Bandit 14-15 Walkthrough

Intro

This is a walkthrough of how I solved OverTheWire's Bandit 14-15 problem. To start, I analyzed the commands ssh, telnet, nc, openssl, s_client, and Nmap. I ruled out openssl and s_client because they use SSL encryption, which the goal doesn't mention. Nmap is a scanning tool, so it won't do. Leaving ssh, telnet, and nc (Netcat). The ssh command isn't commonly used for transferring files, unlike telnet and netcat, but I attempted to use it anyway.

Note: I omitted the passwords for Bandit 14 and 15 throughout this write-up.

Attempt #1

Using the credentials from the previous level, I used ssh to connect to the server. `ssh bandit14@bandit.labs.overthewire.org -p 2220`. Then, I tried SSH into bandit15, with "bandit15" as the user and localhost as the host at port 30000. This attempt produced the following result:

```
bandit14@bandit:~$ ssh bandit15@localhost -p 30000
Connection closed by 127.0.0.1 port 30000
```

Attempt #2

Clearly, that didn't work. Next, I tried Netcat because I had previous experience with it. I used a Netcat cheat sheet and crafted this command: `nc localhost 30000`. I got this response after I executed the command and pasted the flag for bandit14.

```
bandit14@bandit:~$ nc localhost 30000
[FLAG14_REDACTED]
Correct!
[FLAG15_REDACTED]
```

Yay! Objective complete.

Attempt #3

I was reading telnet's manpage while writing this walkthrough, and I realized that it is very similar to Netcat. They are both designed for remote interfacing but have different protocols. As an experiment, I retried the problem using telnet. I once again found a cheat sheet that gave me the command below.

```
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
[FLAG14_REDACTED]
Correct!
[FLAG15_REDACTED]

Connection closed by foreign host.
```

Summary

There are two ways to solve Bandit 14-15. Both Netcat and telnet can open an interface with the server where you can enter the password for Bandit 14, and the server will respond with the password for Bandit 15.