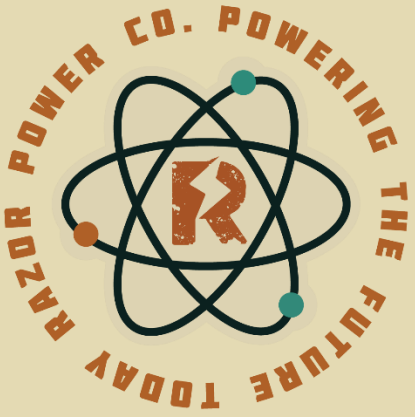
RazorHack 2024 Writeup



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

RPCO-M-41x01-10

a.k.a. Network Recon

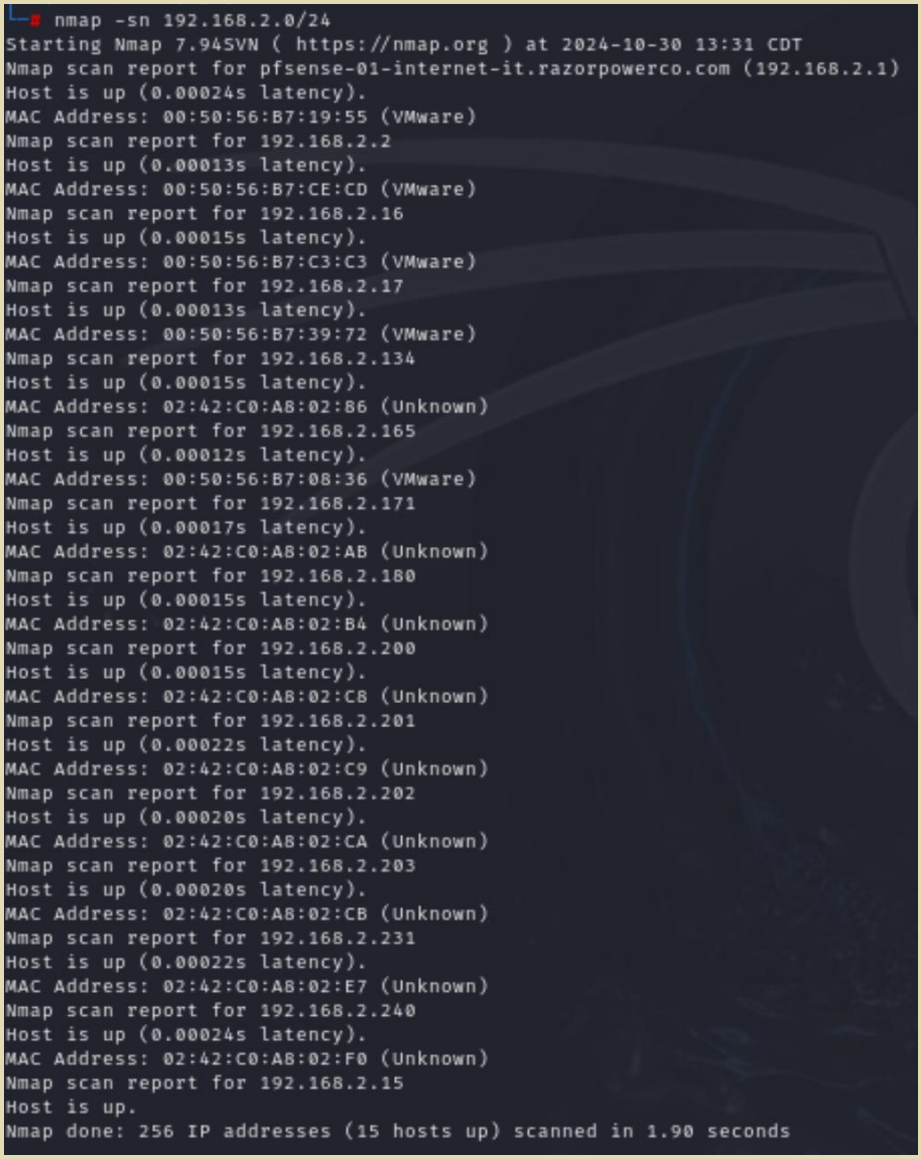
RazorPower Co. CIO Shane Barnabas has hired you and your team of private security consultants to help him figure out who or what is causing weird occurrences at RPCo’s new reactor plants.

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

Author: Henry

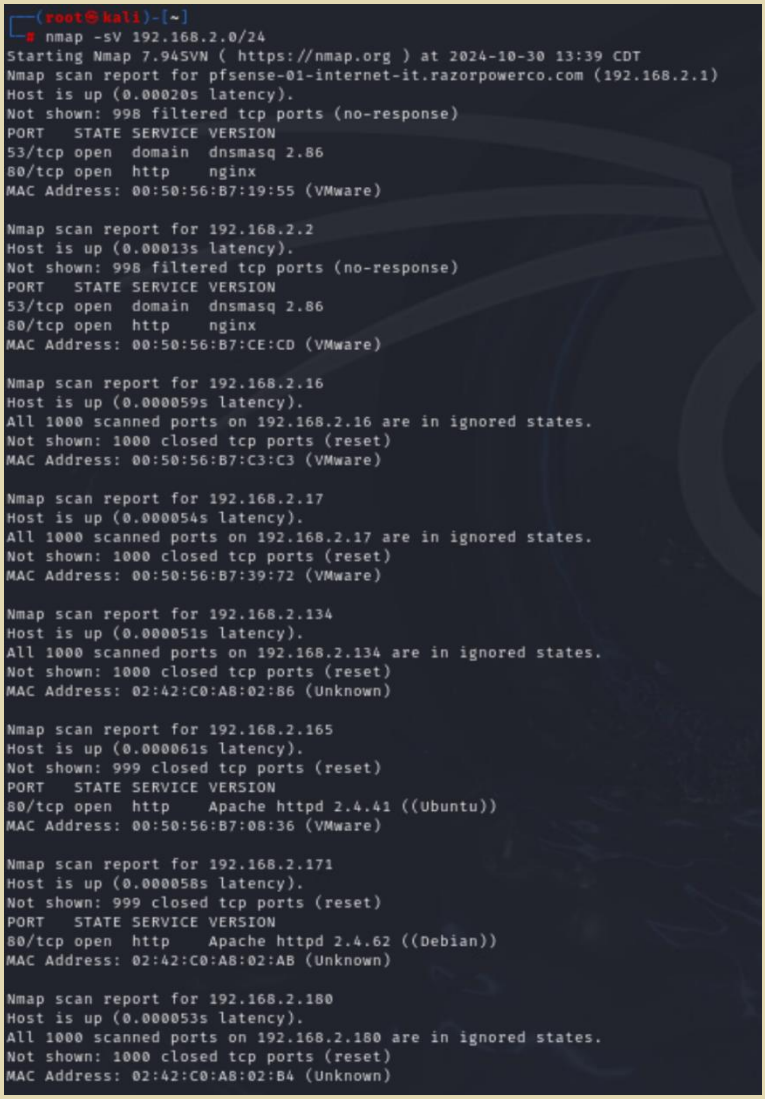
In this challenge, participants are tasked with finding all the active IPs and services on the IT network of RazorPower Co. This involved using the NetLab environment each team was provided where three Kali Linux boxes and Tiberius's workstation were provided. In an incident response scenario, you need 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.



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 webservers, 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.



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.

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