

NTLM...still...in 2023

Does APT stand for:
Advanced Persistent Threats
Admins Pressed for Time

Matthew Navarro

matthewgenenavarro@protonmail.com

Why do we care?

- ❖ Notable recent events

- ❖ CVE that involves Outlook
- ❖ MS-RPCE abuse
- ❖ MS-EFSRPC abuse
- ❖ NTLM Relay to AD CS HTTP Endpoints – ESC8
- ❖ New to come...

Microsoft fixes Outlook zero-day used by Russian hackers since April 2022

New NTLM Relay Attack Lets Attackers Take Control Over Windows Domain

Active Directory Open to More NTLM Attacks

NTLM relay attacks explained, and why PetitPotam is the most dangerous

History Lesson

- ❖ LM 1987
- ❖ LM Hash 1987 vulnerable to downgrade attacks
- ❖ NTLMv1 1993 NT 3.1 vulnerable to downgrade attacks
- ❖ NT Hash
- ❖ NTLMv2 >= 1996 NT 4.0 SP4

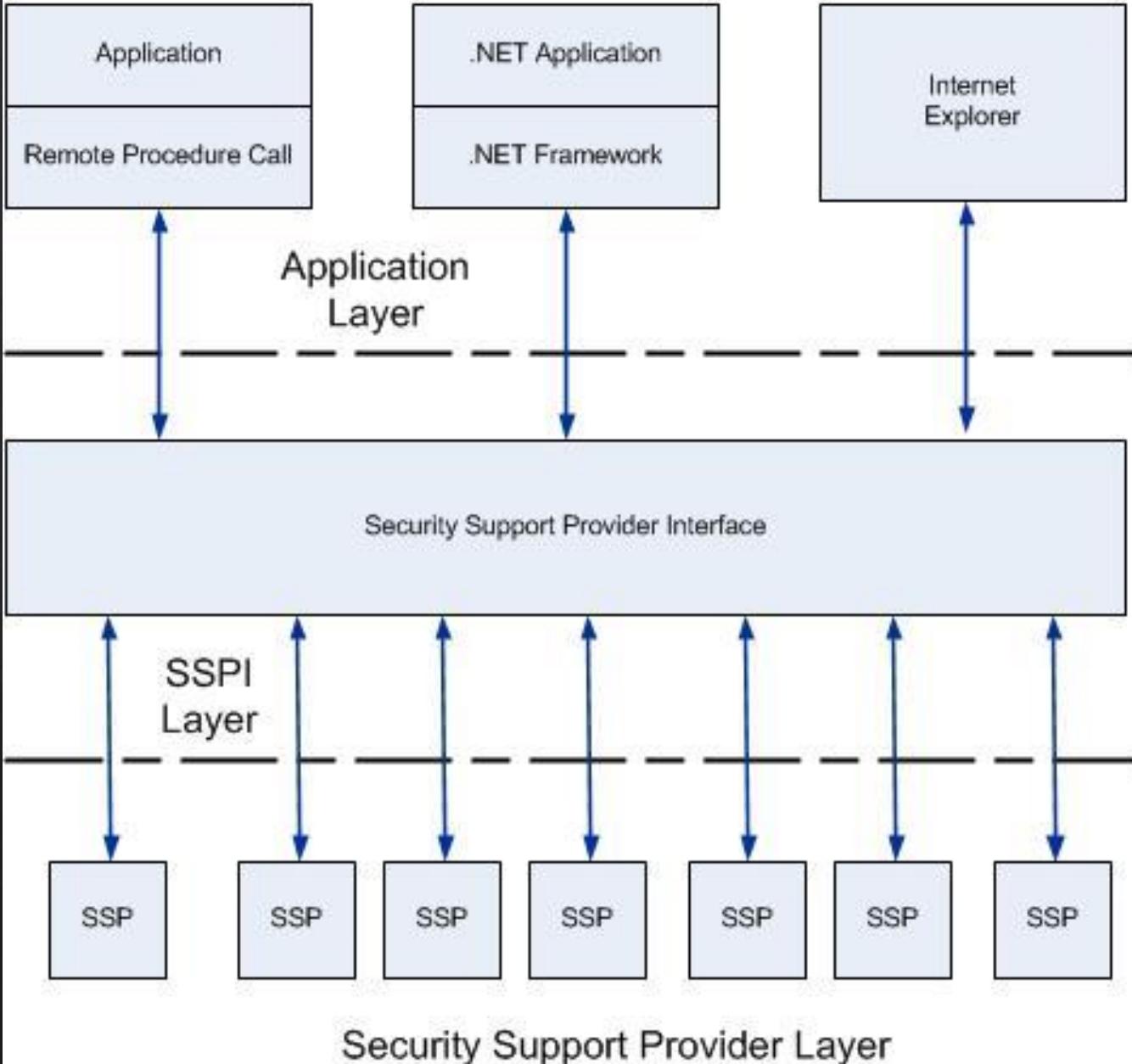
Fancy Words

- ❖ NT Hash/LM Hash – Hash Algorithms
 - ❖ Can be used for Pass-the-Hash
- ❖ NTLM – Authentication Protocol
- ❖ NetNTLM/NTLM hash
 - ❖ Cannot be used for Pass-The-Hash
- ❖ Security Support Provider (SSP) Protocols implement in Modules
- ❖ Security Support Provider Interface (SSPI)

NT Hash vs NetNTLM Hash

- ❖ NT hash Pass-the-Hash
 - ❖ B4B9B02E6F09A9BD760F388B67351E2B
- ❖ Net-NTLM hash Bruteforce/Relay
 - ❖ admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c783031000000000000b45c67103d07d7b95acd12ffa11230e000000052920b85f78d013c31cdb3b92f5d765c783030

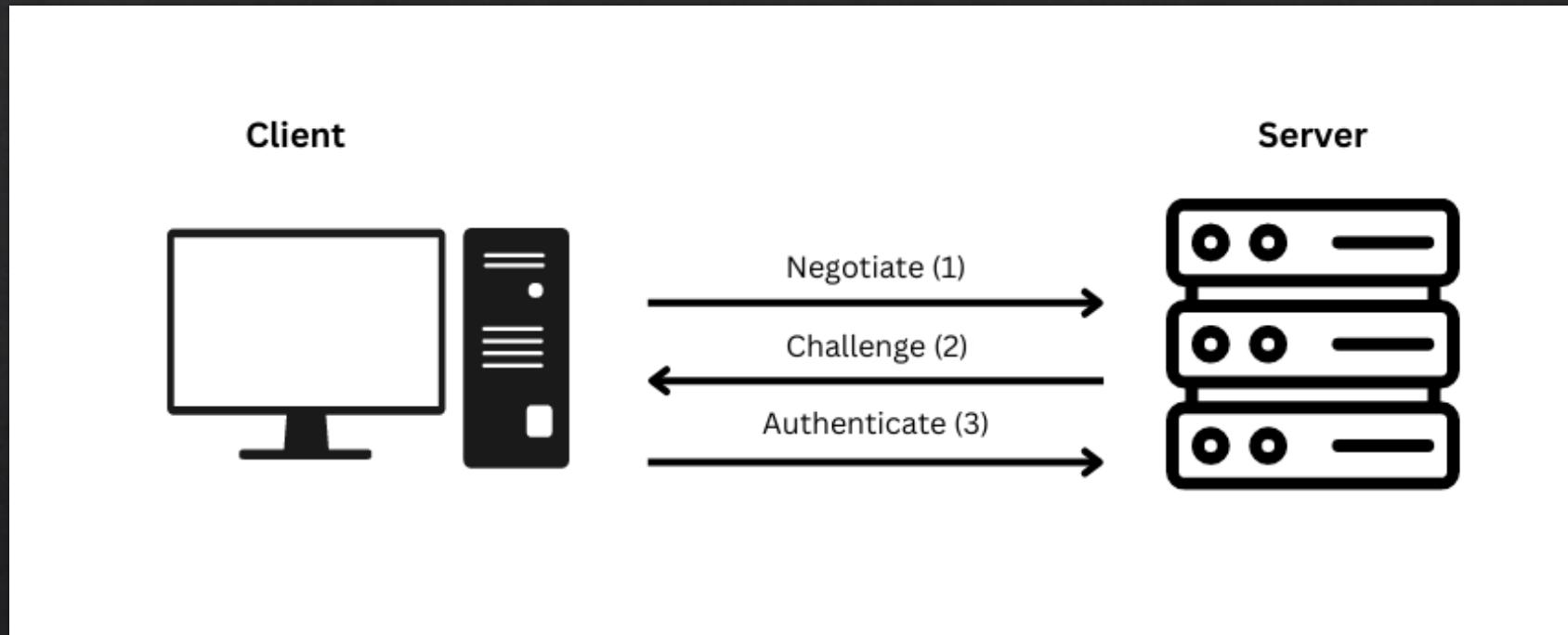
Security Support Provider Interface Architecture



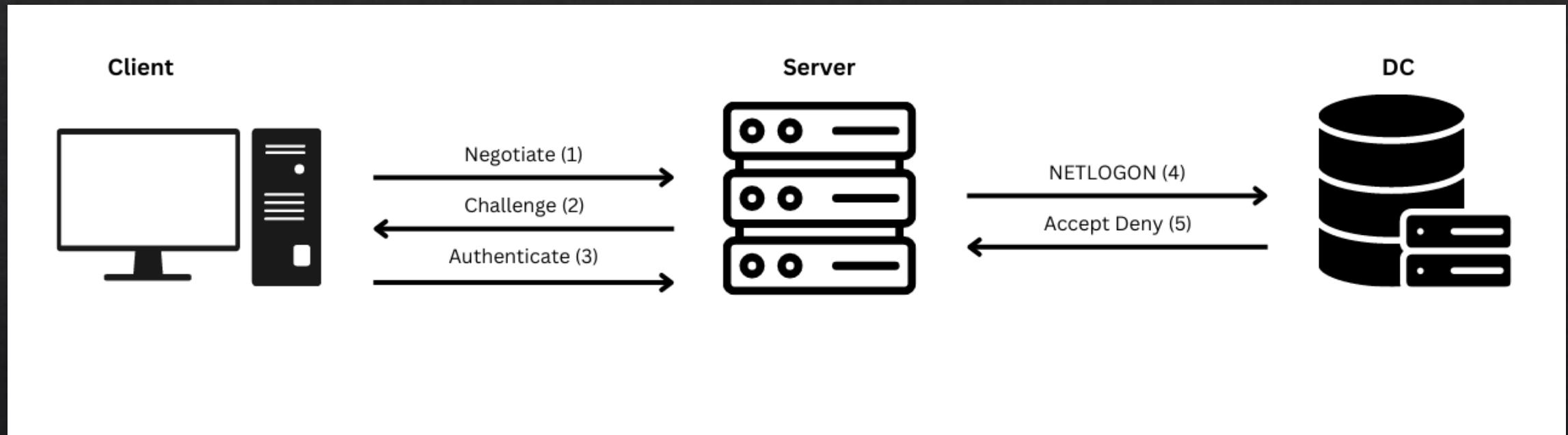
The Moving Pieces

- ❖ (1) NTLM Negotiate
- ❖ (2) NTLM Challenge
- ❖ (3) NTLM Authentication
- ❖ (4) NETLOGON
- ❖ (5) Accept/Deny

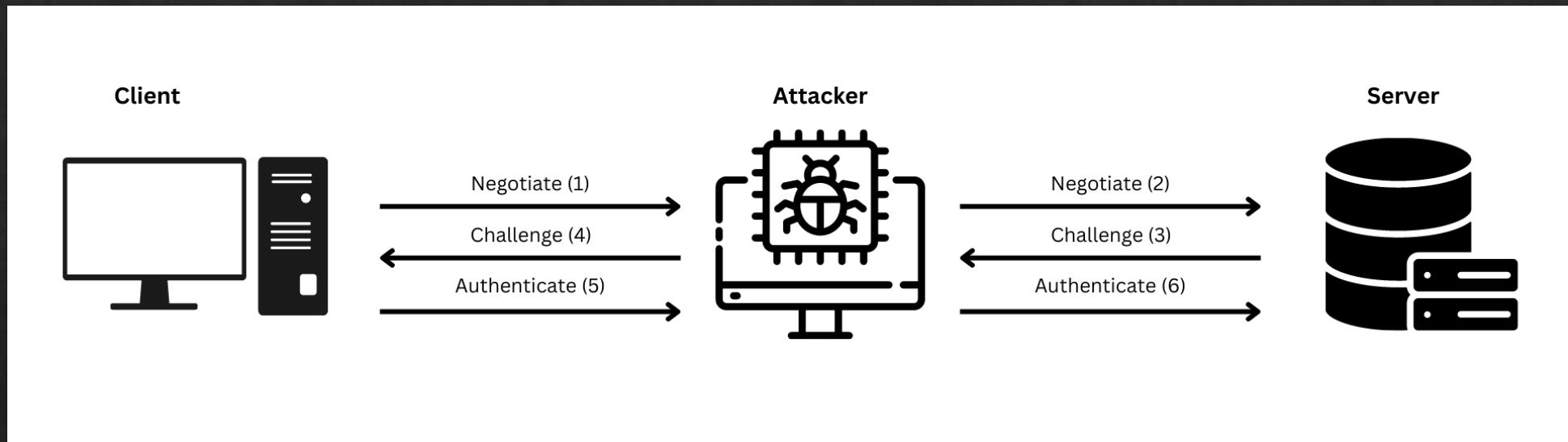
Normal NTLM Traffic w Local Auth



Normal NTLM Traffic w Network Auth



NTLM Relay Traffic

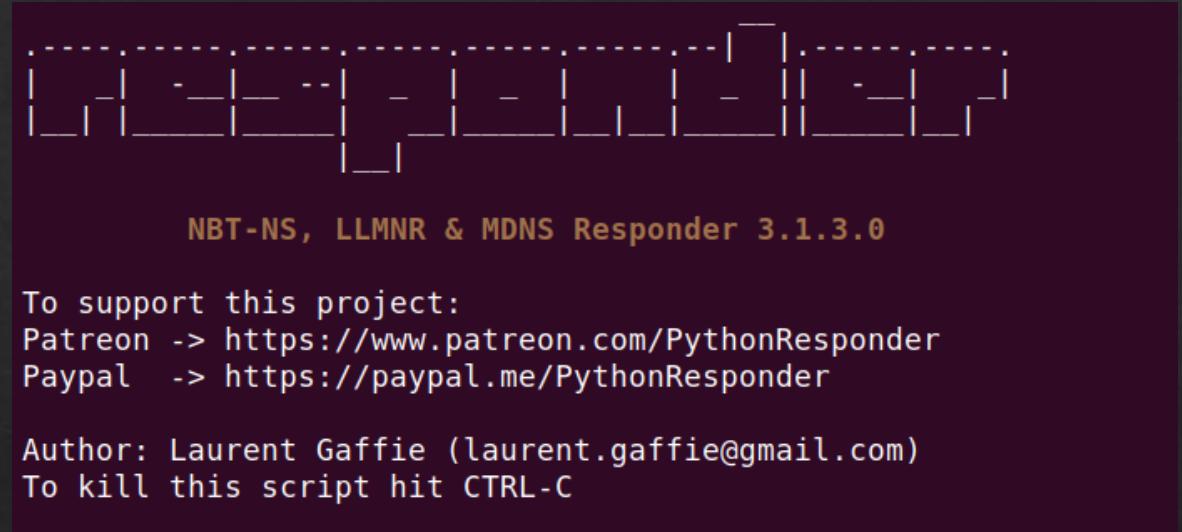


NTLM Relays

- ❖ SMB Relay CVE-1999-0504 1st Relay attack
- ❖ HTTP Relay 2004 but no PoC/2007 HD Moore – Metasploit module
- ❖ LDAP Relay CVE-2017-8563
- ❖ RDP Relay CVE-2018-0886
- ❖ Exchange Relay CVE-2021-28480

Types of NTLM Relay's

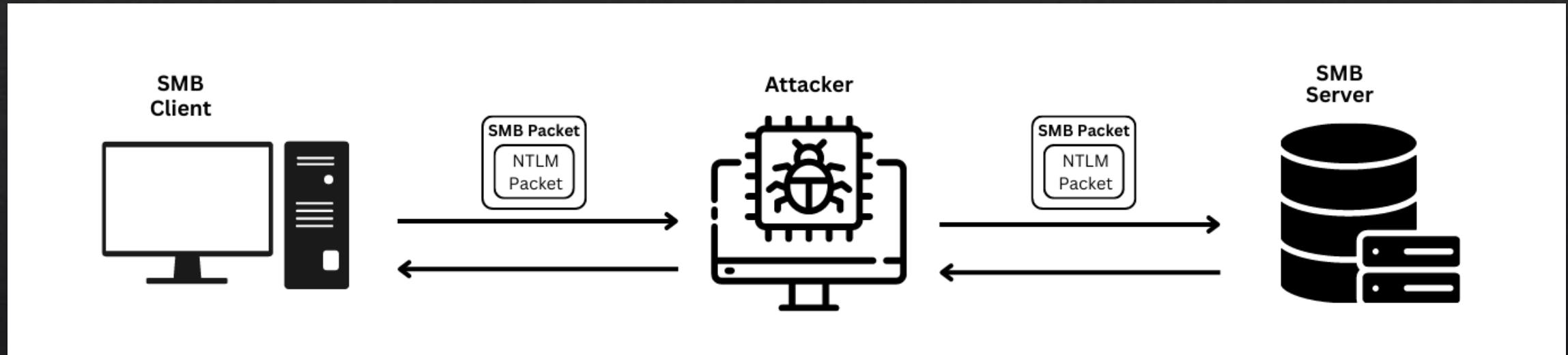
- ❖ Basic Protocol Relay
 - ❖ SMB
 - ❖ HTTP
 - ❖ LDAP
- ❖ Poisoning Attacks
 - ❖ LLMNR
 - ❖ mDNS
 - ❖ mim6
- ❖ Coercion Authentication Attacks
 - ❖ Printerbug MS-RPRN 2017
 - ❖ PetitPotam MS-EFSRPC 2021
 - ❖ ShadowCoerce MS-FSRVP 2021-2022
 - ❖ DFSCoerce MS-DFSNM 2022
 - ❖ CheeseOunce MS-EVEN 2022



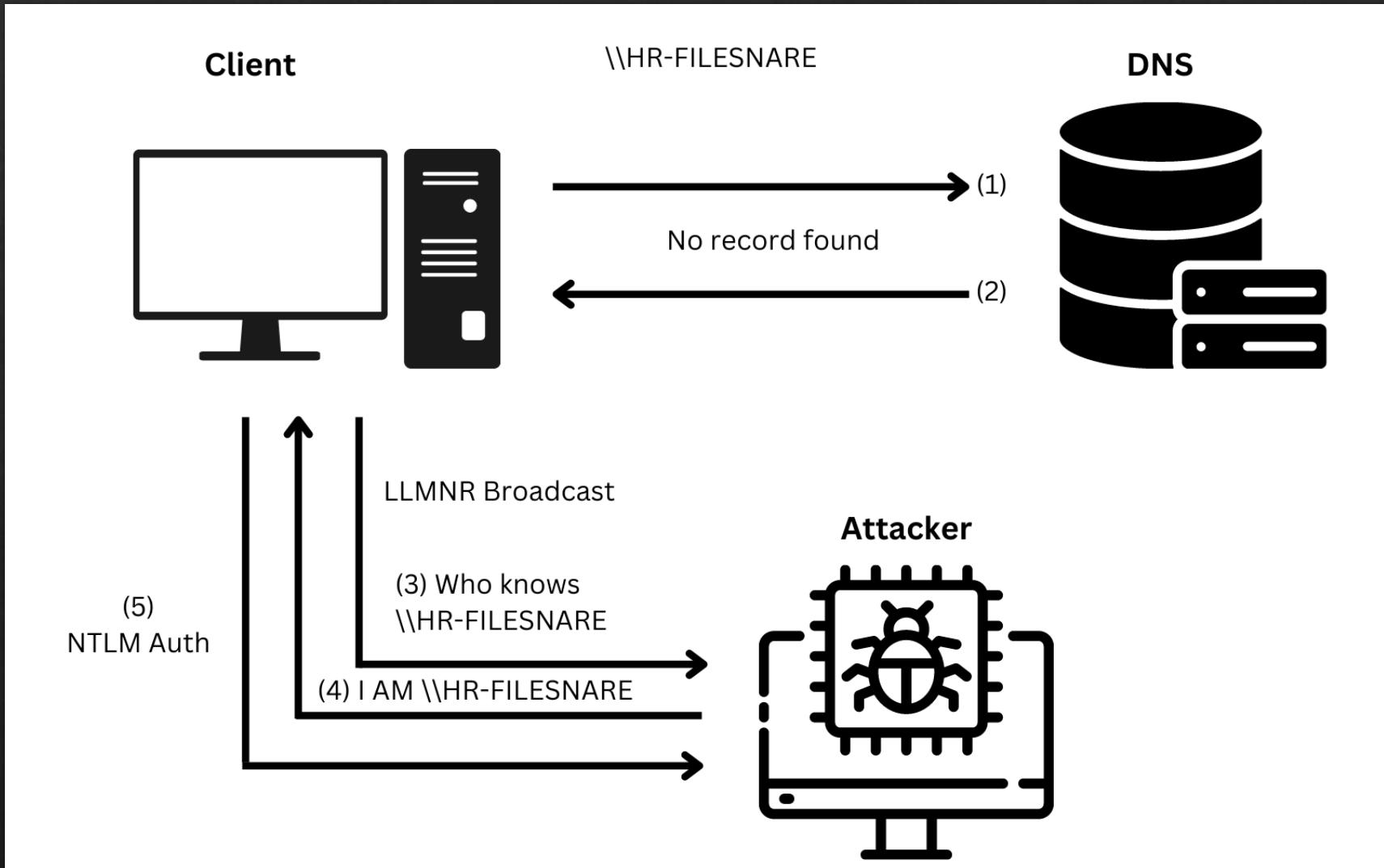
The terminal window shows a PowerShell script with the following text:
PoC to connect to lsarpc and elicit machine account authentication via MS-EFSRPC EfsRpcOpenFileRaw()
by topotam (@topotam77)
Inspired by @tifikin_ & @elad_shamir previous work on MS-RPRN

```
[+] Connecting to ncacn_np:dc-2019-01.lab.local[PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

Protocol Relay Traffic

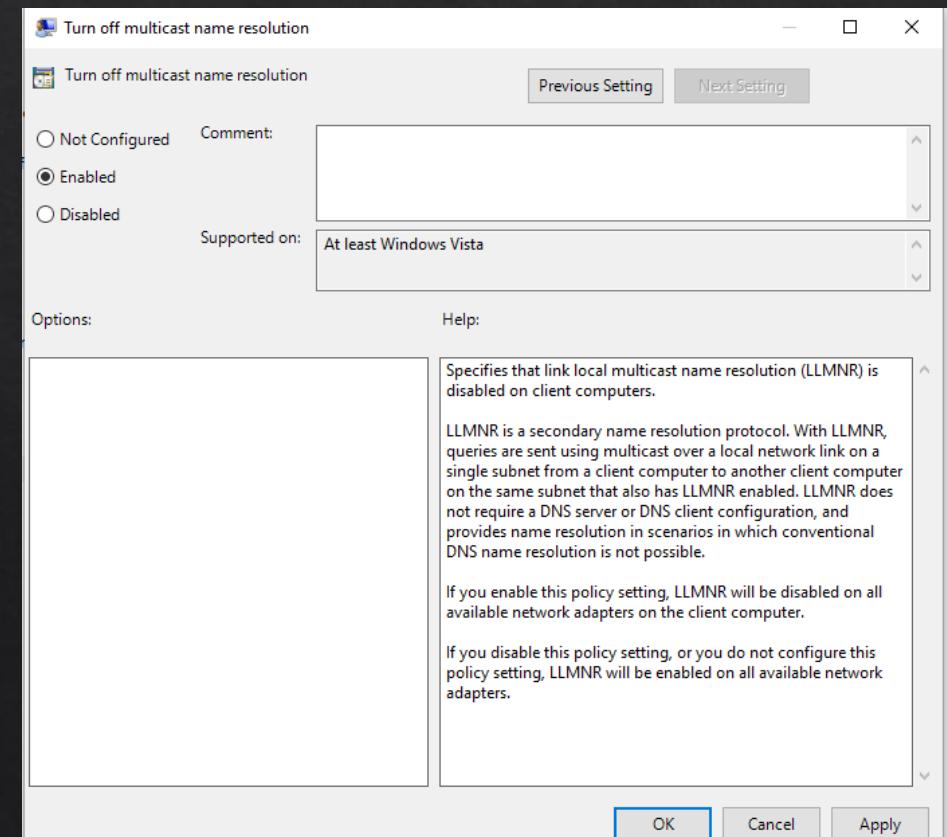


LLMNR Poisoning



Poisoning Mitigations

- ◊ Turn off Link Layer Multicast Name Resolution
- ◊ **Computer Configuration -> Administrative Templates -> Network -> DNS Client**
Enable Turn Off Multicast Name Resolution: Enabled
- ◊ Disable IPv6
- ◊ Identify old logon scripts with responder -A



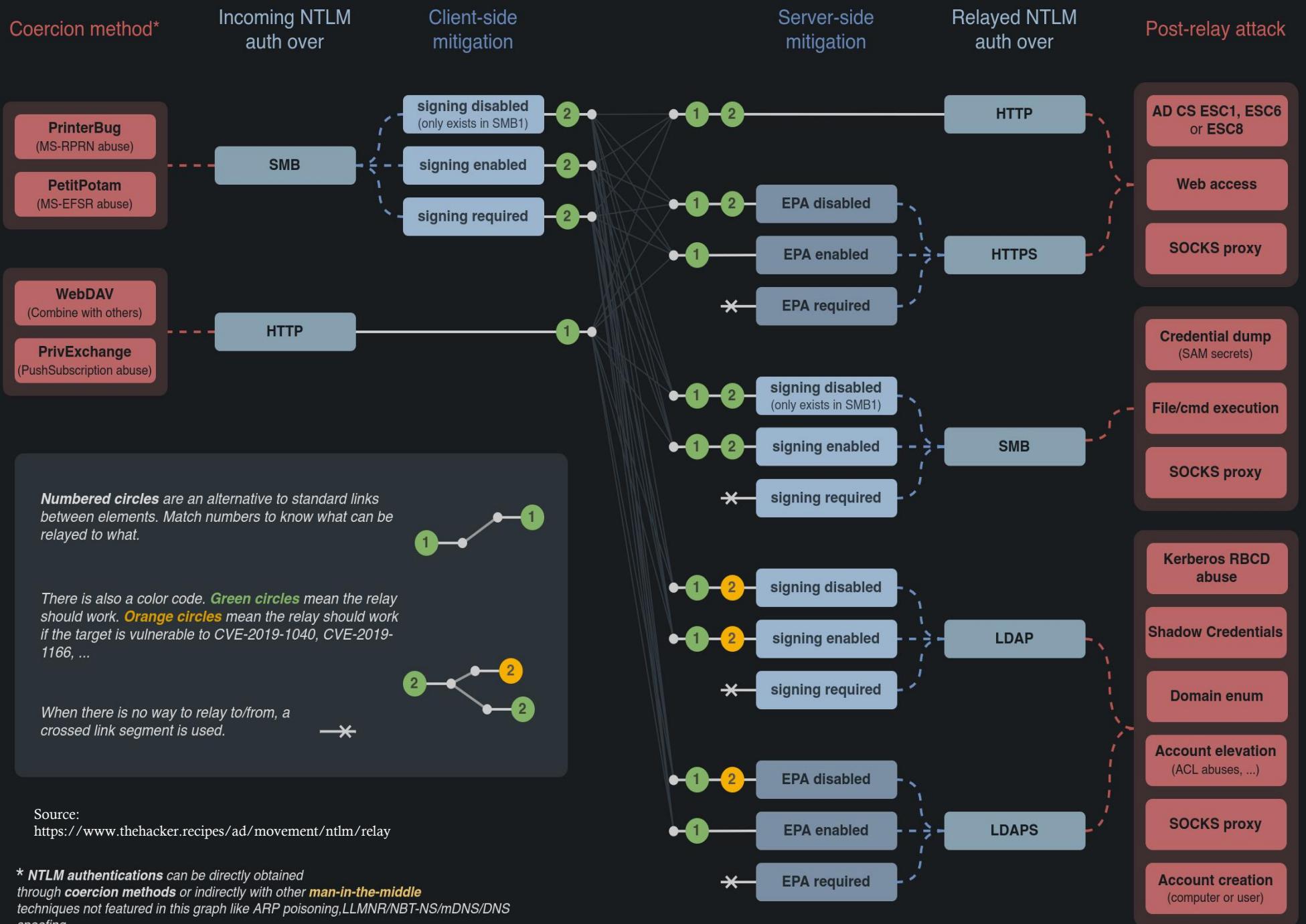
NTLM Coercion

Remote Procedure Calls!!! Modern NTLM abuse

- ❖ Petitpotam testing
 - ❖ Petitpotam.py
 - ❖ August 10, 2021 patch
- ❖ PrinterBug testing
 - ❖ Printerbug.py
- ❖ Mitigations?
 - ❖ Consider disabling printer spooler
 - ❖ Patch!!
 - ❖ Keep on eye on the cybersec community

NTLM Relay Mitigations

- ❖ \$Path = Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options
- ❖ Enable SMB Signing: Microsoft network server/client
 - ❖ Client (always)
 - ❖ Server (always)
- ❖ Enable LDAPS Signing Domain controller: LDAP server signing requirements
- ❖ Enable EAP
- ❖ AUDIT AUDIT AUDIT!!!



Hunting NTLM traffic

- ❖ Domain Controller => Event ID 8004
- ❖ Member Server => Event ID 8003
- ❖ Client => Event ID 8001
- ❖ Enable NTLM auditing
- ❖ All client and servers

Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers = Audit All

8001

Network security: Restrict NTLM: Audit Incoming NTLM Traffic = Enable auditing for all accounts

8003

- ❖ Domain Controllers

Network security: Restrict NTLM: Audit NTLM authentication in this domain = Enable all

8004

Hunting NTLM traffic ID 8001

Event Properties - Event 8001, NTLM

General Details

NTLM client blocked audit: Audit outgoing NTLM authentication traffic that would be blocked.

Target server: cifs/10.0.0.10
Supplied user: (NULL)
Supplied domain: (NULL)
PID of client process: 4
Name of client process:
LUID of client process: 0x2B7C2
User identity of client process: domainadmin
Domain name of user identity of client process: NTMLLAB
Mechanism OID: (NULL)

Audit the NTLM authentication requests from this computer that would be blocked by the target se
cifs/10.0.0.10 if the security policy Network Security: Restrict NTLM: Outgoing NTLM traffic to remot
to Deny all.

Log Name:	Microsoft-Windows-NTLM/Operational		
Source:	NTLM	Logged:	5/15/2023 11:01:31 AM
Event ID:	8001	Task Category:	Auditing NTLM
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	VICTIM.NTMLLAB.local

Event Properties - Event 8001, NTLM

General Details

NTLM client blocked audit: Audit outgoing NTLM authentication traffic that wo
Target server: HTTP/10.0.0.100
Supplied user: domainadmin
Supplied domain: NTMLLAB
PID of client process: 2916
Name of client process: C:\Program Files (x86)\Internet Explorer\iexplore.exe
LUID of client process: 0x81154
User identity of client process: domainadmin
Domain name of user identity of client process: NTMLLAB
Mechanism OID: (NULL)

Audit the NTLM authentication requests from this computer that would be bl
HTTP/10.0.0.100 if the security policy Network Security: Restrict NTLM: Outgoi
set to Deny all.

Hunting NTLM traffic ID 8003

Event Properties - Event 8003, NTLM

General Details

NTLM server blocked in the domain audit: Audit NTLM authentication in this domain

User: domainadmin
Domain: NTMLLAB
Workstation: VICTIM
PID: 4
Process:
Logon type: 3
InProc: true
Mechanism: (NULL)

Audit NTLM authentication requests within this domain that would be blocked if the security policy Network Security: Restrict NTLM: NTLM authentication in this domain is set to Deny for domain servers or Deny domain accounts to domain servers.

If you want to allow NTLM authentication requests in the domain domainadmin, set the security policy Network Security: Restrict NTLM: NTLM authentication in this domain to Disabled.

If you want to allow NTLM authentication requests to specific servers in the domain domainadmin, set the security policy Network Security: Restrict NTLM: NTLM authentication in this domain to Specific servers.

Log Name:	Microsoft-Windows-NTLM/Operational		
Source:	NTLM	Logged:	5/16/2023 7:24:13 PM
Event ID:	8003	Task Category:	Auditing NTLM
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	SRV01.NTMLLAB.local
OnCode:	Info		

Hunting NTLM traffic ID 8004

Event Properties - Event 8004, Security-Netlogon

General Details

Domain Controller Blocked Audit: Audit NTLM authentication to this domain controller.
Secure Channel name: SRV01
User name: domainadmin
Domain name: NTMLLAB
Workstation name: VICTIM
Secure Channel type: 2

Audit NTLM authentication requests within the domain NTMLLAB that would be blocked if the security policy Network Security: Restrict NTLM: NTLM authentication in this domain is set to any of the Deny options.

If you want to allow NTLM authentication requests in the domain NTMLLAB, set the security policy Network Security: Restrict NTLM: NTLM authentication in this domain to Disabled.

If you want to allow NTLM authentication requests to specific servers in the domain NTMLLAB, set the security policy Network Security: Restrict NTLM: NTLM authentication in this domain to Deny for domain servers or Deny domain accounts to domain servers, and then set the security policy Network Security: Restrict NTLM: Add server exceptions in this domain to define a list of servers in the domain NTMLLAB to which clients are allowed to use

Log Name:	Microsoft-Windows-NTLM/Operational		
Source:	Security-Netlogon	Logged:	5/15/2023 8:01:31 PM
Event ID:	8004	Task Category:	Auditing NTLM
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	NTLM-DC.NTMLLAB.local

Questions?

jean@attacker: ~/Desktop

```
jean@attacker:~/Desktop$ rm targets.txt
jean@attacker:~/Desktop$ cme smb 10.0.0.0/24 --gen-relay-list /home/jean/Desktop/targets.txt
```



