Broken Mirrors Shatter the Soul

Deep Dive into Kerberos Reflection Attacks and the SPN/DNS Phenomena

DFIRDeferred

2026

About the Speaker

WHOAMI

Darryl G. Baker

Senior Staff Security Researcher, Netwrix

Creator of Active Directory Hacking Village

Identity Security Instructor

Ham Radio Extra

Social

Twitter

@dfirdeferred

Github

@dfirdeferred

Linkedin

dbaker-cissp-ceh

Focuses

Authentication Protocols

Active Directory/ Entra ID security

Identity Security

Wireless Protocols

Agenda

Act 1: "The Setup"

Kerberos fundamentals, what reflection means

Act 2: "Band-Aid Surgery"

CVE-2025-33073, CVE-2025-58726, and the patch pattern

Act 3: "The Door Nobody Checked"

LDAP reflection, evidence, undocumented behavior

Act 4: "Monday Morning"

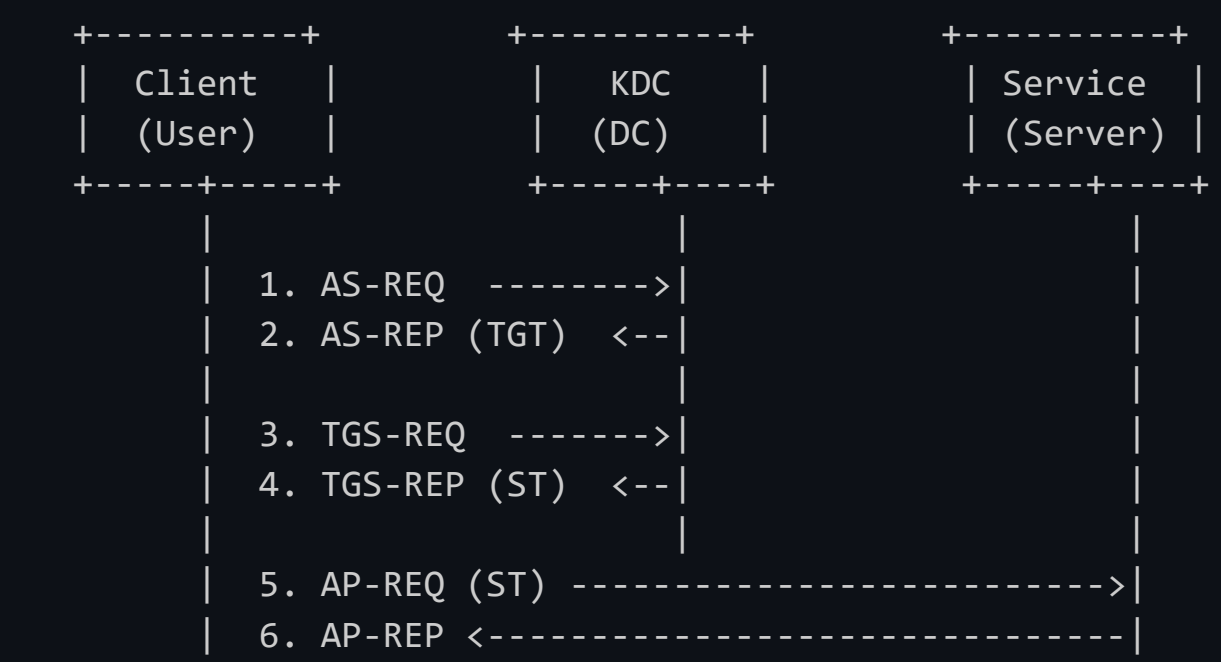
Detection, defense, the real fix

In 2008, Microsoft patched NTLM reflection.

MS08-068. The attack was simple: coerce a machine to authenticate to itself, replay the credential.

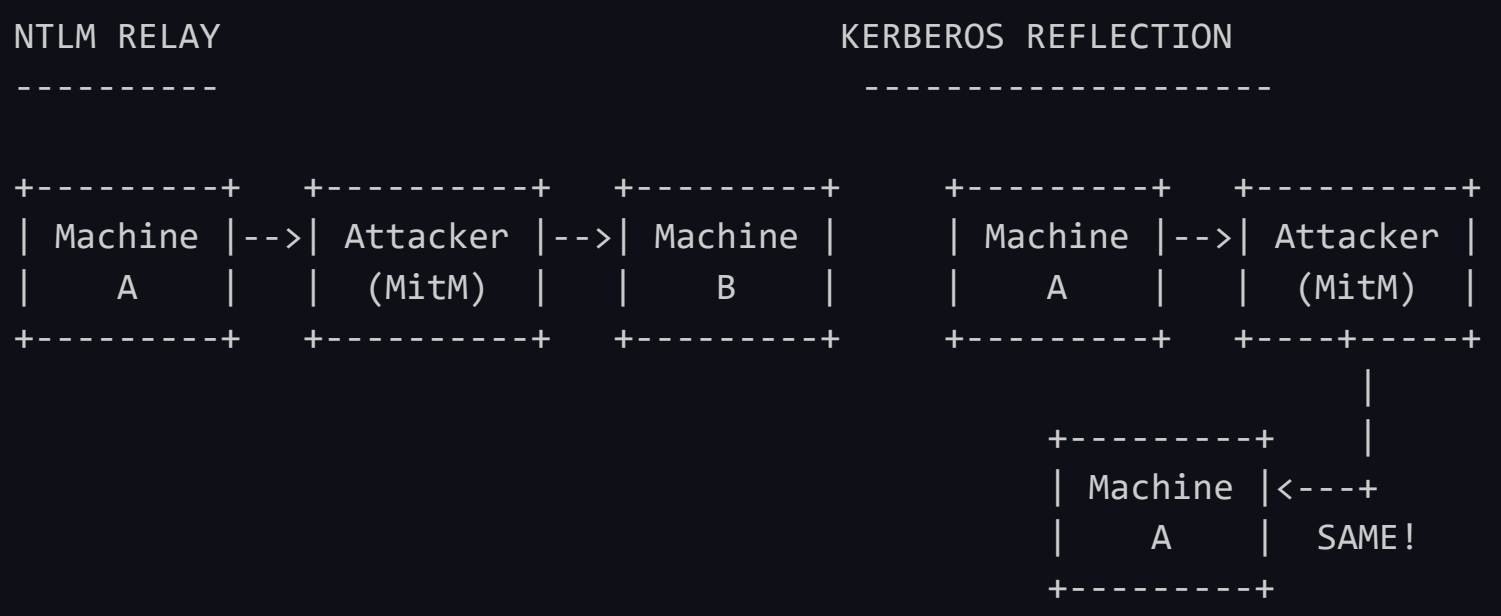
In 2025, the same type of attack works with Kerberos.

Kerberos 101: The Three-Party Dance



Key: TGT = Ticket-Granting Ticket | ST encrypted with service's key
The client CANNOT read the service ticket -- it's opaque

What Is Reflection? (vs. Relay)



Target:	DIFFERENT machine	Target: SAME machine
Privilege:	Victim user's creds	Privilege: SYSTEM (machine acct)
Defense:	MS08-068 (protocol fix)	Defense: SMB-specific only

Why Was Reflection Thought Impossible?

"For years, the assumption was: a service recognizes its own tickets"

RFC 4120, Section 3.2.3 lists 11 verification steps
for accepting a service ticket

NONE of them say: 'check if the ticket came from yourself'

The RFC never forbids reflection. It just doesn't address it.

Windows services trust one thing:
"If I can decrypt it, it's valid."

The Key Insight: One Key, Many Doors

The Building Analogy

A building has one master key

That key opens the front door,
loading dock, fire exit, elevator

The key is the same regardless
of which door you enter

The lock doesn't know which
door you came through

In Kerberos

Machine account (KERBDC$) has
one password hash

Decrypts tickets for:
cifs/KERBDC
ldap/KERBDC
http/KERBDC
host/KERBDC

A cifs/ ticket works on ldap/
because: same key

Reflection Visualized

The Coercion Toolbox

MS-EFSRPC (PetitPotam)

EfsRpcOpenFileRaw

SMB callback to attacker

Any authenticated user

Most widely used

MS-RPRN (PrinterBug)

RpcRemoteFindFirstPrinter...

Callback to attacker

Requires Spooler service

Classic, well-known

MS-DFSNM (DFSCoerce)

NetrDfsAddStdRoot

SMB callback to attacker

Requires DFS Namespace

Less commonly patched

All require only: Authenticated Users privilege (default)

ACT 2

Band-Aid Surgery

Two CVEs, Two Patches, Same Fundamental Problem

CVE-2025-33073: LoopyTicket

METADATA

CVE-2025-33073

RedTeam Pentesting (Jan 2025)

Synacktiv root cause (Mar 2025)

Patched June 2025

Component: mrxsmb.dll

Impact: SYSTEM on any target

CVSS: 8.8 (High)

IMPACT

Any auth user -> SYSTEM

Works without SMB signing

Proven on SRV01

via RemoteRegistry

Multiple independent discoverers:

RedTeam Pentesting

Cameron Stish (GuidePoint)

Synacktiv

CMTI: The SPN Decoupling Trick

The Magic Hostname

The Magic Hostname (existing server name + CMTI):

SRV01[CMTI-BLOB].lab.local

SRV011UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA.lab.local

DNS resolves to attacker IP

SPN constructed as: cifs/KERB-SRV01

Two paths, one hostname:

- DNS -> full string -> attacker
- SPN -> prefix only -> victim

How It Works

How It Works:

CredUnmarshalTargetInfo()
in mrxsmb.dll

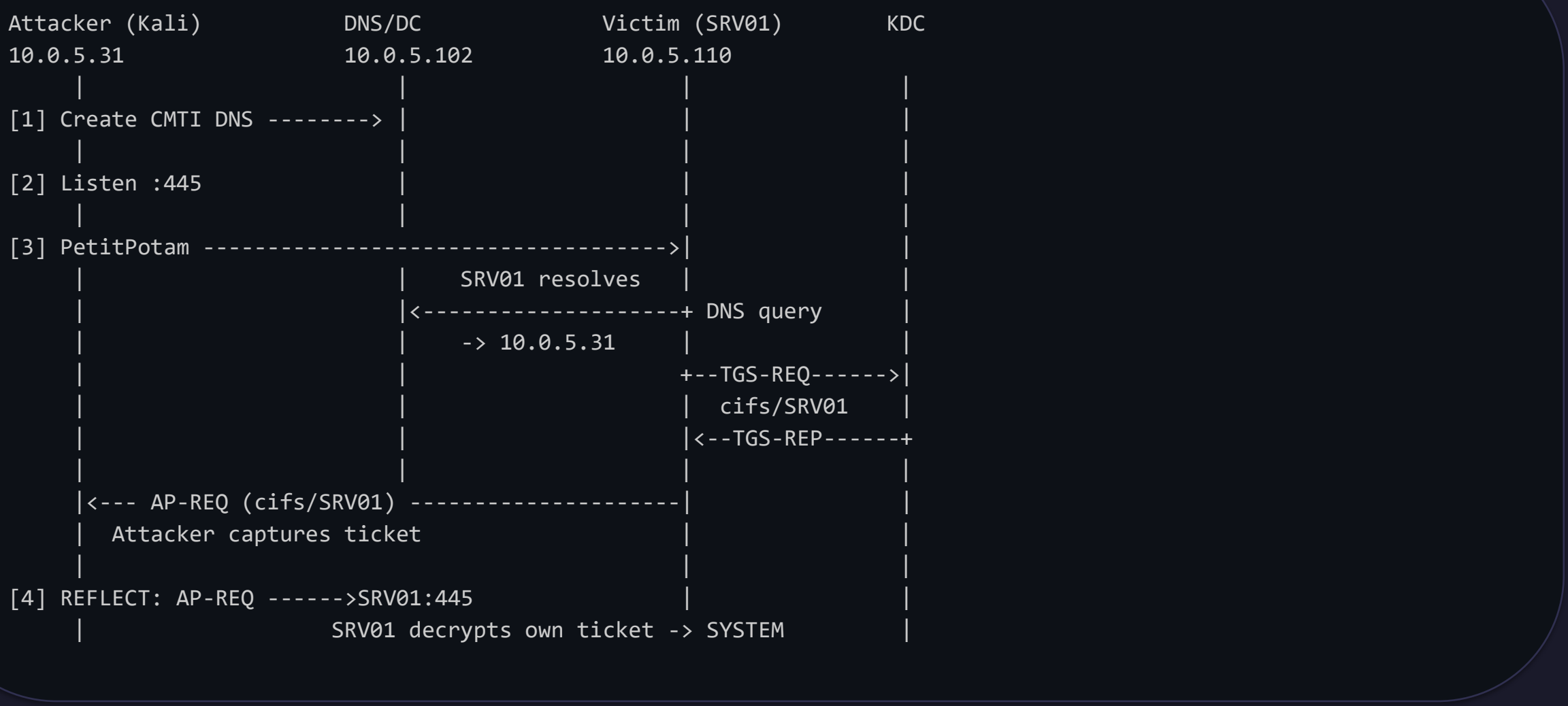
Detects base64 blob:
CREDENTIAL_TARGET_INFORMATIONW

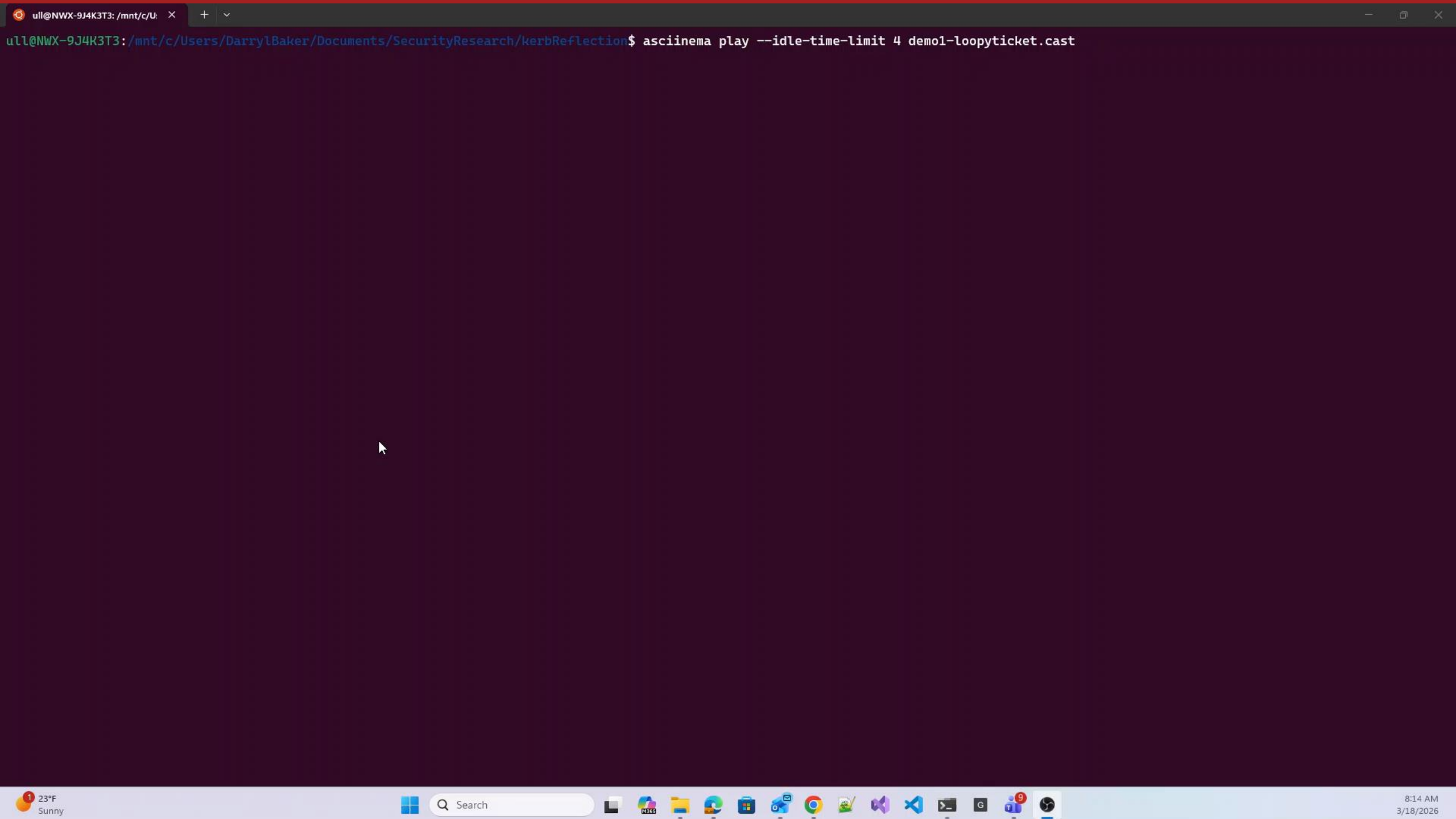
Strips blob -> uses PREFIX for SPN

Uses FULL hostname for DNS

Result: DNS -> attacker,
ticket -> victim's own service

LoopyTicket Attack Flow




ull@NWX-9J4K3T3: /mnt/c/U
ull@NWX-9J4K3T3:/mnt/c/Users/DarrylBaker/Documents/SecurityResearch/kerbReflection$ asciinema play --idle-time-limit 4 demo1-loopyticket.cast
23°F
Sunny
Search
8:14 AM
3/18/2026

What Microsoft Fixed (June 2025)

```
Component: mrxsmb.dll (SMB client driver)
Function:  SmbCeCreateSrvCall

if (CredUnmarshalTargetInfo(hostname)
        == SUCCESS) {
    // CMTI blob detected
    // Abort connection
    return STATUS_INVALID_PARAMETER;
}

// Proceed with normal SMB
// connection...
```

Patch scope:

SMB client ONLY

Does not affect:

- LDAP
- HTTP
- RPC
- Any other service

CMTI blob in hostname?

-> Connection killed

No CMTI blob?

-> No protection

Problem Solved.

One month later, Andrea Pierini of Semperis published a bypass.

No CMTI blob required.

CVE-2025-58726: Ghost SPNs

WHAT IS A GHOST SPN?

What is a Ghost SPN?

SPN registered on machine for
hostname it doesn't own

Common sources:
- Decommissioned servers
- Hostname changes
- Migration leftovers

Example: KERB-SRV02$ has
HOST/deadhost.lab.local

"Every AD environment has them."
"Most admins don't know."

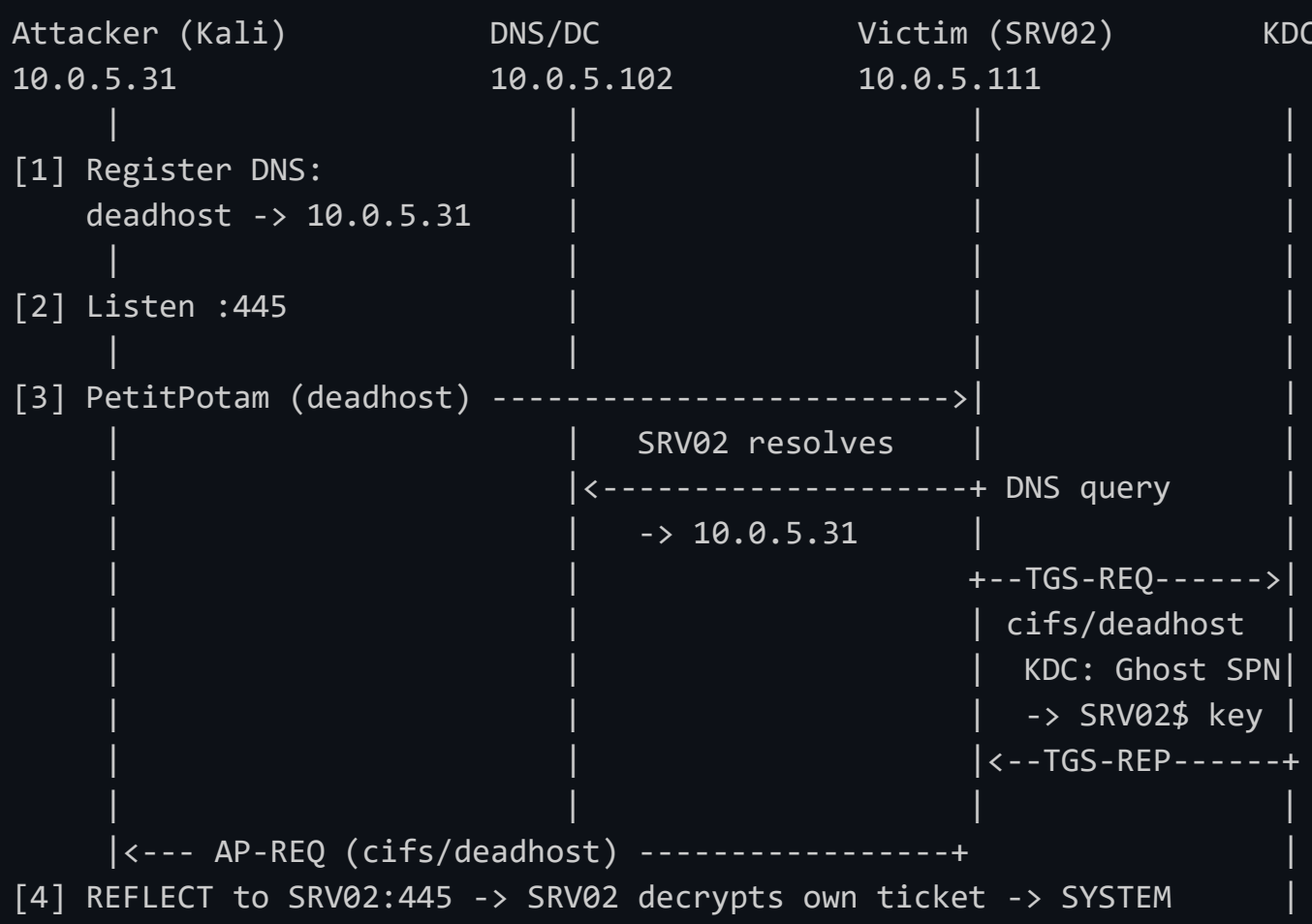
THE ATTACK

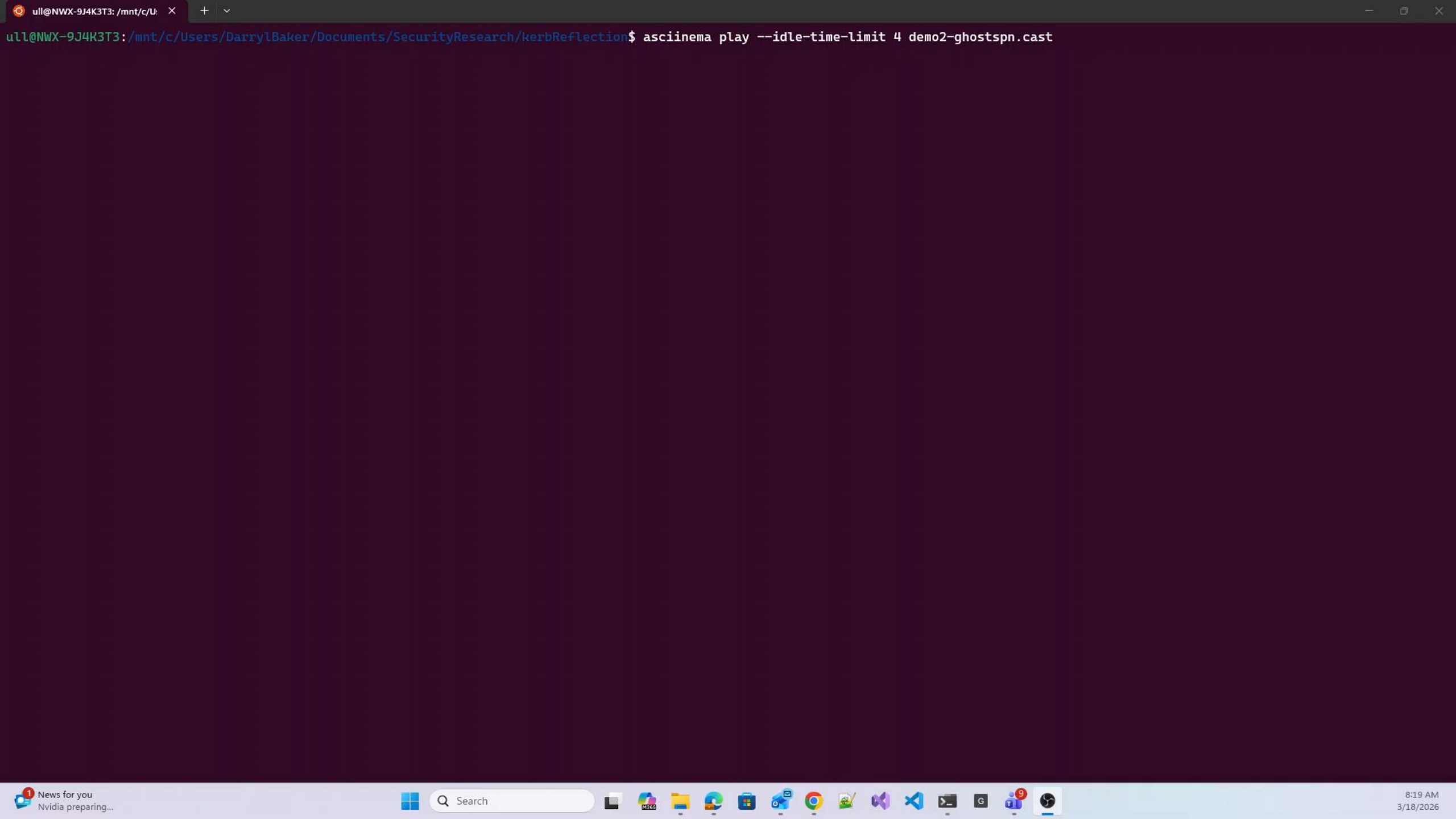
The Attack:

1. Register DNS: deadhost -> attacker
2. Coerce victim to connect
3. KDC maps cifs/deadhost
   -> HOST/deadhost
   -> KERB-SRV02$
4. Ticket encrypted with SRV02 key
   sent to attacker
5. Reflect back -> SYSTEM

No CMTI blob.
June patch irrelevant.

Ghost SPN Attack Flow




ull@NWX-9J4K3T3: /mnt/c/U
ull@NWX-9J4K3T3:/mnt/c/Users/DarrylBaker/Documents/SecurityResearch/kerbReflection$ asciinema play --idle-time-limit 4 demo2-ghostspn.cast
News for you
Nvidia preparing...
Search
8:19 AM
3/18/2026

What Microsoft Fixed (October 2025)

```
Component: srv2.sys (SMB server driver)
Functions: SrvAdminValidateSpn_Old()
           Smb2ValidateLoopbackAddress()

if (SPN_matches_local_machine(ticket)
    && source_is_not_loopback(addr)) {

    return SEC_E_LOGON_DENIED;
        // 0x8009030E
}

// SPN not local OR source is
// loopback -> allow
```

Patch scope:

SMB server ONLY

Does not affect:

- LDAP server
- HTTP server
- RPC endpoints

Logic:

Is SPN mine? AND

Is source remote?

-> REJECT

Feature-flagged for gradual rollout.

The Three-Layer Model (All SMB-Specific)

Layer 1: mrxsmb.dll (Client)

CMTI detection

Blocks outbound CMTI connections

SEC_E_INVALID_TOKEN (0x80090308)

SMB client only

Layer 2: srv2.sys (Server)

SPN validation + loopback check

Blocks inbound reflection

SEC_E_LOGON_DENIED (0x8009030E)

SMB server only

Layer 3: Kerberos SSPI

Self-referral detection (undocumented)

DC refuses own TGS via SMB

SEC_E_LOGON_DENIED (0x8009030E)

SMB auth path only

LDAP, HTTP, RPC: Zero layers of protection

ACT 3

The Door Nobody Checked

LDAP Reflection on the Domain Controller

LDAP Reflection: Cross-Protocol Relay

THE IDEA

The Idea:

DC machine account shares key
for cifs/ and ldap/

If we get a cifs/ ticket, we can
present it to ldap/ service

LDAP does NOT validate sname field
LDAP has NO loopback detection
LDAP has NO source address check

THE ATTACK

The Attack:

1. Create CMTI DNS (attacker IP)
2. Start krbrelayx (SMB->LDAP)
3. PetitPotam coerces DC
4. DC auths with cifs/KERBDC
5. Relay to DC LDAP port 389
6. LDAP SASL bind: success
7. Session as KERBDC$ w/Delegation

Note: Requires CVE-2025-33073
patch missing (1-day)

LDAP Reflection Attack Chain

What LDAP Should Check vs. What It Actually Does

Check	SMB Server (srv2.sys)	LDAP Server (lsass.exe)
SPN service class matches?	YES (cifs/ required)	NO (accepts anything)
Source is loopback?	YES (Smb2ValidateLoopback)	NO (no equivalent)
Ticket is self-referential?	YES (SPN validation)	NO (no validation)
Source IP matches machine?	Implicit via loopback	NO

LDAP trusts one thing: "can I decrypt this ticket?" If yes, you're in.

Honest Assessment: What This Requires

For the CMTI -> LDAP attack (1-day):

DNS Coercion

Requires LDAP signing NOT Required (Server 2019/2022 default)

Requires network access to DC ports 88, 389, 445

Requires any authenticated domain credentials

GSSAPI Signing Limitation:

LDAP bind succeeds

Post-bind ops blocked if LDAP signing enforced

Attacker lacks session key (inside encrypted ticket)

Cannot wrap/unwrap GSSAPI MIC signatures

"Auth succeeds, but exploitation requires no LDAP signing
OR a relay target that doesn't require signing"

Honest about the limitations. This is real, but it's not free.

Beyond Published CVEs

Published patches cover SMB (client + server) and HTTP.sys (CBT only)

I asked: What about everything else?

- Systematic testing of unpatched protocol handlers
- RFC specification gap analysis (16 gaps identified)
- SPN encoding edge case testing
- Cross-protocol relay analysis
- Post-patch residual attack surface assessment

Result: Novel attack vectors discovered

Post-Patch Attack Surface (as of January 2026)

Protocol	Component	Patch Status	Reflection Protection
SMB Client	mrxsmb.dll	Patched (Jun 2025)	CMTI trick blocked
SMB Server	srv2.sys	Patched (Oct 2025)	Loopback + SPN validation
HTTP.sys	HTTP.sys	Patched (Jan 2026)	Channel Binding Token
WebDAV -> LDAP	WebClient + LDAP	UNPATCHED (0-DAY/DAY1)	No self-referral check in WebDAV SSPI
LDAP / LDAPS	lsass.exe	UNPATCHED	None
RPC	rpcrt4.dll	UNPATCHED	None
WinRM over HTTP	HTTP.sys (partial)	PARTIAL	Only HTTPS with EPA
DCOM	Various	UNPATCHED	None

The Breakthrough: What About HTTP?

The SMB self-referral detection (0x8009030E)
is SMB-specific.

HTTP/WebDAV uses a completely different SSPI path
that lacks this check entirely.

Ghost SPN: HTTP/dcghost.lab.local -> KERBDC$

WebDAV callback -> Kerberos AP-REQ (not NTLM!) -> Relay to LDAP

result=0 desc=success

HTTP/WebDAV Bypass: Key Details

PREREQUISITES

Requirements:

HTTP/ SPN on target machine
(not just HOST/ — forces Kerberos)
HOST/ alone = NTLM fallback

WebClient service running on DC
Not installed by default on Server
BUT: installable & sometimes enabled
(backup agents, SharePoint, etc.)

Ghost SPN with HTTP/ class
HTTP/dcghost.lab.local on KERBDC$

DNS record creation rights

SPN CLASS MATTERS

Why HTTP/ vs HOST/:

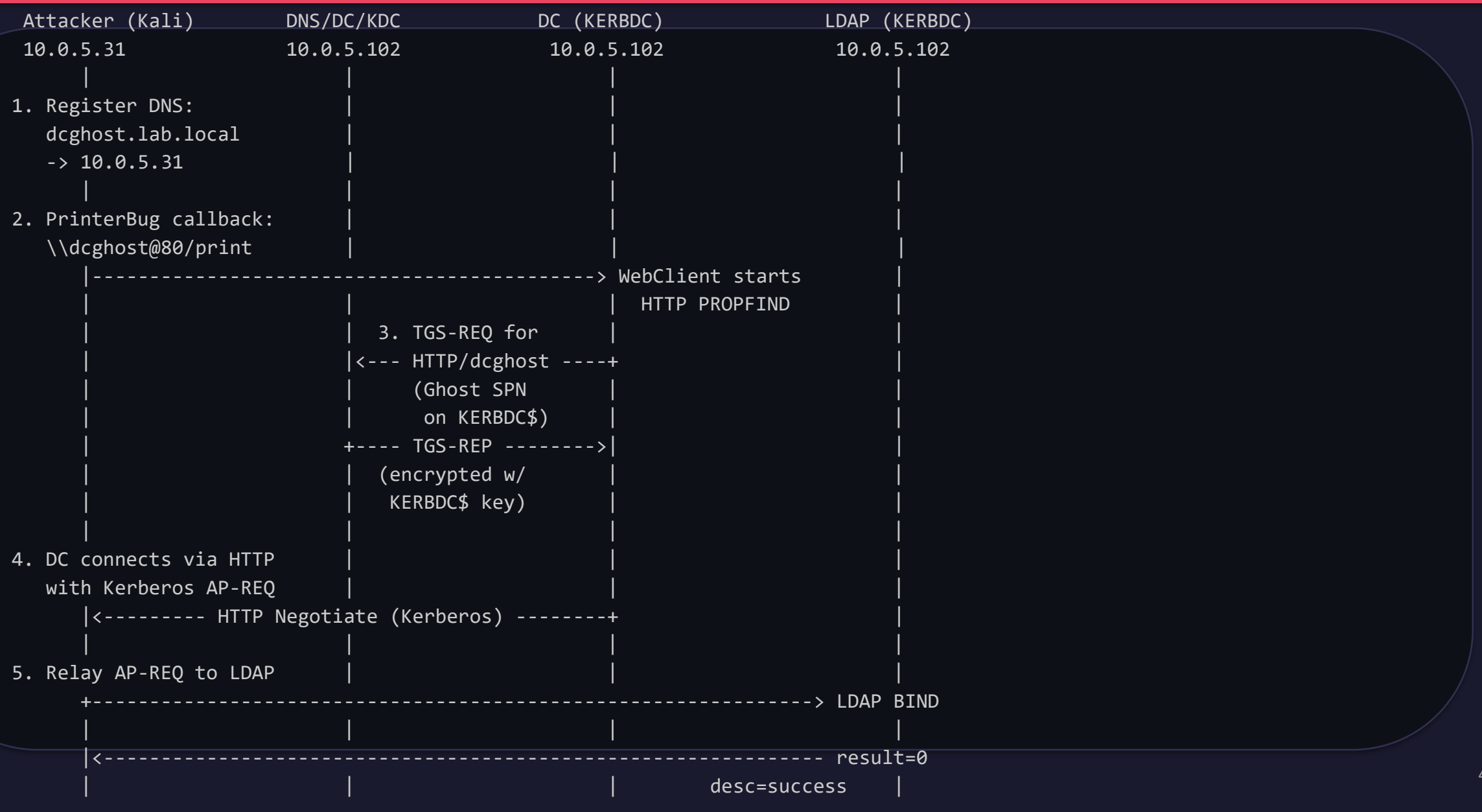
When WebDAV connects to a remote host,
it requests a Kerberos ticket for:
HTTP/<hostname>

If HTTP/ SPN exists -> Kerberos ticket
If only HOST/ SPN -> NTLM negotiation

This is because SPNMappings for
HOST/ do not include HTTP/ by default

The KDC will NOT map HOST/ -> HTTP/
like it maps HOST/ -> CIFS/

HTTP/WebDAV Self-Relay to LDAP — Attack Flow



Why It Works: Four Protections, None Apply

Protection	What It Does	Why It Doesn't Apply
NegpIsLoopback	Detects same-host SSPI negotiation	SMB-only check; HTTP/WebDAV path never calls it
mrxsmb.dll SPN check	Validates SPN in SMB client stack	Only runs in SMB client (mrxsmb.dll), not WebDAV redirector
srv2.sys loopback check	Rejects remote reflection to SMB	We target LDAP, not SMB — srv2.sys not involved
KERB_AUTH_DATA_LOOPBACK	Server-side loopback detection	Exempts machine accounts; DC authenticates as KERBDC$
LDAP validation	No SPN class or loopback check	LDAP accepts any valid Kerberos token — no reflection defense

Honest Assessment: What's New vs What's Known

Individual components are well-known:

WebDAV relay (NTLM)	Known since ~2018 (Dirk-jan, topotam)
Ghost SPNs	CVE-2025-58726 (Pierini, Semperis)
Kerberos reflection	CVE-2025-33073 (RedTeam Pentesting)
NTLMRelay2Self	WebDAV + NTLM, not Kerberos
CVE-2025-33073	Kerberos but via SMB, not WebDAV

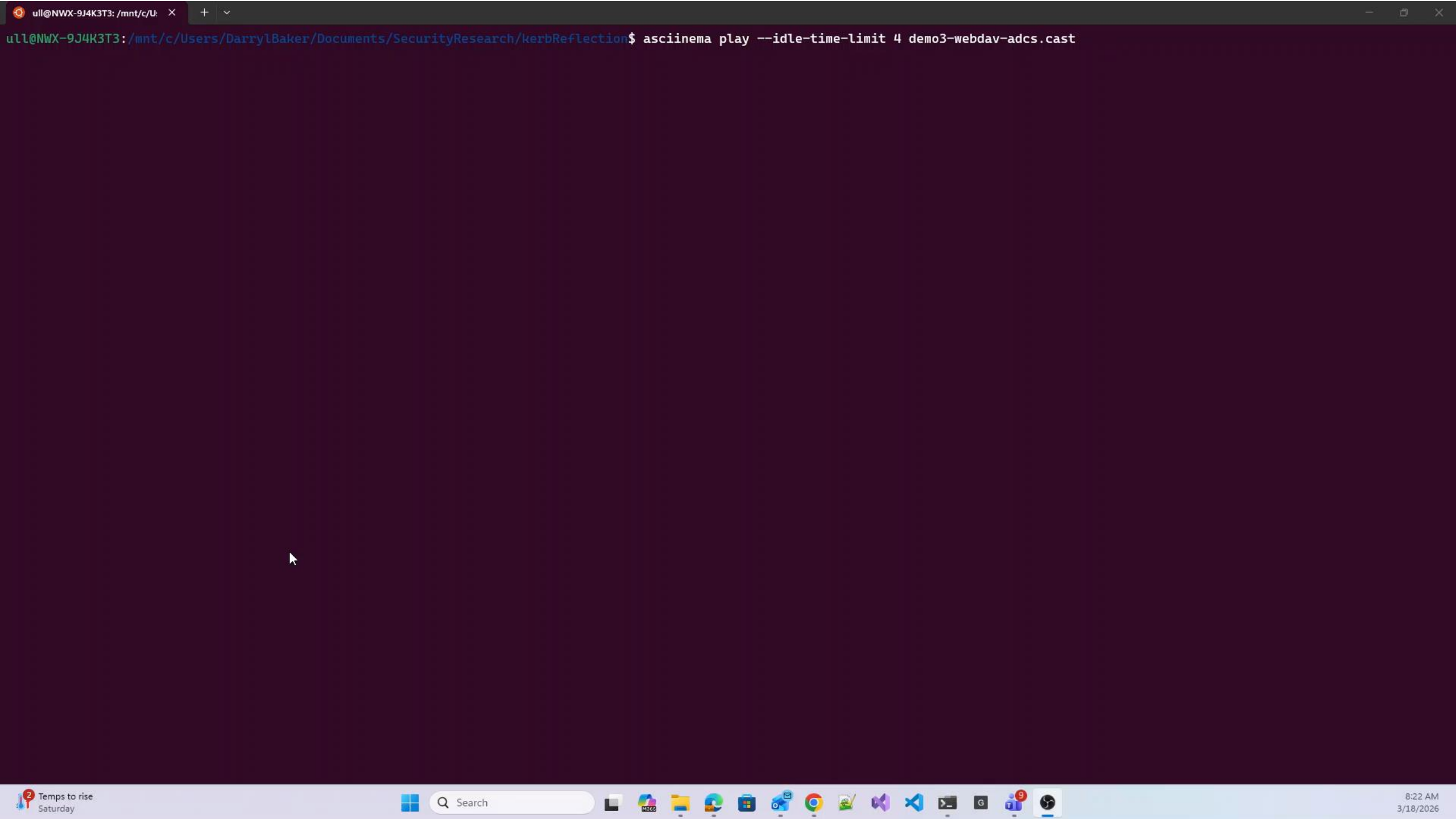
The novel synthesis:

WebDAV + Kerberos + Ghost SPN + LDAP + Same DC

= Bypass ALL existing patches simultaneously

No single prior technique combines these four vectors

to achieve self-relay on a fully-patched domain controller


ull@NWX-9J4K3T3: /mnt/c/U:
ull@NWX-9J4K3T3:/mnt/c/Users/DarrylBaker/Documents/SecurityResearch/kerbReflection$ asciinema play --idle-time-limit 4 demo3-webdav-adcs.cast
Temps to rise
Saturday
Search
8:22 AM
3/18/2026

I found that the LDAP vulnerability
extends beyond what I've shown today.

Additional findings have been submitted to MSRC
for responsible disclosure.

We are coordinating with Microsoft on a fix.

The game of whack-a-mole continues.

Details will be published after the coordinated disclosure window.

RFC Gap Analysis: 16 Specification Gaps

G1 No prohibition on self-referential tickets (CRITICAL)

G3 SPN canonicalization undefined (HIGH)

G4 Mutual authentication is optional (HIGH)

G6 Cross-realm reflection not addressed (HIGH)

G8 No channel binding required for HTTP (HIGH)

G10 'Negotiate Local Call' validation unspecified (CRITICAL)

G13 Datagram mode bypasses local call detection (HIGH)

G15 U2U authentication path differences (MEDIUM-HIGH)

The pattern: each gap represents a class of attacks,

not just one vulnerability. Protocol-level fixes needed.

Full catalog: 16 gaps documented in my whitepaper

ACT 4

Monday Morning

What You Can Do Right Now

Detection: What to Look For

KEY INDICATORS

Key Indicators:

1. Event 4624: Machine account ($)
   Kerberos logon from non-local IP
   Type 3, Delegation

2. Event 4769: Self-referential
   TGS request (X$ requesting X$)

3. Event 5145: Coercion pipe access
   (efsrpc, spoolss, lsarpc, netdfs)

4. DNS anomaly: CMTI blob pattern
   in hostname.

THE CORRELATION

The Correlation:

Event 5145 (coercion) followed by
Event 4624 (reflection) within
5 seconds

Single 4624 from external IP
= suspicious

Correlated with 5145
= near-certain

Deploy both rules together
for highest confidence.

The Hardening Stack (Priority Order)

1. PATCH (Critical)
   June + October 2025 + January 2026

2. LDAP Signing = Required (Critical)
   LDAPServerIntegrity = 2 on every DC

3. LDAP Channel Binding (High)
   Enable on LDAPS connections

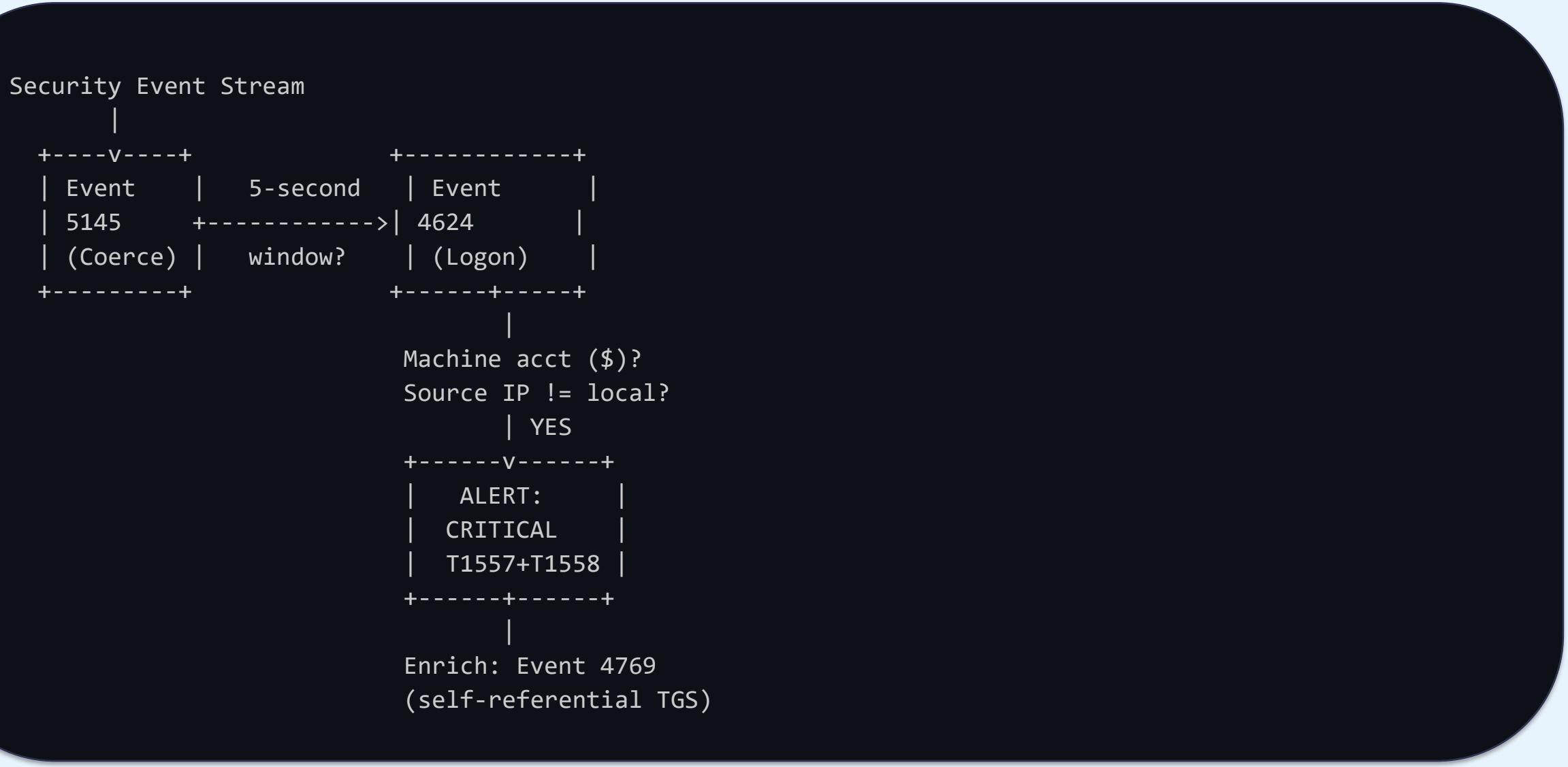
4. Ghost SPN Audit (High)
   Enumerate orphans, run monthly

5. DNS Record ACLs (Medium)
   Restrict authenticated user creation

6. SMB Signing (Medium)
   Enforce on all server roles

7. Coercion Mitigation (Medium)
   Disable Spooler on DCs, deploy RPCFirewall

Detection Rule Logic



The Real Fix: Protocol-Level, Not Service-Level

CURRENT ARCHITECTURE

mrxsmb.dll blocks CMTI (SMB client)

srv2.sys validates SPNs (SMB server)

Kerberos SSPI self-referral
(SMB path only)

LDAP: nothing

HTTP: partial (CBT only)

Each service must implement
its own protection

Miss one -> model collapses

RECOMMENDED ARCHITECTURE

MachineID / source-binding
in Kerberos ticket

Receiving service validates:
not issued for self

SPN class validation
at GSSAPI layer

Loopback detection in
lsass.exe (not per-service)

Fix once, every service
inherits protection

Key Takeaways

1. Kerberos reflection is the new NTLM relay.

   Same concept, higher impact.

2. All current patches are in the SMB stack.

   LDAP and other services have no native protection.

3. LDAP signing enforcement is your best defense.

   Most orgs don't have it enabled.

4. Ghost SPNs are everywhere. Audit yours.

5. Service-level patches are band-aids. Protocol-level changes needed.

Additional findings submitted to MSRC. Stay tuned.

Same lock, different door.

Until Kerberos authentication validates where a ticket came from -- not just that it can be decrypted -- the doors will keep opening.

Thank you.

Questions?

CONTACT

Darryl G. Baker

@DFIRDeferred

dbaker-cissp-ceh

darrylgbaker@menrva-tech.com

Responsible disclosure
inquiries welcome

MSRC case: active

All testing performed in