



Backdoors & Breaches



Incident Response Card Game

Launching in
September 2019

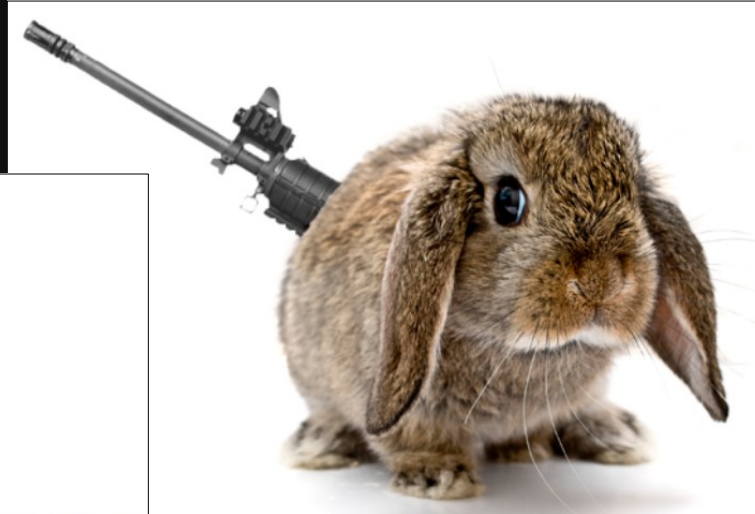
*Request
a Deck!*

Type "Backdoors & Breaches"
into the Questions Window

We'll randomly select a
few requests to get a deck
before the official launch.

Weaponizing Active Directory

Increasing the Chances of Detecting Attackers Early



© Black Hills Information Security
@BHInfoSecurity

David Fletcher

David Fletcher



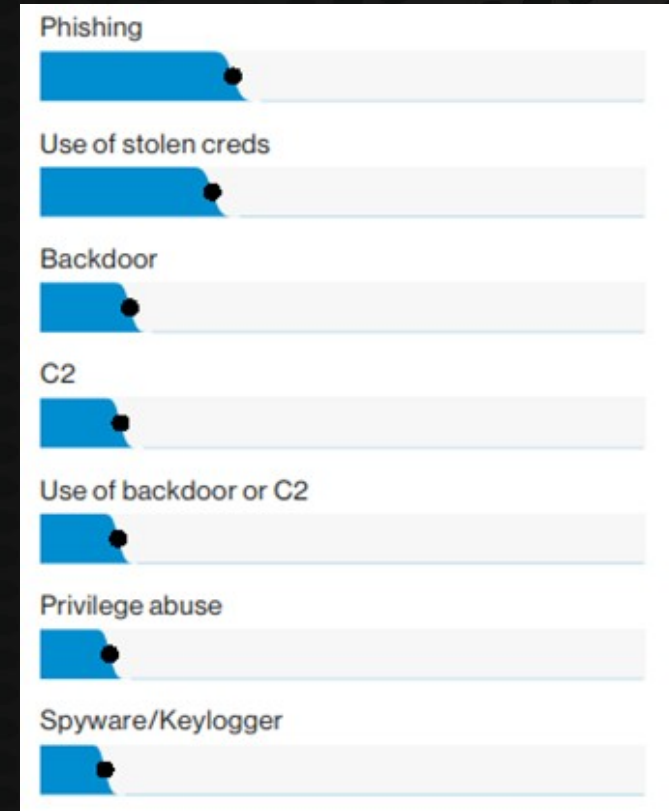
- Security Tester at Black Hills Information Security
- SANS Technology Institute MSISE Graduate
- Many GIAC Certifications including GSE
- Hardware Enthusiast
- WWHF Lab Builder
- Hunter and Fisherman



© Black Hills Information Security
@BHInfoSecurity

Background

- 2019 Verizon DBIR Statistics
 - 32% of breaches included SE attacks
 - Up from 17% in 2013
 - 29% of breaches involved stolen credentials
 - Most are web-based attacks against email portals
 - MFA reduces risk but does NOT eliminate
 - 56% of breaches took months+ to discover
- Our focus is that last bullet!!!



What and Why



- Tactical deception
 - Plant artifacts in the environment
 - Entice attackers to set off tripwire
- Target common attacks
- LOW HANGING FRUIT!!!
 - Perceived low risk of getting caught
 - High reward with success
- Early warning system
- Check our own environments



© Black Hills Information Security
@BHInfoSecurity

WARNING!!!!



- Techniques are used on every test
- Check your own environment
 - Fix where found first
 - Deploy after remediation
- Other Protections Should be In-place
 - LAPS
 - CredentialGuard
 - Defender



© Black Hills Information Security
@BHInfoSecurity

Resources: Users, Groups, & Computers



© Black Hills Information Security
@BHInfoSecurity

Guidance: User Accounts

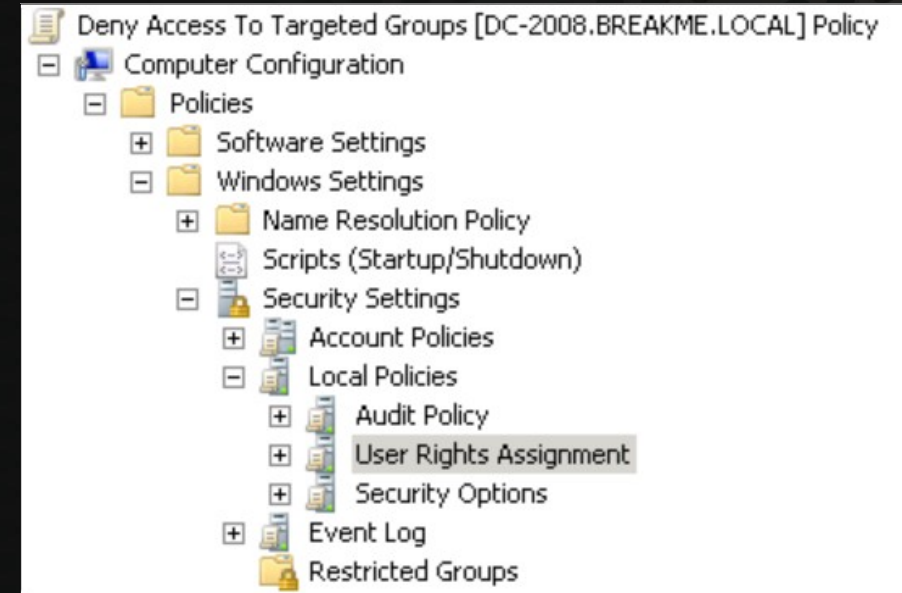


- Planted Credential Account Guideline
 - Account unique to the specific ruse
 - Very strong actual passwords
 - Stored in a password vault
 - Believable planted credentials
 - Employ common password generation techniques
 - Conform with password policy
 - Believable attributes
 - Enabled
 - UserAccountControl
 - Believable group membership



Guidance: Groups

- Use Legitimate Groups
- Seed Dummy Groups
- Dummy Security Group Guidelines
 - Follow organization naming convention
 - Target to user account department
 - No resources to groups



Deny access to this computer from the network	Workstation Admins,
Deny log on as a batch job	Workstation Admins,
Deny log on as a service	Workstation Admins,
Deny log on locally	Workstation Admins,
Deny log on through Remote Desktop Services	Workstation Admins,



Guidance: Computers

- Dummy Computer Account Guidelines
 - Follow organization naming convention
 - Populate attributes as necessary
 - Info
 - Description
 - Comment
 - OperatingSystem
 - Set OperatingSystem to legacy
 - Static DNS entries to honeypot IPs
 - Update pwdLastSet and lastLogonTimestamp



Creativity is King

- Identify critical resources
- Build with those resources in mind
- Make it manageable
 - Departments
 - Organizational Units
- Ecosystem of deception



© Black Hills Information Security
@BHInfoSecurity

Resources: Tools



© Black Hills Information Security
@BHInfoSecurity

Cred Defense Toolkit

- Component we will discuss:
 - ResponderGuard
- Other capabilities:
 - Password auditing
 - Password filter implementation
 - Honey resource generation (in progress)
 - CredDefenseEventParser
 - Event forwarding



© Black Hills Information Security
@BHInfoSecurity

Blog Posts: <https://www.blackhillsinfosec.com/the-creddefense-toolkit/>
<https://www.blackhillsinfosec.com/end-point-log-consolidation-windows-event-forwarder/>

Github: <https://github.com/CredDefense/CredDefense>
Authors: Derek Banks, Beau Bullock, & Brian Fehrman

General Flow

- Identify attack
- Discuss attack
- Discuss deception strategy



© Black Hills Information Security
@BHInfoSecurity

Attack: Reconnaissance



© Black Hills Information Security
@BHInfoSecurity

Attack: Reconnaissance



- Unattended Installation Files
 - C:\Windows\Panther\
- SYSVOL Share
 - Logon Scripts
 - Group Policy Preferences
- Active Directory Schema
 - Attribute Analysis
- File Shares

```
PS C:\WINDOWS\system32> cd C:\Temp
PS C:\Temp> Import-Module .\Get-GPPPassword.ps1
PS C:\Temp> Get-GPPPassword

Changed      : {2012-04-01 08:12:21}
UserNames    : {Administrator (built-in)}
NewName      : {wkstnadm}
Passwords    : {notagoodplaceforavalidpwd!}
File         : \\BREAKME.LOCAL\SYSVOL\breakme.local\Policies\{6056331F-3B4F-4101-97B4-...
              ous\Groups.xml

Changed      : {2011-09-10 12:31:37}
UserNames    : {victim\wkstnadmin}
NewName      : [BLANK]
Passwords    : {notagoodplaceforavalidpwd!}

PS C:\Temp> Import-Module .\PowerUp.ps1
PS C:\Temp> Get-UnattendedInstallFile

UnattendPath
-----
C:\WINDOWS\Panther\Unattend.xml

PS C:\Temp>

PS C:\Temp> Import-Module .\PowerView.ps1
PS C:\Temp> Find-InterestingFile -Path H:\

FullName      : H:\jstrand\SuperSecretEvilPlan
Owner         : BREAKME\jstrand
LastAccessTime : 6/22/2018 5:38:58 PM
LastWriteTime  : 6/22/2018 5:38:58 PM
CreationTime   : 6/22/2018 5:38:58 PM
Length        :

FullName      : H:\jstrand\Passwords.txt
Owner         : BREAKME\jstrand
LastAccessTime : 6/21/2019 6:20:00 PM
LastWriteTime  : 6/21/2019 6:22:33 PM
CreationTime   : 6/21/2019 6:20:00 PM
Length        : 218
```

Commonly Automated Using:

- PowerUp.ps1
- Get-GPPPassword.ps1
- PowerView.ps1



md64"

word>

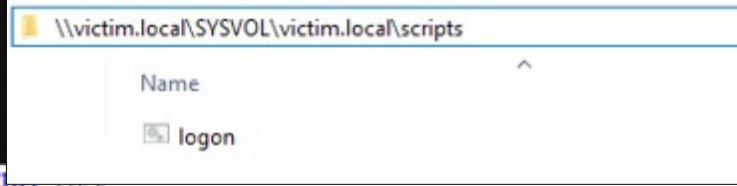
- Context Relevant Alert:
“Credential Usage from UIF”



Deception: Planted Credentials



- SYSVOL Share – Logon Scripts
 - Logon scripts still used by most orgs
 - Net command accepts creds
 - Easy find for attacker
- Context Relevant Alert:
“Credential Usage from Sysvol Script”



```
@ECHO OFF
net use O: /del /yes
net use Z: /del /yes
net use W: /del /yes

net use O: \\fileserver1.victim.local\Departments
net use Z: \\fileserver3.victim.local\Common
net use W: \\cms.victim.local\Developers

net use Z: /del /yes
net use W: /del /yes

net use O: \\fileserver1.victim.local\Departments
net use Z: \\fileserver3.victim.local\Common
net use W: \\cms.victim.local\Developers

net use z: \\192.168.22.11\PII DontTellAnyone /user:victim\serveradmin
```

Net Command with Embedded Credentials



Deception: Planted Credentials



```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4B4C-9934-544FC6D24D26}">
  <User clsid="{DF5F1855-51E5-4D24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2"
  changed="2012-04-01 08:12:21" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
    <Properties action="U" newName="wkstnadm" fullName="" Description=""
    cpassword="Rlf9TTFu60gZuk1j5MLwi8MzCIJphWv15t2MT0aiJP4w30kODHhR6XMD9azeCbW6/jhEi4iFV8APig3FWOM4jw=="
    changeLogon="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator
    (built-in)" expires="never" />
  </User>
</Groups>
<Sched
  changed="2011-09-10 12:31:37" uid="{4501D60E-1D83-45A1-8A51-0D4CF9D8432A}" userContext="0"
  removePolicy="1">
  <Properties action="R" name="Update Local DB" runAs="victim\wkstnadmin"
  cpassword="0tbcUNzn9/szjFFw/wyYlM6uTP1/KpTF6vqShElwWzcDKHhYXdfuWfVUxyBU3zcu16PjKry1myQjF814hhU+aw=="
  logonType="Group">
    <Task version="1.3">
      <RegistrationInfo>
        <Author>victim\Aministrator</Author>
        <Description></Description>
      </RegistrationInfo>
      <Principals>
```



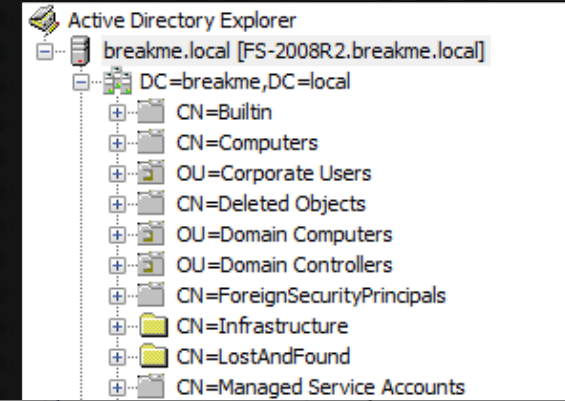
- Group Policy Preferences
 - Key Disclosed*
 - Patched in 2014 (MS14-025)
- Alerting Options:
 - File System Auditing
 - Account Usage
- Context Relevant Alert:
 - “Credential Usage from GPP”



Deception: Planted Credentials



- Active Directory Schema
 - Attributes Readable by Domain Users
 - Credentials Discovered in Attributes
 - Many Tools to Read
 - Powerview.ps1
 - ADExplorer.exe



- Context Relevant Alert:
“Credential Usage from AD Schema”

CN=Administrator,CN=Users,DC=br...	Administrator	9/5/2018 11:06:24 PM	Built-in account for administering the computer/domain
CN=Guest,CN=Users,DC=breakme...	Guest	0x0	Built-in account for guest access to the computer/domain
CN=krbtgt,CN=Users,DC=breakme,...	krbtgt	6/18/2018 9:51:08 PM	Key Distribution Center Service Account
CN=Liller\, Loan,OU=Operations,O...	LLiller	6/21/2018 8:53:00 PM	New User! Password: CantTouchMe18
CN=Radcliffe\, Rachele,OU=Oper...	RRadcliffe	6/21/2018 8:52:56 PM	New User! Password: CantTouchMe18
CN=Silvi\, Sharice,OU=Finance,O...	SSilvi	6/21/2018 8:53:06 PM	New User! Password: CantTouchMe18
CN=Towell\, Tanna,OU=Executive...	TTowell	6/21/2018 8:52:52 PM	New User! Password: CantTouchMe18
CN=Vanderbilt\, Vertie,OU=Informa...	VVanderbilt	6/21/2018 8:52:55 PM	New User! Password: CantTouchMe18
CN=Weekley\, Willodean,OU=Ope...	WWWeekley	6/21/2018 8:52:59 PM	New User! Password: CantTouchMe18

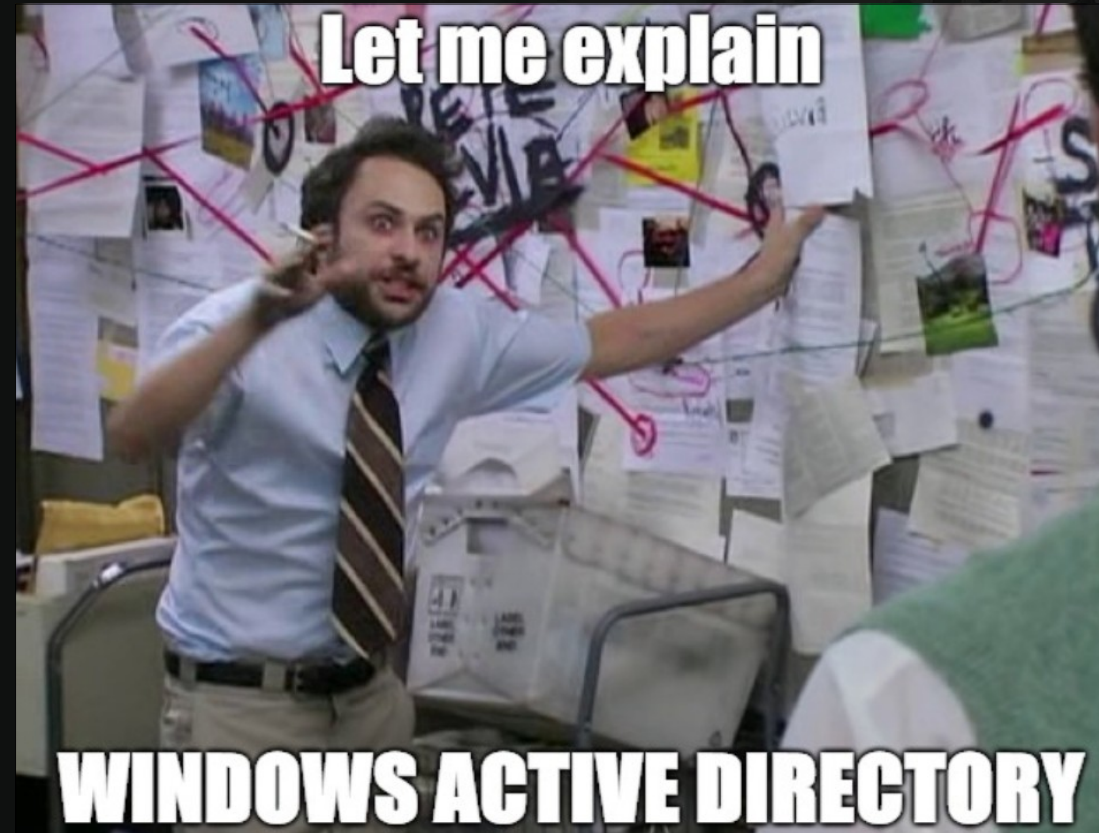
CN=Backup User,OU=Service Acc...	backupuser	6/21/2018 5:40:28 PM	76 51 116 77 51 49 110 33
CN=SQL Service Account,OU=Ser...	sqlsvc	6/21/2018 9:12:32 PM	73 104 56 114 51 112 108 105 99 97 116 49 48 110 33 33



Active Directory Attributes



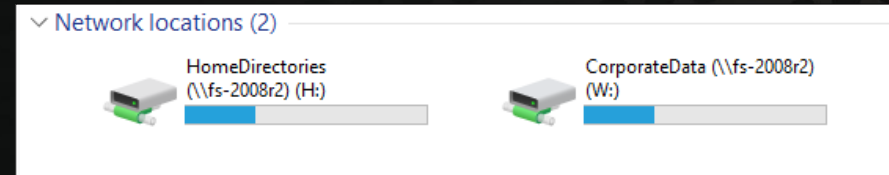
- Active Directory Schema
 - Where to Plant/Check?
 - Comment
 - Description
 - Info
 - Where Else to Check?
 - userPassword
 - unixUserPwd
 - unicodePwd
 - ms-SFU30Password
 - ms-mcs-AdmPwd



Deception: Planted Credentials



- File Shares
 - Start with common mapped drives
 - Plant account credentials in:
 - Root of share
 - Accessible home directory
 - IT-related folders
- Consider domain enumeration:
 - Plant enticing computer accounts
 - Vulnerable Operating Systems
 - Enticing Descriptions



```
PS C:\Temp> Import-Module .\PowerView.ps1
PS C:\Temp> Find-InterestingFile -Path H:\

FullName      : H:\jstrand\SuperSecretEvilPlan
Owner         : BREAKME\jstrand
LastAccessTime : 6/22/2018 5:38:58 PM
LastWriteTime  : 6/22/2018 5:38:58 PM
CreationTime   : 6/22/2018 5:38:58 PM
Length        :

FullName      : H:\jstrand\Passwords.txt
Owner         : BREAKME\jstrand
LastAccessTime : 6/21/2019 6:20:00 PM
LastWriteTime  : 6/21/2019 6:22:33 PM
CreationTime   : 6/21/2019 6:20:00 PM
Length        : 218
```

```
PS C:\Temp> Find-InterestingFile -Path W:\

FullName      : W:\Information Technology\Application Developers\HR App\Web.config
Owner         : BUILTIN\Administrators
LastAccessTime : 6/21/2019 6:16:50 PM
LastWriteTime  : 6/21/2019 1:23:58 PM
CreationTime   : 6/21/2019 6:16:50 PM
Length        : 3893
```



Attack: Password Spraying



© Black Hills Information Security
@BHInfoSecurity

Attack: Password Spray



- Password Spraying:
 - Enumerate password policy
 - Generate list of users
 - One password for population
- Multiple Interfaces:
 - SMB
 - Exchange
 - Lync

```
PS C:\users\sqlsvc\Desktop\tools> net accounts /domain
The request will be processed at a domain controller for domain breakme.local.

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:                                  Never
Lockout duration (minutes):                         30
Lockout observation window (minutes):               30
Computer role:                                       PRIMARY
The command completed successfully.
```

```
PS C:\users\sqlsvc\Desktop\tools> Import-Module .\DomainPasswordSpray.ps1
PS C:\users\sqlsvc\Desktop\tools> Invoke-DomainPasswordSpray -Password Summer2008
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] Removing disabled users from list.
[*] There are 155 total users found.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 9 users gathered from the current user's domain
[*] The domain password policy observation window is set to 30 minutes.
[*] Setting a 30 minute wait in between sprays.

Confirm Password Spray
Are you sure you want to perform a password spray against 9 accounts?
[Y] Yes [N] No [?] Help (default is "Y"): y
[*] Password spraying has begun with 1 passwords
[*] This might take a while depending on the total number of users
[*] Now trying password Summer2008 against 9 users. Current time is 7:27 PM
[*] Writing successes to
[*] SUCCESS! User:jstrand Password:Summer2008
[*] Password spraying is complete
PS C:\users\sqlsvc\Desktop\tools> _
```



Deception: Honey Users



- Fine-grained password policy
- Generate many dummy users
- Set strong passwords
- Monitor for logon attempts

Surname	FirstName	DisplayName	SAMAccountName	Department
Alpha	James	Alpha, James	JAlpha	Information Technology
Bravo	Leslie	Bravo, Leslie	LBravo	Operations
Charlie	Shelly	Charlie, Shelly	SCharlie	Operations
Delta	Bridgette	Delta, Bridgette	BDelta	Finance
Echo	Lenita	Echo, Lenita	LEcho	Information Technology
Foxtrot	Jerrold	Foxtrot, Jerrod	JFoxtrot	Operations
Golf	Ula	Golf, Ula	UGolf	Finance
Hotel	Edra	Hotel, Edra	EHotel	Operations
India	Ossie	India, Ossie	OIndia	Operations
		Juliette, Dino	DJuliette	Operations
		Kilo, Shaunna	SKilo	Finance
		Lima, Remona	RLima	Finance



- Context Relevant Alert:
“Password spray in progress”*
* This will also generate other account related alerts



Attack: Kerberoasting



© Black Hills Information Security
@BHInfoSecurity

Attack: Kerberoast

- Query DC for SPNs
- Request tickets for each account
- Crack passwords
- Low risk of detection
- High reward

sAMAccountName	servicePrincipalName
FS-2008R2\$	ldap/FS-2008R2.breakme.local/Forest
DC-2008\$	RestrictedKrbHost/DC-2008.breakme.
TESTER-WIN10\$	TERMSRV/TESTER-WIN10;TERMS
krbtgt	kadmin/changepw
sqlsvc	SQL/SQL2005DB.breakme.local
RRevel	SQL/TFSDEV.breakme.local



```
PS C:\users\sqlsvc\Desktop\Tools> Import-Module .\Autokerberoast.ps1
PS C:\users\sqlsvc\Desktop\Tools> Invoke-Autokerberoast
Requested Tickets:
ID#1:
SPN: SQL/SQL2005DB.breakme.local
SAMACCOUNTNAME: sqlsvc
DISTINGUISHED NAME: CN=SQL Service Account,OU=Service Accounts,DC=breakme,DC=local

ID#2:
SPN: SQL/TFSDEV.breakme.local
SAMACCOUNTNAME: RRevel
DISTINGUISHED NAME: CN=Revel\, Renato,OU=Information Technology,OU=Corporate Users,DC=breakme,DC=local

Captured TGS hashes:
$krb5tgs$23$*ID#1_SAMACCOUNTNAME: sqlsvc; DISTINGUISHEDNAME: CN=SQL Service Account,OU=Service Accounts
cal SPN: SQL/SQL2005DB.breakme.local *$E719DD3F6C24BBA4CCD060949DC0DFBD$5E43D45668B7AD9074432374B5845C7
0AA91B57F28B7553ED0DCECB5DE331E933C4F2217878616DC45D5FA19A34652F240D3EA3862C603FF57D57A3C000B8601D19087
2702E5807FD12E8F803457AB4BA3BD51A0B058EA4DF183E40E9322879B0950412C698D0B056432BEEAFC327305D3388E8F16545
E475BDFF3EB17EC0F56E7BFF7163BDBC4D952EC29EB9B8F4CACD1C1A703C330D455F644FB85DC55322CB0D693AA2EE26BB19D69
3EE8D224DA6D78BDBBBF43610C04D5A8C2C7C6EC09874135BCDA47B1DED34C75551C091C30F6E74BD68900F0D29F0686AB2EA10
DCB749AB93DCE243936DB875BEEA2AAA96E756F0B3FCE33027481558BE50F3BABB4ABABB28EF4875C2A3D6C5B7F97E28712C1A5
```



Deception: Honey User(s)



- Generate honey user(s)
- Assign SPN to account
- Monitor for Event ID 4769

```
C:\Users\Administrator.000>SetSPN -a SQL/SQL2005DB.breakme.local breakme\sqlsvc
Registering ServicePrincipalNames for CN=SQL Service Account,OU=Service Accounts,DC=breakme,DC=local
SQL/SQL2005DB.breakme.local
Updated object

C:\Users\Administrator.000>SetSPN -a SQL/TFSDEV.breakme.local breakme\rrevel
Registering ServicePrincipalNames for CN=Revel\, Renato,OU=Information Technology,OU=Corporate Users,DC=breakme,DC=local
SQL/TFSDEV.breakme.local
Updated object
```

- Context Relevant Alert:
“Kerberoast attack in progress”



Attack: Multicast DNS Poisoning



© Black Hills Information Security
@BHInfoSecurity

Attack: Multicast DNS Poisoning



- Default Configuration Abuse
 - LLMNR
 - NBNS
 - SMB Signing
- Attacker activates spoofer
 - Credential harvesting
 - SMB relay

```
PS C:\users\sqlsvc\Desktop\Tools> Invoke-Inveigh -NBNS Y -LLMNR Y -ConsoleOutput Y
[*] Inveigh 1.4 started at 2019-06-30T16:51:36
[+] Elevated Privilege Mode = Enabled
WARNING: [!] Windows Firewall = Enabled
[+] Primary IP Address = 172.16.25.100
[+] Spoofer IP Address = 172.16.25.100
[+] ADIDNS Spoofer = Disabled
[+] LLMNR Spoofer = Enabled
[+] LLMNR TTL = 30 Seconds
[+] mDNS Spoofer = Disabled
[+] NBNS Spoofer For Types 00,20 = Enabled
[+] NBNS TTL = 165 Seconds
[+] SMB Capture = Enabled
[+] HTTP Capture = Enabled
[+] HTTPS Capture = Disabled
[+] HTTP/HTTPS Authentication = NTLM
[+] WPAD Authentication = NTLM
[+] WPAD NTLM Authentication Ignore List = Firefox
[+] WPAD Default Response = Enabled
[+] Machine Account Capture = Disabled
[+] Console Output = Full
[+] File Output = Disabled
WARNING: [!] Run Stop-Inveigh to stop
[*] Press any key to stop console output
[+] [2019-06-30T16:52:10] SMB(445) negotiation request detected from 172.16.25.11:57097
[+] [2019-06-30T16:52:11] SMB NTLMv2 challenge/response captured from 172.16.25.11(FS-2008R2):
Administrator::BREAKME:005A7A5BB4732646:9941DBAB263A292A0940CF9BDE6A30D7:010100000000000006EB5B07390
00000000002000E0042005200450041004B004D004500010018005400450053005400450052002D00570049004E00310030
061006B006D0065002E006C006F00630061006C00030034005400650073007400650072002D00570069006E003100300021
```

Commonly Executed Using:

- Inveigh.ps1
- Responder.py



Detection: ResponderGuard



- ResponderGuard:
 - Unicast NBNS requests
 - Listens for responses
 - Application Event ID 8415
 - Optionally send honey creds
- Problem:
 - Inveigh “EvadeRG” Option

```
#### Honey Token Seed Section ####
#### Set $Username and $Password to your own Honeytoken domain/user you want to alert on ####

#Submitting a honey token user credential to the listening Responder if enabled
If ($HoneyTokenSeed)
{
    $Username = "breakme\Administrator"
    $Password = "Summer2019"
    $ResponderShare = "\\$ip\c$"
    Write-Output "[*] Submitting Honey Token Creds $Username : $Password to $ResponderShare!"
    $sharecmd = "net use r: $ResponderShare /User:$Username $Password 2>&1"
    $cmdout = Invoke-Expression -Command $sharecmd -ErrorAction SilentlyContinue
}
```

- Context Relevant Alerts:
 - “Multicast DNS Poisoning Detected”
 - “Multicast DNS Poisoning Credential Use”

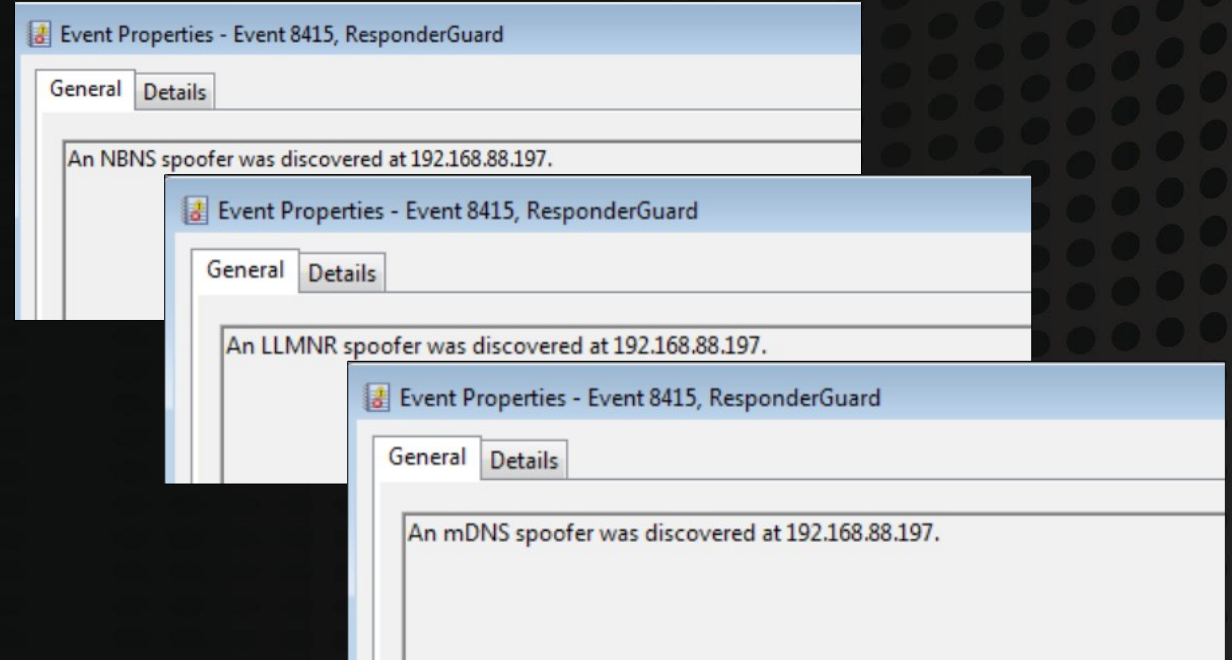
```
PS C:\Users\Administrator.BREAKME\Desktop> Import-Module .\ResponderGuard.ps1
PS C:\Users\Administrator.BREAKME\Desktop> Invoke-ResponderGuard -CidrRange 172.16.25.0/24 -LoggingEnabled
[*] Setting up event logging.
[*] EventLog source ResponderGuard already exists.
[*] Now creating a list of IP addresses from the 172.16.25.0/24 network range.
[*] A list of 255 addresses was created.
[*] ResponderGuard received an NBNS response from the host at 172.16.25.255 for the hostname SPIBKEOWYU!
[*] An event was written to the Windows Event log.
```



Deception: ResponderGuard Agent



- ResponderGuard Agent:
 - Broadcast/Multicast Requests
 - NBNS, LLMNR, and/or mDNS
 - Works like ResponderGuard
 - Deploy via GPO



```
PS C:\Users\David Fletcher\Desktop> Import-Module .\ResponderGuard.ps1
PS C:\Users\David Fletcher\Desktop> Invoke-ResponderGuardAgent -SearchHost FakeMachine -NBNSEnabled -LLMNR
nabled -HoneyTokenSeed -ConsoleOutput
[*] Setting up event logging.
[*] EventLog source ResponderGuard already exists.
[*] Entering processing loop. To gracefully stop processing, press the Q key.
[*] ResponderGuard received an NBNS response from the host at 192.168.88.197 for the hostname FAKEMACHINE!
[*] An event was written to the Windows Event log.
[*] Submitting Honey Token Creds HoneyDomain\HoneyUser : Summer2019! to \\192.168.88.197\c$!
[*] ResponderGuard received an LLMNR response from the host at 192.168.88.197 for the hostname FakeMachine
[*] An event was written to the Windows Event log.
[*] Submitting Honey Token Creds HoneyDomain\HoneyUser : Summer2019! to \\192.168.88.197\c$!
[*] ResponderGuard received an mDNS response from the host at 192.168.88.197 for the hostname FakeMachine!
[*] An event was written to the Windows Event log.
[*] Submitting Honey Token Creds HoneyDomain\HoneyUser : Summer2019! to \\192.168.88.197\c$!
```



Attack: SQL Server Abuse



© Black Hills Information Security
@BHInfoSecurity

Attack: PowerUpSQL



- Enumerates SQL servers
- Searches use:
 - SPN
 - Naming
 - Broadcast
 - Scanning
- Checks for accessibility
- Evaluates for configuration errors

```
PS C:\Users\sqlsvc\Desktop\Tools> $servers = Get-SQLInstanceDomain
VERBOSE: Grabbing SPNs from the domain for SQL Servers (MSSQL*)...
VERBOSE: Parsing SQL Server instances from SPNs...
VERBOSE: 1 instances were found.
PS C:\Users\sqlsvc\Desktop\Tools> $servers

ComputerName      : FS-2008R2.breakme.local
Instance          : FS-2008R2.breakme.local,1433
DomainAccountSid  : 150000052100022110517265223412924717570232402156
DomainAccount     : sqlsvc
DomainAccountCn   : SQL Service Account
Service          : MSSQLSvc
Spn               : MSSQLSvc/FS-2008R2.breakme.local:1433
LastLogon         : 7/4/2019 6:11 PM
Description       :
```



<https://github.com/NetSPI/PowerUpSQL/>



© Black Hills Information Security
@BHInfoSecurity

Detection: Honeyport



- Use existing honey users
- Assign SPNs to accounts
- HoneyPort on selected computers
- Alert on any interaction

```
C:\Users\Administrator.000>SetSPN -a MSSQLSvc/FS-2008R2.breakme.local:1433 breakme\sqlsvc
Registering ServicePrincipalNames for CN=SQL Service Account,OU=Service Accounts,DC=breakme,DC=local
MSSQLSvc/FS-2008R2.breakme.local:1433
Updated object
```

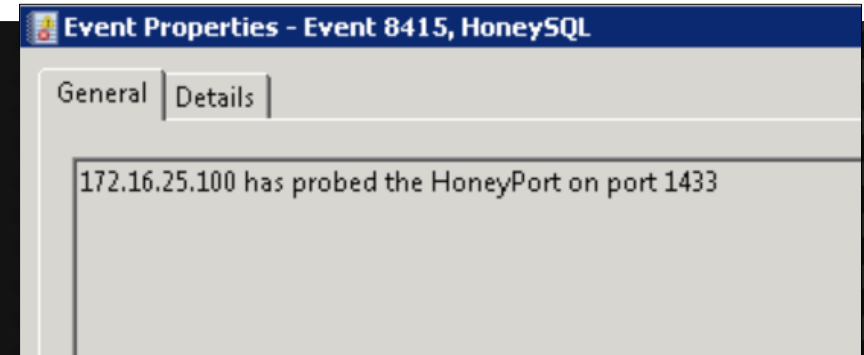
```
PS C:\Users\administrator.BREAKME\Desktop> .\honeyport.ps1 -Ports 1433
[*] EventLog source HoneySQL already exists.
Starting job that will listen for connections on port 1433

WARNING: column "Command" does not fit into the display and was removed.
```

Id	Name	State	HasMoreData	Location
1	HoneyPort	Running	True	localhost

```
PS C:\Users\sqlsvc\Desktop\Tools> $servers | Get-SQLConnectionTestThreaded
VERBOSE: Creating runspace pool and session states
VERBOSE: FS-2008R2.breakme.local,1433 : Connection Failed.
VERBOSE: TESTER-WIN10 : Connection Failed.
VERBOSE: Closing the runspace pool
```

ComputerName	Instance	Status
FS-2008R2.breakme.local	FS-2008R2.breakme.local,1433	Not Accessible
TESTER-WIN10	TESTER-WIN10	Not Accessible



- Context Relevant Alert:
“SQL Enumeration Attack in Progress”

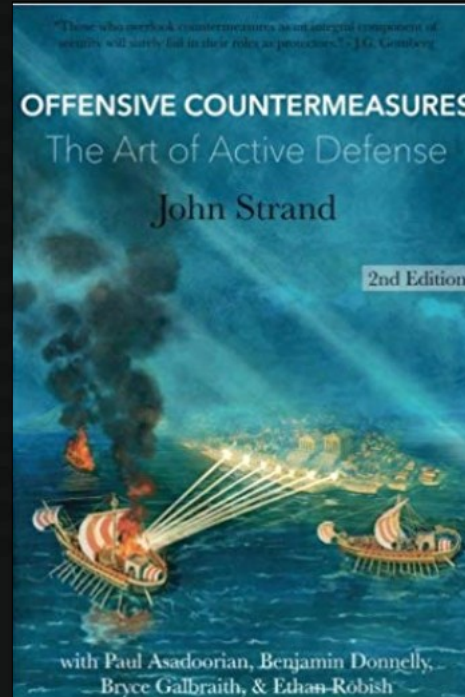


Conclusions



- No cost solutions
- Early warning system
- Extensible to other attacks
- Reduce MTTD

- Run these yourself first!!
 - GetGPPPassword
 - PowerUp
 - PowerView
 - Inveigh/Responder
 - PowerUpSQL
 - Active Directory Explorer



© Black Hills Information Security
@BHInfoSecurity

Questions?

- Resources:

- Our Con: <https://www.wildwesthackinfest.com/>
- Blog: <https://www.blackhillsinfosec.com/blog/>
- Twitter: @BHInfoSecurity



© Black Hills Information Security
@BHInfoSecurity