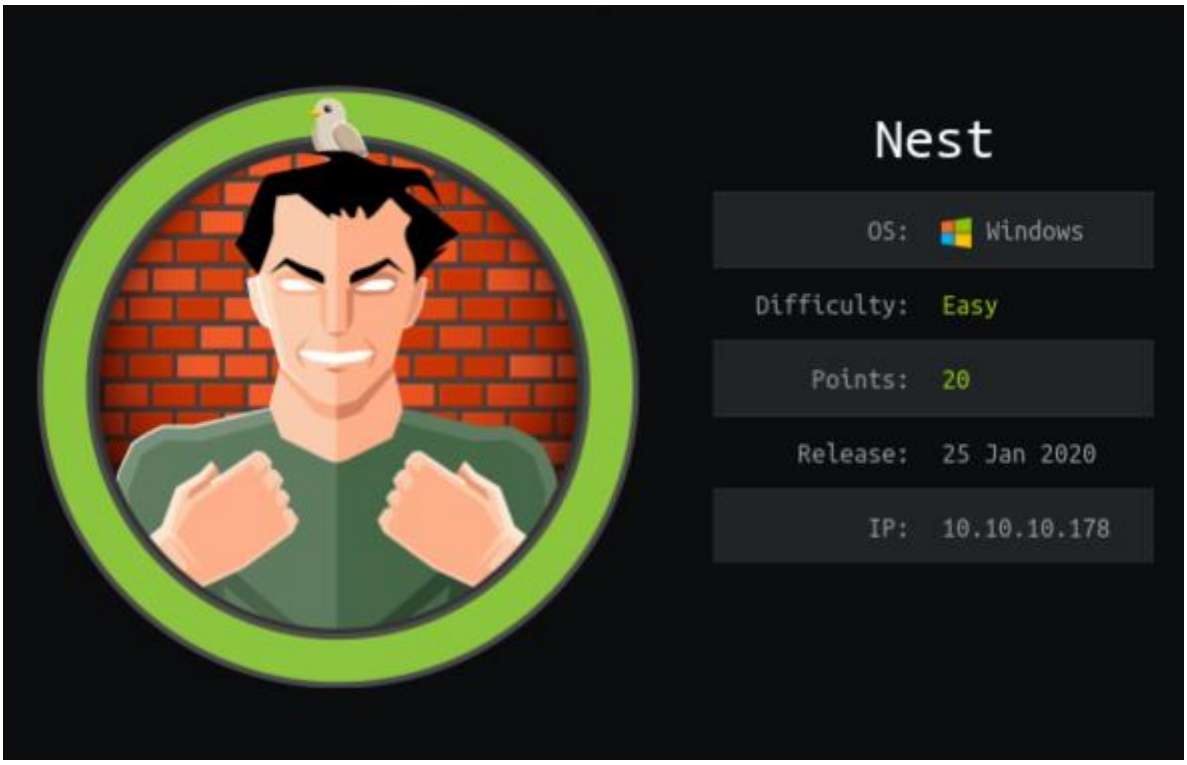
HackTheBox – Nest Cookbook



Tools:

- Nmap (Kali Linux)
- Visual Studio (https://visualstudio.microsoft.com)
- DnSpy (https://www.softpedia.com/get/Programming/Debuggers-Decompilers-Dissasemblers/dnSpy.shtml#download) or (https://github.com/0xd4d/dnSpy/tree/master/dnSpy/dnSpy)
- smbclient (Kali Linux)

Learning Outcomes

- Playing with smbclient
- Editing with VB.net codes
- Using disassembler such as DnSpy

*The **unintended way** will not be explained or shown as it was expressed by the creator of the box that it is not the correct method to find the flag.

Enumeration Step:

- Use nmap to perform a very thorough scan. (**nmap –help** will help you a lot)
- Learn about SMB enumeration. Plenty of articles online.

Gain Access

- Learning smb enumeration should be able to give you enough hints on using the smb service.
- Once entered, the only keyword here **"ENUMERATION"**, search everything like an FBI agent would.
- When one starts work, you'll receive an email with information.
- Started work yet? If you did, it is time to re-enter places you weren't given access for previously.
- Sometimes when one is lost, you have to search to configure certain things yourself or reconfigure it.
- Like a Detective you seemed to have come across another suspect that may have information. From knowing this suspect's history, try jumping over even when you can't see it when it is listed. Enter the hidden world.
- Found the missing husband of Mrs. Smith yet? She misses him and it would help if you found something about him.
- It is troublesome to travel between worlds in order to learn the hidden world of the suspect, why not bring that hidden world to your world as it would make life easier. (**smbget** may be able to help you in here)
- Once you managed to bring everything to your place, now you have to search through everything.

Editing Part

- You found a Visual Studio file, let's edit it.
- Debug the errors accordingly and you still can't get the info needed?
- Try adding some of your ingredients to make sure the flavor you want comes out.
- The taste disappears too fast before you know what it is? Try adding an ingredient that waits for you to add something before the taste disappears. (Maybe Reading a line helps?)
- After editing everything, you should have what is required to enter that user's world.

Gaining Privileges

- Try viewing this user's world, maybe it will provide you clues and the first flag you seek is in this world.
- Came across a deBug that is there and yet not there or empty? Try understanding what it is for maybe you don't have all the information.

- Once you learned enough about it, you start to see that there are multiple streams to draw the information you need in this smb. Choose wisely and remember to include the name of the stream to draw from. (**get** will help you here)
- When you figured how to capture this ghost file, it will help you in the phase of obtaining things for escalating privileges.
- Remember what you did in the past, there was another port that was unvisited. Maybe **telnet** could help you?
- With telnet's help, you search around like an FBI agent. You will know what files you need when you see it.
- Due to being unable to bring back a certain configuration file that contains the Administrator's info, you can recreate and give it the same name.
- Found any similar files as the ones you found previously?

Editing the Executables

- DnSpy is your best friend here.
- Try looking directly inside the H****** only. You will come across the Main():void.
- Edit method/class of it
- Apply what you learned previously and to display what you need.
- Remember to save your changes by closing DnSpy.
- Executed the file but nothing? Did you seek the power of Powershell?
- Still nothing? Maybe just like me you didn't know that something is needed to pass together with this executable.
- Once you obtained the password. The rest is up to you FBI agent for you now have access to EVERYTHING.