Blocky walkthrough

Index

List of pictures

Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Reconnaissance

The results of an initial nMap scan are the following:

Figure 1 - nMap scan results

Open ports are 21, 22, 80 and 25565. So, this machine has FTP and SSH services enabled, a web application running on port 80 and a Minecraft service running on port 25565. Also, nMap has revognized Linux as OS, but it didn't identify the version.

The web application can be reached adding a new entry in the $/etc/hosts$ file.

Initial foothold

Analyzing the application I found it is developed using WordPress. Also, I found a name account as shown in the following picture:

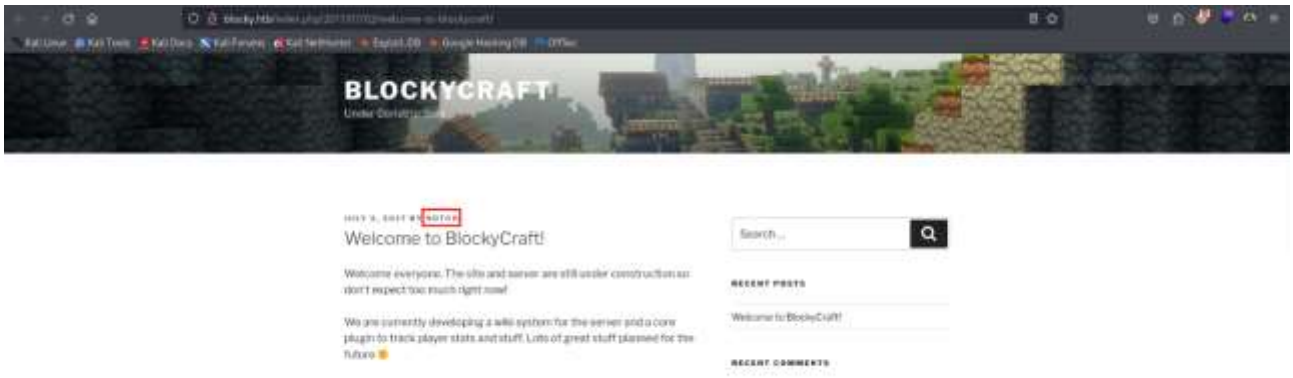

Figure 2 - User found

I run dirbuster to try to find some other interesting content and I found out the $/wiki/$ and $/plugins/$ paths. The interesting one in this case is the second one:

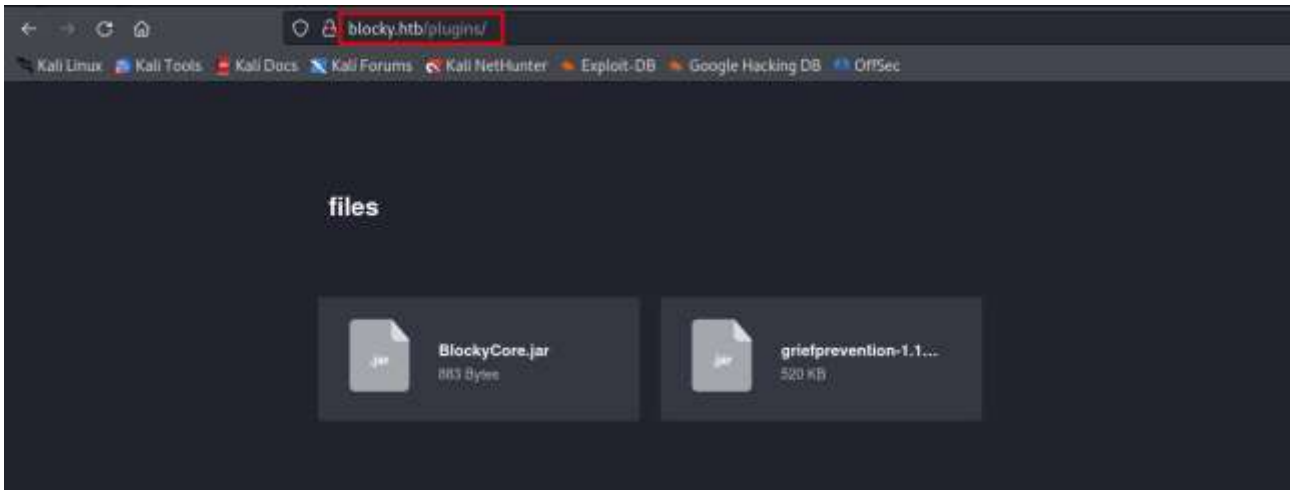

Figure 3 - Plugin paths on the web application

User flag

I tried to analyze these files. So, I decompiled the **BlockyCore.jar** file running the following command:

$$javap\ -c\ BlockyCore$$

Reading the decompiled code, I found out database credentials, as shown in the following figure:

```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ javap -c BlockyCore
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Warning: File ./BlockyCore.class does not contain class BlockyCore
Compiled from "BlockyCore.java"
public class com.myfirstplugin.BlockyCore {
  public java.lang.String sqlHost;

  public java.lang.String sqlUser;

  public java.lang.String sqlPass;

  public com.myfirstplugin.BlockyCore();
    Code:
       0: aload_0
       1: invokespecial #12                 // Method java/lang/Object."<init>":()V
       4: aload_0
       5: ldc           #14                 // String localhost
       7: putfield      #16                 // Field sqlHost:Ljava/lang/String;
      10: aload_0
      11: ldc           #18                 // String root
      13: putfield      #20                 // Field sqlUser:Ljava/lang/String;
      16: aload_0
      17: ldc           #22                 // String 8YsqfCTnvxAUeduzjNSXe22
      19: putfield      #24                 // Field sqlPass:Ljava/lang/String;
      22: return

  public void onServerStart();
    Code:
       0: return

  public void onServerStop();
    Code:
       0: return

  public void onPlayerJoin();
    Code:
       0: aload_0
       1: ldc           #33                 // String TODO get username
       3: ldc           #35                 // String Welcome to the BlockyCraft!!!!!!!
       5: invokevirtual #37                 // Method sendMessage:(Ljava/lang/String;Ljava/lang/String;)V
       8: return

  public void sendMessage(java.lang.String, java.lang.String);
    Code:
       0: return
}
```

Figure 4 - Database credentials

At this point I tried an SSH connection. In the web application I found out a name, now I have a password, so I used these credentials to establish an SSH connection:

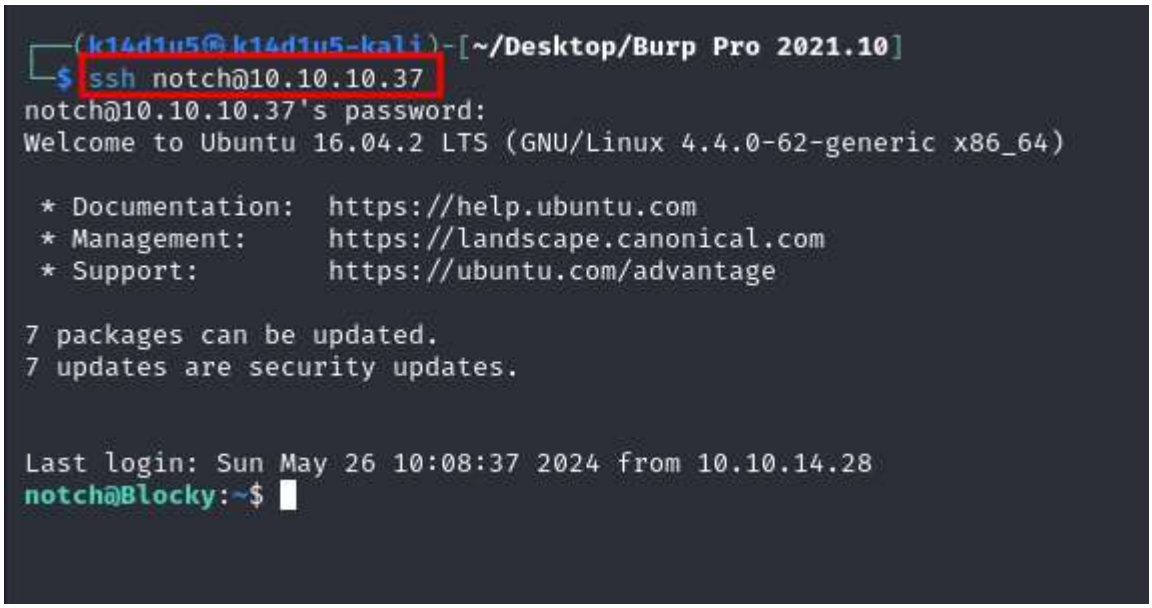

Figure 5 - SSH user connection

I forgot to take a screenshot about the flag, but it is as usual in the user's **home** directory and I was able to retrieve it at this point.

Privilege escalation

The privilege escalation is very easy. Analyzing the $sudo\ -l$ command output, I found out that user can do all he/she wants as sudo. So, the privilege escalation and the root flag are the following:

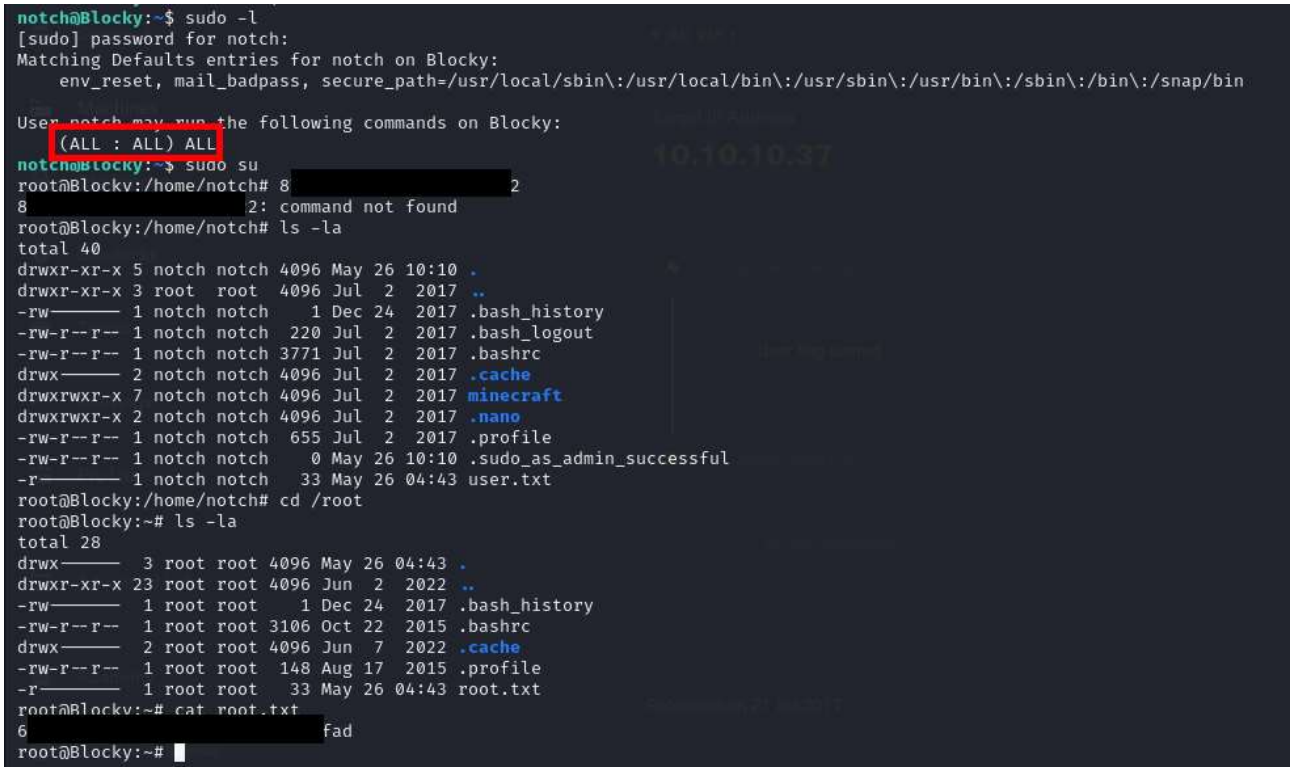

Figure 6 - Privesc and root flag