Bandit Write-Up: Levels 15—>20

OverTheWire Bandit Write-Up: Level 15 → Level 16

This write-up covers the transition from **Level 15 to Level 16** in OverTheWire's Bandit wargame, including the SSH connection process and solving the challenge. The format follows the same structure as the previous write-ups, with screenshots provided for reference.

Level 15 → Level 16: Submitting the Password Using SSL/TLS

Level Goal

- The password for the next level can be retrieved by submitting the password of the current level to port 30001 on `localhost` using SSL/TLS encryption.

Steps to Solve Level 15 → Level 16

1. Log into Bandit15

Command

`ssh` `bandit15@bandit.labs.overthewire.org` `-p 2220`

Password for SSH Login

- The password for `bandit15` is: `8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo`

```
┌──(llamafart㉿jaivanti)-[~]
└─$ ssh bandit15@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit15@bandit.labs.overthewire.org's password:

      ,----..            ,----,         .---.
     /   /   \        ,/   .`|        /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :    | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

Explanation

- The `ssh` command is used to connect to the Bandit server.
- `bandit15` is the username for Level 15.
- `bandit.labs.overthewire.org` is the server address.
- `-p 2220` specifies the port number.

2. Submit the Password to Port 30001 Using SSL/TLS

Command

`openssl s_client -connect localhost:30001`

```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
   i:CN = SnakeOil
   a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
```

Explanation

- The `openssl s_client` command is used to connect to a server using SSL/TLS.
- `connect localhost:30001` specifies the server and port to connect to.
- After establishing the connection, paste the password for Level 15.

Input

`8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo`

Output

`Correct!`
`kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx`

3. Logout

Command

`logout`

```
read R BLOCK
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed
bandit15@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.

┌──(llamafart㉿jaivanti)-[~]
└─$
```

Password for Level 16

- The password for `bandit16` is: `kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx`

Screenshots

```
┌──(llamafart㉿jaivanti)-[~]
└─$ ssh bandit15@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                       This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit15@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \        ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :    | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
   i:CN = SnakeOil
   a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
```

```
read R BLOCK
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed
bandit15@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.

┌──(llamafart㉿jaivanti)-[~]
└─$
```

- The screenshot shows the terminal after logging into `bandit15`.

- The `openssl s_client -connect localhost:30001` command is used to establish an SSL/TLS connection.
- The screenshot shows the terminal after submitting the password for Level 15.
- The server responds with the password for Level 16.

Conclusion

This level teaches how to interact with SSL/TLS encrypted services using the `openssl s_client` command. By establishing a secure connection and submitting data, you can retrieve information or perform actions on remote servers. This skill is essential for working with secure network protocols and services in real-world scenarios.

Level 16 → Level 17: Finding and Submitting to an SSL/TLS Server

Level Goal

- The credentials for the next level can be retrieved by submitting the password of the current level to a port on `localhost` in the range 31000 to 32000. First, find out which of these ports have a server listening on them. Then, find out which of those speak SSL/TLS and which don't. There is only 1 server that will give the next credentials; the others will simply send back whatever you send to them.

Steps to Solve Level 16 → Level 17

1. Log into Bandit16

Command

`ssh` `bandit16@bandit.labs.overthewire.org` `-p 2220`

Password for SSH Login

- The password for `bandit16` is: `kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx`

```
┌──(llamafart㉿jaivanti)-[~]
└─$ ssh bandit16@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit16@bandit.labs.overthewire.org's password:

      ,----..            ,----,         .---.
     /   /   \        ,/   .`|        /. ./|
    /   .     :      ,`    .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :    | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  | \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /        '   :  |     :    '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

Explanation

- The `ssh` command is used to connect to the Bandit server.
- `bandit16` is the username for Level 16.
- `bandit.labs.overthewire.org` is the server address.
- `-p 2220` specifies the port number.

2. Scan for Open Ports in the Range 31000-32000

Command

`nmap localhost -p 31000-32000`

Explanation

- The `nmap` command is used to scan for open ports on `localhost`.
- `-p 31000-32000` specifies the port range to scan.
- The output shows which ports are open and listening.

3. Test Each Open Port for SSL/TLS

Commands

`openssl s_client -connect localhost:<port>`

Explanation

- The `openssl s_client` command is used to connect to a server using SSL/TLS.
- Replace `<port>` with each open port found in the previous step.
- Test each port to see if it responds with the credentials for the next level.

4. Submit the Password to the Correct Port

Command

`openssl s_client -connect localhost:31790`

Input

`kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx`

Output

`Correct!`

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

5. Logout

Command

`logout`

```
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 16:30 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00022s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
bandit16@bandit:~$ ncat --ssl localhost 31046
Ncat: Input/output error.
bandit16@bandit:~$ ncat --ssl localhost 31518
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
^C
bandit16@bandit:~$ ncat --ssl localhost 31691
Ncat: Input/output error.
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

^C
bandit16@bandit:~$
```

Private Key for Level 17

- The private key for `bandit17` is:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

Screenshots

```
┌──(llamafart㉿jaivanti)-[~]
└─$ ssh bandit16@bandit.labs.overthewire.org -p 2220
                      _                     _ _ _
                     | |__   __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


                    This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit16@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`    .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :    | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  | \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

```
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 16:30 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00022s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
bandit16@bandit:~$ ncat --ssl localhost 31046
Ncat: Input/output error.
bandit16@bandit:~$ ncat --ssl localhost 31518
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
^C
bandit16@bandit:~$ ncat --ssl localhost 31691
Ncat: Input/output error.
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

^C
bandit16@bandit:~$
```

- The screenshot shows the terminal after logging into `bandit16`.
- The `nmap localhost -p 31000-32000` command is used to scan for open ports.
- The screenshot shows the terminal after submitting the password for Level 16.
- The server responds with the private key for Level 17.

Conclusion

This level teaches how to scan for open ports and interact with SSL/TLS encrypted services using the `nmap` and `openssl s_client` commands. By identifying the correct port and submitting the password, you can retrieve the credentials for the next level. These skills are essential for working with network services and secure protocols in real-world scenarios.

Level 17 → Level 18: Finding the Changed Password

Level Goal

- There are 2 files in the home directory: `passwords.old` and `passwords.new`. The password for the next level is in `passwords.new` and is the only line that has been changed between `passwords.old` and `passwords.new`.

Steps to Solve Level 17 → Level 18

1. Log into Bandit17

Command

`ssh -i key` `bandit17@bandit.labs.overthewire.org` `-p 2220`

Private Key for SSH Login

- The private key for `bandit17` is:


```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSXiJSWL7TqeXh+cAMTSMLOJf7+BrJ0bArnxd9YYXT2bRPQ
Ja6Lzb558YWB7Z1870Rio+rw4LCDCNA21UvLE/GL2GWyuKNOK51Cd5TbLJZEKQTu
dxv1W8+TFVE1l04f7HVM6EpTscdbxU+bCXWkfjURb7by96ottoJPsX8MBTaKzh3
VBgsy1/sN3RqRBCGU40foozyfAMT8sim/uYv5206IgeuZ/ujbjy-
-----END RSA PRIVATE KEY-----
```

```
┌──(llamafart㉿jaivanti)-[~/key]
└─$ chmod 400 key

┌──(llamafart㉿jaivanti)-[~/key]
└─$ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220
                      _
                     | |__   __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


                   This is an OverTheWire game server.
           More information on http://www.overthewire.org/wargames


     ,----..            ,----,          .---.
    /   /   \        ,/   .`|         /. ./|
   /   .     :      ,`    .'  :     .--'.  ' ;
  .   /   ;.  \   ;    ;     /    /__./ \ : |
 .   ;   /  ` ; .'___,/    ,' .--'.   '   \' .
 ;   |  ; \ ; | |    :    | /___/ \ |    ' '
 |   :  | ; | ' ;    |.';  ; ;   \  \;      :
 .   |  ' ' ' : `----'  |  |  \   ;  `      |
 '   ;  \; /  |     '   :  ;   .   \    .\  ;
  \   \  ',  /      |   |  '    \   \   ' \ |
   ;   :    /       '   :  |     :   '  |--"
    \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

Explanation

- The `ssh -i` command is used to log into the server using a private key.
- `key` is the private key file.
- `bandit17` is the username for Level 17.
- `bandit.labs.overthewire.org` is the server address.
- `-p 2220` specifies the port number.

2. List the Contents of the Home Directory

Command

`ls`

Explanation

- The `ls` command lists all files and directories in the current directory.
- This reveals the files `passwords.old` and `passwords.new`.

3. Compare the Files to Find the Changed Password

Command

`diff passwords.old passwords.new`

Explanation

- The `diff` command compares the contents of two files and shows the differences.
- The output indicates the line that has been changed between `passwords.old` and `passwords.new`.

4. Logout

Command

`logout`

```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< ktfgBvpMzWKR5ENj26IbLGSblgUG9CzB
---
> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
bandit17@bandit:~$
```

Password for Level 18

- The password for `bandit18` is: `x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO`

Screenshots

```
┌──(llamafart㉿jaivanti)-[~/key]
└─$ chmod 400 key

┌──(llamafart㉿jaivanti)-[~/key]
└─$ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220
                      _                     _ _ _
                     | |__   __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


                    This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames


      ,----..            ,----,         .---.
     /   /   \         ,/   .`|        /. ./|
    /   .     :      ,`    .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :    | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< ktfgBvpMzWKR5ENj26IbLGSblgUG9CzB
---
> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
bandit17@bandit:~$
```

- The screenshot shows the terminal using the private key to log into `bandit17`.
- The screenshot shows the terminal after logging into `bandit17`.
- The `diff passwords.old passwords.new` command is used to find the changed password.

Conclusion

This level teaches how to compare files to find differences using the `diff` command. By identifying the changed line, you can retrieve the password for the next level. This skill is useful for analyzing changes in files and logs in real-world scenarios.

Level 18 → Level 19: Bypassing a Modified `.bashrc`

Level Goal

- The password for the next level is stored in a file `readme` in the home directory. Unfortunately, someone has modified `.bashrc` to log you out when you log in with SSH.

Steps to Solve Level 18 → Level 19

1. Log into Bandit18

```
┌──(llamafart㉿jaivanti)-[~]
└─$ ssh bandit18@bandit.labs.overthewire.org -p 2220
                      _                     _ _ _
                     | |__   __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


                    This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`    .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :    | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

```
  Enjoy your stay!

Byebye !
Connection to bandit.labs.overthewire.org closed.

┌──(llamafart㉿jaivanti)-[~]
└─$ 
```

```
┌──(llamafart㉿jaivanti)-[~]
└─$ cat /etc/shells
# /etc/shells: valid login shells
/bin/sh
/usr/bin/sh
/bin/bash
/usr/bin/bash
/bin/rbash
/usr/bin/rbash
/bin/dash
/usr/bin/dash
/usr/bin/pwsh
/opt/microsoft/powershell/7/pwsh
/usr/bin/screen
/usr/bin/tmux
/bin/zsh
/usr/bin/zsh
```

Command

`ssh` bandit18@bandit.labs.overthewire.org `-p 2220 -t '/bin/sh'`

Password for SSH Login

- The password for `bandit18` is: `x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO`

Explanation

- The `ssh` command is used to connect to the Bandit server.
- `bandit18` is the username for Level 18.
- `bandit.labs.overthewire.org` is the server address.
- `p 2220` specifies the port number.
- `t '/bin/sh'` forces the use of the `/bin/sh` shell, bypassing the modified `.bashrc`.

2. List the Contents of the Home Directory

Command

`ls`

Explanation

- The `ls` command lists all files and directories in the current directory.
- This reveals the file `readme`.

3. Read the Contents of `readme`

Command

`cat readme`

Explanation

- The `cat` command displays the contents of `readme`.
- The output shows the password for Level 19.

4. Logout

Command

`logout`

Password for Level 19

- The password for `bandit19` is: `cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8`

```
┌──(llamafart㉿jaivanti)-[~]
└─$ ssh bandit18@bandit.labs.overthewire.org -p 2220 -t "/bin/sh"
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
$ ls
readme
$ cat readme
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
$
```

Screenshots

```
┌──(llamafart㉿jaivanti)-[~]
└─$ ssh bandit18@bandit.labs.overthewire.org -p 2220
                      _                     _ _ _
                     | |__   __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


                    This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`    .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :    | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /        '   :  |     :   '  |--"
     \   \ .'         ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

```
  Enjoy your stay!

Byebye !
Connection to bandit.labs.overthewire.org closed.

┌──(llamafart㉿jaivanti)-[~]
└─$ 
```

```
┌──(llamafart㉿jaivanti)-[~]
└─$ cat /etc/shells
# /etc/shells: valid login shells
/bin/sh
/usr/bin/sh
/bin/bash
/usr/bin/bash
/bin/rbash
/usr/bin/rbash
/bin/dash
/usr/bin/dash
/usr/bin/pwsh
/opt/microsoft/powershell/7/pwsh
/usr/bin/screen
/usr/bin/tmux
/bin/zsh
/usr/bin/zsh
```

```
┌──(llamafart㉿jaivanti)-[~]
└─$ ssh bandit18@bandit.labs.overthewire.org -p 2220 -t "/bin/sh"
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
$ ls
readme
$ cat readme
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
$ 
```

- The screenshot shows the terminal after logging into `bandit18` using the `/bin/sh` shell.
- The `ls` command lists the `readme` file.
- The `cat readme` command displays the password for Level 19.
- The screenshot shows the terminal listing valid login shells using the `cat /etc/shells` command.
- The screenshot shows the terminal after logging out of `bandit18`.

Conclusion

This level teaches how to bypass a modified `.bashrc` file by specifying a different shell during SSH login. By using the `-t '/bin/sh'` option, you can avoid being logged out and access the necessary files. This skill is useful for troubleshooting and accessing systems with restricted or modified configurations.

Level 19 → Level 20: Using a Setuid Binary

Level Goal

- To gain access to the next level, you should use the setuid binary in the home directory. Execute it without arguments to find out how to use it. The password for this level can be found in the usual place (`/etc/bandit_pass`), after you have used the setuid binary.

Steps to Solve Level 19 → Level 20

1. Log into Bandit19

Command

`ssh` `bandit19@bandit.labs.overthewire.org` `-p 2220`

Password for SSH Login

- The password for `bandit19` is: `cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8`

```
┌──(llamafart㉿jaivanti)-[~]
└─$ ssh bandit19@bandit.labs.overthewire.org -p 2220
                      _                     _ _ _   _ |_
                     | |__  __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


                    This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit19@bandit.labs.overthewire.org's password:

      ,----..            ,----,         .---.
     /   /   \        ,/   .`|        /. ./|
    /   .     :      ,`   .'  :    .--'.  ' ;
   .   /   ;.  \   ;    ;     /   /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :    | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |      '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :    '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

Explanation

- The `ssh` command is used to connect to the Bandit server.
- `bandit19` is the username for Level 19.
- `bandit.labs.overthewire.org` is the server address.
- `-p 2220` specifies the port number.

2. List the Contents of the Home Directory

Command

`ls`

Explanation

- The `ls` command lists all files and directories in the current directory.

- This reveals the setuid binary `bandit20-do`.

3. Execute the Setuid Binary Without Arguments

Command

`./bandit20-do`

Explanation

- The `./bandit20-do` command executes the setuid binary.
- The output provides instructions on how to use the binary.

4. Use the Setuid Binary to Read the Password

Command

`./bandit20-do cat /etc/bandit_pass/bandit20`

Explanation

- The `./bandit20-do` command runs the specified command (`cat /etc/bandit_pass/bandit20`) with the privileges of the `bandit20` user.
- The output shows the password for Level 20.

5. Logout

Command

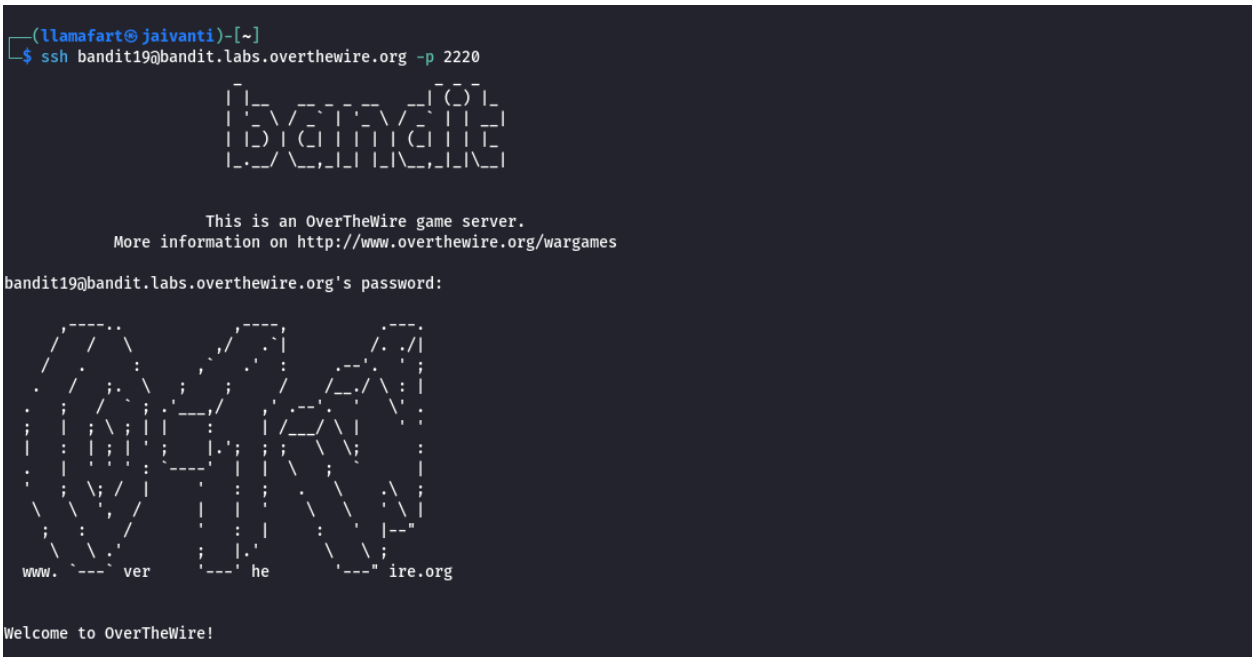
`ls`

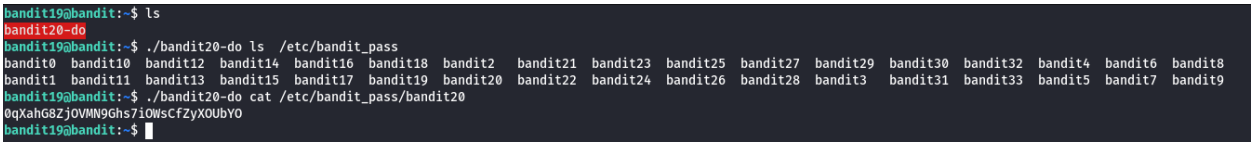
```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do ls  /etc/bandit_pass
bandit0  bandit10  bandit12  bandit14  bandit16  bandit18  bandit2   bandit21  bandit23  bandit25  bandit27  bandit29  bandit30  bandit32  bandit4  bandit6  bandit8
bandit1  bandit11  bandit13  bandit15  bandit17  bandit19  bandit20  bandit22  bandit24  bandit26  bandit28  bandit3   bandit31  bandit33  bandit5  bandit7  bandit9
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
bandit19@bandit:~$
```

Password for Level 20

- The password for `bandit20` is: `0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO`

Screenshots





- The screenshot shows the terminal during the SSH login process for `bandit19`.
- The screenshot shows the terminal after logging into `bandit19`.
- The `ls` command lists the `bandit20-do` binary.
- The `./bandit20-do cat /etc/bandit_pass/bandit20` command is used to read the password for Level 20.

Conclusion

This level teaches how to use a setuid binary to execute commands with the privileges of another user. By leveraging the `bandit20-do` binary, you can access files that are otherwise restricted. This skill is essential for understanding and managing permissions in Linux systems.

Got it! Here's the write-up for **Level 20 → Level 21** in the exact format of your first prompt:

Level 20 → Level 21: Using a Setuid Binary for Network Communication

Level Goal

- To gain access to the next level, you should use the setuid binary in the home directory. This binary connects to `localhost` on a specified port, reads a line of text, and compares it to the password for `bandit20`. If the password is correct, it transmits the password for `bandit21`.

Steps to Solve Level 20 → Level 21

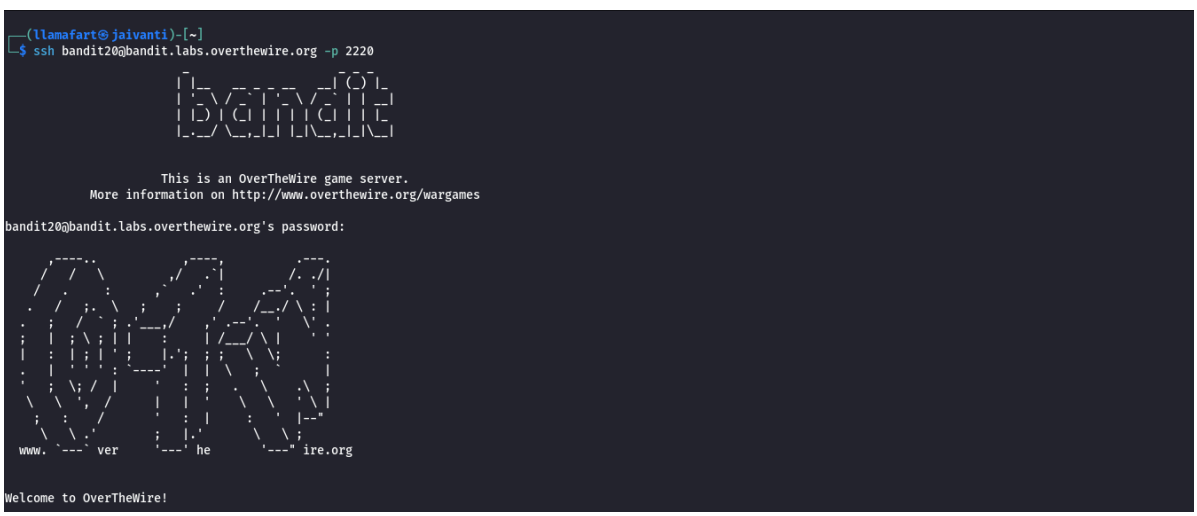
1. Log into Bandit20

Command

`ssh` bandit20@bandit.labs.overthewire.org `-p 2220`

Password for SSH Login

- The password for `bandit20` is: `0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO`



Explanation

- The `ssh` command is used to connect to the Bandit server.
- `bandit20` is the username for Level 20.
- `bandit.labs.overthewire.org` is the server address.

- `-p 2220` specifies the port number.

2. List the Contents of the Home Directory

Command

`ls`

Explanation

- The `ls` command lists all files and directories in the current directory.
- This reveals the setuid binary `suconnect`.

3. Execute the Setuid Binary Without Arguments

Command

`./suconnect`

Explanation

- The `./suconnect` command executes the setuid binary.
- The output provides instructions on how to use the binary.

4. Set Up a Listener on a Port

Command

`echo "0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO" | nc -lp 1234 &`

Explanation

- The `echo` command sends the password for `bandit20` to a netcat (`nc`) listener.
- `lp 1234` specifies that netcat should listen on port `1234`.
- The `&` runs the command in the background.

5. Use the Setuid Binary to Retrieve the Password

Command

`./suconnect 1234`

Explanation

- The `./suconnect` binary connects to `localhost` on port `1234`.
- It reads the password for `bandit20` and verifies it.
- If the password is correct, it sends the password for `bandit21`.

6. Logout

Command

`logout`

```
bandit20@bandit:~$ ls
suconnect
bandit20@bandit:~$ file suconnect
suconnect: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=4c95669a71860e303b714721dc
bandit20@bandit:~$ echo "0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO" | netcat -lp 1234 &
[1] 2756127
bandit20@bandit:~$ jobs
[1]+  Running                 echo "0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO" | netcat -lp 1234 &
bandit20@bandit:~$ ./suconnect 1234
Read: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
Password matches, sending next password
EeoULMCra2q0dSkYj561DX7s1CpBuOBt
[1]+  Done                    echo "0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO" | netcat -lp 1234
bandit20@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.

┌──(llamafart㉿jaivanti)-[~]
└─$
```

Password for Level 21

- The password for `bandit21` is: `EeoULMCra2q0dSkYj561DX7s1CpBuOBt`

Screenshots

```
┌──(llamafart㉿jaivanti)-[~]
└─$ ssh bandit20@bandit.labs.overthewire.org -p 2220
                      _                     _ _ _
                     | |__   __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


                    This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit20@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \        ,/   .`|         /. ./|
    /   .     :     ,`    .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :    | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ', /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

```
bandit20@bandit:~$ ls
suconnect
bandit20@bandit:~$ file suconnect
suconnect: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=4c95669a71860e303b714721dc
bandit20@bandit:~$ echo "0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO" | netcat -lp 1234 &
[1] 2756127
bandit20@bandit:~$ jobs
[1]+  Running                 echo "0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO" | netcat -lp 1234 &
bandit20@bandit:~$ ./suconnect 1234
Read: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
Password matches, sending next password
EeoULMCra2q0dSkYj561DX7s1CpBuOBt
[1]+  Done                    echo "0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO" | netcat -lp 1234
bandit20@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.

┌──(llamafart㉿jaivanti)-[~]
└─$
```

- The screenshot shows the terminal during the SSH login process for `bandit20`.
- The screenshot shows the terminal after logging into `bandit20`.
- The `ls` command lists the `suconnect` binary.
- The `./suconnect 1234` command is used to retrieve the password for Level 21.

Conclusion

This level teaches how to use a setuid binary to interact with a network daemon and retrieve sensitive information. By leveraging the `suconnect` binary, you can verify the password for the current level and obtain the password for the next level. This skill is essential for understanding network communication and privilege escalation in Linux systems.