Bandit Wargame

What is the Bandit Wargame?

The bandit wargame is a sequence of challenges aimed at teaching user some of the basic Linux command-line tools with a "hacking" mindset in a gamified fashion. Being able to navigate the Linux terminal is an essential skill to have in the long run, and this (ungraded) assignment hopes to get you started on that road (special emphasis on "*started*").
The website description itself states the most important strategy to progress in the wargame:
You will encounter many situations in which you have no idea what you are supposed to do. ***Don't panic! Don't give up!*** *The purpose of this game is for you to learn the basics. Part of learning the basics, is reading a lot of new information. If you've never used the command line before, a good first read is this introduction to user commands.*

Instructions

Go to `https://overthewire.org/wargames/bandit/` to access the bandit wargame.

Entering Level 0

To get started, you need to access the bandit server. The server has different users for different levels. As mentioned in the website instructions, the user for the zeroth level is *bandit 0*.
You will use the SSH (Secure Shell) protocol to communicate with the server. SSH is a protocol used to securely send commands and data over to a remote machine over an insecure network. The protocol uses several cryptographic techniques you'll learn in this course to enable authentication and ensure encryption of the data being sent over the insecure network.

1. Open up your terminal (if on Linux/Mac) or open up WSL Ubuntu (if on Windows).

2. The `ssh` command-line tool can be used to communicate with a remote server using the SSH protocol (yes, the protocol is named SSH and the command-line tool is called `ssh`). The format for using the `ssh` CLI tool (at least for now) is:

   ```
   ssh <username>@<hostname> -p <port_number>
   ```

   In our case, the username is *bandit0* as given to us in the instructions. The hostname is *bandit.labs.overthewire.org* and the port number is *2220*. So, submit
   `ssh bandit0@bandit.labs.overthewire.org -p 2220` into the terminal.

3. If asked whether you're sure about continuing to connect, enter *yes*.

4. **Note about IITB Wireless:** IITB Wireless blocks non-standard ports such as port *2220* used by the bandit server. If you're unable to connect to the server while on the IITB Wireless network, this is most likely the reason. This could be mitigated in one of two ways:

   (a) Create a wifi hotspot from your phone using your mobile data. Connect your laptop to this hotspot.

   (b) Use a VPN of your choice on your laptop.

5. When asked for the password, enter the password *bandit0* as given in the instructions. When you type in the password, it wouldn't be visible on your terminal. Don't worry, your password is still being typed, this is just a security mechanism to ensure no one peering into your computer screen can read off either your password or the length of your password.

6. If you see the OTW logo printed on your terminal, you're in! Make sure to read the instructions and descriptions that pop up on your terminal when you login to get a better understanding of the structure of the challenges!

Level 0 → Level 1

As mentioned in the instructions for Level 0 → Level 1 on the bandit website, the password is written in the readme file located at the home directory.

1. Enter `ls` into the terminal to list the files on the current directory (which is the home directory, represented by ∼). Note that it list `readme` as a file present in the directory.

2. Enter `cat readme` to read the contents of the readme file. `cat` is used to read the contents of files.

3. Note down the password (or copy it to the clipboard). Enter `exit` to terminate the SSH connection to the remote server.

4. Access the next level by entering `ssh bandit1@bandit.labs.overthewire.org` into your terminal. When asked for a password, enter the password you had obtained.

Level 1 → Level 2 and Beyond

You can now proceed through the levels on your own. The instruction for each level can be found in the bandit website. Solving these levels would require Googling and learning more about Linux CLI tools and certain "hacks" about some of them. The bandit website even lists down some helpful reading material and useful commands for each level. Search them up on Google to both increase your Linux CLI prowess and to progress deeper into the bandit wargame.

Assignment

You can go as far as you please; in fact, you could even try completing the entire bandit wargame. However, for the purposes of this (ungraded) assignment, you can consider completing `Level 13` → `Level 14` as the end of the assignment.

Python References

Enter Python!

We would be using Python in the labs for this course to script exploits and the likes. An elementary understanding of the Python language would completely suffice. In addition to that, the following concepts/libraries in Python could come in handy with respect to the cryptography labs.

Bytes Objects and Bytes Arrays

These come in use a lot in cryptographic applications. You can learn more about them at https://www.w3resource.com/python/python-bytes.php.

PyCryptodome Library

This is a very useful library in python for cryptographic purposes. This can be installed by running the command

```
pip install pycryptodome
```

on the terminal.
This library has a lot of useful functions which you can pick up as you progress with the labs. You will see some of them used in the scripts provided to you and you can even use some of the functions in the library to ease writing your solution scripts!
You can refer to https://pycryptodome.readthedocs.io/en/latest/src/api.html for documentation on this library. Refer to this page as you come across functions used from this library in your labs.

[Optional] Pwntools

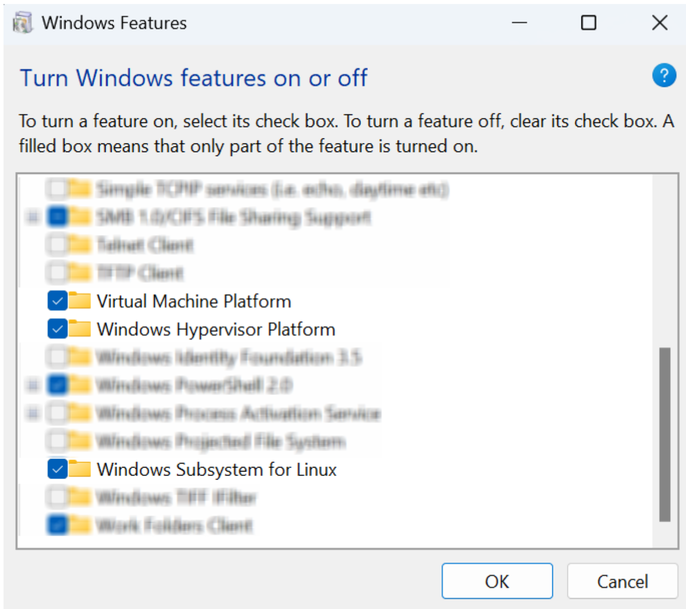
In some challenges, you will need to interact with a remote server. We will use the pwntools library to enable this communication. For the purposes of the labs in this course, you will always be given template code that does the server communication for you so you will **never** need to code it up yourself; however, if you plan on solving CTF challenges outside of this course, picking up this library is a must.
You can refer to https://github.com/Gallopsled/pwntools-tutorial/blob/master/tubes.md for an introduction on how to use pwntools to interact with remote servers and local processes.

Windows - WSL Ubuntu Installation

Instructions

1. On Windows Search, search for *Turn Windows features on or off*. Make sure the following boxes are checked:

    - Virtual Machine Platform
    - Windows Hypervisor Platform
    - Windows Subsystem for Linux

    Windows Features

    Turn Windows features on or off

    To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

    □ Simple TCPIP services (i.e. echo, daytime etc)
    ☑ SMB 1.0/CIFS File Sharing Support
    □ Telnet Client
    □ TFTP Client
    ☑ Virtual Machine Platform
    ☑ Windows Hypervisor Platform
    □ Windows Identity Foundation 3.5
    ☑ Windows PowerShell 2.0
    □ Windows Process Activation Service
    □ Windows Projected File System
    ☑ Windows Subsystem for Linux
    □ Windows TIFF IFilter
    ☑ Work Folders Client

    You might be asked to reboot your system. Go ahead and do it.

2. Press **Windows Key** (⊞) + **R** to open *Run*. Type in `powershell.exe` and press **Enter** to open up Windows PowerShell.

3. Enter `wsl --list --online` into the PowerShell console to see all the available distros on your system.

4. Enter `wsl --update; wsl --update --pre-release` to ensure that the most recent version of WSL installed in your system.

5. Enter `wsl --install -d Ubuntu-22.04` to install the distro on your machine. If asked for a username and password, create a username and password for your Linux account.
    Important: Remember your username and password!

6. If you enter the WSL terminal, enter `exit` to exit and continue. If not, continue ahead regardless.

7. Reboot your system once.

8. Open up PowerShell again and type in `wsl` to launch Ubuntu-22.04 on WSL on your machine. Congratulations! You're now inside the matrix!