TP2: Attaque d'un réseau d'entreprise, pivoting et NTLM

Introduction :

Afin de mieux comprendre les rouages de sécurité qui entrent en jeux dans une entreprise, nous allons nous mettre dans la peau d'un attaquant et voir les différentes sécurités et vulnérabilités en place sur un réseau d'entreprise classique.
Le but du TP sera de passer Administrateur de domaine sur le réseau de l'entreprise ECorp.
L'entreprise ECorp dispose d'un réseau interne avec des serveurs windows à jour et toutes les machines windows sont protégées par un anti-virus à jour.
Un serveur linux hébergeant le site web extranet de l'entreprise est exposé sur internet, des règles de firewall assez strictes n'exposent que le port 80

Exercice 1 : Formulaire de contact

Après avoir évalué la surface d'exposition du site, le formulaire de contact vous semble vulnérable à une vulnérabilité classée dans le top 10 OWASP.
Recherchez et exploitez une vulnérabilité web sur le formulaire de contact pour prendre le contrôle de l'interface d'administration du site
L'administrateur du site est joignable via le formulaire de contact et lis régulièrement les messages envoyés par les employés ☺

Exercice 2 : Accès système

La partie d'administration du site comporte plusieurs pages intéressantes. Essayez de repérer une vulnérabilité qui permettrait d'évaluer du code et de prendre la main sur le système.

Exercice 3 : Shell

Malheureusement SSH est bloqué par le firewall ☹.
Obtenez un reverse shell sur le système en utilisant un outil comme pupy ou meterpreter.

Exercice 4 : Découverte du réseau interne

Scannez le réseau interne de l'entreprise afin d'énumérer les machines et services accessibles.
Cherchez en priorité les services qui ont l'air d'être :

- Vulnérables et référencés dans une CVE
- Fait maison ☺. Ces services sont en général peu testés et très souvent vulnérables.

Coup de chance nmap est installé sur la gateway ECorp !

Exercice 5 : Pivoting

Utilisez les fonctions de pivoting de pupy ou meterpreter pour investiguer les services WEB intéressants depuis votre machine.

Vous pouvez utiliser au choix :

- Le module forward de pupy :
  - forward –L 8118 pour créer un proxy socks localement
  - forward –L 1234 :<ip> :1234 pour forwarder un port
  - forward –R 1234 :<ip> :1234 pour ouvrir un port sur le serveur linux et le forwarder vers votre machine
- La fonction « portfwd » de meterpreter pour forwarder un port
- Le module auxiliary/server/socks4a pour créer un listener socks
-

NB : dans notre cas, pour simplifier vous n'avez pas besoin d'utiliser le remote port forward (-R). Dans un vrai réseau d'entreprise les machines internes ne peuvent pas parler directement sur internet et doivent passer par un proxy.

Exercice 6 : Capturez un challenge-response NTLM

Exploitez la SSRF et capturez un challenge-response NTLM.
Pour cela vous pouvez utiliser : responder -A -I <iface>
Essayez quelques minutes de casser le hash net-ntlm capturé.
Si vous n'y arrivez pas, le mot de passe est trop fort, passez à l'étape suivante !

Exercice 7 : Effectuer une attaque « NTLM relay » et exploitez le service vulnérable

Cette attaque fonctionne sur les réseaux windows à jour, dans leur configuration par défaut, depuis plus de 10 ans …
Identifiez une machine vulnérable au NTLM relay (sbm signing not mandatory) et exploitez ça.

- Utilisez ntlmrelayx.py de impacket avec l'option –c <commande> pour exploiter la vulnérabilité et lancer des commandes sur le windows.
- Déposez et lançez un payload pupy ou meterpreter sur le serveur windows.
- Attention : Il y a un anti-virus et le TP précédent sur les bypass AV vous sera utile ☺

Pivoting sur le domain windows :

Récupérez les mots de passe en mémoire via mimikatz. Si vous ne trouvez pas de mot de passe privilégié, trouvez un autre moyen de récupérer des credentials et de rebondir sur le contrôleur de domaine.

Bonus : dumper NTDS.dit

Récupérez tous les hashs des utilisateurs du domaine et crackez les ☺
Il y a plusieurs techniques, chosissez en une ! vssadmin, dcsync, …

Extra Bonus pour les warriors :

Allez sur /change_level.php, passez la difficulté du CTF à medium et recommencez le TP !