# User Auditing and Password Policy PrivEsc Lab

Welcome ladies and gentlemen to your (probably) first experimentation with hacking tools. The purpose of this and the other labs during Advanced Camp is to allow you to learn and understand the importance of the material the instructors teach you. Today’s lab will focus on the vulnerabilities of having an insecure password and the usefulness of password policies using the one and only Hydra.

### Check that the tools are in your VM

1. Log in to the VM as user (password is password lol)
2. Ryan should have installed Hydra and added three users: user, jay, and kay. A README file containing the users’ passwords should be in user’s Desktop directory, and there should be a rockyou.txt file in /opt.
   1. Install the hydra package if it is not there. How do you do that again?
   2. Add any missing users. What commands do you use to do that (pls don’t tell me you have short-term memory)?
   3. If there is no README in the Desktop, no need to make a new file. jay’s password is 123456, and kay’s password is ringring. If these users are missing, assign their respective passwords to them.
      1. Pro tip: You should never have a plaintext file on your computer since it gives intel to attackers, and if you do, delete it. It’s ok for you to keep this file because this is just an exercise.
   4. If there is no rockyou.txt, go to this site to get the compressed version of the file: <https://wiki.skullsecurity.org/Passwords>
      1. Once downloaded, unzip the file by running this command: bunzip2 rockyou.txt.bz2. Move it to /opt. What cmds do you need here?
      2. Have you ever heard of this file before?
3. Hydra works on remote services. For this lab, we will use SSH to test this tool out. Install openssh-server. No hardening needed. We will save that for tomorrow.
4. Also install libpam-cracklib and fcrackzip, as we will use them to test out passwords.

### Basic Bruteforce Attacks

In this first part of the lab, we will test how secure a password due to its length. Fcrackzip is a password cracker that brute forces passwords of .zip files that have less than or equal to 7 characters, and we will use this tool to test this out.

1. Make your files that you will compress to make the zip files: touch [file name]
2. Compress the folders with a password using the command zip -e [folder name].zip [file name]
   1. Make the password of one of the .zip files shorter than the other
   2. Make the passwords <= 7 characters
3. Run Fcrackzip on the zipped file with the shorter password. Record the time it takes to find the password.
4. Do the same with the zipped file with the longer password.

Which zipped file took longer to crack?

### Dictionary Attacks

This is where we will start using Hydra. Yay! The more specific bruteforce attack that you will perform is a dictionary attack, where you use the phrases in a wordlist as the passwords you will test against the user accounts. rockyou.txt is a very popular wordlist used in dictionary attacks. Pro tip: CyberPatriot sees these tools as malicious because of their use. You should remove them on an actual competition image.

1. To conduct the dictionary attack, run the command hydra -l [user] -P /opt/rockyou.txt ssh://localhost
   1. Try this on every user. Which users’ passwords did you crack? Which user wasn’t exposed? How fast did it take for the passwords to be tested and found (if they were cracked)?
2. Take a look into rockyou.txt. Observe the different dictionary passwords in the file and the large number of them. Yeah, that’s a lot of insecure passwords for you to look out for.

### Testing out Password Checks

The objective of this exercise is to observe how password checks work using libpam-cracklib. Refer to the slides if you need to

1. Choose one of the password check options mentioned in the slides to test.
2. Try to change a user’s password using the command passwd user. Give a new password that includes an element that the check you chose would prohibit. Remember that password for later. Take note any messages that you get when you make the password.
   1. Ex: if you wanted to check the reject\_username option, make a password that includes the username of the user whose password you are changing
3. Implement the password check option. Edit the /etc/pam.d/common-password file to do so.
4. Try changing another user’s password using the same password you used on the previous user. Did you get any new messages? Were you able to change the user’s password?
5. Repeat steps 1-4, choosing a different option each time. You should do this about 5 more times so that this exercise doesn’t turn into busy work.