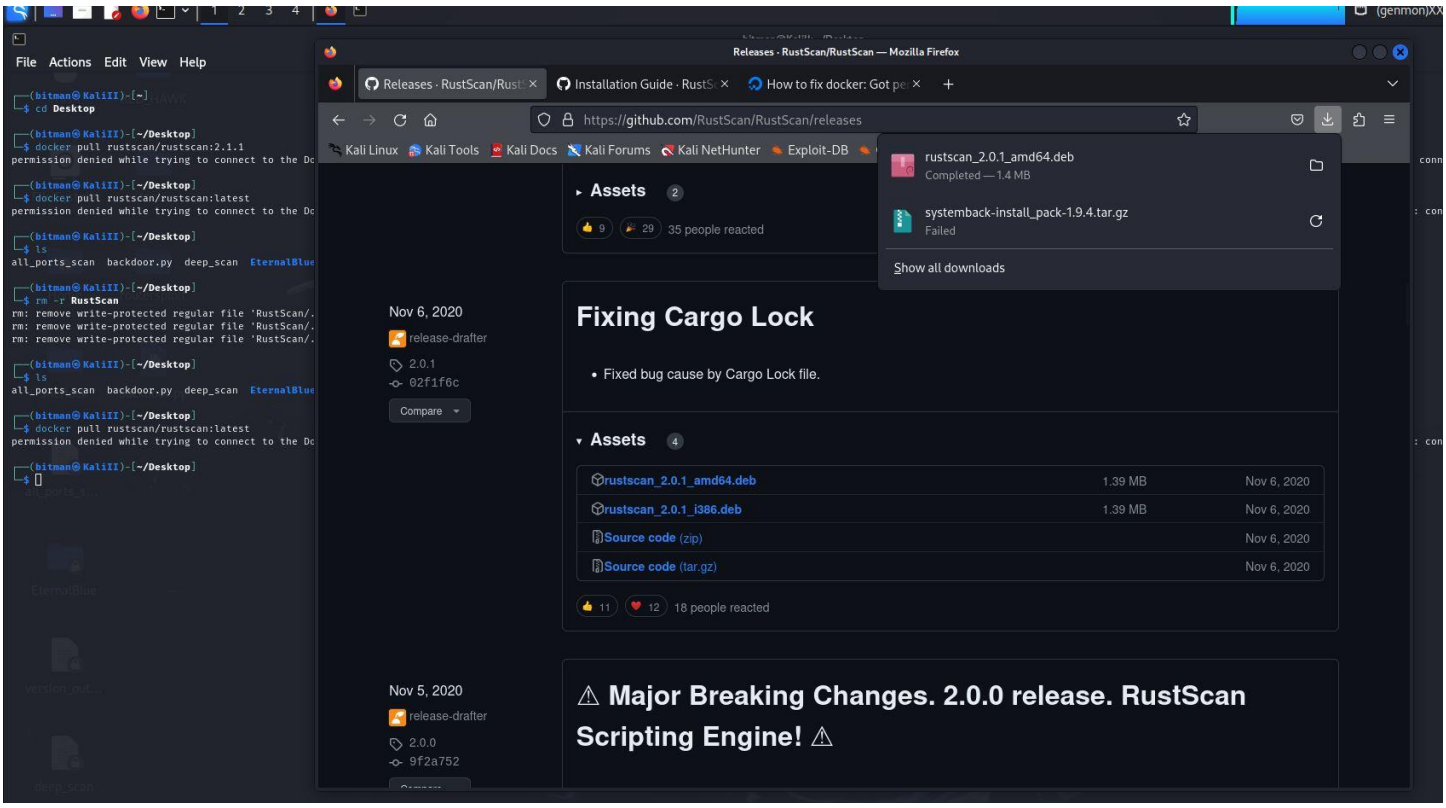


Figure 5.

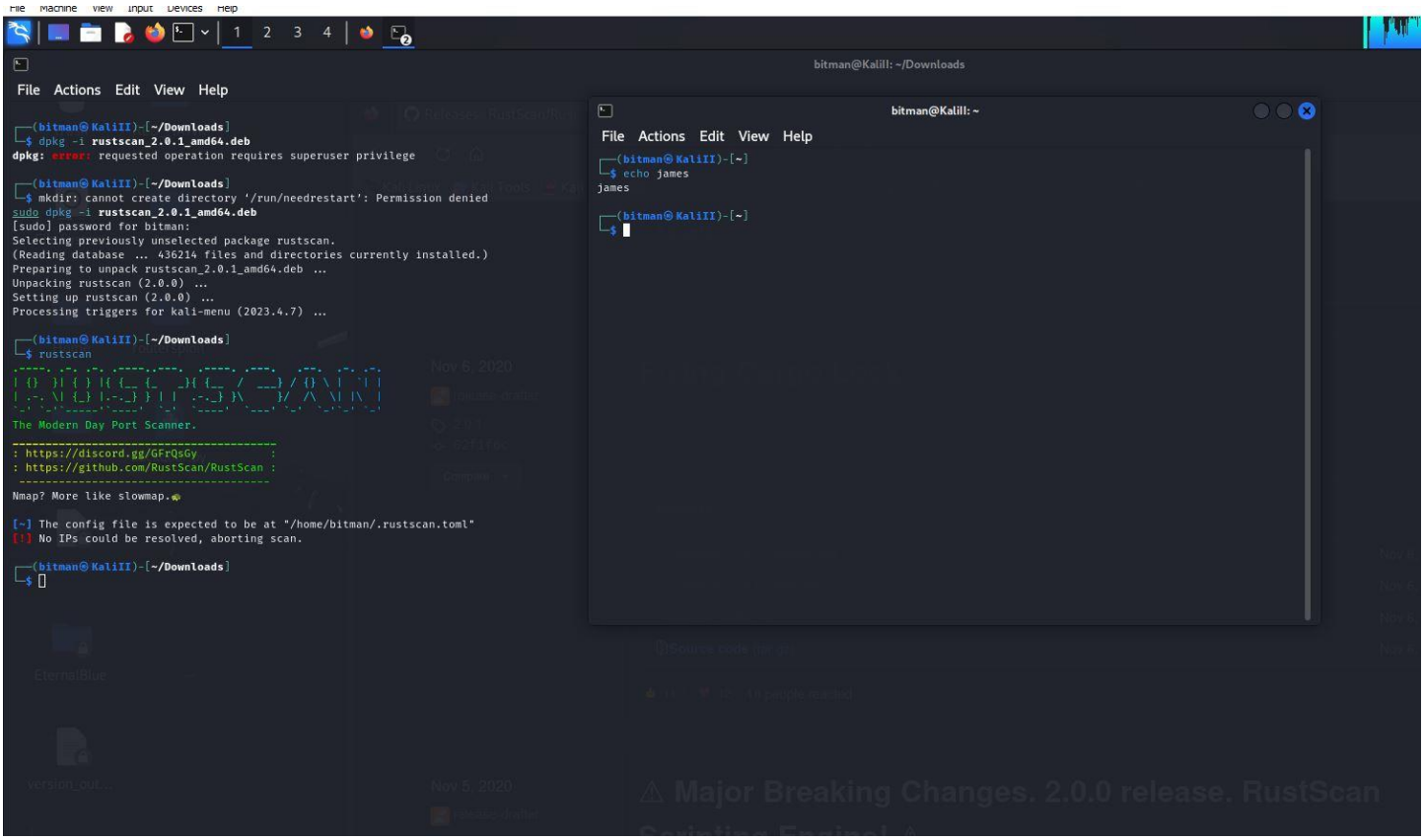

File Machine View Input Devices Help
1 2 3 4
bitman@KaliII: ~/Downloads
File Actions Edit View Help
┌──(bitman㉿KaliII)-[~/Downloads]
└─$ dpkg -i rustscan_2.0.1_amd64.deb
dpkg: error: requested operation requires superuser privilege
┌──(bitman㉿KaliII)-[~/Downloads]
└─$ mkdir: cannot create directory '/run/needrestart': Permission denied
sudo dpkg -i rustscan_2.0.1_amd64.deb
[sudo] password for bitman:
Selecting previously unselected package rustscan.
(Reading database ... 436214 files and directories currently installed.)
Preparing to unpack rustscan_2.0.1_amd64.deb ...
Unpacking rustscan (2.0.0) ...
Setting up rustscan (2.0.0) ...
Processing triggers for kali-menu (2023.4.7) ...
┌──(bitman㉿KaliII)-[~/Downloads]
└─$ rustscan
The Modern Day Port Scanner.
: https://discord.gg/GFrQsGy :
: https://github.com/RustScan/RustScan :
Nmap? More like slowmap.
[~] The config file is expected to be at "/home/bitman/.rustscan.toml"
[!] No IPs could be resolved, aborting scan.
┌──(bitman㉿KaliII)-[~/Downloads]
└─$
bitman@KaliII: ~
File Actions Edit View Help
┌──(bitman㉿KaliII)-[~]
└─$ echo james
james
┌──(bitman㉿KaliII)-[~]
└─$

Figure 6.

```
┌──(bitman㉿KaliII)-[~/Downloads]
└─$ rustscan -r 1-65536 -a 10.0.2.9
error: Invalid value for '--range <range>': the range format must be 'start-end'. Example: 1-1000.

┌──(bitman㉿KaliII)-[~/Downloads]
└─$ rustscan -r 1-65535 -a 10.0.2.9
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
-------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com

[~] The config file is expected to be at "/home/bitman/.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 10.0.2.9:22
Open 10.0.2.9:80
Open 10.0.2.9:135
Open 10.0.2.9:445
Open 10.0.2.9:3306
Open 10.0.2.9:3389
Open 10.0.2.9:5985
Open 10.0.2.9:8009
Open 10.0.2.9:8020
Open 10.0.2.9:8027
Open 10.0.2.9:8282
Open 10.0.2.9:8383
Open 10.0.2.9:8585
Open 10.0.2.9:9200
Open 10.0.2.9:9300
Open 10.0.2.9:47001
Open 10.0.2.9:49153
Open 10.0.2.9:49155
Open 10.0.2.9:49152
Open 10.0.2.9:49154
Open 10.0.2.9:49156
Open 10.0.2.9:49157
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 22:50 CST
Initiating Ping Scan at 22:50
Scanning 10.0.2.9 [2 ports]
Completed Ping Scan at 22:50, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:50
Completed Parallel DNS resolution of 1 host. at 22:50, 0.01s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 22:50
Scanning 10.0.2.9 [22 ports]
Discovered open port 445/tcp on 10.0.2.9
Discovered open port 80/tcp on 10.0.2.9
Discovered open port 22/tcp on 10.0.2.9
```

Figure 7.

```
File  Actions  Edit  View  Help
Completed Parallel DNS resolution of 1 host. at 22:50, 0.01s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 22:50
Scanning 10.0.2.9 [22 ports]
Discovered open port 445/tcp on 10.0.2.9
Discovered open port 80/tcp on 10.0.2.9
Discovered open port 22/tcp on 10.0.2.9
Discovered open port 3389/tcp on 10.0.2.9
Discovered open port 3306/tcp on 10.0.2.9
Discovered open port 135/tcp on 10.0.2.9
Discovered open port 49155/tcp on 10.0.2.9
Discovered open port 49157/tcp on 10.0.2.9
Discovered open port 49152/tcp on 10.0.2.9
Discovered open port 49153/tcp on 10.0.2.9
Discovered open port 8009/tcp on 10.0.2.9
Discovered open port 49156/tcp on 10.0.2.9
Discovered open port 9300/tcp on 10.0.2.9
Discovered open port 8383/tcp on 10.0.2.9
Discovered open port 47001/tcp on 10.0.2.9
Discovered open port 8020/tcp on 10.0.2.9
Discovered open port 9200/tcp on 10.0.2.9
Discovered open port 5985/tcp on 10.0.2.9
Discovered open port 49154/tcp on 10.0.2.9
Discovered open port 8282/tcp on 10.0.2.9
Discovered open port 8027/tcp on 10.0.2.9
Discovered open port 8585/tcp on 10.0.2.9
Completed Connect Scan at 22:50, 0.13s elapsed (22 total ports)
Nmap scan report for 10.0.2.9
Host is up, received syn-ack (0.019s latency).
Scanned at 2024-02-12 22:50:05 CST for 0s

PORT      STATE SERVICE         REASON
22/tcp    open  ssh             syn-ack
80/tcp    open  http            syn-ack
135/tcp   open  msrpc           syn-ack
445/tcp   open  microsoft-ds    syn-ack
3306/tcp  open  mysql           syn-ack
3389/tcp  open  ms-wbt-server   syn-ack
5985/tcp  open  wsman           syn-ack
8009/tcp  open  ajp13           syn-ack
8020/tcp  open  intu-ec-svcdisc syn-ack
8027/tcp  open  papachi-p2p-srv syn-ack
8282/tcp  open  libelle         syn-ack
8383/tcp  open  m2mservices     syn-ack
8585/tcp  open  unknown         syn-ack
9200/tcp  open  wap-wsp         syn-ack
9300/tcp  open  vrace           syn-ack
47001/tcp open  winrm           syn-ack
49152/tcp open  unknown         syn-ack
49153/tcp open  unknown         syn-ack
49154/tcp open  unknown         syn-ack
49155/tcp open  unknown         syn-ack
49156/tcp open  unknown         syn-ack
49157/tcp open  unknown         syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Figure 8.