

**Introduction**

Irked est une machine linux dont l’adresse IP est 10.10.10.117.

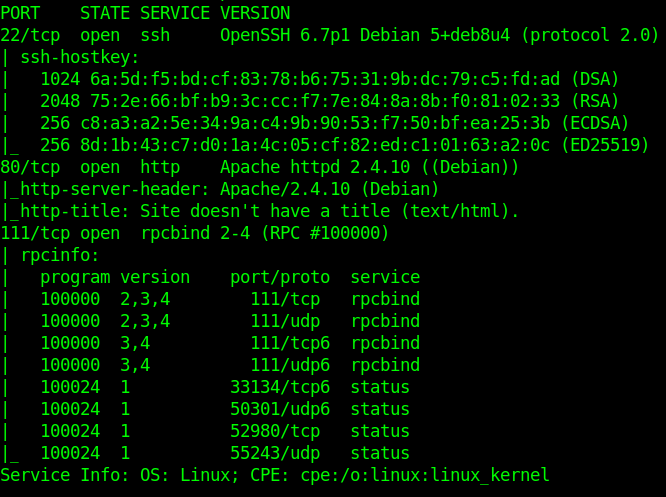
Compétences mises en œuvre :

* Enumération des ports et services.
* Repérer un service faillible.
* Recherche et exploitation avec metasploit.
* Recherche d’information dans une image.
* Elévation de privilège via un fichier ayant le bit SUID.

**Enumération initiale**

On commence par une énumération des ports et services de la machine distante avec nmap :

|  |
| --- |
| $ nmap -T4 -A 10.10.10.117 |



Plusieurs ports sont ouverts :

* 22 pour un serveur ssh.
* 80 pour un serveur web.
* 111 pour un serveur RPC.

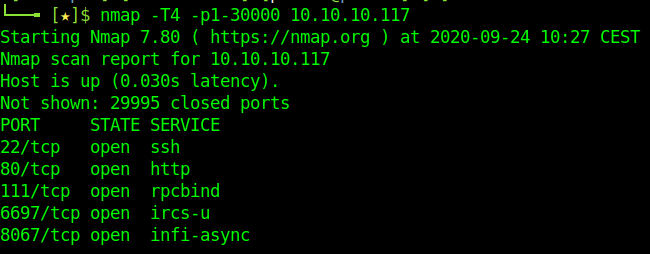
**Obtenir un accès utilisateur**

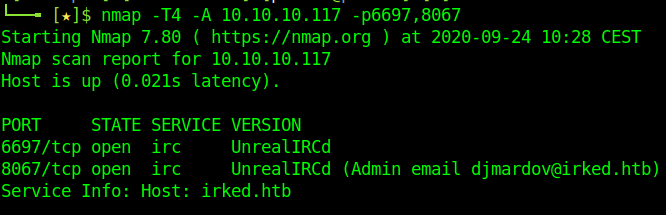
Nous allons aller directement sur le site web, nous avons juste une image et un texte relatant qu’IRC fonctionne à peu près :



IRC en général est dans les ports 6665-6669, nous allons refaire un nmap pour voir si ces ports répondent :

|  |
| --- |
| $ nmap -T4 -p1-30000 10.10.10.117  $ nmap -T4 -A 10.10.10.117 -p6697,8067 |





Le nmap révèle un port pour IRC, plus particulièrement le service UnrealIRCd. Nous allons rechercher avec searchsploit si des exploits sont disponibles pour ce service :

|  |
| --- |
| $ searchsploit unrealIRCd |



Plusieurs exploit sont disponible dont une backdoor sous metasploit que nous allons tenter :

|  |
| --- |
| $ msfconsole  Msf> search unrealircd  Msf > use exploit/unix/irc/unreal\_ircd\_3281\_backdoor |

**Obtenir un accès administrateur**

Bla