

Forum: [Hack Forums](#)

Thread: [pass the hash: Samba/SMB](#)

Termacspain13 - March 11, 2024, 6:06 pm

is anybody good with smb configuration? I want to escalate my privileges inside a network, i have low priv account credentials. I want to configure a samba server to force ntlm authentication

DramaKing - March 12, 2024, 6:35 am

(Mar 11, 2024 06:06 PM)Termacspain13 Wrote: [\[CITE\]](#) is anybody good with smb configuration? I want to escalate my privileges [sic] inside a network, i have low priv account credentials. I want to configure a samba server to force ntlm authentication

Umm, disable anonymous login? I'm not great with Samba configuration, but seeing as the title says "pass the hash" and you're trying to escalate privileges, maybe I don't understand at all.

Termacspain13 - March 13, 2024, 3:34 pm

(Mar 12, 2024 06:35 AM)DramaKing Wrote: [\[CITE\]](#) Umm, disable anonymous login? I'm not great with Samba configuration, but seeing as the title says "pass the hash" and you're trying to escalate privileges, maybe I don't understand at all.

so by configuring the samba server force ntlm authentication i can get their ntlm hash. I have an html file which when they open will redirect them to the samab server, i jsut need to configure the server to force ntlm authen (chatgpt helped but im looking for like a full configuration)

DramaKing - March 13, 2024, 4:24 pm

(Mar 13, 2024 03:34 PM)Termacspain13 Wrote: [\[CITE\]](#) so by configuring the samba server force ntlm authentication i can get their ntlm hash. I have an html file which when they open will redirect them to the samab server, i jsut need to configure the server to force ntlm authen (chatgpt helped but im looking for like a full configuration)

Ok, now I'm understanding. You're using something like 'python3 [ntlm_theft.py](#) -g htm' or just adding a line like '' to an html file. Then all you would need to do is use Impacket's smbserver or Metasploit's auxiliary/server/capture/smb module on your machine. I'm assuming that this is for your own testing or a corporate pentest, so once the file is opened the victim machine should try to connect to you and authenticate with NTLM. You can then try to crack it or relay the NetNTLM exchange to another system with ntlmrelayx.

From what you're saying, you're just using sambad. It shouldn't be that hard to configure ntlm_auth, even though NTLM is proprietary. I'm more than a little surprised that you're using the built-in system service for hacking, though. Sambad won't log anything other than success or fail, so you'll have to sniff the NTLMSSP packets and manually extract the data from the appropriate fields to form the hash. Took me a little bit to get my head around what you were doing, since it is very much the hard way.

Termacspain13 - March 18, 2024, 10:17 am

My bad I thoguht I aswered!!

So itn worked man, thanks so much you saved me a lot of time!!

