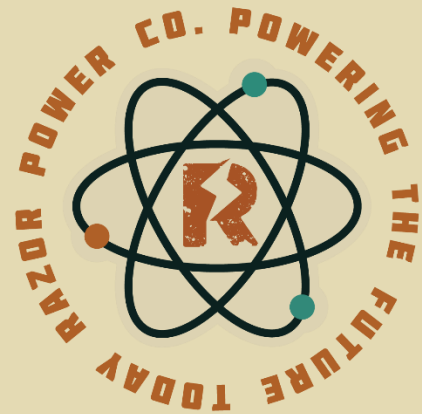


# RazorHack 2024

## Writeup



### “A Good Student Does His Homework” & “You Need It? I Got It”

*RPCO-M-41x01-10*

*a.k.a. Network Recon*

RazorPower Co. CIO Shane Barnabas has hired you and your team of private security consultants to help him figure out who or what is causing weird occurrences at RPCo's new reactor plants.

Your first task? Do some network reconnaissance of the RPCo IT network and see what you can find.

Author: Henry

In this challenge, participants are tasked with finding all the active IPs and services on the IT network of RazorPower Co. This involved using the NetLab environment each team was provided where three Kali Linux boxes and Tiberius's workstation were provided. In an incident response scenario, you need to know what kind of systems, services, and devices you are dealing with. Most of the time this could be provided in briefing material, but we want you as the competitor to use the tools to do this yourself. One of the most common tools that many people jump to is *nmap*.

For the first challenge we are just looking to find which hosts on the network are up. This can be accomplished relatively quickly by using the *nmap -sn {net}* command.

```
└─$ nmap -sn 192.168.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-30 13:31 CDT
Nmap scan report for pfsense-01-internet-it.razorpowerco.com (192.168.2.1)
Host is up (0.00024s latency).
MAC Address: 00:50:56:B7:19:55 (VMware)
Nmap scan report for 192.168.2.2
Host is up (0.00013s latency).
MAC Address: 00:50:56:B7:CE:CD (VMware)
Nmap scan report for 192.168.2.16
Host is up (0.00015s latency).
MAC Address: 00:50:56:B7:C3:C3 (VMware)
Nmap scan report for 192.168.2.17
Host is up (0.00013s latency).
MAC Address: 00:50:56:B7:39:72 (VMware)
Nmap scan report for 192.168.2.134
Host is up (0.00015s latency).
MAC Address: 02:42:C0:A8:02:B6 (Unknown)
Nmap scan report for 192.168.2.165
Host is up (0.00012s latency).
MAC Address: 00:50:56:B7:08:36 (VMware)
Nmap scan report for 192.168.2.171
Host is up (0.00017s latency).
MAC Address: 02:42:C0:A8:02:AB (Unknown)
Nmap scan report for 192.168.2.180
Host is up (0.00015s latency).
MAC Address: 02:42:C0:A8:02:B4 (Unknown)
Nmap scan report for 192.168.2.200
Host is up (0.00015s latency).
MAC Address: 02:42:C0:A8:02:C8 (Unknown)
Nmap scan report for 192.168.2.201
Host is up (0.00022s latency).
MAC Address: 02:42:C0:A8:02:C9 (Unknown)
Nmap scan report for 192.168.2.202
Host is up (0.00020s latency).
MAC Address: 02:42:C0:A8:02:CA (Unknown)
Nmap scan report for 192.168.2.203
Host is up (0.00020s latency).
MAC Address: 02:42:C0:A8:02:CB (Unknown)
Nmap scan report for 192.168.2.231
Host is up (0.00022s latency).
MAC Address: 02:42:C0:A8:02:E7 (Unknown)
Nmap scan report for 192.168.2.240
Host is up (0.00024s latency).
MAC Address: 02:42:C0:A8:02:F0 (Unknown)
Nmap scan report for 192.168.2.15
Host is up.
Nmap done: 256 IP addresses (15 hosts up) scanned in 1.90 seconds
```

You can see in the results we have 15 different hosts up on the 192.168.2.0/24 network. These 15 hosts are the flag for the first challenge *"A Good Student Does His Homework"*.

The next objective in *"You Need It? I Got It"* is to identify all the services that are running on the network. By services we mean anything that has an open port with some kind of software running on it. This could be web servers, FTP ports, DNS, or anything else active on a port on the network. To identify these, we can use a **nmap services detection scan** (`nmap -sV {net}`). You'll notice this scan takes a lot longer to complete. This scan checks the first 1000 ports on each of the active hosts of the specified network.

```
(root@kali) - [~]
# nmap -sV 192.168.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-30 13:39 CDT
Nmap scan report for pfsense-01-internet-it.razorpowerco.com (192.168.2.1)
Host is up (0.00020s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq 2.86
80/tcp    open  http    nginx
MAC Address: 00:50:56:B7:19:55 (VMware)

Nmap scan report for 192.168.2.2
Host is up (0.00013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq 2.86
80/tcp    open  http    nginx
MAC Address: 00:50:56:B7:CE:CD (VMware)

Nmap scan report for 192.168.2.16
Host is up (0.000059s latency).
All 1000 scanned ports on 192.168.2.16 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:50:56:B7:C3:C3 (VMware)

Nmap scan report for 192.168.2.17
Host is up (0.000054s latency).
All 1000 scanned ports on 192.168.2.17 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:50:56:B7:39:72 (VMware)

Nmap scan report for 192.168.2.134
Host is up (0.000051s latency).
All 1000 scanned ports on 192.168.2.134 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:42:C0:A8:02:B6 (Unknown)

Nmap scan report for 192.168.2.165
Host is up (0.000061s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 00:50:56:B7:0B:36 (VMware)

Nmap scan report for 192.168.2.171
Host is up (0.000058s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.62 ((Debian))
MAC Address: 02:42:C0:A8:02:AB (Unknown)

Nmap scan report for 192.168.2.180
Host is up (0.000053s latency).
All 1000 scanned ports on 192.168.2.180 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:42:C0:A8:02:B4 (Unknown)
```

You'll also notice some longer outputs from "unrecognized services". Some of these are custom TCP servers we created for our training challenges. You can see in the dump the console commands the server sends to nmap as it probes the service.

```
Nmap scan report for 192.168.2.203
Host is up (0.000055s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
9999/tcp  open  abyss?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9999-TCP:V=7.94SVNXI=7ND=10/30XTime=67227079XP=x86_64-pc-linux-gnu%
SF:r\NULL,D3,"welcome\x20to\x20the\x20Advanced\x20Math\x20Challenge!\nSolv
SF:e\x20all\x20problems\x20correctly\x20to\x20get\x20the\x20flag\.\nTime\x
SF:20per\x20question\x20decreases\x20as\x20you\x20progress\.\n\nDecode\x20
SF:and\x20solve:\n5XMGMTkWiGgCHjpbWugbnVtYmVvPyBBbnN3ZXIgj3llcycgb3Igj25v
SF:jy4=\n")\r(GetRequest,EE,"welcome\x20to\x20the\x20Advanced\x20Math\x20C
SF:hallenge!\nSolve\x20all\x20problems\x20correctly\x20to\x20get\x20the\x2
SF:0flag\.\nTime\x20per\x20question\x20decreases\x20as\x20you\x20progress\
SF:\.\n\nDecode\x20and\x20solve:\n5XMGMTkWiGgCHjpbWugbnVtYmVvPyBBbnN3ZXIgj
SF:3llcycgb3Igj25vjy4=\nIncorrect\x20answer\.\x20Goodbye!\n")\r(HTTPoition
SF:s,DE,"welcome\x20to\x20the\x20Advanced\x20Math\x20Challenge!\nSolve\x20
SF:all\x20problems\x20correctly\x20to\x20get\x20the\x20flag\.\nTime\x20per
SF:\x20question\x20decreases\x20as\x20you\x20progress\.\n\nDecode\x20and\x
SF:20solve:\nv2hhdCBpcyB0aGUGR0NEIG9mIDM5M1BhbmQzM4Pw=\nIncorrect\x20an
SF:swer\.\x20Goodbye!\n")\r(FourOhFourRequest,EE,"welcome\x20to\x20the\x20
SF:Advanced\x20Math\x20Challenge!\nSolve\x20all\x20problems\x20correctly\x
SF:20to\x20get\x20the\x20flag\.\nTime\x20per\x20question\x20decreases\x20a
SF:s\x20you\x20progress\.\n\nDecode\x20and\x20solve:\n5XMGNTYgY5BwcltZ5Bu
SF:dw1iZXi/IEFuc3dlciAneWVzJyBvcjAnbmBnLg=\nIncorrect\x20answer\.\x20Good
SF:bye!\n")\r(JavaRMI,EE,"welcome\x20to\x20the\x20Advanced\x20Math\x20Chal
SF:lenge!\nSolve\x20all\x20problems\x20correctly\x20to\x20get\x20the\x20fl
SF:ag\.\nTime\x20per\x20question\x20decreases\x20as\x20you\x20progress\.\n
SF:\nDecode\x20and\x20solve:\n5XMGNTYgY5BwcltZ5BudW1iZXi/IEFuc3dlciAneWVz
SF:jyBvcjAnbmBnLg=\nIncorrect\x20answer\.\x20Goodbye!\n")\r(GenericLines,
SF:DE,"welcome\x20to\x20the\x20Advanced\x20Math\x20Challenge!\nSolve\x20al
SF:l\x20problems\x20correctly\x20to\x20get\x20the\x20flag\.\nTime\x20per\x
SF:20question\x20decreases\x20as\x20you\x20progress\.\n\nDecode\x20and\x20
SF:solve:\nv2hhdCBpcyB0aGUGR0NEIG9mIDM1BhbmQzMzA2Pw=\nIncorrect\x20answ
SF:er\.\x20Goodbye!\n")\r(RTSPRequest,DE,"welcome\x20to\x20the\x20Advanced
SF:\x20Math\x20Challenge!\nSolve\x20all\x20problems\x20correctly\x20to\x20
SF:get\x20the\x20flag\.\nTime\x20per\x20question\x20decreases\x20as\x20you
SF:\x20progress\.\n\nDecode\x20and\x20solve:\nv2hhdCBpcyB0aGUGR0NEIG9mIDIS
SF:OSBhbmQzMtA3Pw=\nIncorrect\x20answer\.\x20Goodbye!\n");
MAC Address: 02:42:C0:A8:02:CB (Unknown)
```

Many of you submitted all the information from this first service scan as the flag. However, this scan is incomplete. If you talked to me during the competition or pinged me about your flag you'll notice I asked you a question; what's the available port range for service? This should have prompted you to check the range of numbers that a port can be set to which is 0-65535. You'll then see that the first scan was incomplete and only scanned the first 1000 or 10000 ports of the host. You can then retry your scan with the following modifier: *nmap -sV -p- {net}*. This tells nmap to check all available ports on each host. Using this you will find your missing service on port 11543 on host 192.168.2.180

```
Nmap scan report for 192.168.2.180
Host is up (0.00013s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
11543/tcp  open  tcpwrapped
MAC Address: 02:42:C0:A8:02:B4 (Unknown)
```