Hunting Lateral Movement with Windows Events Logs

SANS Threat Hunting Summit 2018
Mauricio Velazco
@mvelazco

$WHOAMI

- ✘ Peruvian
- ✘ Recovering pentester, threat management lead
- ✘ @mvelazco
- ✘ Derbycon, Bsides, Defcon

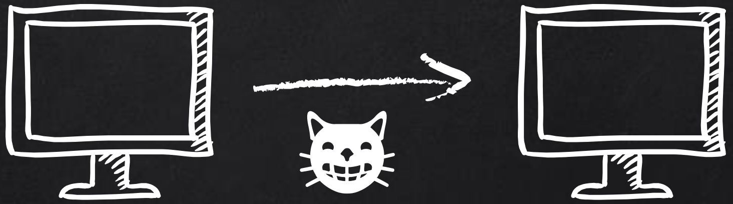
1.

Intro

Lateral Movement

- Techniques that enable an adversary to access and control remote systems on a network.

  https://attack.mitre.org/wiki/Lateral_Movement



Attackers are forced to move in the environment

How?

- ✘ Vulnerability Exploitation
- ✘ Logon Scripts
- ✘ Abusing application deployment software
- ✘ Removable media
- ✘ …….
- ✘ Abusing Windows services/features

> “ *Out of all the incident response engagements that we conducted; 100% of them involved the threat actor compromising valid credentials during the attack.* ”
> https://www.fireeye.com/blog/threat-research/2015/08/malware_lateral_move.html

Windows Services used for LM

- ✘ Server Message Block (SMB)
- ✘ Service Control Manager (SCM)
- ✘ Task Scheduler
- ✘ Windows Management Instrumentation (WMI)
- ✘ Windows Remote Management (WinRM)
- ✘ Distributed Component Object Model (DCOM)
- ✘ Remote Desktop

AppleScript	Application Deployment Software	DCOM
Exploitation	Logon Scripts	Pass the Hash
RDP	Remote File Copy	Remote Services
Removable Media	SSH Hijacking	Shared WebRoot
Tainted Shared Content	Third party Software	ATT&CK™ Adversarial Tactics, Techniques & Common Knowledge
Win RM	Windows Admin Shares (WMI, SCM, Task Sch)	
https://attack.mitre.org/wiki/Lateral_Movement		

2.

The Events

Authentication Events

✘ Account Logon -> Credential validation

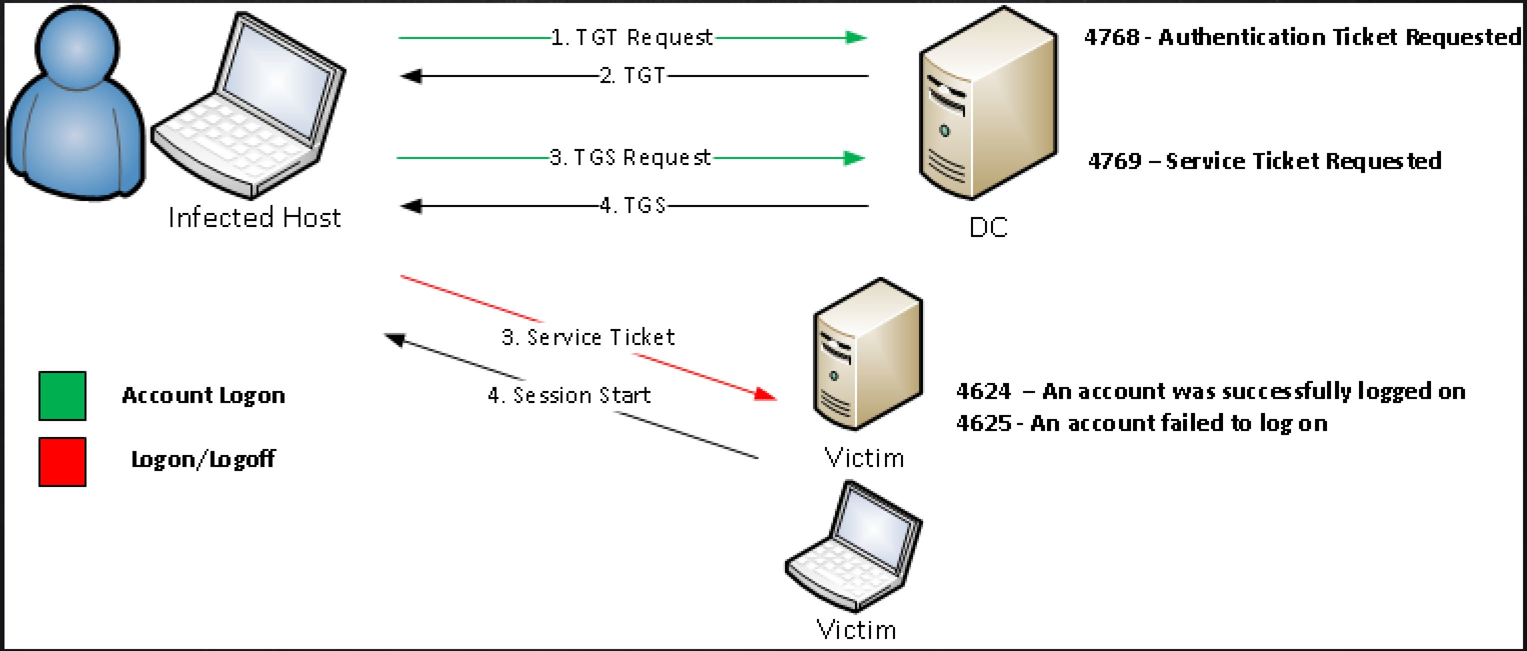
Occurs on the host that is authorative for the credentials

✘ Logon/Logoff -> Creation & Destruction of Sessions

Ocurrs on the host being accessed

https://blogs.msdn.microsoft.com/ericfitz/2005/08/04/deciphering-account-logon-events/

Kerberos



Infected Host

1. TGT Request

2. TGT

3. TGS Request

4. TGS

DC

4768 - Authentication Ticket Requested

4769 – Service Ticket Requested

3. Service Ticket

4. Session Start

Victim

Victim

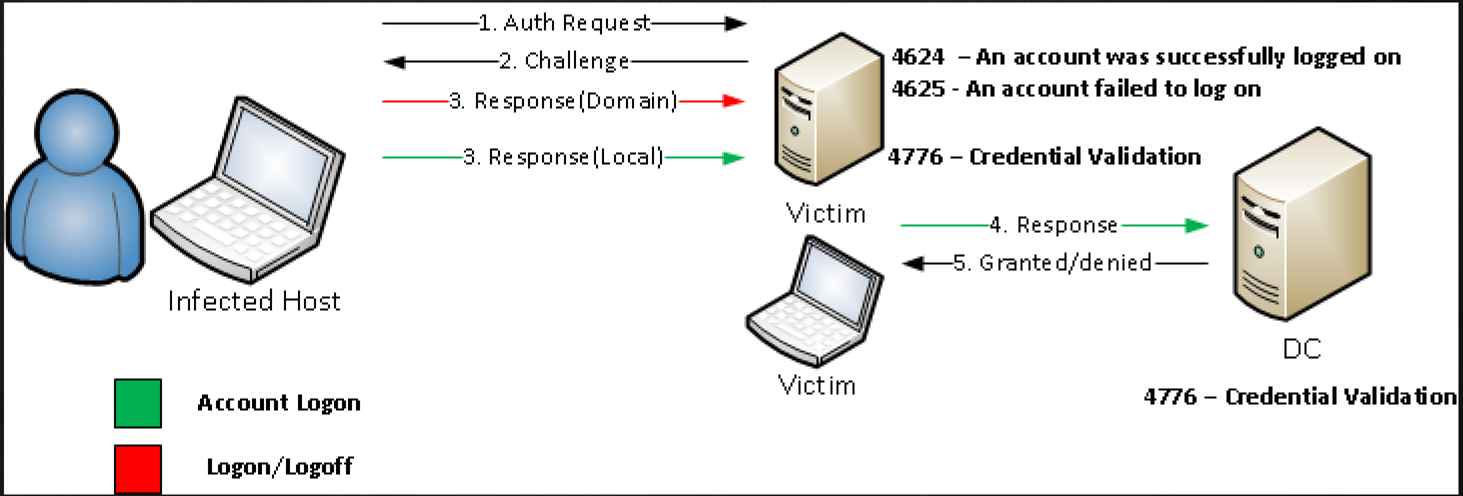
4624 – An account was successfully logged on

4625 - An account failed to log on

🟩 Account Logon

🟥 Logon/Logoff

NTLM



1. Auth Request

2. Challenge

3. Response(Domain)

3. Response(Local)

Infected Host

Victim

4624 – An account was successfully logged on
4625 - An account failed to log on

4776 – Credential Validation

4. Response

5. Granted/denied

Victim

DC

4776 – Credential Validation

🟩 Account Logon

🟥 Logon/Logoff

Account Logon Events

4768: Auth Tkt Requested	4769: Service Tkt Requested	4776: Credential Validation
DC Name	DC Name	Computer Name
Account Name	Account Name	Logon Account
Source Ip	Service Name	Source Workstation
Keywords	Client Address	Error Code
	Keywords	

Hunt Tip #1`

✘ Source Ip requesting TGS for several computers -> Domain Controller Logs

```
Event=4769 And
Service Name=*$
group by (Client Address )
where unique(Service Name) > [Threshold ]
```

✘ This behavior could represent

An adversary moving laterally (or helpdesk deploying software)
Host enumeration (file share, PowerUp Sql, etc)
Bloodhound

Hunt Tip #2`

- ✘ Possible Lateral Movement using NTLM –> Domain Controler Logs

```
Event=4776 And (ComputerName=Dc1 Or ...)
group by (Source Workstation)
Where unique(Computer Name) > [Threshold ]
```

- ✘ This behavior could represent:

  An adversary moving laterally using NTLM based hacking tools like: metasploit, impacket, crackmapexec, smbexec, etc

Logon/Logoff Events

4624	
Computer Name	Account Name
Logon Type	Src Workstation Name
Src Network Address	

4625	
Computer Name	Account Name
Logon Type	Src Workstation Name
Src Network Address	Status
Sub Status	

Hunt Tip #3`

- ✘ Possible Lateral Movement –> Computer Events

```
Event=4624 Or Event=4625 And
(Logon Type=3 Or Logon Type=10)
group by (Src Network Address)
Where unique(Computer Name) > [Threshold ]
```

- ✘ This behavior could represent:

  An adversary moving laterally (or sysadmins working)
  Password Spray / Brute Force Attack
  BloodHound

Services and Tasks

- ✘ System Events
  - 7045: Service Installed
- ✘ Object Access
  - 4698: A scheduled task was created

7045
Service Name
Service File Path
Service Account

4698
Account Name
Task Name
Task Content

TODO: WMI & WinRM

- ✘ WMI-Activity/Trace
  - Event 1: Start of the event sequence
  - Event 2: Actual Event
  - Event 3: End of the event sequence

- ✘ Windows Remote Management
  - Analytical
  - Debug
  - Operational
    - 169: User Authentication

Hunt Tip #4: Edr For The Win

- ✘ Services
  - services.exe
- ✘ WMI
  - wmiprsve.exe
- ✘ Windows Remote Management
  - winrshost.exe
  - wsmprovhost.exe
- ✘ DCOM – MMC20
  - mmc.exe

Hunt Tip #4`

✘ Possible Lateral Movement execution -> Sysmon Events

Event=1 And
(ParentImage=services.exe Or ParentImage… …) And
(Image=cmd.exe Or Image=powershell.exe OR
Image=mshta.exe Or Image=regsvr32.exe … …)

54 application whitelisting bypass techniques

https://github.com/api0cradle/UltimateAppLockerByPassList

3.

Oriana

Oriana 1.0

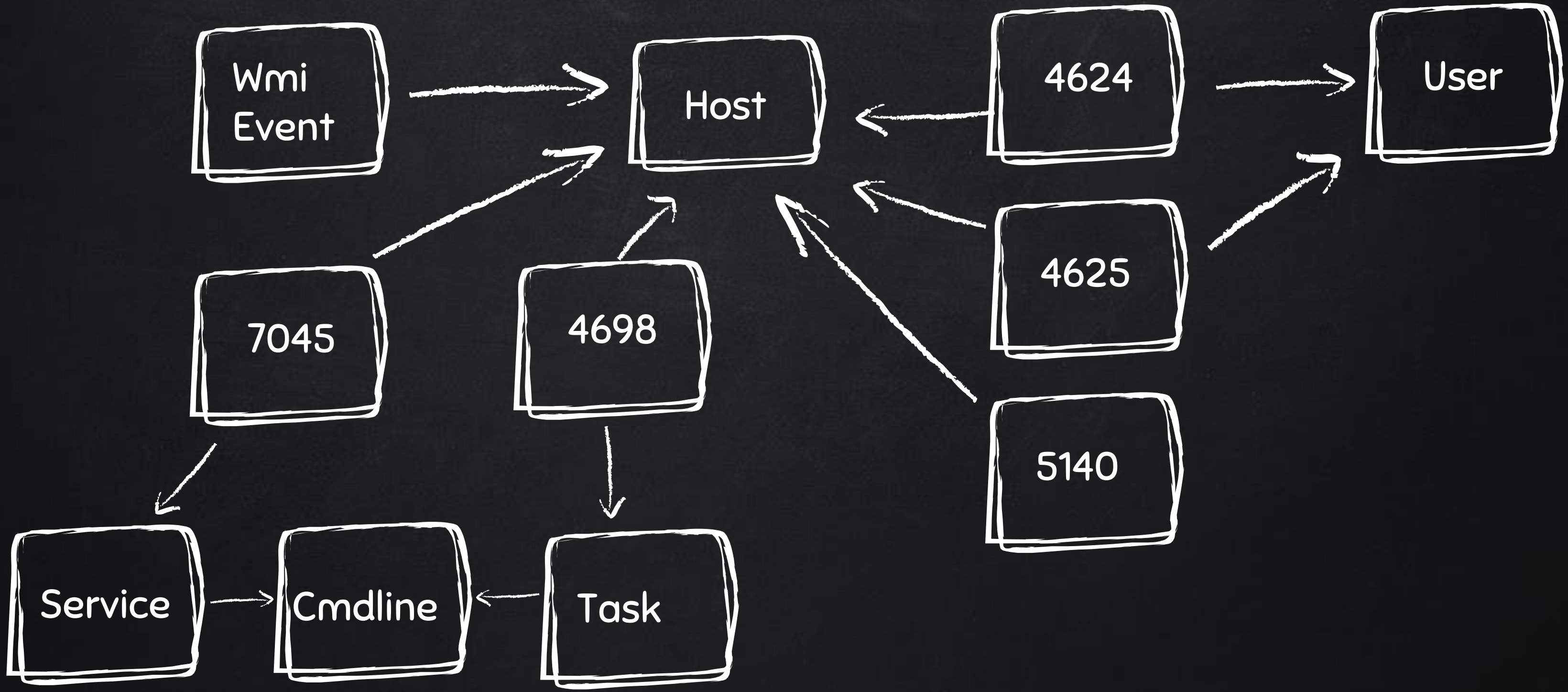
- ✘ Oriana is a threat hunting tool that leverages a subset of Windows events to run analytics and help defenders identify outliers and suspicious behavior in Windows environments.

- ○ Get-WinEvent & Export-CSV

- ○ Django Application, Python 2.7

- ○ Bootstrap & DataTables

Oriana 1.0



Wmi Event

Host

4624

User

7045

4698

4625

5140

Service

Cmdline

Task

HunT 1: Services and Tasks

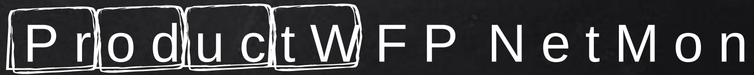
- ✘ 7045 & 4698

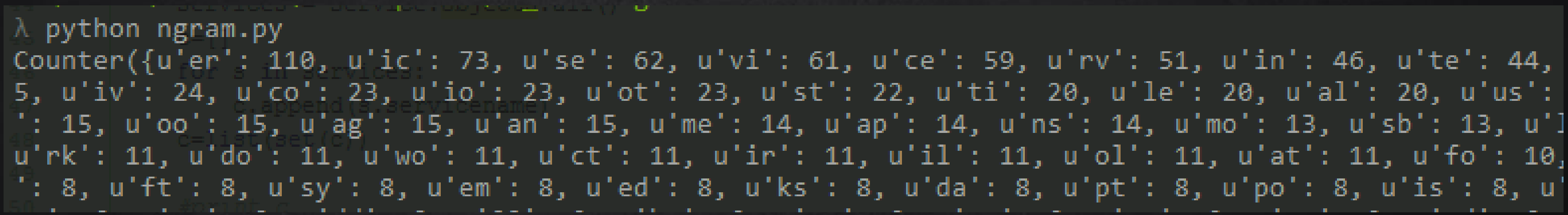
- ✘ Frequency Analysis on
  - Unique Services
  - Unique Tasks

- ✘ Identify "Randomness" of
  - Service Name
  - Task Name

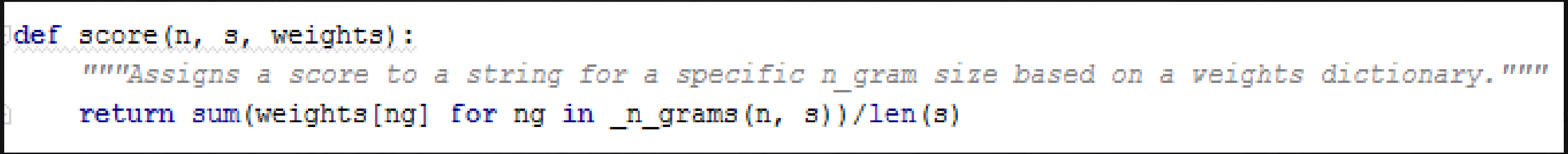
Hunt random: N-gram score

- ✘ Reg expressions are based on a sample and lack context


ProductWFPNetMon



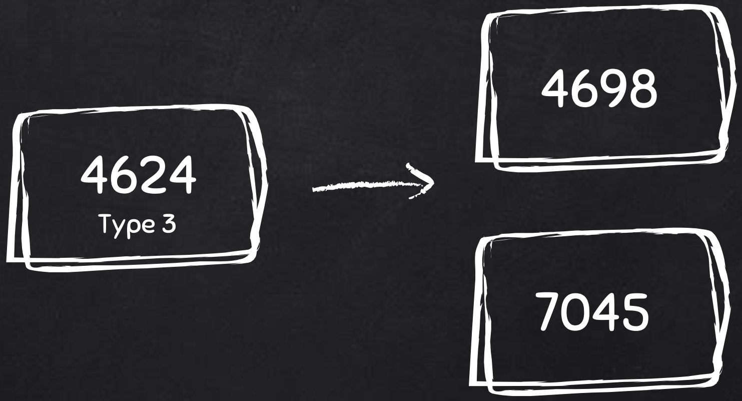
```
λ python ngram.py
Counter({u'er': 110, u'ic': 73, u'se': 62, u'vi': 61, u'ce': 59, u'rv': 51, u'in': 46, u'te': 44,
5, u'iv': 24, u'co': 23, u'io': 23, u'ot': 23, u'st': 22, u'ti': 20, u'le': 20, u'al': 20, u'us':
': 15, u'oo': 15, u'ag': 15, u'an': 15, u'me': 14, u'ap': 14, u'ns': 14, u'mo': 13, u'sb': 13, u'l
u'rk': 11, u'do': 11, u'wo': 11, u'ct': 11, u'ir': 11, u'il': 11, u'ol': 11, u'at': 11, u'fo': 10,
': 8, u'ft': 8, u'sy': 8, u'em': 8, u'ed': 8, u'ks': 8, u'da': 8, u'pt': 8, u'po': 8, u'is': 8, u'
```



```
def score(n, s, weights):
    """Assigns a score to a string for a specific n_gram size based on a weights dictionary."""
    return sum(weights[ng] for ng in _n_grams(n, s))/len(s)
```

DEMO 1

HunT 2: Possible Lateral Movement Event



4624
Type 3

4698

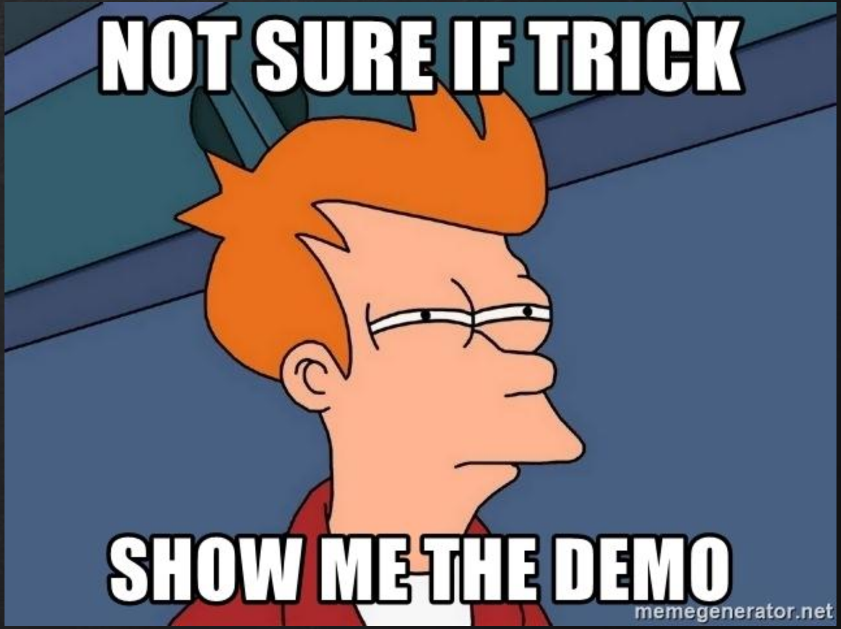
7045

HunT 2: Possible Lateral Movement Session

- ✘ Assumption: Once access has been obtained, an attacker will profile or move laterally to more than one host.

Group possible lateral movement events based on time
(X hour spans)

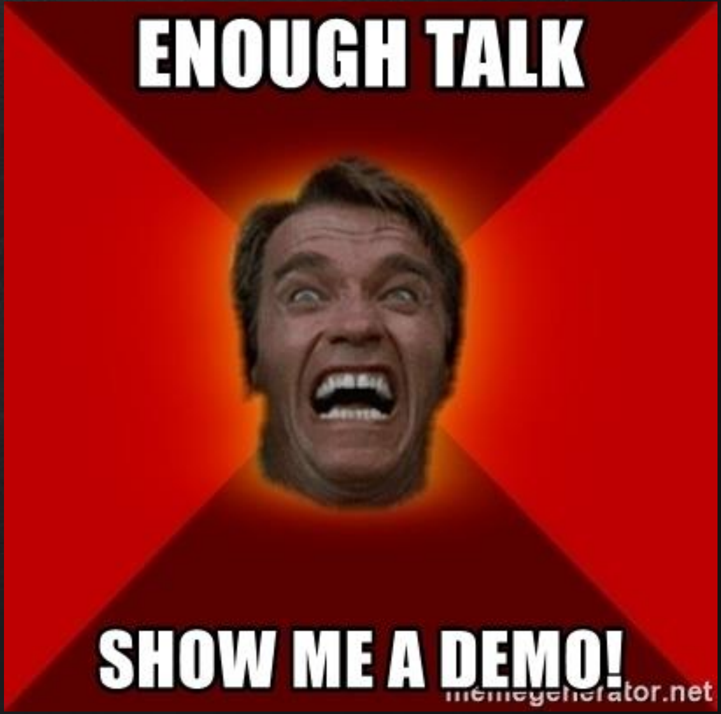
DEMO 2



Hunt 3: Outlier Users/Hosts

- ✘ User
  - # of unique successful authentication events
  - # of unique failed authentication events
  - # of unique hosts a user has authenticated to locally
  - # of unique hosts a user has authenticated to remotely
  - # of unique hosts a user has remotely failed to authenticate
  - # of unique hosts a user has RDP to
- ✘ Host
  - # of unique users that authenticated to a host locally
  - # of unique users that authenticated to a host remotely

DEMO 3



Hunt 4: Suspicious User Behavior

4625: Status & SubStatus

Status	SubStatus	Description
0xC000006D	0xC000006A	Wrong password
0xc000015b	0x0	Acess denied
0xC000006D	0xC0000064	User does not exist
0xc000006e	0xc0000072	Account is disabled

SUB #1 : Privilege Enumeration

- ✘ A user is failing to authenticate to a large number of hosts due to insufficient privileges for the requested logon type

- ✘ This behavior could represent

    An adversary trying to execute remote commands (failing)
    An adversary trying to mount an administrative share
    An adversary enumerating privileges across the network
    An adversary running BloodHound (with no admin privs)

SUB #2 : High number of Destinations

- ✘ A user is successfully authenticating to a large number of hosts

- ✘ This behavior could represent
  - An adversary executing code remotely
  - An adversary enumerating privileges across the network
  - An adversary running BloodHound (with admin privs)

SUB #3 : Roaming User

- ✘ A user account is locally authenticating on several hosts

- ✘ This behavior could represent
  - Compromised credentials usage
  - Credential sharing

SUB #4 : Local Account Spray

- ✘ A local user account is trying to authenticating to a large number of hosts.

- ✘ This behavior could represent
  - An adversary moving laterally with a local account
  - An adversary trying to brute force a local account

DEMO 4

Hunt 5: Suspicious Computer Behavior

https://github.com/mvelazc0/Oriana

Oriana 1.0

- ✘ https://github.com/mvelazc0/Oriana
  - Standalone
  - Docker !
- ✘ https://medium.com/@mvelazco/
- ✘ mauricio.velazco [at] gmail [dot] com
- ✘ @mvelazco

Hunting Lateral Movement with Windows Events Logs

SANS Threat Hunting Summit 2018
Mauricio Velazco
@mvelazco