Ex010

Gary Jones

Contents

Executive Summary

Project Overview

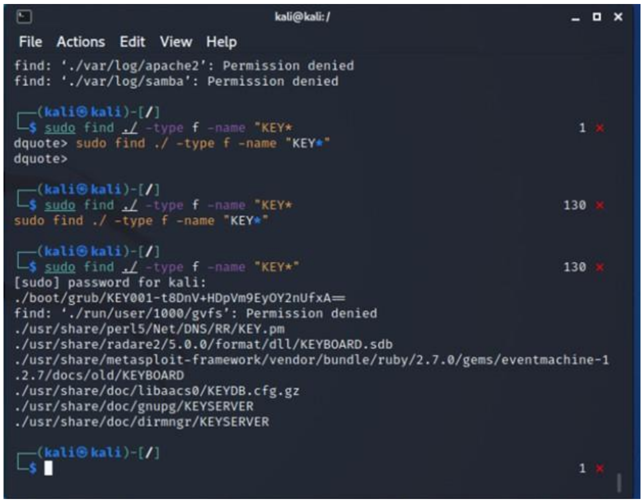
The objective of this project was to identify two keys: KEY001 and KEY002 by utilizing Linux command line arguments on the Kali Virtual Machine.

Summary of Findings

See below for identified Keys:
KEY001: KEY001-t8DnV+HDpVm9Ey0Y2nUfxA=
KEY002: KEY002-kmrMSsSaaSvbbVz3yW0zaw=

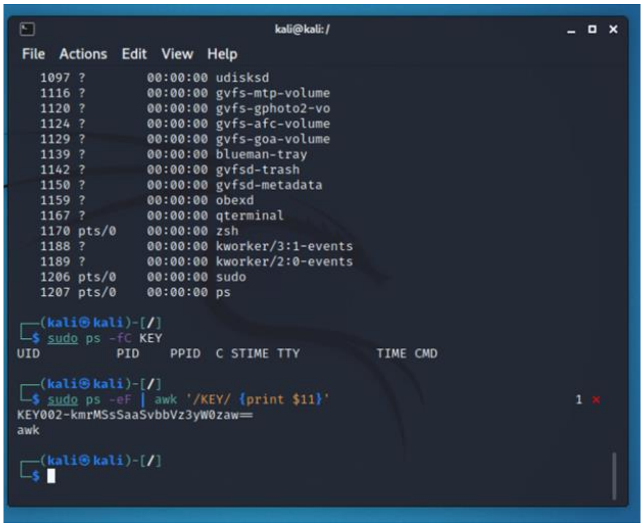
Attack Narrative

In order to identify KEY001 and KEY002 I initially changed directories to be at the root of the system. In other words all directories I searched through were branches of my starting spot. In order to find KEY001 I utilized the find command with sudo to give me full permissions in the system. The keyword I used for the search was ”KEY*” (see figure 1). For KEY002 I used the ps command to search for all active processes and similar to the find command the phrase I searched for was ’KEY’ (see figure 2).



```
find: './var/log/apache2': Permission denied
find: './var/log/samba': Permission denied

┌──(kali㉿kali)-[/]
└─$ sudo find ./ -type f -name "KEY*                                       1 ✗
dquote> sudo find ./ -type f -name "KEY*"
dquote>

┌──(kali㉿kali)-[/]
└─$ sudo find ./ -type f -name "KEY*                                     130 ✗
sudo find ./ -type f -name "KEY*"

┌──(kali㉿kali)-[/]
└─$ sudo find ./ -type f -name "KEY*"                                    130 ✗
[sudo] password for kali:
./boot/grub/KEY001-t8DnV+HDpVm9EyOY2nUfxA==
find: './run/user/1000/gvfs': Permission denied
./usr/share/perl5/Net/DNS/RR/KEY.pm
./usr/share/radare2/5.0.0/format/dll/KEYBOARD.sdb
./usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/eventmachine-1
.2.7/docs/old/KEYBOARD
./usr/share/doc/libaacs0/KEYDB.cfg.gz
./usr/share/doc/gnupg/KEYSERVER
./usr/share/doc/dirmngr/KEYSERVER

┌──(kali㉿kali)-[/]
└─$ █                                                                      1 ✗
```

Figure 1: Screenshot for KEY001.



```
   1097 ?        00:00:00 udisksd
   1116 ?        00:00:00 gvfs-mtp-volume
   1120 ?        00:00:00 gvfs-gphoto2-vo
   1124 ?        00:00:00 gvfs-afc-volume
   1129 ?        00:00:00 gvfs-goa-volume
   1139 ?        00:00:00 blueman-tray
   1142 ?        00:00:00 gvfsd-trash
   1150 ?        00:00:00 gvfsd-metadata
   1159 ?        00:00:00 obexd
   1167 ?        00:00:00 qterminal
   1170 pts/0    00:00:00 zsh
   1188 ?        00:00:00 kworker/3:1-events
   1189 ?        00:00:00 kworker/2:0-events
   1206 pts/0    00:00:00 sudo
   1207 pts/0    00:00:00 ps

┌──(kali㉿kali)-[/]
└─$ sudo ps -fC KEY
UID          PID    PPID  C STIME TTY          TIME CMD

┌──(kali㉿kali)-[/]
└─$ sudo ps -eF | awk '/KEY/ {print $11}'                                  1 ✗
KEY002-kmrMSsSaaSvbbVz3yW0zaw==
awk

┌──(kali㉿kali)-[/]
└─$ █
```

Figure 2: Screenshot for KEY002.