Rapport de Certification eLearnSecurity Certified Professional Penetration Tester (eCPPTv3)

Nom : Morad Halmi
Statut : Étudiant à École 2600
Certification : eCPPTv3 – eLearnSecurity Certified Professional Penetration Tester
Lien de vérification : https://www.credential.net/d12bd51b-a46f-465b-a0a0-864836ebbabe#acc.YSC4fPQl

---

📌 Contexte

L'eCPPTv3 (eLearnSecurity Certified Professional Penetration Tester) évalue la capacité à mener un test d'intrusion complet sur une infrastructure simili-entreprise. Il ne s'agit pas d'un challenge CTF : c'est un environnement opérationnel, à pénétrer, escalader, et compromettre de bout en bout, avec rédaction d'un rapport professionnel.

🧠 Approche

J'ai traité l'examen comme une mission client :

- Recon complète (réseau, AD, web)
- Exploitation ciblée, pas de bruteforce inutile
- Mouvements latéraux multi-OS
- Escalade de privilèges locale et réseau
- Maintien d'accès
- Journalisation et prise de preuves continue

Objectif : **prise de contrôle totale avec preuves d'exploitation**.

🔎 Reconnaissance & Énumération

Recon active et passive dès les premières heures :

- `nmap` + `CrackMapExec` pour le scan de ports + fingerprinting SMB/RDP

- `rpcclient`, `enum4linux`, `GetNPUsers.py` pour l'énumération Active Directory
- Identification d'un contrôleur de domaine et de comptes Kerberoastables

Les données récupérées ont servi directement à l'exploitation.

🌐 Ciblage Web & Accès initial

Un serveur WordPress exposé m'a permis de rentrer :

- `wpscan` → plugin vulnérable → exploitation confirmée à la main
- Récupération de `wp-config.php` → dump MySQL
- Extraction de credentials → bruteforce ciblé → accès WinRM confirmé

⚙️ Post-Exploitation & Escalade

- `PowerUp.ps1` → détection de binaires avec autorisations incorrectes
- `certutil` pour l'import d'outils sans détection
- Extraction de hachages (`sam`, `security`, `system`) + `hashcat` pour crack
- Accès RDP via `xfreerdp`, exécution de payloads PowerShell

🔁 Mouvement latéral & Persistance

- Utilisation de creds récupérés pour pivoter en RDP et WinRM
- Persistance via webshells + services planifiés
- Enumeration réseau interne pour escalader vers le DC

🧰 Stack utilisée

Outils utilisés exclusivement :

- Recon : `nmap`, `CME`, `rpcclient`, `GetNPUsers.py`, `BloodHound`
- Web : `wpscan`, `dirsearch`, `burp`, `sqlmap`
- Exploit : `Metasploit`, `custom scripts`, `PowerUp.ps1`
- Post-Exploitation : `mimikatz`, `certutil`, `netsh`, `wmic`, `schtasks`
- Cracking : `john`, `hashcat`

- Pivot : `xfreerdp` , `WinRM` , `psexec.py` , `smbexec.py`

🎯 Conclusion

Examen exigeant mais réaliste. Pas de magie, pas de raccourcis.
Il faut penser comme un attaquant, agir comme un consultant.
Objectif : compromission complète + reporting professionnel.

Le eCPPTv3 m'a permis de valider mes méthodes, et ma capacité à mener un pentest complet, multi-vectoriel, de façon propre et documentée.

Morad Halmi
Pentester junior – Étudiant à l'École 2600