Laboratory Exercise X – Cyber Basics – Introduction to Password Auditing

Due Date: 2021-10-19
Points Possible: n/a

1. Overview

This laboratory exercise will provide some hands-on experience with password strength analysis using command-line tools in Linux.

Recommended Reading

Wikipedia article titled 'passwd', which introduces and describes the Unix/Linux passwd and shadow files: https://en.wikipedia.org/wiki/Passwd

2. Resources required

This exercise requires a VirtualBox Kali Linux Virtual Machine running on a computer (laptop) or a Kali Linux VM running in the Cyber Range.

3. Initial Setup

From your Cyber Range course, select the **Cyber Basics** environment. Click "start" to start your environment and "join" to get to your Linux desktop login. Log in using these credentials:

Username: **`student`**
Password: **`student`**

4. Tasks

Task 1: Introduction to password auditing.

On Linux systems, user accounts are stored in the **`/etc/passwd`** file (world-readable text file) and passwords are hashed and stored in **`/etc/shadow`** (a text file only readable by root). You have administrative (root) access on your Kali virtual machine – go ahead and "cat" those files to see what they look like (see https://en.wikipedia.org/wiki/Passwd. You'll note that the hashed passwords or stored in the shadow file, which is only readable by users with administrative privileges. On windows systems, hashed passwords are found in the SAM (database) file found in c:\windows\system32\config. This file is not a simple text file – you've got to use special tools to read it.

We'll use a password auditing tool called John the Ripper (JTR), probably the most effective and most widely known password cracker. JTR is available from www.openwall.com/john. You can pay for the "pro" version or select one of the 'official free version' for your operating system. Windows and Unix/Linux executables are available. If you want the best performance and are comfortable

compiling software from the source code, download the latest community-enhanced "jumbo patch" and compile for your specific platform.

JTR can be run in various modes, to include dictionary and hybrid modes, both of which use a "dictionary" provided by the user. Dictionaries are compiled from widely used passwords, words scraped from a company's website, etc.

Exercise 1: Crack Linux passwords. Here we'll create a couple of new accounts on our Linux VM, one with a good password and one with a poor one:

1. Make sure you are at a 'root user' prompt (ends with **#** instead of **$**). If you have a standard user prompt (**$**), use the sudo command to execute the su (switch user) command to become "root" as follows:

```
$ sudo su -
[you will be prompted for your 'sudo password'. On your
 Cyber Range Kali Linux VM it is your student account password.
 Probably 'student'.]
```

2. Create 2 accounts as follows, one with a bad password and one with a good one.

```
# useradd johnsmith      - this is a quick way to add a Linux user account
# passwd johnsmith       - this is used to set user's password
Enter new UNIX password: 12345
Retype new UNIX password: 12345

# useradd janedoe
# passwd janedoe
Enter new UNIX password: <non-dictionary w/with numbers, special chars, etc.>
Retype new UNIX password: <same as above>
```

3. Now let's see which ones we can crack. Copy /etc/shadow to a text file, and run john against it:

```
# cp /etc/shadow ./pass.txt    - copy the shadow file to the john folder
# cat pass.txt                 - see the usernames and encrypted passwords.
# john pass.txt                - let's start cracking!
```

JTR will attempt to decipher the passwords and display any that it 'cracks' as it goes along. It starts in "single crack" mode, mangling username and other account information. It then moves on to a dictionary attack using a default dictionary, then with a hybrid attack, then brute force where it will try every possibly combination of characters (letters, numbers, and special characters) until it cracks them all.

The password for the johnsmith account should be cracked rather quickly. Don't wait for John to crack your 'good' password in brute force mode as it could take months or years to complete. Press [CTRL]-[C] to stop execution.

John uses the following files to manage execution. Most are all stored in the **/usr/share/john** folder on your Kali virtual machine (john.pot is stored elsewhere as indicated):

- **password.lst** is john's default dictionary. You can specify another wordlist on the command line using the **--wordlist=** directive (for example **# john --wordlist=/usr/share/dict/american-english /etc/shadow**
- **john.conf** is read when JTR starts up and has rules for dictionary mangling for the hybrid crack attempt
- **john.rec** is used to record the status of the current password cracking attempt. If john crashes, it will start where it left off instead of starting again from the beginning of the dictionary.
- /root/.john/**john.pot** lists passwords that have already been cracked. If you run john again on the same shadow file, it won't show these cracked passwords unless you delete this file first.

Task 2. More password audit.

John the Ripper's default dictionary (described above) is a short list of common passwords. Sometimes a standard English dictionary is a better option. In this exercise, we will download a Linux shadow file that contains a set of user accounts and hashed passwords, then attempt to determine the passwords.

```
# wget artifacts.virginiacyberrange.net/gencyber/shadow
# john shadow
```

Let John run for a few minutes, then stop with [CTRL]-[C]. How many passwords are revealed?

Now we will run John again with a different dictionary. First, we will make sure an American English dictionary is installed on our Kali Linux system. (If dictionary is already there, the below command will update it.)

```
# sudo apt update; sudo apt install -y wamerican
```

Next, we will run John with the new dictionary by invoking the --wordlist directive at the command line.

```
# john shadow --wordlist=/usr/share/dict/american-english
```

Q: How many of the passwords were revealed this time? _____

Q: Why was this pass more effective? _____

TIPS:

1. Experiment with different password & passphrase scehems at https://www.useapassphrase.com/
2. Use different passphrases for each website you use!
3. Use a password manager, for special, hard to remember passwords like: KeePass2 - https://keepass.info/ LastPass - https://www.lastpass.com/

5. References

- Wikipedia passwd article: https://en.wikipedia.org/wiki/Passwd
- John the Ripper (JTR): www.openwall.com/john

[This portion of the lab exercise template is provided for instructors that will be using this lab in a class they are teaching.]

This exercise makes use of resources provided in the Cyber Range. It is a single Kali Linux virtual machine, or you can choose to have the students complete this exercise with a VirtualBox Kali Linux Virtual Machine on their computer (laptop).

KSAs, from NIST SP 800-181:
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Knowledge:

- K0119: Knowledge of hacking methodologies in Windows or Unix/Linux environment.
- K0129: Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep).
- K0158: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).

Skills:

- S0067: Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).

Knowledge Units (KUs) Addressed:
From: https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf
(you may need to accept an invalid iag.gov SSL certificate to reach this PDF)

- Cyber Threats (CTH)
- Linux System Administration (LSA)
- Operating Systems Hardening (OSH)