ShadowFox's

Cyber Security Internship

Task Report

By

Sumit Vishwambhar

August B1

Table of contents

Task level (**Beginner**):

1. Find all the ports that are open on the website http://testphp.vulnweb.com/
2. Brute force the website http://testphp.vulnweb.com/ and find the directories that are present in the website.
3. Make a login in the website http://testphp.vulnweb.com/ and intercept the network traffic using wireshark and find the credentials that were transferred through the network.
    - Definition
    - Commands
    - Findings
    - Screenshots
    - Mitigation

Task level (**Intermediate**):

1. A file is encrypted using Veracrypt (A disk encryption tool). Decode the password and enter in the veracrypt to unlock the file and find the secret code in it.
2. Find the entry point address of the executable using PE explorer tool and provide the value as the answer as screenshot.
3. Make a deauth attack in your own network and capture the handshake of the network connection between the device and the router and crack the password for the wifi. To crack the password create a wordlist that can include the password of your network.

    - Findings

Task Level (Beginner):

1) **Find all the ports that are open on the website http://testphp.vulnweb.com/**

Step 1 : Open Kali Linux Terminal using the application menu or by pressing Ctrl + Alt + T shortcut key.

Step 2 : Run the nmap command to check for open ports on the website testphp.vulnweb.com.

```
┌──(sumitvish㉿kali)-[~]
└─$ nmap -p- testphp.vulnweb.com
```

Step 3 : Wait for Namp to finish the scan. It takes some time to scan ports. when the scan starts, press the “Enter” key to check the scan’s progress.

```
┌──(sumitvish㉿kali)-[~]
└─$ nmap -p- testphp.vulnweb.com
Starting Nmap 7.91 ( https://nmap.org ) at 2024-08-30 15:29 IST
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 3.50% done; ETC: 15:48 (0:18:24 remaining)
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 4.59% done; ETC: 15:46 (0:15:57 remaining)
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 9.36% done; ETC: 15:46 (0:15:20 remaining)
Stats: 0:02:50 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 17.42% done; ETC: 15:45 (0:13:16 remaining)
Stats: 0:06:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 50.12% done; ETC: 15:42 (0:06:31 remaining)
Stats: 0:09:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 74.32% done; ETC: 15:41 (0:03:10 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.31s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 65534 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 689.79 seconds
```

Step 4 : Once Nmap port scanning is done, it will show a list of open ports it found on the website. Look at this list to see how many ports are open and which services are running, and if there are any security risks.

```
Stats: 0:09:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 74.32% done; ETC: 15:41 (0:03:10 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.31s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 65534 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 689.79 seconds

┌──(sumitvish㉿kali)-[~]
└─$
```

The result of the scan shows that only port 80, which is used for HTTP, is open on this website.

Answer: Only port 80 which is used for websites, is HTTP was found to be open on this website.

Mitigation: Protecting computer devices from cyber crimes like 'Port Scanning' is extremely important.

Firewall protection: Firewalls prevent unauthorized access to the computer network, thus preventing cyber attacks like the occurrence of attacks on open ports. A proper firewall ensures that ports are not open for vulnerable attacks by Cybercriminals.

TCP wrappers: These enable administrators to have the flexibility to permit or deny access to servers based on IP addresses and domain names.

Regular port scanning : This regular check can help detect any suspicious port scanning activity immediately and it can then be taken into action and prevented if timely detected.

Conclusion :

Checking for open ports on a website is very important for security. We found that only one port was open on the website http://testphp.vulnweb.com/. To make the website safer, we need to close unnecessary ports and fix problems. By doing this, we can make our website much safer.

2) **Brute force the website http://testphp.vulnweb.com/ and find the directories that are present in the website.**

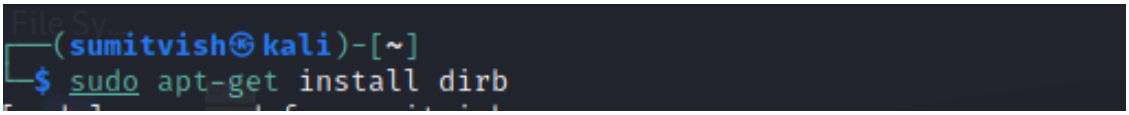
Dirb is like a detective tool for finding hidden directories and files on websites.

Here's how we can use it:

Step 1: Install Dirb (if not already installed)

If you're using Kali Linux, Dirb might already be installed. If not, you can install it using a command like this:

sudo apt-get install dirb



Step 2: Open Terminal
Launch the terminal on your system. This is where you'll run Dirb.

Step 3: Run Dirb
Type the following command into the terminal,
replacing **http://testphp.vulnweb.com/** with the website you want to search:
dirb http://testphp.vulnweb.com/

Findings:
DIRECTORY: http://testphp.vulnweb.com/admin/

- http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
- http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
- http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)

DIRECTORY: http://testphp.vulnweb.com/CVS/

- http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
- http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
- http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
- http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)

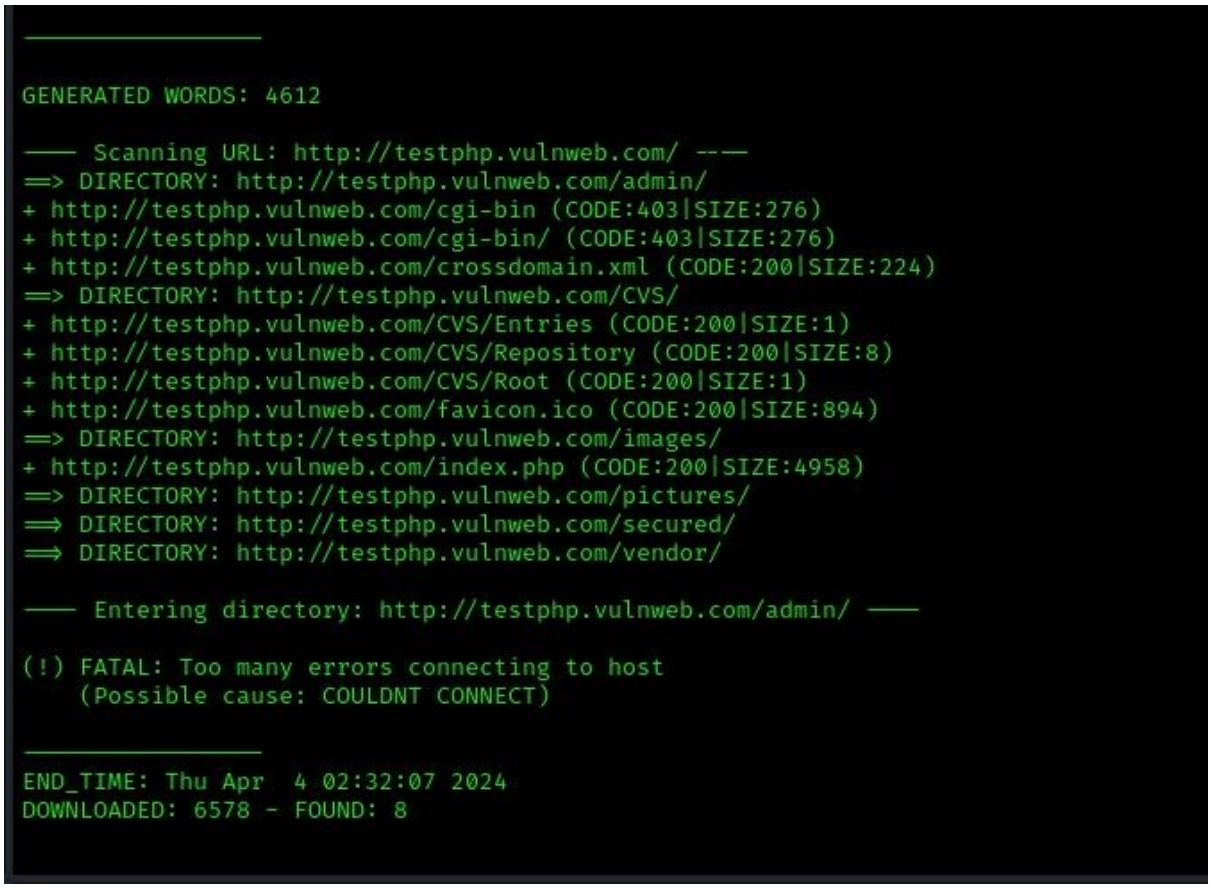
DIRECTORY: http://testphp.vulnweb.com/images/

- http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)

DIRECTORY: http://testphp.vulnweb.com/pictures/

DIRECTORY: http://testphp.vulnweb.com/secured/

DIRECTORY: http://testphp.vulnweb.com/vendor/



Mitigation:

- Use Strong Passwords
- Restrict Access to Authentication URLs.
- Limit Login Attempts.
- Use CAPTCHAs.
- Use Two-Factor Authentication (2FA)
- Set Up IP Access Restrictions.

3) **Make a login in the website http://testphp.vulnweb.com/ and intercept the network traffic using Wireshark and find the credentials that were transferred through the network.**

Intercepting Network Traffic using Wireshark on Linux and Finding Credentials Transferred through the Network

Step 1: Install Wireshark

Install Wireshark using the command :

apt-get install wireshark

Step 2: Launch Wireshark

Start Wireshark using the command line or menu bar.

Wireshark

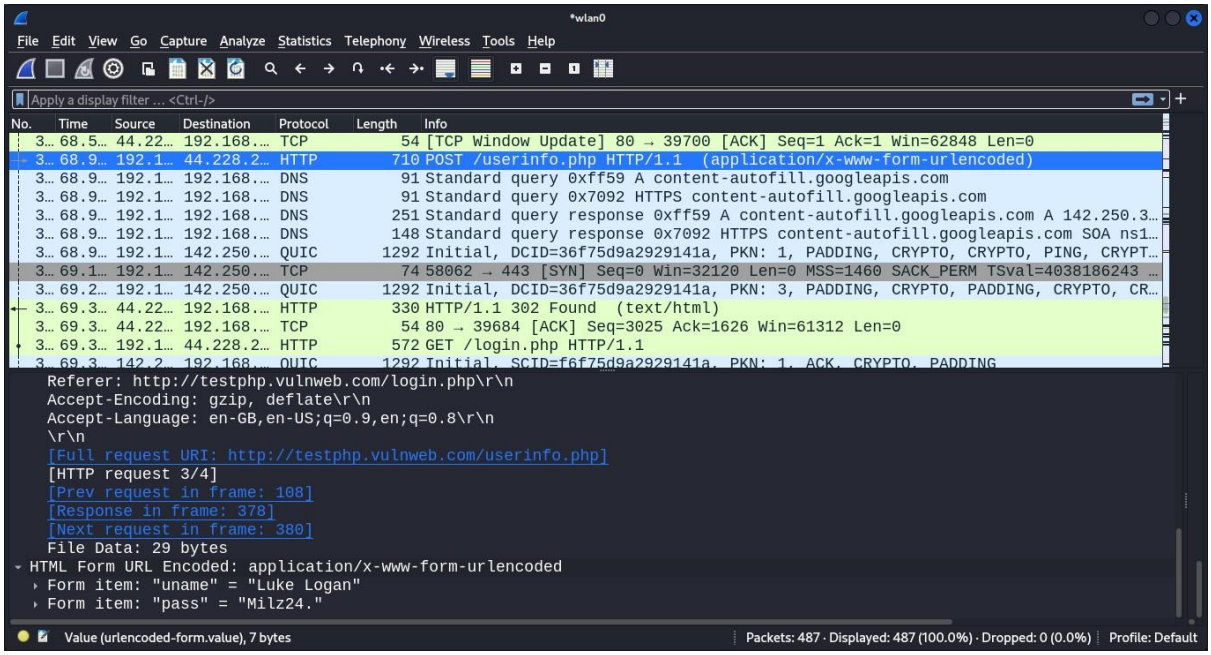
Step 3: Select the Network Interface

Choose the network interface you want to monitor.

Findings:

Login credentials

- Uname : Luke Logan
- Pass : Milz24.



Mitigations:

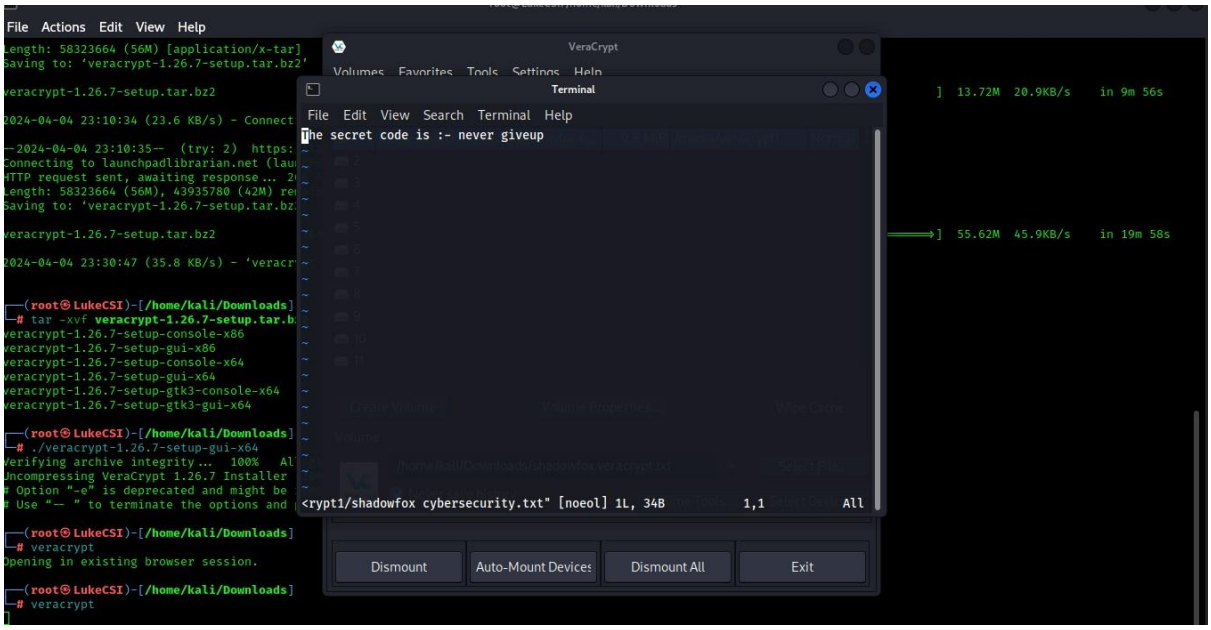
- Monitor Network Traffic. Ensure you have complete visibility of incoming, outgoing and internal network traffic, with the ability to automatically detect threats, and understand their context and impact.
- Segregate Your Network. Divide a network into zones based on security requirements. This can be done using subnets within the same network, or by creating Virtual Local Area Networks (VLANs), each of which behaves like a completely separate network.
- Deploying Firewalls and Intrusion Detection Systems
- Regularly Updating and Patching Systems
- Implementing strong Access Controls
- Utilizing Advanced Encryption Technologies

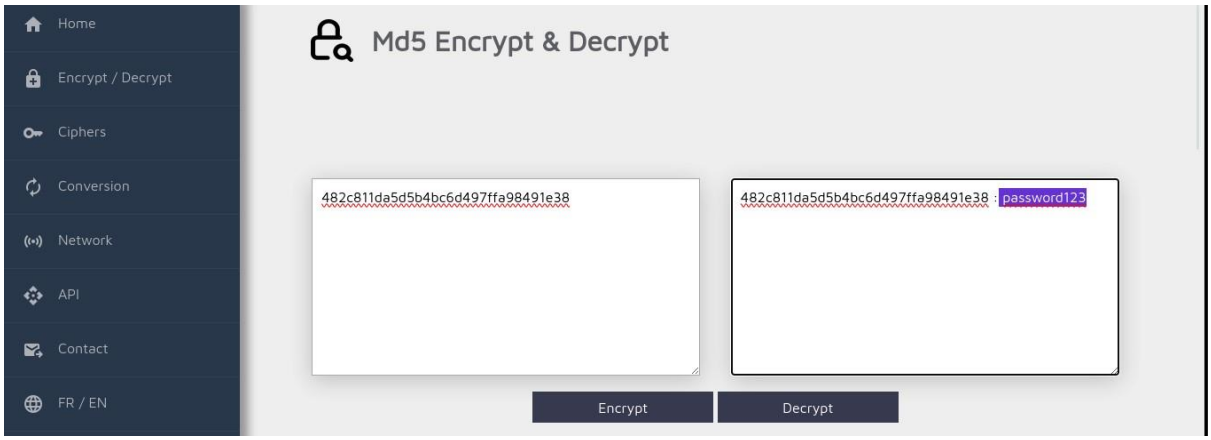
Task level (Intermediate):

1. **A file is encrypted using Veracrypt (A disk encryption tool). Decode the password and enter in the veracrypt to unlock the file and find the secret code in it.**

Findings : password123

Secret Code : never giveup

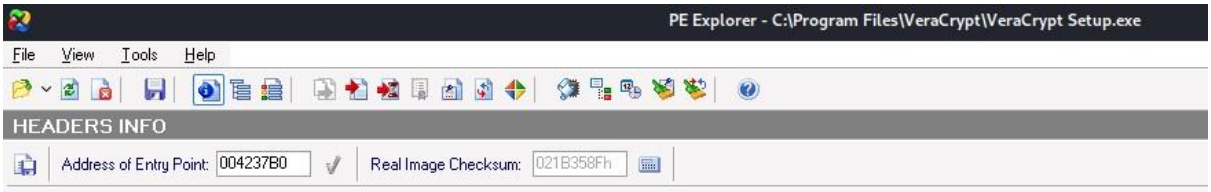


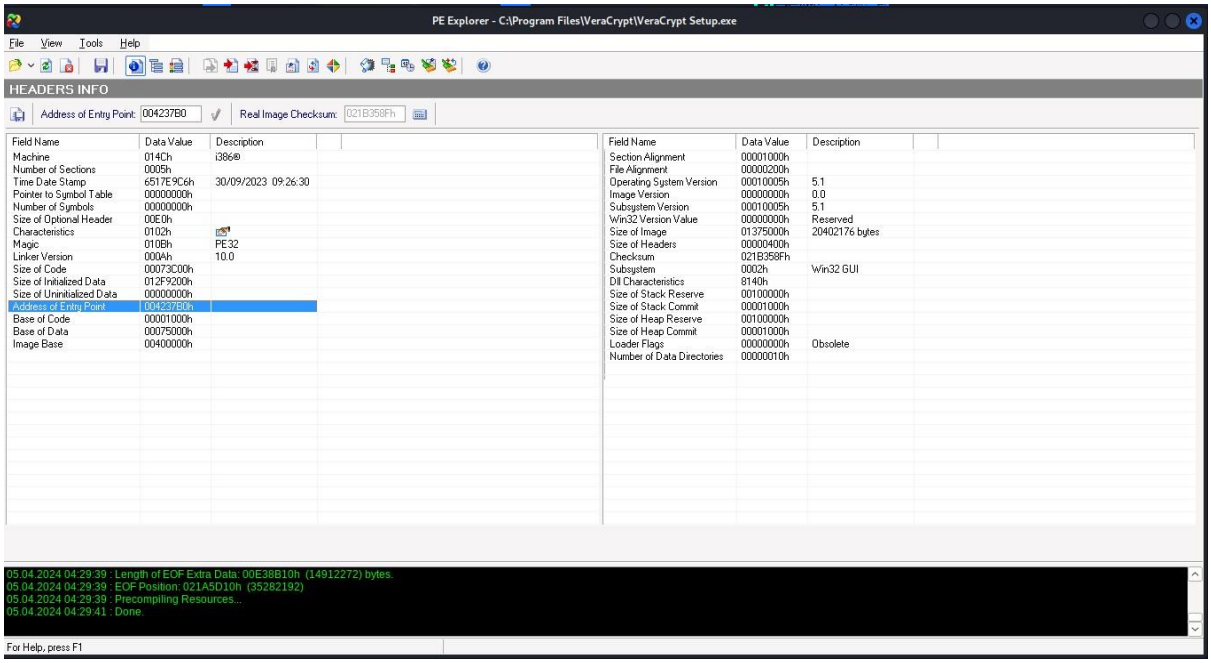


2) Find the entry point address of the executable using PE explorer tool and provide the value as the answer as screenshot.

Findings:

Entry point address : 004237B0





3) **Make a deauth attack in your own network and capture the handshake of the network connection between the device and the router and crack the password for the wifi. To crack the password create a wordlist that can include the password of your network.**

- **Findings**

crack the password for the wifi

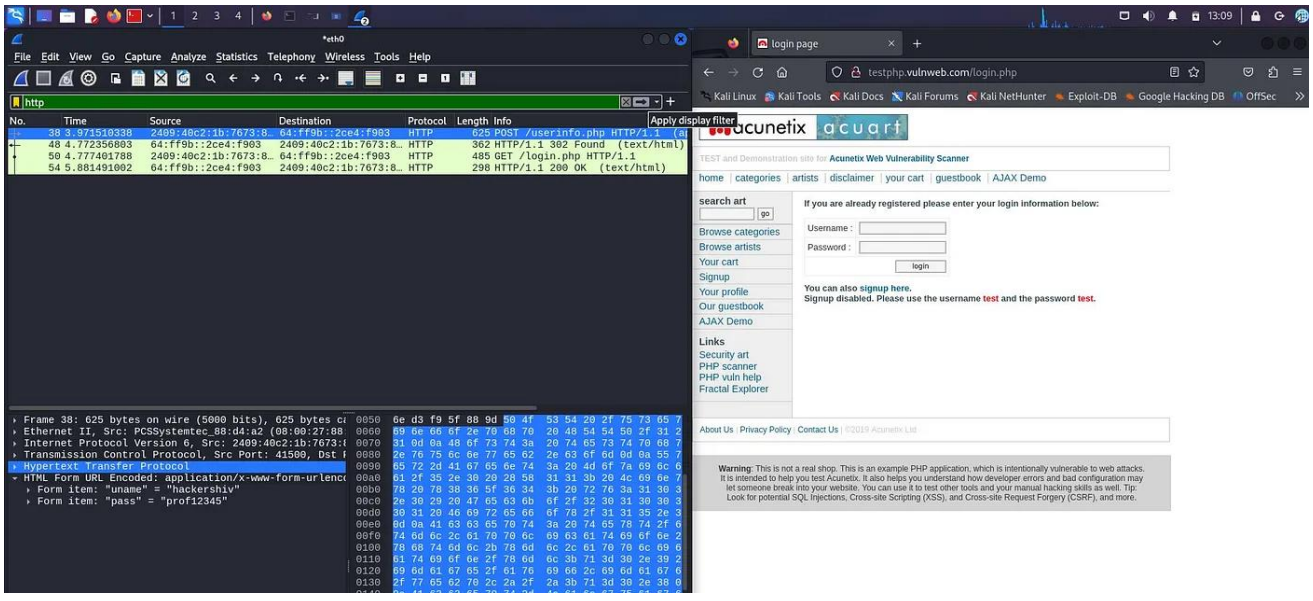
Password cracking is the process that involves computational methods to guess or retrieve a password from stored or transmitted data, typically employing algorithms executed by a computer. Password cracking attacks are due to the widespread use of weak passwords, poor password management practices, and the increasing sophistication of password-cracking tools and techniques used by cybercriminals to gain unauthorized access to a target computer system or online account by guessing or cracking the password.

Password cracking can be accomplished for several reasons such as:

- gaining access to sensitive information
- stealing data or resources
- conducting espionage

Commands

- airmon-ng
- airmon-ng start wlan0mon
- Airmon-ng check kill



- airodump-ng wlan0mon

Airodump-ng - - -bssid - - -channel number - - - write hack ● aireplay-ng --deauth 20 -a BSSID -e STATION wlan0mon

Mitigation

- Enable encryption on your router.
- Never use a dictionary word as a password
- Use strong passwords
- Regularly change your passwords. The longer one password goes unchanged, the more likely it is that a hacker will find a way to crack it. ● Using firewalls on each network access point.
- Changing the default admin account of the router that has Wi-Fi enabled.
- Disabling WPS on your wireless router.
- Preventing the broadcast of your SSID.