



Putting NTLM in the Doghouse

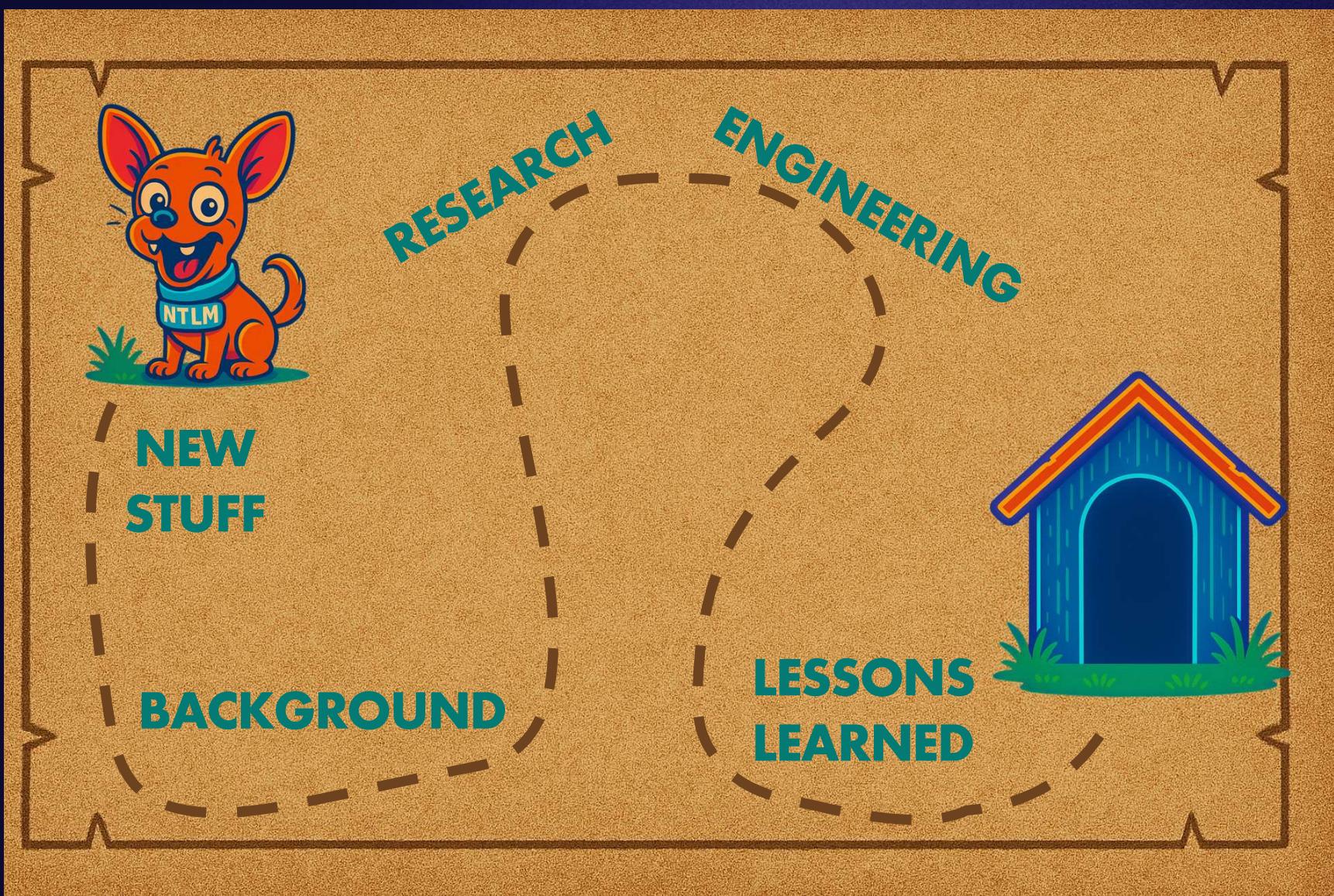
The journey of modeling NTLM
relay and authentication coercion
attacks in BloodHound

Lee Chagolla-Christensen & Rohan Vazarkar
SpecterOps



Introductions





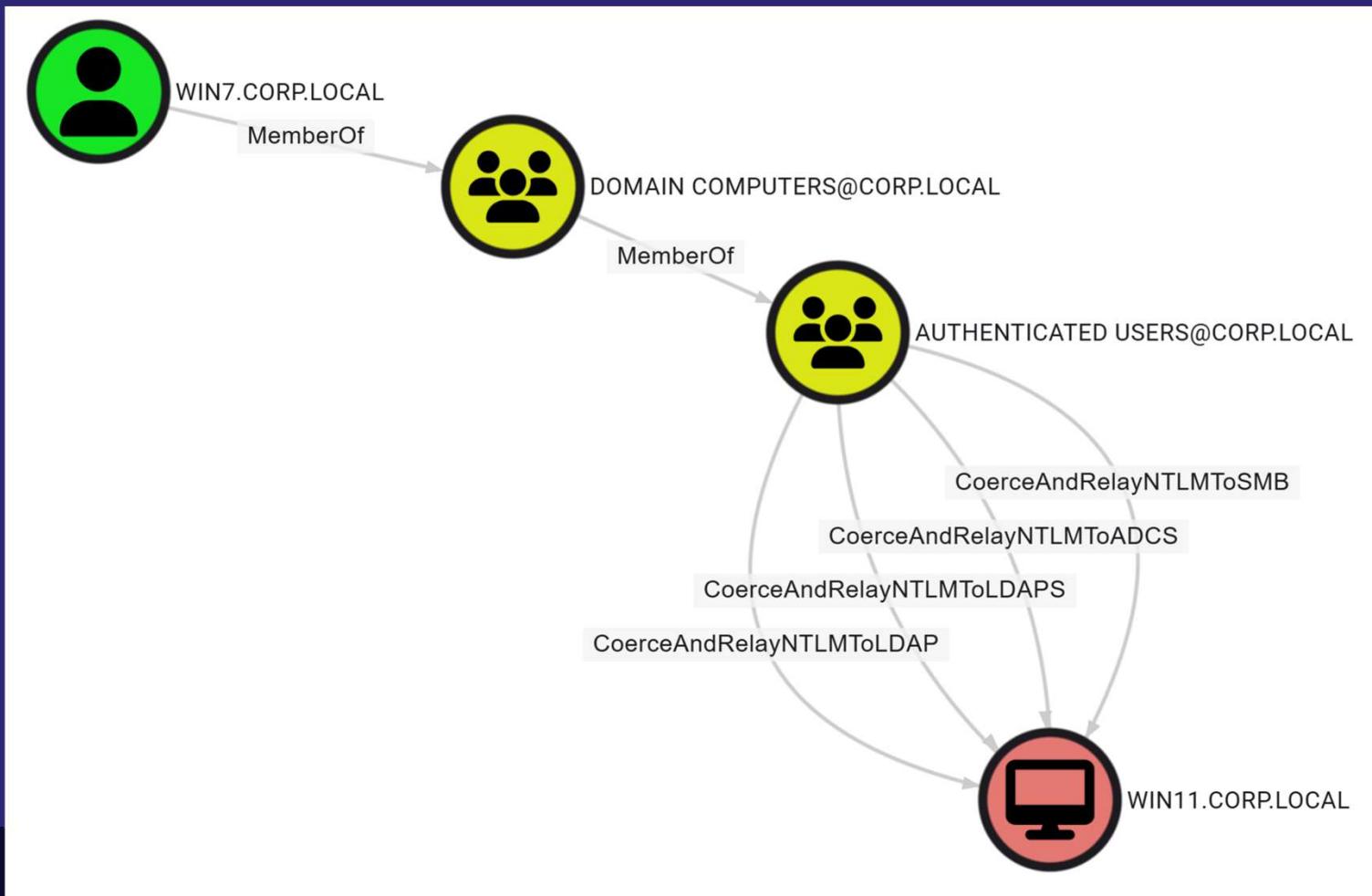
TLDR: 4 New BloodHound Edges

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, SPNTTargets, 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



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

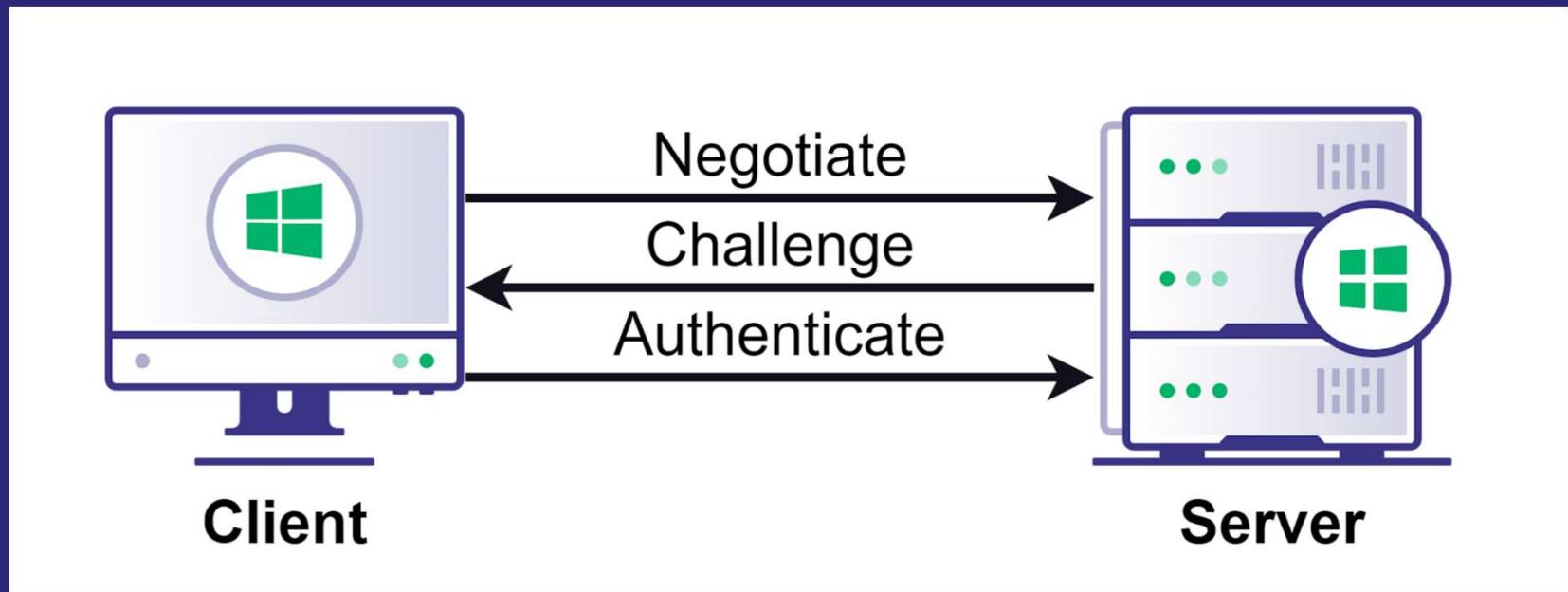


NTLM

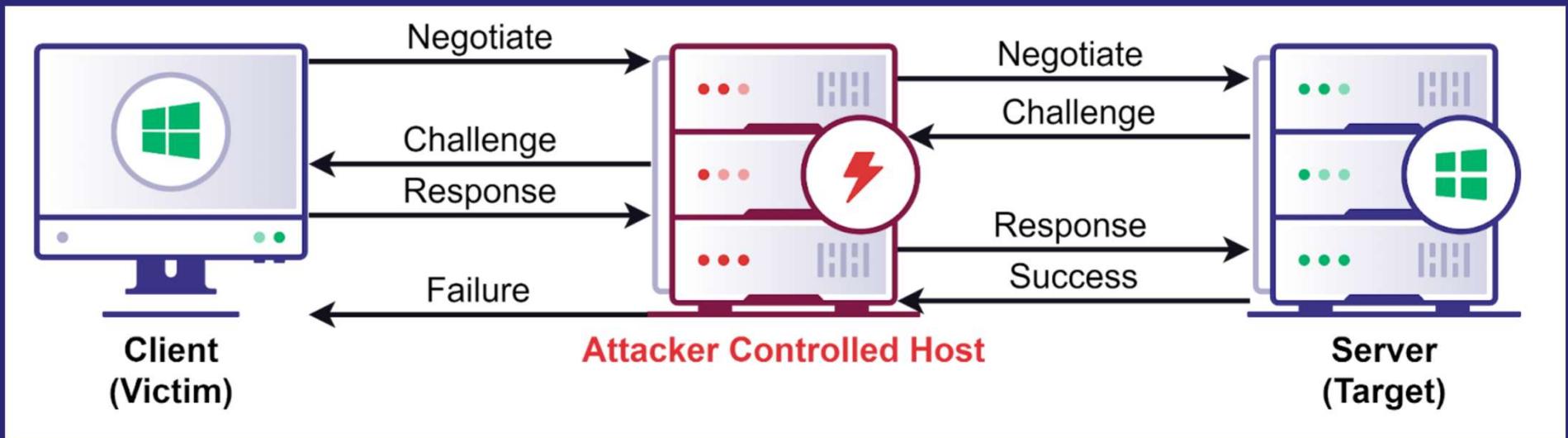
NTLMv1 is removed. LANMAN and NTLMv2 are no longer under active feature development and are deprecated. NTLMv2 will continue to work but will be removed from Windows Server in a future release. Replace calls to NTLM to calls to Negotiate, which try to authenticate with Kerberos and only fall back to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

NTLM Authentication Messages

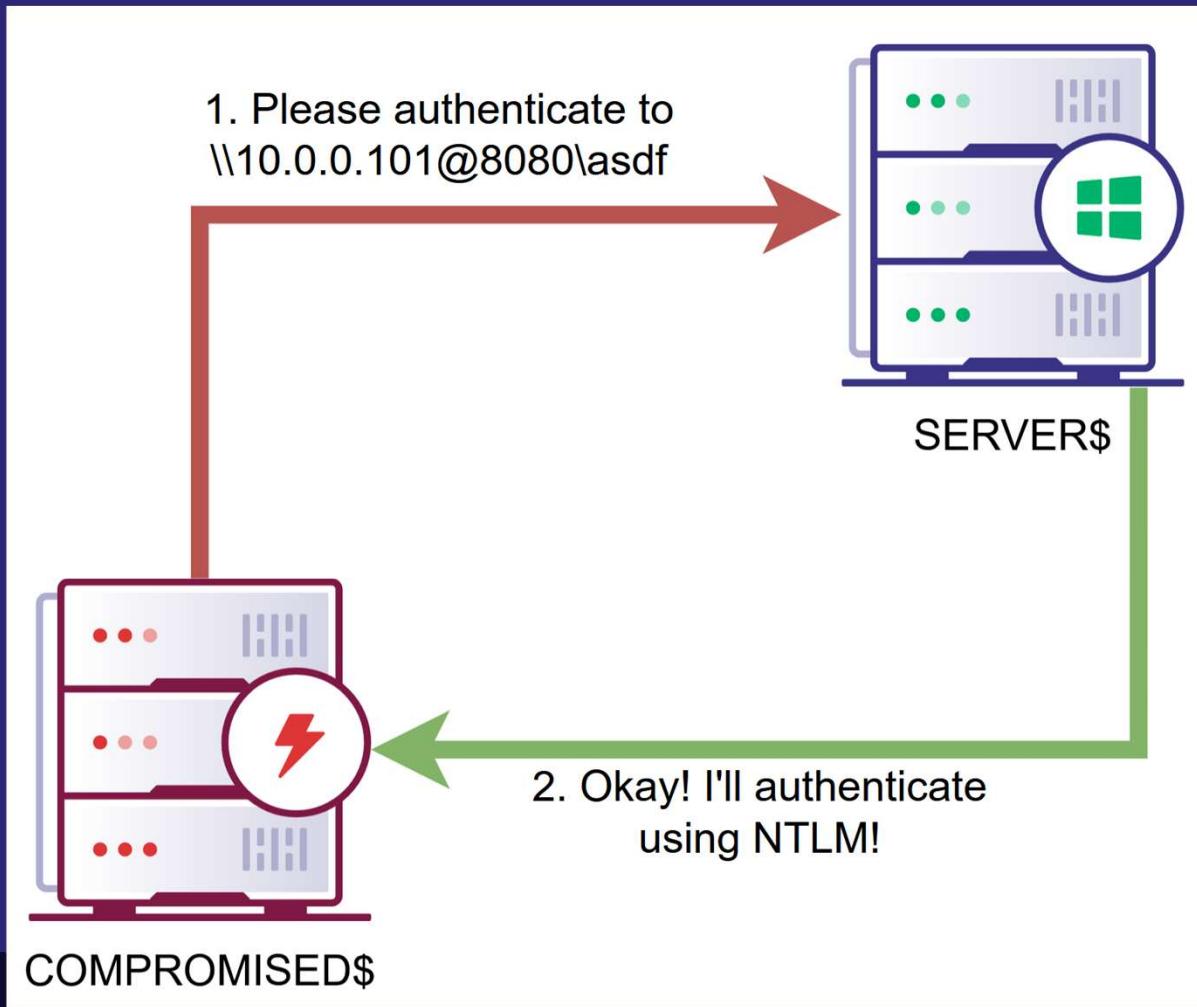
The basic, big idea



Edge Component 1: NTLM Relay



Edge Component 2: Coerced Computer Authentication

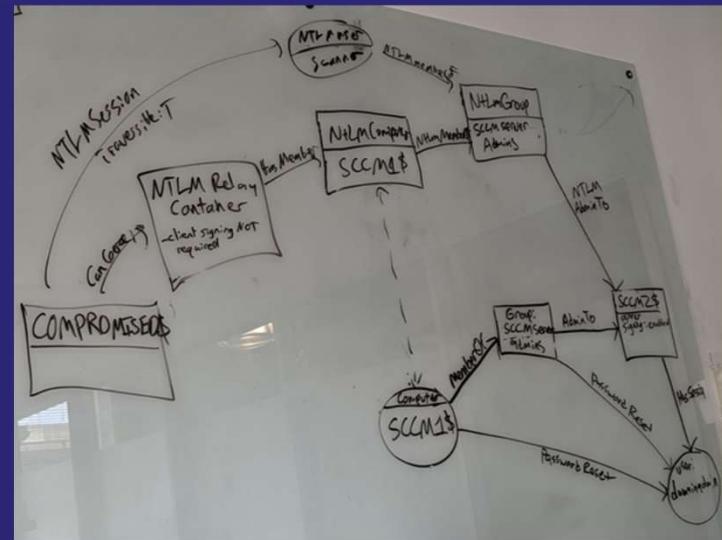
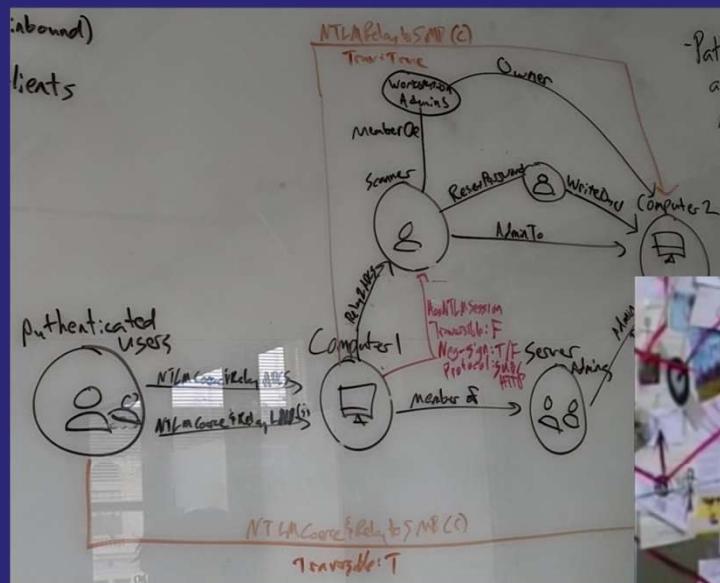


Examples:

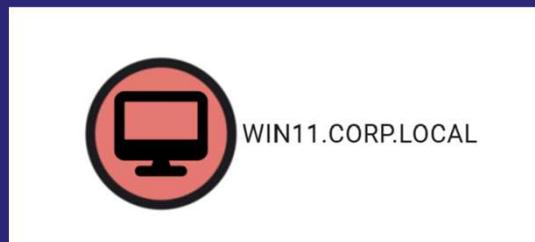
- SpoolSample
- PetitPotam
- Coercer

Early Relay Modeling

Lee, Will, and Elad



CoerceAndRelayNTLMToSMB

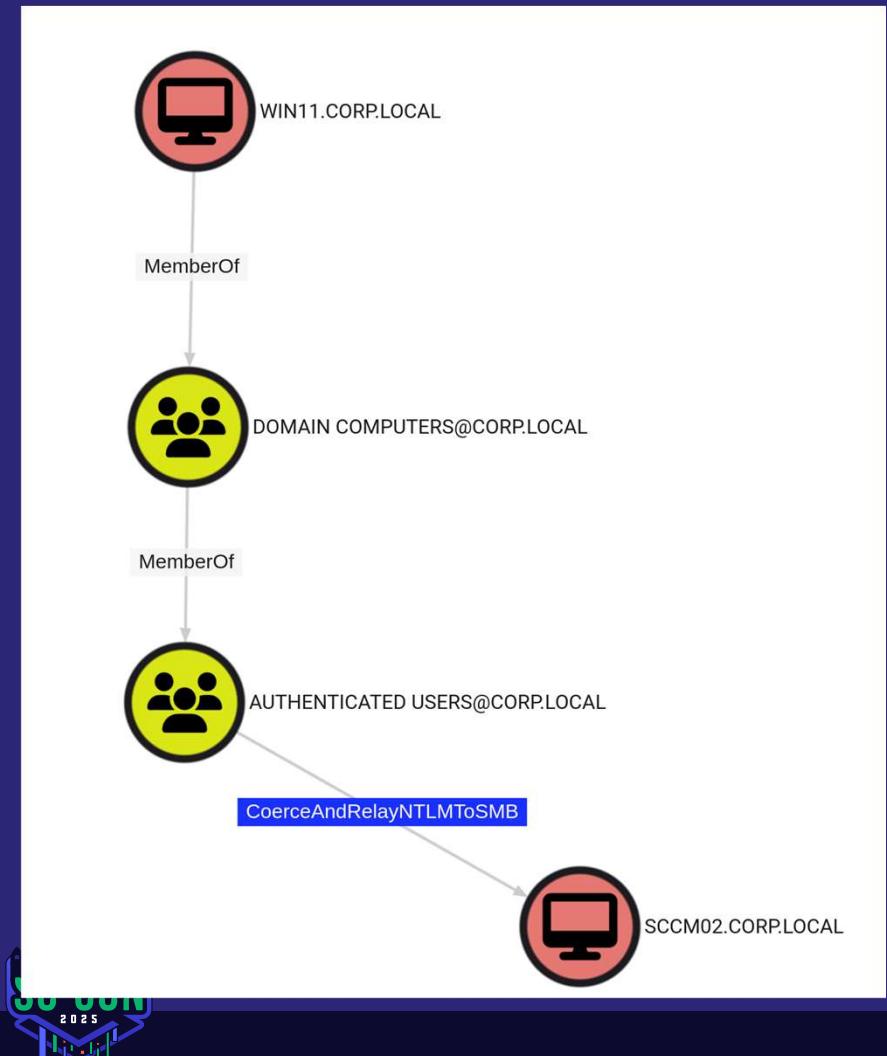


Setup:

- Attacker compromises WIN11
- SCCM01 has local admin to SCCM02



CoerceAndRelayNTLMToSMB



Coercion (Source) Target Requirements

- Outbound NTLM Allowed

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

Relay Target Requirements:

- SMB signing not required

– Coercion Targets

The nodes in this list are valid relay sources for this attack

 SCCM01.CORP.LOCAL

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_PROCESSING_REQUIRED
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

✓ NetBIOS Session Service

 Message Type: Session message (0x00)

 Length: 372

✓ SMB2 (Server Message Block Protocol version 2)

 > SMB2 Header

 ✓ Negotiate Protocol Response (0x00)

 [Preatuh Hash: 13c9d0484e564d13e83a8c91a2b292578fd11-7a20b08edc0f6d571c73b2017c1cdh277b45a0d0d5de7213278558dded]

 > StructureSize: 0x0041

 > Security mode: 0x01, Signing enabled

Note: it's enabled but NOT required!

0000 00 15 50
0010 01 a0 b3
0020 e6 65 01
0030 00 fe 62
0040 00 00 00
0050 00 00 01
0060 00 00 00
0070 00 00 00
0080 05 00 b8
0090 75 c4 af
00a0 80 00 3b
00b0 00 00 80
00c0 01 05 05
00d0 01 04 01
00e0 01 02 02
00f0 2a 86 48

16

CoerceAndRelayNTLMToADCS (ADCS ESC8)

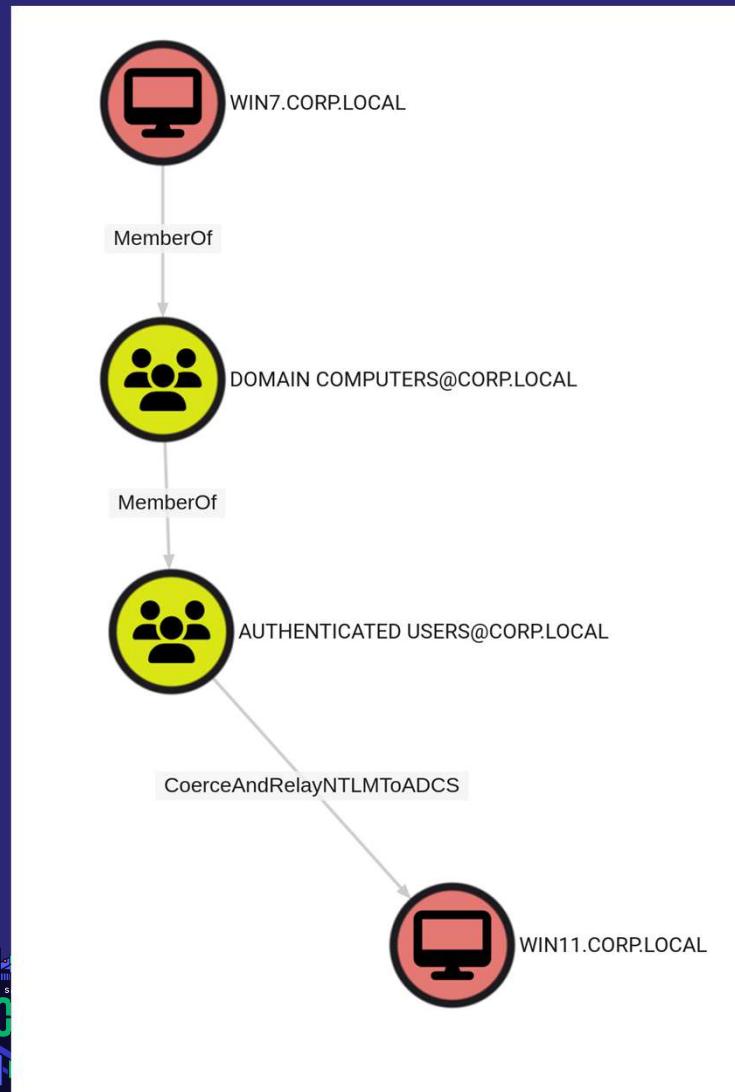


-	CA1@CORP.LOCAL	▲
Has Basic Constraints:	FALSE	
Has Enrollment Agent Restrictions:	FALSE	
Has Vulnerable Endpoint:	TRUE	
HTTP Enrollment Endpoints:	http://DC01.CORP.LOCAL/certsrv/	
HTTPS Enrollment Endpoints:	https://DC01.CORP.LOCAL/certsrv/	



Setup:

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



CoerceAndRelayNTLMToADCS (ADCS ESC8)

Coercion (Source) Target Requirement
- Outbound NTLM Allowed

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

Edge Composition

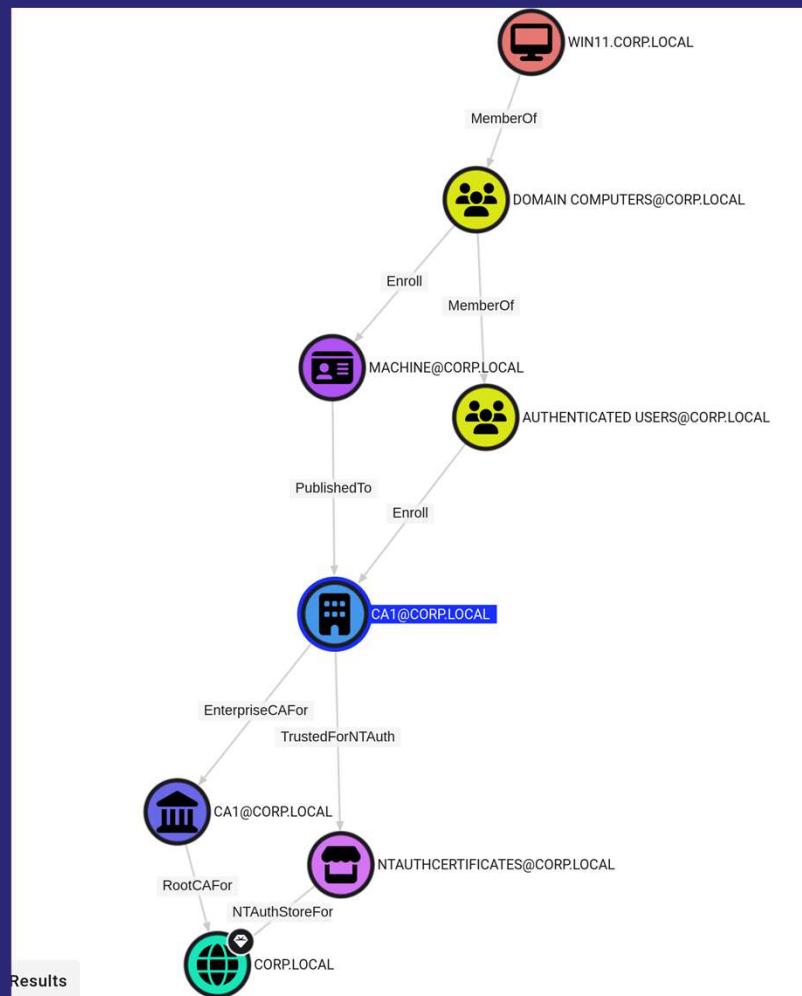
There's a lot going on there!

– 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.



Results

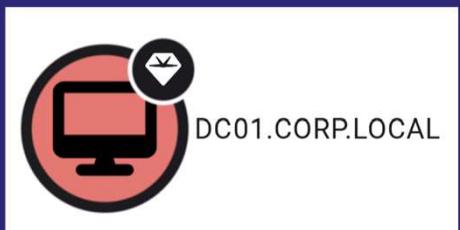
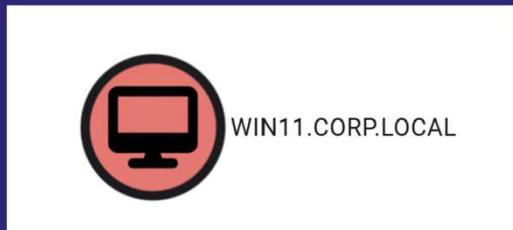


Mitigation: Removal or Extended Protection for Authentication(EPA) / Channel Binding?

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

```
▼ 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
  ▼ 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
```





– DC01.CORP.LOCAL	
LDAP Available:	TRUE
LDAP Signing:	FALSE
LDAPS Available:	TRUE
LDAPS EPA:	FALSE

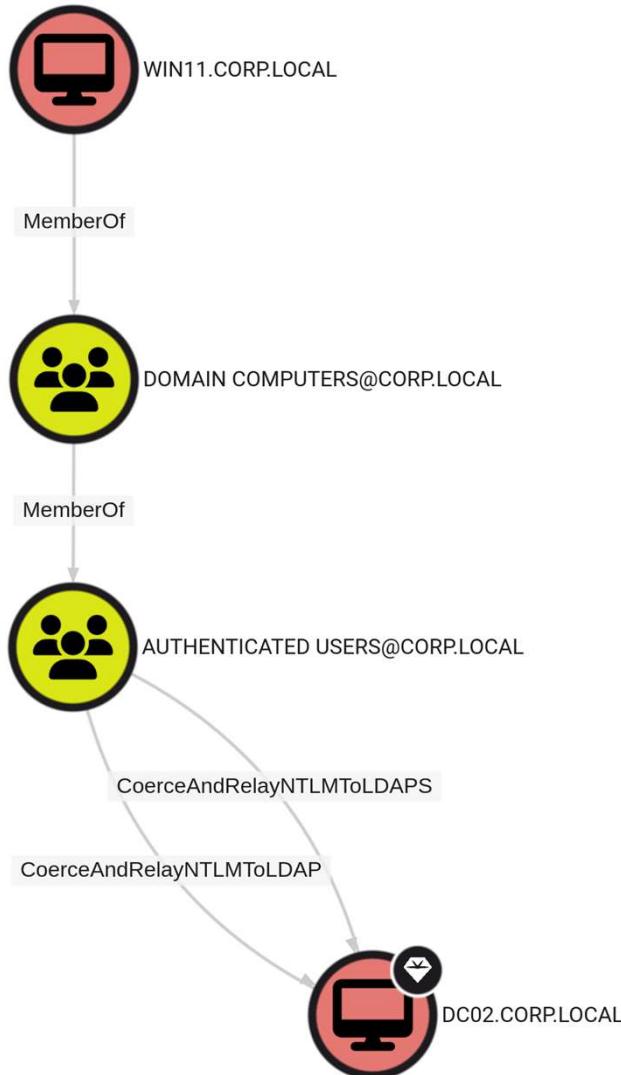
– DC02.CORP.LOCAL	
User Account Control:	532480
WebClient Running:	TRUE

CoerceAndRelayNTLMToLDAP(S)

Setup:

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





CoerceAndRelayNTLMToLDAP(S)

Coercion (Source) Target Requirements

- Outbound NTLM Allowed
- WebClient service running

Relay Target (LDAP) Requirements:

- 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, Negotiate 160, Negotiate 256, Negotiate 512, Negotiate 1024, Negotiate 2048, Negotiate 4096, Negotiate 8192, Negotiate 16384, Negotiate 32768, Negotiate 65536, Negotiate 131072, Negotiate 262144, Negotiate 524288, Negotiate 1048576, Negotiate 2097152, Negotiate 4194304, Negotiate 8388608, Negotiate 16777216, Negotiate 33554432, Negotiate 67108864, Negotiate 134217728, Negotiate 268435456, Negotiate 536870912, Negotiate 1073741824, Negotiate 2147483648, Negotiate 4294967296, Negotiate 8589934592, Negotiate 17179869184, Negotiate 34359738368, Negotiate 68719476736, Negotiate 137438953472, Negotiate 274877906944, Negotiate 549755813888, Negotiate 1099511627776, Negotiate 2199023255552, Negotiate 4398046511104, Negotiate 8796093022208, Negotiate 17592186044416, Negotiate 35184372088832, Negotiate 70368744177664, Negotiate 140737488355328, Negotiate 281474976710656, Negotiate 562949953421312, Negotiate 112589990684264, Negotiate 225179981368528, Negotiate 450359962737056, Negotiate 900719925474112, Negotiate 180143985094824, Negotiate 360287970189648, Negotiate 720575940379296, Negotiate 1441151880758592, Negotiate 2882303761517184, Negotiate 5764607523034368, Negotiate 11529215046068736, Negotiate 23058430092137472, Negotiate 46116860184274944, Negotiate 92233720368549888, Negotiate 18446744073709976, Negotiate 36893488147419952, Negotiate 73786976294839904, Negotiate 147573952589679808, Negotiate 295147905179359616, Negotiate 590295810358719232, Negotiate 1180591620717438464, Negotiate 2361183241434876928, Negotiate 4722366482869753856, Negotiate 9444732965739507712, Negotiate 18889465931479015424, Negotiate 37778931862958030848, Negotiate 75557863725916061696, Negotiate 151115727458232123392, Negotiate 302231454916464246784, Negotiate 604462909832928493568, Negotiate 1208925819665856987136, Negotiate 2417851639331713974272, Negotiate 4835703278663427948544, Negotiate 9671406557326855897088, Negotiate 19342813114653711794176, Negotiate 38685626229307423588352, Negotiate 77371252458614847176704, Negotiate 154742504917229694353408, Negotiate 309485009834459388706816, Negotiate 618970019668918777413632, Negotiate 1237940039337837554827264, Negotiate 2475880078675675109654528, Negotiate 4951760157351350219309056, Negotiate 9903520314702700438618112, Negotiate 19807040629405400877236224, Negotiate 39614081258810801754472448, Negotiate 79228162517621603508944896, Negotiate 158456325035243207017889792, Negotiate 316912650070486414035779584, Negotiate 633825300140972828071559168, Negotiate 1267650600281945656143118336, Negotiate 2535301200563891312286236672, Negotiate 5070602401127782624572473344, Negotiate 10141204802555565249144946688, Negotiate 20282409605111130498289893376, Negotiate 40564819210222260996579786752, Negotiate 81129638420444521993159573504, Negotiate 162259276840889043986319147008, Negotiate 324518553681778087972638294016, Negotiate 649037107363556175945276588032, Negotiate 1298074214727112351890553176064, Negotiate 2596148429454224703781106352128, Negotiate 5192296858908449407562212704256, Negotiate 10384593717816898815124425408512, Negotiate 20769187435633797630248850817024, Negotiate 41538374871267595260497701634048, Negotiate 83076749742535190520995403268096, Negotiate 166153499485070381041988806536192, Negotiate 332306998970140762083977613072384, Negotiate 664613997940281524167955226144768, Negotiate 1329227995880563048335910452285336, Negotiate 2658455991761126096671820904570672, Negotiate 5316911983522252193343641809141344, Negotiate 1063382396704450438668728361828268, Negotiate 2126764793408900877337456723656536, Negotiate 4253529586817801754674913447313072, Negotiate 8507059173635603509349826894626144, Negotiate 17014118347271207018697653789252288, Negotiate 34028236694542414037395307578504576, Negotiate 68056473389084828074785615157009152, Negotiate 136112946778169656149571230354018304, Negotiate 272225893556339312298542460708036608, Negotiate 544451787112678624597084921416073216, Negotiate 1088903574245357249194168842832146432, Negotiate 2177807148490714498388337685664292864, Negotiate 4355614296981428996776675371328585728, Negotiate 8711228593962857993553350742657171456, Negotiate 17422457187925715987106701485314342912, Negotiate 34844914375851431974213402970628685824, Negotiate 69689828751702863948426805941257371648, Negotiate 139379657503405727896854011882514743296, Negotiate 278759315006811455793708023765029486992, Negotiate 557518630013622911587416047530058973984, Negotiate 1115037260027245823174320950660117947968, Negotiate 2230074520054491646348641901320235895936, Negotiate 4460149040108983292697283802640471791872, Negotiate 8920298080217966585394567605280943583744, Negotiate 17840596160435933170789155210561887167488, Negotiate 35681192320871866341578310421123774334976, Negotiate 71362384641743732683156620842247548679952, Negotiate 14272476928348746536631324168449497759904, Negotiate 28544953856697493073262648336898995519808, Negotiate 57089907713394986146525296673797991039616, Negotiate 114179815426789972293055933447595982178232, Negotiate 228359630853579944586111866895191964356464, Negotiate 456719261707159889172223733790383928712928, Negotiate 913438523414319778344447467580767857255856, Negotiate 1826877046828639556688895335161535714511712, Negotiate 3653754093657279113377790670323071428523424, Negotiate 7307508187314558226755581340646142850446848, Negotiate 1461501637462911645351176268129284570089696, Negotiate 2923003274925823290702352536258568540179392, Negotiate 584600654985164658140470507251713708035884, Negotiate 1169201309770329316280941014503427416071768, Negotiate 2338402619540658632561882029006854832143536, Negotiate 4676805239081317265123764058013709664287072, Negotiate 9353610478162634530247528116027419328574144, Negotiate 1870722095632526906049515623205423865748288, Negotiate 3741444191265053812098731246410847734966576, Negotiate 7482888382530107624197462492821695469933152, Negotiate 1496577676506021524394934495614390939866304, Negotiate 2993155353012043048789868991228781879732608, Negotiate 5986310706024086097579737982457563759465216, Negotiate 1197262141204817215115945596491512718893032, Negotiate 2394524282409634430231891192983025437786064, Negotiate 4789048564819268860463782385966050875572128, Negotiate 9578097129638537720927564771932101751144256, Negotiate 19156194259277075441855329543862203502285112, Negotiate 38312388518554150883710659087724407004570224, Negotiate 7662477703707830176742131817544881400904448, Negotiate 15324955407415660353484263635089762801808996, Negotiate 30649910814831320706968527270179525603617992, Negotiate 61299821629662641413937054540359051207235884, Negotiate 122599643259325282827874109080718102414477768, Negotiate 245199286518650565655748218161436204828955536, Negotiate 490398573037301131311496436322872409657911072, Negotiate 980797146074602262622992872645744819315821544, Negotiate 1961594292149204525245985745294889638631642888, Negotiate 3923188584298409050491971490589779277263285776, Negotiate 7846377168596818100983942981179558554526575552, Negotiate 1569275433719363620196884596235911709855351104, Negotiate 3138550867438727240393769192471823419710702088, Negotiate 6277101734877454480787538384943646839421404176, Negotiate 12554203469754908961575176769887293678842808352, Negotiate 25108406939509817923150353539774587357685616704, Negotiate 50216813879019635846300707079549174715371233408, Negotiate 100433627588039271692601414159098349430742466816, Negotiate 200867255176078543385202828318196698861484933632, Negotiate 401734510352157086770405656636393397723417867264, Negotiate 803469020704314173540811313272786795446835734528, Negotiate 160693804140862834708162662654557359089367147056, Negotiate 321387608281725669416325325309114718178734294112, Negotiate 642775216563451338832650650618228363577468588224, Negotiate 128555043312690267766530130123645672715493717648, Negotiate 257110086625380535533060260247291344290987435296, Negotiate 514220173250761071066120520494582688581974770592, Negotiate 102844034651532214213224040898916537716394941184, Negotiate 205688069303064428426448081797833075432789882368, Negotiate 411376138606128856852896163595666150865579764736, Negotiate 822752277212257713705792327181332301731159529472, Negotiate 1645504554424515427411584654362664603462319058944, Negotiate 3291009108849030854823169308725329206924638117888, Negotiate 6582018217698061709646338617450658413849276235776, Negotiate 1316403643539612341929267723490131682769853251552, Negotiate 2632807287079224683858535446980263365539706503104, Negotiate 5265614574158449367717070893960526731079413006208, Negotiate 10531229148316897335434141787921053462158260012416, Negotiate 21062458296633794670868283575842106924316520024832, Negotiate 42124916593267589341736567151684213848633040049664, Negotiate 84249833186535178683473134303368427692666080099328, Negotiate 168499666373070357366946686606736855385332160198656, Negotiate 336999332746140714733893373213473710770664320397312, Negotiate 673998665492281429467786746426947421541328640794624, Negotiate 1347997330984562858935574932853894843082657281589248, Negotiate 2695994661969125717871149865707789686165314563178496, Negotiate 5391989323938251435742299731415579372330629126358992, Negotiate 1078397864767650287448599466283115864661258251317896, Negotiate 2156795729535300574897198932566231729322516502635792, Negotiate 4313591459070601149794397865132463458645033005275584, Negotiate 8627182918141202299588795730264926917290066010551168, Negotiate 17254365836282404598575911460529853834801332021102336, Negotiate 34508731672564809197151822921059707669602664042204672, Negotiate 69017463345129618394303645842119415339205328084409344, Negotiate 13803492669025923678860731168423883067841065616811888, Negotiate 27606985338051847357721462336847766135682131233623776, Negotiate 55213970676103694715442924673695332273664262467247552, Negotiate 11042794135206738923085849344738766454732852934495504, Negotiate 22085588270413477846171698689477532909457705868991008, Negotiate 44171176540826955692343397378955065818915411737982016, Negotiate 88342353081653911384686794757890131637830823475964032, Negotiate 17668470616326782276937398951578026327661646691928064, Negotiate 35336941232653564553874797903156052655323293383856128, Negotiate 70673882465307129107749595806312105310646586767712256, Negotiate 141347764930614258215491911612622026603131734135424512, Negotiate 28269552986122851643098382322524405320626346827084904, Negotiate 56539105972245703286196764645048810641252683654169808, Negotiate 11307821194489406657239332930097762128251336730833816, Negotiate 22615642388978813314478665860195524256502673461667632, Negotiate 45231284777957626628957331720391048513005346923335264, Negotiate 9046256955591525325791466344078209602600569384667056, Negotiate 18092513911183050651582932688156419205201138773334112, Negotiate 36185027822366101303165865376312838404022775546674224, Negotiate 7237005564473220260633173075262567680804551109338848, Negotiate 14474011128946404521266860150525335361611102218677696, Negotiate 28948022257892809042533720301050670723222204437355392, Negotiate 57896044515785618085067440602101341446444408874710784, Negotiate 11579208903571323617013488120420268289288817754851156, Negotiate 23158417807142647234026976240840536577777635509702312, Negotiate 46316835614285294468053952481681071555555271019404624, Negotiate 9263367122857058893610790496336214311111054203880928, Negotiate 18526734245714117787221580992672428622222108407761856, Negotiate 37053468491428235574443161985344857244444416815523712, Negotiate 74106936982856471148886323970689114888888236631047424, Negotiate 14821387396571294229773264794137822977777747326209488, Negotiate 29642774793142588459546529588275645955555594652418976, Negotiate 59285549586285176919093059176551291915555599304837952, Negotiate 11857109917257035383818611835310258383111119860967592, Negotiate 23714219834514070767637223670620518766311119721935184, Negotiate 4742843966902814153527444734124103753266223943940368, Negotiate 9485687933805628307054889468248207506533338887880736, Negotiate 18971375867611256614109778964496015013066677755761472, Negotiate 37942751735222513228219557928992030026133375511522944, Negotiate 7588550347044502645643911585798406005206675102304588, Negotiate 15177100694089045291278223715968012010133510504609176, Negotiate 30354201388178090582556447431936024020267020092418352, Negotiate 60708402776356181165112895463872048040413401848366704, Negotiate 12141680555271236233022579092754096080826803696673408, Negotiate 24283361110542472466045158185508192161653607393347216, Negotiate 48566722221084944932090316371016383843267214786674432, Negotiate 97133444442169889864180632742032767686534401573488864, Negotiate 19426688884433977972836126484065535341513483114697728, Negotiate 38853377768867955945672252968131070683068802283395456, Negotiate 77706755537735911891344505936262141366137604566789912, Negotiate 15541351107547923582688901187252428333275209013359824, Negotiate 31082702215095847165377802374504856666550418026719648, Negotiate 62165404430191694330755604749009713333100804053439296, Negotiate 12433080860383338867151209499819426666201608010687892, Negotiate 24866161720766677734302418998388453333203216021375784, Negotiate 49732323441533355468604837996776906666406416042751568, Negotiate 99464646883066710937209675993553813333412832085503136, Negotiate 198929293766133421874019351
```

Engineering

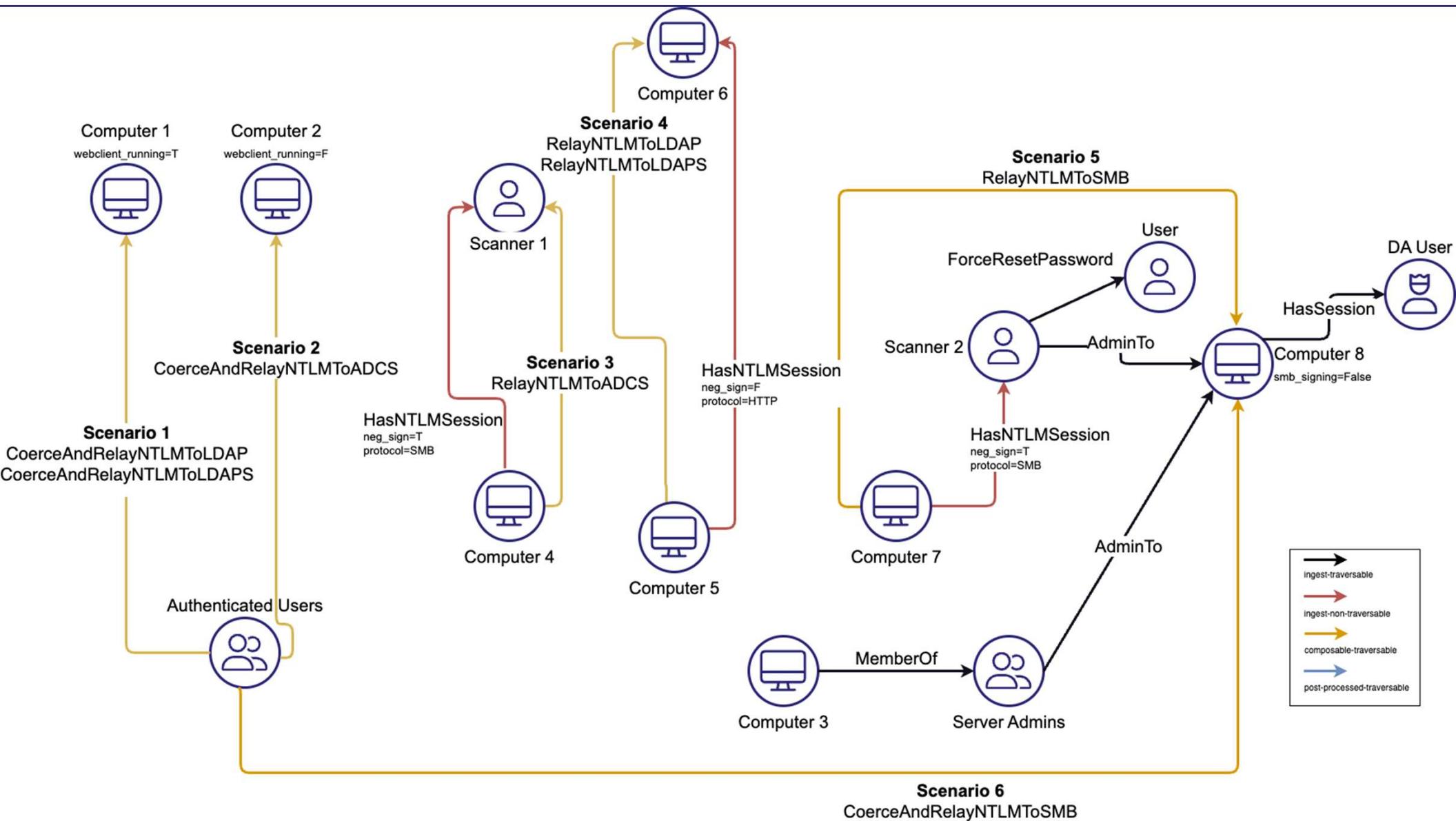
The boring part of the talk



Engineering Handoff Process

- Research provided documentation on all the new edges in a private github repo.
- Each attack primitive was provided with all the information needed for each edge's info panels
- Rough post processing guidelines were created to show the ideal workflow and test harnesses were created using arrows.app to allow us to model expected behavior for positive cases





Engineering Process

- Always have a Jonas on your team
 - Did rough translation between expectations and actual code.
 - Ended up doing 50% of the translation work for us.
- Decomposed work into JIRA tickets and linked them all into a big initiative.
- Did estimations on time taken
 - (which were as per usual wildly off)
- Assigned an engineering team to go to work (including yours truly)



Engineering Process

- Deployed our first release with NTLM information in early access a few weeks ago.
- Saw immediate jumps in exposure across many environments (more work!)
- Identified bugs from our early adopters and worked on triaging them rapidly. Final NTLM release will likely be next week barring any other bugs being found!



Triumphs!

Making a note here, huge success



Greatly improved handoff process

- Our previous research to engineering handoff was ADCS, which ended up being a big of a disaster internally (for many, many reasons).
- ADCS Post Processing was a "from-scratch" which blew out our timeline significantly. NTLM got to leverage a lot of that hard work from before
- Learned tons of stuff from that process and implemented lessons learned.
- This process was significantly smoother than our previous effort, which shows great progress



Proving out complex non-standard primitives

- NTLM coercion is different from any of our other attack primitives in that its directionality is different
- Any user can perform NTLM relay, so how do we model this appropriately?
- Research team came up with a clever idea to tie this to authenticated users, allowing us to model within the confines of our graph and reflect the severity of these issues appropriately

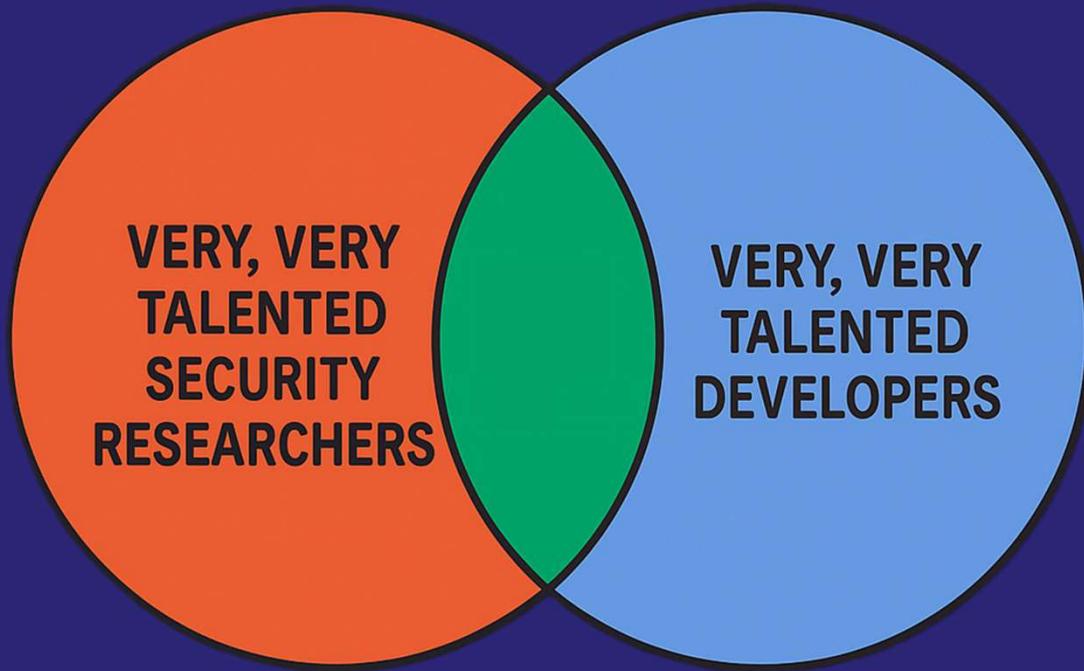


Lessons Learned

Oh man...so many



Engineers are not researchers (and vice versa)



- Understanding AD primitives is hard as a domain expert.
 - It's impossible as an engineer with no background



Engineers are not researchers and vice versa

- Many of the post processing primitives were sufficiently complicated that without extremely specific instructions (handholding) it was difficult for engineers to produce a working example
- LDAP vs LDAPS – Engineers think this is plural LDAP. We know differently
- Nuances around how AD behaves complicates the problem (Protected Users, Restrict Outbound NTLM)



The more time that passes, the harder it gets

Research and development are not carried out in tandem

- Result: when engineering was happening, the researchers involved were no longer fresh on the research and were working on other things
- Created a delay for interfacing with research due to assessment priorities

Lessons Learned

- Minimize time of research to time of engineering,
- Have a researcher available for testing near end of engineering



Communication about specifics

- During review, engineering determined based on naming that a file was part of a third-party dependency, and so vendored it (referenced a specific commit, changed the file to the original version with minimal modifications)
 - Accidentally removed a very subtle but important modification.
- Resulted in Lee spending 3+ days tracking down something that was extremely basic

Lesson Learned: Communicate changes



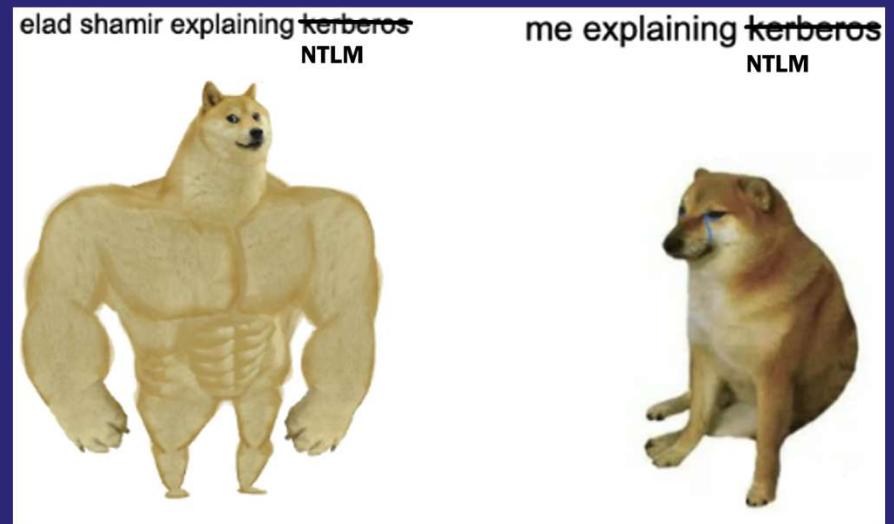
Test Data

- Good and comprehensive test data
 - Covers both positive AND negative test cases for each primitive.
 - Test data needs to be representative of a real environment,
 - Not a simple harness that illustrates the issue
- Test data needs to cover edge cases properly, so we accurately simulate real environments
- End to end testing is important! Harnesses are prone to human error during generation or fixing things that are not reflective of what the collector is actually sending over
- Thank you early access users!



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?
- Keep an eye out for Elad Shamir's upcoming post!





Thank you!

Any Questions?



Lee Chagolla-Christensen | lee@specterops.io

Rohan Vazarkar | rvazarkar@specterops.io