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

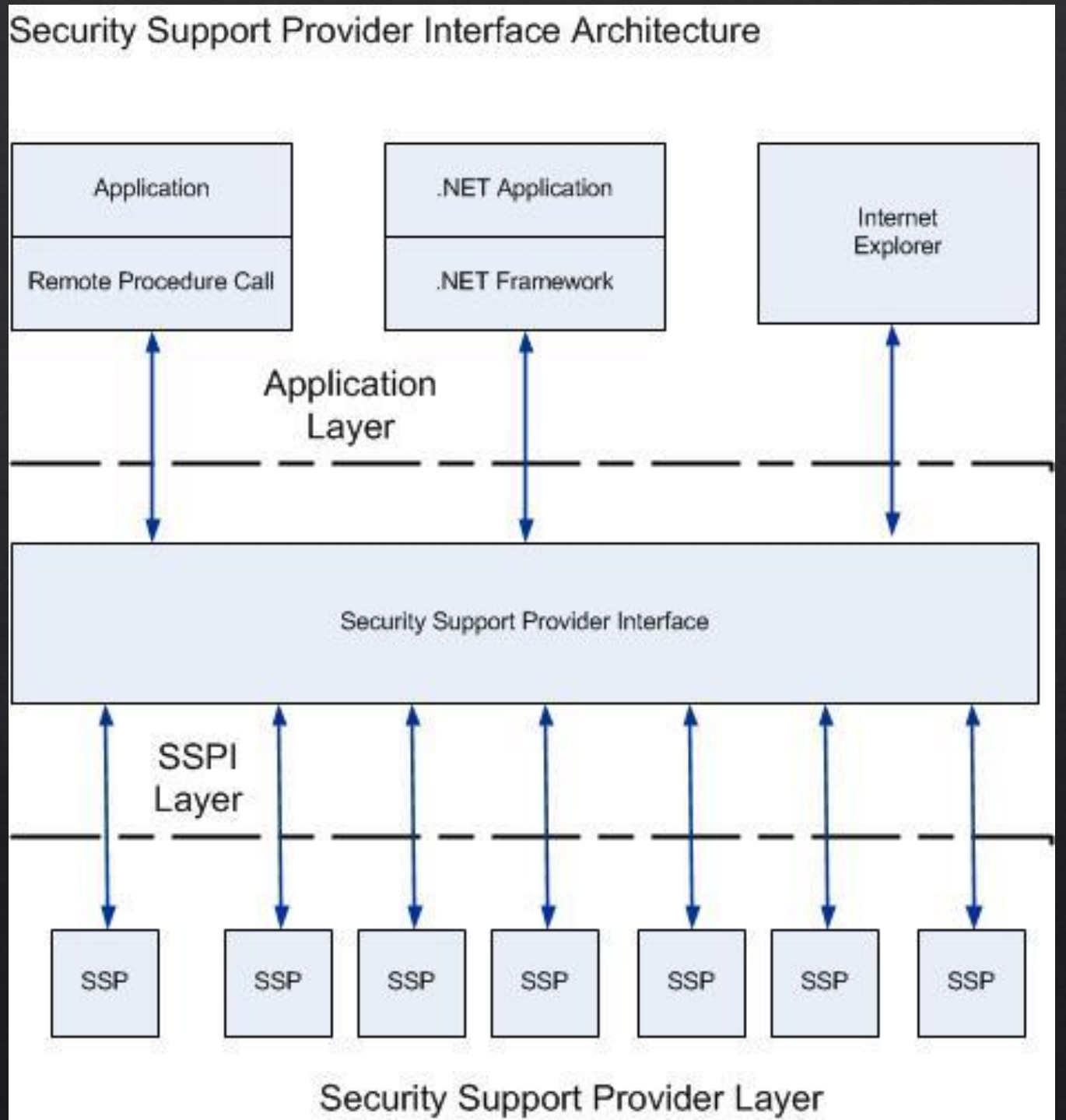
- LM 1987
- LM Hash 1987 vulnerable to downgrade attacks
- NTLMv1 1993 NT 3.1vulnerable to downgrade attacks
- NT Hash
- NTLMv2 >= 1996 NT 4.0 SP4

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:88dcbe4446168966a153a0064958dac6:5c7830315c78303100000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030

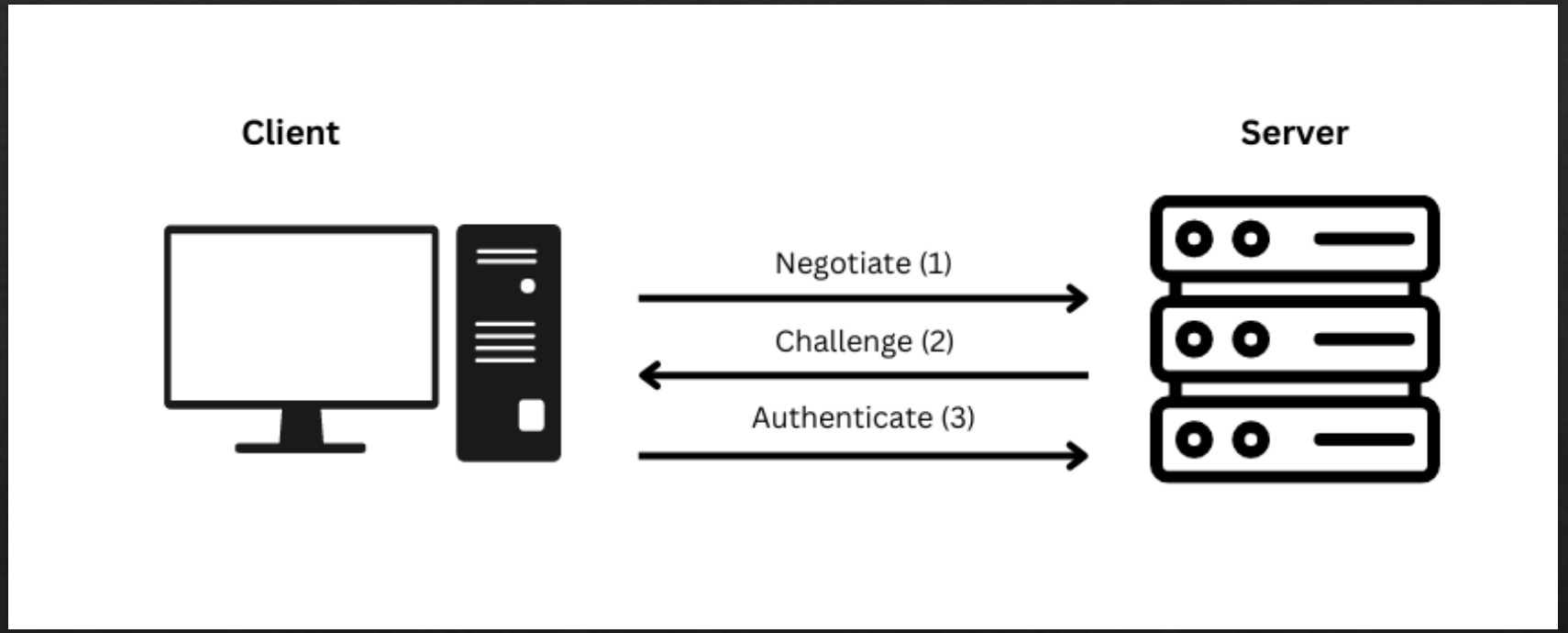


Source:
https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/security-support-provider-interface-architecture

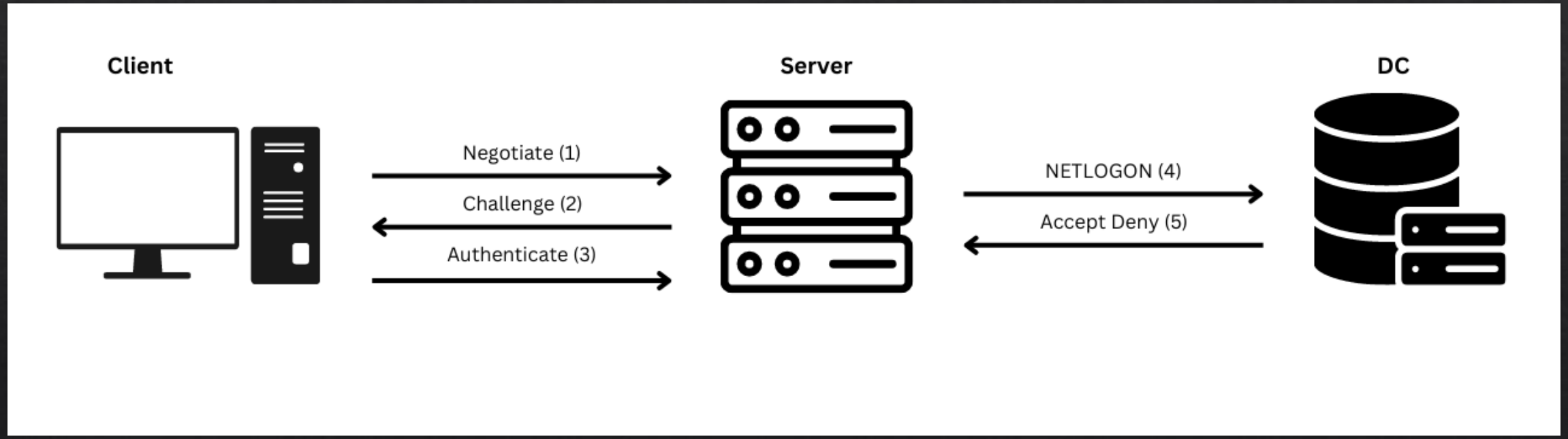
The Moving Pieces

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

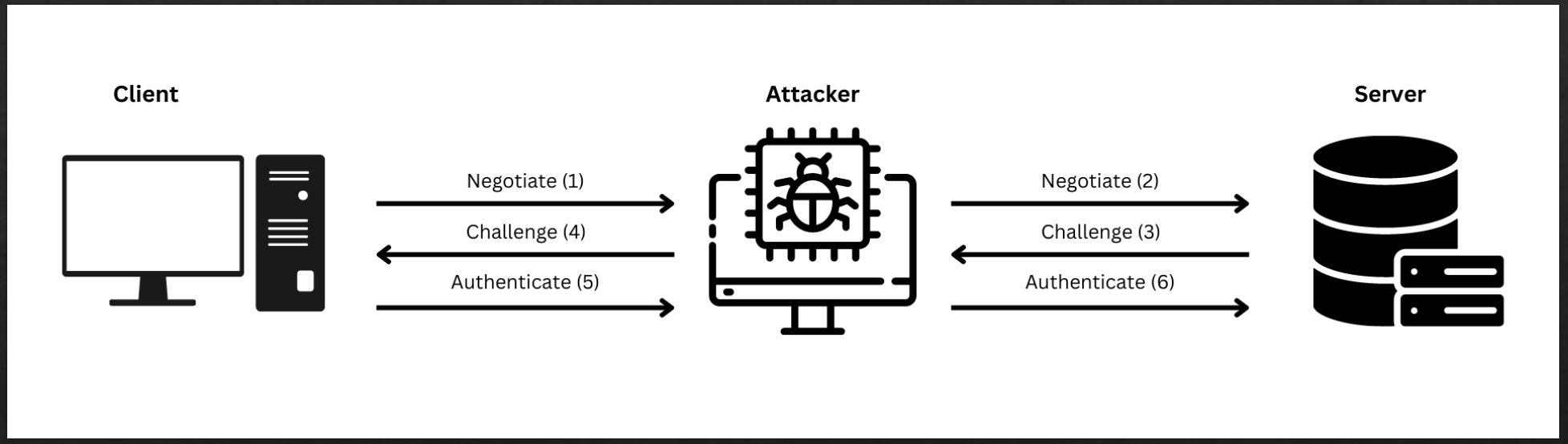
Normal NTLM Traffic w Local Auth



Normal NTLM Traffic w Network Auth



NTLM Relay Traffic

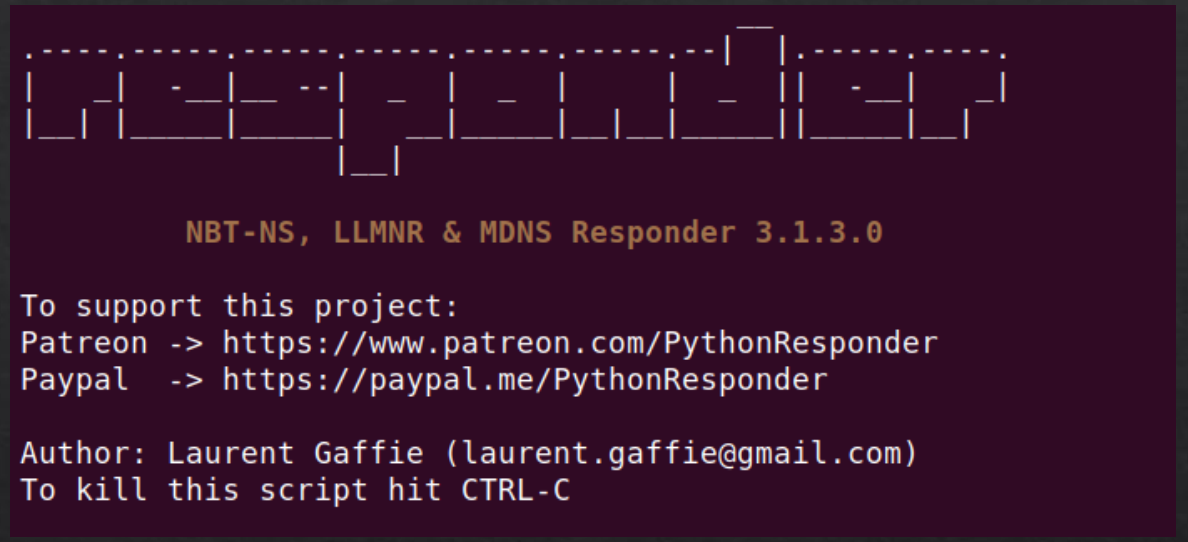


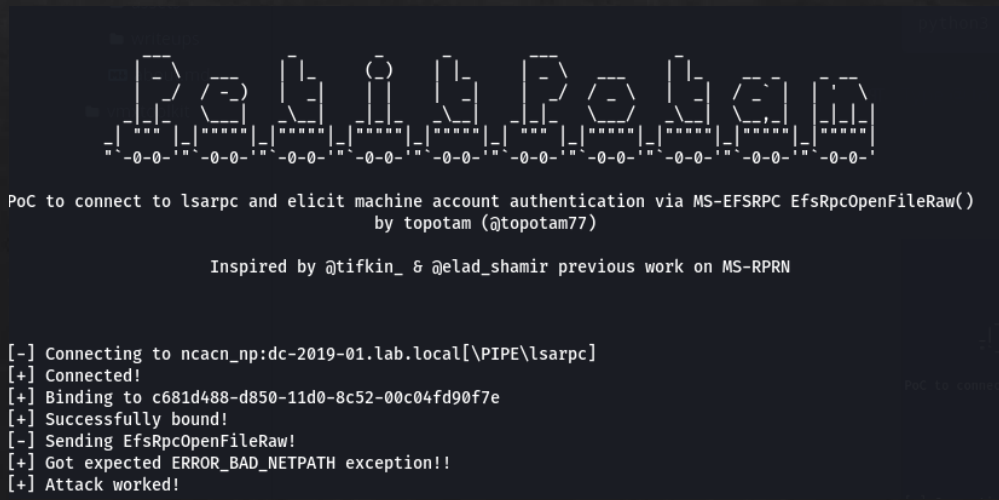
NTLM Relays

- 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

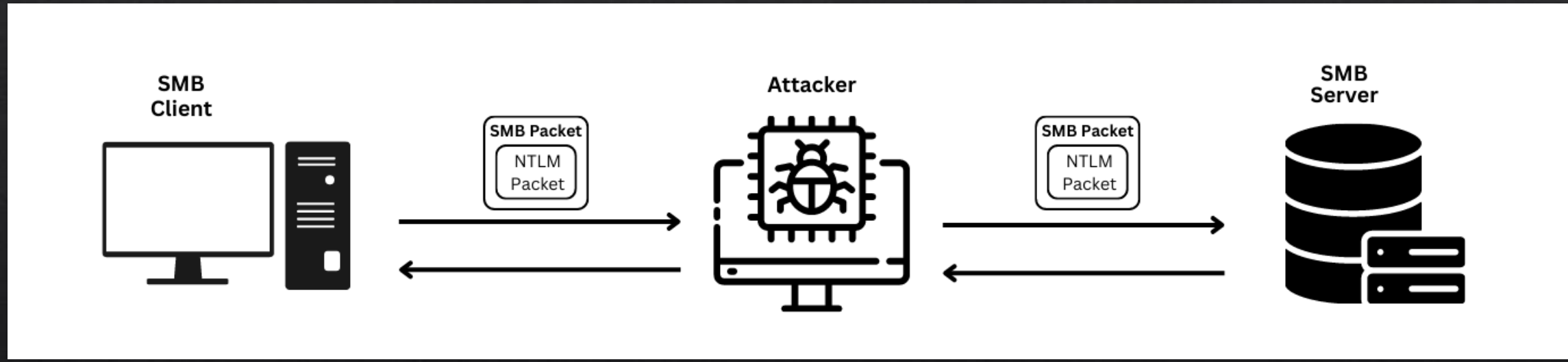
Types of NTLM Relay's

- 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

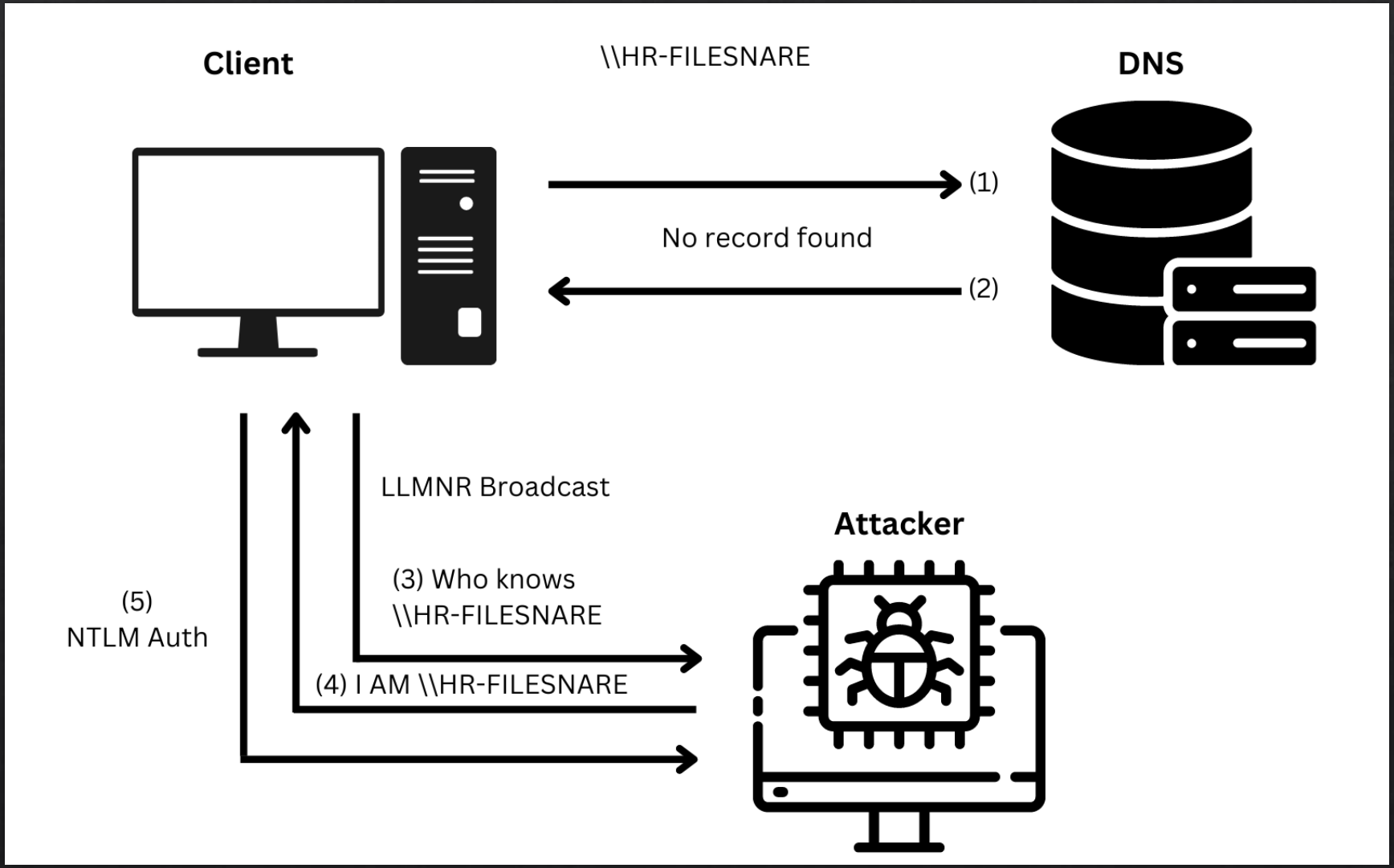




Protocol Relay Traffic

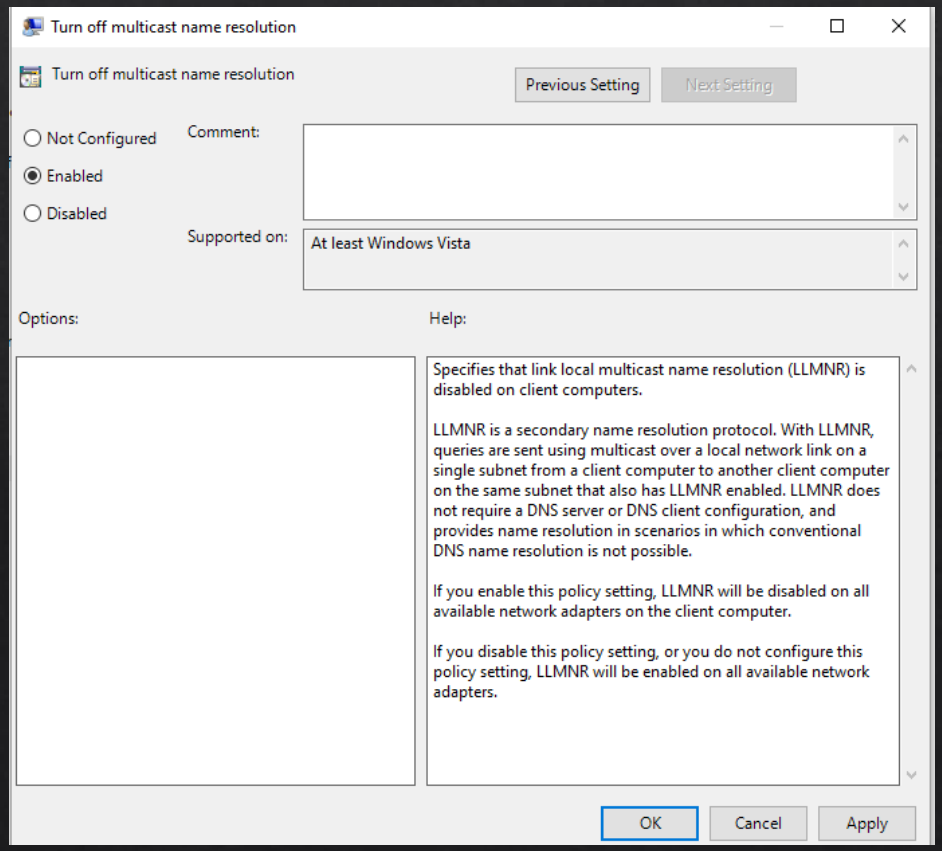


LLMNR Poisoning



Poisoning Mitigations

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



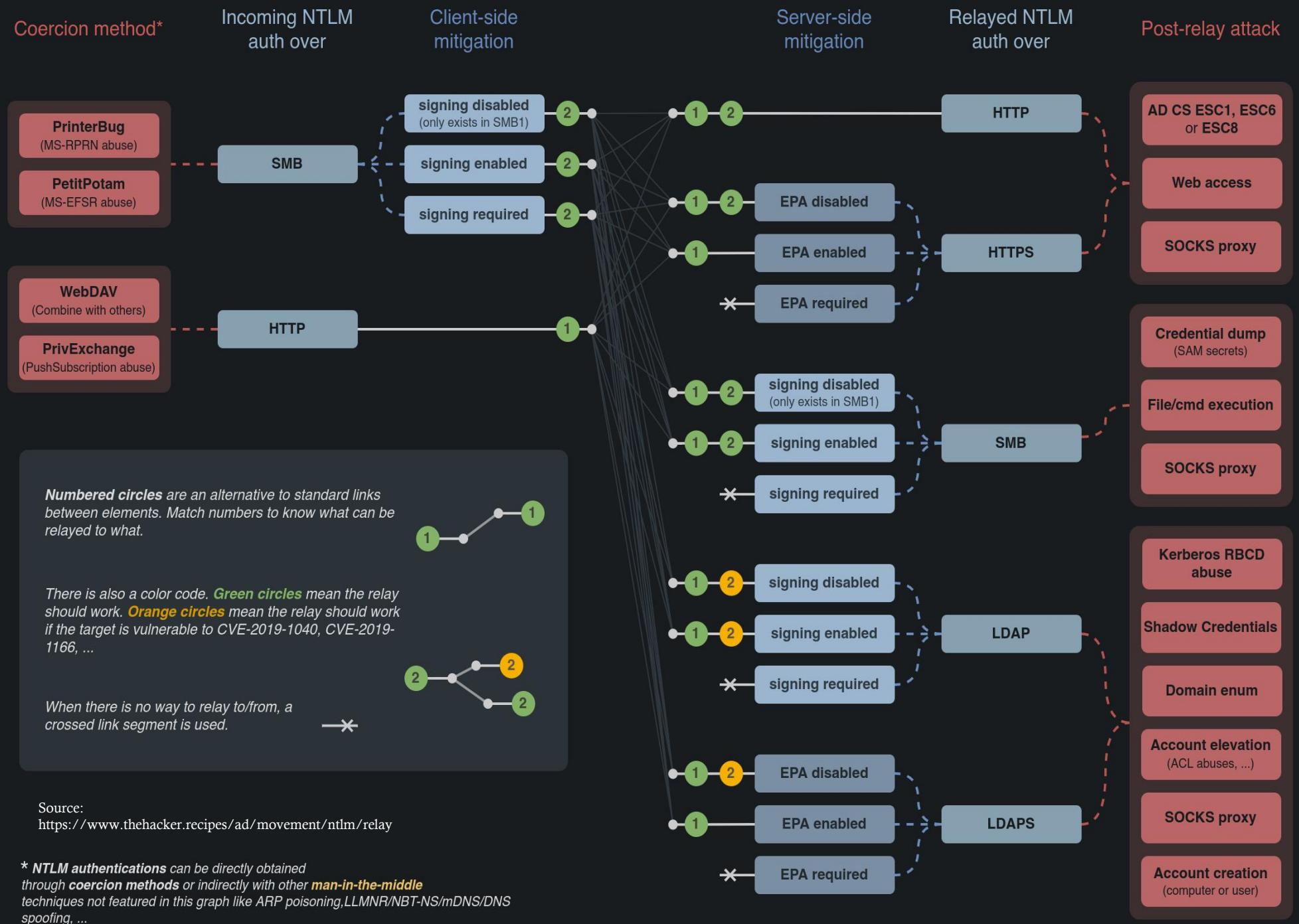
NTLM Coercion

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!!!



Source:
https://www.thehacker.recipes/ad/movement/ntlm/relay

* ***NTLM authentications*** *can be directly obtained through* ***coercion methods*** *or indirectly with other* ***man-in-the-middle*** *techniques not featured in this graph like ARP poisoning,LLMNR/NBT-NS/mDNS/DNS spoofing, ...*

Hunting NTLM traffic

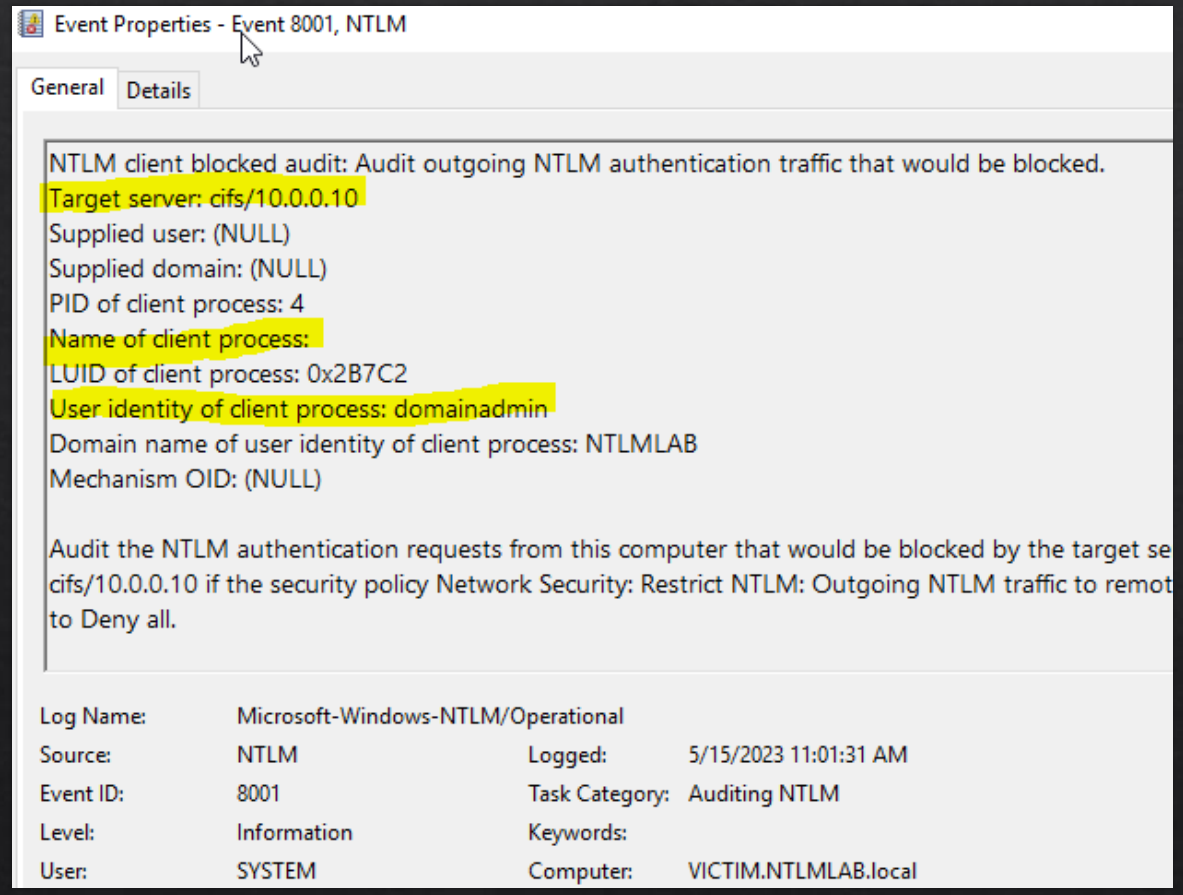
- Domain Controller => Event ID 8004
- Member Server => Event ID 8003
- Client => Event ID 8001
- Enable NTLM auditing
- All client and servers

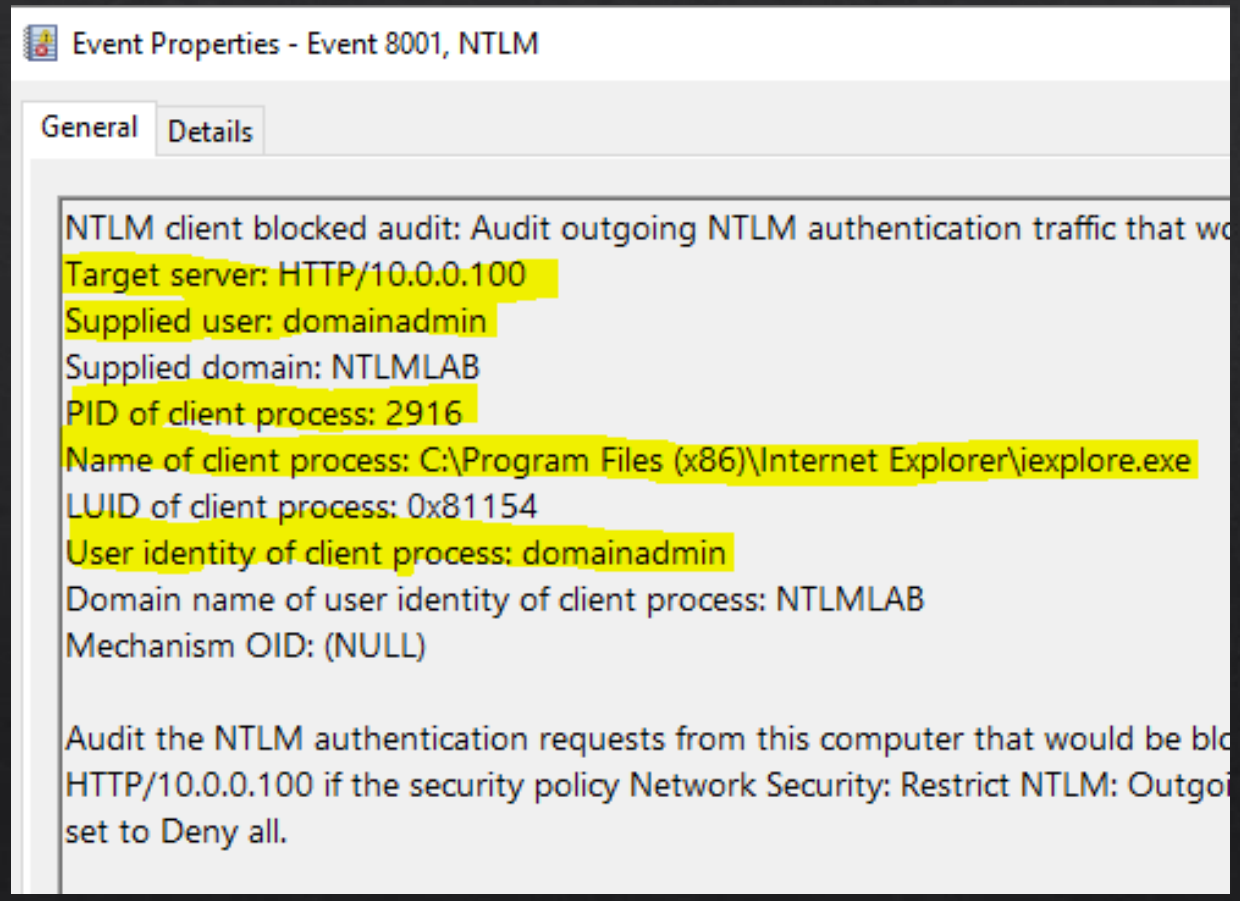
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers = Audit All	8001
Network security: Restrict NTLM: Audit Incoming NTLM Traffic = Enable auditing for all accounts	8003

- Domain Controllers

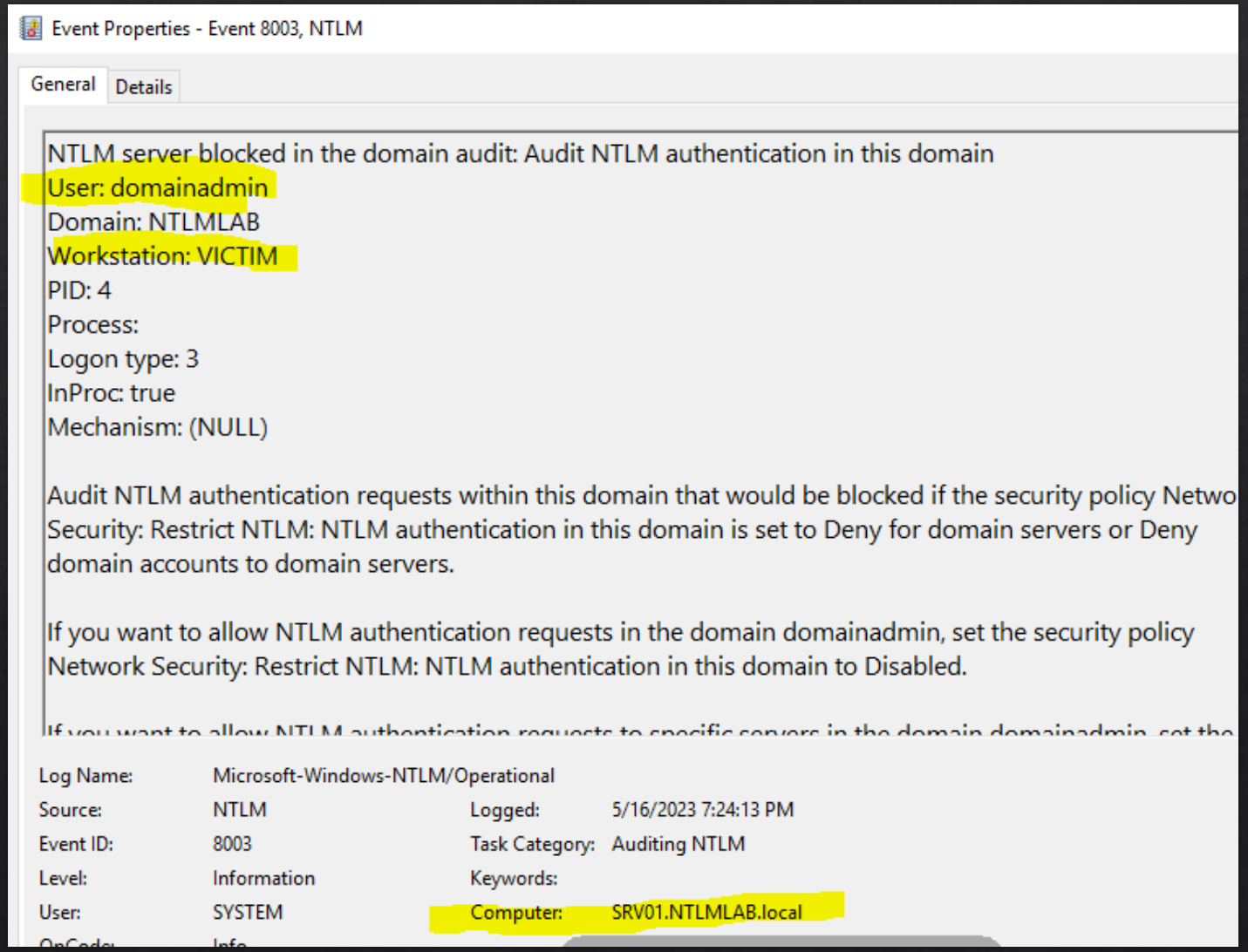
Network security: Restrict NTLM: Audit NTLM authentication in this domain = Enable all	8004

Hunting NTLM traffic ID 8001

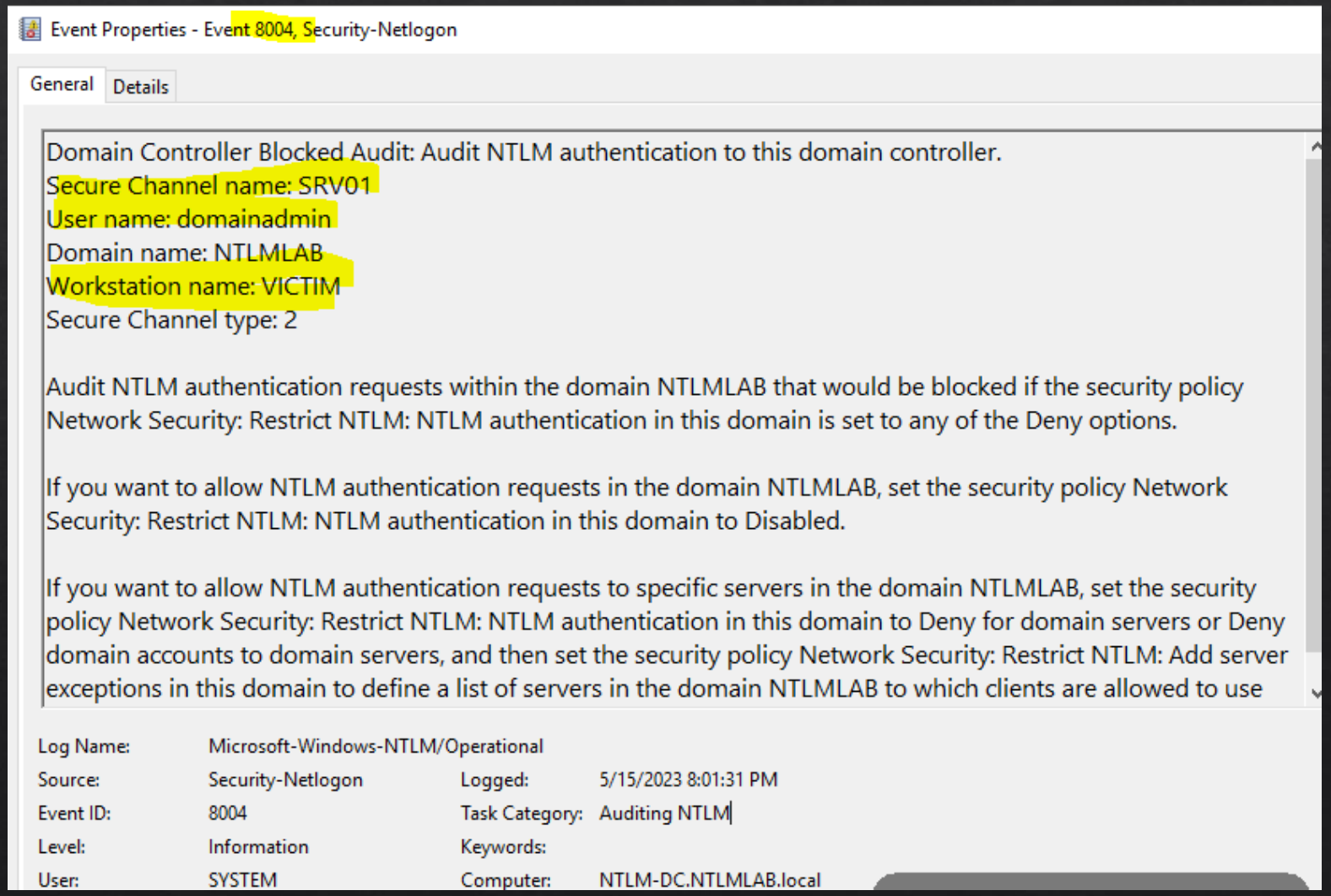




Hunting NTLM traffic ID 8003



Hunting NTLM traffic ID 8004



Questions?

attacker [Running] - Oracle VM VirtualBox

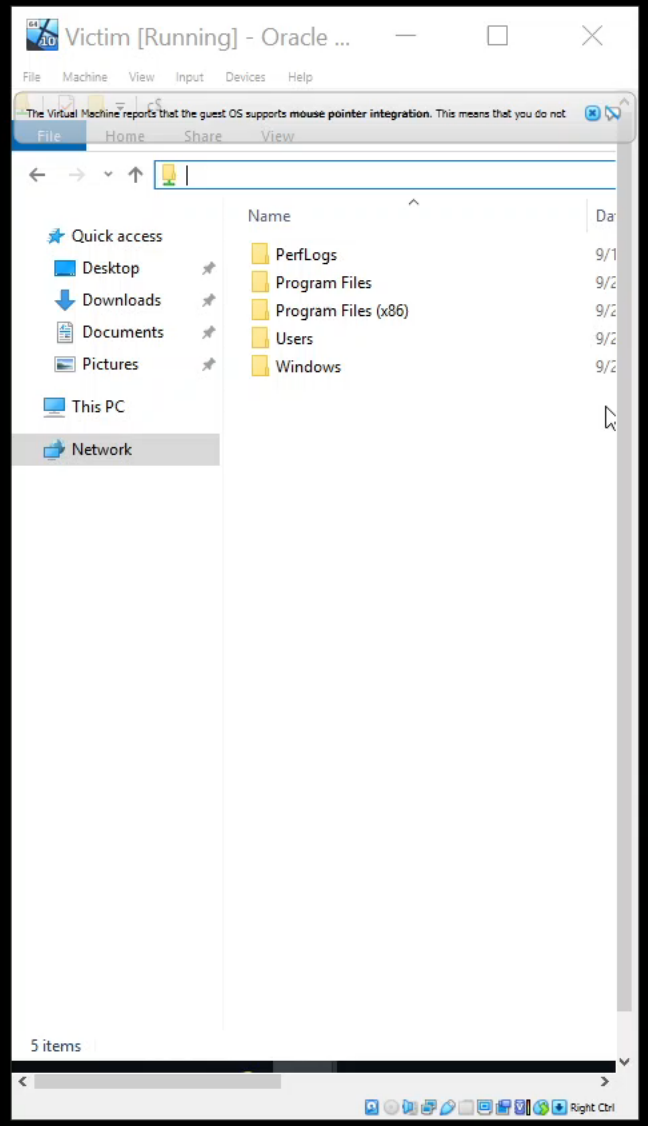
File Machine View Input Devices Help

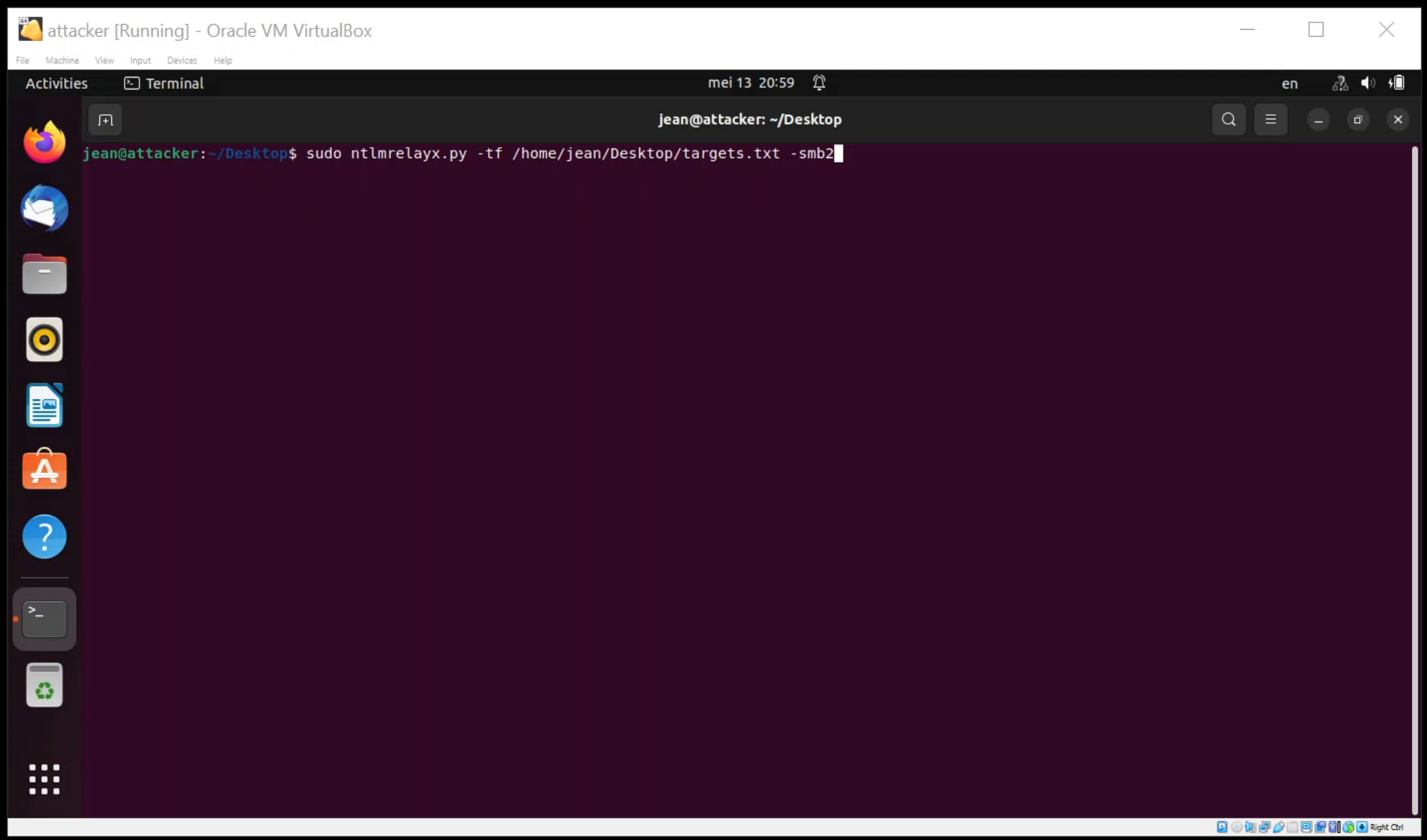
Activities Terminal mei 13 00:54 en

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
```

Right Ctrl


Victim [Running] - Oracle ...
File Machine View Input Devices Help
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not
File Home Share View
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
PerfLogs
Program Files
Program Files (x86)
Users
Windows
5 items
Right Ctrl


attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
mei 13 20:59
en
jean@attacker: ~/Desktop
jean@attacker:~/Desktop$ sudo ntlmrelayx.py -tf /home/jean/Desktop/targets.txt -smb2
Right Ctrl

1:59 PM
5/13/2023