**INFOTC 3001 - Advanced Cyber Security**

**Laboratory # 4 - Password attack**

1. **Objectives**
2. Understand Brute force and Dictionary attacks.
3. Understand basic cryptography concepts.
4. Generate a customized passwords file.
5. Exploit vulnerabilities using SMTP and FTP protocols.
6. **Material Required**

Kali Linux, Metasploitable 2.

1. **Activity**
2. Download Metasploitable 2 from <https://metasploit.help.rapid7.com/docs/metasploitable-2>
3. Configure Metasploitable 2 with the 192.168.166.199/24 IP address (use msfadmin/msfadmin credentials), and connect it to the VMnet2 or ‘Private to my Mac’ vSwitch.
4. **Review Questions**
5. Why does a Hash algorithm fail? Your answers should include the term ‘collision Resistant’.
6. Inquire about the relationship that exists between *hashing functions* and *cryptocurrency*, write a summary of your findings. (minimum of 100 words).
7. Mention 2 advantages and 2 disadvantages of using Brute Force attack
8. Mention 2 advantages and 2 disadvantages of using Dictionary attack.
9. Read the article <https://nakedsecurity.sophos.com/2016/08/18/nists-new-password-rules-what-you-need-to-know/> Do you agree or disagree with the NIST password rules? Give reasons to support your position.
10. Provide an example of using a flag not covered in the lecture for the crunch command, we used -f -t and -p flags. Provide a screesshot and explain the output.
11. By using hydra tool agains Metasploitable 2, we were able to ennumerate: ftp, user, postgres and service accounts. Use the service account with ftp over Metasploitable 2 to verify if there is some useful information for that account. Describe your findings and attach a screenshot.
12. Inquire about the medusa tool and obtain a similar output as we did with the hydra tool i.e. find 4 users accounts and 4 passwords. Include a screenshot.
13. We used the user account with ftp to download a private key to our local system from Metasploitable 2. One of the commands that the user account executed (according to the bash\_history file) was:  
      
    sudo cat ~/.ssh/id\_rsa.pub >> /home/msfadmin/.ssh/authorized.keys

From the previous command, we can see that apparently there is a msfadmin home directory for a msfadmin user.

Verify if you can ssh to Metasploitable 2 by using msfadmin user and the private key you downloaded from there. Include a screenshot.