2018

Vulnérabilités sous Windows

Exploitation de vulnérabilités sous Windows

Cédric BERTRAND
bertrandcedriccc@gmail.com
30/10/2018

Sommaire

2 Objet du document

Ce document a pour but de montrer quelques vulnérabilités sous Windows.

Prendre des notes et des captures d'écran.

Ce TP pourra être potentiellement ramassé à la fin du cours.

Distribution à utiliser : Kali ou Machine Linux pour effectuer les tests

3 Vulnérabilités sous Windows

3.1 Obtenir un accès à la machine

3.1.1 Accès physique

A partir d'un accès physique, obtenez un accès au système (considérez que la machine virtuelle est un système physique et tenter de trouver d'obtenir un compte utilisateur)

Indice : Démarrer sur une clé ou le lecteur cd-rom

Indice n°2 : Récupérer les hashes, ajouter un compte…

Outils utilisés :

- Samdump (http://theevilbit.blogspot.com/2013/01/backtrack-forensics-samdump-samdump2.html)
- Impacket : https://github.com/SecureAuthCorp/impacket
- OphCrack iso

3.1.2 Accès réseau

Obtenir un accès à la machine à partir d'une vulnérabilité réseau

Indice : scan nessus

3.2 Pass-the-Hashes

3.2.1 Récupération des hashes du système

https://www.top-password.com/blog/tag/extract-hashes-from-sam-file/

Utiliser un outil de dump des mots de passe (wce, mimikatz, hashdump, etc.) pour récupérer les mots de passes / hashes du système Windows

1- Utiliser Metasploit :

Module hashdump de Metasploit

Module mimikatz de Metasploit

2- Utiliser les outils sans metasploits

Utiliser Mimikatz directement (https://github.com/gentilkiwi/mimikatz)

Utiliser un outil de Dump (ex : pwdump, wce)

3.2.1.1 Utilisation avancée de mimikatz (pour pentesteurs)

Faire un dump mémoire et récupérer les identifiants mimikatz via ce dump mémoire

Faire un dump de la mémoire vive :

3.2.2 Cassage des hashes

Casser (trouver les mots de passe associés) des hashes (john, hashcat, etc.)

(note : Mimikatz récupère les mots de passe en clair, casser les dumps récupérés avec des outils tels que hashdump, wce, etc.)

Lien :

- Cracker ntlm avec john : https://www.securitynewspaper.com/2018/11/27/crack-windows-password-with-john-the-ripper/
- Cracker ntlm hashcat : https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4

3.2.3 Utilisation des hashes pour s'authentifier avec l'attaque pass-the-hashes

Réaliser une authentification pass-the-hash avec le compte « admin » (utiliser le hash du compte et le mot de passe directement)

- Module psexec (metasploit)
- Outil pth-winexe (kali)

Lien :

- utiliser pth-winexe : https://github.com/byt3bl33d3r/pth-toolkit
- module psexec : https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/

3.3 Backdooring Windows

3.3.1 Accessibilité

Installer une backdoor sous Windows

Tester la backdoor suivante : https://www.raymond.cc/blog/backdoor-reset-administrator-password-add-new-user-windows-7/

3.3.2 Netcat

Créer une backdoor avec netcat

https://www.offensive-security.com/metasploit-unleashed/persistent-netcat-backdoor/

3.3.3 Base de registre

Refaire la backdoor précédente. Mais cette fois, créer la clé manuellement (avec regedit)

Lien : http://www.geek-space.fr/fr/pc/44-windows/116-demarrage-regedit-registre-run.html

3.3.4 Tâches planifiées

Ajouter une backdoor via les tâches planifiées

Lien : https://www.malekal.com/les-taches-planifiees-de-windows/

4 Création d'une pièce jointe malicieuse

Créer un document word ou excel (avec macros) afin d'exécuter un fichier malveillant

Attention il n'y a pas de version d'Office installée sur le poste Windows, utilisez votre poste ou une machine virtuelle avec Windows.

Lien : https://openclassrooms.com/fr/courses/1438346-redigez-facilement-des-documents-avec-word/1443761-macros-et-vba

https://support.office.com/en-gb/article/automatically-run-a-macro-when-opening-a-workbook-1e55959b-e077-4c88-a696-c3017600db44

Afin de ne pas endommager votre machine, vous pouvez utiliser ce fichier exécutable (inoffensif) : https://lepouvoirclapratique.com/temp_malicious_dchsdqbuqbvbvveys/test.exe

Quelques articles pour vous aider :

https://www.abatchy.com/2017/03/powershell-download-file-one-liners

https://www.vdalabs.com/2017/12/04/part-3-malware-analysis-bromium/

https://unit42.paloaltonetworks.com/unit42-unique-office-loader-deploying-multiple-malware-families/

https://blog.jourdant.me/post/3-ways-to-download-files-with-powershell

https://www.addictivetips.com/windows-tips/download-files-from-powershell-windows-10/

https://enigma0x3.net/2014/03/18/vba-powershell-malware/

4.1 Exécuter un fichier exécutable

Créer une macro qui permette de télécharger et d'exécuter un fichier exécutable à l'ouverture du document word.

Chemin pour un fichier exécutable de test (Windows 32 bits) : https://lepouvoirclapratique.com/temp_malicious_dchsdqbuqbvbvveys/test.exe

Chemin pour un fichier exécutable de test (Windows 64 bits) : https://lepouvoirclapratique.com/temp_malicious_dchsdqbuqbvbvveys/test64.exe

4.2 Exécuter un script powershell

Utiliser un script du framework Nishang (https://github.com/samratashok/nishang)

Exemple : https://github.com/samratashok/nishang/blob/master/Gather/Get-Information.ps1

5 Infection automatisée

5.1.1 Infection automatique avec une page web

Tester le module browser_autopwn de metasploit :

- Lancer le module browser_autopwn sur le poste attaquant
- Récupérer l'url associée au module
- Sur le poste Windows vulnérable, se connecter à l'url associée au module

(Ne pas prendre en compte les avertissements)

Lien : https://blog.rapid7.com/2015/07/15/the-new-metasploit-browser-autopwn-strikes-faster-and-smarter-part-1/