

# OverTheWire Bandit Wargame

---

Name : Prateek

Intern ID : 166

The **Bandit wargame** is a series of beginner-friendly Linux challenges hosted on the **OverTheWire** platform. Its primary goal is to teach players the basics of using the **Linux command-line environment**, navigating the filesystem, handling files, and performing simple security-related tasks. Each level introduces Linux commands and concepts that help build foundational skills for security, system administration, and Capture the Flag (CTF) challenges.

## Core Commands Used

Throughout these levels, the following Linux commands and tools were essential:

- **ssh** → Connect securely to a remote machine (used to log into each level).
- **ls** → List files and directories in the current location.
- **cd** → Change directory.
- **pwd** → Print the current working directory.
- **cat** → Display the contents of a file.
- **file** → Identify the file type.
- **du** → Show file/directory disk usage (often to locate files by size).
- **find** → Search for files by name, size, permissions, etc.
- **grep** → Search for text patterns inside files.
- **sort** → Sort lines of text.
- **uniq** → Filter out or detect duplicate lines.
- **strings** → Extract human-readable strings from binary files.
- **base64** → Encode/decode base64 data.
- **tr** → Translate or replace characters (e.g., ROT13).
- **tar** → Extract or compress .tar archive files.
- **gzip/gunzip** → Compress/uncompress .gz files.
- **bzip2/bunzip2** → Compress/uncompress .bz2 files.
- **xxd** → Create or reverse hexdumps.
- **cp** → Copy files.
- **mv** → Move/rename files.

- **mkdir** → Create a new directory.
- **mktemp -d** → Create a temporary directory with a random name.
- **less/more** → View file contents page by page.
- **head/tail** → View first or last lines of a file.
- **nc (netcat)** → Read/write data to network connections (send password to ports).
- **telnet** → Simple TCP connection tool (like nc, older).
- **ncat** → Enhanced netcat with SSL support.
- **socat** → Advanced tool to connect or forward between sockets.
- **openssl s\_client** → Connect to SSL/TLS services and interact with them.
- **nmap** → Network mapper, scans for open ports and services.
- **netstat** → Show active network connections/ports (older tool).
- **ss** → Modern replacement for netstat to view sockets.
- **whoami** → Show the current logged-in username.
- **id** → Show user ID and group ID.
- **chmod** → Change file permissions.
- **touch** → Create an empty file or update timestamps.
- **echo** → Print text or pass strings into commands.
- **man** → Display manual pages (help) for commands.

## Level Summaries (0 → 20)

### Level 0 → 1

Login via SSH using given credentials. Learn to connect to a remote system.

### Level 1 → 2

Find password stored in a file named `` which requires './' to access.

### Level 2 → 3

Password hidden in a file with spaces in its name; escape spaces with quotes or backslashes.

### Level 3 → 4

Look inside a hidden file in a directory.

### Level 4 → 5

Identify the human-readable file among many using 'file' command.

### Level 5 → 6

Find file based on conditions: human-readable, specific size, non-executable using 'find'.

### Level 6 → 7

Search for password in a file owned by user bandit7 and group bandit6.

### Level 7 → 8

Password hidden inside a text file; use 'grep' to locate it.

### Level 8 → 9

Sort and find unique password string using 'sort' and 'uniq'.

### Level 9 → 10

Extract printable characters from binary file with 'strings'.

### Level 10 → 11

Password is encoded in base64; decode using 'base64 -d'.

### Level 11 → 12

ROT13 encoding used; decode using 'tr'.

### Level 12 → 13

Password hidden in a repeatedly compressed file; use 'xxd', 'tar', 'gzip', 'bzip2' iteratively.

### Level 13 → 14

Use provided SSH private key to login as bandit14.

### Level 14 → 15

Send current password to correct localhost port (31000-32000) using 'nc' and 'openssl'.

### Level 15 → 16

Submit password via SSL-enabled service using 'openssl s\_client'.

### Level 16 → 17

Scan ports with 'nmap', test SSL with 'openssl', retrieve private SSH key for next login.

### Level 17 → 18

Use 'diff' to compare files and spot password difference.

### Level 18 → 19

Escape forced command shell; use SSH with options to bypass.

### Level 19 → 20

Setuid binary used to execute commands as bandit20 and read their password.

## Level 20 → 21

Connect to localhost with special binary and port forwarding to retrieve next password.

```
File Edit View
d8BcFry9gPum8p3LmXkAtMhPvfe0950k9TL5wqbu9AlbsgTcCkKQnPeNc
YNN600P2lbcBrvgT9YCNL6C+zkuf052y0Q9qkQwFTQpJTFaUttJom+asvlpmsBA
vLY966wVsvzHnqBunJ7lycTXMTuikkd4w7F77kDjH0AXyxcUp1DGL5150mama
+T0MgEGcYEABtPxP0GRJ+IQkX262JH3dE1kzabky5mo1wUqVdsX0NhxigRRH0T
8c8hAU8B2G82s08vUHK/fur850Efc91ncnC2zcrpqsgHifKLxrlgtT+q0pfzmx
SattdtBfG0syA7hmM2JwF3lms50m7SLme+tb0ALy0P2j0HhP5KcPFEAyphd
KCtnH/PwJulhtFz/nwXhLidZ0FyeiE/v45bMaymax7R/b0E7kaszx1Exdyt
SghatdcGknydlbp7YyusavP2paJHjd3etcfHABahjm7enc1vccsxx3155lwg0A
R57h3glez1lvj3a0wHv1ZvtszK6ZV60FAu0ECgVAbJ046T4hyPSTj193V5HdI
TtieK7XrvXU1+iu7rnkGAXFmLFtqeQsr7P3/lemmEYseTDAFmly9FL2m0Q0KcG
R8VdSk8r9FGLS+9akcVSPi/MEKlWpXinB30HyimtiG2c53qGIZFHdQmJE60iu
lBk4HwPv0bmsSRutp00K0BqJlFciH0mHMG0JX0PwrtBOCdfkmJomB0l
bhloelyZ9FseXsgt8BXRsqXuz7Wts0AgUhbDd.q/Z3Q7YfZ0K04ZEnabvXnv4ku
Y0dJHd500KvDQWuucyLRAWuISeXw9a/9p7fpxm0TSgyvafLF2HIAEwyZ8qAm
77pBAOGAfmj1dJp+Ez8duyn3ie036yrttF5NS53LABxfpdlc1gtvGCMW+9Cq0b
dxv1W8+TFVEB1104f7HvM6EptscdbXu+bcXukfJurb70y9G0tT9JpX8MBTakh3
y8gsyl/sH3Rg8cGU40f00zyfAMT81m/uYV52061geuz/uj3jY+

17 x2gLTjFwH0hQ80wBmN362QKcFrqG10
< QqPdV6c2Ncstw7dg4MbSh4vXwY7pHmE
---
> x2gLTjFwH0hQ80wBmN362QKcFrqG10
18 cGpHakXv0UngPAVjbmYUgHvN9z13j8
19 ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8Zj0VMN9Ghs7i0WscFzyX0ubY0
20
bandit20@bandit:/etc/bandit_pass$ echo "0qXahG8Zj0VMN9Ghs7i0WscFzyX0ubY0" | netcat -lp 1234 &
[1] 3058122
bandit20@bandit:/etc/bandit_pass$ jobs
[1]+  Running                  echo "0qXahG8Zj0VMN9Ghs7i0WscFzyX0ubY0" | netcat -lp 1234 &
./suconnect 1234
EeoULMCra2q8dskYj561DX7s1cpBu0Bt

Ln 68, Col 1 1056 characters Plain text 100% Windows (CRLF) UTF-8
24°C Mostly cloudy 17:18 16-08-2025
```

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
bandit20@bandit:/etc$ cd /bandit_pass
-bash: cd: /bandit_pass: No such file or directory
bandit20@bandit:/etc$ cd bandit_pass
bandit20@bandit:/etc/bandit_pass$ ls
bandit0 bandit13 bandit18 bandit22 bandit27 bandit31 bandit6
bandit11 bandit14 bandit19 bandit23 bandit28 bandit32 bandit7
bandit10 bandit15 bandit2 bandit24 bandit29 bandit33 bandit8
bandit11 bandit16 bandit20 bandit25 bandit3 bandit4 bandit9
bandit12 bandit17 bandit21 bandit26 bandit30 bandit5
bandit20@bandit:/etc/bandit_pass$ cat bandit19
cat: bandit19: Permission denied
bandit20@bandit:/etc/bandit_pass$ echo "0qXahG8Zj0VMN9Ghs7i0WscFzyX0ubY0" | n
etcat -lp 1234 &
[1] 3058122
bandit20@bandit:/etc/bandit_pass$ jobs
[1]+  Running                  echo "0qXahG8Zj0VMN9Ghs7i0WscFzyX0ubY0" | netca
t -lp 1234 &
bandit20@bandit:/etc/bandit_pass$ ls
bandit0 bandit13 bandit18 bandit22 bandit27 bandit31 bandit6
bandit11 bandit14 bandit19 bandit23 bandit28 bandit32 bandit7
bandit10 bandit15 bandit2 bandit24 bandit29 bandit33 bandit8
bandit11 bandit16 bandit20 bandit25 bandit3 bandit4 bandit9
bandit12 bandit17 bandit21 bandit26 bandit30 bandit5
bandit20@bandit:/etc/bandit_pass$ cd ..
bandit20@bandit:/etc$ cd ..
bandit20@bandit:/etc$ ls
behemoth formulaone libx32 opt srv
bin bin.usr-is-merged home lost+found proc sys
boot lib manpage root tmp
dev lib32 media sbin utumno
```

### OverTheWire: Level Goal: Bandit

SSH Information  
Host: bandit.labs.overthewire.org  
Port: 2220

## Bandit Level 20 → Level 21

### Level Goal

There is a setuid binary in the homedirectory that does the following: it makes a connection to localhost on the port you specify as a commandline argument. It then reads a line of text from the connection and compares it to the password in the previous level (bandit20). If the password is correct, it will transmit the password for the next level (bandit21).

**NOTE:** Try connecting to your own network daemon to see if it works as you think

### Commands you may need to solve this level

ssh, nc, cat, bash, screen, tmux, Unix 'job control' (bg, fg, jobs, &, CTRL-Z, ...)

```
File Edit View H1 I E V ...
> x2gLTjFwH0hQ80wBmN362QKcFrqG10
18 cGpHakXv0UngPAVjbmYUgHvN9z13j8
19 ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8Zj0VMN9Ghs7i0WscFzyX0ubY0
20 EeoULMCra2q8dskYj561DX7s1cpBu0Bt
```