

# 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

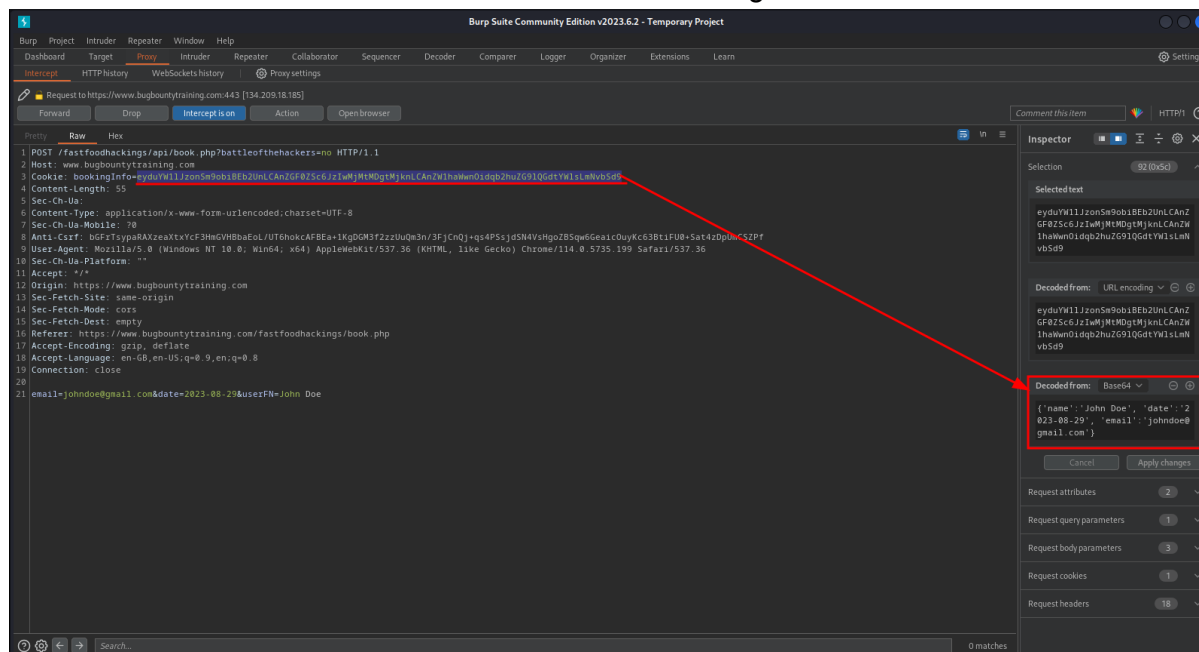
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.74 seconds
```

## 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.

```
dagr8est@kali:~$ nikto -h pbs.org -ssl
- Nikto v2.5.0

+ Multiple IPs found: 54.225.198.196, 54.225.206.152, 64:ff9b::36e1:c6c4, 64:ff9b::36e1:ce98
+ Target IP: 54.225.198.196
+ Target Hostname: pbs.org
+ Target Port: 443

+ SSL Info: Subject: /CN=www.pbs.org
           Ciphers: ECDHE-RSA-AES128-GCM-SHA256
           Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Start Time: 2023-09-05 03:49:03 (GMT.5)

+ Server: openresty
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-pbs-fwsrvname' found, with contents: ip-10-193-153-184.ec2.internal.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.pbs.org/
```

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.

```
[02:40:07] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[02:40:07] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[02:40:10] [INFO] target URL appears to have 11 columns in query
[02:40:12] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 50 HTTP(s) requests:

Parameter: cat (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: cat=1 AND 5150=5150

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: cat=1 AND GTID_SUBSET(CONCAT(0x716b707871,(SELECT (ELT(7840=7840,1))),0x716b767671),7840)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
  Payload: cat=1 AND SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b707871,0x74656a6e684451546b616b73424c465a634a54477273704d5343674c7a50685879684c636377634f,0x716b767671),NULL,NULL,NULL--
```

## 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.

```
File Actions Edit View Help Help
dagr8est@kali: ~/Videos
dagr8est@kali:~/Videos$ fcrackzip -v -u -D -p ./rockyou.txt Locked.zip
found file 'Secret_Document.txt', (size cp/uc 24/ 12, flags 9, chk bc46)
PASSWORD FOUND!!!!: pw = hellothere
```

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.

```
dagr8est@kali: ~/Videos
File Actions Edit View Help
dagr8est@kali:~/Videos$ binwalk hello.jpg

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0             0x0          JPEG image data, JFIF standard 1.01
30            0x1E         TIFF image data, little-endian offset of first image directory: 8
1801          0x709        Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"
86856         0x15348      Zip archive data, at least v2.0 to extract, compressed size: 151849, uncompressed size: 152413, name: greenpill.jpg
238726        0x3A486      End of Zip archive, footer length: 22
238748        0x3A49C      Zip archive data, at least v1.0 to extract, compressed size: 41267125, uncompressed size: 41267125, name: redpill.jpg
41505892      0x2795464    End of Zip archive, footer length: 22
41506102      0x2795536    End of Zip archive, footer length: 22
```

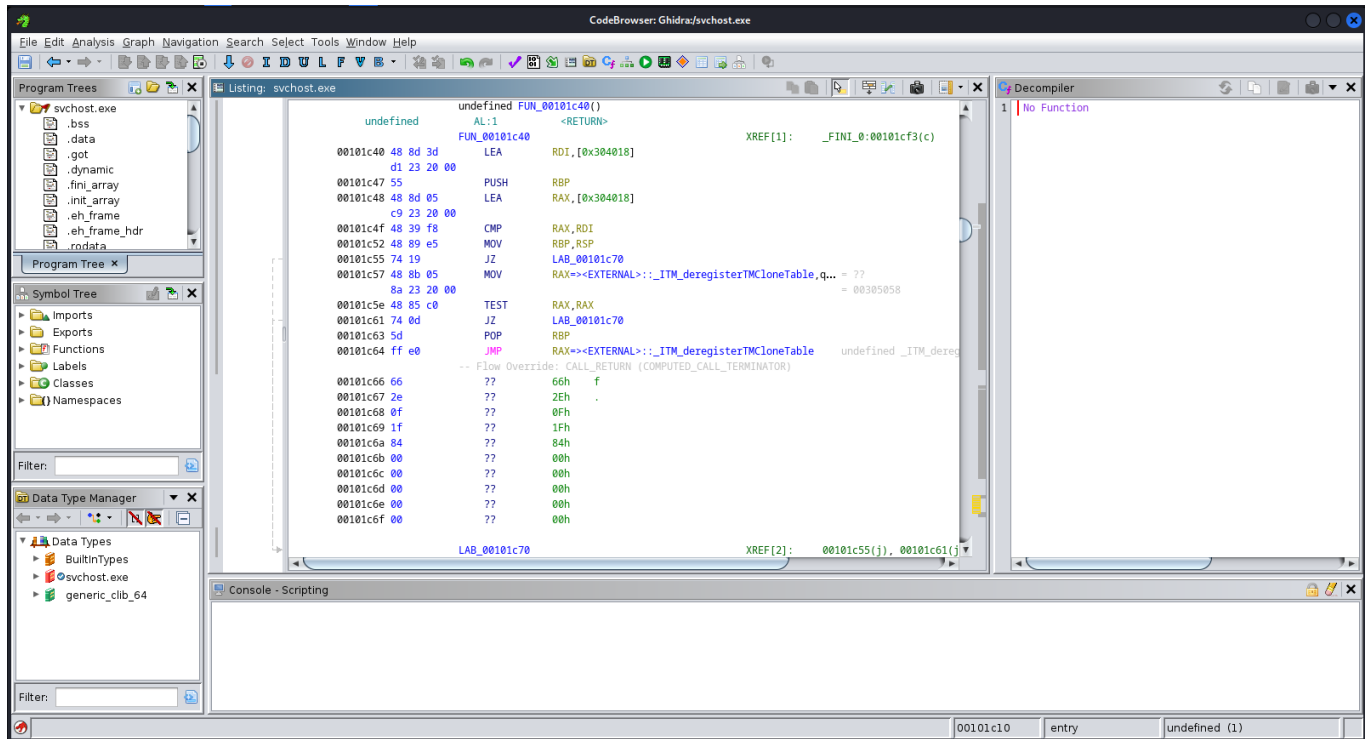
We can see that this image is actually a zip file with other images hidden inside it.

## 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.

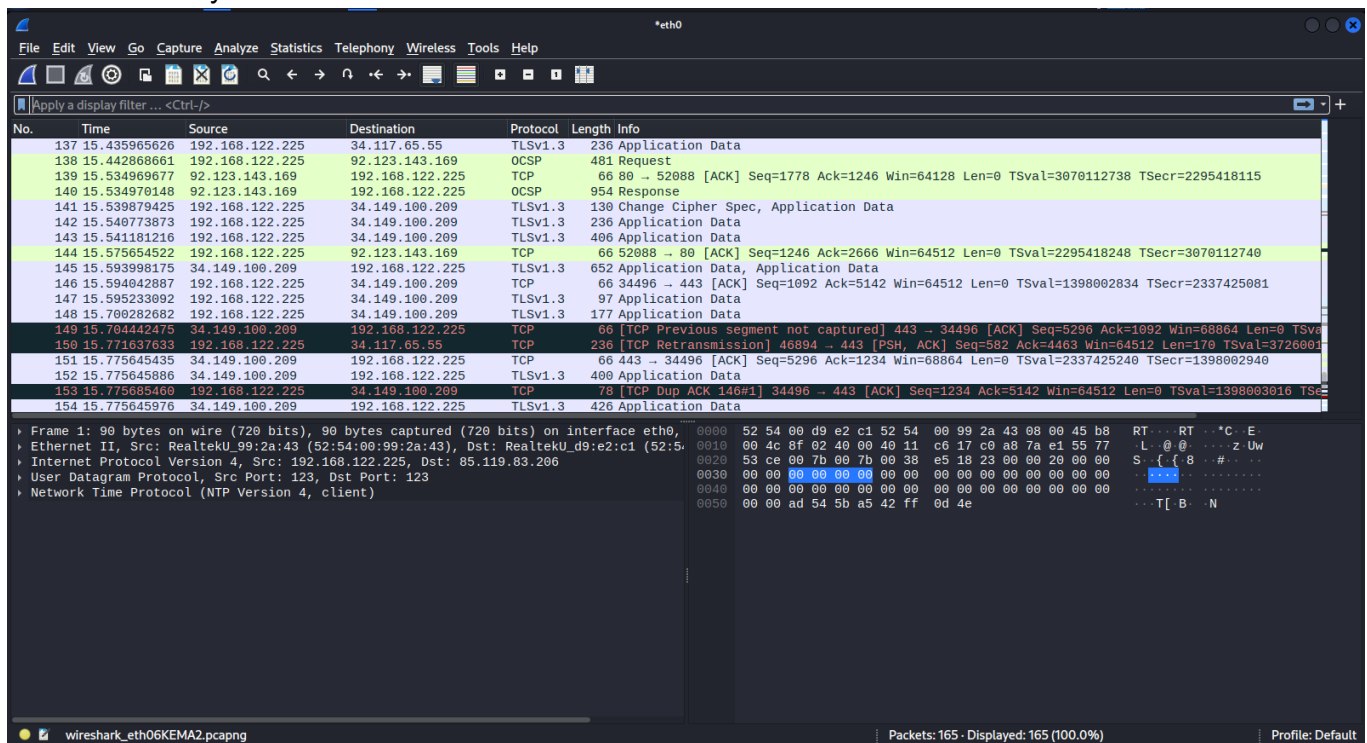
Reverse engineering a sample exe file gives the following code which can be viewed in the code browser



## 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.

