4TO. CONGRESO INTERNACIONAL

SEGURIDAD INFORMÁTICA

28 - 30 de Noviembre - La Paz, Bolivia

Identificando Shadow Admins en entornos de Active Directory

Javier Silva

Senior Security Consultant

whoami

- Ingeniero de Sistemas, Universidad Loyola.
- OSCP (Offensive Security Certified Professional).
- CRTP (Certified Red Team Professional).
- Incident Response/Threat Hunting.
- Red Team Operator (en proceso).
- ISO 27001/27032.

contenido

- Conceptos basicos de Active Directory.
- Pentesting sobre Active Directory.
- Grupos privilegiados comúnes.
- Bloodhound para recolección y análisis de información.
- Escenario 1: Privilegios de grupos heredados.
- Escenario 2: ACLs permisivas para movimiento lateral.
- Escenario 3: Resource Based Constrained Delegation.
- Escenario 4: NTLM Relay entre equipos.
- Preguntas.

conceptos_basicos_de_active_directory

- **Solución de Microsoft usada comunmente para gestión de accesos e identidades.**
- **Autentica y autoriza a todos los usuarios y equipos asociados a un dominio interno.**
- **Consiste de una serie de componentes, como ser:**
  - Objetos (Usuarios, equipos, GPOs, grupos, enlaces)
  - Forests/Trees/Domains
  - Unidades organizacionales

ejemplo_estructura_active_directory

pentesting_sobre_active_directory

- Objetivo ideal – Obtener privilegios de administración de dominio.
- Evaluar la gestion de accesos definida, privilegios otorgados a usuarios y equipos, como tambien la configuración desplegada.
- Un escaneo de vulnerabilidades sobre los servidores NO es suficiente.

grupos_privilegiados_comunes

.Grupos existentes por defecto en cualquier instancia de Active Directory.

- Domain Admins
- Enterprise Admins
- Schema Admins
- Administrators

.Objetivos principales de grupos APT al realizar la intrusion a la red interna.

.Control total sobre el dominio interno y cualquier equipo/usuario asociado a este.

grupos_privilegiados_comunes

.Domain Admins.

- Este grupo tiene, por defecto, privilegios administrativos sobre todos los equipos y servidores asociados al dominio interno.

.Enterprise Admins.

- Este grupo tiene privilegios administrativos sobre todos los dominios en un Forest

.Schema Admins.

- Este grupo tiene privilegios para realizar cambios sobre el esquema definido, donde este es la definición de todos los objetos y atributos que conforman el Forest.

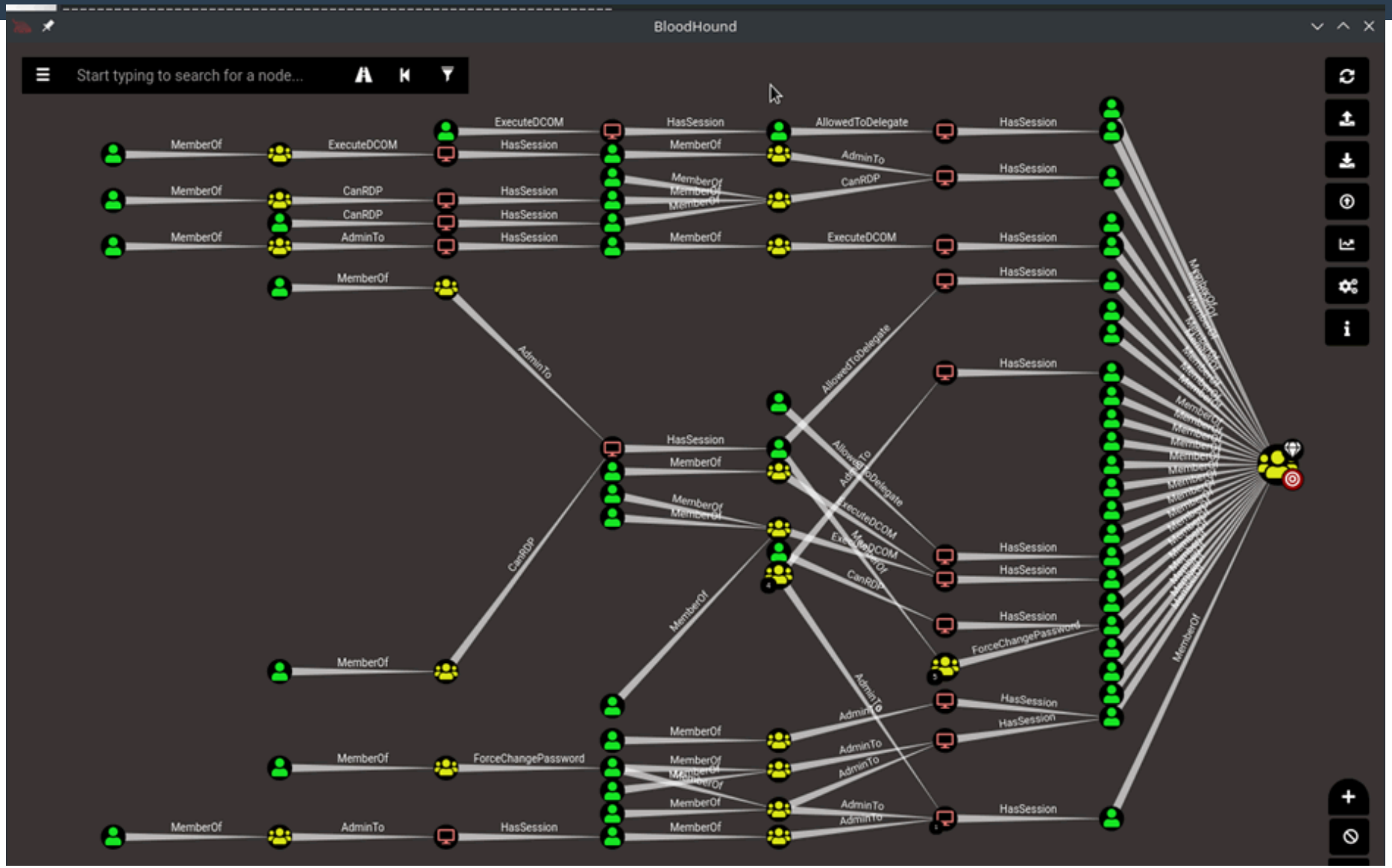
.Administrators.

- Este grupo tiene privilegios administrativos sobre los controladores de dominio.

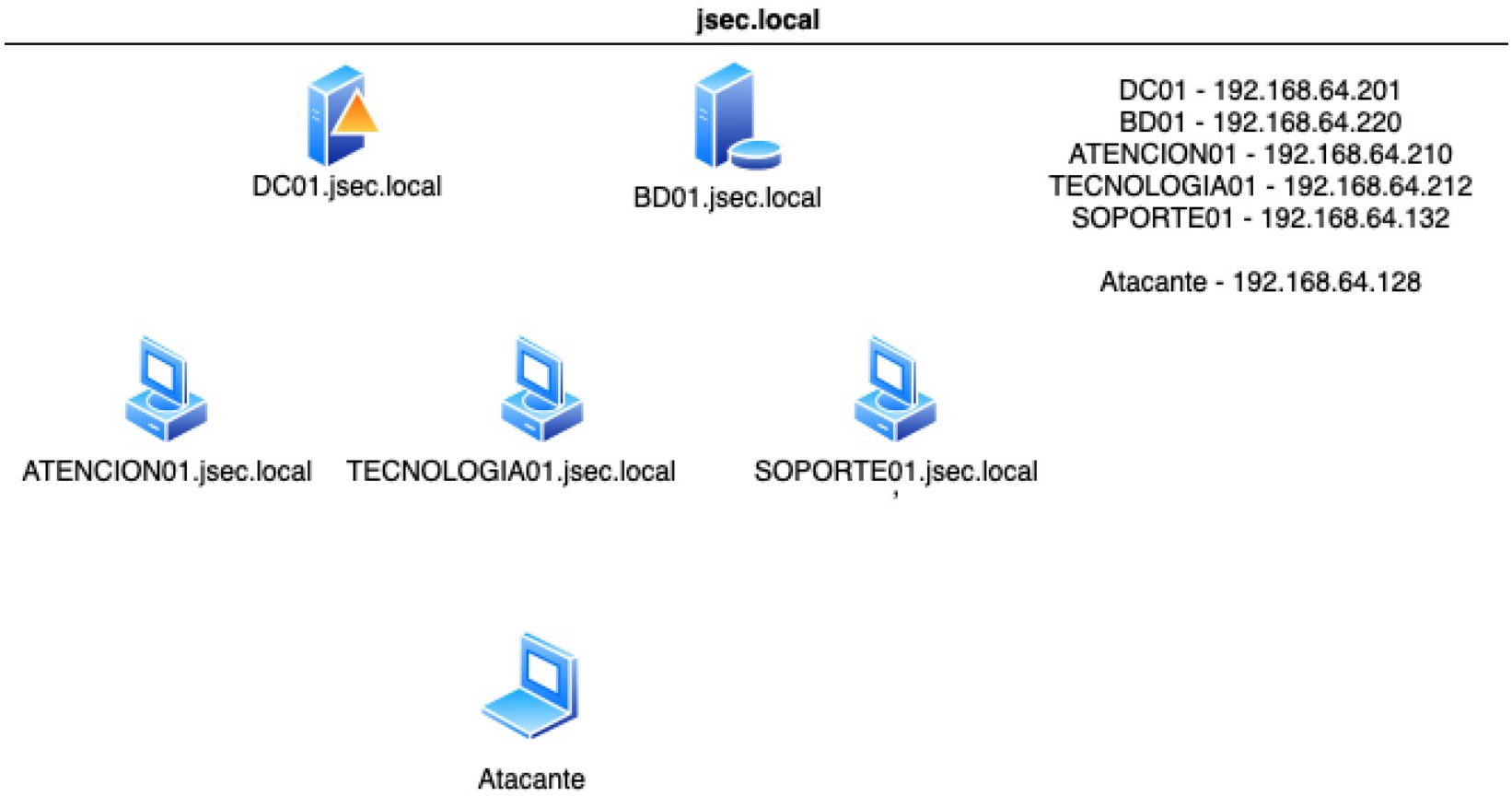
bloodhound

- Herramienta para extraer información de un dominio interno, obteniendo todos los objetos y sus relaciones.
- Utiliza teoría de grafos para la busqueda de vectores de ataque existentes en un Active Directory.
- Tecnología utilizada: Javascript para la vista, linkurious como motor de analisis, electron para el despliegue en distintos sistemas operativos, Neo4j como base de datos y un ingestor en C#, Python o Powershell

bloodhound


BloodHound
Start typing to search for a node...
MemberOf
ExecuteDCOM
HasSession
CanRDP
AdminTo
AllowedToDelegate
ForceChangePassword

ambiente


jsec.local
DC01.jsec.local
BD01.jsec.local
DC01 - 192.168.64.201
BD01 - 192.168.64.220
ATENCION01 - 192.168.64.210
TECNOLOGIA01 - 192.168.64.212
SOPORTE01 - 192.168.64.132
Atacante - 192.168.64.128
ATENCION01.jsec.local
TECNOLOGIA01.jsec.local
SOPORTE01.jsec.local
Atacante

escenario_1

SEGUNDO CONGRESO TECNOLOGÍA Y GOBIERNO

VIDEO

Se asume una brecha en la red interna.
Visibilidad directa de los componentes del Active Directory.
Usuarios comprometidos: demo y demo_privs.
Vector de ataque:
Usuario demo_privs miembro del grupo “NUEVO_SOPORTE”, el cual es miembro del grupo “ADMIN_T1”, a la vez, este ultimo pertenece al grupo “Domain Controllers”, el cual cuenta con privilegios “ForceChangePassword” sobre el usuario “Admin”.

escenario_1

- **Bloodhound-python:**
  - https://github.com/fox-it/BloodHound.py
- **Crackmapexec:**
  - https://github.com/Porchetta-Industries/CrackMapExec
- **Powerview:**
  - https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1
- **Bloodhound:**
  - https://github.com/BloodHoundAD/BloodHound

escenario_2

VIDEO

Se asume una brecha en la red interna.
Visibilidad directa de los componentes del Active Directory.
Usuarios comprometidos: acl_administrators, cosme.fulanito.
Vector de ataque:
Usuario ACL_Administrators con privilegios “GenericAll” sobre el grupo “Administrators” de dominio.

escenario_2

.Bloodhound-python:

- https://github.com/fox-it/BloodHound.py

.Crackmapexec:

- https://github.com/Porchetta-Industries/CrackMapExec

.Active Directory DLL:

- https://github.com/samratashok/ADModule

.Bloodhound:

- https://github.com/BloodHoundAD/BloodHound

escenario_3

SEGUNDO CONGRESO TECNOLOGÍA Y GOBIERNO

VIDEO

Se asume una brecha en la red interna.
Visibilidad directa de los componentes del Active Directory.
Usuarios comprometidos: rbcd_user.
Vector de ataque:
Usuario rbcd_user con privilegios “GenericAll” sobre el controlador de dominio, por lo que se crea un nuevo equipo de dominio para realizar el ataque “Resource Based Constrained Delegation”

escenario_3

- **Bloodhound-python:**
  - https://github.com/fox-it/BloodHound.py
- **Crackmapexec:**
  - https://github.com/Porchetta-Industries/CrackMapExec
- **RBCD Attack en Python:**
  - https://github.com/tothi/rbcd-attack/blob/master/rbcd.py
- **Bloodhound:**
  - https://github.com/BloodHoundAD/BloodHound
- **Impacket:**
  - https://github.com/SecureAuthCorp/impacket

escenario_4

SEGUNDO CONGRESO TECNOLOGÍA Y GOBIERNO

VIDEO

Se asume una brecha en la red interna.
Visibilidad directa de los componentes del Active Directory.
Usuarios comprometidos: demo
Vector de ataque:
El usuario de dominio perteneciente al equipo ”SOPORTE01” cuenta con privilegios adminstrativos sobre el equipo “TECNOLOGIA01” y visceversa, dado que ninguno de los dos equipos requiere la firma de mensajes SMB, se realiza un ataque de Relay para la obtencion de privilegios administrativos.

escenario_4

- **Bloodhound-python:**
  - https://github.com/fox-it/BloodHound.py
- **Crackmapexec:**
  - https://github.com/Porchetta-Industries/CrackMapExec
- **Printerbug:**
  - https://github.com/dirkjanm/krbrelayx/blob/master/printerbug.py
- **Bloodhound:**
  - https://github.com/BloodHoundAD/BloodHound
- **Impacket:**
  - https://github.com/SecureAuthCorp/impacket

recomendaciones

SEGUNDO CONGRESO TECNOLOGÍA Y GOBIERNO

Pentesters.

Una evaluación de Active Directory debe ser completa, no depender de scanners de vulnerabilidades.
Enumerar a profundidad, explorar los privilegios de los usuarios y equipos obtenidos.
Identificar todos los posibles objetivos interesantes, no solo los domain admins.
Los hashes NTLM son igual de válidos que una contraseña.

Sysadmins.

Realizar una limpieza en el dominio interno, eliminando los privilegios innecesarios sobre objetos importantes.
Monitorear accesos de usuarios privilegiados sobre equipos no relacionados con la funcion del usuario.
Contar con un minimo de administradores de dominio.
Si hay que escoger, mejor estresarse cerrando las brechas de seguridad que intentando recuperar los servicios afectados por un ataque real.

contacto

SEGUNDO CONGRESO TECNOLOGÍA Y GOBIERNO

Javier Silva

Correo

Javieralejandrosilva.93@gmail.com

Linkedin

https://www.linkedin.com/in/javier-silva-24a81414a/

Blog

https://jsec-rt.com

¿Preguntas?