

007 Write-up

Introduction

The 007 warmup machine is an ideal starting point with Remote Desktop Protocol (RDP). On this machine, you will learn how to identify and exploit vulnerabilities caused by misconfiguration of RDP services. You will also explore in detail the basic operation of RDP and how to establish connections. This exercise will help you understand RDP vulnerabilities and strengthen your cybersecurity skills.

Remote Desktop Protocol (RDP)

Remote Desktop Protocol (RDP) is a protocol developed by Microsoft that allows users to remotely access another computer over a network. RDP is equipped with security and functionality features such as data encryption, session management and device routing.

Information Gathering

Let's start gathering information by doing a port scan of our target machine.

```
root@hackerbox:~# nmap 172.20.3.146
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-06 06:51 CST
Nmap scan report for 172.20.3.97
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 52:54:00:E0:92:52 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
```

As a result of the port scan, we discover that 4 ports are open. When we did research on the open port 3389, we found that the RDP service is running, through which we can establish a remote desktop connection to the computer.

Task 1

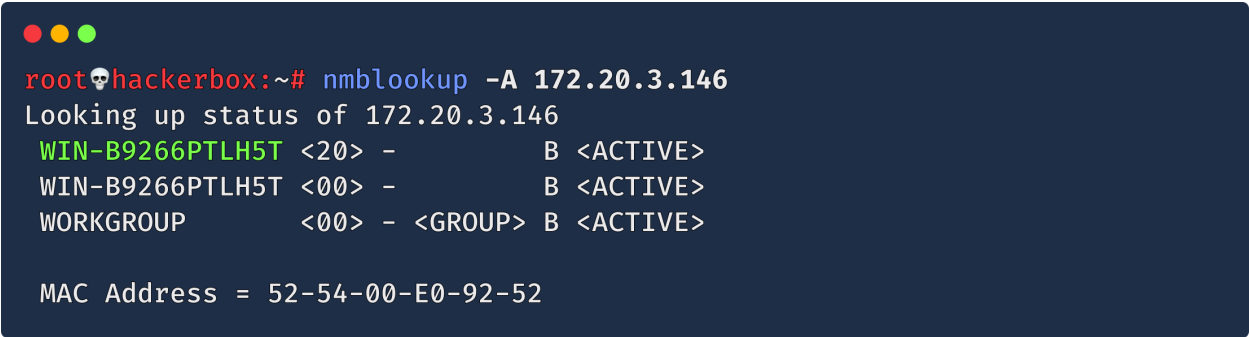
We can get the hostname of the target machine through the NetBIOS service. For this we can simply use the **nmblookup** tool.

nmblookup

```
nmblookup [options] <netbios-name>
```

-A : This parameter is used to learn the NetBIOS name of a computer from its IP address.

-B : This parameter is used to learn the IP address of a computer from its NetBIOS name.

A terminal window with a dark blue background and light blue text. The prompt is 'root@hackerbox:~#'. The command 'nmblookup -A 172.20.3.146' is entered. The output shows the status of 172.20.3.146, listing NetBIOS names and their status: WIN-B9266PTLH5T <20> - B <ACTIVE>, WIN-B9266PTLH5T <00> - B <ACTIVE>, and WORKGROUP <00> - <GROUP> B <ACTIVE>. The MAC address is also displayed as 52-54-00-E0-92-52.

```
root@hackerbox:~# nmblookup -A 172.20.3.146
Looking up status of 172.20.3.146
WIN-B9266PTLH5T <20> -      B <ACTIVE>
WIN-B9266PTLH5T <00> -      B <ACTIVE>
WORKGROUP      <00> - <GROUP> B <ACTIVE>

MAC Address = 52-54-00-E0-92-52
```

Task 2

RDP stands for **Remote Desktop Protocol**.

Task 3

Usually the default authorized user on Windows computers is the **Administrator** user.

System Access

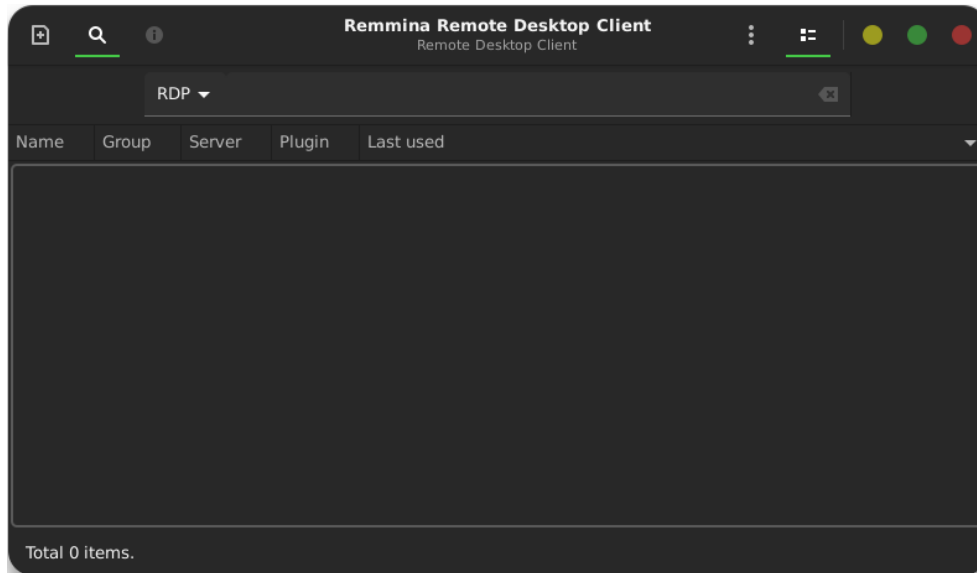
Let's try to connect to the target machine via the RDP protocol as the Administrator user we guessed.

There are many tools that can be used to establish an RDP connection to a remote computer. Microsoft Remote Desktop, FreeRDP, rdesktop, Remmina are some of the tools that can be used for RDP connection.

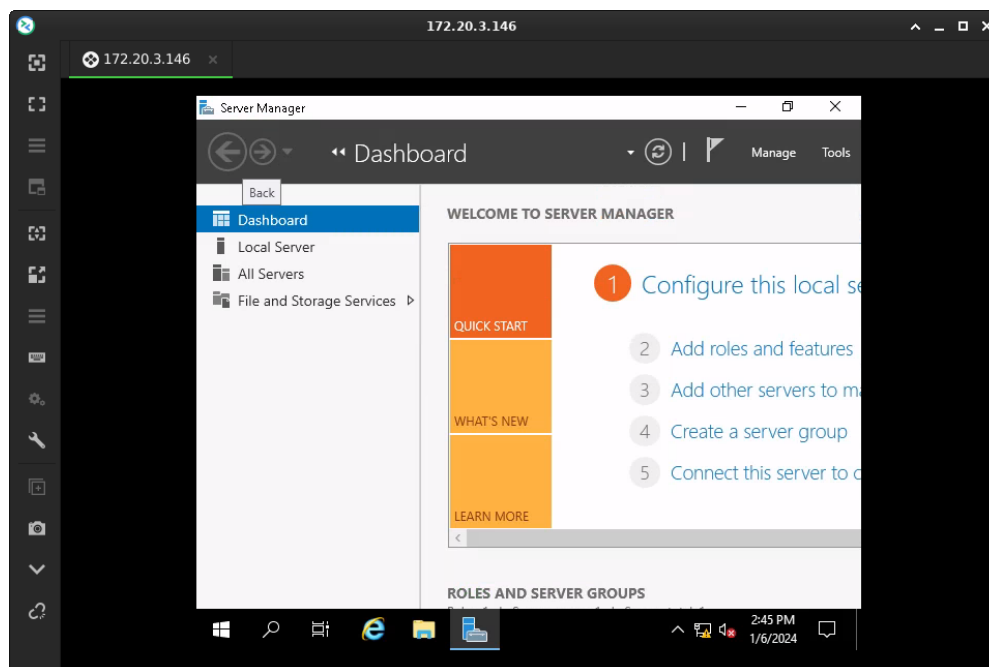
Task 4

Let's try to establish an RDP connection with Remmina, an open-source project.

To do this, let's start Remmina, which comes installed in HackerBox.

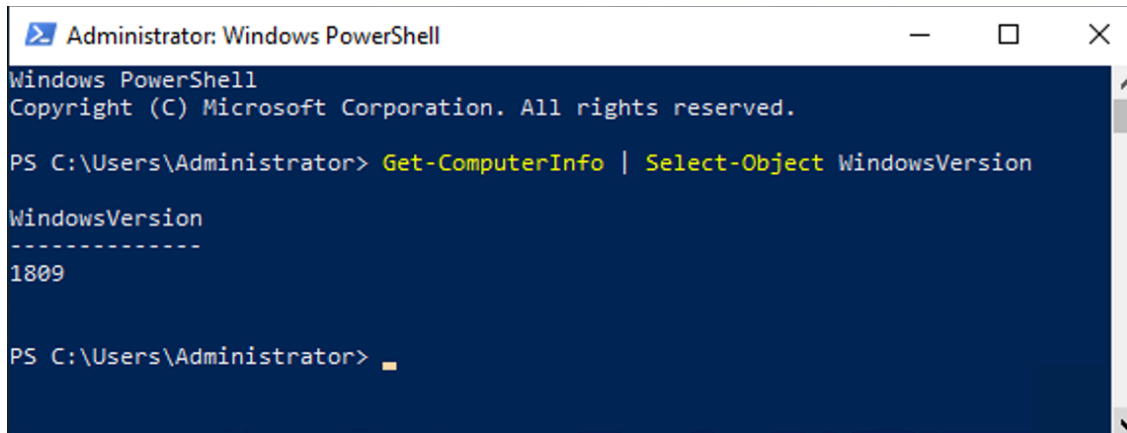


Let's type the IP address of the target machine in the RDP section, then enter the username as Administrator, leave the password blank and try to connect.



We can say that this Windows computer, which had the RDP service turned on, was misconfigured because it allowed a passwordless connection. Due to the misconfiguration, we successfully set up the remote desktop connection without a password.

Now let's run the **Get-ComputerInfo | Select-Object WindowsVersion** command in PowerShell to get the Windows version.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

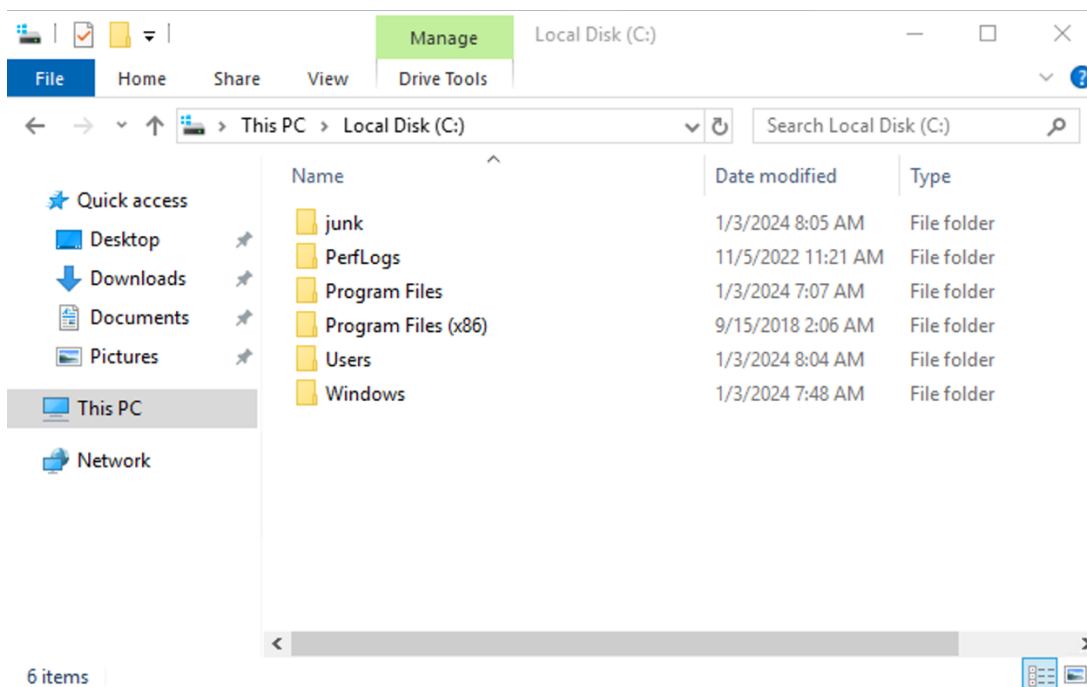
PS C:\Users\Administrator> Get-ComputerInfo | Select-Object WindowsVersion

WindowsVersion
-----
1809

PS C:\Users\Administrator>
```

Task 5

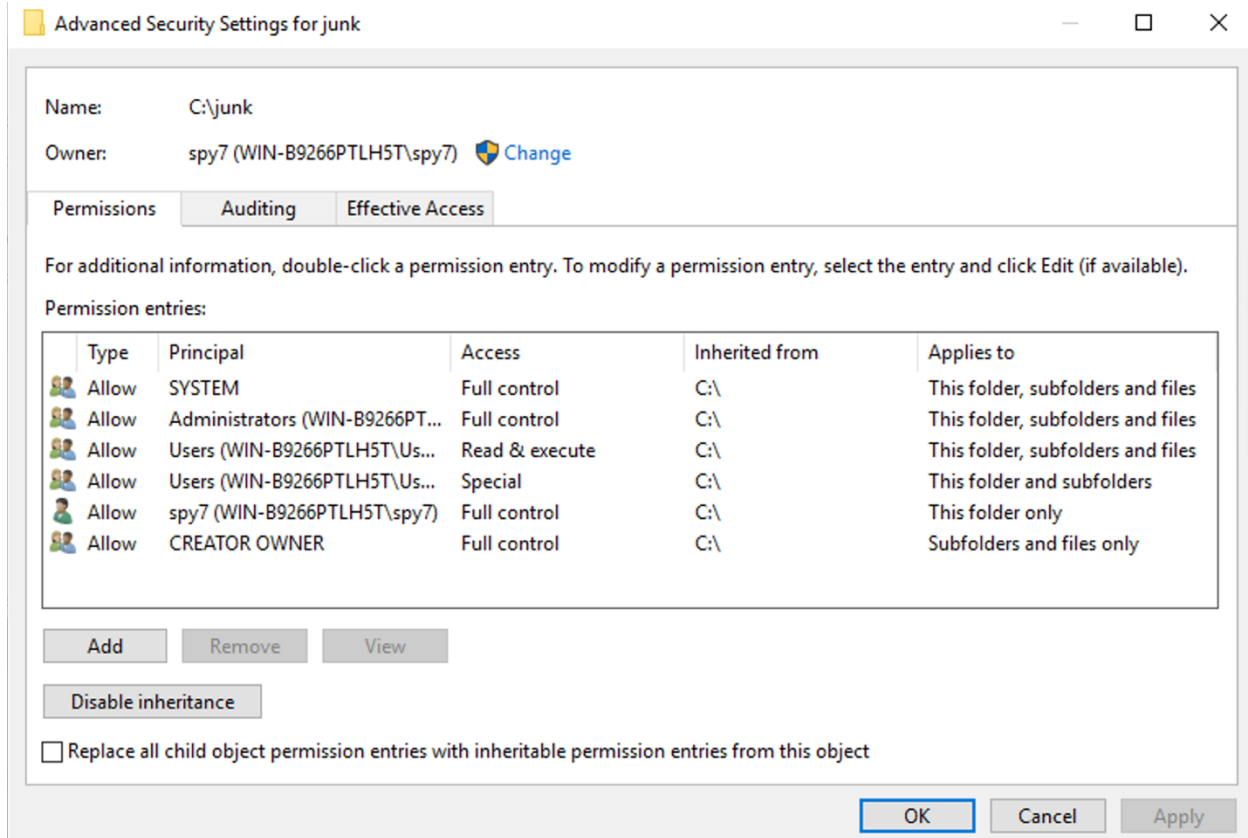
Let's check the files and folders under the C directory.



Looking at the list, the **junk** folder looks suspicious.

Task 6

To identify the user who owns this folder, we go to Properties -> Security -> Advanced.



As seen above, the folder is owned by the **spy7** user.

💪 We have identified the user who owns the suspicious folder.

-

Congratulations 🎉

✨ You have successfully completed all tasks in this warmup.