Tiger Write-up

Introduction

Tiger warmup is an ideal starting point for basic practice with the VNC service. On this machine, you will learn how to find and exploit vulnerabilities caused by misconfiguration of the VNC service. You will also learn the basics of how VNC works and how to connect to it.

Virtual Network Computing (VNC)

Virtual Network Computing (VNC) is a desktop sharing system that provides access to a remote computer through a graphical interface. It enables the transmission of images, keyboard and mouse inputs between two computers over the Internet or local network, enabling them to work on a remote system. VNC uses the RFB (Remote Framebuffer) protocol and is platform independent, meaning it can be used on different operating systems.

Task 1

VNC stands for; **`Virtual Network Computing`**.

Information Gathering

Let's start gathering information by running a port scan on our target machine.

Task 2

As a result of our port scan, we found that port **`5901`** was open.

```
root💀hackerbox:~# nmap -sV 172.20.6.141
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 07:45 CST
Nmap scan report for 172.20.6.141
Host is up (0.00037s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
5901/tcp open  vnc     VNC (protocol 3.8)
MAC Address: 52:54:00:E2:63:7F (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

System Access

Task 3

In this task, we need to connect to the target machine with VNC to access the requested information.

There are many tools to connect with VNC. Let's try to establish a VNC connection using a tool called **`Remmina`**.

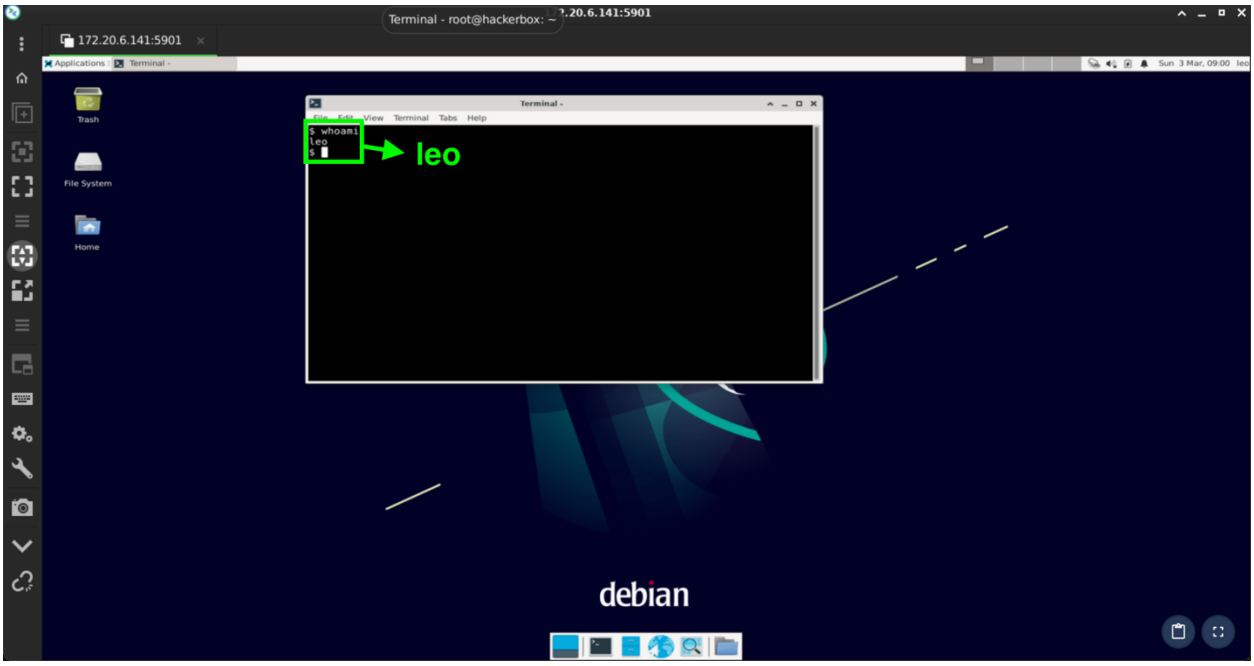
In HackerBox, you can find and run the **`Remmina`** tool in applications.

We open the Remmina tool, select the **`VNC`** protocol as shown in the image above and type the **`IP`** address and **`port`** number of the target machine.

Then press **`enter`** and try to connect.

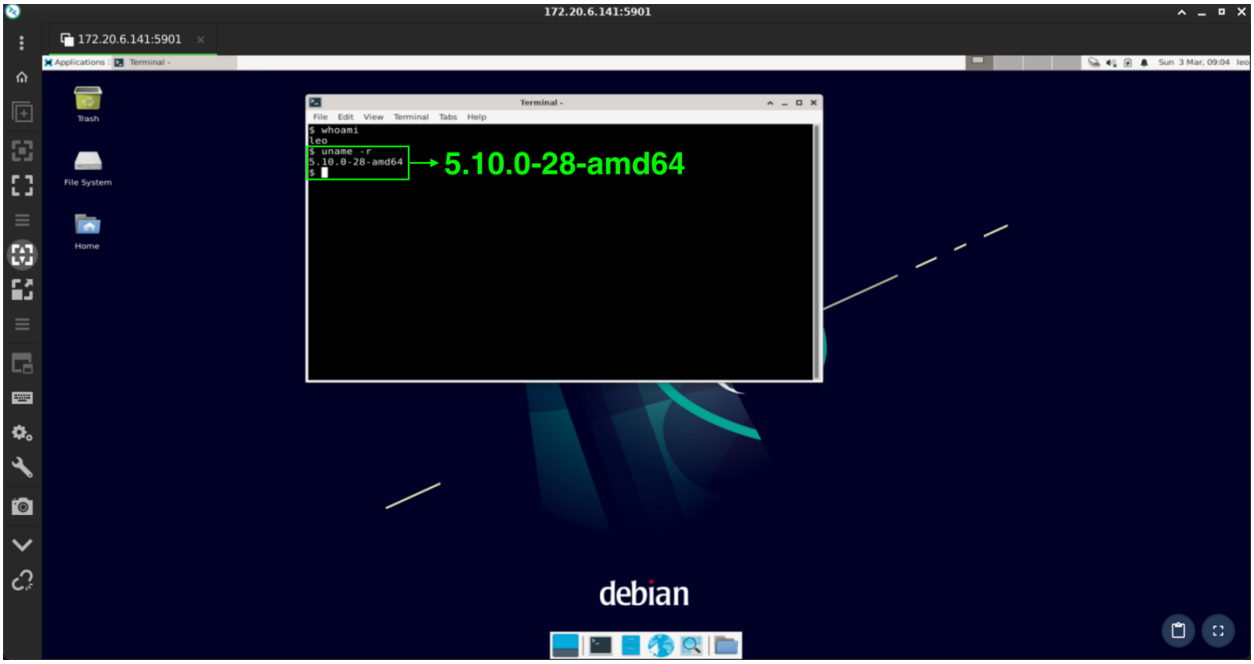
Yes, we were able to connect with VNC. **`The VNC service running on the target machine is configured in an insecure way and a direct connection can be established without a password`**. We now have direct access to the target machine.

We can open the terminal and execute the **`whoami`** command to access the requested information in the task.



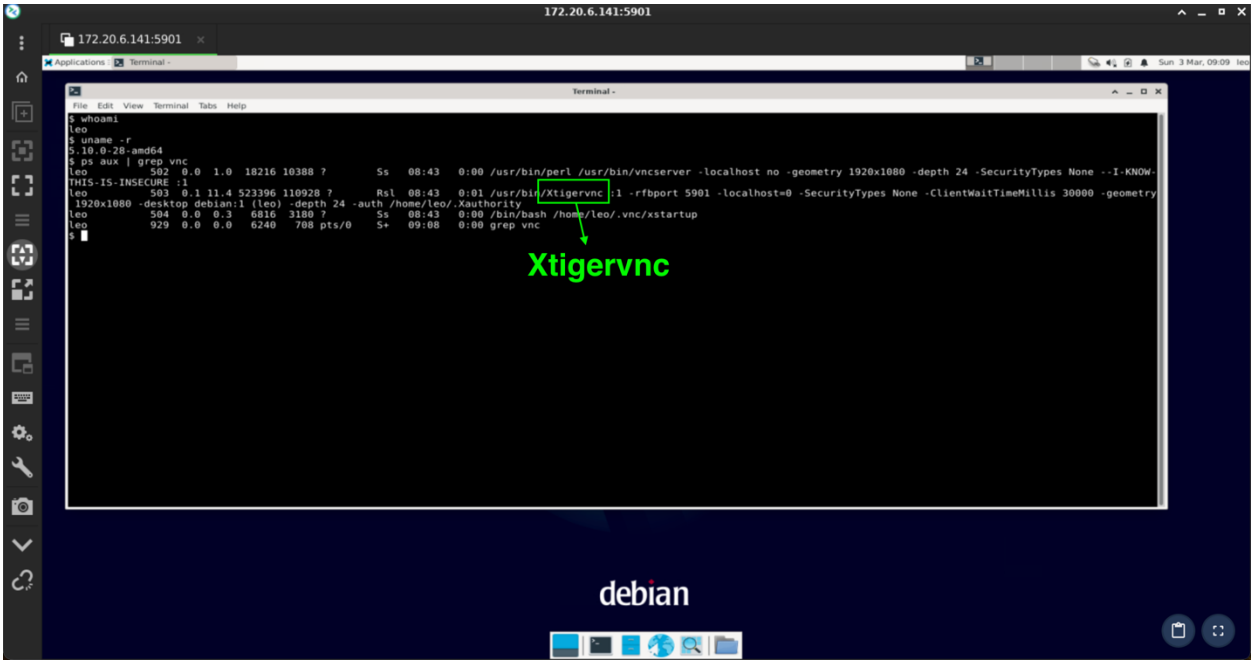
Task 4

Let's run `uname -r` to find out the Linux kernel version requested in the task.



Task 5

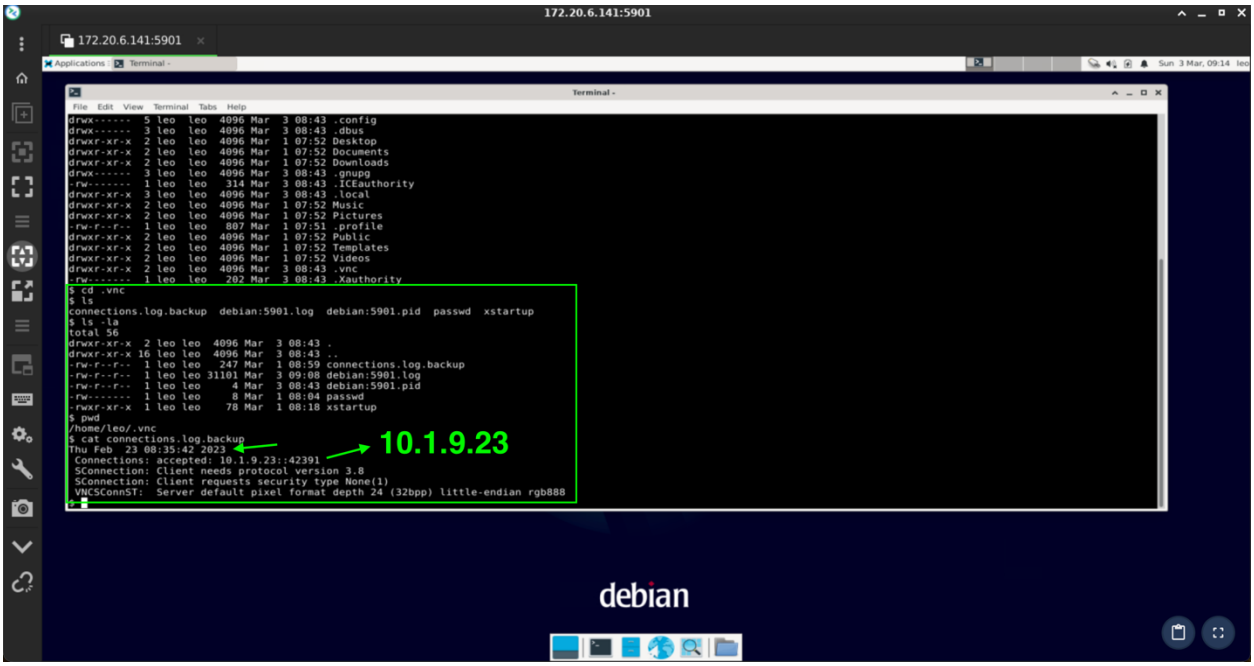
Let's first list the active processes and do a search within these processes to find out the running VNC software. For this, let's run `ps aux | grep vnc` command.



Task 6

On **`February 23, 2023`**, let's go through the **`log`** files to find the **`IP`** address of the computer that established the **`VNC`** connection.

Searching through the files, we found a remarkable file called **`connections.log.backup`** in the **`/home/leo/.vnc`** directory.



💪 We identified the IP address that established the VNC connection to the machine.

-

Congratulations 🙌

✨ You have successfully completed all the tasks in this warmup.