Penetration Test Report

Pulkit Sanadhya

5th September 2019

Contents

Executive Summary

Background

The Background revolves around finding the KEY003 as a part of a filename in the assigned kali attack machine as well as a finding the KEY002 as part of a process name.

Recommendation Summary

The kali linux attack machine will be used to find the required keys using multiple linux commands in the CLI.

Technical Report

Information Gathering

Active Intelligence

Initially , as the problem statement asserts that KEY003 can be found as a part of the filename in the file system which gives us a clue for proceeding further. So , all we needed was to run the command *"find"*.

The input to CLI interface was :
*root@kali: / find. maxdepth 5 -name "*KEY003*"*

which resulted in the following output:
./boot/grub/ThisistheKEY003:3UXthL6E+G4Y1S5qfKjdFw==

So, finally we can affirm that the required key is:
KEY003:3UXthL6E+G4Y1S5qfKjdFw

Secondly , according to the problem statement we can easily deduce that we need to find a process and search that process for the key so we have to use the command *"ps aux"* to list all the processes and we have to use grep command also along with it to find all the processes having the string 'key' as a part of their name.

So , after giving the following command:
root@kali: / ps aux (piping operator) grep 'key'.

We observed the output where the process name and hence the required key was found to be :
KEY002:/LL10yxHS/CxSf93wVHelg

Conclusion

So , it can be concluded that we were successfully able to find the required keys *KEY002:3UXthL6E+G4Y1S5qfKjdFw and KEY003:3UXthL6E+G4Y1S5qfKjdFw* as per the problem statement.