**ServMon walkthrough**

# **Index**

[Index 1](#_Toc193833020)

[List of pictures 1](#_Toc193833021)

[Disclaimer 2](#_Toc193833022)

[Reconnaissance 2](#_Toc193833023)

[Initial foothold 3](#_Toc193833024)

[User flag 3](#_Toc193833025)

[Privilege escalation 4](#_Toc193833026)

[Personal comments 5](#_Toc193833027)

[References 5](#_Toc193833028)

# **List of pictures**

[Figure 1 - nMap scan results (part 1) 2](#_Toc193833031)

[Figure 2 - nMap scan results (part 2) 2](#_Toc193833032)

[Figure 3 - Anonymous login via FTP 3](#_Toc193833033)

[Figure 4 - List of passwords found 3](#_Toc193833034)

[Figure 5 - SSH login as Nadine 4](#_Toc193833035)

[Figure 6 - User flag 4](#_Toc193833036)

[Figure 7 - Administrative password found 4](#_Toc193833037)

[Figure 8 - netcat uploaded on the target 5](#_Toc193833038)

[Figure 9 - Privilege escalation exploit 5](#_Toc193833039)

[Figure 10 - Privilege escalation and root flag 5](#_Toc193833040)

# **Disclaimer**

I do this box to learn things and challenge myself. I’m not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who are willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just to say: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

# **Reconnaissance**

The results of an initial nMap scan are the following:

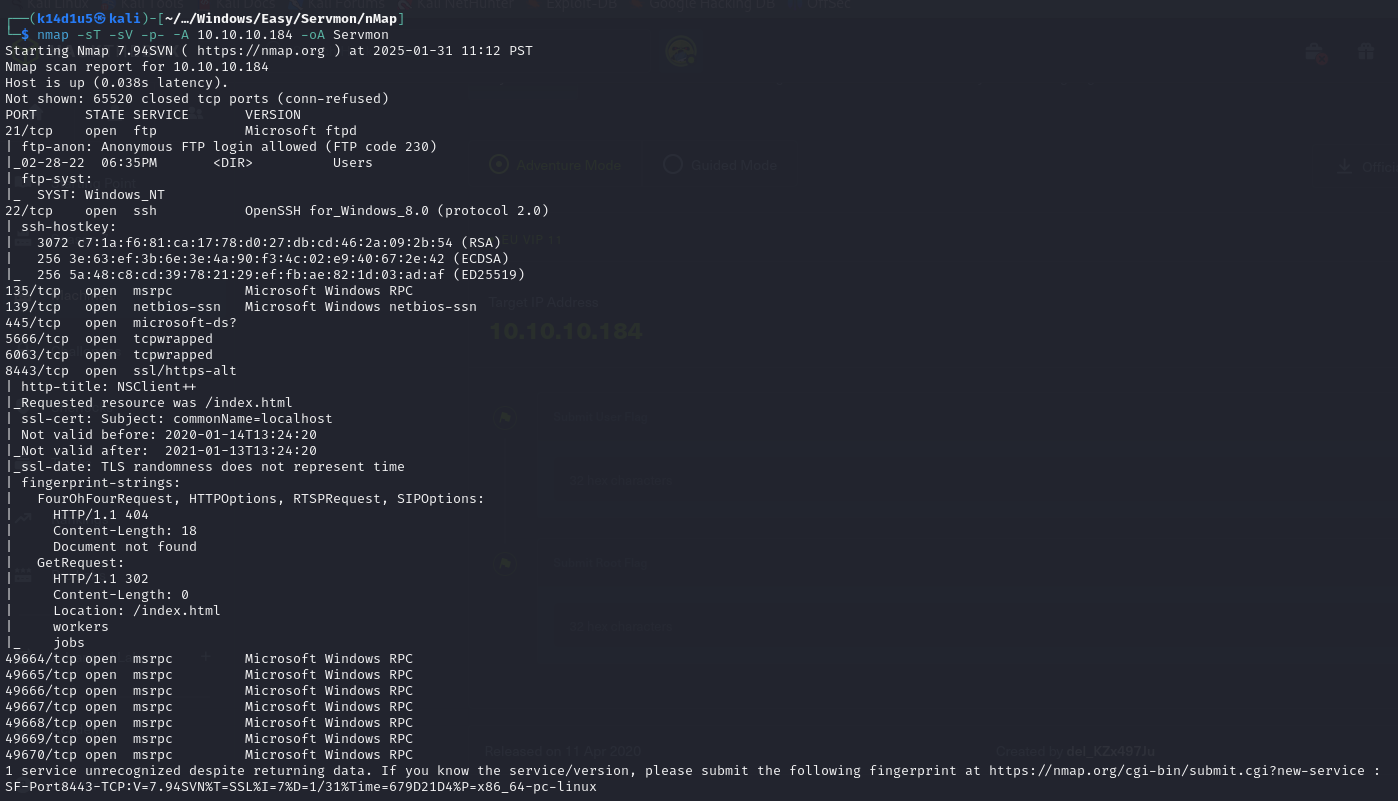


Figure 1 - nMap scan results (part 1)

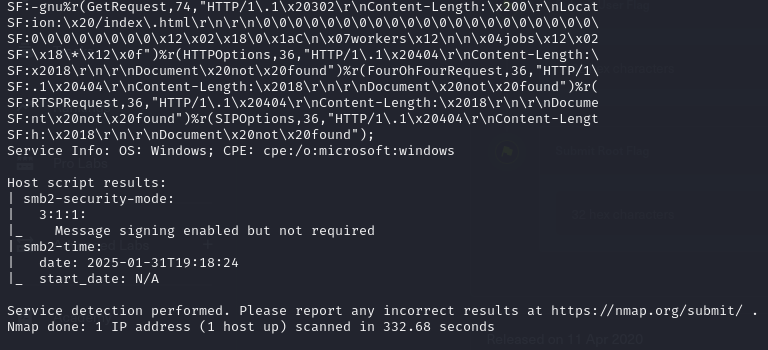


Figure 2 - nMap scan results (part 2)

Open ports are 21, 22, 135, 139, 445, 5666, 6063, 8443, 49664, 49665, 49666, 49667, 49668, 49669, 49670. So, the following services were enabled: FTP (21), SSH (22), RPC (135, 49664, 49665, 49666, 49667, 49668, 49669, 49670), NetBIOS (139), SMB (445), a web application (8443). Also, the service is unknown for two ports (5666, 6063). Lastly, nMap was able to recognize Windows as operative system.

# **Initial foothold**

First of all, I tried to establish an anonymous connection via FTP (of course when the FTP service is enabled). As shown in the following figure, this test was successful and I found out two possible usernames and two interesting files:

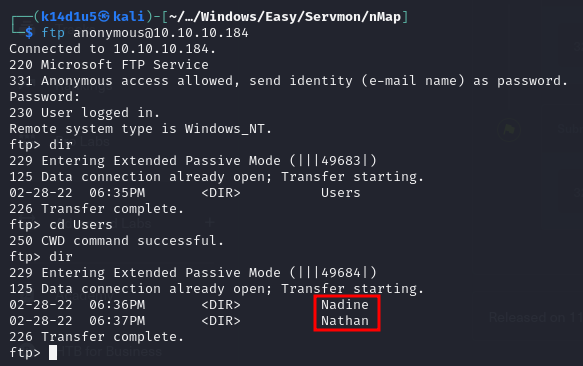


Figure 3 - Anonymous login via FTP

In particular, the file in the folder talked about a password left on the Nathan Desktop. The file in the folder talked about a checklist. However, Nathan didn’t complete all tasks. At this point I tried several things to understand how I can access and log in the machine. After several tries, I run again nMap to look for known vulnerabilities (using the script). In this way, I found a new port not previously shown: port 80.

# **User flag**

When I browsed the target IP on port 80, I reached a login form. Since I had a web application, I knew the OS was Windows and I knew the location of a specific file, I tried to exploit the web application via a path traversal vulnerability. Luckly, I was able to read passwords in the password file left on the Nathan desktop, as shown in the following figure:

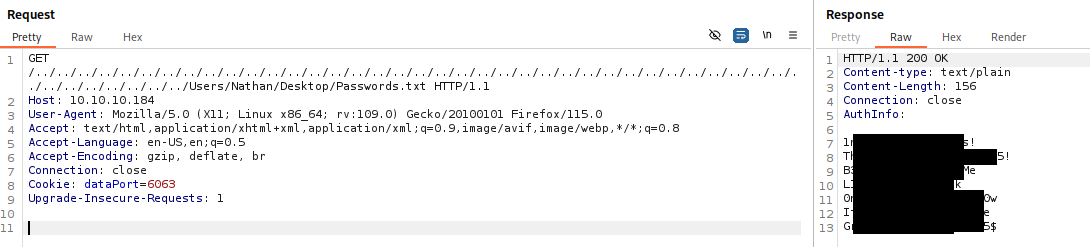


Figure 4 - List of passwords found

I have a list of usernames (Nathan and Nadine) and a list of passwords, now. So, I can try the SSH login. Luckly, it was successful with user:

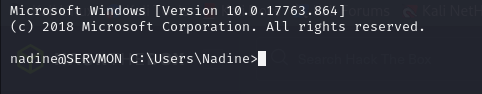


Figure 5 - SSH login as Nadine

At this point I was able to retrieve the user flag:

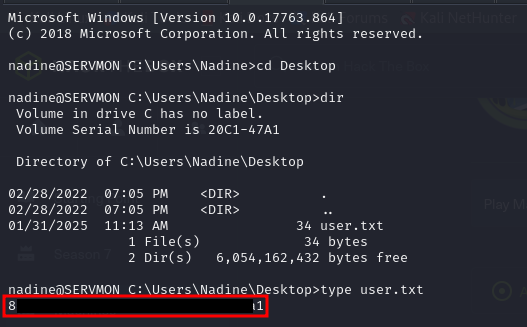


Figure 6 - User flag

# **Privilege escalation**

I needed to escalate my privileges. To do so, I tried to use WinPeas, but it didn’t work (and it was deleted after few minutes). So, I searched for some interesting information on the file system. In this way, I found a custom program named . So, I looked in his specific file and I found an administrative password in the configuration file:

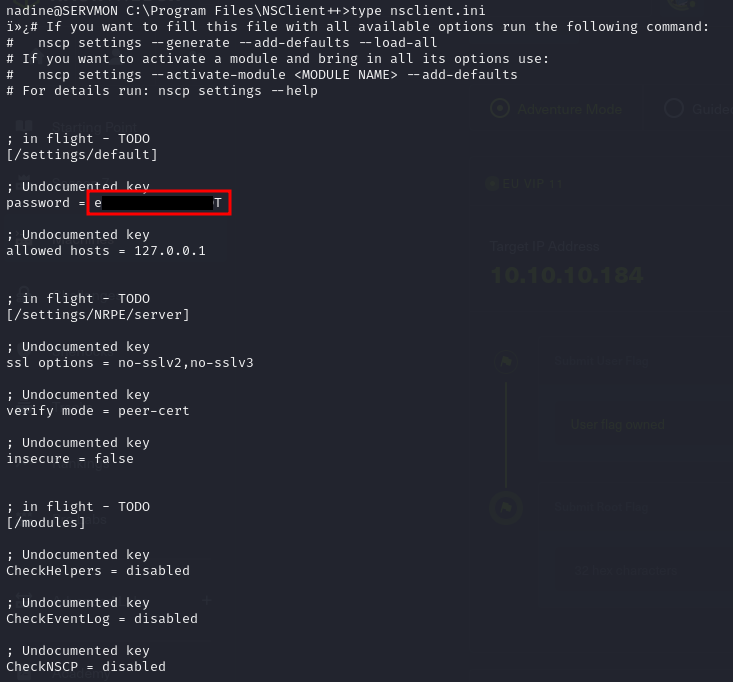


Figure 7 - Administrative password found

Also, I looked for an exploit against on the Internet. Luckly, I found a very interesting one. In particular, this exploit led to RCE. When I tried it to execute the command, I noted that it was executed as . All I needed to do was to obtain a shell via the exploit. To do so, I uploaded the program on the target:

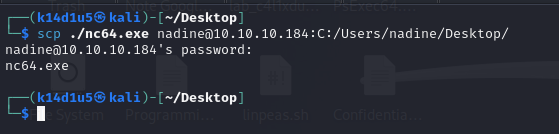


Figure 8 - netcat uploaded on the target

At this point, I run again the exploit to run netcat using the command in the following figure:

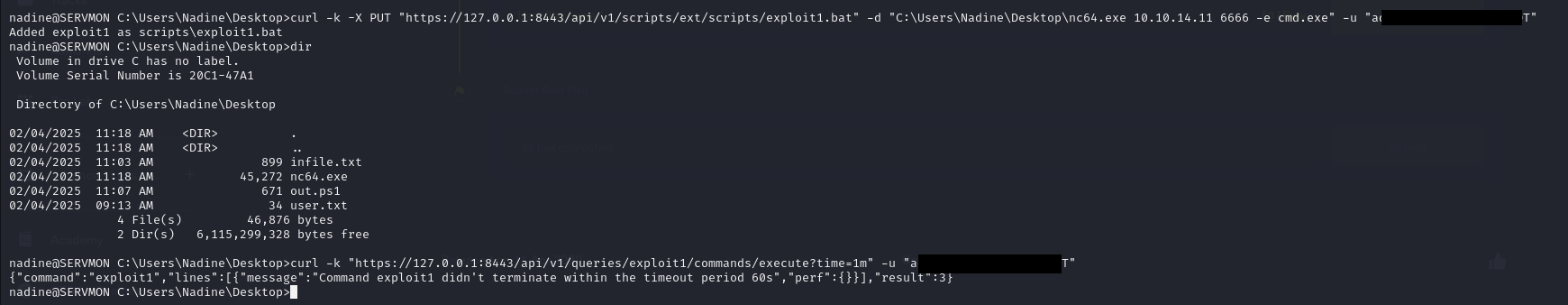


Figure 9 - Privilege escalation exploit

In this way, I obtained a shell as and I retrieved the root flag:

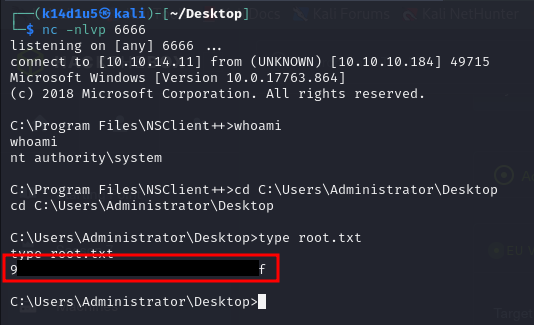


Figure 10 - Privilege escalation and root flag

# **Personal comments**

This box is quite easy but it was very fun to complete it. In my opinion, it is very strange that one of the passwords that Nadine left on the Nathan desktop (to give him HIS password) worked to log in via SSH as Nadine. I really hate this kind of solution, because in my opinion is unlikely and unbelievable. I rated this box as Easy on the Hack The Box platform.

# **References**

NSClient++ exploit: <https://github.com/xtizi/NSClient-0.5.2.35---Privilege-Escalation/blob/master/exploit.py>.