

RED TEAM LAB

CYBERTHREATFORCE v1



MACHINE RECAP

Réseau Local :

Hostname	IP	OS
Workstation-1	172.16.0.101	Windows-10
Workstation-2	172.16.0.102	Windows-10
Workstation-3	172.16.0.103	Windows-10
Workstation-4	172.16.0.104	Windows-10
Hostname	IP	OS
Evilbankdc	172.16.0.201	Windows Serveur 2019
Evilbankfiles	172.16.0.205	Windows Serveur 2019
Evilbankcloud (preprod)	172.16.0.113	Ubuntu Server 20.04
Evilbankweb (preprod)	172.16.0.114	Ubuntu Server 20.04

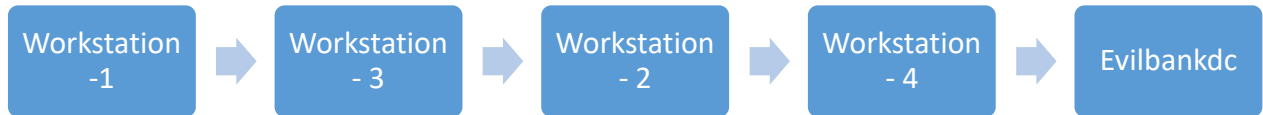
Admin Network :

Hostname	IP	OS
LogConcetrator	172.17.0.202	Linux/Windows

DMZ :

Hostname	IP	OS
MailServ01 (spoofing mail)	192.168.100.201	Ubuntu Server 20.04
EvilBankMail	192.168.100.202	Ubuntu Server 20.04
EvilBankWebPub	192.168.100.116	Ubuntu Server 20.04

Schéma Exploitation



Résumé du lab

DMZ :

Le joueur arrivera dans la partie VPN, il aura accès à la DMZ (MailServ01, EvilbankwebPub et evilbankmail).

Il aura un compte à MailServ01 qui servira pour envoyer des mails.

EvilBankWebPub aura un DNS (evilbank.com) pour permettre à l'utilisateur d'accéder à celle-ci.

La machine EvilBankWebPub sera un site vitrine de l'entreprise qui permettra à l'utilisateur d'avoir des informations sur l'entreprise.

EvilBankMail sera le serveur mail de l'entreprise, c'est ici que seront reçus les mails envoyés aux employés de l'entreprise.

Réseau Local :

C'est le réseau local de l'entreprise, les workstations sont les machines des utilisateurs de l'entreprise.

Evilbankdc est le domain controller de l'entreprise, Evilbankfiles est le serveur de fichier de l'entreprise c'est ici que seront les dossiers partagés avec samba.

Evilbankcloud(preprod) est un serveur en preprod, l'entreprise commence petit à petit à passer au cloud. Le serveur cloud est preprod certains utilisateurs commencent à l'utiliser pour tester le service.

Evilbankweb(preprod) l'entreprise met en place un site web en local, celui-ci est encore développement. Seulement un utilisateur) accès à celui-ci.

Exploitation du lab

Workstation-1 :

Pour commencer, l'attaquant devra énumérer le site web de l'entreprise (EvilBankWebPub). Sur le site il trouvera plusieurs adresses mail ainsi que des informations sur l'entreprise.

Pour exploiter cette machine, il faudra envoyer un mail de phishing à une personne de l'entreprise. Cependant toutes les pièces jointes ne seront pas ouvertes.

En effet, il faudra en premier lieu envoyer un email type demande d'information et l'utilisateur (employé de evilbank) reprendra avec un mail qui aura une signature de l'entreprise.

L'attaquant devra re-envoyer un mail en spoofant le mail par celui d'un autre salarié (présent sur le site web) avec la signature (obtenus lors du premier envoi de mail). Le mail devra contenir une pièce jointe avec un document word/excel contenant une macro avec un payload.

L'employé ouvrira le mail avec la pièce jointe qui donnera un accès à la machine, celui-ci aura un accès à un membre de l'OU Employees.

Une fois sur la machine, il devra énumérer les comptes présents dans DPAPI (Data Protection API) de Windows. Un compte sera enregistré sur Evilbankweb(preprod).

L'utilisateur utilise google chrome, il pourra obtenir les comptes via mimikatz ou sharpchromium.

Le compte obtenu permettra de se connecter sur le wordpress mais cependant il utilise le compte d'un utilisateur de l'OU Helpdesk.

Avec le compte de celui-ci je vais pouvoir faire un smbexec sur Workstation-3.

Workstation-3 :

La personnes sur cette ordinateur prepare un programme pour permettre une connection à une base de donnée distante.

L'attaquant devra télécharger le projet visual studio (.sln) et regarder le code source.

Dans le code source, le mot de passe de connection à la base de donnée est le même que le mot de passe nextcloud qu'utilise l'utilisateur.

L'attaquant devra donc forward le port 80 et crée une VM windows et installé NextCloud pour pouvoir ouvrir une session NextCloud et ainsi acceder au dossier cloud de IT-Support.

Une fois avec la session ouverte, l'attaquant devra déposer un malware dans le dossier IT-Support qui serra exécuter par un utilisateur Workstation-2 (UO : Responsable).

Workstation-2 :

Une fois avec un accès sur Workstation-2 la personne aura les permissions de l'utilisateur sur la session (UO : Responsable). Cette personnes à les permissions de modifier une GPO qui est appliquer sur Workstation-3.

L'utilisateur devra modifier la GPO pour que celle-ci execute une commande powershell qui executera le payload et donnera un accès à la machine.

Workstation-4 :

Une fois sur la session, l'utilisateur devra voler le token d'un process qui a les permissions de Domain Admins et qui ainsi pourra faire un DCSync sur le domaine controller.

Avec le DCSync il aura une liste de compte avec les NTLM, un compte avec un mot de passe faible qui a la permissions Domain Admins et d'effectuer une connection RDP sur le Domain Controller.

EvilBankDC :

Une fois que l'utilisateur à une connection RDP, il peut flag le domaine !!