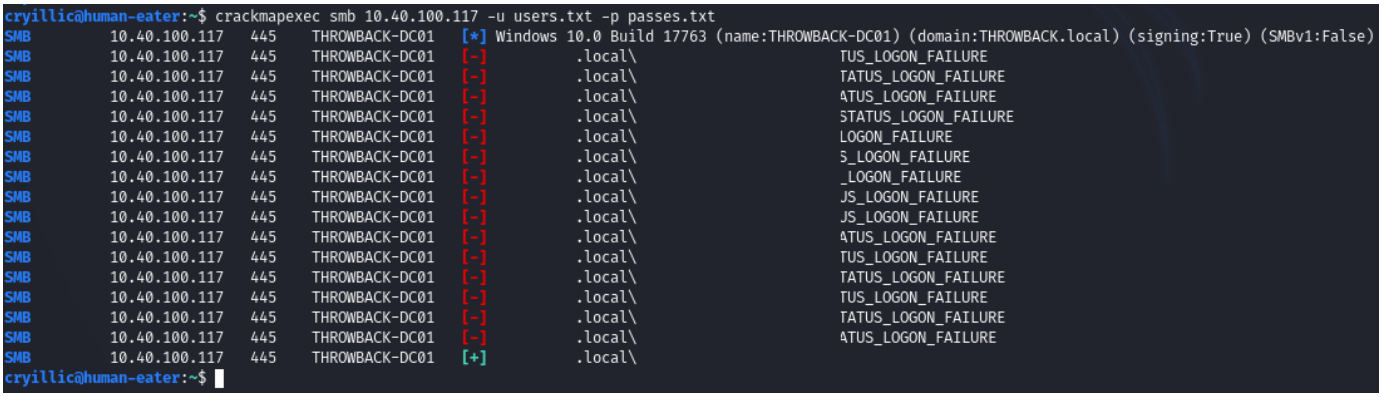
29

Now that we have dumped a list of users on the domain we need to generate a wordlist of users and attempt to password spray.

Password Spraying with crackmapexec
Password spraying with crackmapexec is much easier than password spraying a login portal with hydra. To password spray domain users with crackmapexec you will first have to format your user list similar to how you formatted it with hydra. After formatting our user list we can use crackmapexec to password spray across the domain and gain access to domain accounts.
We can not only use the user list we got from the database or namely but we can also use a custom password list rather than spraying one password at a time.
1.) proxychains crackmapexec smb 10.200.x.117 -u users.txt -p passes.txt
When running the password spray make sure to tunnel it through proxychains or it cannot validate with the domain controller.



Password spraying the domain controller with crackmapexec

Note: It may be necessary to use the --continue-on-success flag in newer versions of CrackMapExec

After password spraying if successful we should have a valid set of credentials to log into the domain controller with. Remember that the network is segmented and you will need to pivot again to access the domain controller.

Answer the questions below

What user was successfully password sprayed?

Submit

What was the password for the user?

Submit