EX010 Team 2

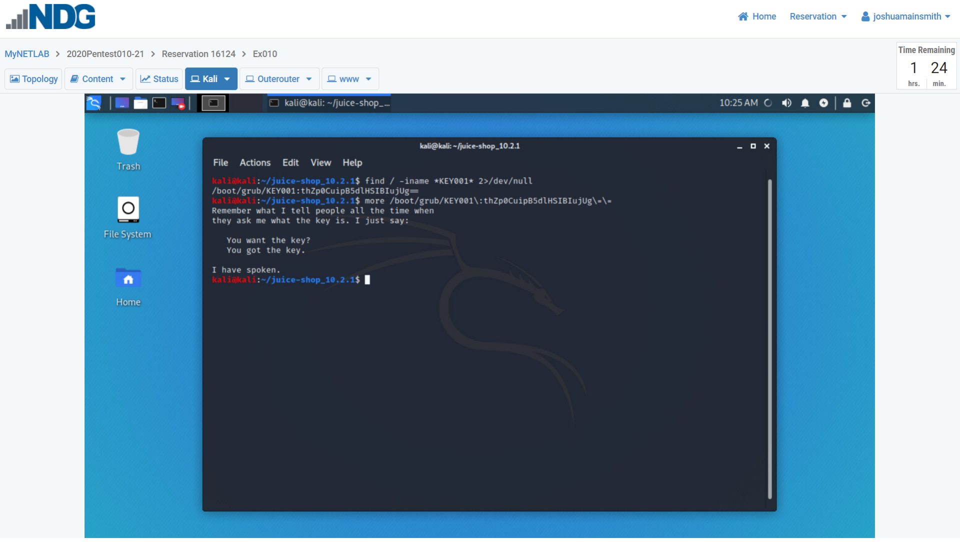
Joshua Main-Smith

2020-09-17

Attack Narrative

KEY001

The hint given to us was that KEY001 was part of a file name and that we should use **find** to search for it.
So, we began by searching the entire machine using the **find** command for a file that probably had the string KEY001 included. We used the flag **-iname**, the case insensitve version of **-name**, along with ***KEY001***. The * surrounding KEY001 are wildcards we included in case KEY001 is located somewhere in the middle of a file name. we were able to find the key this way, but there were a lot of *Permission Denied* instances cluttering the output. For a cleaner output, we followed this guide, resulting in only KEY001 outputting.
The full command used is **find / -iname *KEY001* 2>/dev/null**, which can also be seen in the screenshot below along with the value of the key.



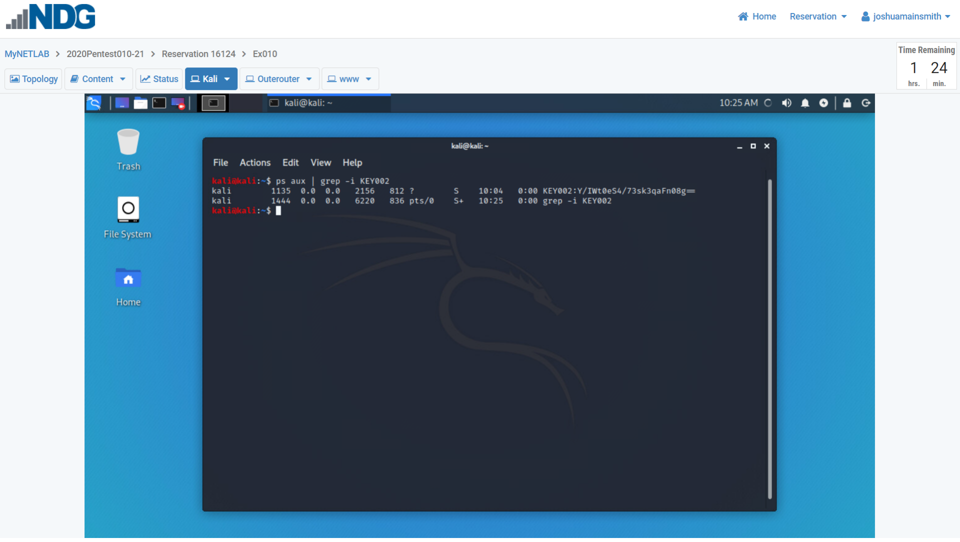
```
kali@kali:~/juice-shop_10.2.1$ find / -iname *KEY001* 2>/dev/null
/boot/grub/KEY001:thZp0CuipB5dlHSIBIujUg==
kali@kali:~/juice-shop_10.2.1$ more /boot/grub/KEY001\:thZp0CuipB5dlHSIBIujUg\=\=
Remember what I tell people all the time when
they ask me what the key is. I just say:

   You want the key?
   You got the key.

I have spoken.
kali@kali:~/juice-shop_10.2.1$ 
```

KEY002

The hint given for finding KEY002 was that the command to be used lifts the ”only yourself” restriction. After a brief Google search, we came across this man page under the **a** flag. This manual page is for the **ps** command, which is used to display active processes.The flags we used were **aux**, with **a** being the ”lift yourself restriction”, **x** lifting the ”must have a tty” restriction. Both of these together show all active processes. The **u** flag is used just for formatting purposes. Doing this alone will show KEY002 among a lot of other active processes. So, we piped this to **grep -i KEY002** (case insensitive) to make the output a little cleaner.
The full command is **ps aux | grep -i KEY002**, as can also be seen in the screenshot below along with the value of KEY002.



```
kali@kali:~$ ps aux | grep -i KEY002
kali        1135  0.0  0.0   2156   812 ?        S    10:04   0:00 KEY002:Y/IWt0eS4/73sk3qaFn08g==
kali        1444  0.0  0.0   6220   836 pts/0    S+   10:25   0:00 grep -i KEY002
kali@kali:~$ 
```

Zoom Meeting Links

September 11, 2020
September 16, 2020 - 1
September 16, 2020 - 2