

Lab 8 Student Handout:

Due Date: by date specified in D2L.

Read the instructions about where to post the assignment.

Purpose:

To gain an understanding of how to utilize John the Ripper and create rules to crack passwords.

Scenario:

You have been asked to verify the complexity of passwords used in the organization. You must retrieve the shadow file, develop the necessary rules, and retrieve the passwords.

Assignment:

Connect to the server with the following IP address. A.A.57.2A

Your local IP received through DHCP should automatically be in the correct range.

This is an **INDIVIDUAL** lab. Everyone must solve this lab on your own. Do **NOT** share results from any portion of this lab with another student.

Use a transfer protocol to retrieve the file. **Do not use** SSH, FTP, TELNET, instead use something trivial.

The username to use to retrieve this file is: Administrator

The password to use to retrieve this file is: Password1

The file you need is called shadow and it is in the administrator home directory.

Submit the following items:

- Command used to retrieve the password file.
- Your rules file (optimized to break the rules solve just the passwords in question)
- The command you used with john to run the rules above.
- No other report is required for this lab.

There are 10 passwords to be broken.

You will receive 10 points for each you break.

Demo does **NOT** count.

There are also 5 elite passwords. You do **NOT** have to break these passwords. If you **DO** break one, one elite password broken is worth 2 regulars. If you break 2 elite's, you get a 100% on the assignment.

Scope:

All the tools you need to complete this lab are available on the computers in the lab.