PenTest Lab Exercise Ex010 – Kali Netlab

Goal

Learn how to use the Netlab server and log in to Kali. Find two keys.

Tasks

1. Log in to the Netlab server and schedule the PenTest Ex010 Lab.

2. Start up the lab and log in to your Kali VM. The username and password will be given in a Canvas announcement. **Change your password!** Never keep default credentials!

3. **Look for and find two keys on your kali attack box.** The string `KEY###-xxxxxxxxxxxxxxxxxxxxxx==` describes the form of these keys. They are 31 character strings: the string `KEY` followed by three digits followed by a dash followed by 22 characters from set {`A-Za-z0-9+/`} followed by two equal signs.

   `KEY001` can be found as part of a file name somewhere in the filesystem of your Kali VM. You may want to use `find` to identify it. The file's content reiterates the vague information I've already provided that tells how you can determine an encryption key (which is the base64 decoded value of `KEY000`). That encryption key will serve as the basis for decrypting the final exam leeway string.

   One ***process*** for finding `KEY002` is somewhat more complex. Consider using one of the linux commands presented in my slides. You'll need to provide that command an argument that (according to the man page) *lifts the "must have a tty" restriction.*

4. Note the key values for `KEY001` and `KEY002`.

5. Create a (very) brief report explaining what you did.

   Even though the report is brief, use LaTeX and the PenTest report template document to produce it. (There's no better time to learn than now!)

   Your report must include an attack narrative but all other elements of the report should be removed. Although searching for information on a machine is a valid penetration testing activity, none of what you do for this exercise would actually have an impact on a penetration test.

In your report, briefly but clearly tell me what steps you took to find the keys and what the keys were.

6. In this, as in all other exercises, make sure you read the exercise description carefully to see what information I demand that you provide. The grading rubric for these exercises is always, “Did you provide the information I demanded.” Look for phrases like, “tell me,” or “explain how.” If I tell you, “You may want to,” this is not a demand and is included for you to explore further and learn more. If you really want to understand what this penetration testing thing is about, always explore further!

7. Though I do not require it, you may want to save the keys you found. You can store them on the plunder server (`plunder.pr0b3.com`). If you want to decrypt the key string, it is best to avoid typos that will naturally be introduced by typing the long key strings. Cut-and-paste is your friend as are other methods of exfiltration that do not require typing long seemingly meaningless strings.