Arrow Write-up

Introduction

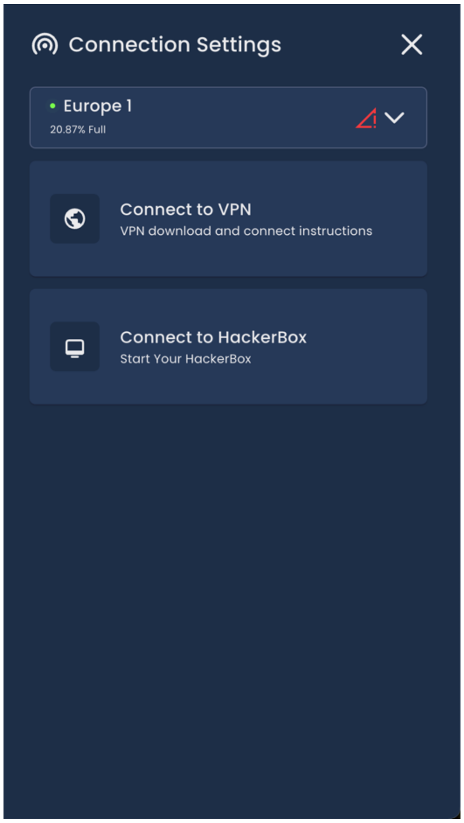
The Arrow warmup machine offers an easy and enjoyable starting point for beginners in the world of cybersecurity. How can a machine be hacked using weak authentication credentials over a telnet service? While searching for the answer to this question, you will learn both the technical challenges of this machine and the basic concepts in cybersecurity.

For beginners, working with this type of machine develops not only technical skills but also problem-solving abilities. This article will assist in gaining practical experience as well as hands-on reinforcement of theoretical knowledge, which is critical in cybersecurity.

Preparation

There are 2 methods you can use to solve scenarios, labs, warmup machines, etc. in Hackviser; VPN and HackerBox.

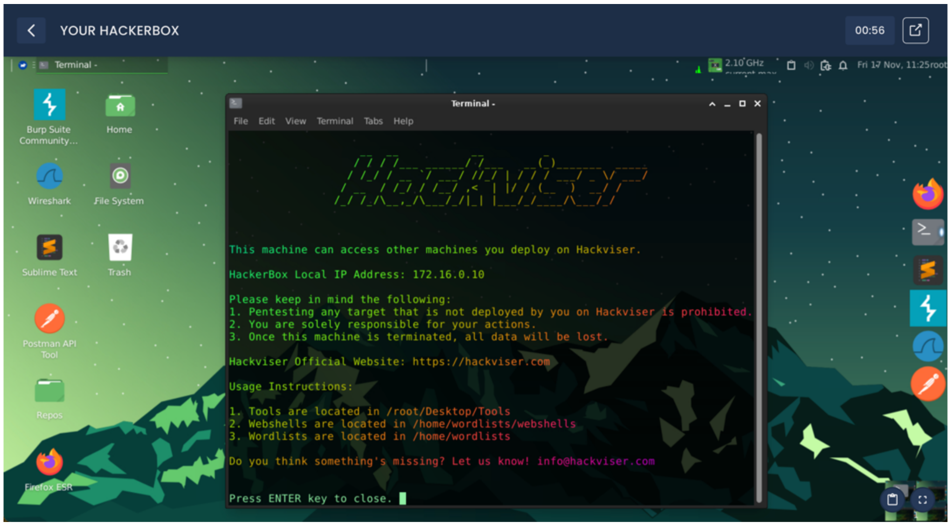
When we click on the `Connect` button in the AppBar, we will see `VPN` and `HackerBox` options.



HackerBox (Recommended)

You can start a HackerBox by clicking the **Connect** button in the Appbar and then clicking the **Connect to HackerBox** button in the window that opens.

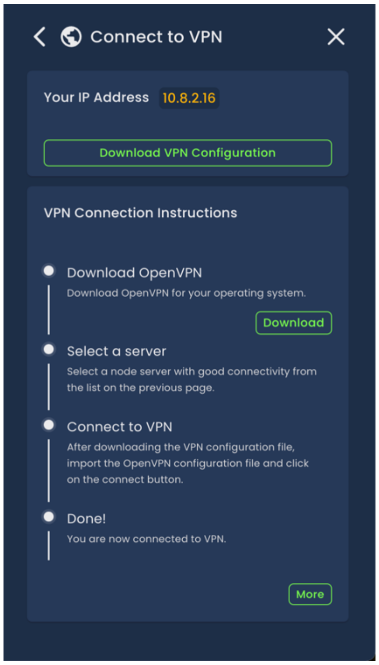
After starting the HackerBox, you can access the HackerBox by clicking the **Go to HackerBox** button.



```
This machine can access other machines you deploy on Hackviser.

HackerBox Local IP Address: 172.16.0.10

Please keep in mind the following:
1. Pentesting any target that is not deployed by you on Hackviser is prohibited.
2. You are solely responsible for your actions.
3. Once this machine is terminated, all data will be lost.

Hackviser Official Website: https://hackviser.com

Usage Instructions:

1. Tools are located in /root/Desktop/Tools
2. Webshells are located in /home/wordlists/webshells
3. Wordlists are located in /home/wordlists

Do you think something's missing? Let us know! info@hackviser.com


Press ENTER key to close.
```

OpenVPN

When you connect to a VPN, you can perform cyber security activities using your own computer. You can connect to VPN by clicking on the **Connect** button on the AppBar and then clicking on the **Connect to VPN** button in the window that opens.



Your IP Address 10.8.2.16

VPN Connection Instructions

- Download OpenVPN
  Download OpenVPN for your operating system.
- Select a server
  Select a node server with good connectivity from the list on the previous page.
- Connect to VPN
  After downloading the VPN configuration file, import the OpenVPN configuration file and click on the connect button.
- Done!
  You are now connected to VPN.

You must first download the OpenVPN client software to your computer by following the VPN connection instructions in the window that opens.

After installing the OpenVPN client software, you can connect to the VPN with the downloaded VPN configuration file by clicking the **Download VPN Configuration** button.

If you are connected to Hackviser with HackerBox or VPN, you are ready to solve scenarios, warmup machines, labs, etc.!

What is Telnet?

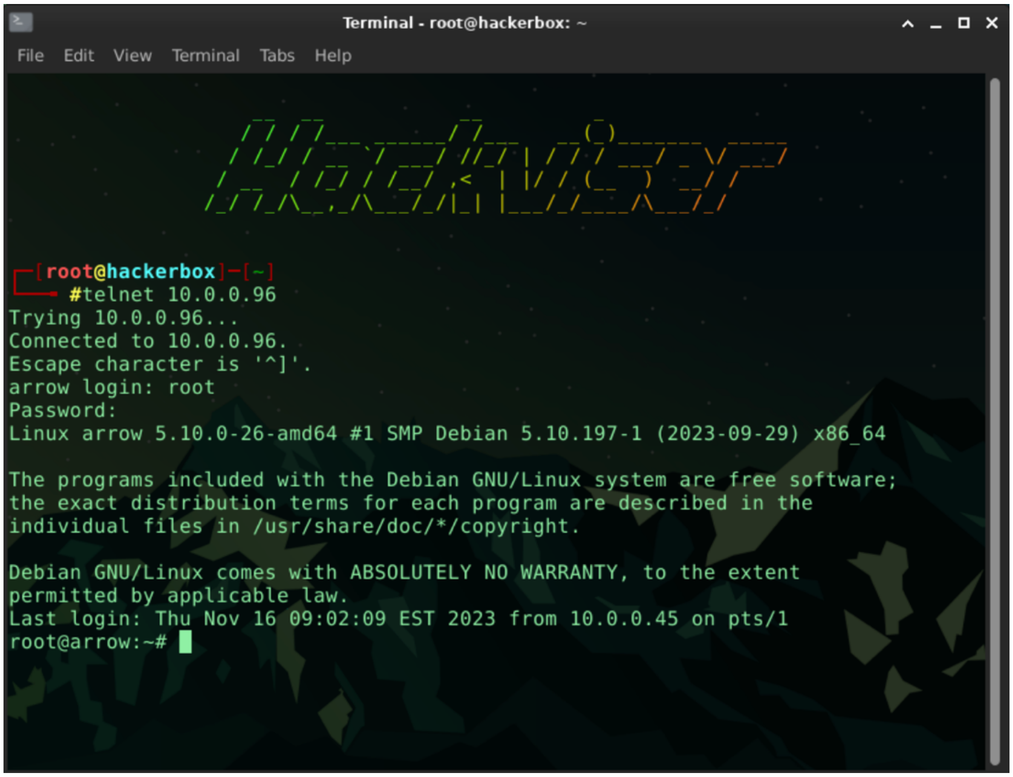
Telnet (**Tel**etype **Net**work) is a text-based network protocol used to connect to a computer remotely. Developed in 1969 and widely used in the early days of the Internet, it is specifically designed for interacting with network devices, servers or other endpoints. It provides a login interface with a username and password so that users can execute commands as if they were on the local terminal of that computer.

The major disadvantage of Telnet is that data transmission is not encrypted. This means that any information transmitted, especially usernames and passwords, can potentially be intercepted by malicious actors. This vulnerability makes Telnet a especially risky option in modern network environments where sensitive data is processed.

The following command sequence is used to connect to a server with the telnet protocol.

```
telnet <SERVER-IP-ADDRESS> <PORT-NUMBER>
```

Note: If the telnet service uses port 23 by default, we do not need to specify a port number when connecting.


Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help

```
┌─[root@hackerbox]─[~]
└──╼ #telnet 10.0.0.96
Trying 10.0.0.96...
Connected to 10.0.0.96.
Escape character is '^]'.
arrow login: root
Password:
Linux arrow 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov 16 09:02:09 EST 2023 from 10.0.0.45 on pts/1
root@arrow:~# 
```

As seen in the example above, we enter the username and password information when connecting to the telnet service.

After entering this information correctly, we are connected to a remote computer with the telnet protocol.

-

We will analyze the security risks of the Telnet service and how its vulnerabilities can be detected and exploited using the `Arrow` warmup machine.

Information Gathering

In cybersecurity, every successful attack is based on gathering in-depth information about the target system. In this sense, the "Information Gathering" process is critical to the success of attacks against the target machine. In this section, we will cover the first and most important stage of the penetration process, the information gathering steps involving the `Telnet` service.

At this stage, we are aiming to obtain detailed information by performing scans directly on the target system. With our scans, more specific information is obtained, such as the version of the Telnet service, the ports it is running on, and other service information running on the system.

The tools and methods to be used in this process may vary depending on the structure and security level of the target system. For example, popular port scanning tools such as `nmap` and `rustscan` can be used at this stage.

nmap

Nmap (Network Mapper) is a powerful open-source tool widely used in network security. Its main function is to perform network scans to detect the existence of devices on the network, the services they run and open ports. It is used by cybersecurity experts to find vulnerabilities, map network structures and test security defenses.

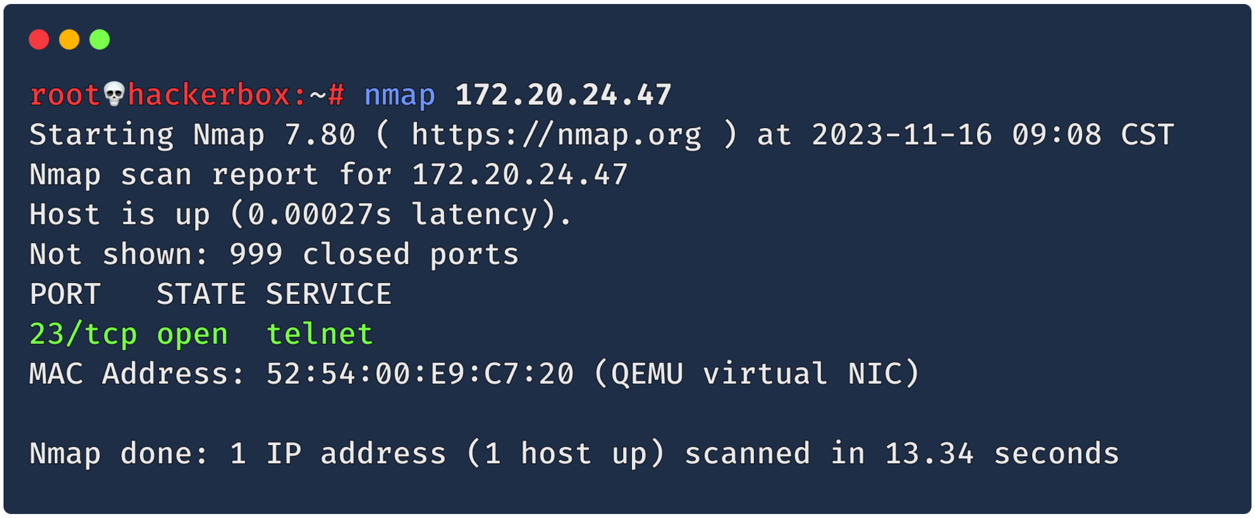
Nmap has a command-line based interface and offers a flexible and wide range of scanning options.

The usage and some important parameters of the Nmap tool are as follows.

```
nmap <TARGET>
```

```
-sS : It scans the ports of the target machine with TCP SYN packets.
      nmap -sS <TARGET>

-sT : It scans the ports of the target machine with TCP Connect packets.
      nmap -sT <TARGET>

-sV : Detects the versions of services running on the target machine.
      nmap -sV <TARGET>

-A :  Aggressive scanning. Performs a comprehensive scan on the target.
Performs service version, operating system detection and script scanning.
      nmap -A <TARGET>

-O :  It tries to detect the operating system running on the target system.
      nmap -O <TARGET>

-p :  Used to scan specific ports or a range of ports.
      nmap -p 80,443 <TARGET> // Scans ports 80 and 443.
      nmap -p 1-2000 <TARGET> // Scans ports between 1 and 2000.
      nmap -p- <TARGET>       // Scans all ports (65,536).
```

Task 1, Task 2
We run an nmap scan on the target machine to get open port and service information.



```
root💀hackerbox:~# nmap 172.20.24.47
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-16 09:08 CST
Nmap scan report for 172.20.24.47
Host is up (0.00027s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 52:54:00:E9:C7:20 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

Initial Access

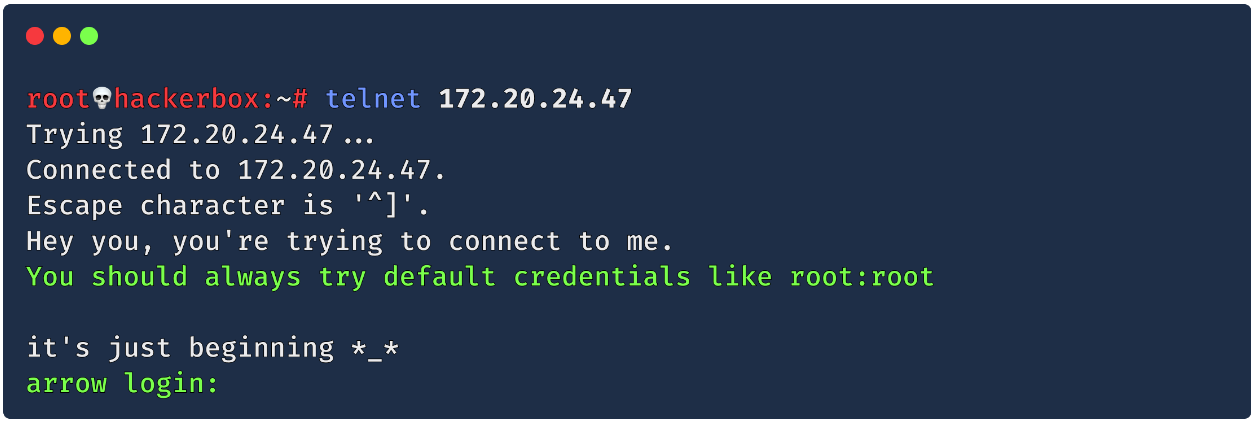
This is the stage where the knowledge gained in the previous information gathering phase is put into practical application and the first real interaction with the target system begins. This is a critical step in making a comprehensive assessment of the security status of the system.

Activities performed during the access phase usually include exploiting vulnerabilities, bypassing firewalls and privilege escalations on the system. During this process, ethical hackers or security analysts test the security measures in the target system and identify potential vulnerabilities.

Task 3, Task 4

We will try to connect to the telnet service that we discovered working by doing a port scan in the previous step. For this, let's run the following command.

```
telnet 172.20.24.47
```



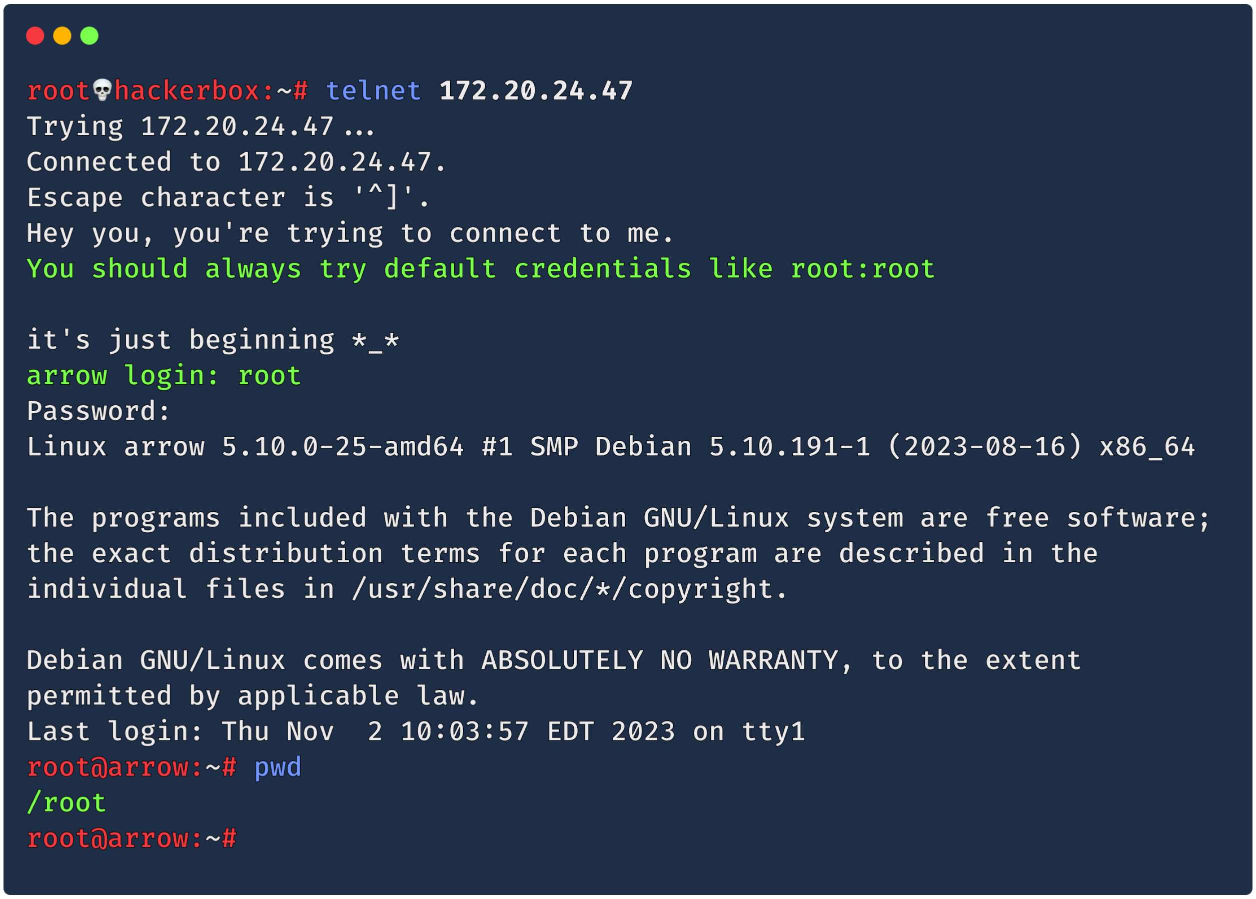
```
root💀hackerbox:~# telnet 172.20.24.47
Trying 172.20.24.47...
Connected to 172.20.24.47.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login:
```

When trying to connect to the target machine with Telnet, we get a hint. The hint tells us to try very simple passwords that can be used by default, such as **`root`** for the username and **`root`** for the password.

Also, in the line that says **`arrow login`**, we see that the hostname of the machine we are trying to connect to is **`arrow`**.

Task 5

To complete task 5, let's login with the `root:root` credentials given to us as a hint.



```
root💀hackerbox:~# telnet 172.20.24.47
Trying 172.20.24.47...
Connected to 172.20.24.47.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login: root
Password:
Linux arrow 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov  2 10:03:57 EDT 2023 on tty1
root@arrow:~# pwd
/root
root@arrow:~#
```

After login, we just need to run the `pwd` command to view our working directory.

-

Congratulations 🙌

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