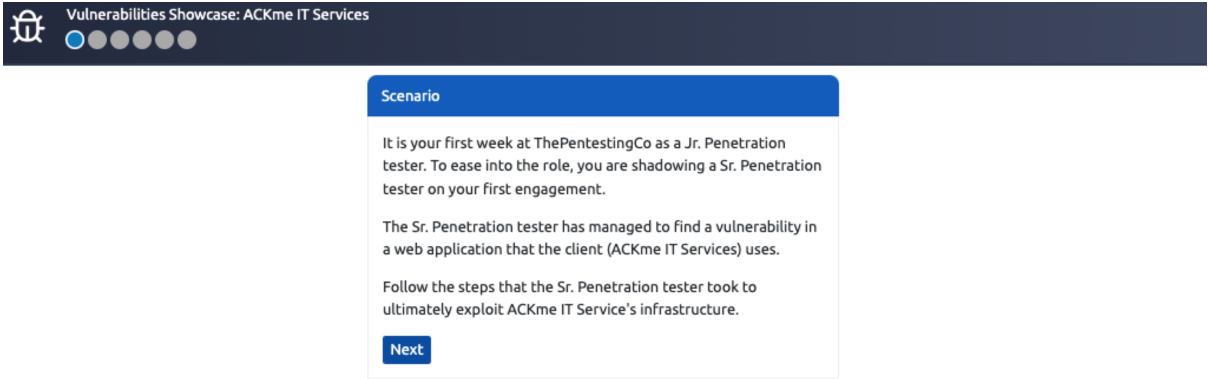
Vulnerability 101

Task 6 Showcase: Exploiting Ackme's Application

Deploy the site associated with this work and follow the procedures taken by the Sr. Penetration Tester to exploit a vulnerability in the infrastructure of ACKme IT Service.

INTRODUCTION

- Test the IP address: **240.228.189.136**
- Any other IP or machine is out of scope

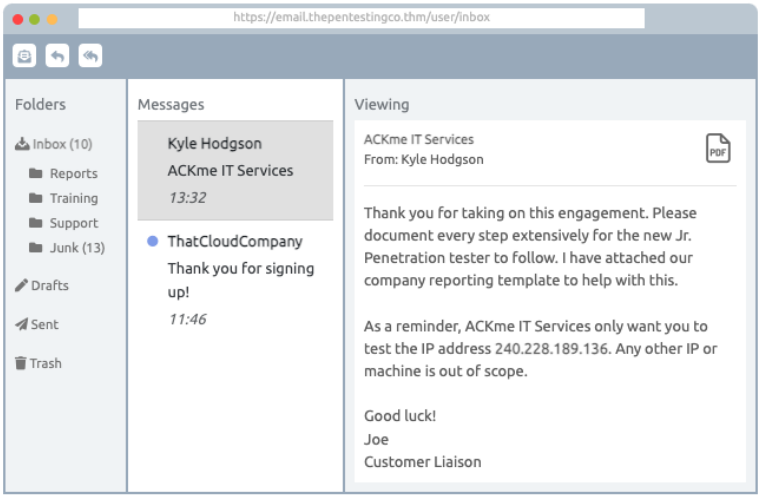


Scenario

It is your first week at ThePentestingCo as a Jr. Penetration tester. To ease into the role, you are shadowing a Sr. Penetration tester on your first engagement.

The Sr. Penetration tester has managed to find a vulnerability in a web application that the client (ACKme IT Services) uses.

Follow the steps that the Sr. Penetration tester took to ultimately exploit ACKme IT Service's infrastructure.



Kyle Hodgson
ACKme IT Services
13:32

ThatCloudCompany
Thank you for signing up!
11:46

ACKme IT Services
From: Kyle Hodgson

Thank you for taking on this engagement. Please document every step extensively for the new Jr. Penetration tester to follow. I have attached our company reporting template to help with this.

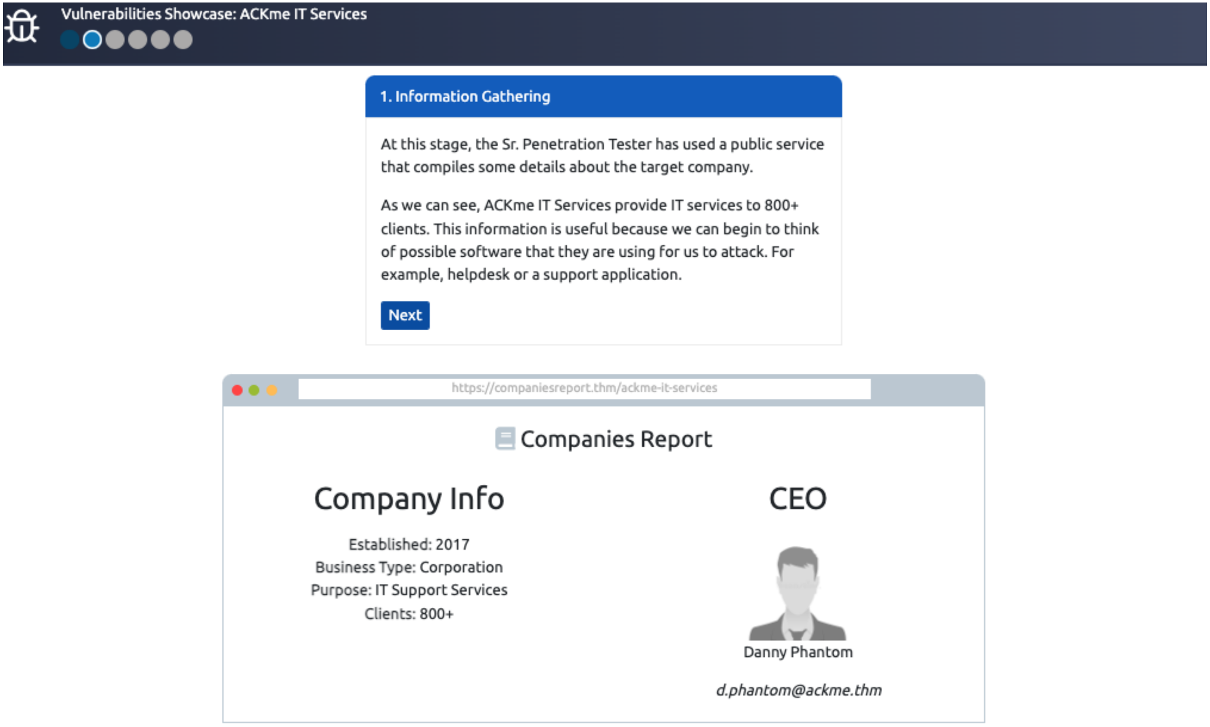
As a reminder, ACKme IT Services only want you to test the IP address 240.228.189.136. Any other IP or machine is out of scope.

Good luck!
Joe
Customer Liaison

(1) INFORMATION GATHERING

- **Established:** 2017
- **Business Type:** Corporation
- **Purpose:** IT Support Services
- **Clients:** 800+

This knowledge is significant because it allows us to **start thinking about what software they might be employing to attack us**. As an example, consider a **helpdesk or a support program**.



Vulnerabilities Showcase: ACKme IT Services

1. Information Gathering

At this stage, the Sr. Penetration Tester has used a public service that compiles some details about the target company.

As we can see, ACKme IT Services provide IT services to 800+ clients. This information is useful because we can begin to think of possible software that they are using for us to attack. For example, helpdesk or a support application.

https://companiesreport.thm/ackme-it-services

Companies Report

Company Info

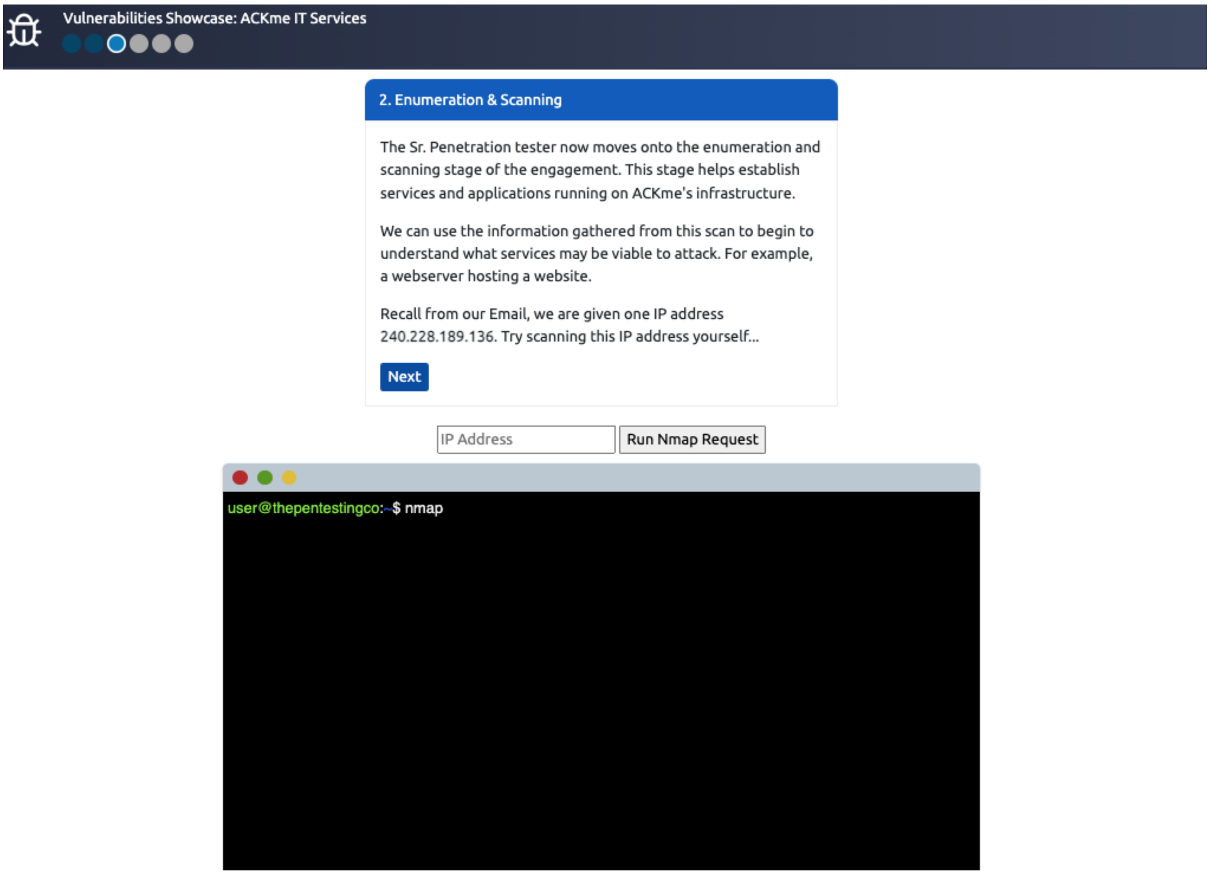
Established: 2017
Business Type: Corporation
Purpose: IT Support Services
Clients: 800+

CEO

Danny Phantom

d.phantom@ackme.thm

(2) ENUMERATION & SCANNING



2. Enumeration & Scanning

The Sr. Penetration tester now moves onto the enumeration and scanning stage of the engagement. This stage helps establish services and applications running on ACKme's infrastructure.

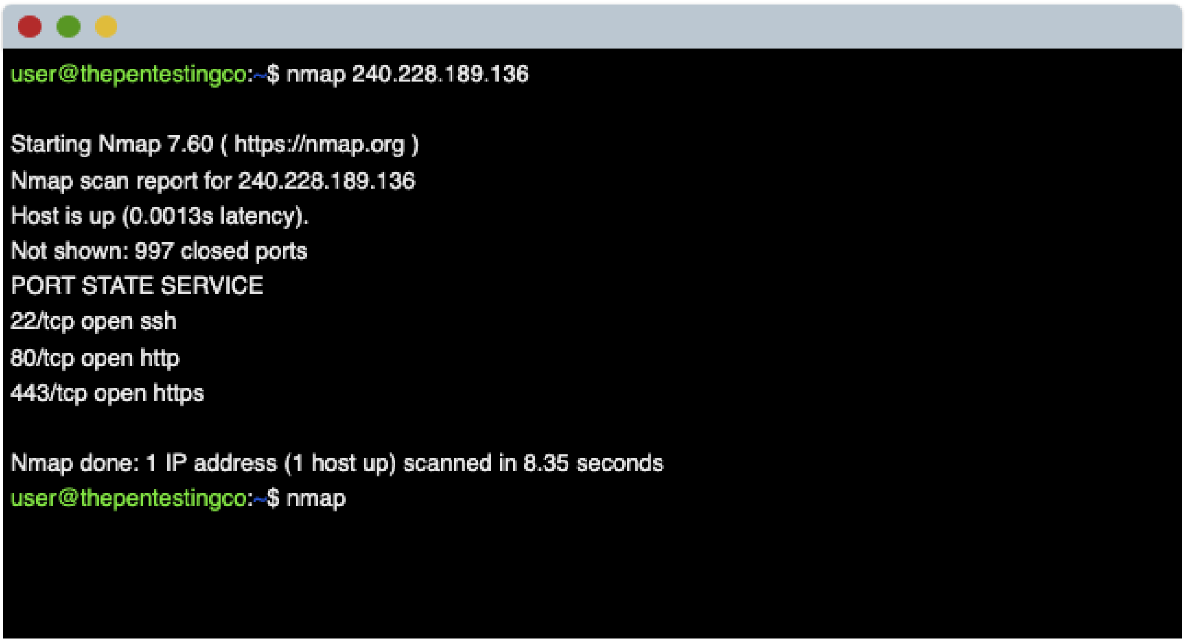
We can use the information gathered from this scan to begin to understand what services may be viable to attack. For example, a webserver hosting a website.

Recall from our Email, we are given one IP address 240.228.189.136. Try scanning this IP address yourself...

```
user@thepentestingco:~$ nmap
```

3)Open Ports Found:

- Port 22 (SSH)
- Port 80 (HTTP)
- Port 443 (HTTPS)



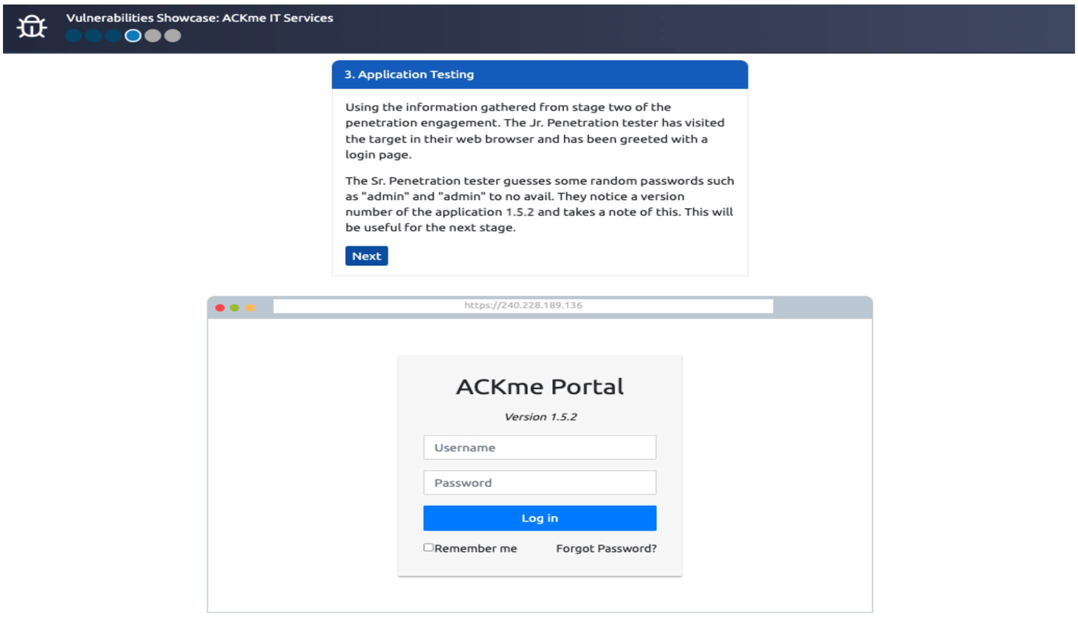
```
user@thepentestingco:~$ nmap 240.228.189.136

Starting Nmap 7.60 ( https://nmap.org )
Nmap scan report for 240.228.189.136
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 8.35 seconds
user@thepentestingco:~$ nmap
```

Nmap Result

(3) APPLICATION TESTING

We initially discovered three open ports and are now able to access the “portal,” and we can normally test it using a random login and password, such as “**admin:admin**” to begin.However, the application has a “**version number**,” which might be very beneficial.

- **Version Number:** 1.5.2



3. Application Testing

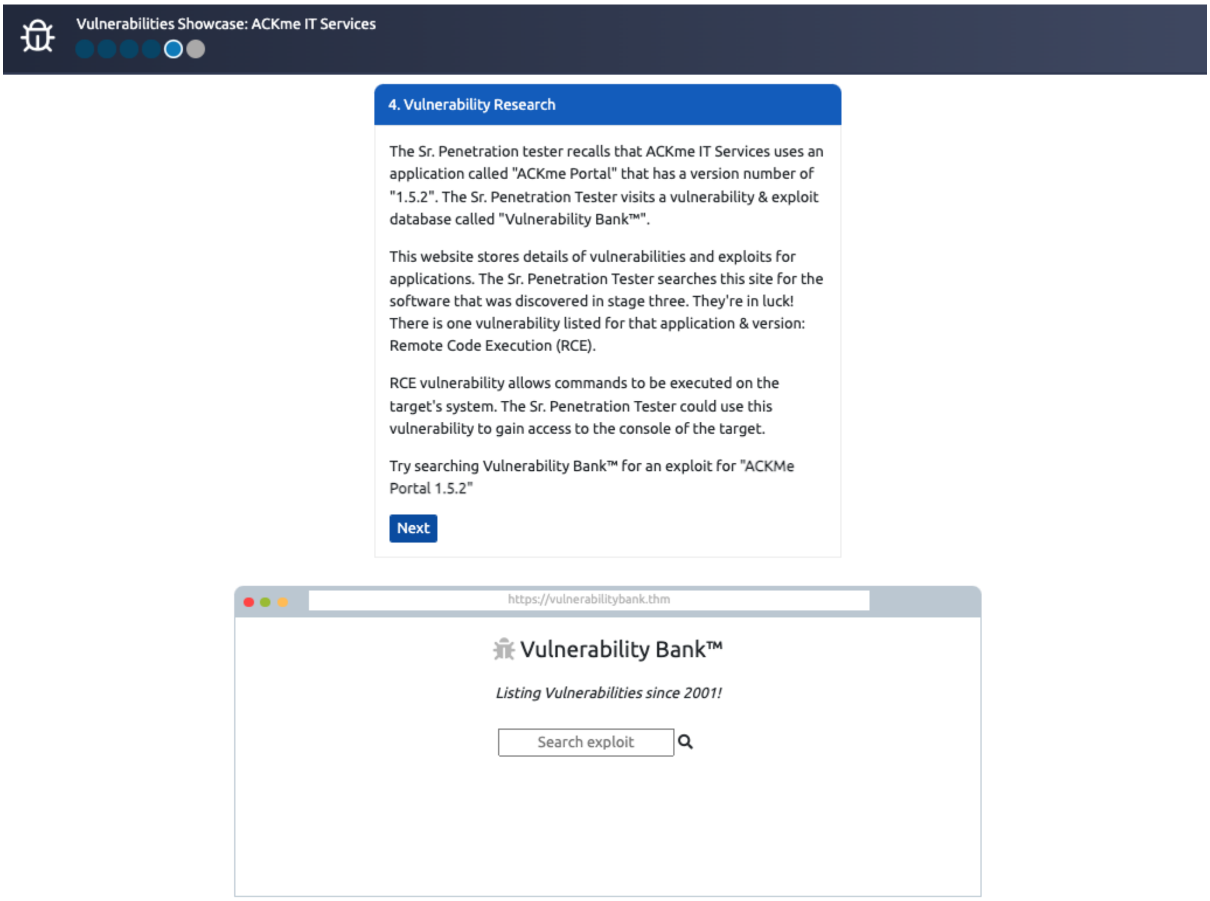
Using the information gathered from stage two of the penetration engagement. The Jr. Penetration tester has visited the target in their web browser and has been greeted with a login page.

The Sr. Penetration tester guesses some random passwords such as "admin" and "admin" to no avail. They notice a version number of the application 1.5.2 and takes a note of this. This will be useful for the next stage.

(4) VULNERABILITY RESEARCH

It’s the same as “Exploit-DB,” which allows us to search the “vulnerability bank” for vulnerabilities on the site.

- **Search:** ACKMe Portal 1.5.2



4. Vulnerability Research

The Sr. Penetration tester recalls that ACKme IT Services uses an application called "ACKme Portal" that has a version number of "1.5.2". The Sr. Penetration Tester visits a vulnerability & exploit database called "Vulnerability Bank™".

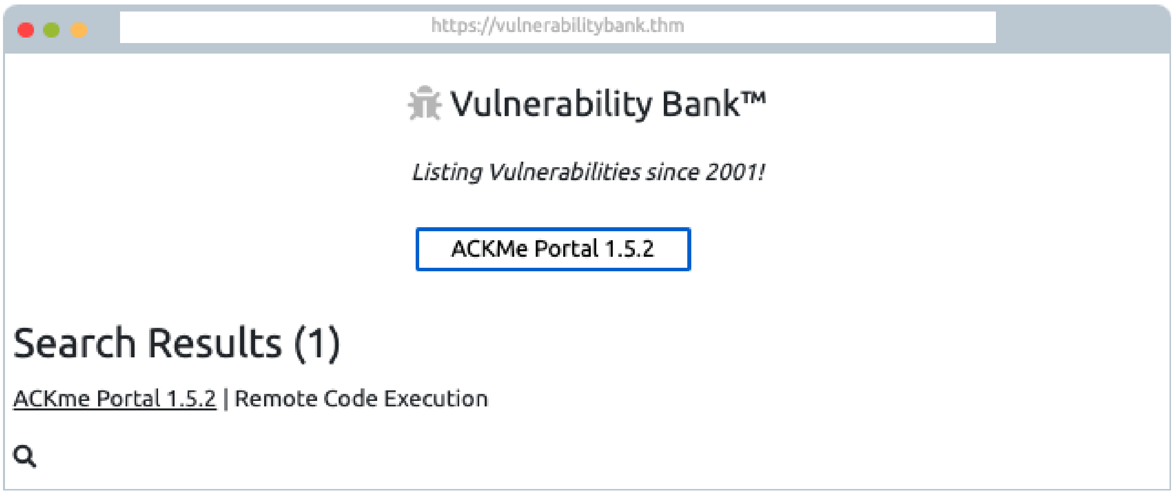
This website stores details of vulnerabilities and exploits for applications. The Sr. Penetration Tester searches this site for the software that was discovered in stage three. They're in luck! There is one vulnerability listed for that application & version: Remote Code Execution (RCE).

RCE vulnerability allows commands to be executed on the target's system. The Sr. Penetration Tester could use this vulnerability to gain access to the console of the target.

Try searching Vulnerability Bank™ for an exploit for "ACKMe Portal 1.5.2"

Next
https://vulnerabilitybank.thm
Vulnerability Bank™
Listing Vulnerabilities since 2001!
Search exploit

- **Found:** Remote Code Execution (RCE)



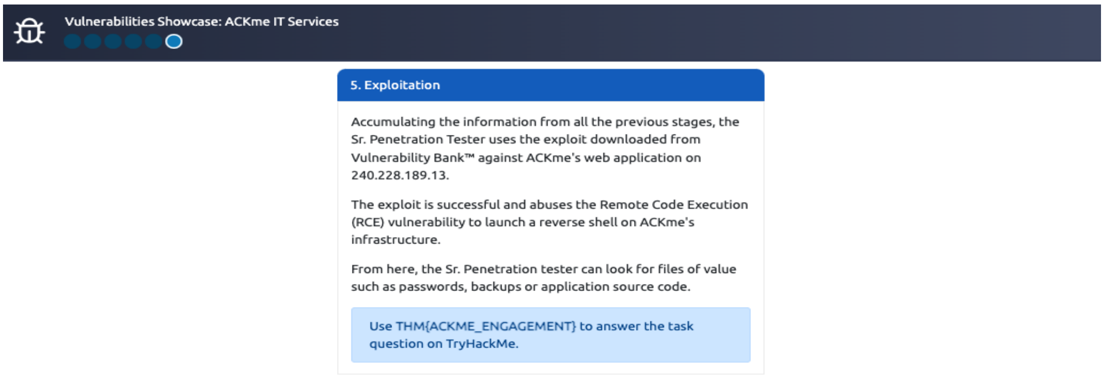
https://vulnerabilitybank.thm
Vulnerability Bank™
Listing Vulnerabilities since 2001!
ACKMe Portal 1.5.2

Search Results (1)

ACKme Portal 1.5.2 | Remote Code Execution

(5) EXPLOITATION

Utilize the exploit downloaded from the “Vulnerability Bank” to attack the “victim.” In this situation, it is “RCE,” and as a result, we can conduct a reverse shell attack on the victim, obtaining files and information such as passwords, secret files, application source code, and so on.



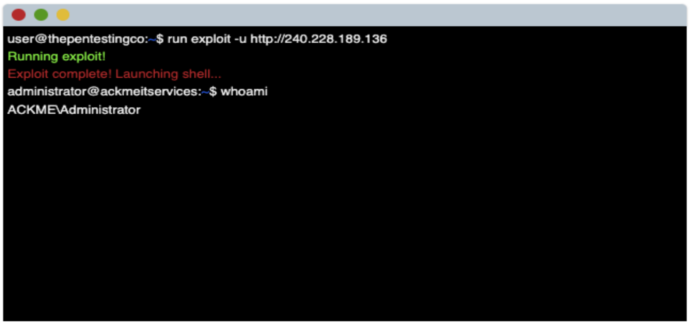
5. Exploitation

Accumulating the information from all the previous stages, the Sr. Penetration Tester uses the exploit downloaded from Vulnerability Bank™ against ACKme's web application on 240.228.189.13.

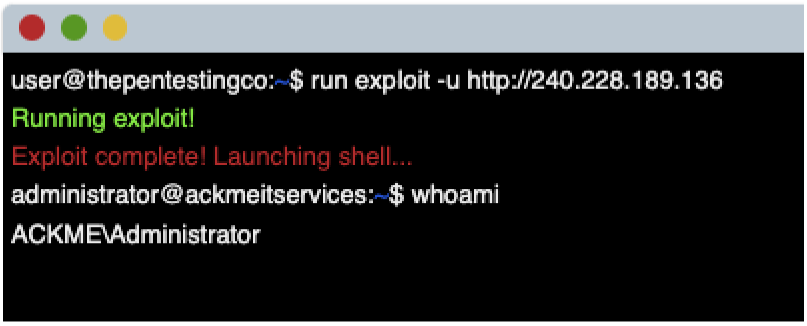
The exploit is successful and abuses the Remote Code Execution (RCE) vulnerability to launch a reverse shell on ACKme's infrastructure.

From here, the Sr. Penetration tester can look for files of value such as passwords, backups or application source code.

Use THM{ACKME_ENGAGEMENT} to answer the task question on TryHackMe.



```
user@thepentestingco:~$ run exploit -u http://240.228.189.136
Running exploit!
Exploit complete! Launching shell...
administrator@ackmeitservices:~$ whoami
ACKME\Administrator
```



```
user@thepentestingco:~$ run exploit -u http://240.228.189.136
Running exploit!
Exploit complete! Launching shell...
administrator@ackmeitservices:~$ whoami
ACKME\Administrator
```

Follow along with the showcase of exploiting ACKme’s application to the end to retrieve a flag. What is this flag?

Answer: THM{ACKME_ENGAGEMENT}