OverTheWire Bandit Walkthrough – Levels 0 to 20

This document is a walkthrough of the first 20 levels of the OverTheWire Bandit wargame, which focuses on Linux-based security challenges. Completing these levels demonstrates hands-on skills with Linux commands, file system navigation, and basic security practices.

## Level 0

Login via SSH: ssh bandit0@bandit.labs.overthewire.org -p 2220, password: bandit0

## Level 1

Read file named '-': cat ./- or cat -- -

## Level 2

Find and read a hidden file: ls -a, then cat .hidden

## Level 3

Read a file in 'inhere': cd inhere, ls, then cat <filename>

## Level 4

Identify human-readable file: file ./\*, then cat the appropriate file

## Level 5

Find file with 1033 bytes: find . -type f -size 1033c

## Level 6

Find file with user bandit7, group bandit6, 33 bytes: find / -user bandit7 -group bandit6 -size 33c 2>/dev/null

## Level 7

Find line containing 'millionth': grep 'millionth' data.txt

## Level 8

Find unique line: sort data.txt | uniq -u

## Level 9

Decode base64: cat data.txt | base64 -d

## Level 10

Decode with ROT13: cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'

## Level 11

Extract with xxd and decode: xxd -r data.txt > newfile, then check format and decode

## Level 12

Get password stored in a hexdump encoded file

## Level 13

Use ssh key: ssh -i sshkey.private bandit14@localhost

## Level 14

Connect via nc and extract password: nc localhost 30000

## Level 15

Connect via SSL: openssl s\_client -connect localhost:30001

## Level 16

Port scan with nmap or nc to find service, then connect and retrieve password

## Level 17

Connect via SSH with password from port, extract password using grep

## Level 18

Get password stored in a bash script file

## Level 19

Run binary with different permissions, extract password from result

## Level 20

Find SUID binary and execute it to get password