Ex010 - Netlab Kali

Simon Tobon

2021-07-08

Contents

Attack Narrative

In this Exercise we were tasked to find KEY001 and KEY002 using Kali Linux commands.
For KEY001 the professor hints that we should use the find command to locate this KEY. I first cd into the root directory by using cd .. twice. The following command was then run to accomplish this task:

```
find . –name "*KEY001*"
```

This outputted: **KEY001:thZp0CuipB5dlHSIBIujUg==**. So KEY001 was very simple to obtain.

For KEY002 the professor mentions that we must lift the "only-yourself restriction." By searching on Google for Linux commands with the only yourself restriction the **ps** command is the only one that mentions it in its man page. The ps command looks at process status, which is a good sign since in the Exercise instructions the word process is emphasized. This led me to believe that ps had to be the command used to find the KEY. I lifted the only yourself restriction and terminal process restriction with the following command:

```
ps ax | grep KEY002
```

This command lists all the processes in the environment and then pipes the result through grep to find process titles that contain KEY002. By using this command I was able to find KEY002.
KEY002:Y/IWt0eS4/73sk3qaFn08g==.
I then, finally, saved the keys to my Plunder server by SSH

```
ssh stobon@plunder.pr0b3.com
```

They were stored into a text file using Nano.