Various tools from Kali

1. Information Gathering

Nmap

Network Mapper is a network exploration tool that can find the services and the version running on the website. It tells the ports open on the website so that the attacker can figure out how to exploit the weakness.

A scan of https://demo.testfire.net/ gives us the following result.

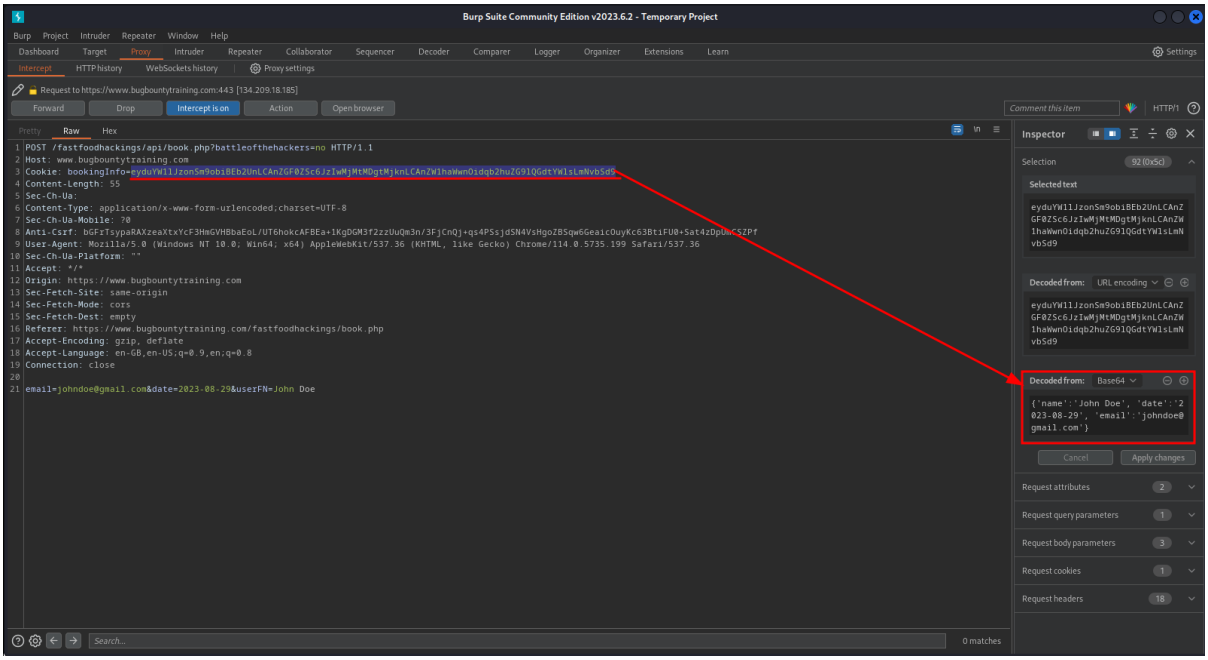
```
dagr8est@kali:~$ nmap -sV 65.61.137.117
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 03:25 IST
Nmap scan report for 65.61.137.117
Host is up (0.22s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE   VERSION
80/tcp   open   http      Apache Tomcat/Coyote JSP engine 1.1
443/tcp  open   ssl/http  Apache Tomcat/Coyote JSP engine 1.1
8080/tcp open   http      Apache Tomcat/Coyote JSP engine 1.1
8443/tcp closed https-alt

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.74 seconds
```

2. Web Application Analysis

Burpsuite

It is a set of tools that allows the user to perform various tests on the websites. It combines tools like proxy, scanner, intruder, interceptor and much more. It is used by a lot of security professionals.

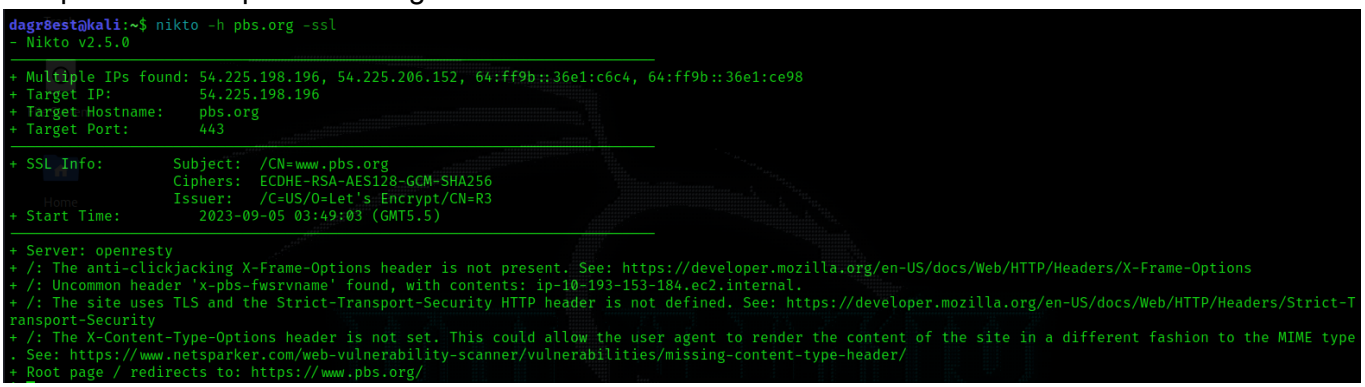
On fast food hackings, we can use the interceptor module to intercept the booking request and then use the built in base64 decoder to find out the data being transmitted.



3. Vulnerability Analysis

Nikto

It is an open source web server vulnerability scanner. It is used to identify security issues. It provides a comprehensive report informing the user about the software and vulnerabilities.



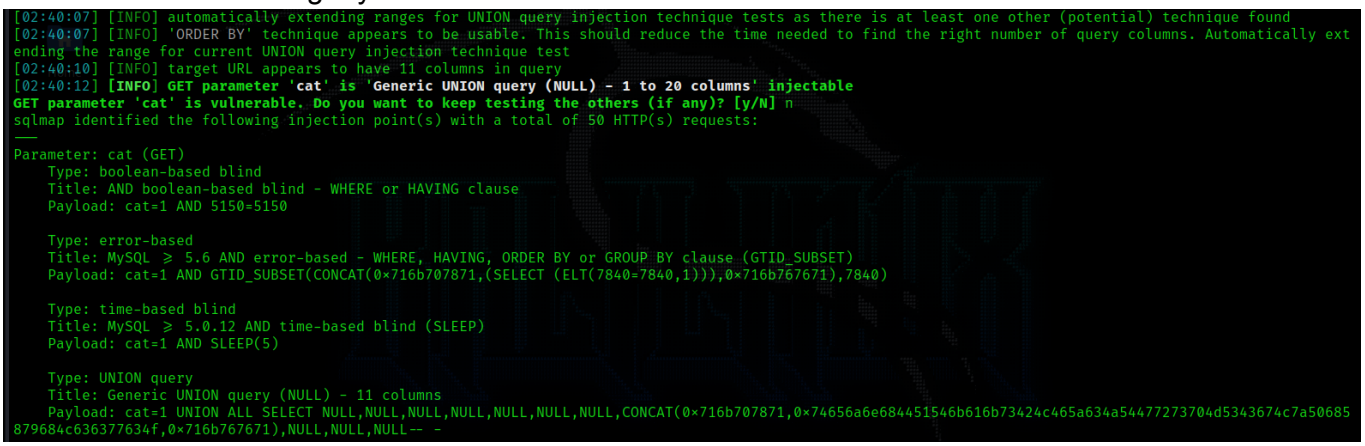
A scan of pbs.org yields the following result.

4. Database Assessment

SQLMap

This application can be used to detect and exploit SQL injection flaws. It can automatically scan the web page for multiple types of databases and try the necessary types of exploits.

While testing http://testphp.vulnweb.com/listproducts.php?cat=1 with SQLMap, it automatically detects that the website is using MySQL and there are some vulnerabilities.

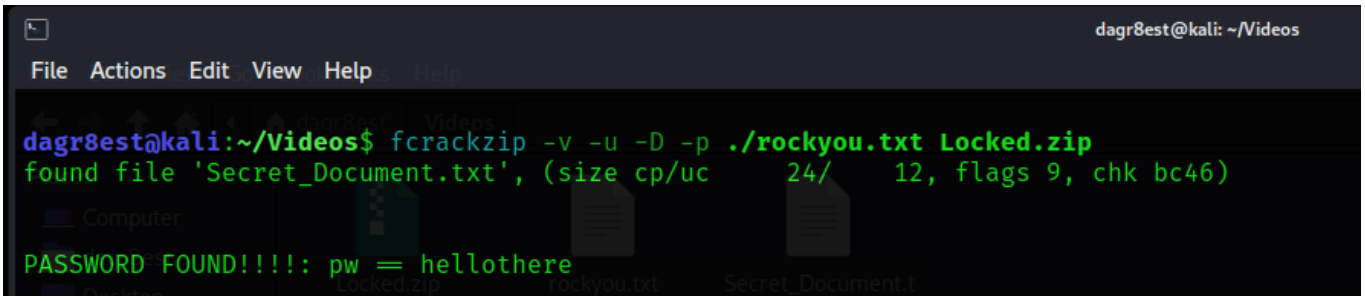


5. Password Attacks

fcrackzip

This tool is used to brute force the password of a zip file. It is very efficient and allows users to crack open locked zip files.

There is a zip file with a password lock (Locked.zip) and a wordlist (rockyou.txt). We can use the brute force function in fcrackzip to find the password of the zip file.



The password of the zip file is found and displayed.

6. Wireless Attacks

fern wifi cracker

It is a tool included in Kali linux that allows users to assess the security of a wireless network. It can be used to crack WEP, WPA and WPA2 keys, perform deauthentication attacks and capture network packets.

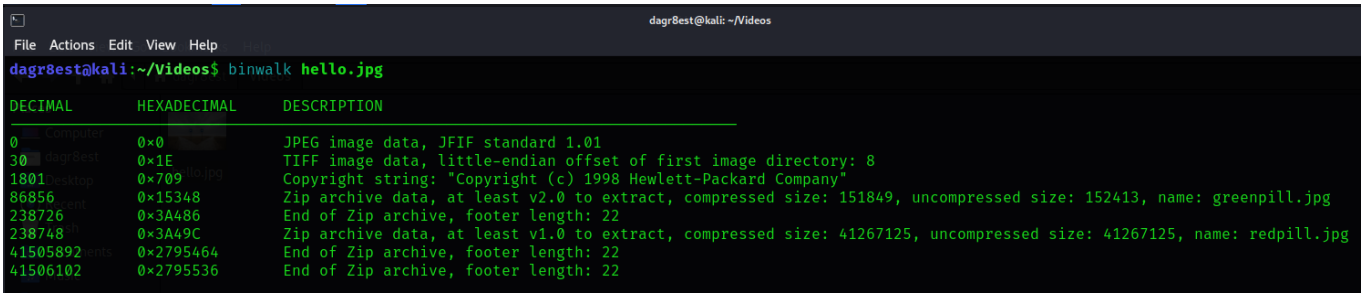
7. Forensics

Binwalk

This is a firmware analysis tool. It can tell the user what data is enclosed within the file.

This is a photo from a CTF event.

Just by looking at it, we can't see anything. If we run binwalk on this image, we can see if there are any files that are hidden inside it.



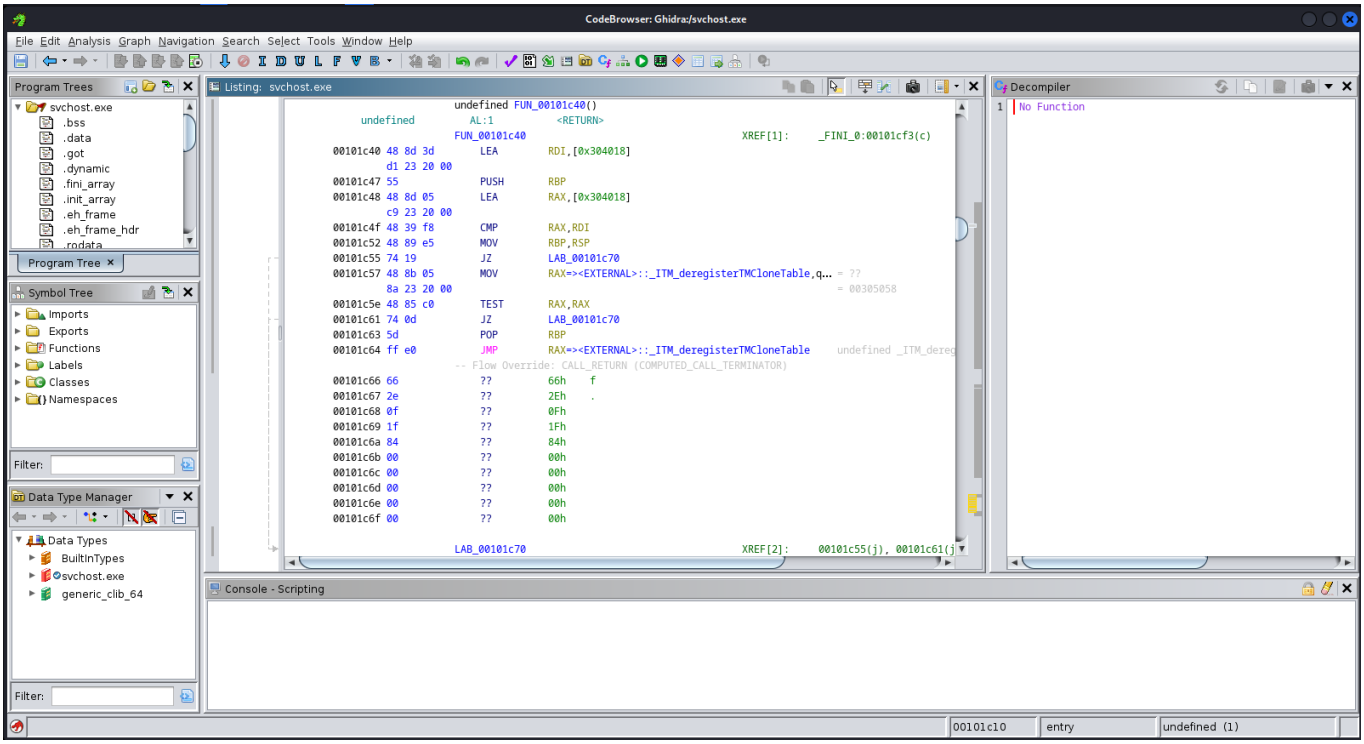
We can see that this image is actually a zip file with other images hidden inside it.

8 . Reverse Engineering

Ghidra

This is an open source reverse engineering designed by the NSA. It decompiles the binaries into a language that is human understandable and allows the engineers to understand how the program works.

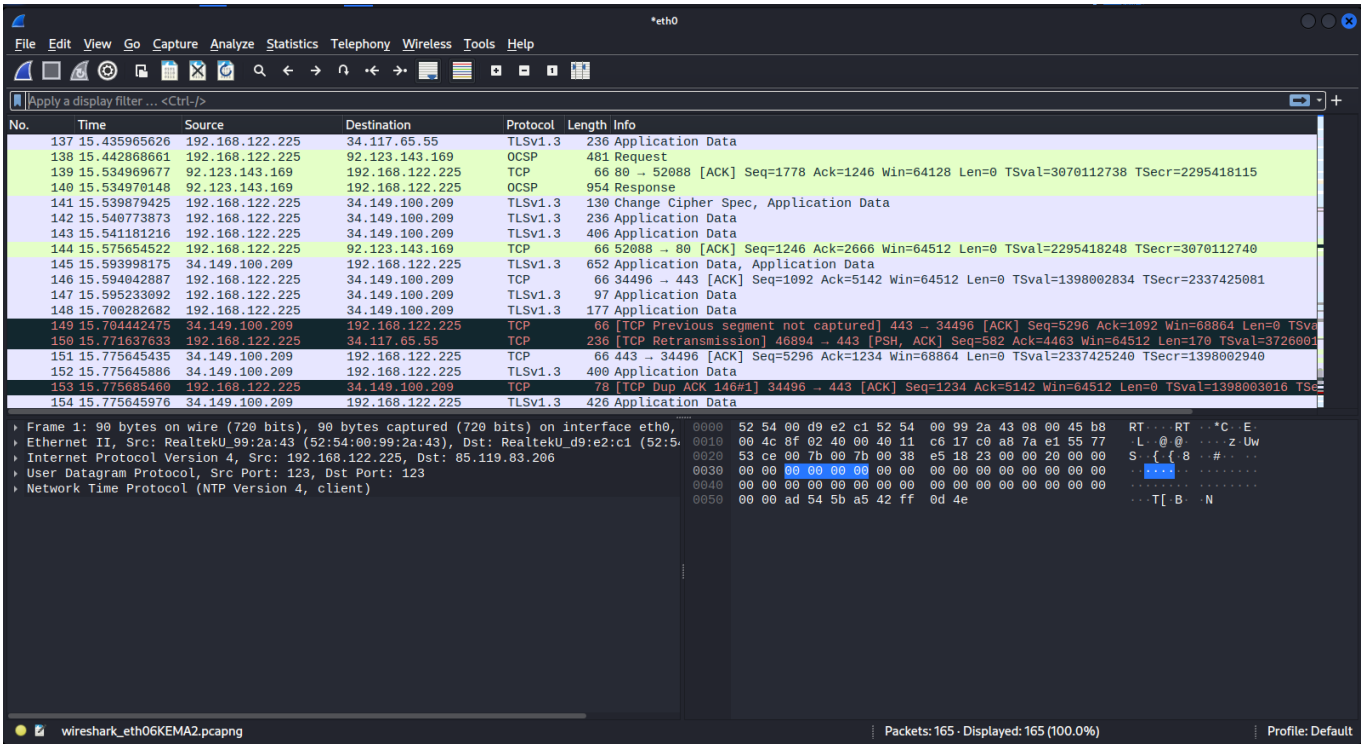
Reverse engineering a sample exe file gives the following code which can be viewed in the code browser



9. Sniffing & Spoofing

Wireshark

It is an open source network protocol analyser. It allows the user to capture data packets being transmitted over a network. This allows them to analyse the potential security threats for enhanced network security.



10. Exploitation Tools

Metasploit Framework

This is an open-source penetration testing tool for assessing and exploiting vulnerabilities in computer systems. It equips security professionals with a vast array of exploits, payloads, and auxiliary modules. Its user-friendly interface and extensive database make it an essential resource for ethical hacking and security assessments.

11. Social Engineering Tools

Social-Engineer Toolkit

It is an open source penetration testing toolkit that assists ethical hackers to execute social engineering attacks. It offers a lot of attack vectors like spear-phishing and credential harvesting. It is mainly used to assess an organisation's susceptibility to social engineering threats.