Putting NTLM in the Doghouse

The journey of modeling NTLM relay and authentication coercion attacks in BloodHound

Lee Chagolla-Christensen & Will Schroeder

Rohan Vazarkar & Justin Kohler

Introductions

NEW STUFF

BACKGROUND

RESEARCH

NTLM IN THE WILD

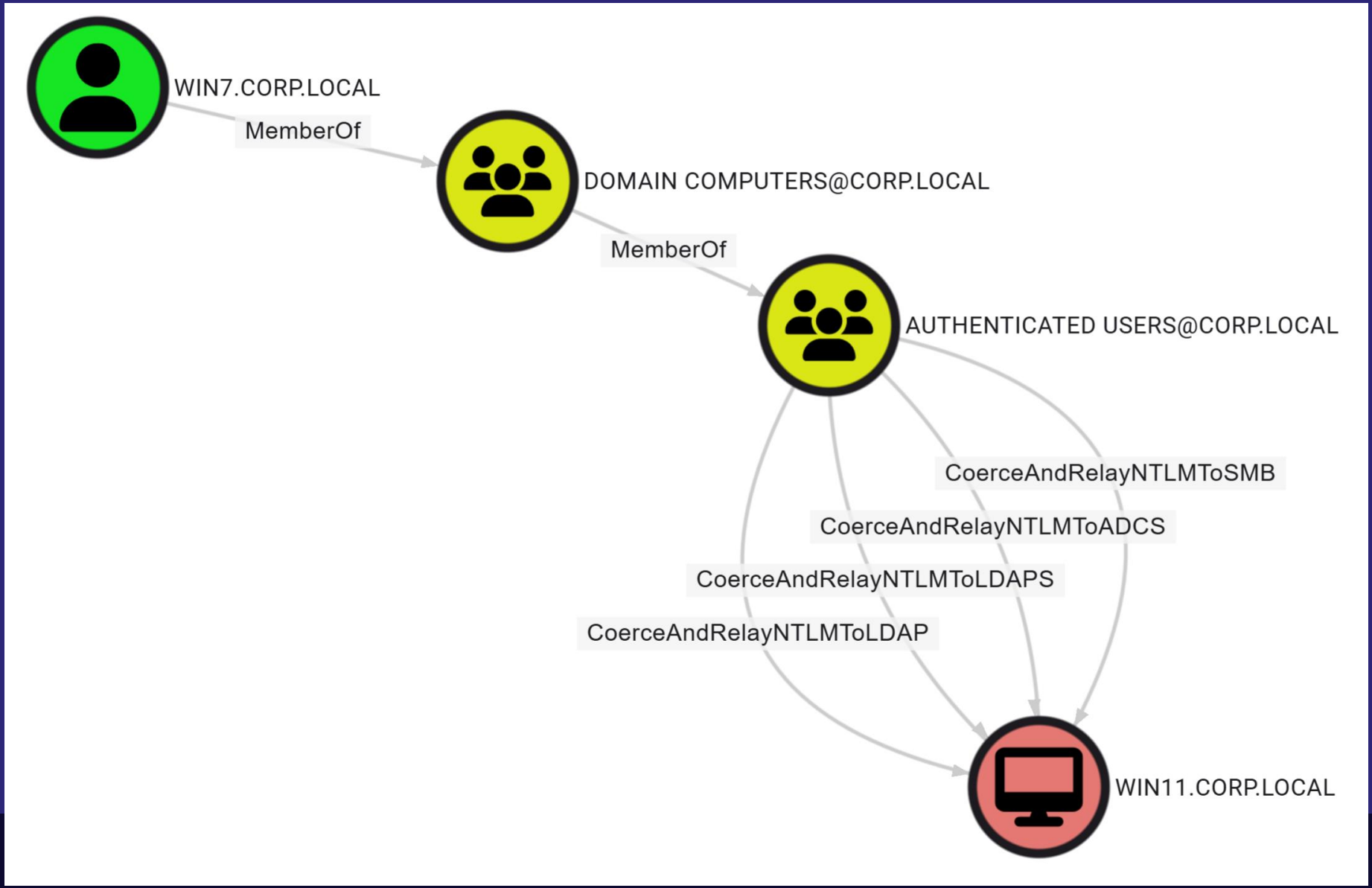
LESSONS LEARNED

TLDR: 4 New BloodHound Edges

A powerful combo: Authentication Coercion + NTLM Relay

- CoerceAndRelayNTLMToSMB
- CoerceAndRelayNTLMToADCS
- CoerceAndRelayNTLMToLDAP
- CoerceAndRelayNTLMToLDAPS

A Powerful Combo: Authentication Coercion + NTLM Relay



Collection Options

WebClientService, LdapServices, SmbInfo, NTLMRegistry

```
PS C:\> .\SharpHound.exe --help
2025-03-30T13:00:18.9526342-07:00|INFORMATION|This version of SharpHound is compatible with the 5.0.
0 Release of BloodHound
SharpHound 2.6.1+340aaa6c3f765960645caf012eee7a35550129ce
Copyright (C) 2025 SpecterOps

  -c, --collectionmethods      (Default: Default) Collection Methods: Group, LocalGroup, LocalAdmin,
                               RDP, DCOM, PSRemote, Session, Trusts, ACL, Container, ComputerOnly,
                               GPOLocalGroup, LoggedOn, ObjectProps, SPNTargets, UserRights,
                               Default, DCOnly, CARegistry, DCRegistry, CertServices,
                               WebClientService, LdapServices, SmbInfo, NTLMRegistry, All
```

All collectable as a low-priv user!*

Background

The basics of Authentication Coercion and NTLM Relay

Why did we model NTLM relay?

Prioritization:

- Intuition
- RICE: Priority = (Reach * Impact * Confidence) / Effort
- Assessment work shows prevalence of relay attack paths
- Very ripe set of impactful targets (AD CS, SCCM, LDAP, MSSQL)
- Current assessment/operator workflows weren’t ideal
- Plumbing is useful for modeling other future attack primitives

Isn’t Microsoft getting rid of NTLM?

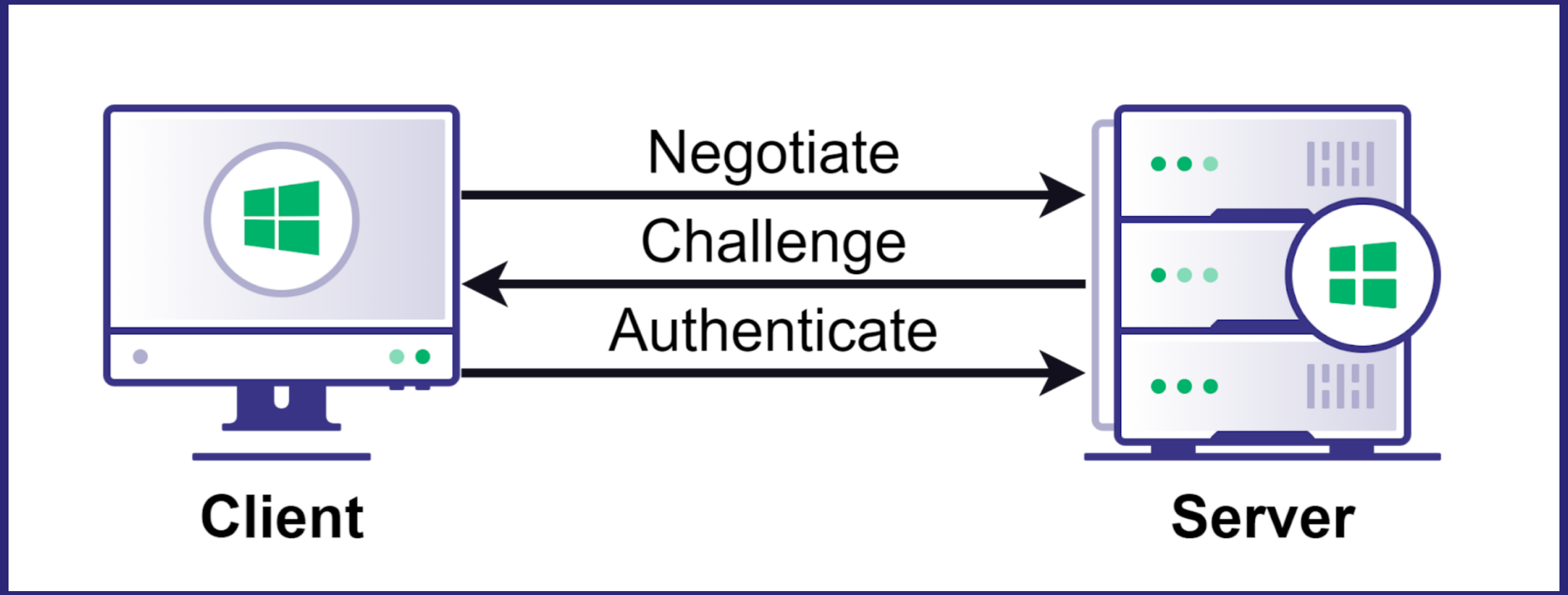
NTLM: “I’m not dead yet!”

- Legacy systems
- IAKERB is not enabled…yet
- Still enabled by default
  - Deprecated so far, not disabled / removed

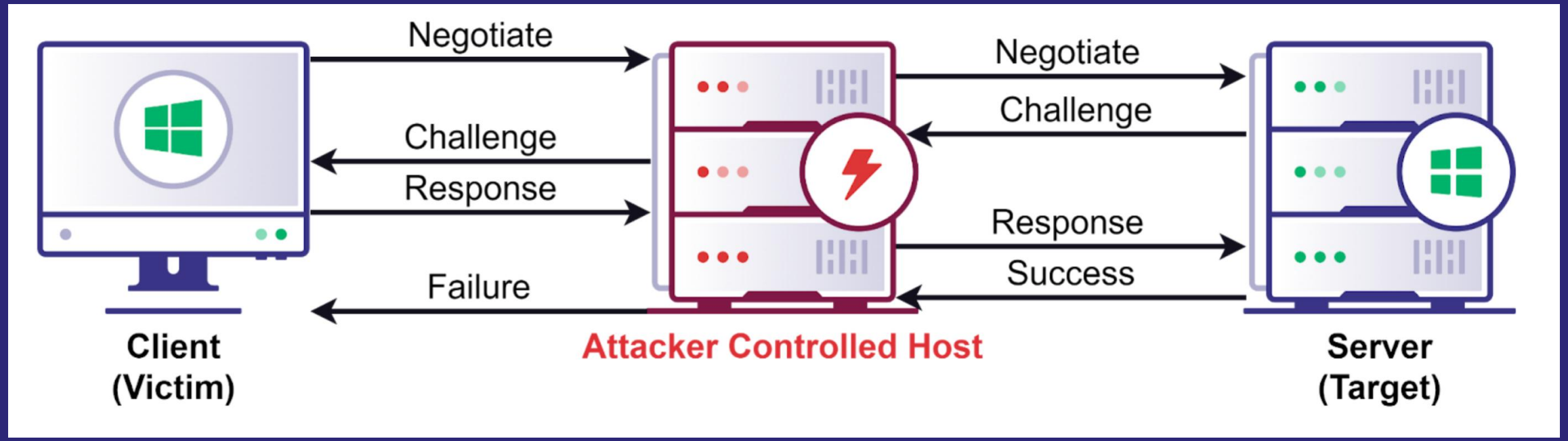
NTLM	NTLMv1 is removed. LANMAN and NTLMv2 are no longer under active feature development and are deprecated. NTLMv2 will continue to work but will be removed from Windows Server in a future release. Replace calls to NTLM to calls to Negotiate, which try to authenticate with Kerberos and only fall back to NTLM when necessary. For more information, see The evolution of Windows authentication.

NTLM Authentication Messages

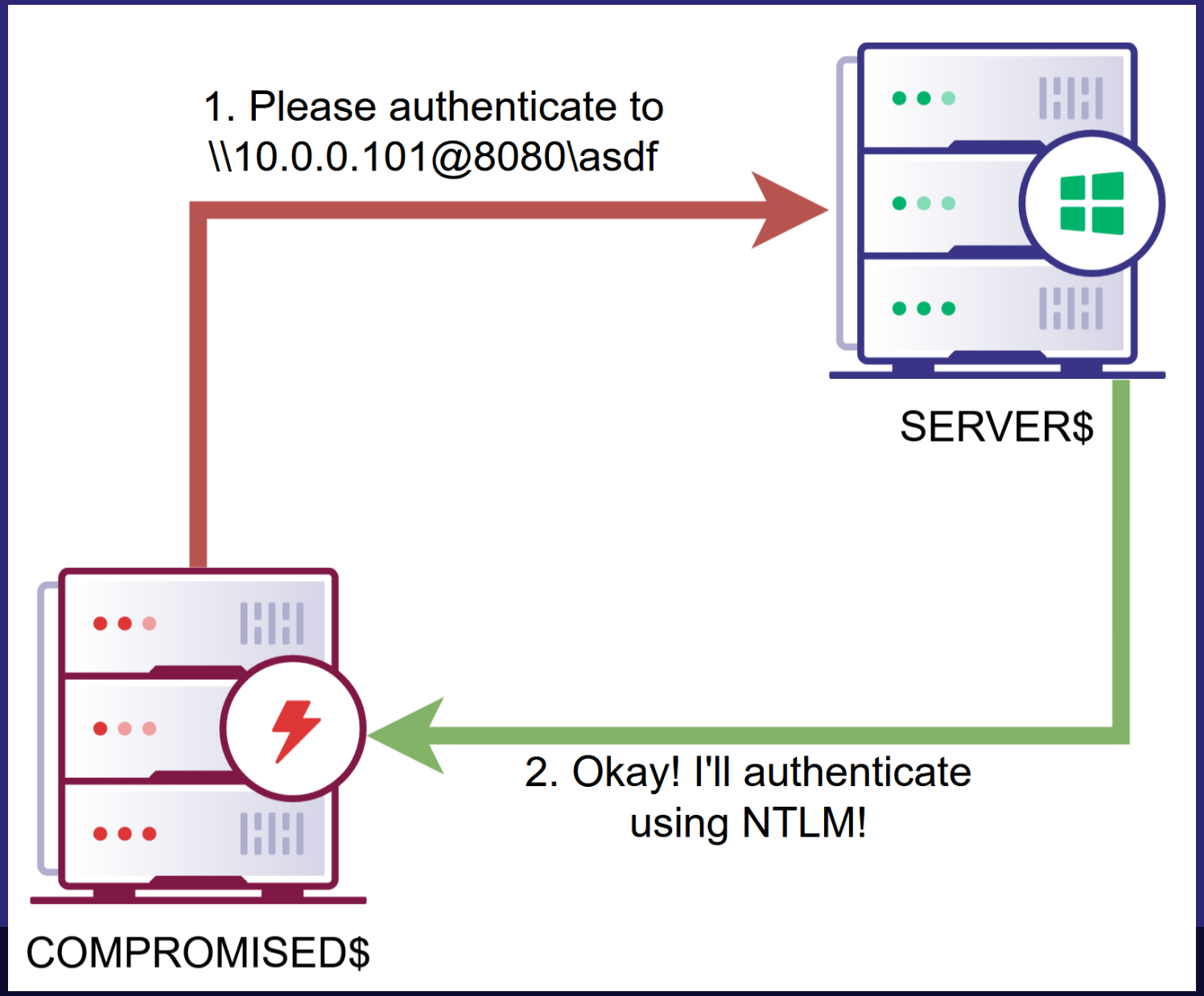
The basic, big idea



Edge Component 1: NTLM Relay

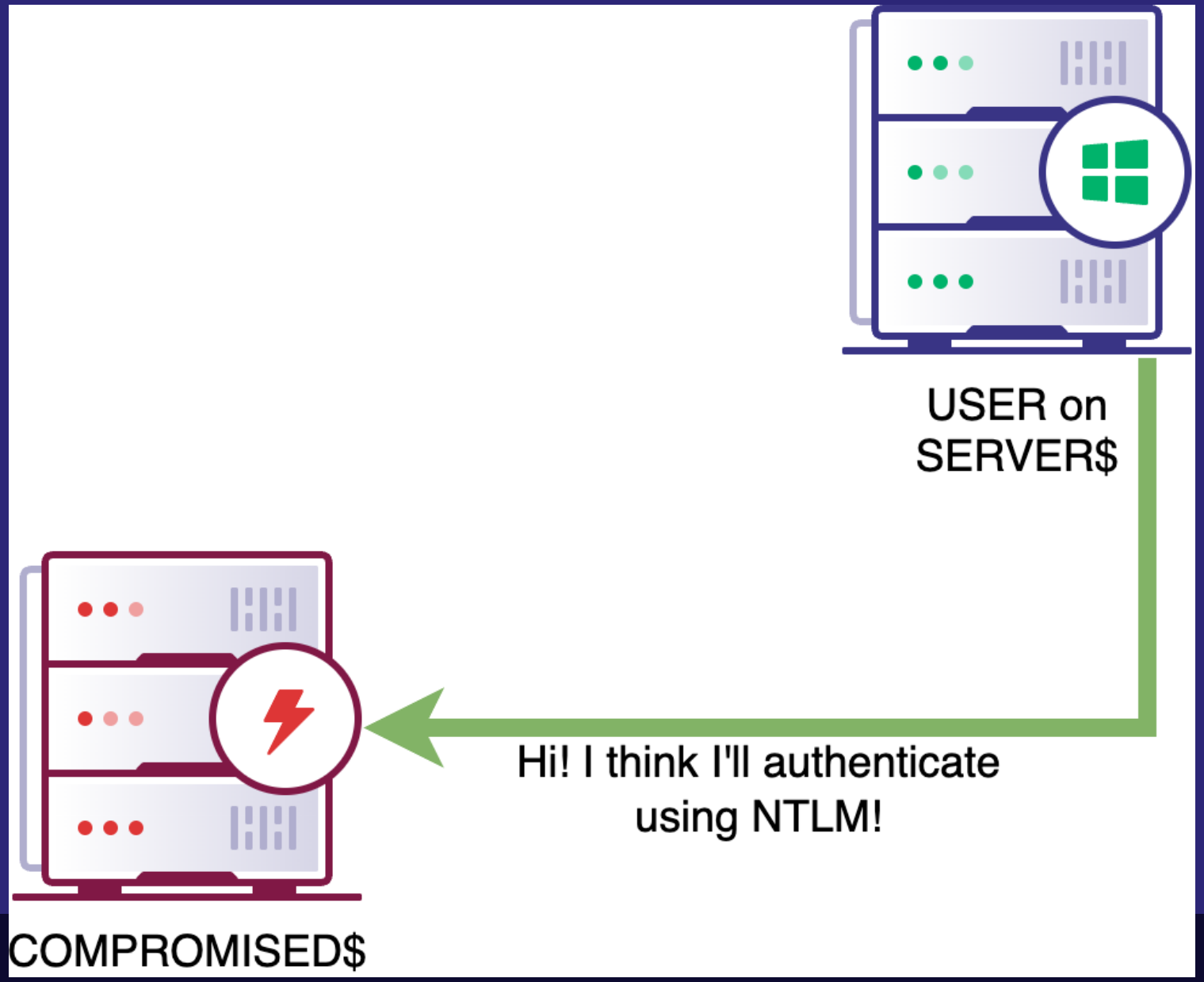


Edge Component 2: Coerced Computer Authentication



Examples:
- SpoolSample
- PetitPotam
- Coercer

Edge Component 2.5: Passive Authentication

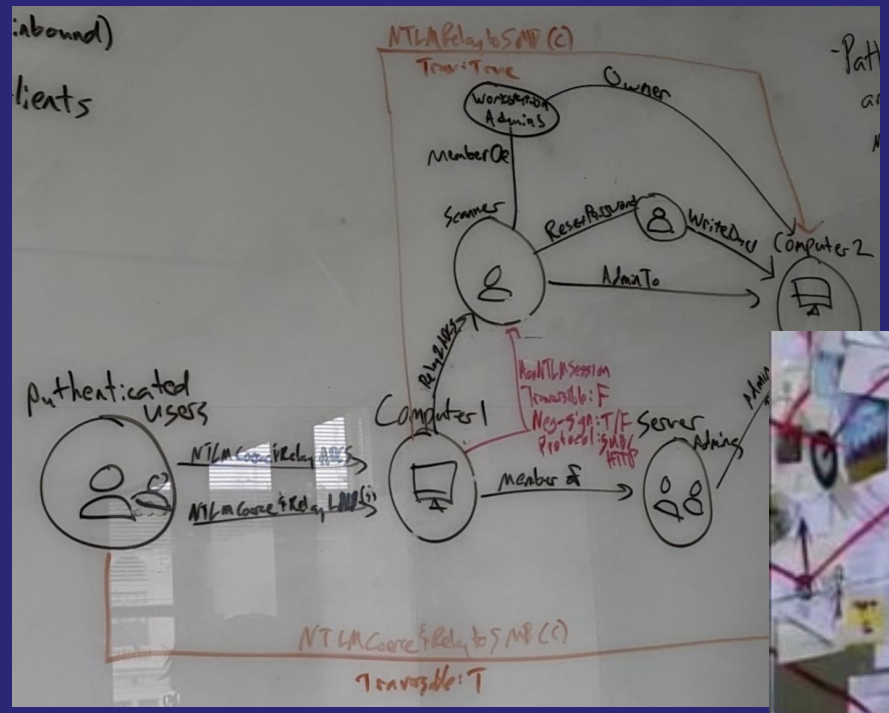


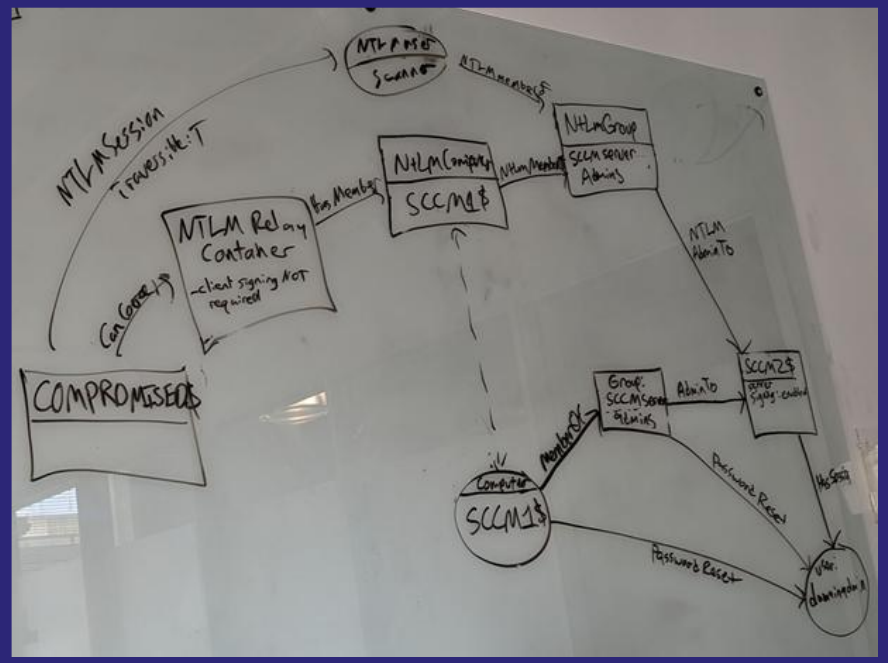
Not Currently Implemented in BloodHound!

Requires event logs from each affected host or each Domain Controller

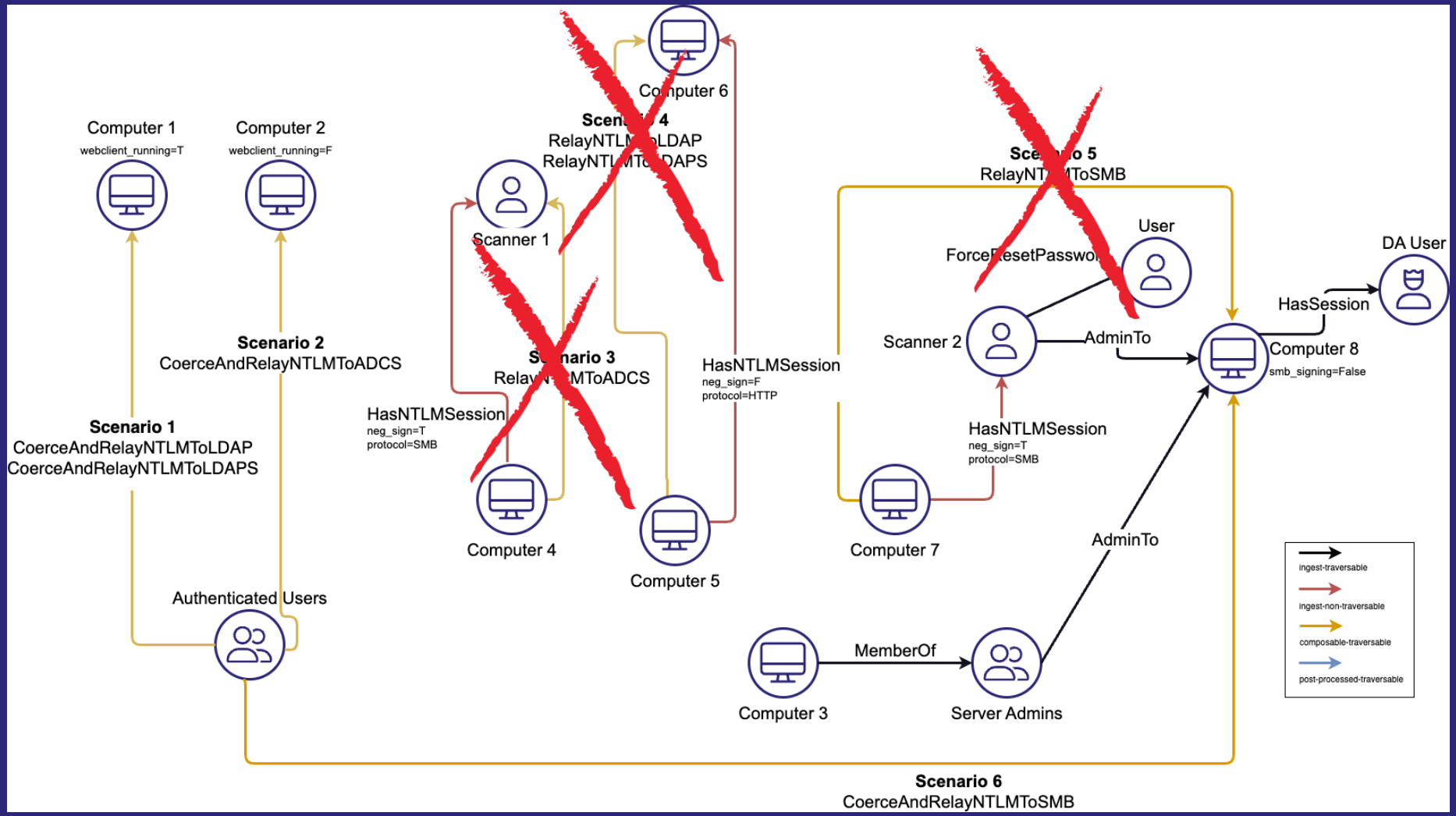
Early Relay Modeling

Lee, Will, and Elad





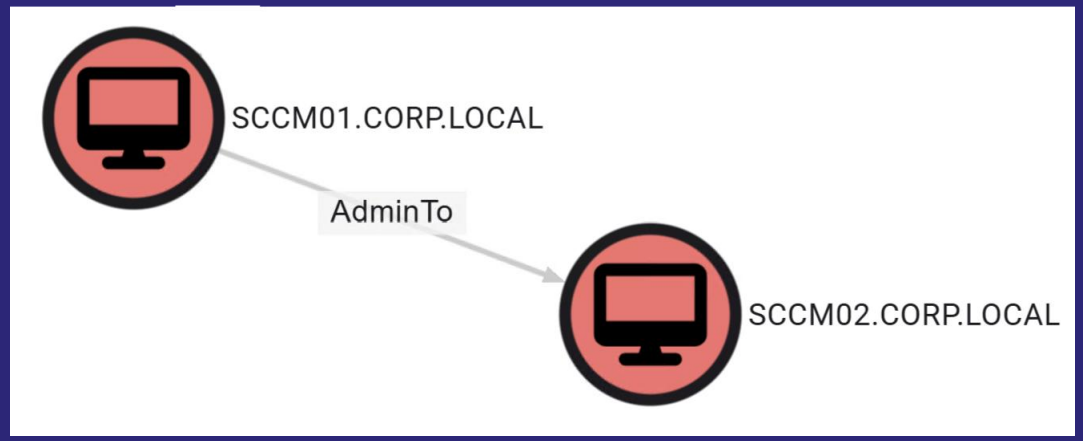
Later Relay Modeling

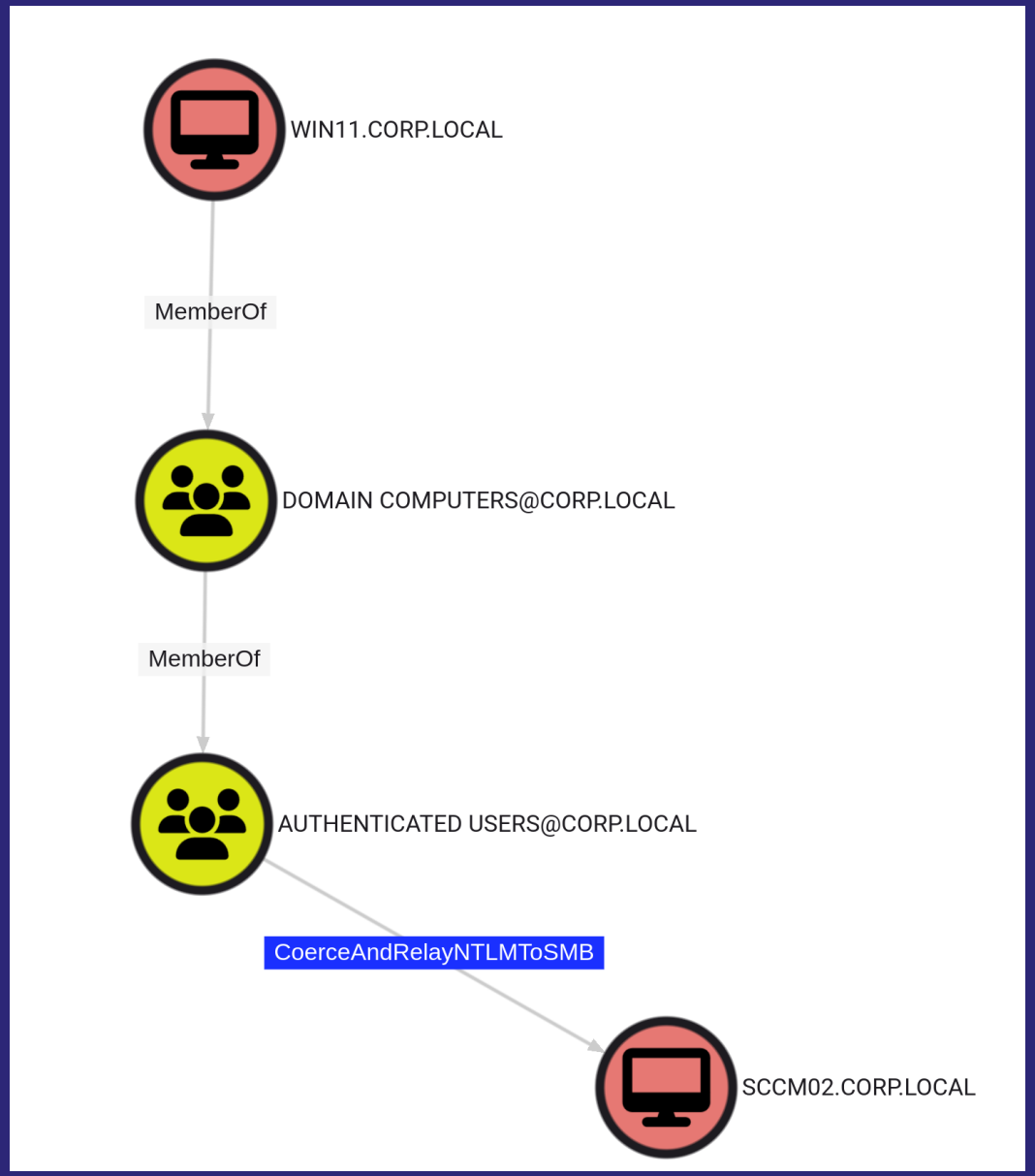


CoerceAndRelayNTLMToSMB

<u>Setup:</u>

- Attacker compromises WIN11
- SCCM01 has local admin to SCCM02





CoerceAndRelayNTLMToSMB

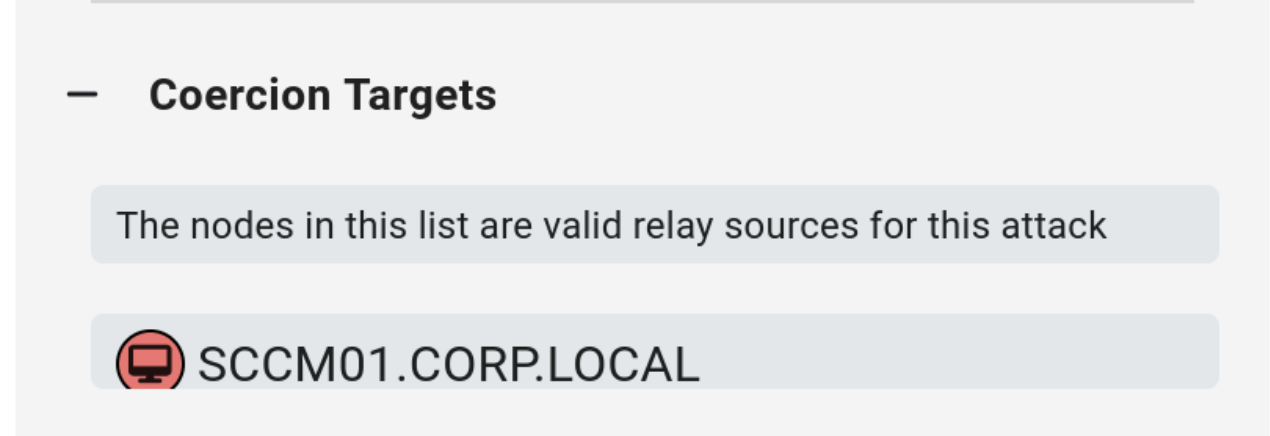
Coercion (Source) Target Requirement

- Outbound NTLM Allowed

Key: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\
Value: RestrictSendingNTLMTraffic

Relay Target Requirements:

- SMB signing not required



Mitigation: SMB Signing

- Protection negotiated between client/server in the SMB1/2 negotiate messages' "Security Mode" field
  - Note: this is different than signing/sealing (session security) negotiated in the NTLM protocol
  - Controlled by HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
    - Value: EnableSecuritySignature / RequireSecuritySignature
- Can be enumerated unauthenticated (nmap, nxc,Invoke-SMBEnum, Responder's RunFinger.py, FeigongSec/NTLMINFO)

No.	Time	Source	Destination	Protocol	Length	Info
10	1.229742	192.168.230.200	192.168.230.101	SMB2	306	Negotiate Protocol Response
11	1.229890	192.168.230.101	192.168.230.200	SMB2	350	Negotiate Protocol Request
12	1.230633	192.168.230.200	192.168.230.101	SMB2	430	Negotiate Protocol Response
13	1.231976	192.168.230.101	192.168.230.200	SMB2	220	Session Setup Request, NTLMSSP_NEGOTIATE
14	1.232776	192.168.230.200	192.168.230.101	SMB2	347	Session Setup Response, Error: STATUS_MORE_PR
15	1.233336	192.168.230.101	192.168.230.200	SMB2	641	Session Setup Request, NTLMSSP_AUTH, User: CO

```
> Frame 12: 430 bytes on wire (3440 bits), 430 bytes captured (3440 bits) on interface \Device\NPF_{50FE6B39-79AB-4F4
> Ethernet II, Src: Microsoft_00:33:10 (00:15:5d:00:33:10), Dst: Microsoft_00:33:0f (00:15:5d:00:33:0f)
> Internet Protocol Version 4, Src: 192.168.230.200, Dst: 192.168.230.101
> Transmission Control Protocol, Src Port: 445, Dst Port: 53378, Seq: 253, Ack: 370, Len: 376
v NetBIOS Session Service
    Message Type: Session message (0x00)
    Length: 372
v SMB2 (Server Message Block Protocol version 2)
  > SMB2 Header
  v Negotiate Protocol Response (0x00)
      [Preauth Hash: 13c9d0484e564d13e83a8c91e2b293578fd1a7e29b98edce6d574c73b2917c1cdb377b45aeded5de7213278558dded
    > StructureSize: 0x0041
    > Security mode: 0x01, Signing enabled
```

Note: it's enabled but NOT required!

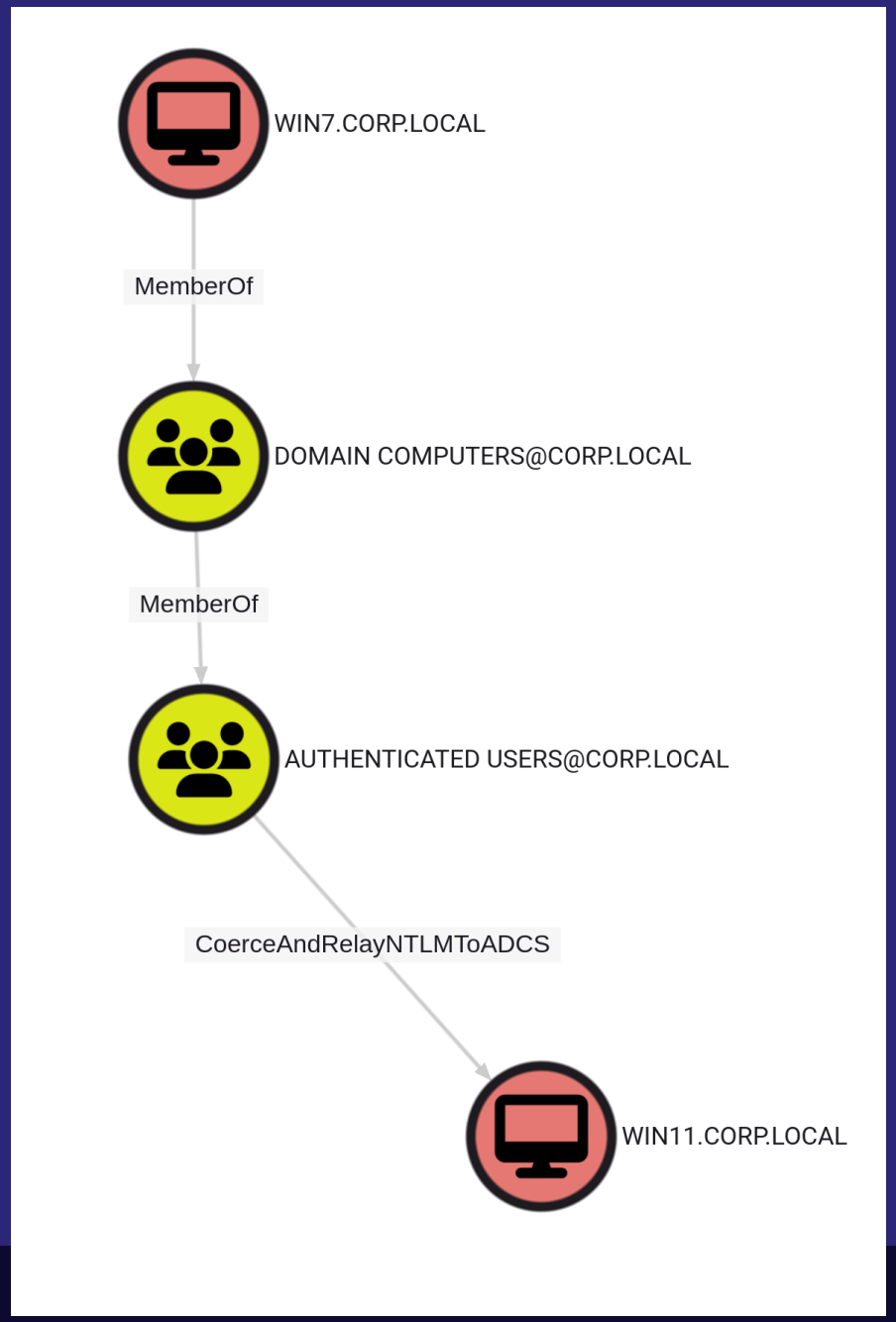
CoerceAndRelayNTLMToADCS (ADCS ESC8)

CA1@CORP.LOCAL

Has Basic Constraints:	FALSE
Has Enrollment Agent Restrictions:	FALSE
Has Vulnerable Endpoint:	TRUE
HTTP Enrollment Endpoints:	http://DC01.CORP.LOCAL/certsrv/
HTTPS Enrollment Endpoints:	https://DC01.CORP.LOCAL/certsrv/

<u>Setup:</u>

- Attacker compromises WIN7
- ADCS installed with web enrollment endpoints (new property on CA)
- Target machine (WIN11) can enroll in an applicable certificate template



CoerceAndRelayNTLMToADCS (ADCS ESC8)

<u>Coercion (Source) Target Requirement</u>

- Outbound NTLM Allowed

<u>Relay Target (AD CS) Requirements:</u>

- An HTTP enrollment endpoint
- HTTP enabled or HTTPS w/o Extended Protection for Authentication (EPA, a.k.a. channel binding)

Edge Composition

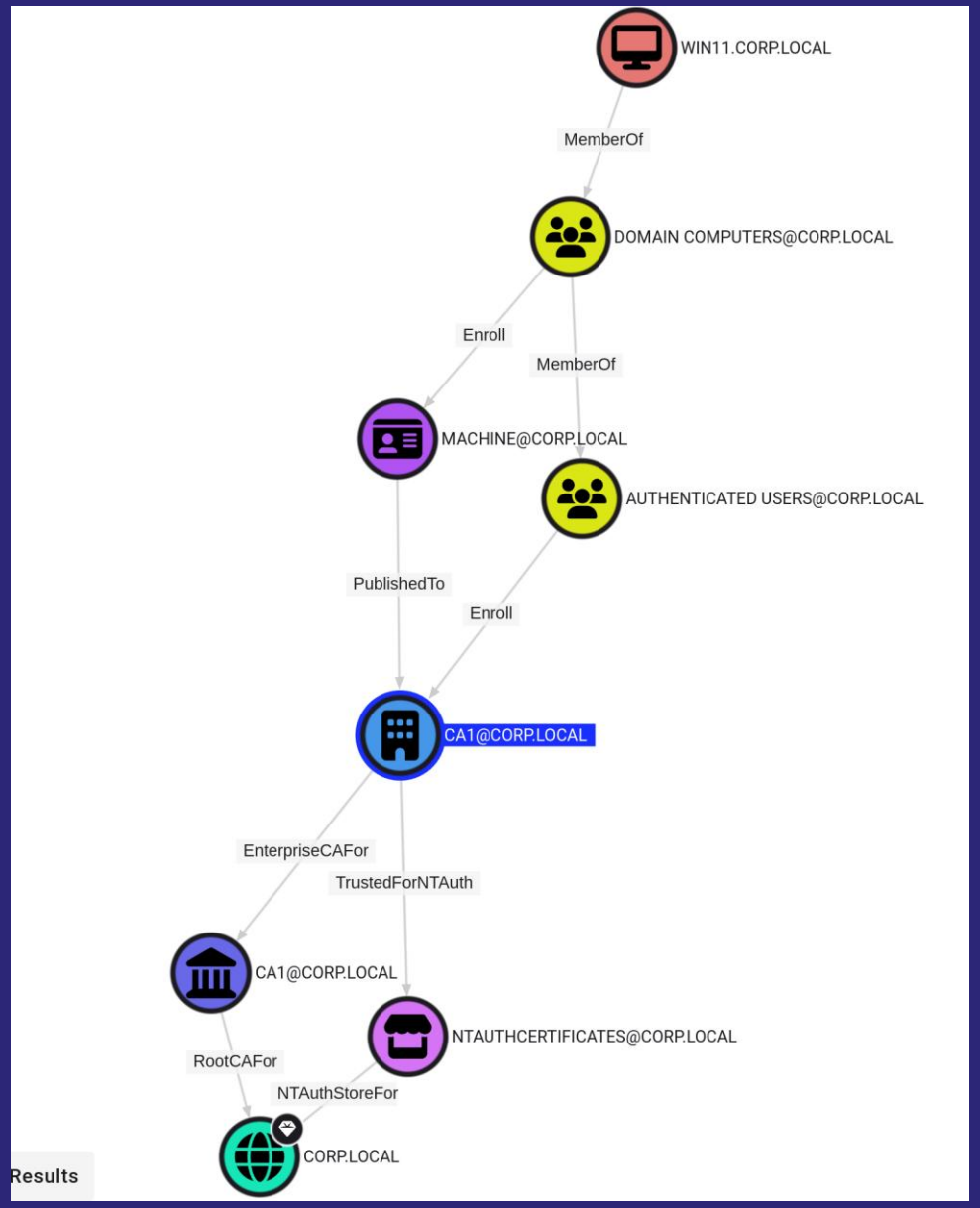
There’s a lot going on there!

Composition

The relationship represents the effective outcome of the configuration and relationships between several different objects. All objects involved in the creation of this relationship are listed here:

- MACHINE@CORP.LOCAL
- DOMAIN COMPUTERS@CORP.LOCAL
- SCOMSERVER.CORP.LOCAL
- CORP.LOCAL
- AUTHENTICATED USERS@CORP.LOCAL
- CA1@CORP.LOCAL
- NTAUTHCERTIFICATES@CORP.LOCAL
- CA1@CORP.LOCAL

Activate Windows
Go to Settings to activate Windows.



Mitigation: Removal or Extended Protection for Authentication(EPA) / Channel Binding?

- Binds a token from the outer secure protocol (TLS) into an NTLM Authenticate message
- SharpHound currently requires a ***low privileged*** user to enumerate it

```
v NTLMv2 Response: 6e61d6b7d705b96cfde81fe6460440e00101
    NTProofStr: 6e61d6b7d705b96cfde81fe6460440e0
    Response Version: 1
    Hi Response Version: 1
    Z: 000000000000
    Time: Dec 13, 2023 17:01:17.079303800 UTC
    NTLMv2 Client Challenge: 0cf195d22fa51aa1
    Z: 00000000
  > Attribute: NetBIOS domain name: SHENANIGANS
  > Attribute: NetBIOS computer name: DC1
  > Attribute: DNS domain name: shenanigans.labs
  > Attribute: DNS computer name: DC1.shenanigans.labs
  > Attribute: DNS tree name: shenanigans.labs
  > Attribute: Timestamp
  v Attribute: Flags
      NTLMV2 Response Item Type: Flags (0x0006)
      NTLMV2 Response Item Length: 4
      Flags: 0x00000002
  > Attribute: Restrictions
  > Attribute: Channel Bindings
  > Attribute: Target Name: cifs/dc1.shenanigans.labs
  > Attribute: End of list
    padding: 00000000
> Domain name: shenanigans
> User name: alice
> Host name: DEV
> Session Key: 4f85c5294d41c8468849a2a86c5db882
> Negotiate Flags: 0xe2888215, Negotiate 56, Negotiate Ke
> Version 10.0 (Build 20348); NTLM Current Revision 15
  MIC: 2b020190f4cfb90d5d91ff9be02fdc5c
```

CoerceAndRelayNTLMToLDAP(S)

DC01.CORP.LOCAL

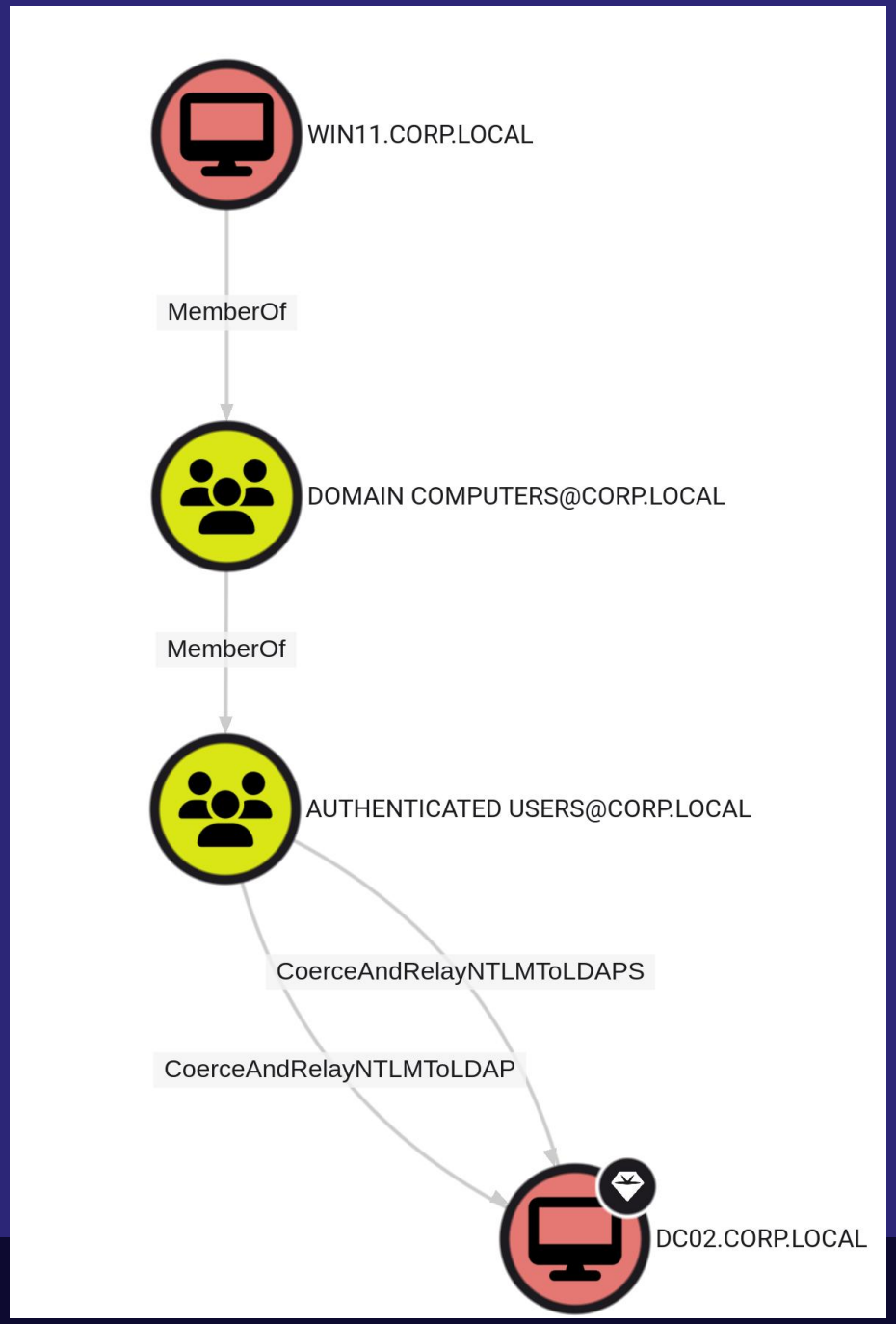
LDAP Available:	TRUE
LDAP Signing:	FALSE
LDAPS Available:	TRUE
LDAPS EPA:	FALSE

DC02.CORP.LOCAL

User Account Control:	532480
WebClient Running:	TRUE

<u>Setup:</u>

- Attacker compromises WIN11
- Domain Controller
- Target computer (DC02) has the WebClient service running / installed



CoerceAndRelayNTLMToLDAP(S)

<u>Coercion (Source) Target Requirement</u>

- Outbound NTLM Allowed
- WebClient service running

<u>Relay Target (LDAP) Requirements:</u>

- LDAP: No signing

- LDAPS:
    - Extended Protection for Authentication
    - OR LDAP signing disabled

https://offsec.almond.consulting/bypassing-ldap-channel-binding-with-starttls.html

Mitigation: LDAP Signing + LDAPS Channel Binding

Enforce both!

- Signing in this case refers to the signing bit in the NTLM messages

```
Session Key: 4f85c5294d41c8468849a2a86c5db882
Negotiate Flags: 0xe2888215, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negoti
    1... .... .... .... .... .... .... .... = Negotiate 56: Set
    .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
    ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
    ...0 .... .... .... .... .... .... .... = Negotiate 0x10000000: Not set
    .... 0... .... .... .... .... .... .... = Negotiate 0x08000000: Not set
    .... .0.. .... .... .... .... .... .... = Negotiate 0x04000000: Not set
    .... ..1. .... .... .... .... .... .... = Negotiate Version: Set
    .... ...0 .... .... .... .... .... .... = Negotiate 0x01000000: Not set
    .... .... 1... .... .... .... .... .... = Negotiate Target Info: Set
    .... .... .0.. .... .... .... .... .... = Request Non-NT Session: Not set
    .... .... ..0. .... .... .... .... .... = Negotiate 0x00200000: Not set
    .... .... ...0 .... .... .... .... .... = Negotiate Identify: Not set
    .... .... .... 1... .... .... .... .... = Negotiate Extended Security: Set
    .... .... .... .0.. .... .... .... .... = Target Type Share: Not set
    .... .... .... ..0. .... .... .... .... = Target Type Server: Not set
    .... .... .... ...0 .... .... .... .... = Target Type Domain: Not set
    .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
    .... .... .... .... .0.. .... .... .... = Negotiate 0x00004000: Not set
    .... .... .... .... ..0. .... .... .... = Negotiate OEM Workstation Supplied: Not set
    .... .... .... .... ...0 .... .... .... = Negotiate OEM Domain Supplied: Not set
    .... .... .... .... .... 0... .... .... = Negotiate Anonymous: Not set
    .... .... .... .... .... .0.. .... .... = Negotiate NT Only: Not set
    .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
    .... .... .... .... .... ...0 .... .... = Negotiate 0x00000100: Not set
    .... .... .... .... .... .... 0... .... = Negotiate Lan Manager Key: Not set
    .... .... .... .... .... .... .0.. .... = Negotiate Datagram: Not set
    .... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
    .... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
    .... .... .... .... .... .... .... 0... = Request 0x00000008: Not set
    .... .... .... .... .... .... .... .1.. = Request Target: Set
    .... .... .... .... .... .... .... ..0. = Negotiate OEM: Not set
    .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
```

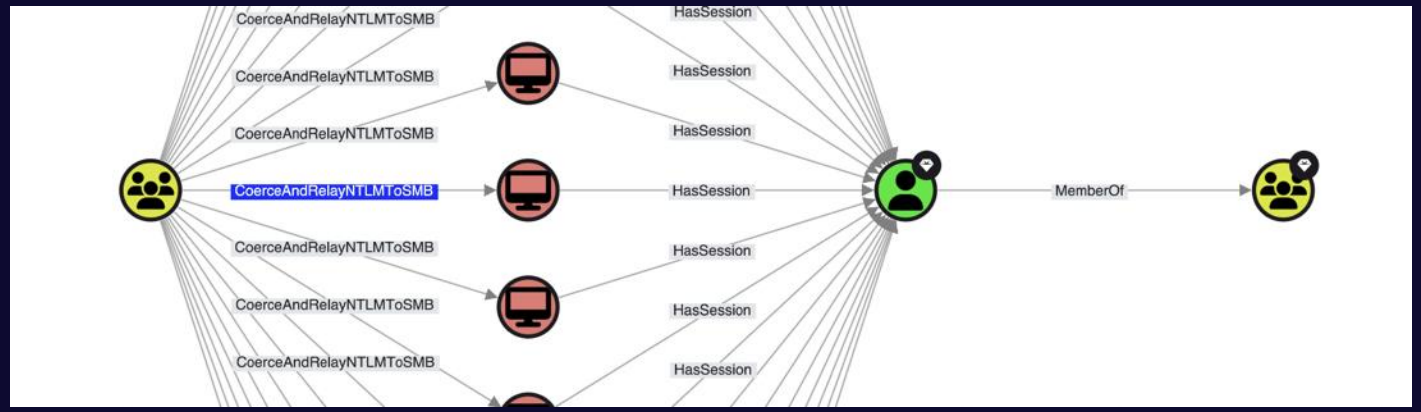
But what does this *actually* look like?

TL;DR NTLM in BloodHound

Why It Matters

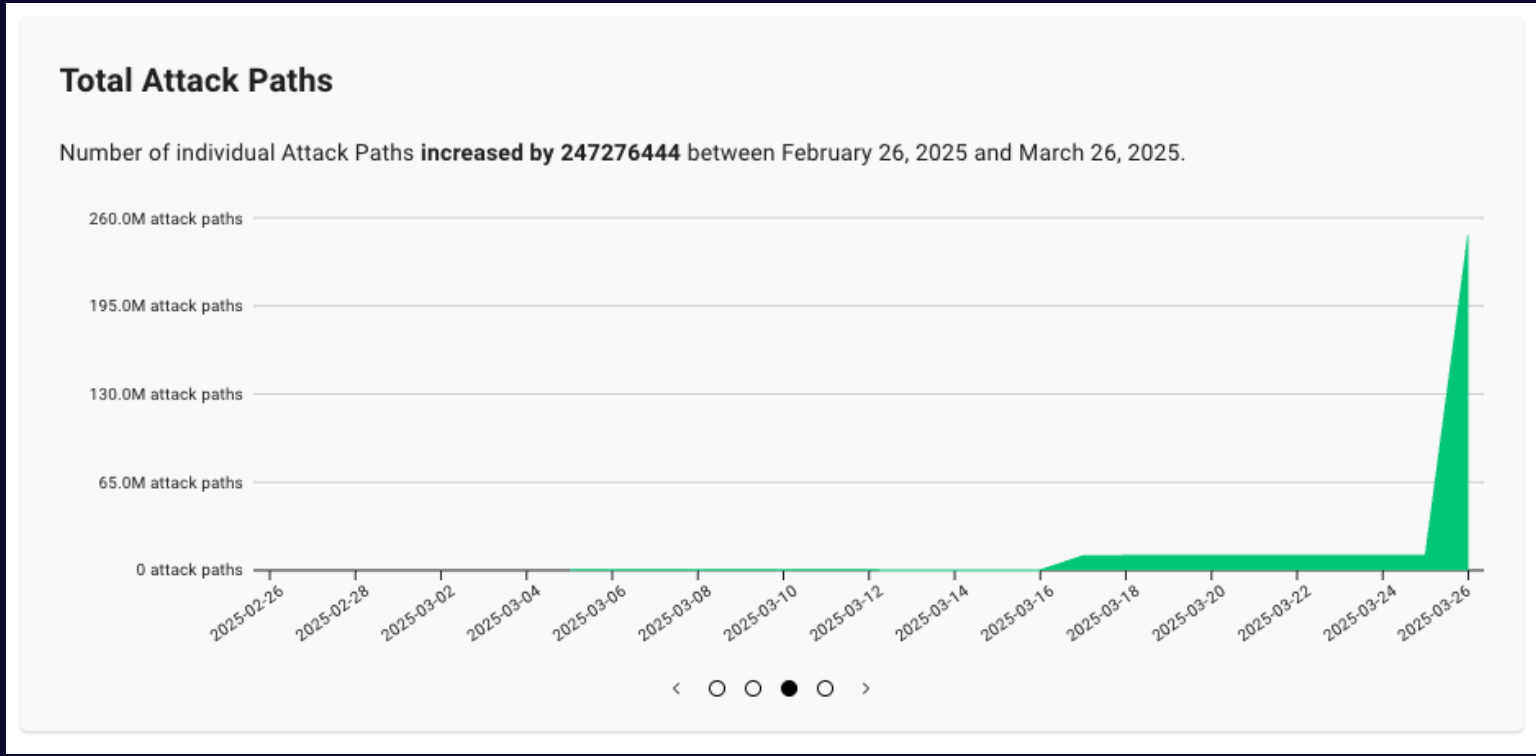
NTLM relay attacks create a troubling scenario where any authenticated user in your environment can *potentially*:

- Compromise systems without needing passwords
- Move laterally with minimal footprint
- Gain control of critical systems
- Bypass traditional security controls
- Execute attacks most security technologies fail to detect



An NTLM relay Attack Path to compromise the environment

It’s…. bad



The *average* exposure introduced by NTLM Attack Paths is 97%

Why we built it

Visualize the Invisible: Map all NTLM relay attack paths across your environment, showing exactly how attackers could move from initial access to critical assets

Understand Real Risk: Identify which systems are vulnerable to NTLM relay attacks based on their current configurations (SMB, LDAP, AD CS, client compatibility)

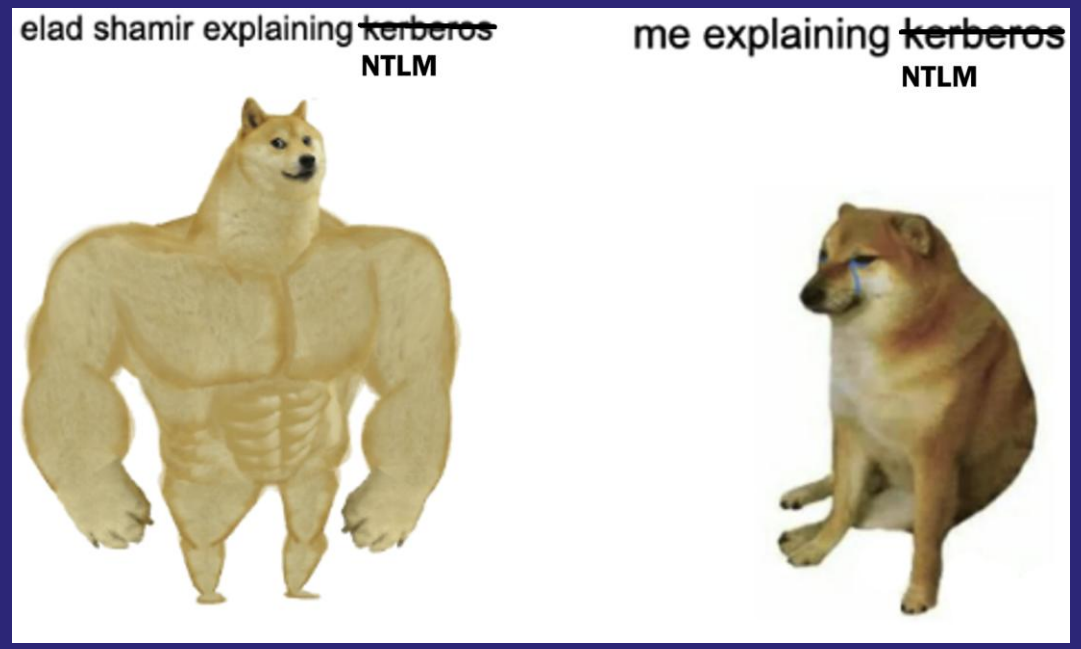
Prioritize Effectively: Focus remediation on the most critical attack paths rather than trying to "fix everything everywhere"

Preserve Legacy Systems: Targeted remediations preserve business-critical legacy communications while removing relay attack paths from the attacker's arsenal.

Measure Security Improvement: Track your progress in eliminating NTLM relay attack paths over time

The Future and Final Thoughts

- Expand beyond coerced computer authentication
  - E.g. network scanner accounts?
- Data collection for other NTLM attacks/defenses.
- IAKERB kills NTLM?
- Check out Elad Shamir's in-depth post* for more details!
- We will be at RSA (booth 349)!



* https://specterops.io/blog/2025/04/08/the-renaissance-of-ntlm-relay-attacks-everything-you-need-to-know/

Thank you!

Questions?

BLOODHOUND
ENTERPRISE

BLOODHOUND

Lee Chagolla-Christensen | lee@specterops.io

Rohan Vazarkar | rvazarkar@specterops.io

Will Schroeder | wschroeder@specterops.io

Justin Kohler | jkohler@specterops.io