### **TryHackMe: Juicy Details**

#### **Scenario:**

**Introduction**

You were hired as a SOC Analyst for one of the biggest Juice Shops in the world and an attacker has made their way into your network.

Your tasks are:

* Figure out what techniques and tools the attacker used
* What endpoints were vulnerable
* What sensitive data was accessed and stolen from the environment

An IT team has sent you a **zip file** containing logs from the server. Download the attached file, type in “I am ready!” and get to work! There’s no time to lose!

#### **Task-1**

**1.Are you ready?**

**Answer:** I am ready!

#### **Task-2**

**Reconnaissance**

Analyze the provided log files.

Look carefully at:

* What tools the attacker used
* What endpoints the attacker tried to exploit
* What endpoints were vulnerable

1. **What tools did the attacker use? (Order by the occurrence in the log)**

To find the tools used by the attacker we can check the access.log file, more specifically the user agent section of the logs. But If we cat the output there are too many logs to manually check. Hence we use the cut command

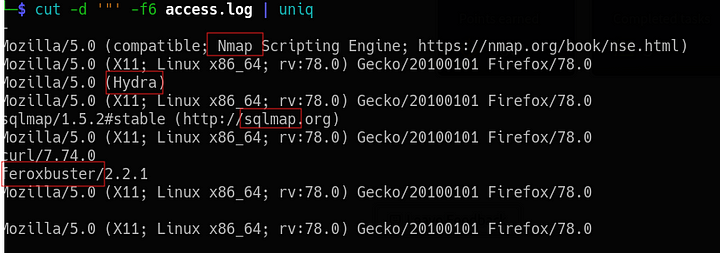
cut -d '"' -f6 access.log | uniq

cut: this command is used to extract sections from each line of input data.

d: specifies the delimiter which is the double quote (“) in this case

f: specifies the field to cut or the field to display

uniq: only displays the uniq values

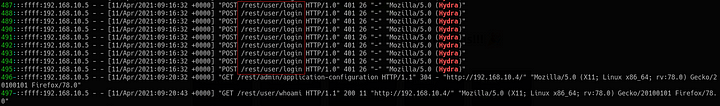
cut command output

Answer: Nmap, Hydra, sqlmap, feroxbuster.

**2.What endpoint was vulnerable to a brute-force attack?**

This can also be found in the access log file. we can cat the access.log file and the grep the contents for Hydra which is a tool widely used for brute-force attacks

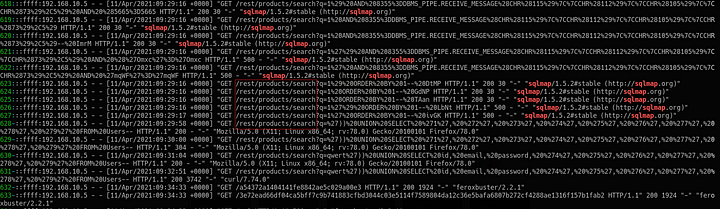
cat access.log | grep Hydra

output showing the endpoint vulnerable to Brute-Force

**Answer:** /rest/user/login

**3.What endpoint was vulnerable to SQL injection?**

cat access.log | grep sqlmap

Output showing SQLi vulnereable endpoint

**Answer:** /rest/products/search

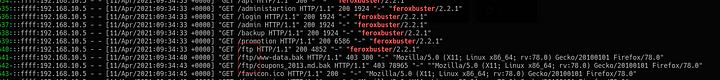
**4.What parameter was used for the SQL injection?**

The answer to this can be found in the above output.

**Answer:** q

**5.What endpoint did the attacker try to use to retrieve files? (Include the /)**

The answer to this can be seen by using the cat command to output the access.log file and then grep for feroxbuster. We can see that after feroxbuster the attacker was able to obtain the files from this endpoint.

output showing the endpoint used to retrieve files.

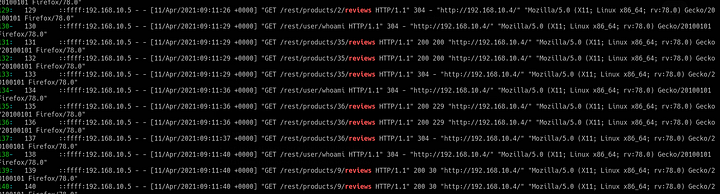
Answer: /ftp

#### **Task-3**

1. What section of the website did the attacker use to scrape user email addresses?

I had to check the hint for this question, which says “Where can customers usually comment on a shopping website”. With this hint I searched the access.log file for “reviews”.

cat access.log | grep reviews

output showing attacker accessing the reviews page

From the output we can see that the attcker accessed different user reviews

**Answer:** product reviews

2.Was their brute-force attack successful? If so, what is the timestamp of the successful login? (Yay/Nay, 11/Apr/2021:09:xx:xx +0000)

I checked for the logs in which Hydra was used and then searched for a 200 response.

cat access.log | grep Hydra | grep 200

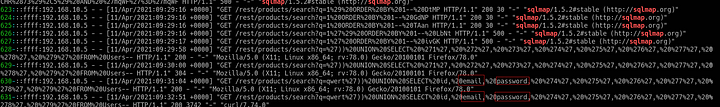
Output showing successful Brute-Force login

**Answer:** yay, 11/Apr/2021:09:16:31 +0000

**3.What user information was the attacker able to retrieve from the endpoint vulnerable to SQL injection?**

For this I checked the logs which were generated after the attacker finished with sqlmap.

cat access.log | grep sqlmap -n10

Output showing the information accessed by attacker through SQLi

Answer: email, password

**4.What files did they try to download from the vulnerable endpoint?**

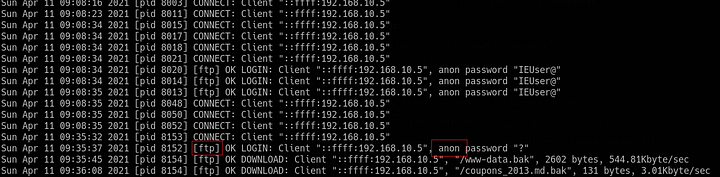
This was already visible in the output when we checked for the endpoint used to extract file in Task-2 question 5

Answer: coupons\_2013.md.bak, www-data.bak

**5.What service and account name were used to retrieve files from the previous question? (service, username)**

For this we can check the vsftpd.log file, which will contain the activity of the ftp server.

cat vsftpd.log

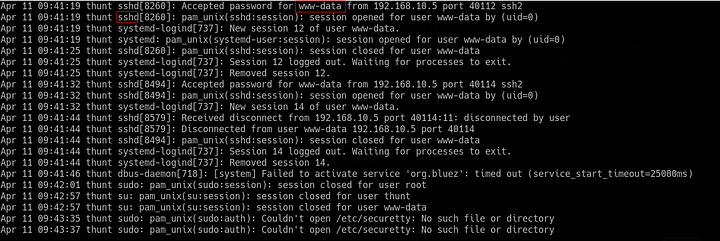
output from the vsftpd log file

**Answer:** ftp, anonymous

**6.What service and username were used to gain shell access to the server? (service, username)**

For this we can check the auth.log file.

cat auth.log

output of the auth.log file

**Answer:** ssh, www-data

This is the end of the room.