

Forum:[Hack Forums](#)

Thread: [\[TUT\] Windows Password Cracking - Breaking the NTLM Hash - By Insight](#)

Hinch - September 3, 2015, 5:54 am

If this is not allowed contact me and ill remove

Article: Windows Password Cracking: Breaking NTLM Hashes
BREAKING THE NTLM HASH:

TABLE OF CONTENTS :

- 1 - What is NTLM?
- 2 - How does NTLM work?
- 3 - Windows Integrated Authentication
- 4 - Pass the Hash
- 5 - NTLM Relaying Methods (including EXTERNAL relaying)
- 6 - Security Implications

-- What is NTLM? --

NTLM is a protocol used within windows for password storage and network authentication, NTLM hashes use MD4 encryption and when used for network authentication the hashed NTLM string is used rather than the original plaintext password.

A typical NTLM hash is case sensitive, has an unlimited length and is a stronger networking hashing algorithm than its counterpart LM network hash. NTLM is the protocol used specifically for password hashing whereas NTLM-AUTH is used for network-based remote authentication requests when interacting with services. There are various different flavours of NTLM, such as NTLM-AUTH, NTLM-V1, NTLM-V2, NTLM2, and flavours can vary based on whether they are signed or not.

-- How does NTLM work? --

NTLM authenticates with remote services through a 'handshake' that consists of three messages being sent, known as type1, type2, and type3.

typical type1 message (handshake initiation/NTLMSSP_NEGOTIATE):

NTLMSSP identifier: NTLMSSP

NTLM Message Type: NTLMSSP_NEGOTIATE (0x0000001)

Flags: 0x00088207
Calling workstation domain: NULL
Calling workstation name: NULL

What is happening here is that the client is interacting with the server, initiating a 'handshake' listing which flags it supports, and the name of the workstation and the domain in which it belongs to.

typical type2 message (Sever Response/NTLMSSP_CHALLENGE):

NTLMSSP identifier: NTLMSSP
NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
Domain: DOMAIN
Flags: 0x62818215
NTLM Challenge: 1122334455667788
Reserved: 000000
Address List
 Length: 102
 Maxlen: 102
 Offset: 68
Domain NetBIOS Name: DOMAIN
Server NetBIOS Name: HOSTNAME
Domain DNS Name: DOMAIN.TLD
Server DNS Name: SEVER.DOMAIN.TLD
List Terminator

in a type1 message the server does not yet know who the person initiating the handshake is as no informantion about that has been sent (other that domain info which is not of much use). In the type2 message, the server responds with its supported flags and domain information. It also responds with the NTLM Challenge string. This string has a unique dynamic value and it is used to salt the password hash to add an extra layer of security. The client then authenticates and completes the handshake with a type3 message.

typical type3 message (final auth/NTLMSSP_AUTH):

NTLMSSP identifier: NTLMSSP
NTLM Message Type: NTLMSSP_AUTH (0x00000003)
Lan Manager Response: 74795D4390C7DDEFB7DAD5D4373066CBF05D633F47F4F12B
NTLM Response: 74795D4390C7DDEFB7DAD5D4374066CBF05D633F47F4F12B
Domain name: DOMAIN
User name: USERNAME
Host name: HOSTNAME
Session Key: Empty
Flags: 0x00008205

The NTLM response is generated due to the server challenge being hashed with the password challenge. The username and workstation name for the domain it belongs to are also sent, alongside a session key if session signing is supported for the authentication. The examples above are typical for NTLM-1, NTLM-2 is different in

the sense that it uses a client challenge as a form of mitigation against attempted rainbow table attacks. NTLM-2 also has additional parameters added into the password response.

- Windows Integrated Authentication -

Windows integrated authentication is a method of network authentication that is used to prevent the user from having to re-enter their password when connecting to different services. For example, when you connect to a domain you are connecting to a network share and other services, but windows will not ask you to re-enter your password to authenticate the connection to each individual service, instead it just queries the API and gets the information back that is used to automatically authenticate, HTTP is used in the context of local security, "trusted site zones" are used as a form of security allowing this to only take place with a local one-word domain name. It then performs a DNS query relating to the domain name and queries the DNS hostname, then sends a broadcast request across the local network for the domain info.

- Pass The Hash -

Pass The Hash is a well known attack-vector that exploits NTLM by allowing the attacker to successfully authenticate to a remote service without needing the plaintext password, it instead authenticates using the NTLM hash. This bypasses the need to crack the NTLM hashes in order to require the password, as it allows practically the same level of access that would be obtained by doing so. This attack generally is used after the hashes have been obtained from local storage within volatile memory (for example the result of a cold-boot attack). The problem with this attack method is that it generally requires local admin access on the system so that the level of privilege escalation isn't much.

- NTLM Relaying + Methods -

NTLM relaying is a less-known attack method which does not require existing admin access to be performed, but instead can be performed from a guest account as long as a connection can be made to the network on which the attack is being performed. An issue with NTLM as shown within the packet handshake is that there is no kind of verification that the destination host is the host that you are supposed to authenticate to, yet the authentication is made anyway. NTLM Relaying works by setting up a rogue server which takes in the authentication requests and relays them to another target server. In 2008 windows patched the vulnerability where an attacker could bounce an NTLM request back to themselves (via SMB or even telnet through the use of the IE telnet:// exploit), but due to the way that the protocol is designed they could still be bounced to other hosts. There are many different protocols in which NTLM can be relayed to, besides the obvious protocols which are affected such as SMB and HTTP, other protocols include MSSQL, LDAP, RDP, PPTP, and many other protocols.

In order to exploit NTLM efficiently using this method, a HTTP and SMB Rogue Server needs to be setup on a remote connection. The rogue server needs to keep the use

authenticating as much as possible (rather than disconnecting after a single auth, on Windows LAN for SMB you can make it authenticate around 30 times in total before terminating the connection). In order to do this we need to figure out who the user is in order to keep them authenticating (something which generally isn't known until the type3 handshake response). This can sometimes be tricky to do, as within SMB the source IP and Port is not enough information if the attack is being performed externally, within HTTP, WPAD and similar requests do not always support cookies. The rogue HTTP server should use a HTTP-302 Redirect with Keep-Alive in order to keep the socket open, preventing the session from closing, meaning that once the authentication is complete, we know who the target user is for the rest of that session due to the connection remaining open. As for controlling authentication with the rogue SMB server before bouncing them to other services, some payloads need to be added. WPAD implementation is a must as it will check DNS and then check broadcasting to the network. By default Windows will automatically authenticate to the WPAD server over HTTP using the currently logged in user credentials which can then be spoofed and responded to (although there are limitations as you would have to typically be internal to the network or would have to spoof NBNS or DNS).

Social Engineering can be used by including a UNC network path within image tags for example, the browser would automatically connect back to windows and then authenticate with the network share and attempt to grab the image or whatever it may be, ranging from javascript to iframes. Some browsers attempt to mitigate this by checking to see whether the network share is within the file security context - this can easily be bypassed by setting headers for a forced download, which is then opened from the download location resulting in access to the file security context which will lead to automatic authentication to the SMB share which will then authenticate to the rogue server. There are still problems with this method as it relies on the victim downloading something, although a way around these problems are the use of commonly-used browser plugins in

order to establish the authentication to the rogue server via SMB. Common plugins such as iTunes and Quicktime are easily affected as you can create a playlist with a UNC network path which will automatically authenticate and bypass the local security context.

Another method that can be used for automatic authentication to the rogue server is through the use of vulnerable email clients. For example if an HTML email which contains a network share is read using Outlook then it will automatically authenticate. desktop.ini files can also be generated to say that the icon resource or wallpaper for that folder is a network share, resulting in automatic authentication with the credentials, this method also works with .lnk files.

The final method I will cover that can be used for automatic authentication to the rogue server is the traditional man-in-the-middle attack used to redirect NTLM-AUTH requests or to inject the HTML content previously covered into webpages viewed by the victim.

-- Security Implications --

Within MSSQL:

- Potential database access (read, write, modify, etc..)

Within SMB:

- Enumerate users/groups
- Access File Shares
- Execute Commands
- Cannot connect to Domain Controllers unless SMB Signing bypass is written

LDAP:

- Enumerate domain users/group memberships
- Change Passwords
- Add users to groups
- Relay domain admin to user workstation
- Authenticate to Domain Controller

Exchange Web Services (used by most organisations, allowing external NTLM relaying):

- Get email contacts
- Setup email rules

Vulnerable Systems:

NTLM is used by default in all versions of windows, including windows 8 and windows 2012. It is also used massively within corporate environments. Many protocols are vulnerable (practically any vulnerable that has NTLM support is vulnerable to local NTLM relaying and certain protocols are even vulnerable to external NTLM relaying using some of the described methods).

All credit goes to the creator who is also in the group insight.

m.duran - September 3, 2015, 7:43 am

Good tutorial! Very informative!

Hinch - September 4, 2015, 9:34 am

Thanks for that i have told it to the creator

spradebassen - September 4, 2015, 9:36 am

This is a pretty detailed thread, people might find this useful.

Nomad.Null - September 4, 2015, 11:20 am

Outstanding tutorial for NTLM cracking. I didn't see OphCrack in there though. It's a powerful rainbow-table attack suite for acquiring local administrator account passwords through brute-force. It requires local access, but it is pre-boot, which bypasses the drive-lock, and is extremely fast. If you are trying to preserve the admin password to avoid detection and have physical access to a domain machine, there are few better ways.

However, I understand that this focused mostly on remote exploitation and acquisition of the NTLM hash. This is an outstanding tutorial for that exact purpose.

Big Vouch.

kmz2200 - September 4, 2015, 11:48 am

Uh.... or you just can use konboot o.o

Hinch - *September 5, 2015, 4:03 am*

(Sep 4, 2015 11:48 AM)kmz2200 Wrote: [\[CITE\]](#) Uh.... or you just can use konboot o.o
Never had this so i wouldnt know i personally have never lost my windows password