CPSC2106 INFORMATION SECURITY

# Lab 2: Mitigation and Deterrent Techniques – Password Cracking

## NISGTC Security + Lab Series

## Lab 8: Mitigation and Deterrent Techniques – Password Cracking

Complete the attached lab in Netlab+.

To log in to Netlab+ go to <http://netlab.columbusstate.edu>.

Reserve a pod for individual use.

**Note:** Step 7 in Section 2 (Cracking Windows Passwords) does not work because hashcat is not installed in the system. Because the system is not connected to the Internet we cannot install it. Therefore, Step 7 will not work for you but if it had worked, you’d get the output you see in the file.

Take screenshots of your work at these steps and **copy them in this document:**

Step 16 of 1.1 on page 10

Step 2 of 1.2 on page 10

Step 6 of 2.1 on page 12

Step 12 of 3.1 on page 15

Step 13 of 3.2 on page 19

Note: You can use the Snipping Tool to take the screenshots on a Windows machine

**Provide answers to these questions (in this document. Please use a different color for your responses)**

1. **In the lab, where and how was John the Ripper used? Describe briefly how it works.**
2. **What is the name of the tool used to crack the ntlm hashes?**
3. **How did you get the shadow file from the DVL in the lab?**

**Submit your assignment in the Dropbox in CougarView.**

**Grading Rubric:**

|  |  |
| --- | --- |
|  | MaxPoints |
| Screenshots from Lab | 5 |
| Answers to questions | 4 |
| Style | 1 |
| Total | 10 |