

# Bandit: Level 0 → 1 — Cheat-sheet & README

A compact, friendly guide for completing OverTheWire **Bandit** Level 0 → 1. Includes the tools used, quick commands, and helpful tips.

---

## Overview

This README covers the exact steps and common tools used to complete Bandit **Level 0 → 1**. It's designed to be a quick reference while you practice on the challenge server.

## Credentials & Connection

- **Host:** `bandit.labs.overthewire.org`
- **Port:** `2220`
- **Level 0 credentials:**
- **User:** `bandit0`
- **Password:** `bandit0`

**SSH command to connect:**

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

---

## Tools Used (what they do and examples)

`ssh`

Secure shell — used to connect to the remote Bandit server.

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Notes: - `-p 2220` specifies the custom port Bandit uses. - If you see a host key warning, use `ssh-keygen -R` to remove the old entry (see below).

`ls`

Lists files in the current directory.

```
ls -la
```

Useful to check for files like `readme`.

`cat`

Prints file contents to the terminal. Used to read the `readme` file containing the next-level password.

```
cat readme
```

`file`

Identifies the type of a file (text, binary, etc.). Helpful if a file doesn't look like plain text.

```
file readme
```

`less` / `more`

Pagers to view long files one page at a time. Quit with `q`.

```
less filename
```

`ssh-keygen -R`

Removes an entry from `~/.ssh/known_hosts` if the server's host key changed.

```
ssh-keygen -R "[bandit.labs.overthewire.org]:2220"
```

---

## Quick step-by-step workflow

### 1. Connect to the server:

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

### 2. List files in the home directory:

```
ls -la
```

### 3. Read the `readme` file to get the password for level 1:

```
cat readme
```

#### 4. Log into level 1 using the password you found.

---

## Tips & Safety

- Avoid putting passwords on the command line in long-term practice; let `ssh` prompt you interactively when possible.
  - Don't share CTF passwords publicly if you plan to continue the challenge series.
  - Use `less` for longer files to avoid flooding your terminal.
  - If you encounter host key warnings, remove the old host key with `ssh-keygen -R "[host]:port"` and reconnect to accept the new key.
- 

## Want more?

If you want, I can: - Add Level 1 → 2 walkthrough steps in the same file. - Create a printable one-page cheat-sheet. - Generate a short shell alias or script to automate the connect step (safe option that prompts for a password).

Good luck and enjoy Bandit! 🎯