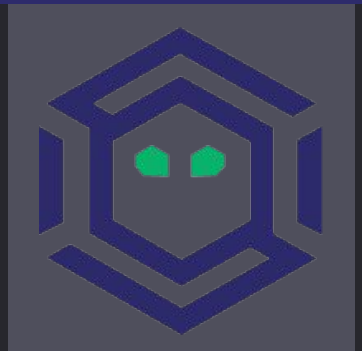
Tactics, Techniques and Procedures for Attacking Active Directory

BlackHat USA 2019

- Link to this deck:

  https://bit.ly/2ZQIfGY



Ryan Hausknecht

Andy Robbins

Rohan Vazarkar

Julian Catrambone

Kelly Villanueva

Calvin Hedler

Carlo Alcantara

You can find us at:
Specterops.io
@SpecterOps

Outline (morning segment 1)

10:00-10:15:	Derivative Local Admin Lecture
10:15-10:30:	Lab
10:30-10:45:	ACL Attacks
10:45-11:00:	Lab
11:00-11:15:	Kerberos Attacks
11:20:	Room changeover

Outline (morning segment 2)

11:30-11:45:	Derivative Local Admin Lecture
11:45-12:00:	Lab
12:00-12:15:	ACL Attacks
12:15-12:30:	Lab
12:30-12:45:	Kerberos Attacks

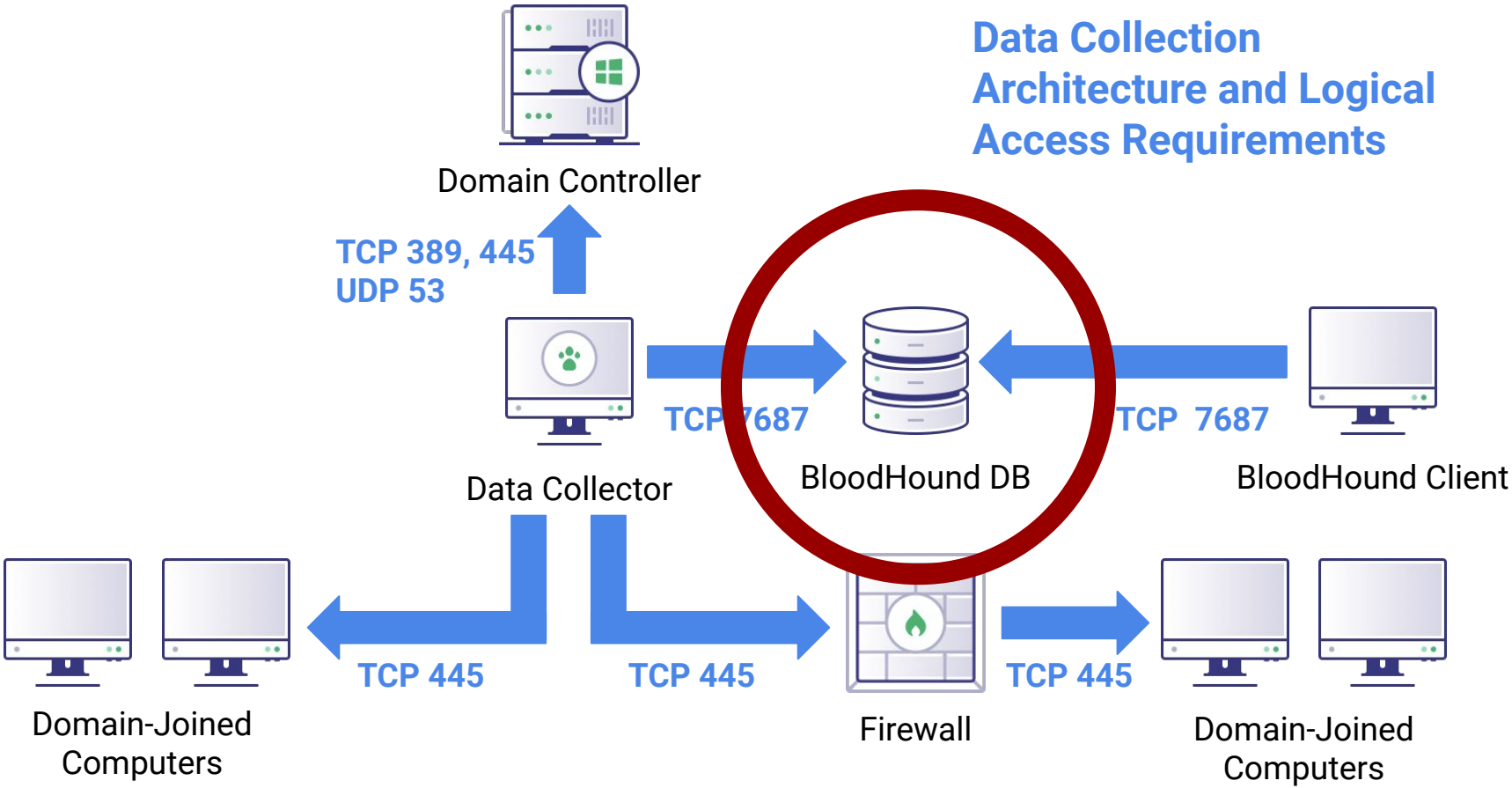
Outline (afternoon segment 1)

2:00-2:15:	Derivative Local Admin Lecture
2:15-2:30:	Lab
2:30-2:45:	ACL Attacks
2:45-3:00:	Lab
3:00-3:15:	Kerberos Attacks
3:30:	Room changeover

Outline (afternoon segment 2)

3:45-4:00:	Derivative Local Admin Lecture
4:00-4:15:	Lab
4:15-4:30:	ACL Attacks
4:30-4:45:	Lab
4:45-5:00:	Kerberos Attacks
5:15:	Room shutdown

Data Collection Architecture and Logical Access Requirements



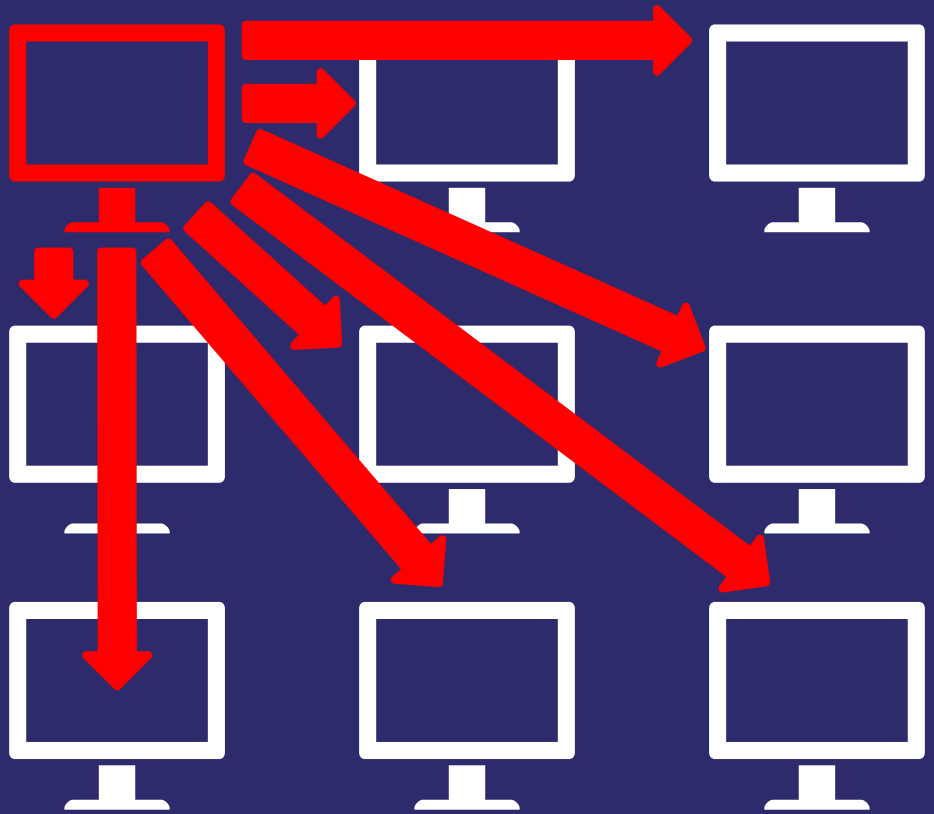
Data Collection w/ SharpHound

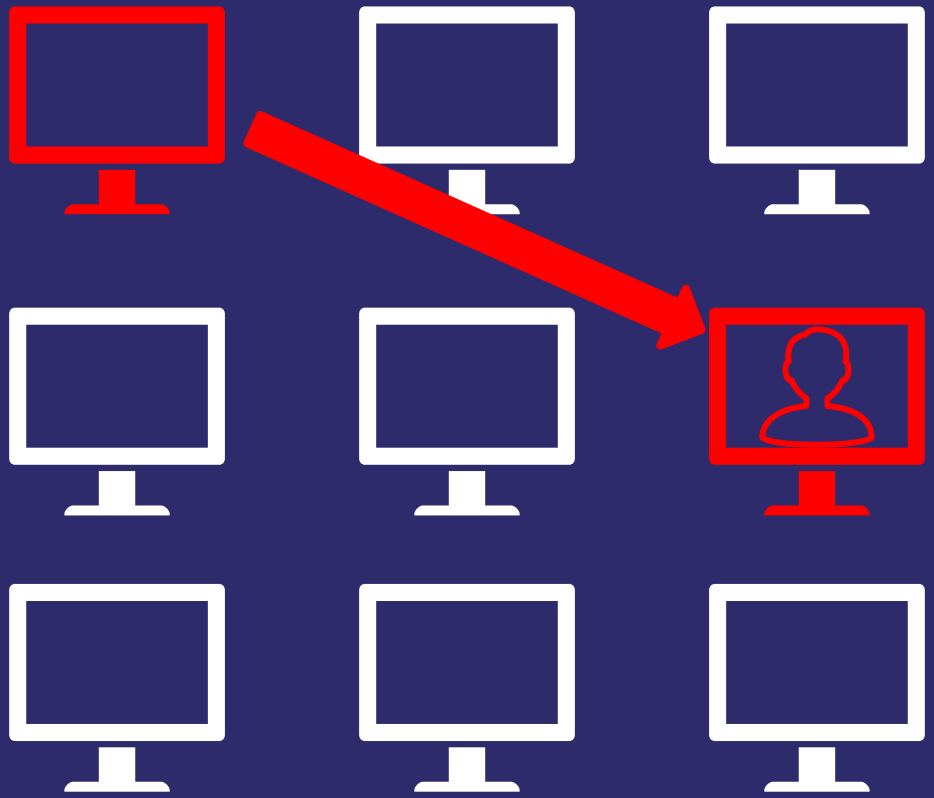
- Go to https://github.com/BloodHoundAD/BloodHound/tree/master/Ingestors
- Download “SharpHound.exe”
- Run the following as a user that has admin rights on each Windows endpoint:
- `sharphound.exe -c all,loggedon`
- This will generate a zip file.
- Open the BloodHound UI
- Drag and drop the zip file into the BloodHound UI

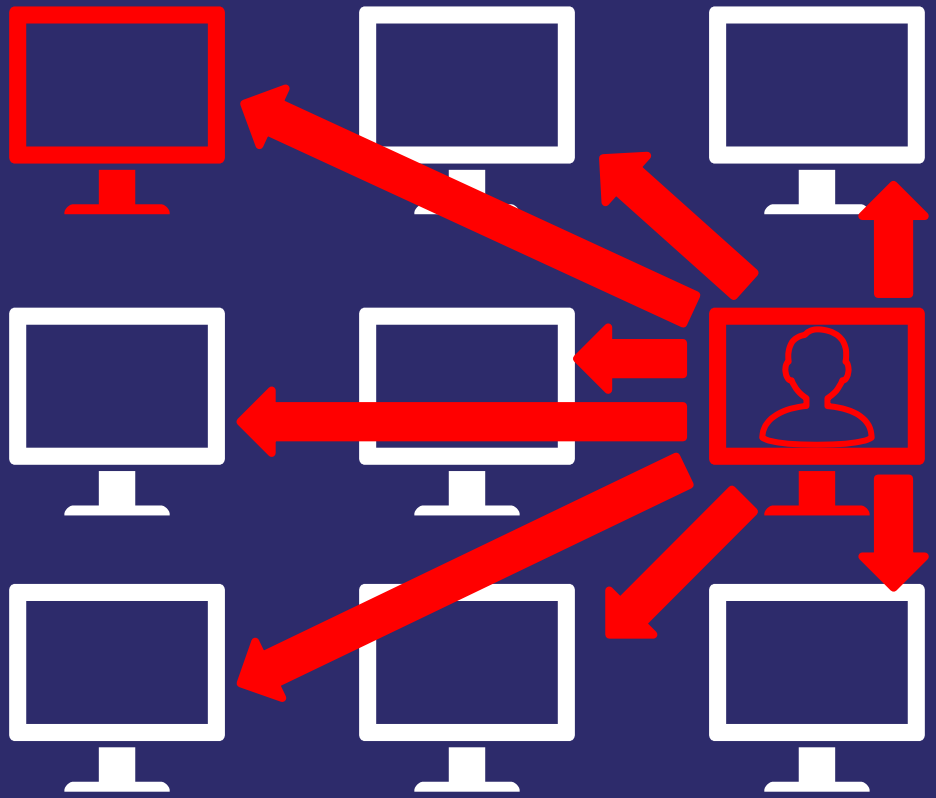
Data Collection w/ SharpHound

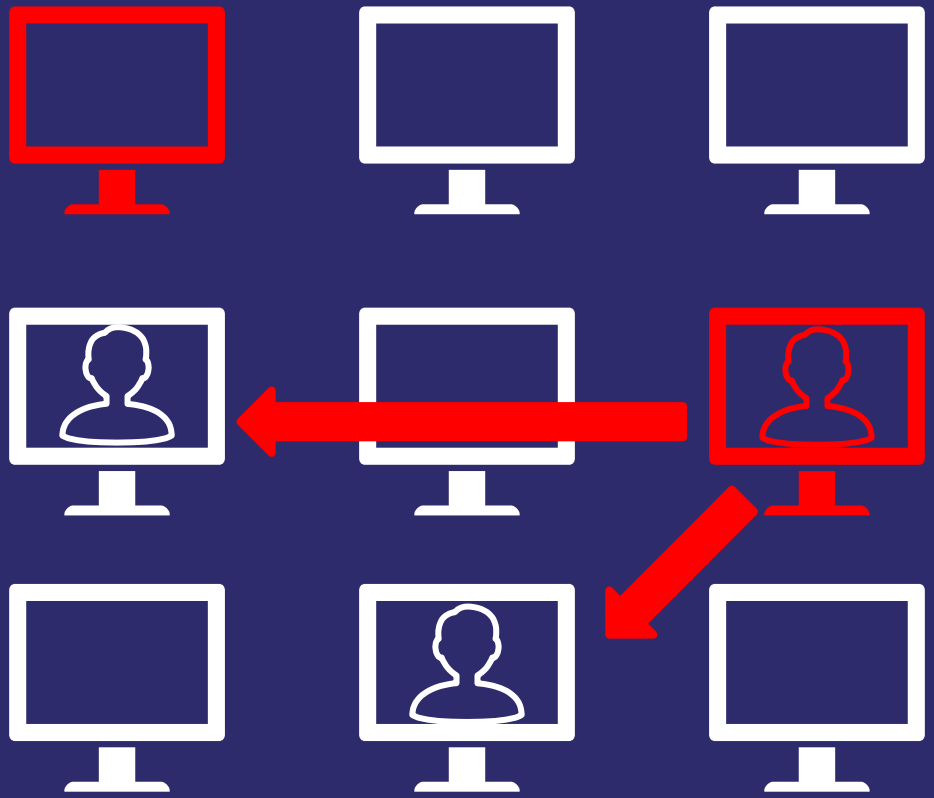
- This will collect:
  - AD security group memberships
  - Group, user, domain and computer properties (SID, enabled, sensitive and cannot be delegated, etc.)
  - Interactive user logons per computer
  - Local admin, Remote Desktop user, DCOM users per computer
  - Abusable ACEs from security principals
  - Domain trusts
  - OU structure and GPO Links

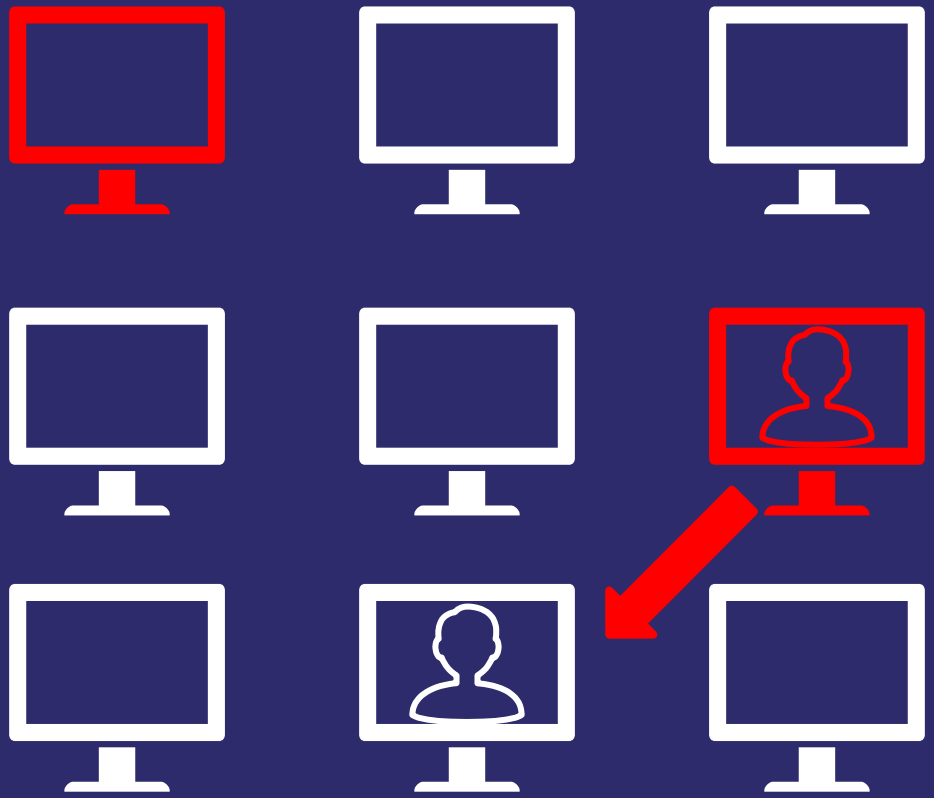
Derivative Local Admin

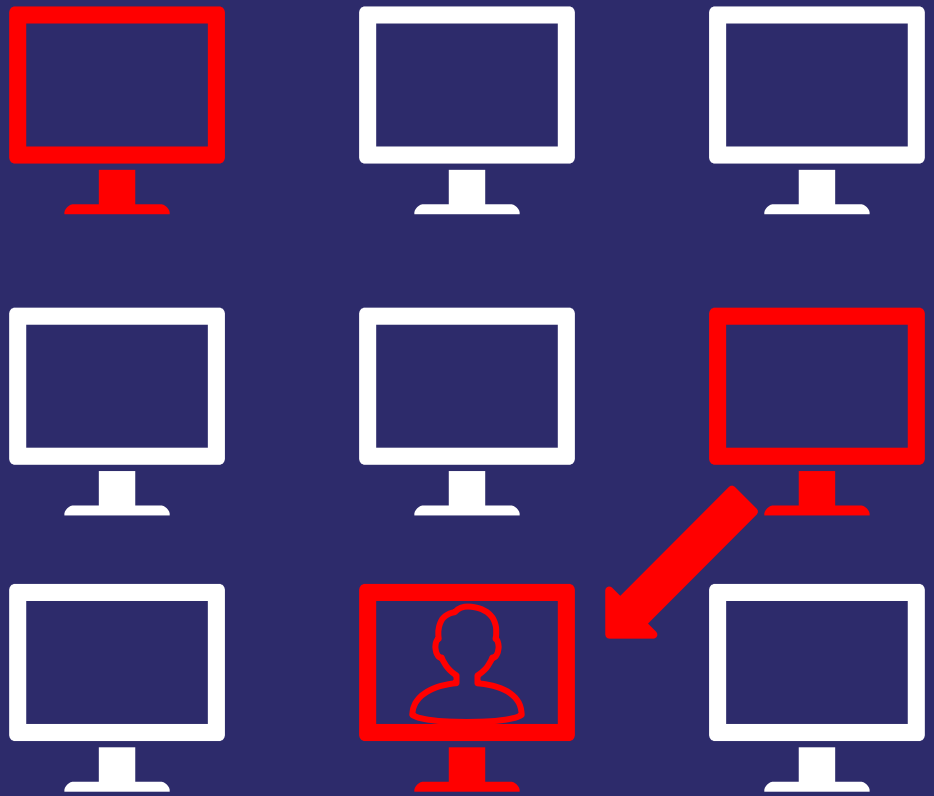


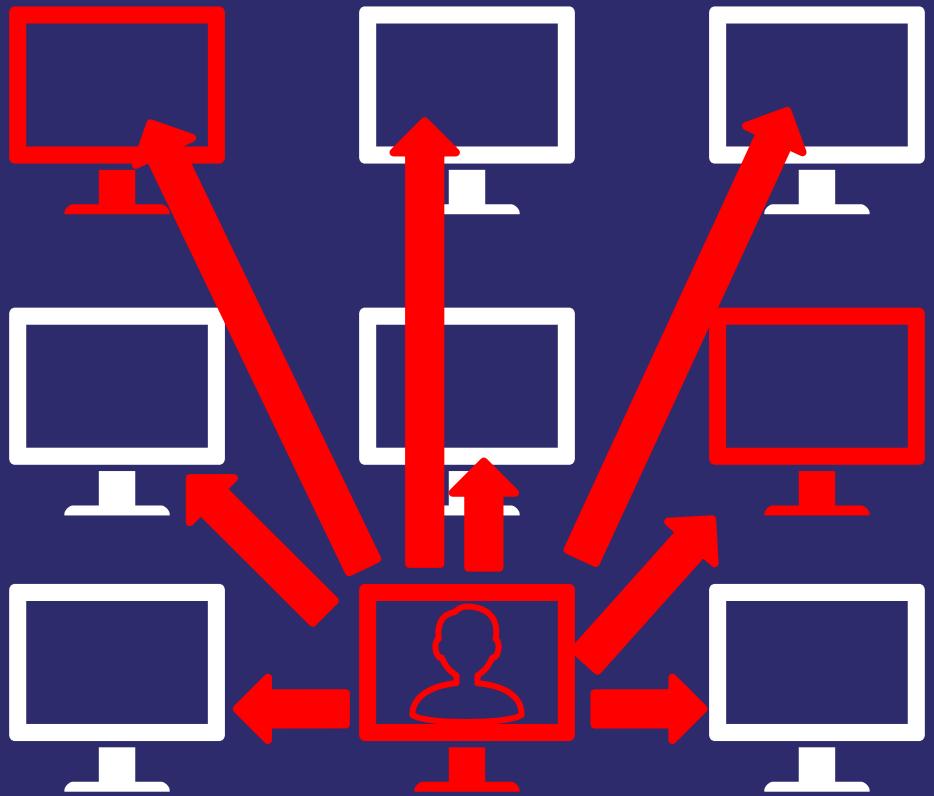


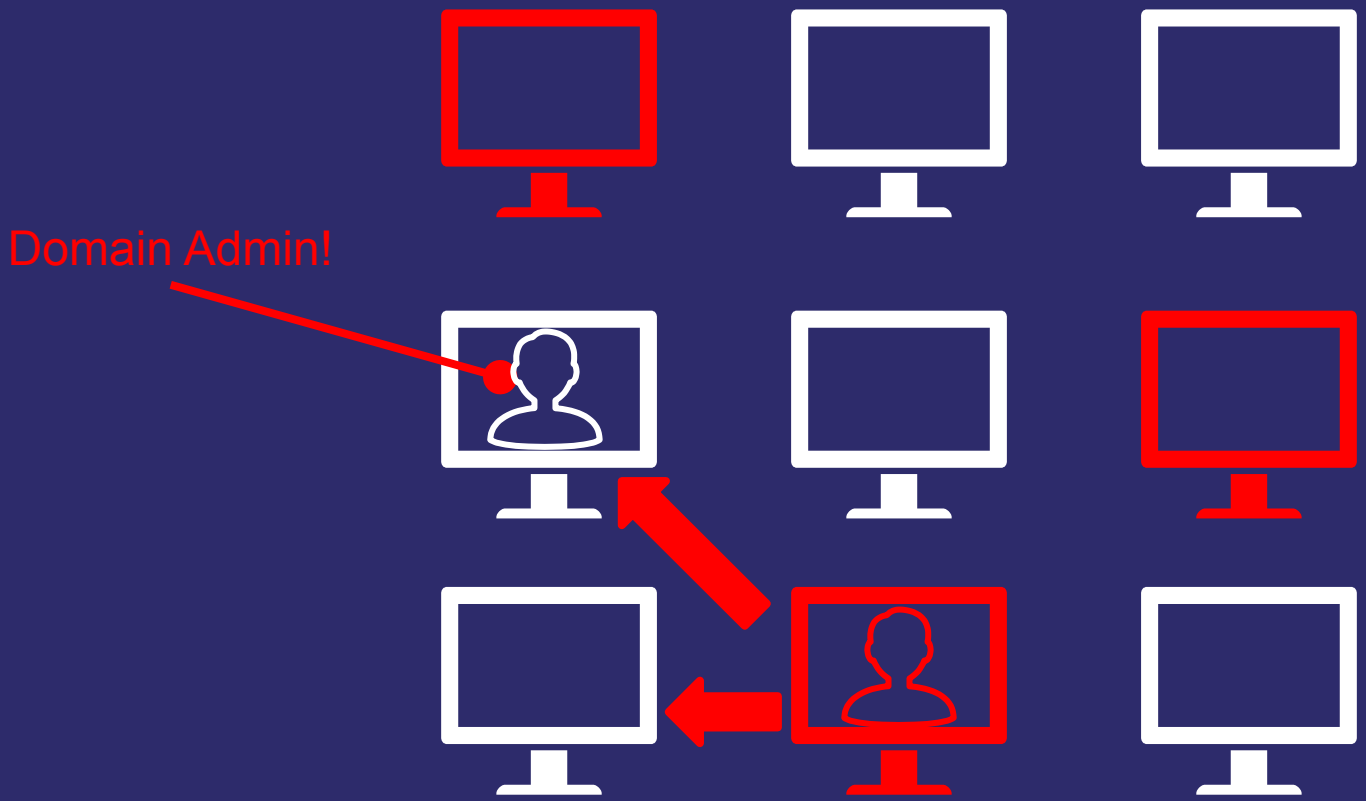


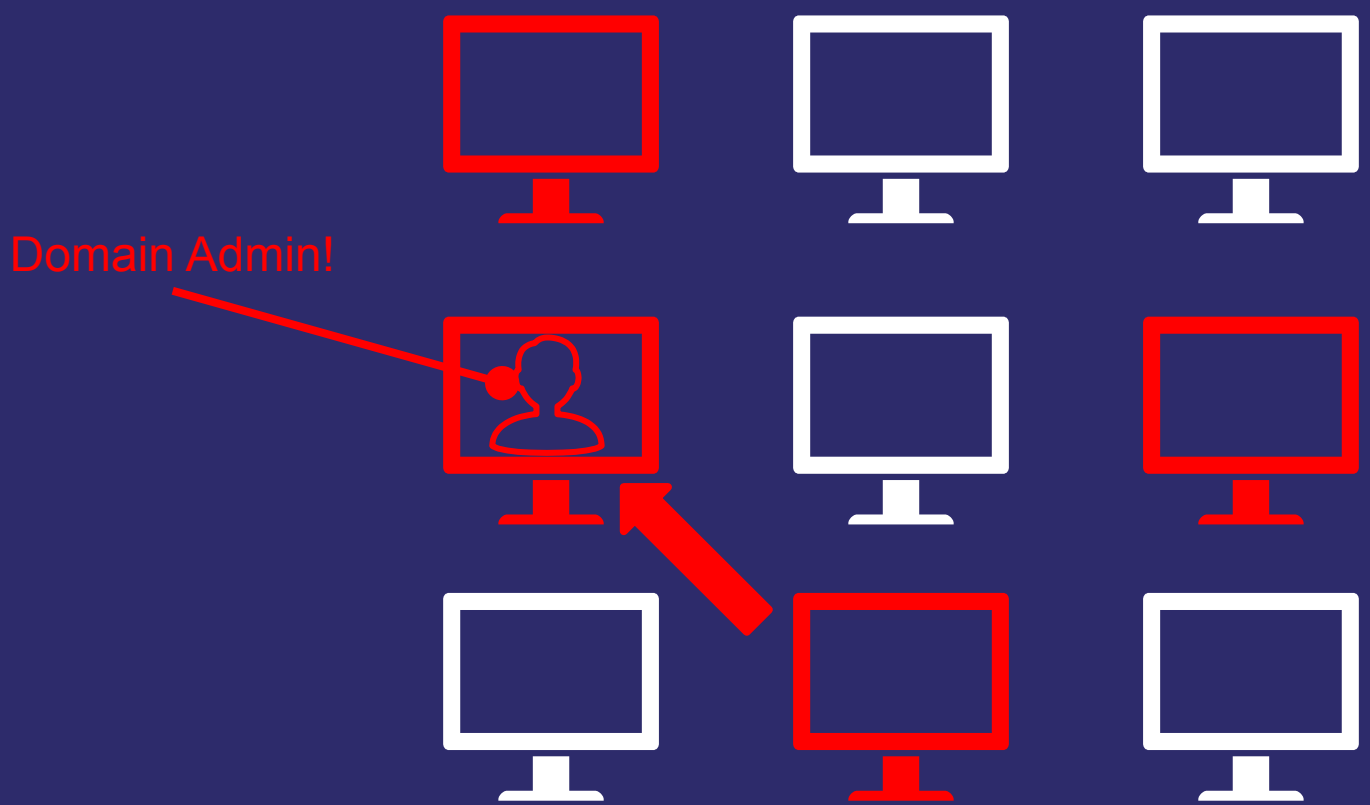









Domain Admin!


Domain Admin!

An effective, albeit tedious and naive approach...

Target Users:
Admin-1
Admin-2
Admin-3
Admin-4
Admin-5

Admin-1 Uses These Systems:
Computer-1
Computer-2
Computer-3

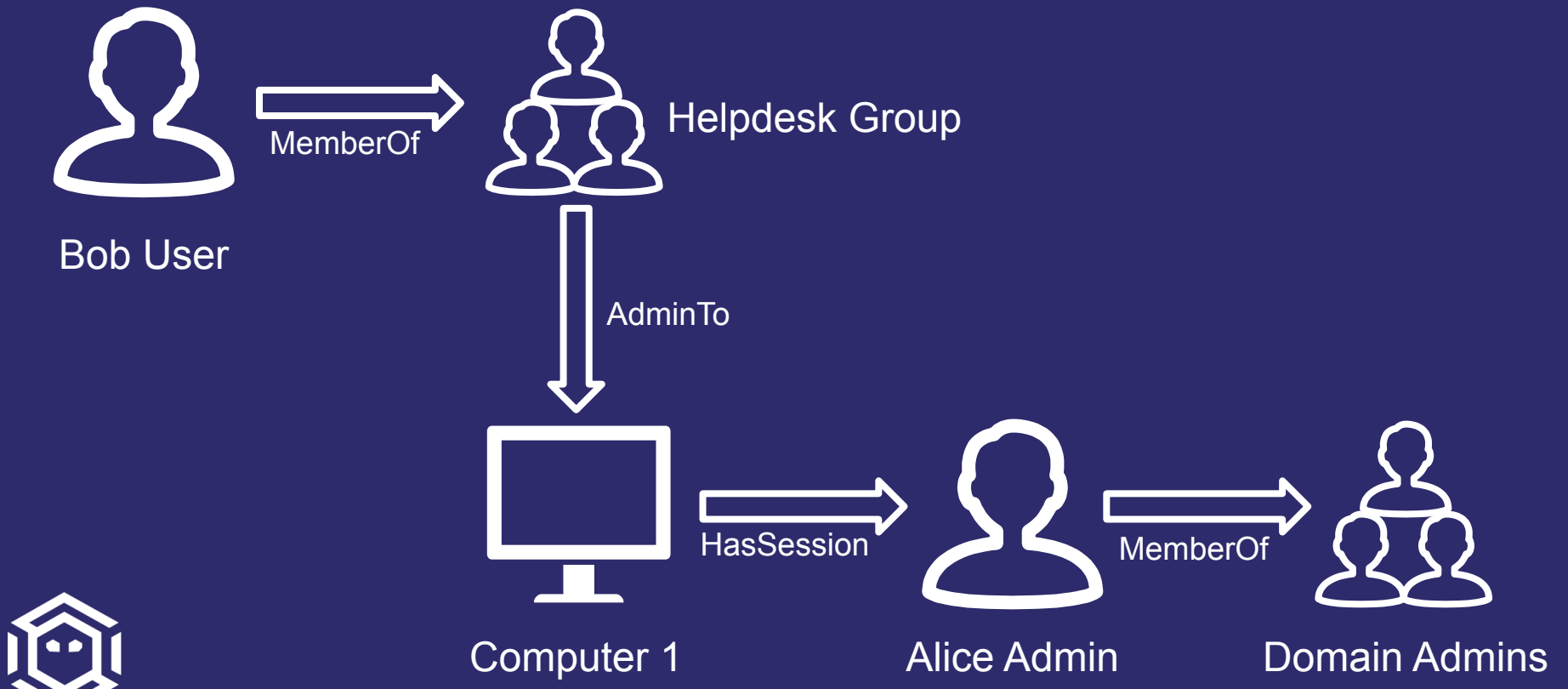
Admins on Computer-1:
Admin-1
Admin-2
Admin-10
Group-11

Members of Group-11:
Admin-5
Admin-6
Admin-7
Admin-8

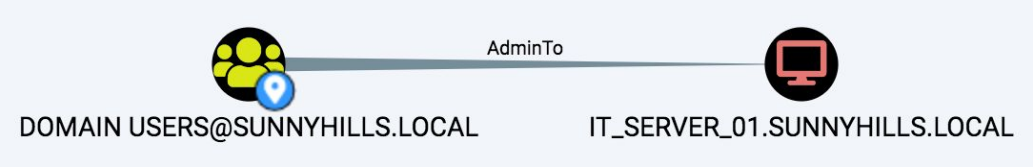
Members of Group 11 Use These Systems:
Computer-1
Computer-2
Computer-5

Admins on Computer-5:
Admin-1
Admin-2
Admin-10
Admin-15

Admin-15 Uses These Systems:
Computer-1
Computer-2
Computer-10


MemberOf
Helpdesk Group
Bob User
AdminTo
HasSession
MemberOf
Computer 1
Alice Admin
Domain Admins

Local Admin Abuses



- Local administrators by default have full control of a system.
- This includes SeDebugPrivilege, which allows admins to debug running processes (e.g.: lsass.exe)
- Local admins also by default have remote desktop, DCOM, SCM, WinRM, and WMI access (i.e.: remote code execution)
- Local admins can also disable/bypass host-based security controls, even those that are “protected”
- Bottom line: local admins own computers and anyone else who interactively logs onto the computer.
- Forensic artifact: admins generate 4688 events when spawning high integrity process

Cobalt Strike

Cobalt Strike View Attacks Reporting Help

external	internal	user	computer	note	pid	last
192.168.204.229	192.168.204.229	alice.operations	WIN10-001		912	31ms
192.168.204.229 ∞∞∞	192.168.204.221	SYSTEM *	WIN10-002		6600	1s
192.168.204.221 ∞∞∞	192.168.204.231	SYSTEM *	WIN10-003		340	1s

Event Log X | Listeners X | Web Log X | Sites X | Beacon 192.168.204.229@912 X | Beacon 192.168.204.221@6600 X | Beacon 192.168.204.231@340 X

```
      aes256_hmac       (4096) : f920eb731bdd8d83a6e0a9a4aa2ace3c71f71c4c84720820fae35383399926fa
      aes128_hmac       (4096) : 06bb6dfecfcfd1815fb4bcb813abf5a1
      des_cbc_md5       (4096) : 32a7c43219ea04fb

* Primary:Kerberos *
    Default Salt : CONTOSO.LOCALkrbtgt
    Credentials
      des_cbc_md5       : 32a7c43219ea04fb

* Packages *
    Kerberos-Newer-Keys

* Primary:WDigest *
    01  c3400d67b2324a154c289fabdaf99f50
    02  b1243bf898cb2832c2c205ecbcc81ad1
    03  5ca5d761796240aa9dcbb0395c5414ef
    04  c3400d67b2324a154c289fabdaf99f50
    05  b1243bf898cb2832c2c205ecbcc81ad1
    06  30475617bc3d5d936e102ed21094bda4
    07  c3400d67b2324a154c289fabdaf99f50
    08  7bb7cba5df87e6d1536ca9e2a6d9e191
    09  7bb7cba5df87e6d1536ca9e2a6d9e191
    10  97e1bf64441851a2467e8637802f77cb
    11  a55185db9f574987049d4fda6c9e8081
    12  7bb7cba5df87e6d1536ca9e2a6d9e191
    13  73af6f91f2d939c9c599403f0550be8f
    14  a55185db9f574987049d4fda6c9e8081
    15  6adbf1c0a14ac2b728f6df8ddec48d9f
    16  6adbf1c0a14ac2b728f6df8ddec48d9f
    17  331804583c753b473431cdcb5c5eee16
    18  acd4a04665a9f1640d8f2c8cd9947794
    19  8b9e3105aeaee10dcdffaf9bc00e39c2
    20  34ec43969b2b4defcba8985ee4a7ce73
    21  fd78aeba613041852ee2da8f245789c7
    22  fd78aeba613041852ee2da8f245789c7
    23  fc46fecb1ad9971befab660652e30b78
    24  051a6017a27700f8c3d3f2e6d583b135
```

[WIN10-003] SYSTEM */340 last: 1s

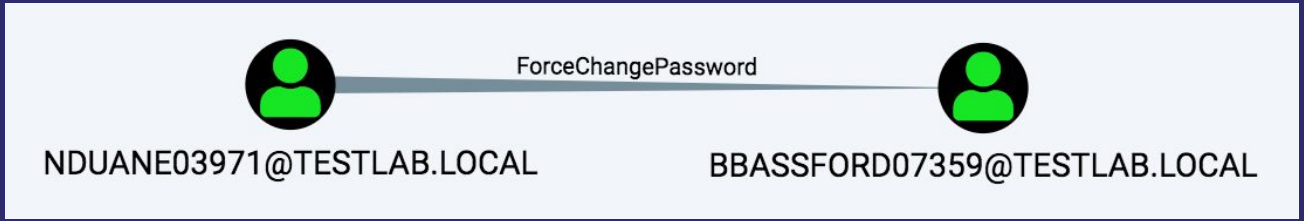
beacon>

Lab

- Download the BloodHound GUI here: https://github.com/BloodHoundAD/BloodHound/releases
- Open the BloodHound GUI and connect to the BloodHound database at bolt://206.189.85.93:7687/
- Username: neo4j
- Password: BloodHound
- Find the shortest paths to the Domain Admins group in each domain
- Inspect the local admin rights for the user KXUNA@JAPAN.LOCAL
- Inspect the inbound local admin rights on the computer IO@JAPAN.LOCAL
- Explore other nodes in the database and the attack paths between them
- **TIP: Right click the edge (relationship) and click “help”**

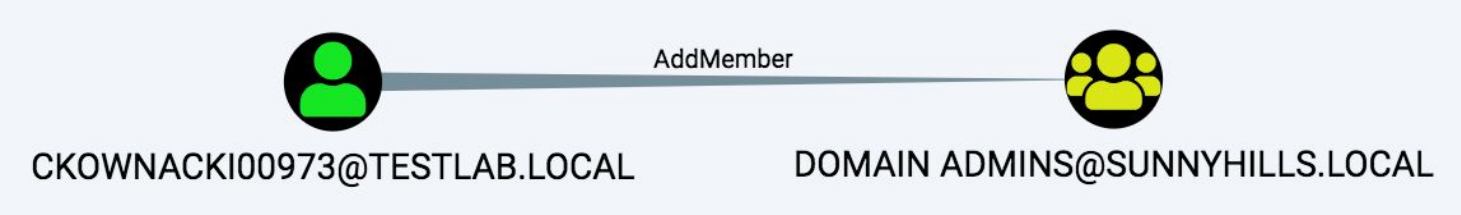
ACL Attacks

ForceChangePassword



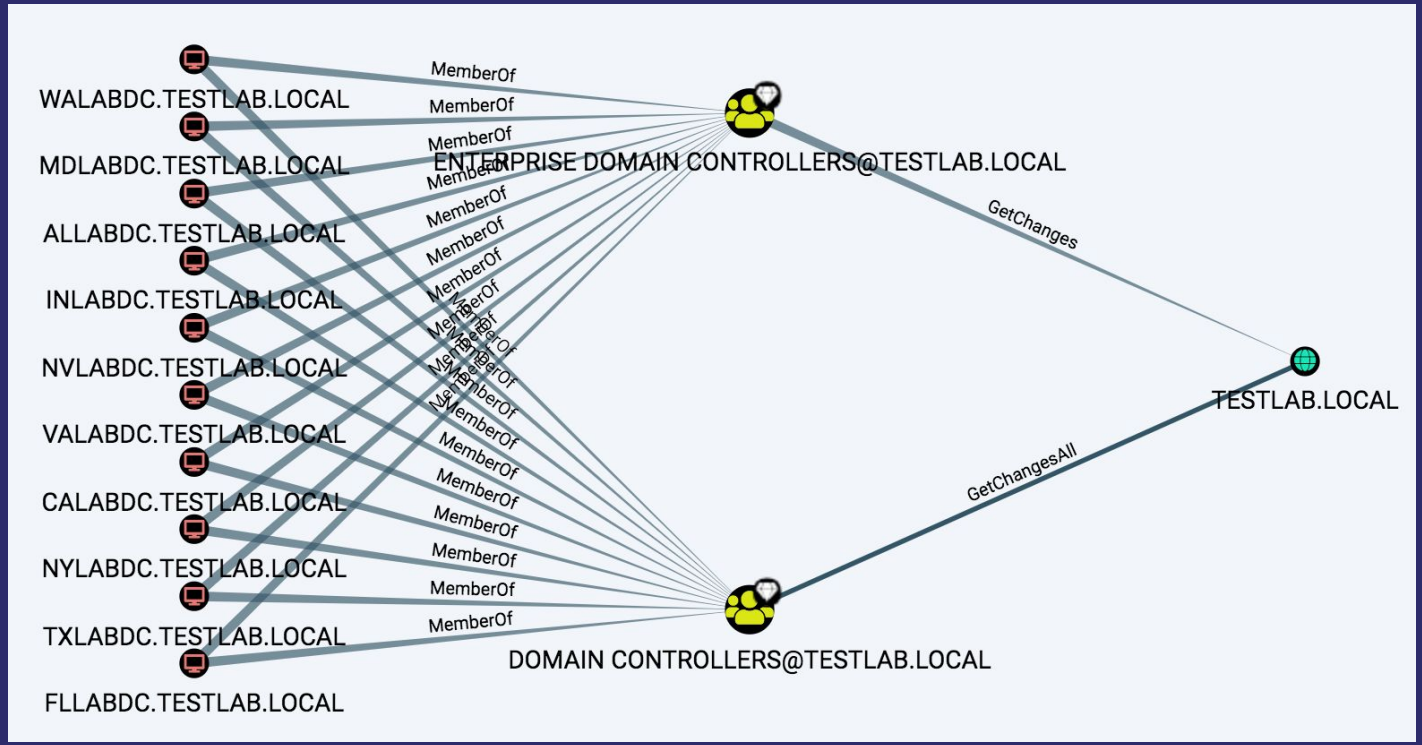
- The user NDUANE03971 can change the user BBASSFORD07359's password without knowing the current password
- This is as easy as "net user BBassford07359 Password1 /domain"
- The new password must meet the domain's password complexity and age requirements
- This then gives NDUANE the ability to impersonate BBASSFORD, and use whatever privileges BBASSFORD has to continue the attack path.
- With domain admin or dcsync-equivalent privileges, an attacker can set BBASSFORD's password back to what it was before. If done quickly enough, the user will have no idea their password ever changed.
- Forensic artifact: Generates a 4724 and 4738 event on the DC that handled the request.

AddMember



- The user CKOWNACKI00973 can add arbitrary principals to the group Domain Admins.
- This is as easy as “net group “Domain Admins” CKOWNACKI00973 /add /domain”
- This then gives CKOWNACKI00973 the same privileges as the Domain Admins group, and the attacker can continue their attack path.
- Forensic artifact: Generates a 4728 event on the DC that handled the request

DCSync


WALABDC.TESTLAB.LOCAL
MDLABDC.TESTLAB.LOCAL
ALLABDC.TESTLAB.LOCAL
INLABDC.TESTLAB.LOCAL
NVLABDC.TESTLAB.LOCAL
VALABDC.TESTLAB.LOCAL
CALABDC.TESTLAB.LOCAL
NYLABDC.TESTLAB.LOCAL
TXLABDC.TESTLAB.LOCAL
FLLABDC.TESTLAB.LOCAL
MemberOf
ENTERPRISE DOMAIN CONTROLLERS@TESTLAB.LOCAL
DOMAIN CONTROLLERS@TESTLAB.LOCAL
GetChanges
GetChangesAll
TESTLAB.LOCAL

DCSync (continued)

- DCSync is the combination of two privileges: DS-Replication-Get-Changes and DS-Replication-Get-Changes-All
- This privilege allows a principal to remotely retrieve credential material (NT hashes) via the MS-DRSR protocol
- Most commonly, attackers will abuse DCSync rights to gather the *krbtgt* account credential material, then craft golden tickets
- Forensic artifacts: DsGetNCChanges on the wire – see https://adsecurity.org/?p=1729

GPO Control

- Control of GPOs opens up incredible attack possibilities. You truly can do anything with GPO.
- GPO control is especially interesting because you don't require logical access to your target computer, or computers used by your target user
- Risk is dependent on what objects the GPO applies to, which we will demonstrate later.
- Forensic artifact: GPO changes generate 5137 events on DCs

Lab

- Download the BloodHound GUI here: https://github.com/BloodHoundAD/BloodHound/releases
- Open the BloodHound GUI and connect to the BloodHound database at bolt://206.189.85.93:7687/
- Username: neo4j
- Password: BloodHound
- Find the shortest paths to the Domain Admins group in each domain
- Inspect the outbound privileges for the user YFAN@TOKYO.JAPAN.LOCAL
- Inspect the inbound privileges against the group DOMAIN ADMINS@TOKYO.JAPAN.LOCAL
- **TIP: Right click the edge (relationship) and click “help”**

Kerberos Attacks

Three Kerberos Issues to Focus on

1. “Kerberoast”
2. Unconstrained Delegation
3. Constrained Delegation

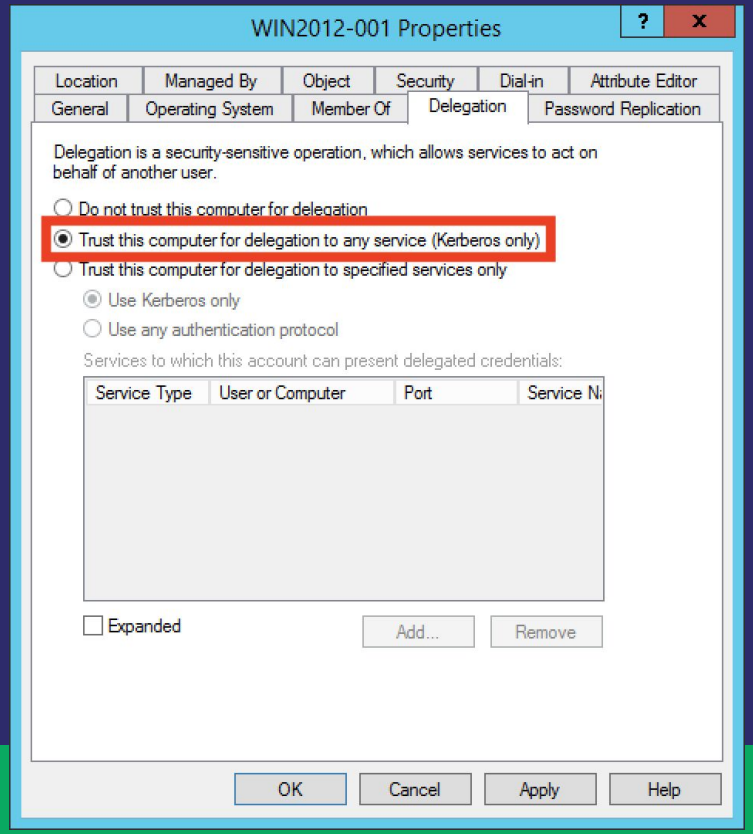
Kerberoast

- Technique created by Tim Medin in 2014
- Any domain-authenticated principal can request a TGS ticket for a Kerberos service in the domain
- That ticket is signed/encrypted using the NTLM hash of the account associated with the service
- Weak passwords = easily cracked TGS tickets
- **Any user account with an SPN is potentially vulnerable to this attack**

Unconstrained Delegation

- Computers may be trusted for delegation to any kerberos service on any system
- Once an account authenticates to that system via kerberos, the computer can fully impersonate that user to any other system in AD
- If a domain admin authenticates to that system, even using a non-interactive logon, that domain admin is owned!

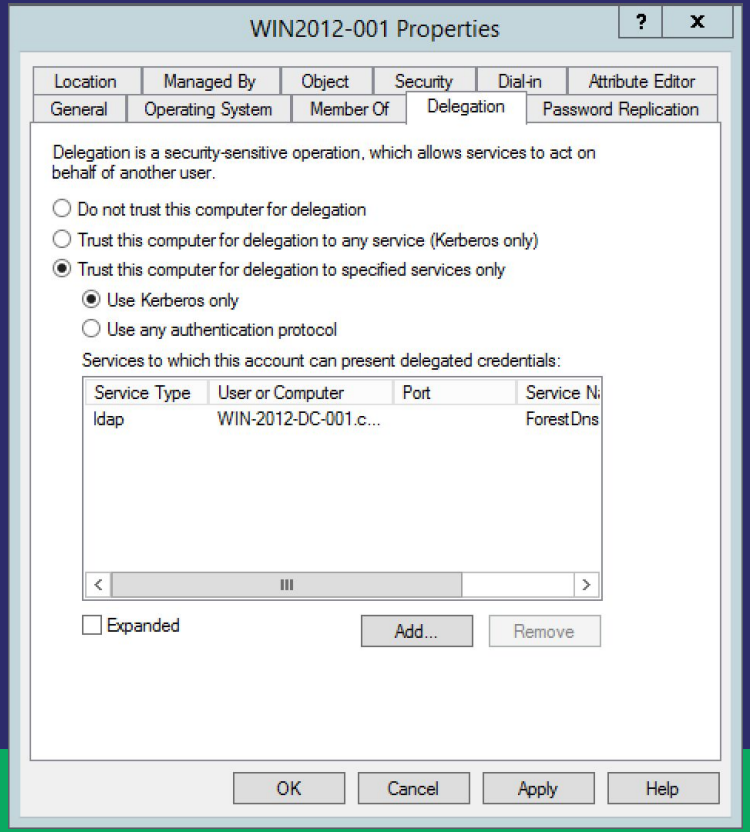
Unconstrained Delegation



Constrained Delegation

- Users/Computers may be trusted for delegation to specific services on specific systems
- In reality, the service portion of the ticket is not verified, meaning you can target ANY service!
- That computer can then impersonate **any** user in the domain at **any** time to those specific services
- Accounts marked as “Sensitive and Cannot be Delegated”, or added to the “Protected Users Group” are not vulnerable to this attack

Constrained Delegation



THANKS!

- specterops.io
- @SpecterOps
- @_wald0
- @CptJesus
- Link to this deck: `https://bit.ly/2ZQIfGY`
- Join the BloodHound Slack: https://bloodhoundgang.herokuapp.com