22

Now that we have enumerated and attacked all initial vectors we can begin to collect the credentials that we have as well as what footholds we have on the network, to see how we could laterally move throughout the network. The first thing to do when we have credentials but don't know what to do with them is to pass the hash with them. This check each IP and validates the credentials. You will need to practice passing the hash with the hash you dumped in Task 20 as well as the hash from Task 10.

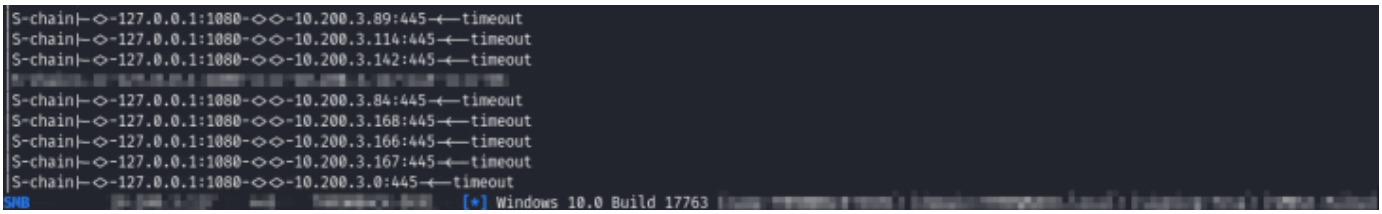
Pass the Hash Overview
Pass the hash (PtH) is an attack wherein we can leverage found NTLM or LanMan hashes of user passwords in order to successfully authenticate as the user they belong to. This is possible due to well-intentioned security ‘feature’ within Windows where passwords, prior to being sent over the network, are hashed in a predictable manner. Done originally with the intent of avoidance of password disclosure, we can leverage this feature to capture and replay hashes, allowing us to authenticate as our victim users. In this section, we’ll dig into this further with the tool crackmapexec.

Installing crackmapexec
1.) sudo apt install crackmapexec
Note: We have received reports that the latest version of CrackMapExec segfaults, we recommend using a prior version like 5.0.2dev until further updates are released.

Crackmapexec help menu

Conquering Hashes with crackmapexec
1.) Configure proxychains to the proxy server that will be sending your requests. You will need a proxy

server to pivot to the other machines and bypass segmentation. You can also utilize sshuttle as a proxy server to pivot.
2.) proxychains crackmapexec smb 10.200.x.0/24 -u -d -H



Success! We got a hit passing the hash!

To continue on you can either use the hashes from mimikatz or cracked passwords from Task 10 to pass the hash then access the device(s). To access the device(s) you can either use the hashes with evil-winrm or you can attempt to crack the hashes and use ssh or rdp.

Answer the questions below

What two users could successfully pass the hash to THROWBACK-WS01? (In alphabetical order)

Correct Answer