Slides: https://github.com/h3xg4m3s

Twitter: @h3xg4m3s Slides linked in tweet

Attacking Active Directory

RYAN PRESTON

Slack: awsm

Attacking Active Directory
Defining Active

"The Active Directory directory service is a distributed database that stores and manages information about network resources, as well as application-specific data from directory-enabled applications."

https://technet.microsoft.com/en-us/library/cc759073%28v=ws.10%29.aspx

Attacking Active Directory
Defining Active

What's an active directory
-A list of objects
-*Everything* is an object

What's a Forest
-a complete instance of active directory.
-top level container holding all domain containers
-*Security* boundary

What's a Domain
-Container object
-*Administrative* boundary

Objects
-Users, Systems, Resources, Services

Attacking Active Directory
Defining Active

What's an active directory
-A list of objects
-*Everything* is an object

What's a Forest
-a complete instance of active directory.
-top level *container* holding all domain containers
-*Security* boundary

What's a Domain
-Container object
-*Administrative* boundary

Objects
-Users, Systems, Resources, Services

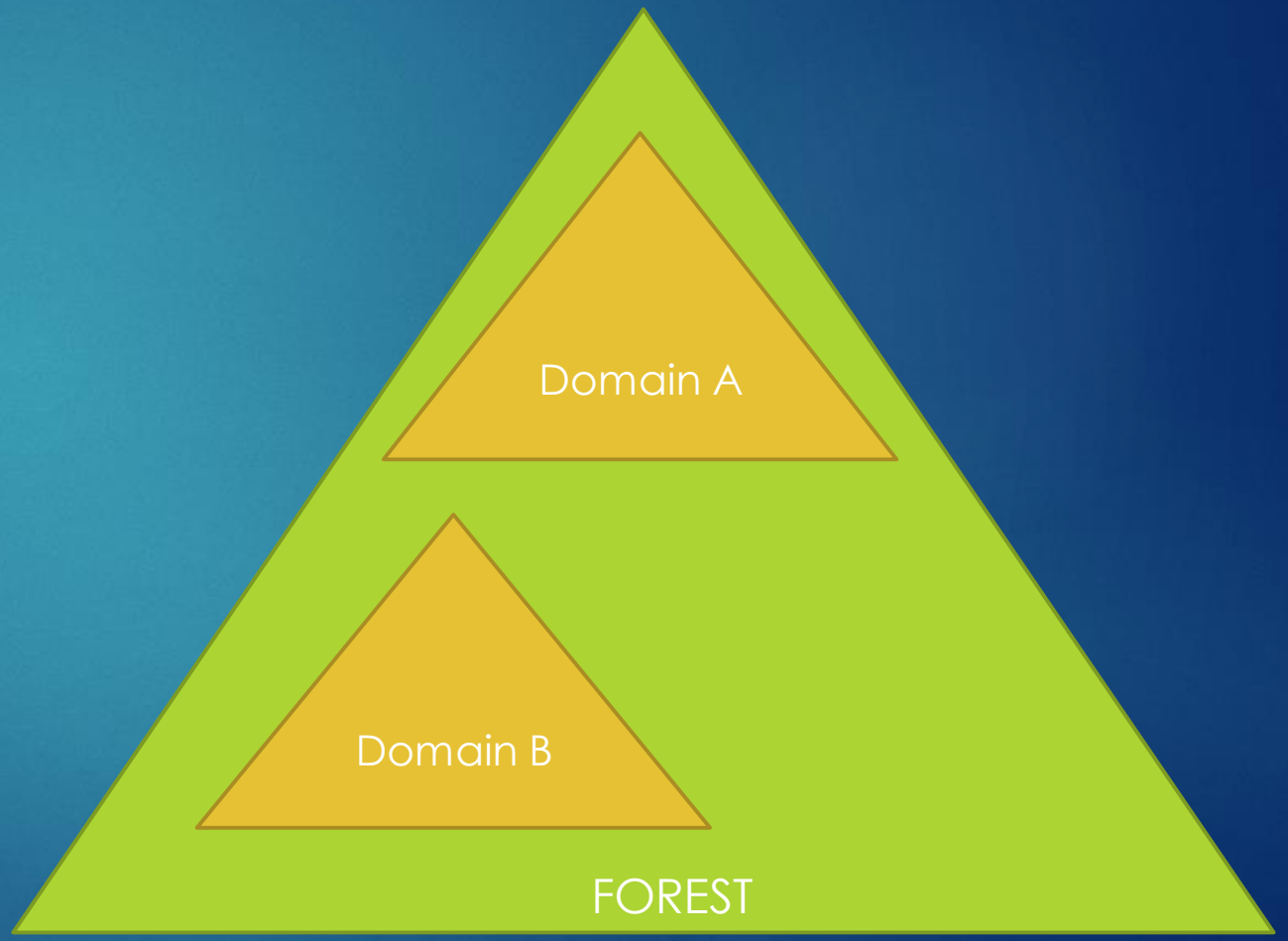
Attacking Active Directory
Defining Active

What's an active directory
-A list of objects
-*Everything* is an object

What's a Forest
-a complete instance of active directory.
-top level container holding all domain containers
-*Security* boundary

What's a Domain
-*Container* object
-*Administrative* boundary

Objects
-Users, Systems, Resources, Services



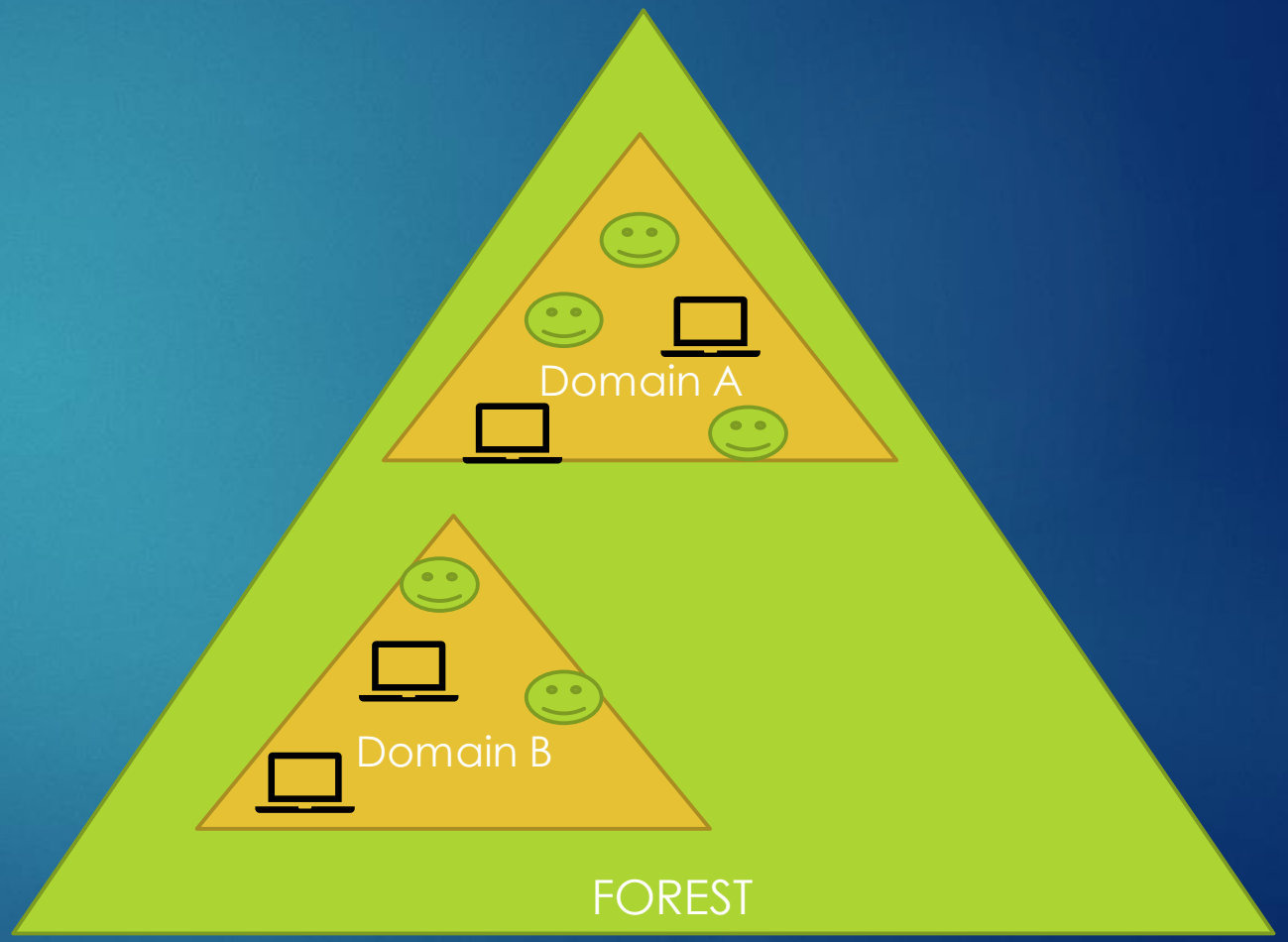
Attacking Active Directory
Defining Active

What's an active directory
-A list of objects
-*Everything* is an object

What's a Forest
-a complete instance of active directory.
-top level container holding all domain containers
-*Security* boundary

What's a Domain
-*Container* object
-*Administrative* boundary

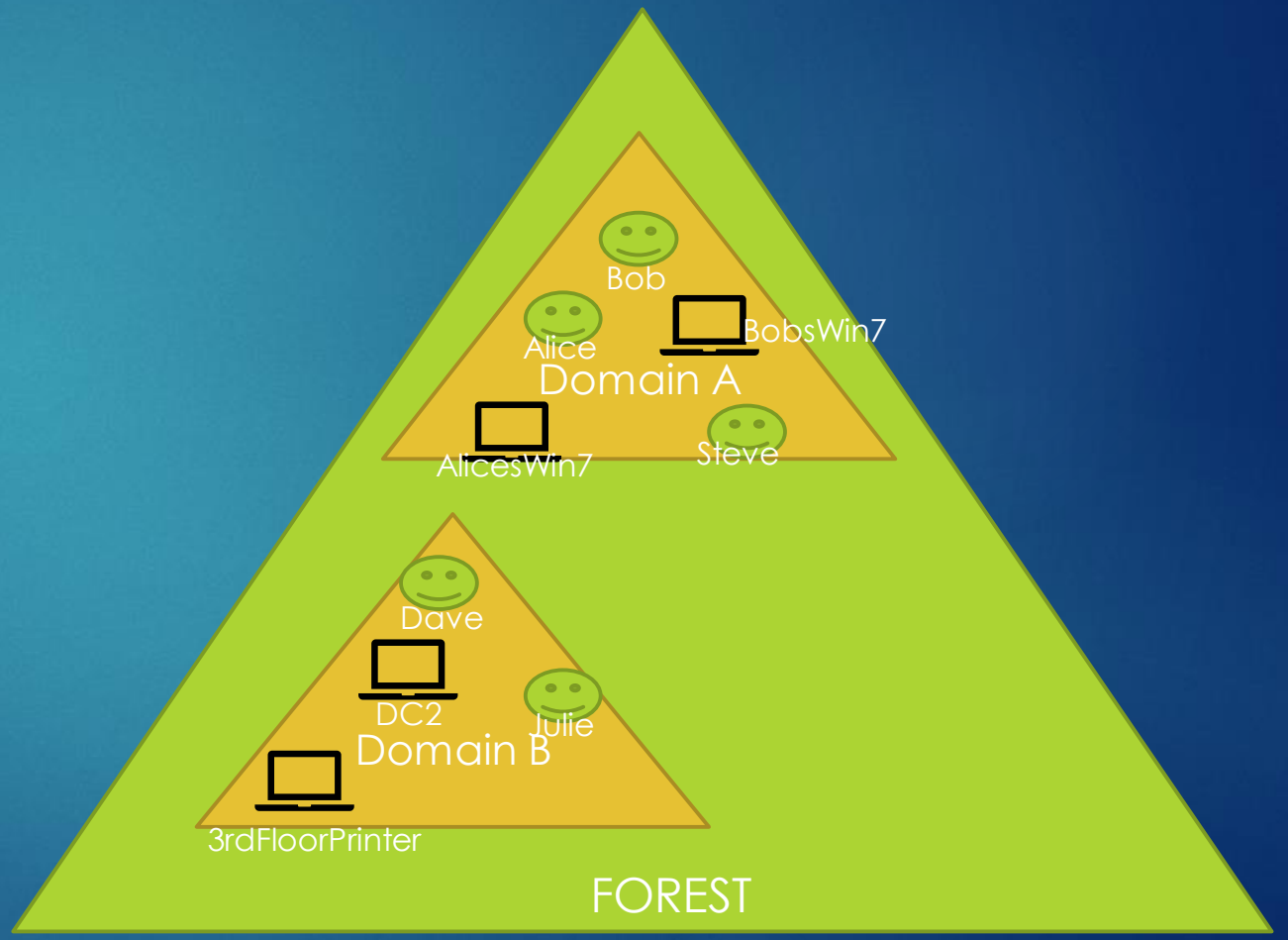
Objects
-Users, Systems, Resources, Services



Attacking Active Directory
Defining Active

Objects have attributes
-names
-IP address
-location
-permissions

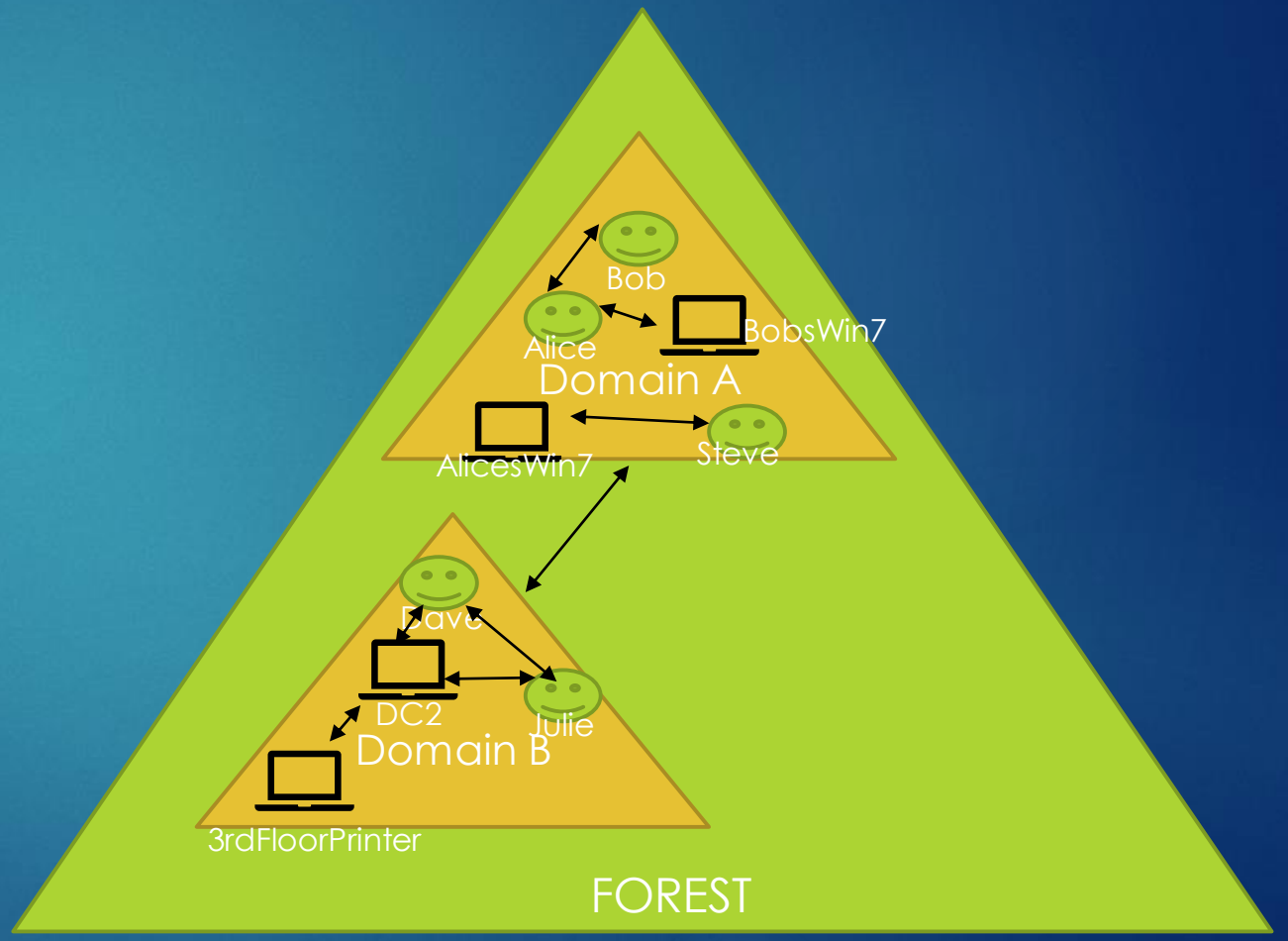
What's so Active?
-Always changing
-Replicating data throughout
-Attributes create relations



Attacking Active Directory
Defining Active

Objects have attributes
-names
-IP address
-location
-permissions

What's so Active?
-Always changing
-Replicating data throughout
-Attributes create relations



Attacking Active Directory

Attacking Active Directory
Penetration Testing

Attacking Active Directory should not be confused with a Pentest

Attacking Active Directory
Penetration Testing

Generic Pentest:

1. Pre-engagement Interactions (scoping)
2. Intelligence Gathering (Recon)
3. Vulnerability Analysis (Scanning)
4. Exploitation
5. Post Exploitation --- where we fall
6. Reporting

Attacking Active Directory
What is Involved

uber l33t 0-dayz !?!?!

Attacking Active Directory
What is Involved

~~uber l33t 0-dayz !?!?!~~
-Not necessarily
-Often not at all

Exploiting weaknesses in configurations

Attacking Active Directory
What is Involved

~~uber l33t 0-dayz !?!?!~~
-Not necessarily
-Often not at all

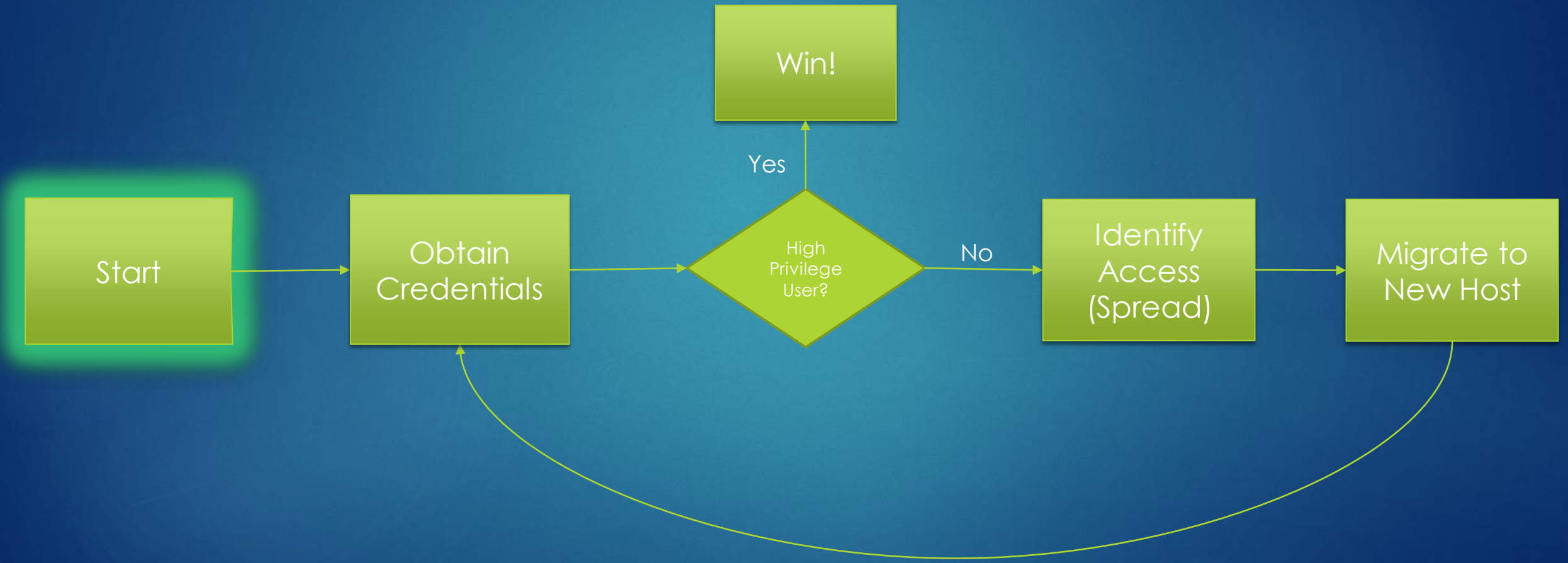
Exploiting weaknesses in configurations

Discovering hidden and/or unintended relationships inside Active Directory

Attacking Active Directory
Endgame

- All the passwords!
- Find the loot!
- Provide remediation and detection advice.

Attacking Active Directory Basic Theory



Attacking Active Directory
External Attack Surface

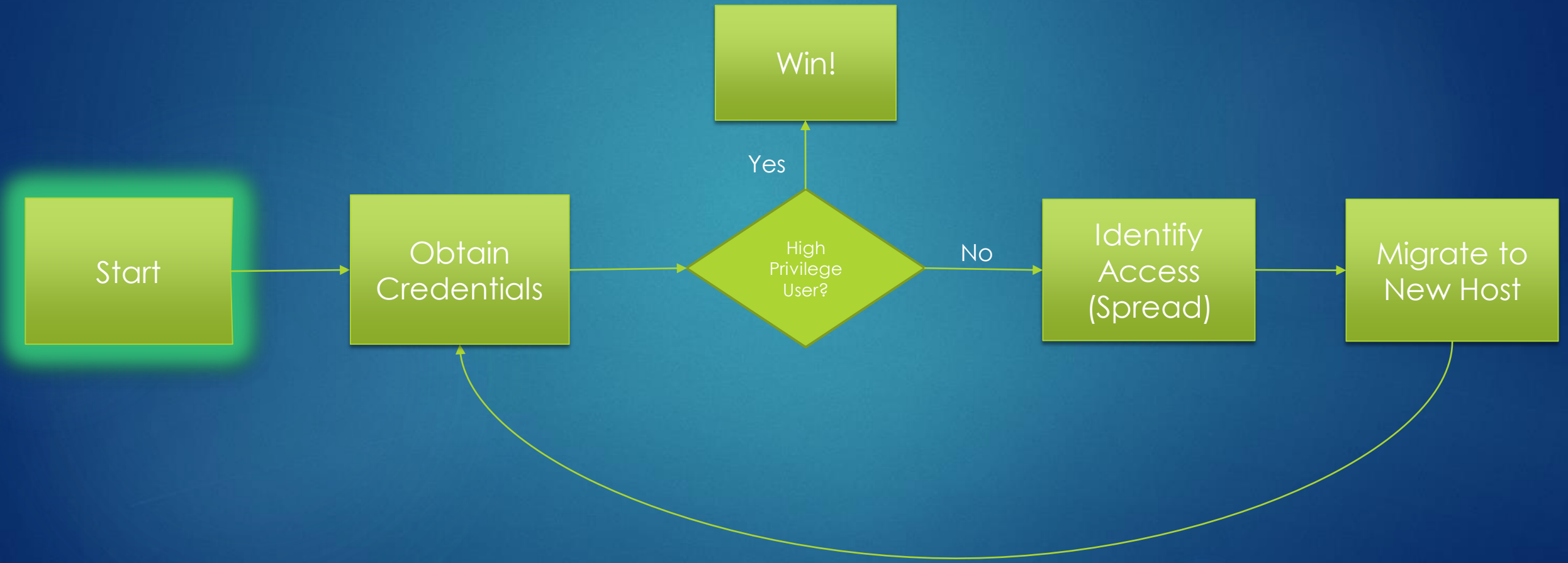
3 *Primary* ~~Endpoints~~ Entry points

Web Servers
-no DA's should log in here*

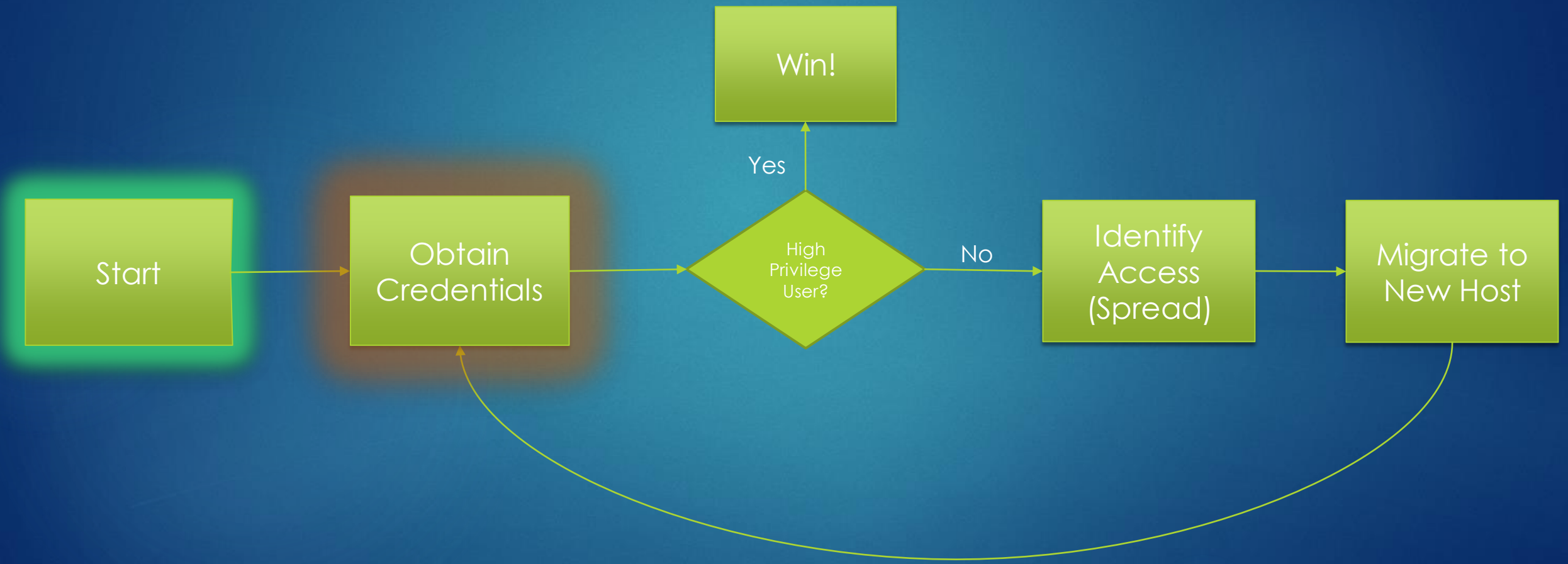
Users!

VPN

Attacking Active Directory Basic Theory



Attacking Active Directory
Get Creds!



Attacking Active Directory Obtaining Credentials

Pre-Compromise

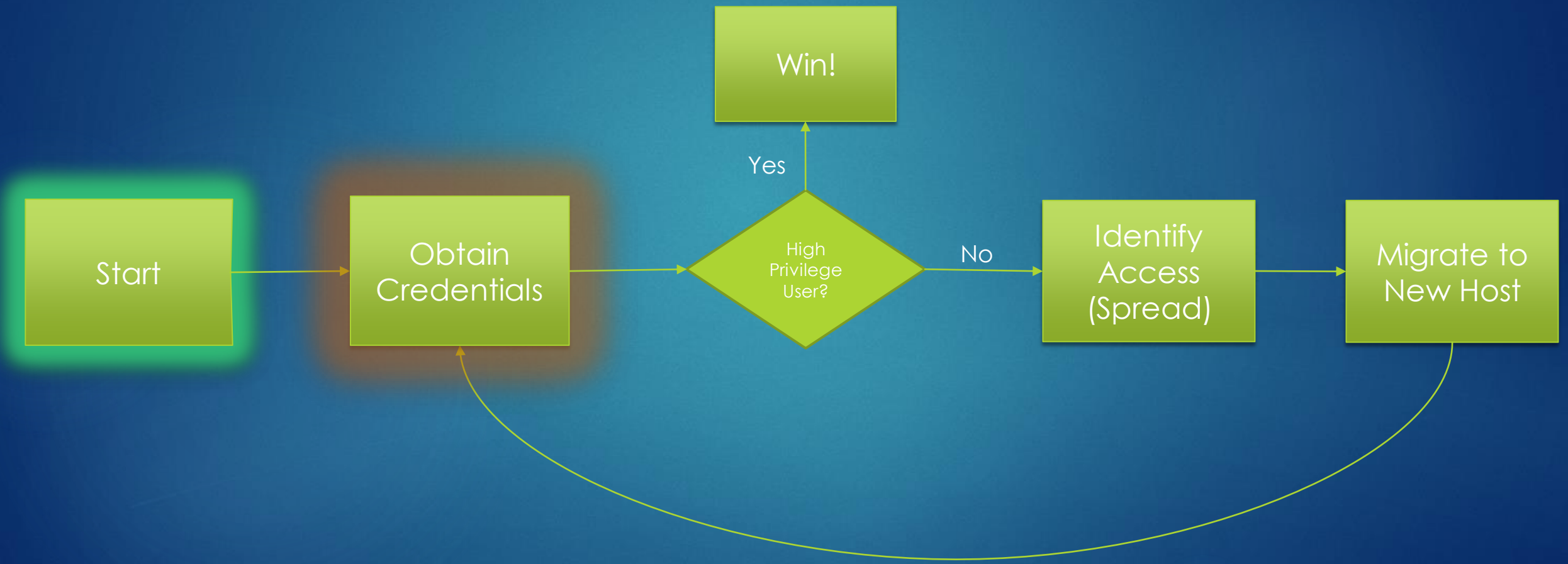
Responder
Phishing
Password Spraying
Default Credentials

Post-Compromise

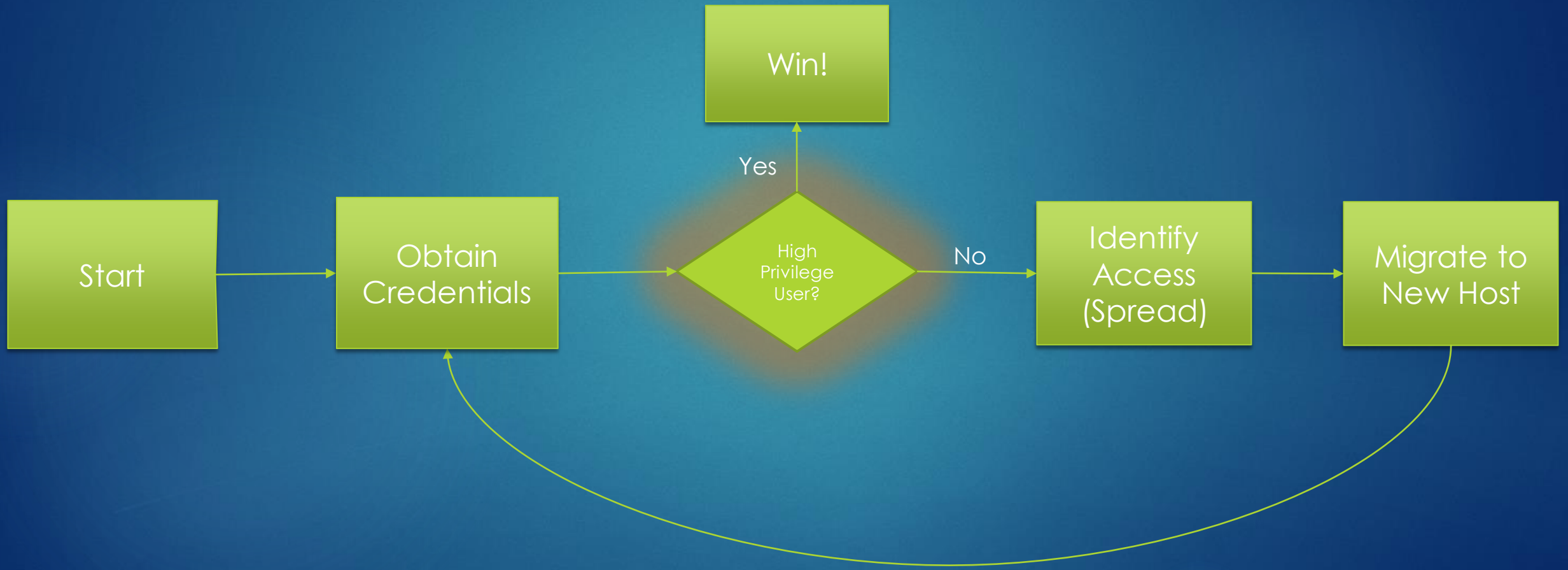
Mimikatz
ProcDump
Passwords.csv
GPP Passwords in SYSVOL
Kerberoasting

Actual Exploit ?!?
-ms08-067
-ms14-068
-ms17-010
-Deserialization
-SQLi
-etc..

Attacking Active Directory
Have Creds



Attacking Active Directory
Check yo Privilege



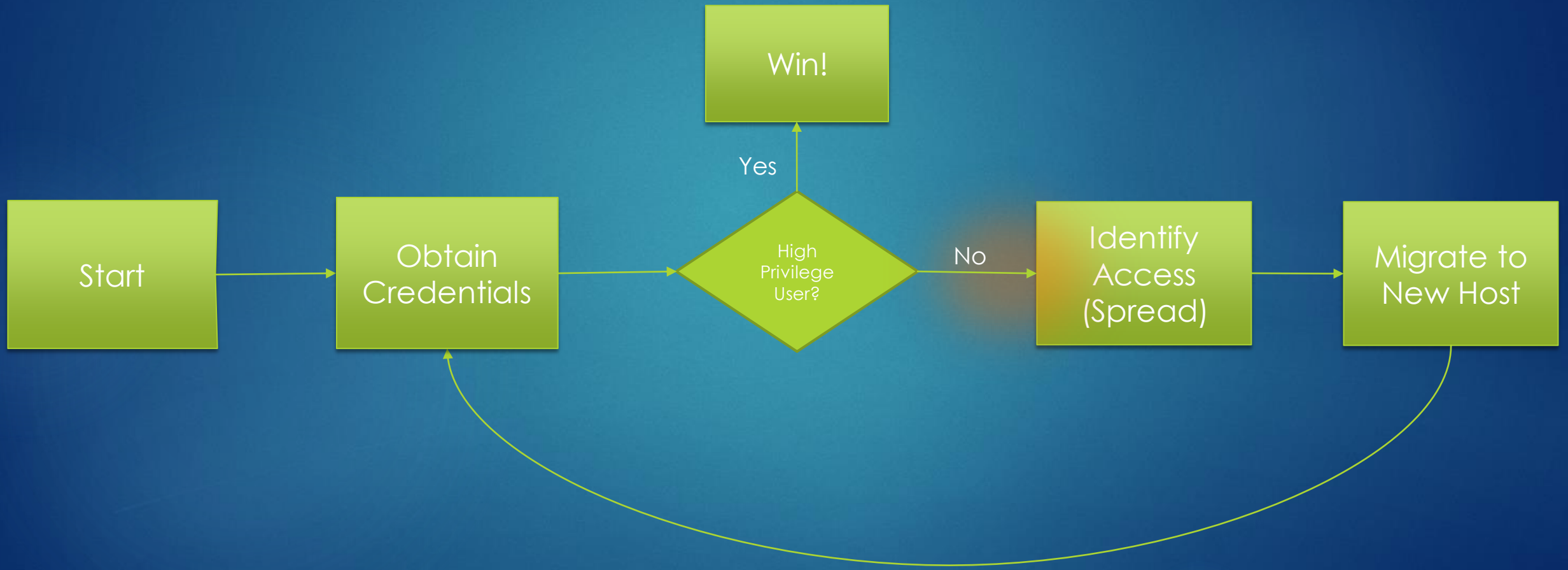
@h3xg4m3s

Attacking Active Directory

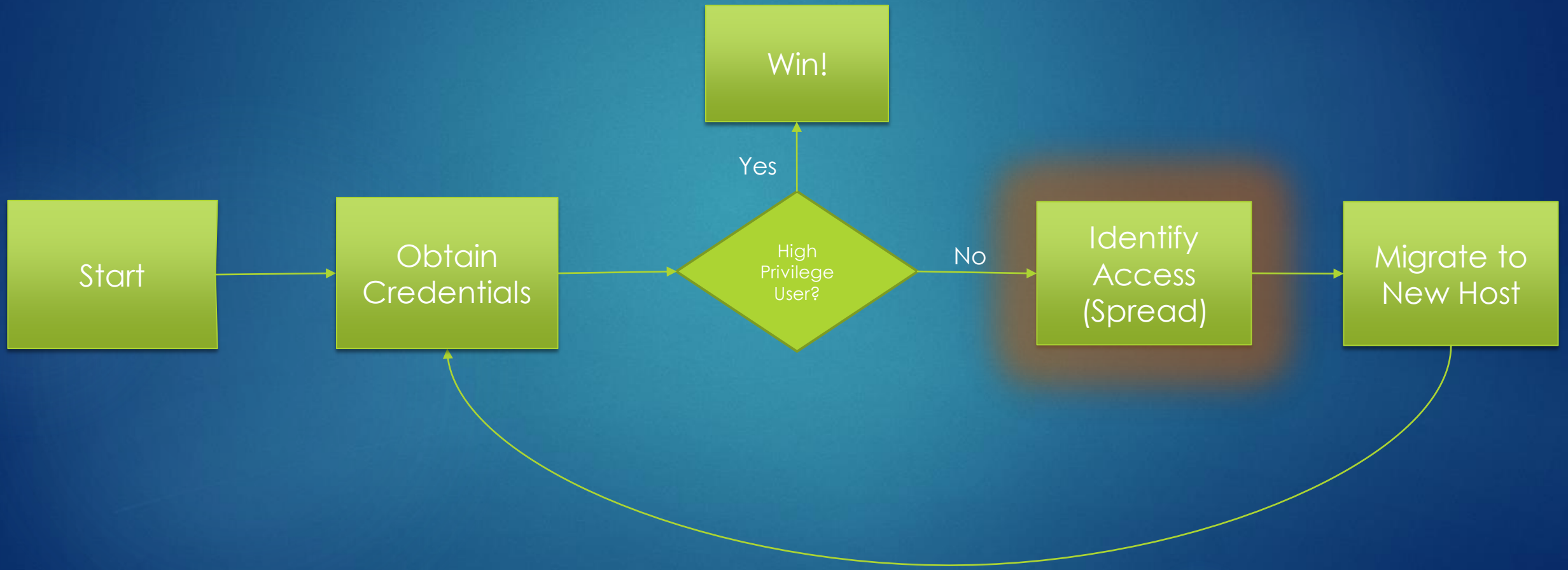
Privileged Accounts	
Enterprise Admins	Account Operators
Domain Admins	Backup Operators
Schema Admin	Print Operators
BUILTIN\Administrators	Server Operators
Domain Controllers	Group Policy Creators Owners
Read-only Domain Controllers	Cryptographic Operators

https://technet.microsoft.com/en-us/library/dn579255(v=ws.11).aspx#BKMK_Admins

Attacking Active Directory Not Privileged



Attacking Active Directory
Where can we go?



Attacking Active Directory Identify Access

Where are the privileged users?

Where can this user go?

How can I get those high privileged accounts?

Attacking Active Directory
Identify Access

Metasploit

post/windows/gather/local_admin_search_enum
auxiliary/scanner/smb/smb_login

NMAP

nmap 192.168.0.1 -script=smb-enum-groups.nse –script=smb-enum-users.nse –script-args 'smbdomain=DOMAIN,smbuser=USER,smbpass/smbhash=X

PowerView (Also included in Empire)

Invoke-FindLocalAdminAccess
Invoke-CheckLocalAdminAccess
Invoke-ShareFinder –CheckAdmin
Get-NetLocalGroup –ListGroups <workstation>
Invoke-EnumerateLocalAdmin (returns the local admin group for each machine in the domain)

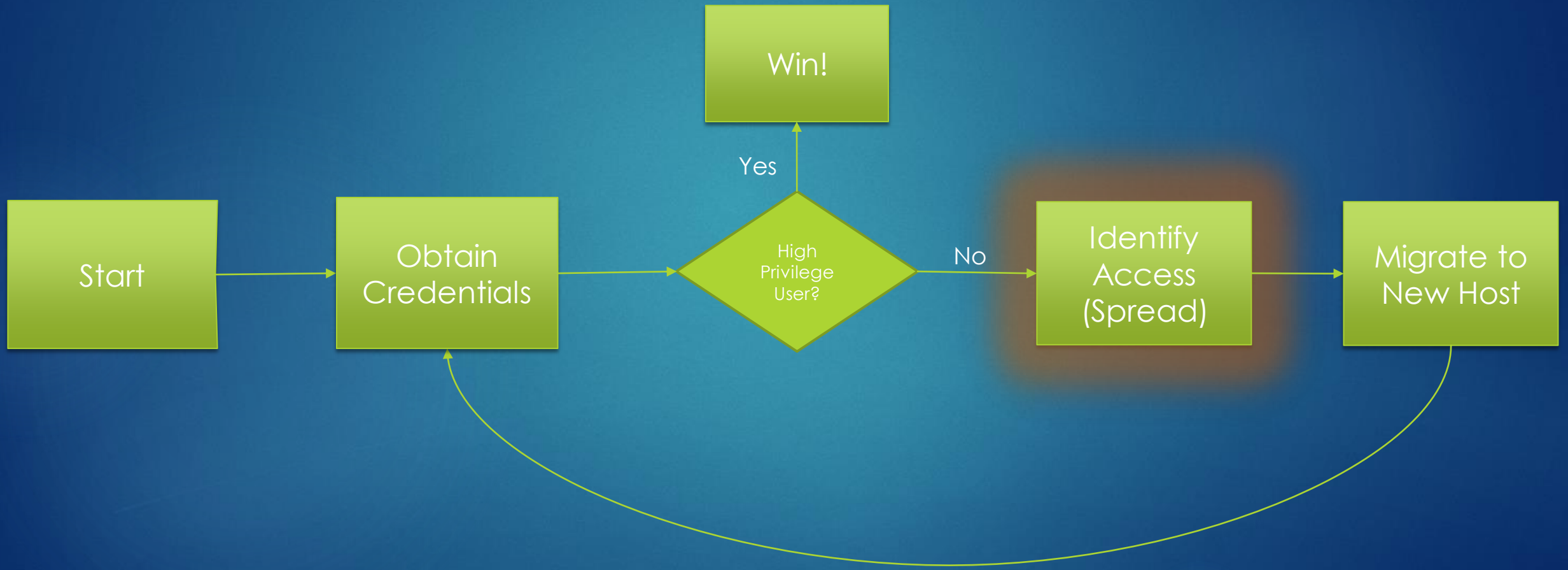
Command Line

whoami /groups
net user <username> /domain

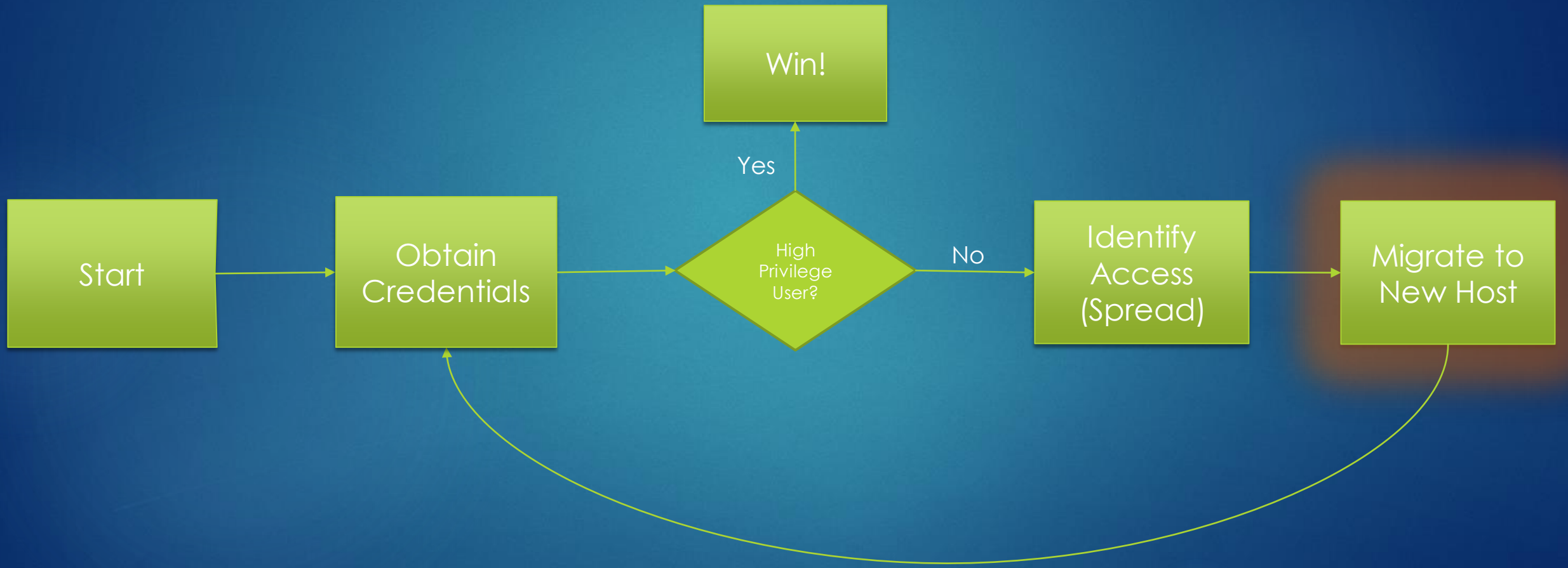
Powershell

```
function get-localadmin {
  param ($strcomputer)

  $admins = Gwmi win32_groupuser –computer $strcomputer
  $admins = $admins | ? {$_.groupcomponent –like '*"Administrators"'}

  $admins |% {
  $_.partcomponent –match ".+Domain\=(.+)\,Name\=(.+)$" > $nul
  $matches[1].trim("") + "\" + $matches[2].trim("")
} }
```

Attacking Active Directory Access has been Identified



Attacking Active Directory
On the move



Attacking Active Directory Lateral Movement

Moving Laterally Techniques

- ✓ Psexec
- ✓ Netsh
- ✓ PS Remoting
- ✓ WMI
- ✓ Pass-the-Hash
- ✓ Overpass-the-Hash
- ✓ Pass-the-ticket
- ✓ Golden Tickets
- ✓ Token Impersonation
- ✓ Skeleton Key
- ✓ Silver Tickets
- ✓ RDP
- ✓ Unauthed VNC

Attacking Active Directory
Pass the hash sidenote

Moving Laterally Techniques

- ✓ Psexec
- ✓ Netsh
- ✓ PS Remoting
- ✓ WMI
- ✓ Pass-the-Hash
- ✓ Overpass-the-Hash
- ✓ Pass-the-ticket
- ✓ Golden Tickets
- ✓ Token Impersonation
- ✓ Skeleton Key
- ✓ Silver Tickets
- ✓ RDP
- ✓ Unauthed VNC

But.. But.. MSFT Fixed pass the hash back in 2014 see KB2871997

Attacking Active Directory
Pass the hash sidenote

"Accounts that are members of the localgroup 'Administrators' are no longer able to execute code with WMI or PSEXEC"

Well…….

Except for the RID 500 built-in Administrator account, even if it's renamed.

AND

Domain accounts that are granted administrative privileges over a machine can still pass-the-hash.

http://www.harmj0y.net/blog/penetesting/pass-the-hash-is-dead-long-live-pass-the-hash/

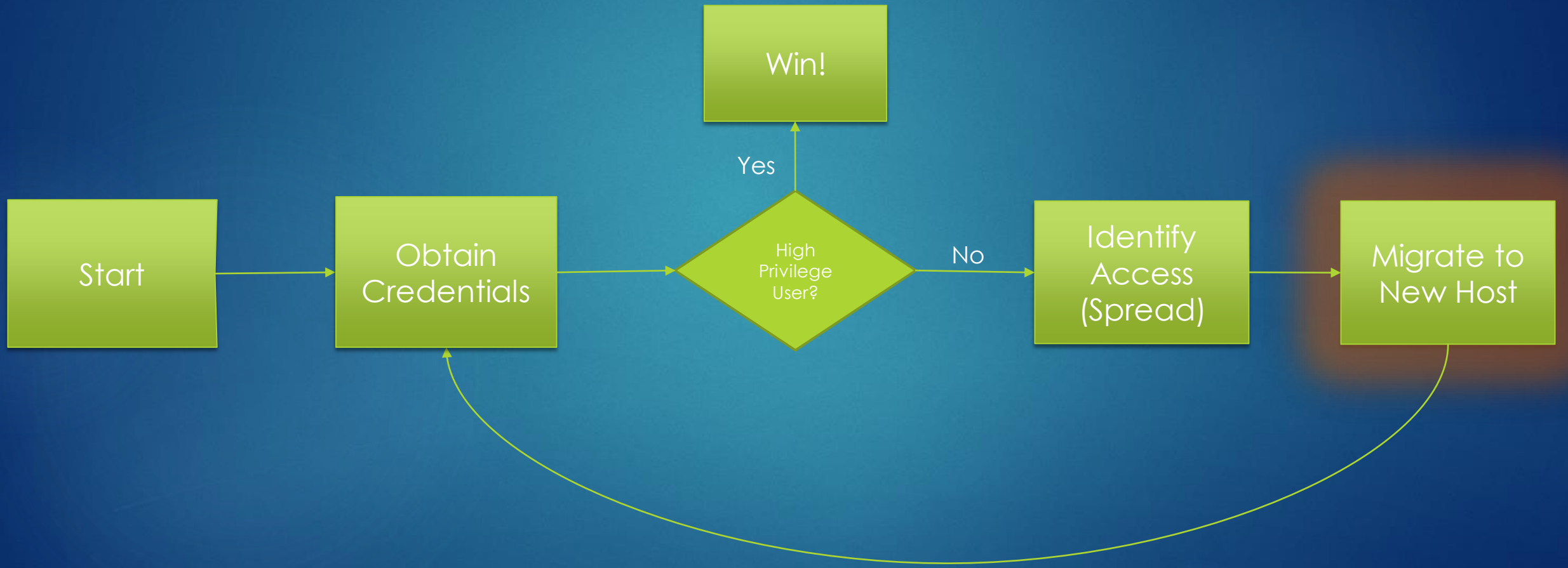
Attacking Active Directory

- Up to date environment
- Default Administrator Account Disabled
- Obtained creds for a local admin user from a different box

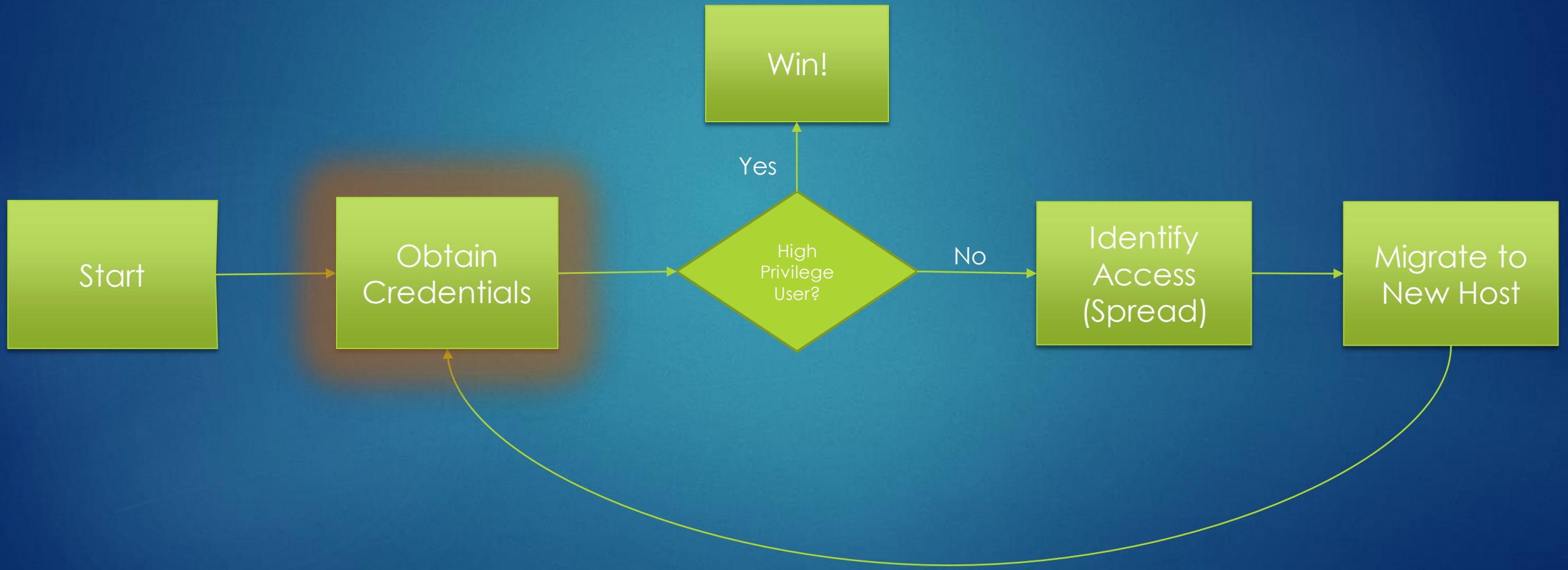
If you can crack the hash or obtain the plaintext creds (mimikatz?)
you can still RDP into the box

http://www.harmj0y.net/blog/penetesting/pass-the-hash-is-dead-long-live-pass-the-hash/

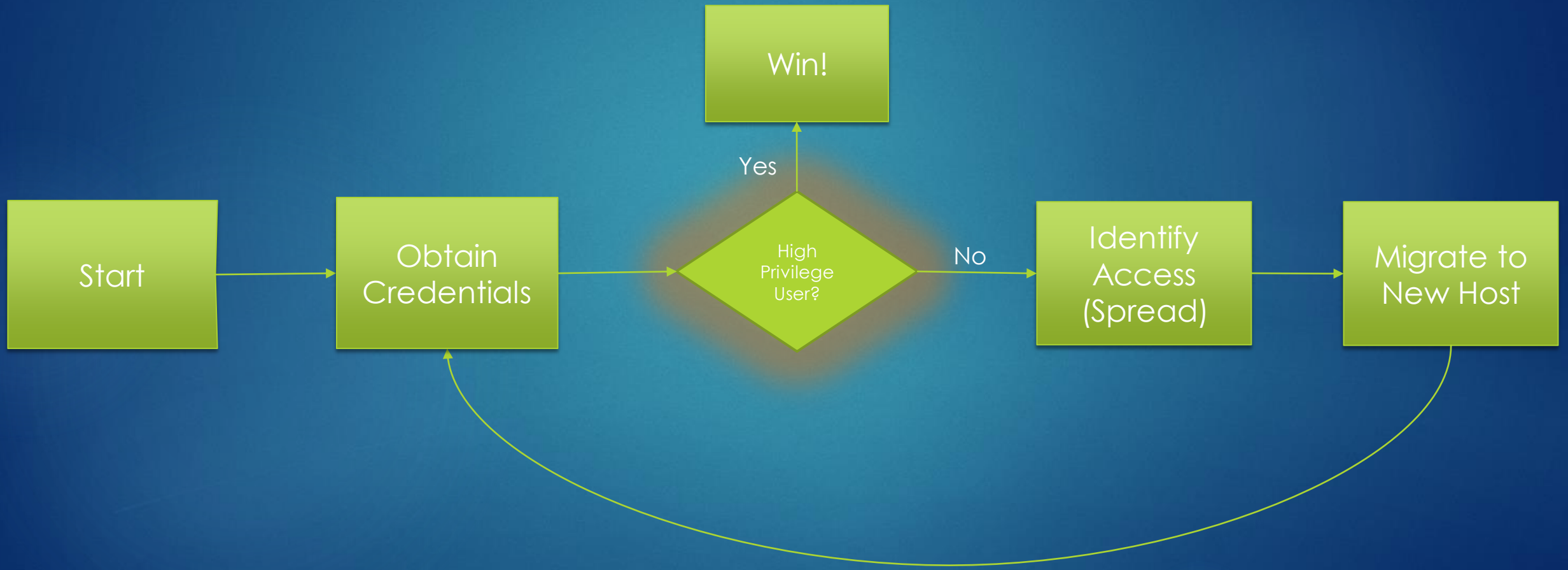
Attacking Active Directory
Back to Theory



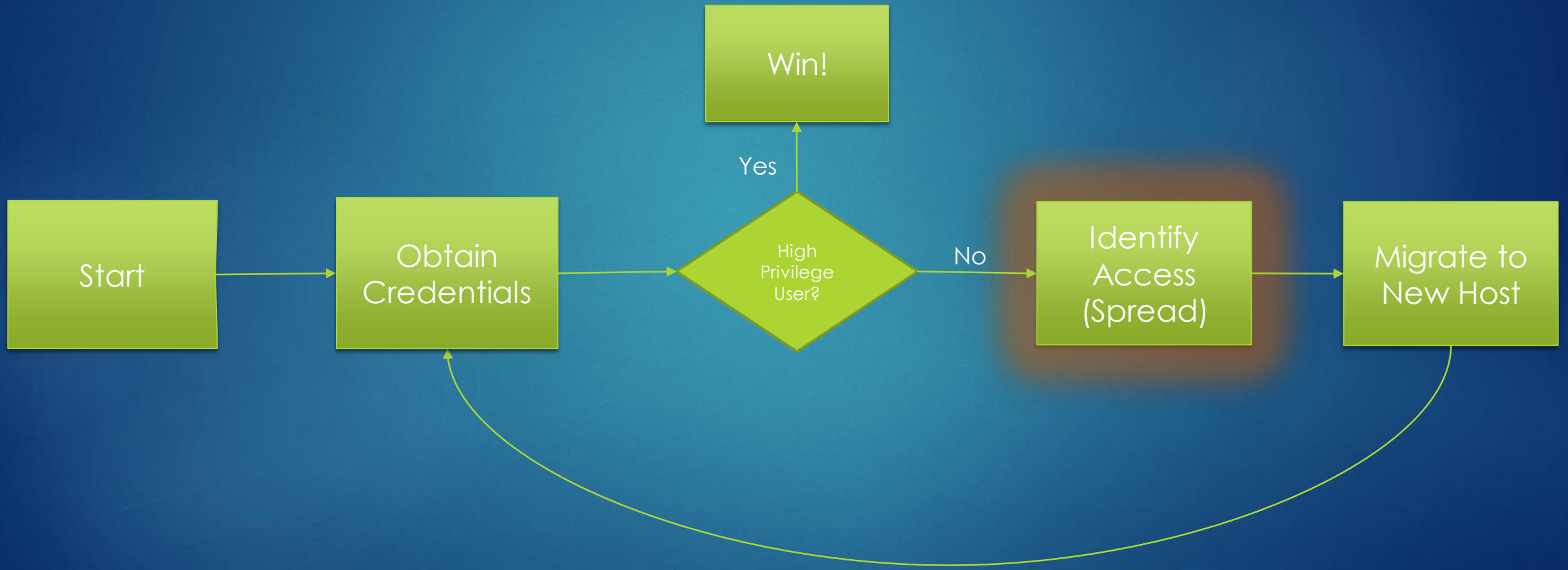
Attacking Active Directory
Rinse and Repeat



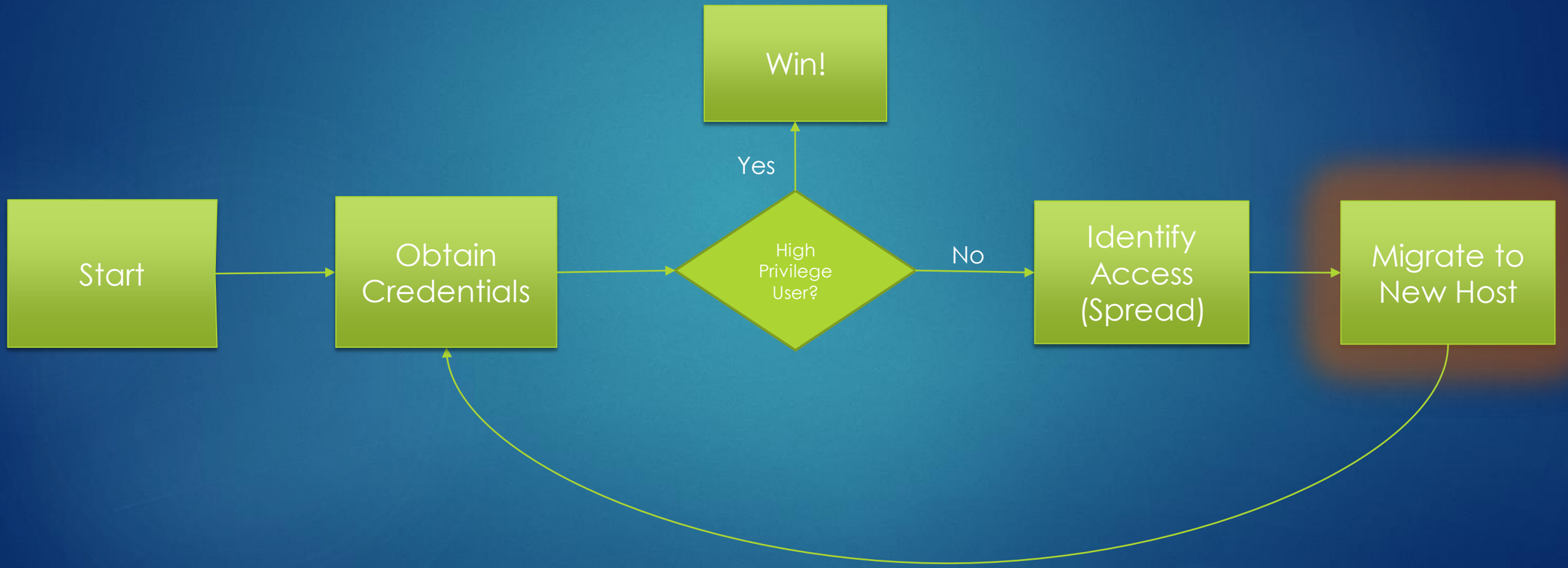
Attacking Active Directory
Rinse and Repeat



Attacking Active Directory
Rinse and Repeat



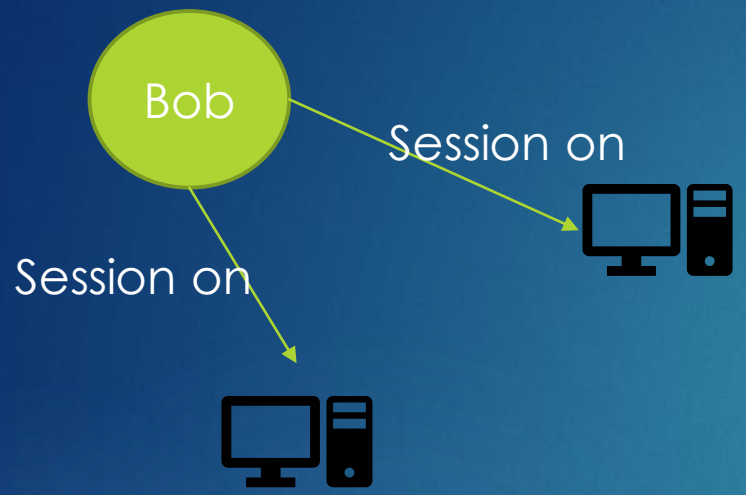
Attacking Active Directory
Rinse and Repeat



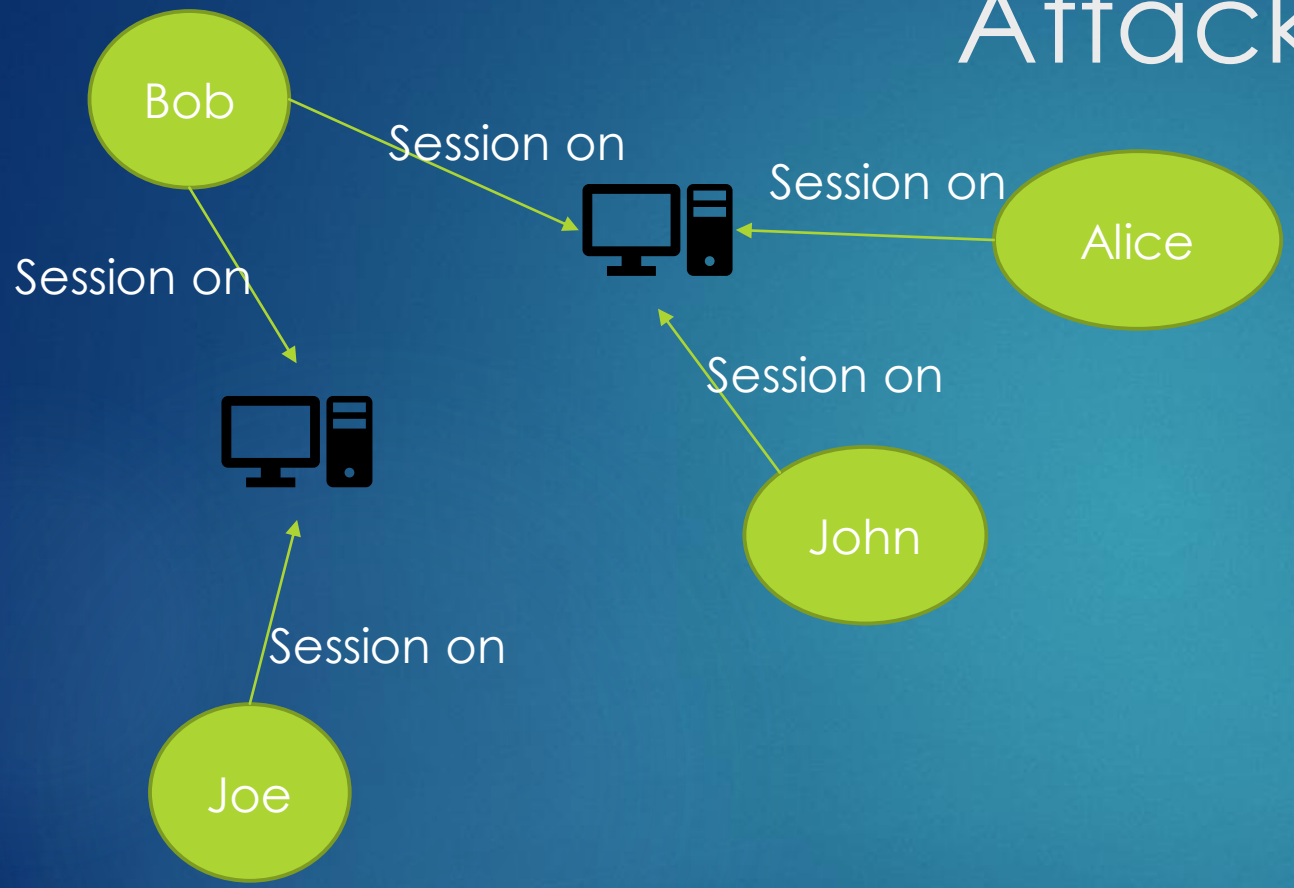
Attacking Active Directory
Back to Theory

Bob

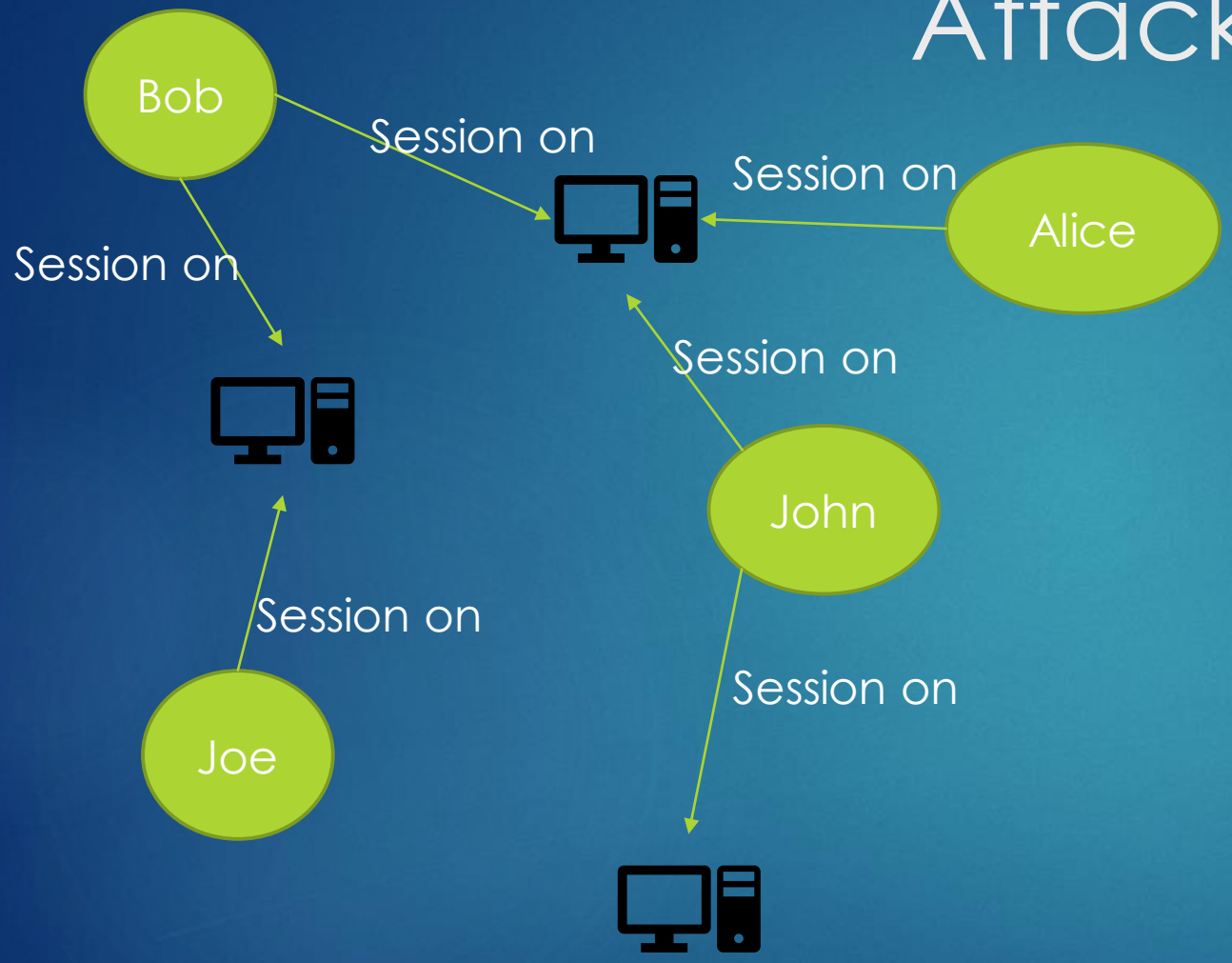
Attacking Active Directory Attack Path



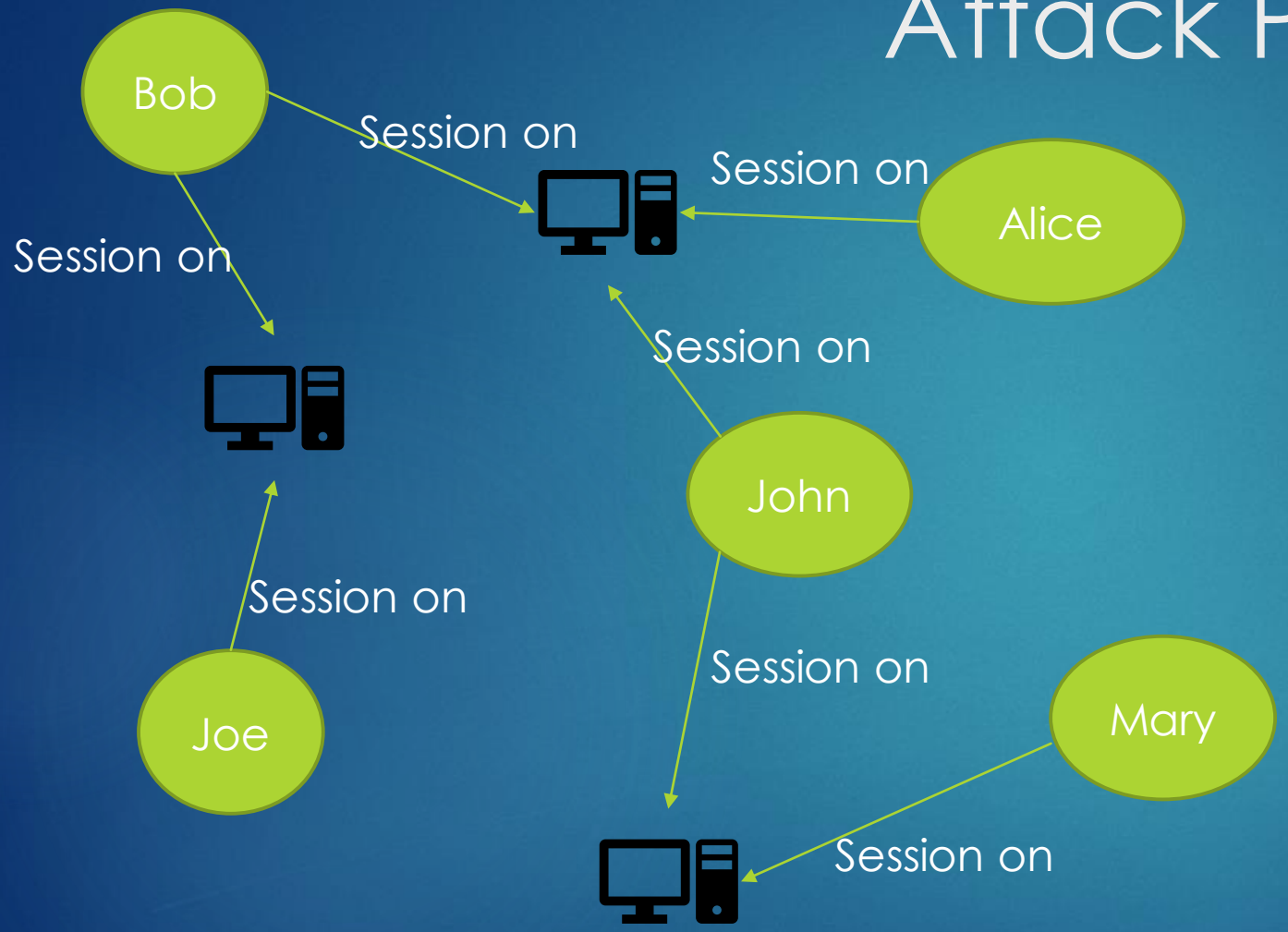
Attacking Active Directory Attack Path



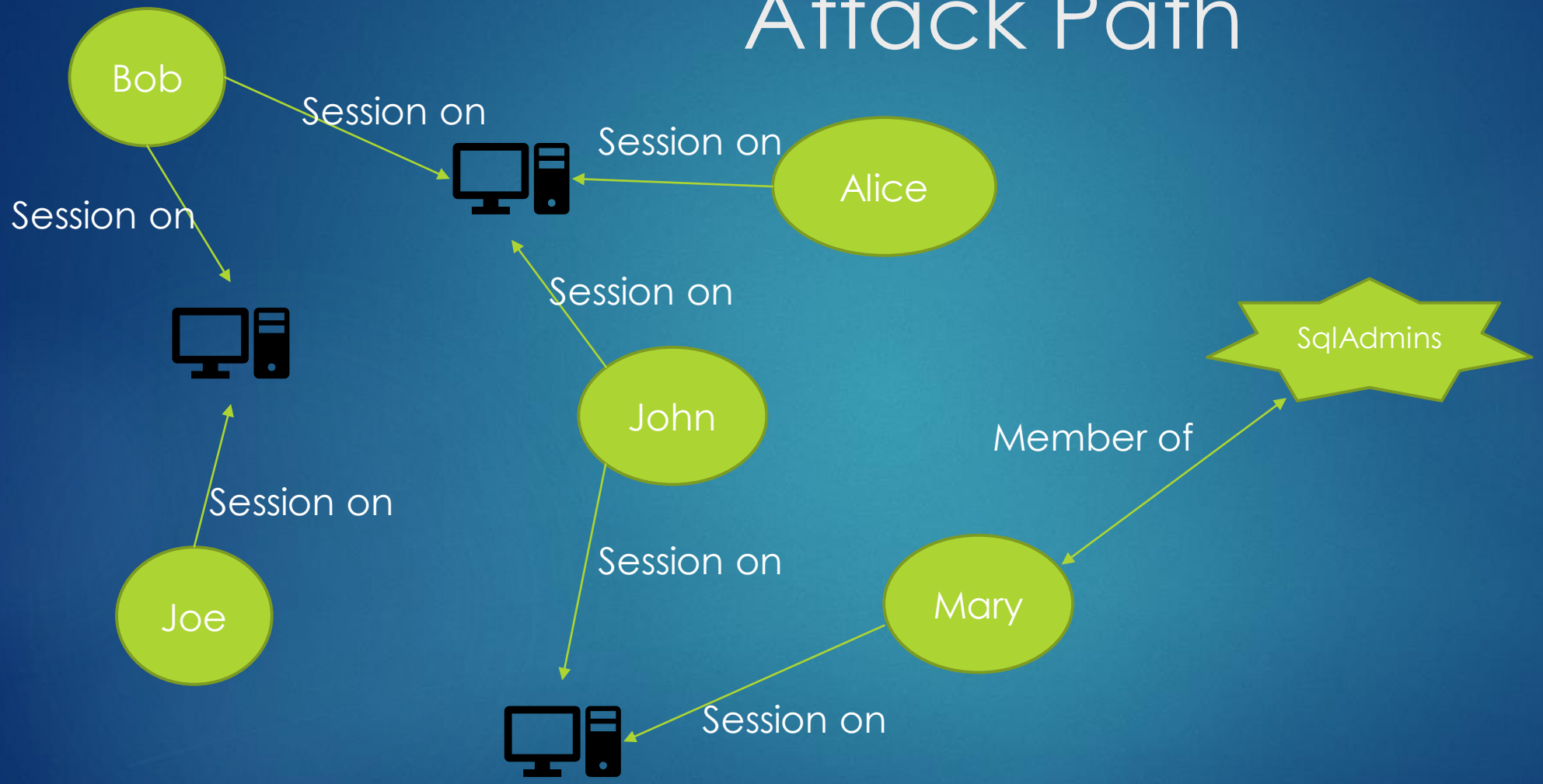
Attacking Active Directory Attack Path



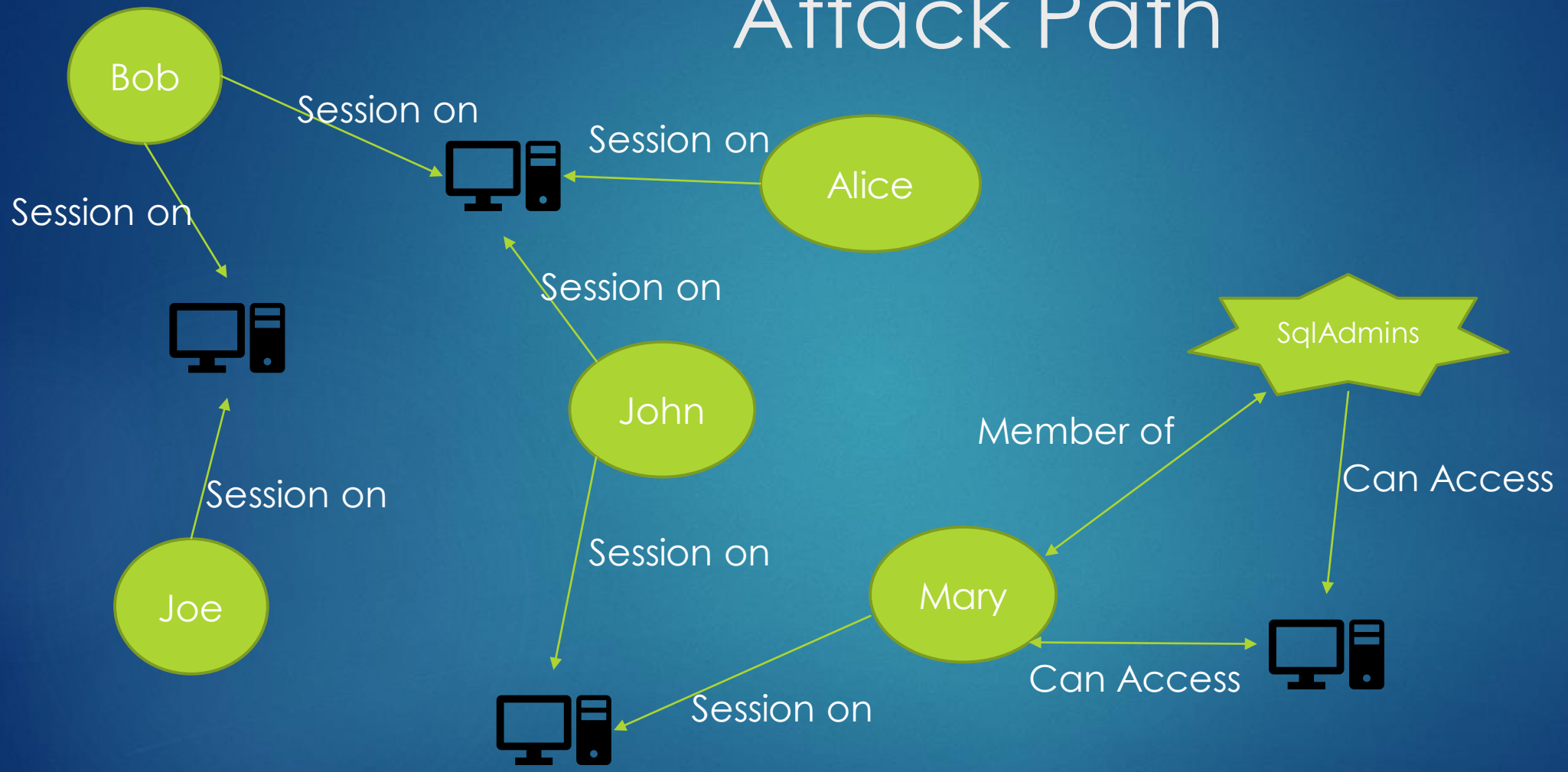
Attacking Active Directory Attack Path



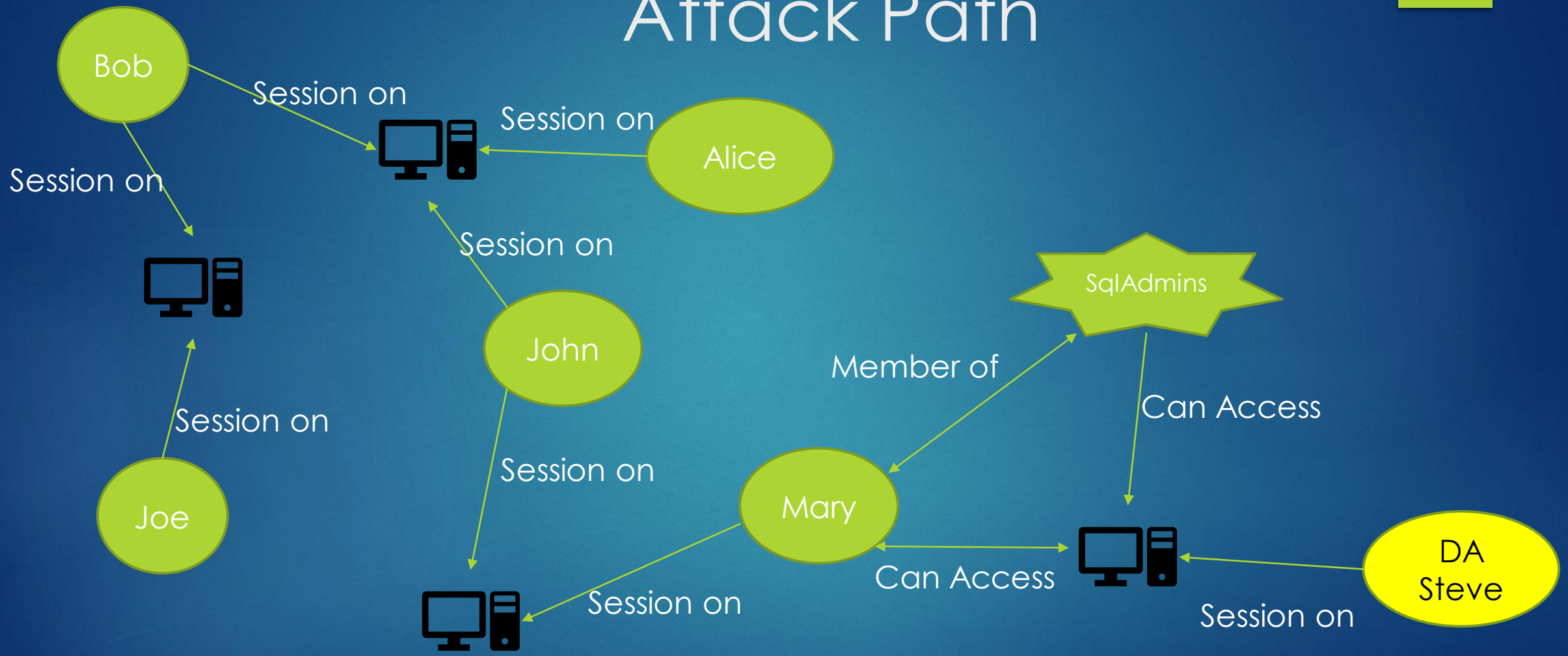
Attacking Active Directory Attack Path



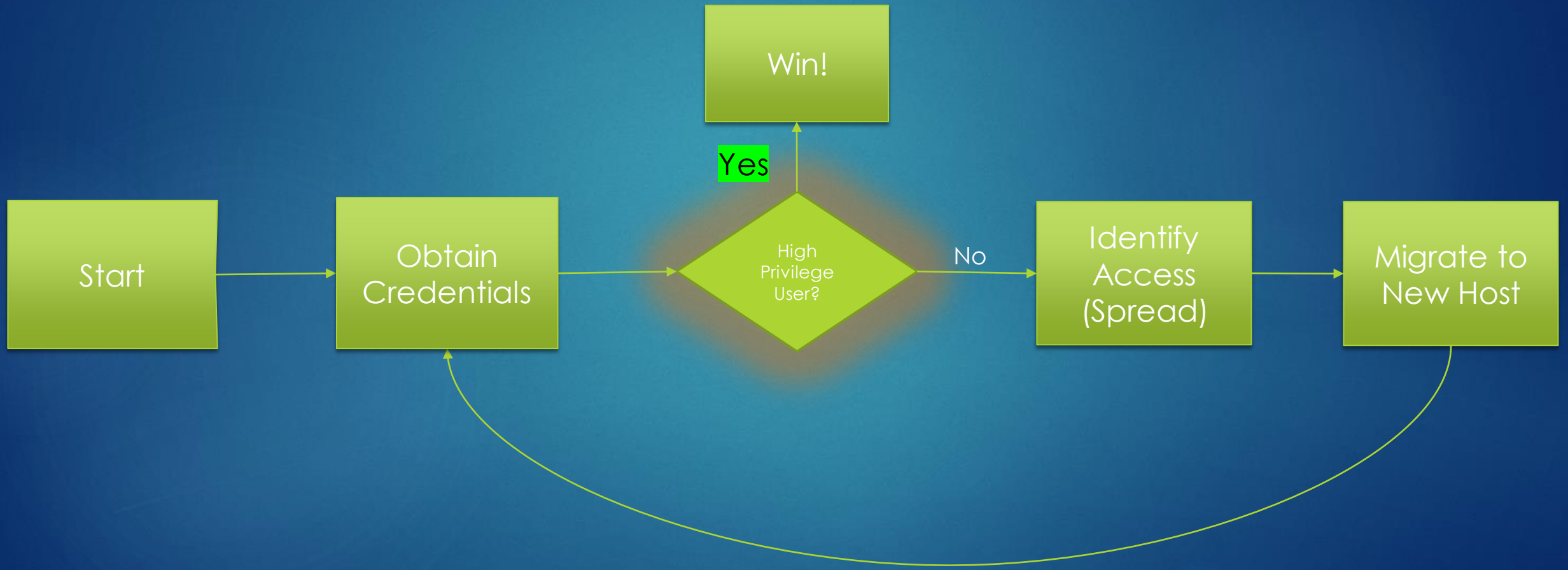
Attacking Active Directory Attack Path



Attacking Active Directory Attack Path

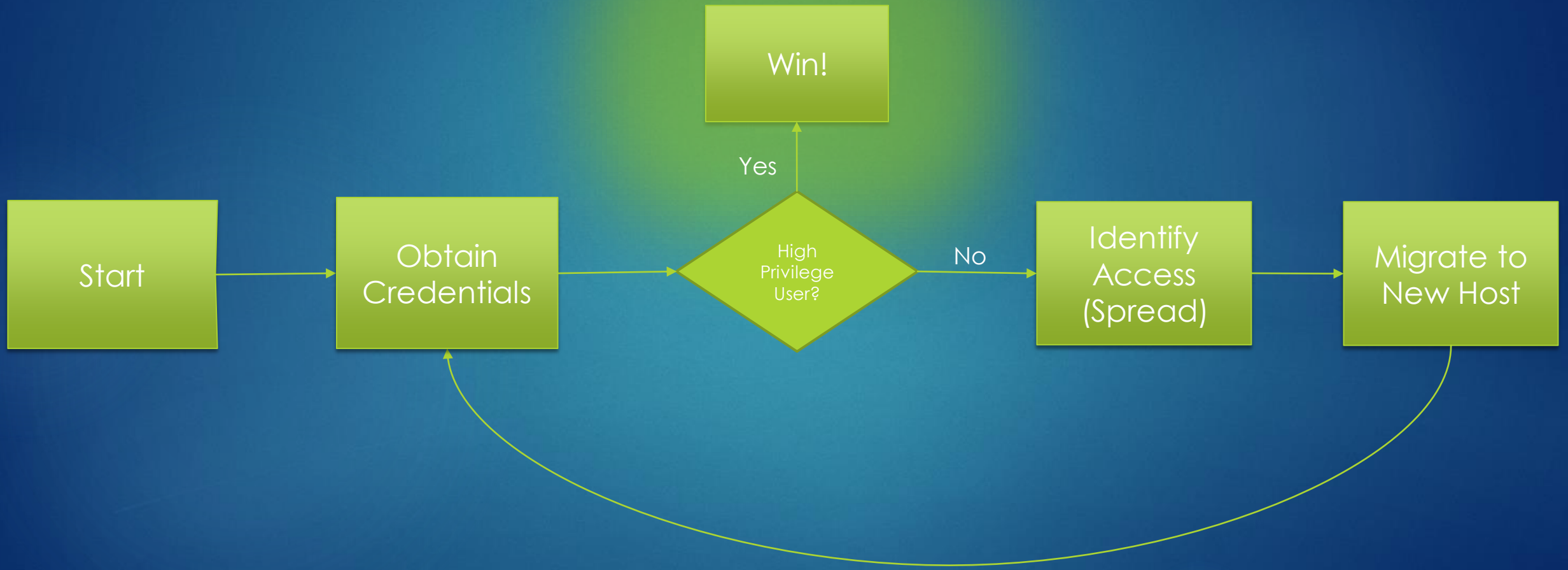


Attacking Active Directory Finally have High Privilege?!!



Attacking Active Directory

WIN



Attacking Active Directory

Attacking Active Directory Domain Admin

Do the hashdance

DCSync
Hashdump the DC
Volume Shadow Copy
ntdsxtract https://github.com/csababarta/ntdsxtract

Never Leaving

Golden Tickets
(lesser) Silver Tickets

Attacking Active Directory
You're not done!

- What is important?
- What do they value?
- Enterprise Admin?
- *Nix Environments?

Attacking Active Directory

Attacking Active Directory Toolz

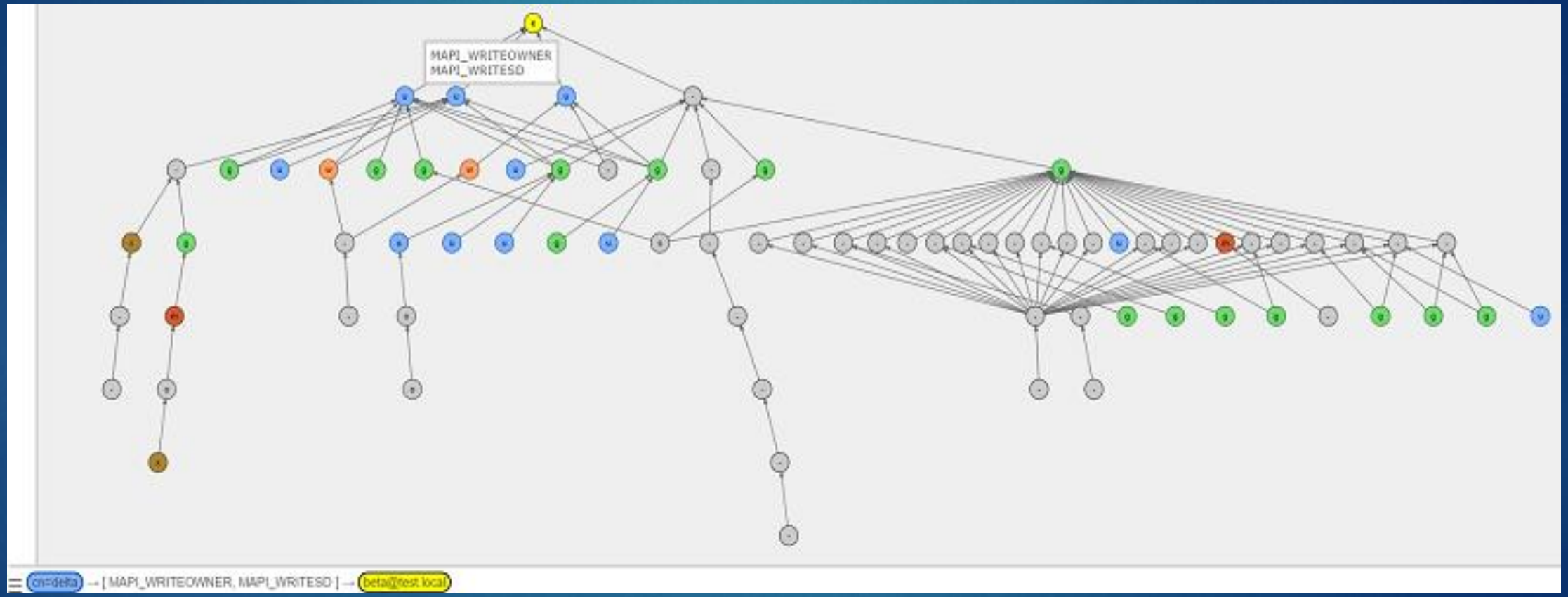
PowershellEmpire	https://github.com/EmpireProject/Empire
Metasploit	https://www.metasploit.com/
CrackMapExec	https://github.com/byt3bl33d3r/CrackMapExec
Responder	https://github.com/lgandx/Responder
Impacket	https://github.com/CoreSecurity/impacket
PowerSploit	https://github.com/PowerShellMafia/PowerSploit
Bloodhound	https://github.com/BloodHoundAD/BloodHound
Sharphound	https://github.com/BloodHoundAD/SharpHound
mimikatz	https://github.com/gentilkiwi/mimikatz/

Attacking Active Directory
Bloodhound / Sharphound

BloodHound is developed by @_wald0, @CptJesus, and @harmj0y.

Attacking Active Directory AD-Control-Paths

Latest AD-Control-Paths release "Who Can Read the CEO's Emails Edition"



Based off AD-Control-Paths By Lucas Bouillot and Emmanuel Gras
https://github.com/ANSSI-FR/AD-control-path

Attacking Active Directory Offensive AND Defensive

- Fantastic tools for both **Red** and **Blue** teams!

Quickly identify ‘control relations’ between objects in Active Directory

Highly complex attack paths visualized in graphs

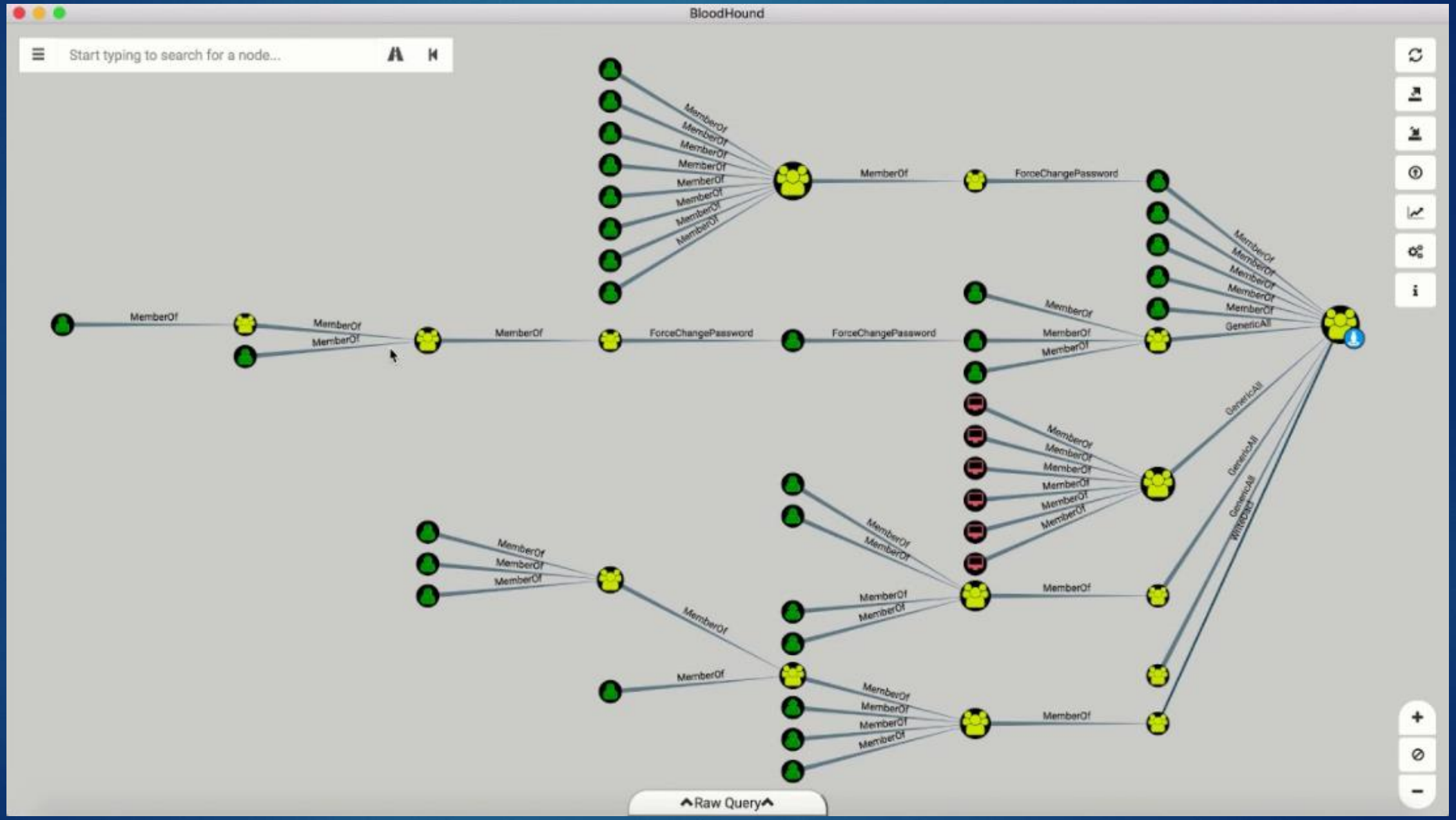
Attacking Active Directory Fast

Fantastic tools for both **Red** and **Blue** teams!

➡ Quickly identify ‘control relations’ between objects in Active Directory

Highly complex attack paths visualized in graphs

Bloodhound


BloodHound
Start typing to search for a node...
MemberOf
ForceChangePassword
GenericAll
Raw Query

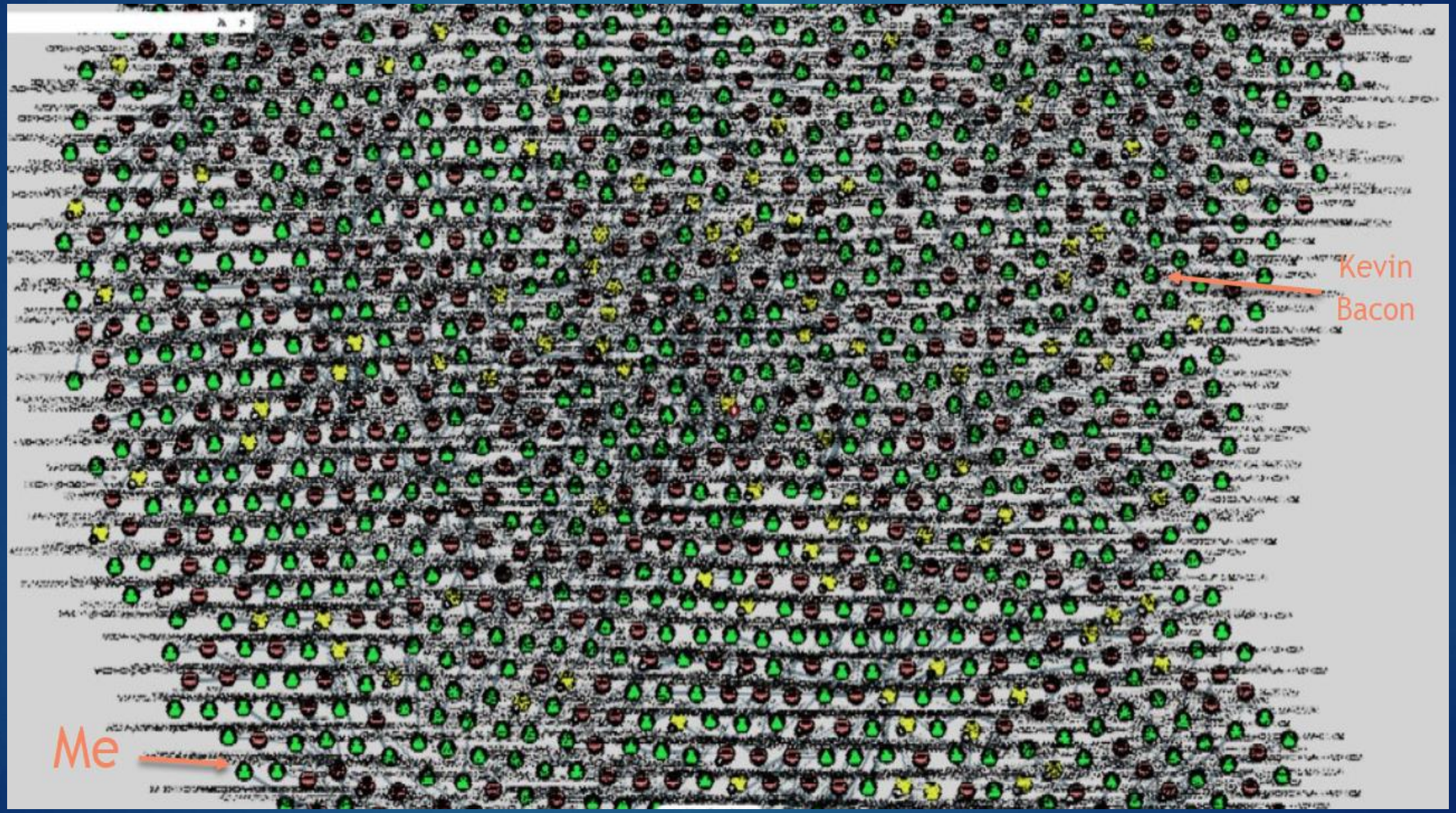
Attacking Active Directory Graphs on Fleek

Fantastic tools for both **Red** and **Blue** teams!

Quickly identify ‘control relations’ between objects in Active Directory

➡ Highly complex attack paths visualized in graphs

Six Degrees of Separation



Attacking Active Directory Setup – Kali Linux

1. Install Bloodhound

```
root@EVILRICK:~# apt update && apt install bloodhound
```

2. Start the neo4j server

```
root@EVILRICK:~# neo4j console
```

3. Authenticate to the provided sample graph database at bolt://localhost:7687. The default username is "neo4j", and the password is " neo4j ".
4. In a different console window, start bloodhound.

```
root@EVILRICK:~# bloodhound
```

https://github.com/BloodHoundAD/BloodHound/wiki/Getting-started