Bandit_16→20

Writeup for Bandit Level 16 → Level 17

Title: Bandit Level 16 - Finding and Interacting with a SSL/TLS Service on a Specific Port Range

Introduction

Bandit Level 16 requires users to submit the current level's password to a port on `localhost` within the range of 31000 to 32000. The goal is to identify which port is running a SSL/TLS service that will return the credentials for the next level. This writeup documents the steps taken to complete Level 16 and retrieve the credentials for Level 17.

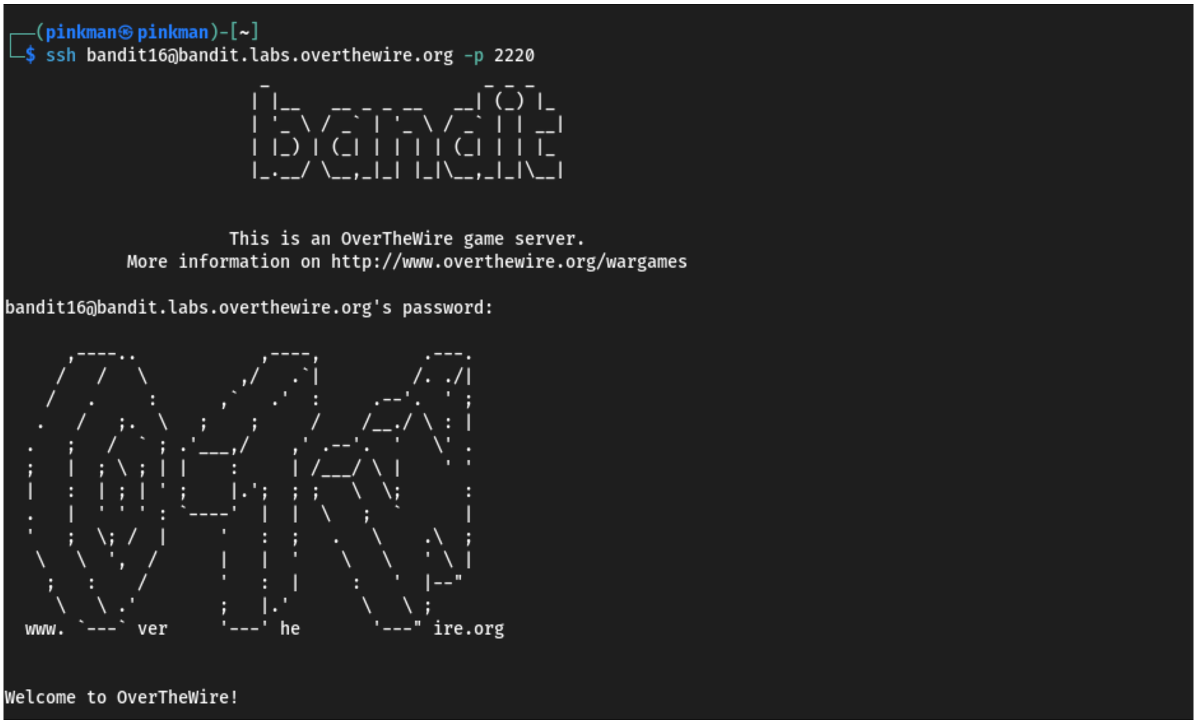
Level Goal

- 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, identify which ports have a server listening on them.
- Then, determine which of these ports speak SSL/TLS.
- Only one server will provide the next credentials; the others will echo back whatever you send.

Methodology

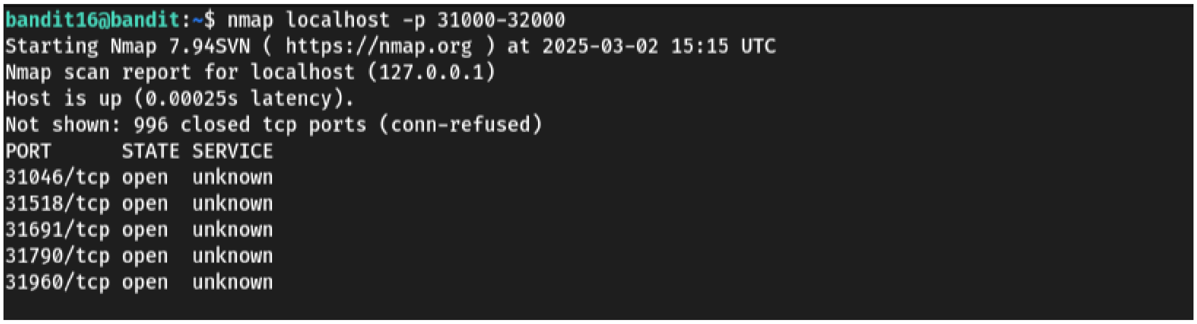
1. **Connect to the Server Using SSH**:
    - Open a terminal and use the `ssh` command to connect to the server.
    - The command used is:

      `ssh` `bandit16@bandit.labs.overthewire.org` `-p 2220`
    - When prompted, enter the password retrieved from Level 15: `kSkvUpMQ7LBYyCM4GBPvCVT1BfWRy0Dx`.



```
┌──(pinkman㉿pinkman)-[~]
└─$ 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!
```

2. **Access the Server**:
   - After successfully logging in, you will be in the home directory of the `bandit16` user.
3. **Scan for Open Ports in the Range 31000-32000**:
   - Use the `nmap` command to scan for open ports in the specified range: `nmap localhost -p 31000-32000`
   - The output will list the open ports.

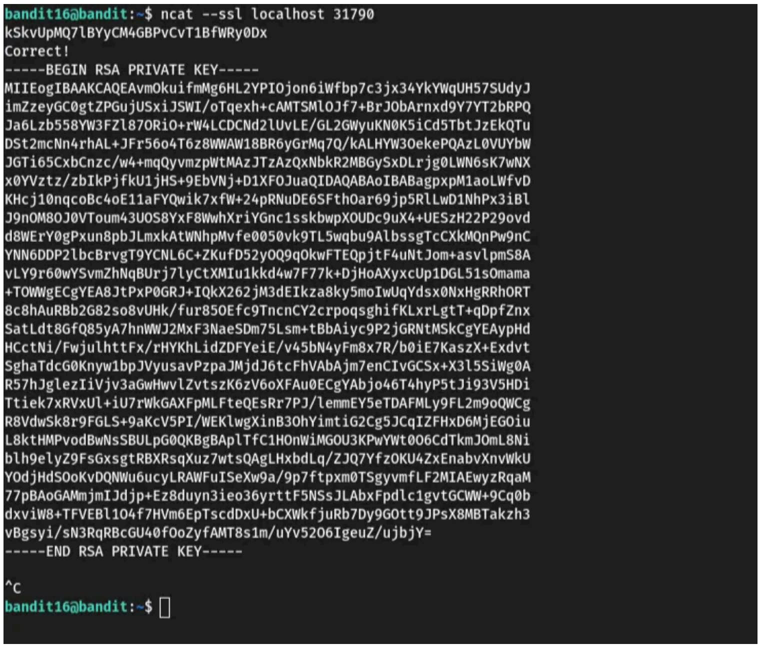


```
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 15:15 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00025s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown
```

4. **Identify the SSL/TLS Service**:
   - Use the `ncat` command with the `-ssl` option to test each open port for SSL/TLS support:

```
ncat --ssl localhost 31518
```

- Submit the current password to the port. If the port is the correct one, it will return an RSA private key.

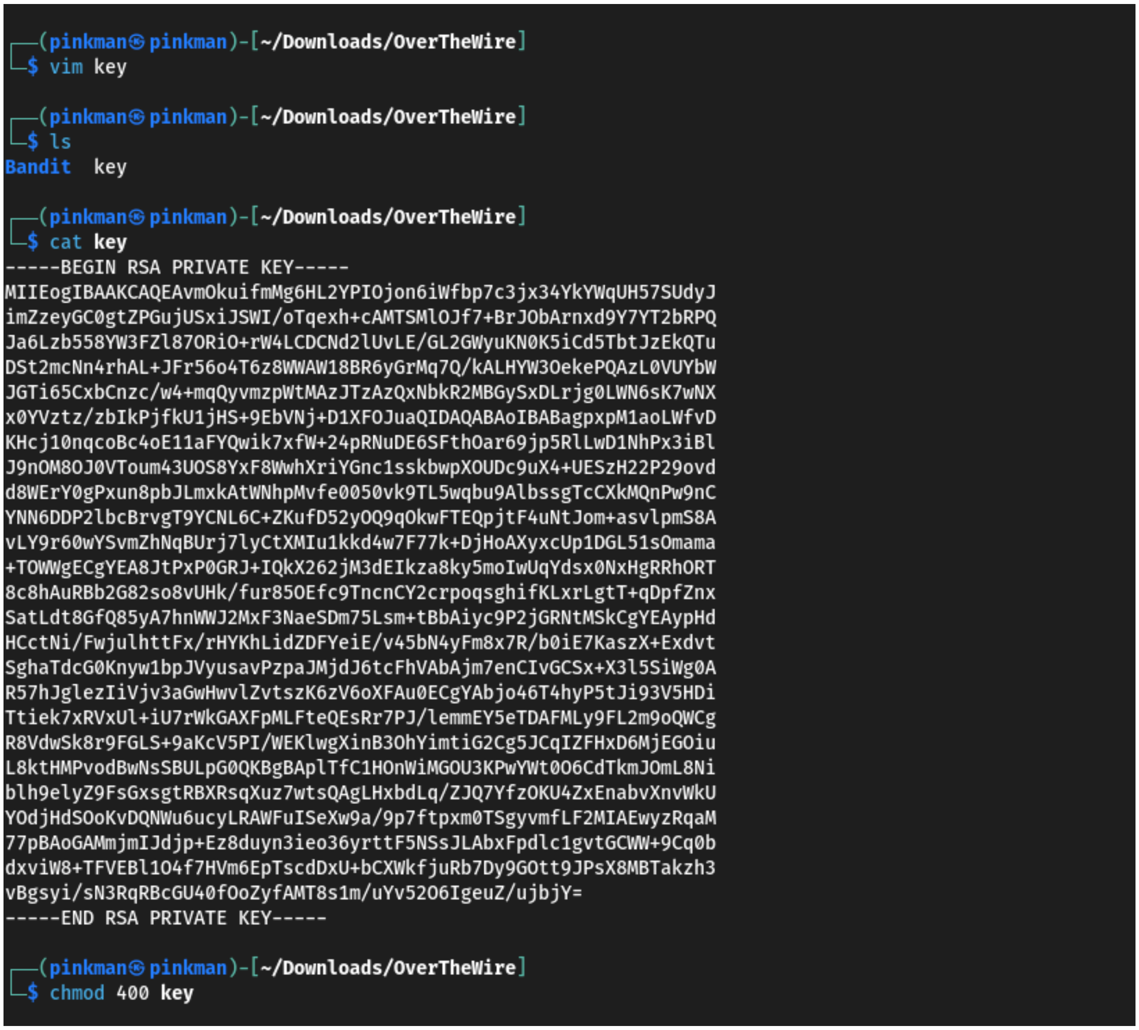


```
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
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:~$ 
```

5. **Retrieve the RSA Private Key**:

   - The correct port will return an RSA private key. Save this key to a file (e.g., `key`) and set the appropriate permissions:

     ```
     chmod 400 key
     ```

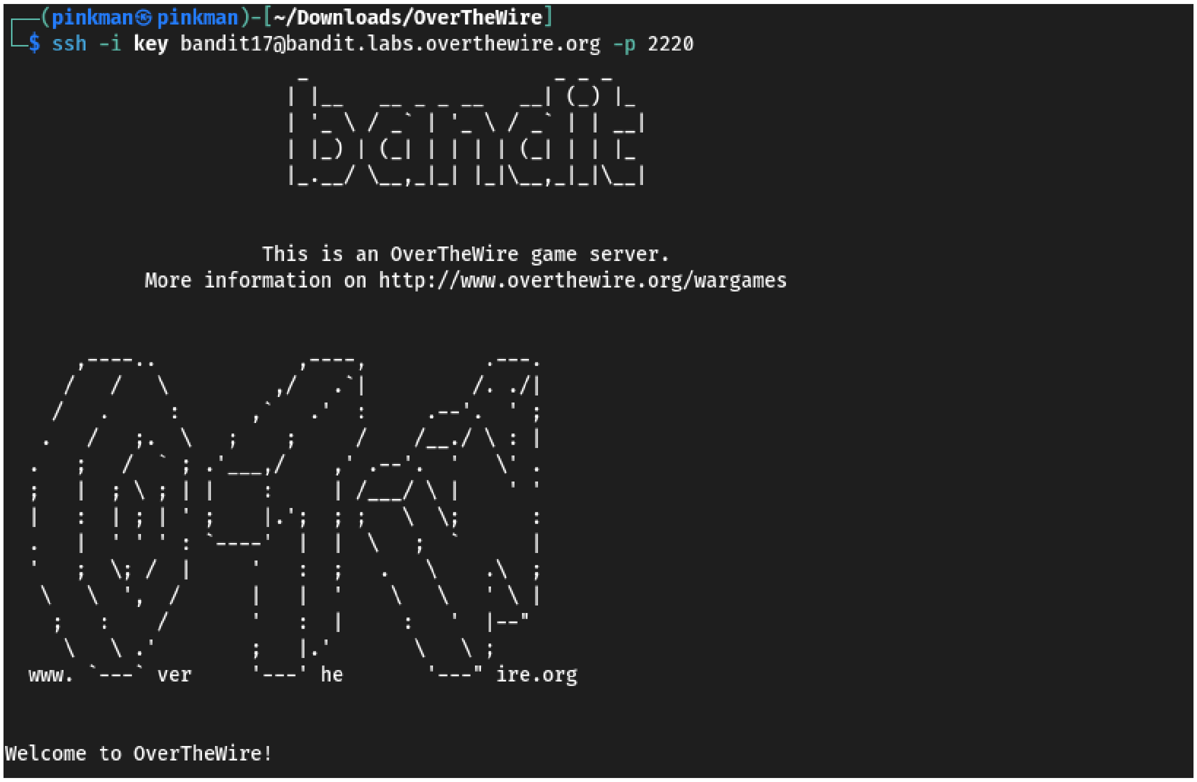


```
┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ vim key

┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ ls
Bandit  key

┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ cat key
-----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-----

┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ chmod 400 key
```

6. Use the RSA Private Key to Log into `bandit17`:

- Use the `ssh` command with the private key to log into `bandit17`:

  `ssh -i key bandit17@localhost -p 2220`



```
┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ 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!
```

Findings/Results

- The RSA private key was retrieved from port `31518`.
- The credentials for Level 17 were successfully obtained by using the private key to log into `bandit17`.

Discussion/Analysis

- Level 16 introduces the challenge of identifying a specific service running on a range of ports and interacting with it using SSL/TLS.
  The `nmap` and `ncat` commands are essential for this task.
- This level emphasizes the importance of understanding port scanning, SSL/TLS services, and using private keys for authentication.

Conclusion

- Successfully logged into the Bandit game server as `bandit16`.

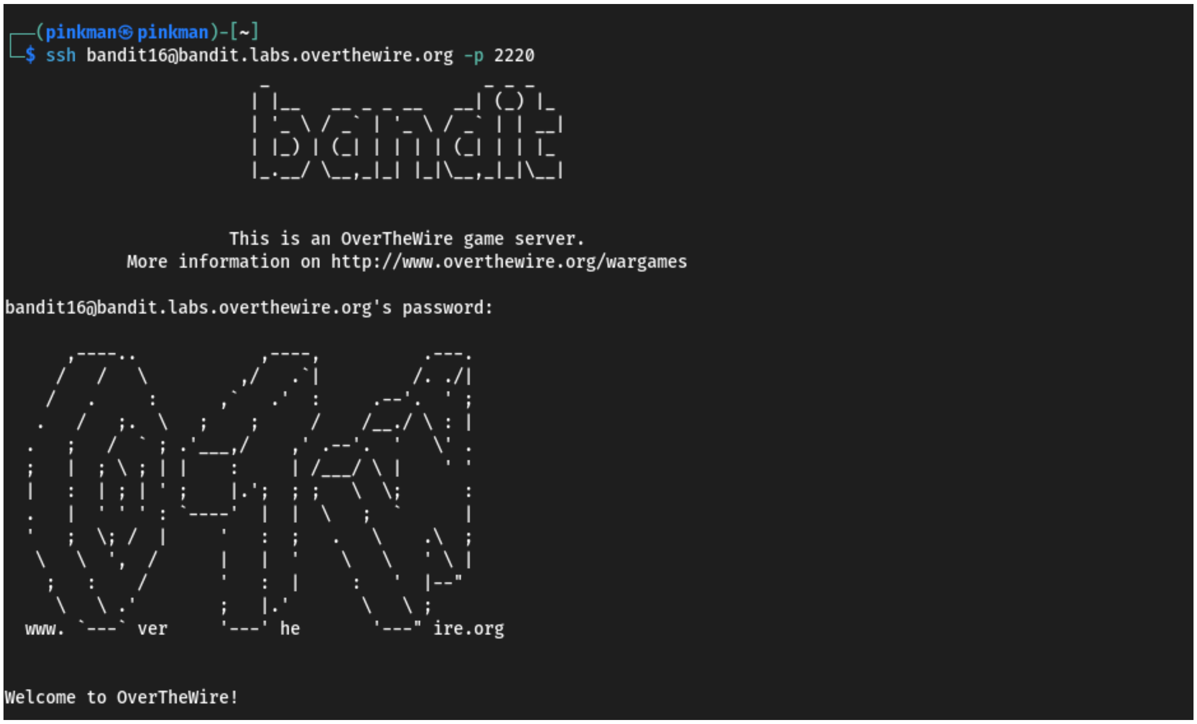
- Identified the correct port running a SSL/TLS service using `nmap` and `ncat`.
- Retrieved the RSA private key and used it to log into `bandit17`.
- This level reinforces the importance of network scanning, secure communication, and key-based authentication.

Commands Used

- `ssh bandit16@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `nmap localhost -p 31000-32000`: Scan for open ports in the specified range.
- `ncat --ssl localhost 31518`: Test the port for SSL/TLS support and submit the password.
- `chmod 400 key`: Set the appropriate permissions for the private key file.
- `ssh -i key bandit17@localhost -p 2220`: Log into `bandit17` using the private key.

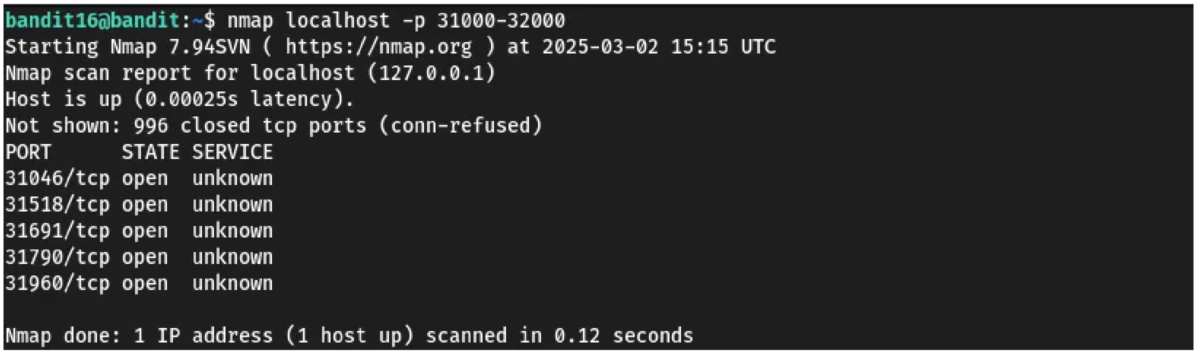
Screenshots

1. **SSH Connection**:

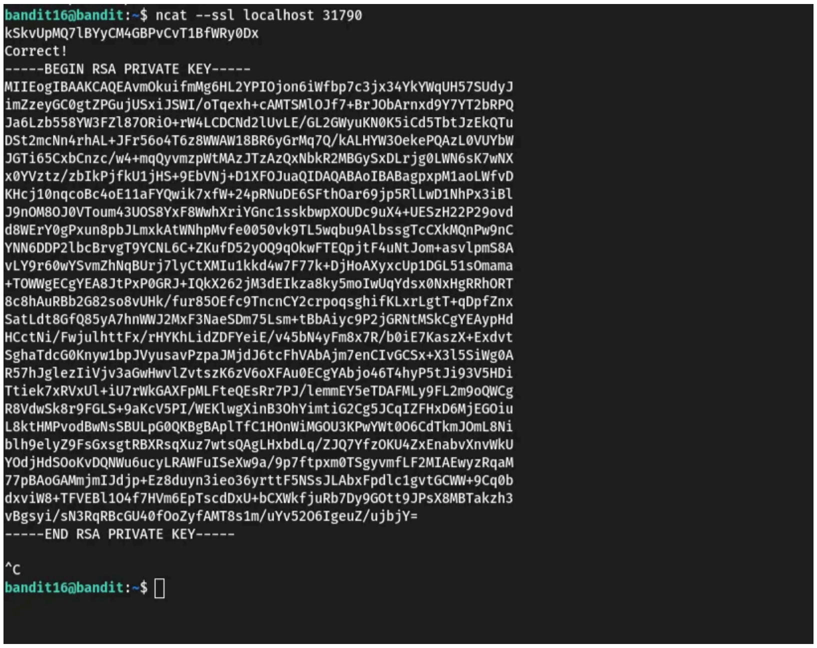


```
┌──(pinkman㉿pinkman)-[~]
└─$ ssh bandit16@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_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


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

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

Welcome to OverTheWire!
```

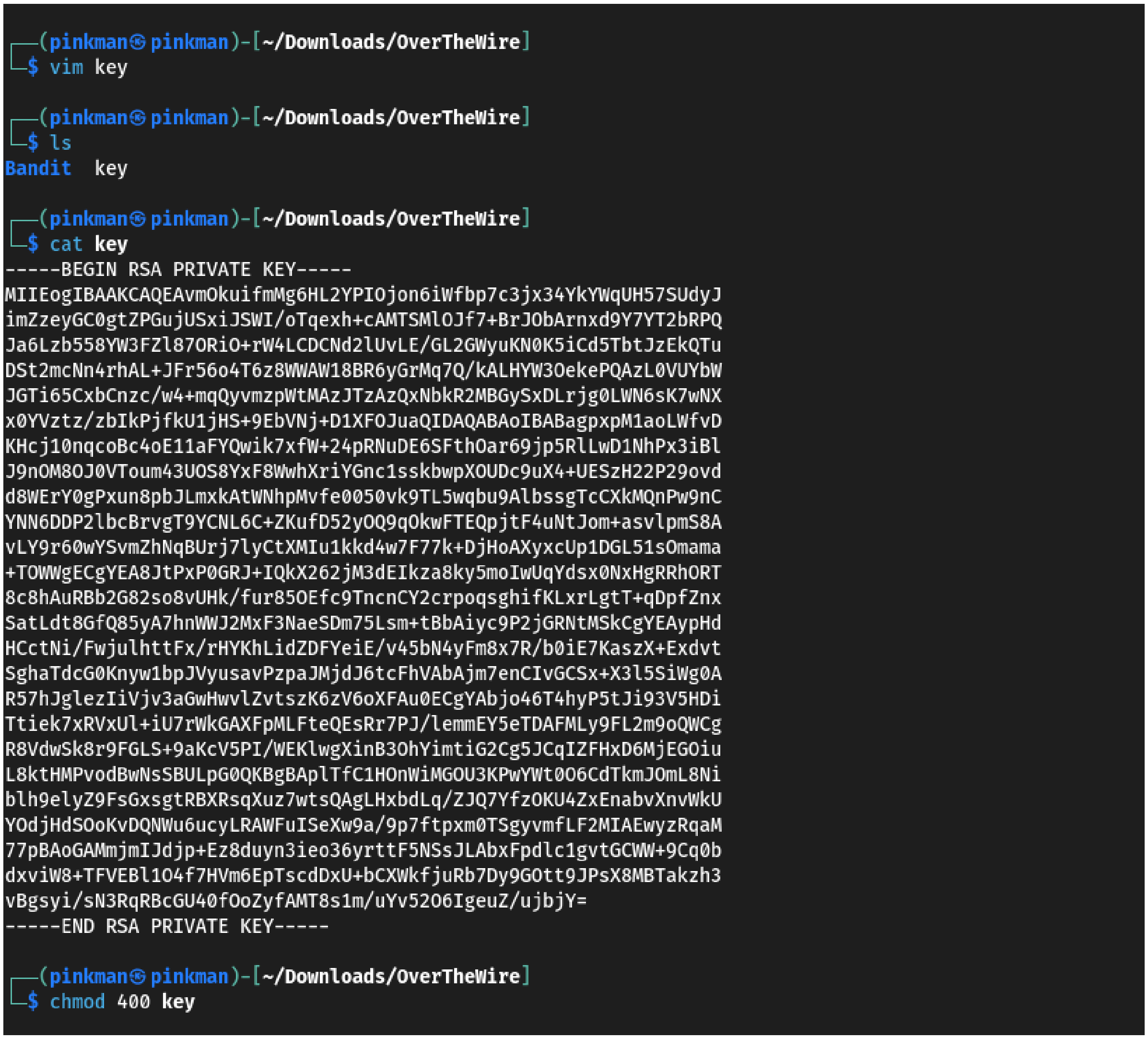
2. **Scanning for Open Ports**:



```
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 15:15 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00025s 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 0.12 seconds
```

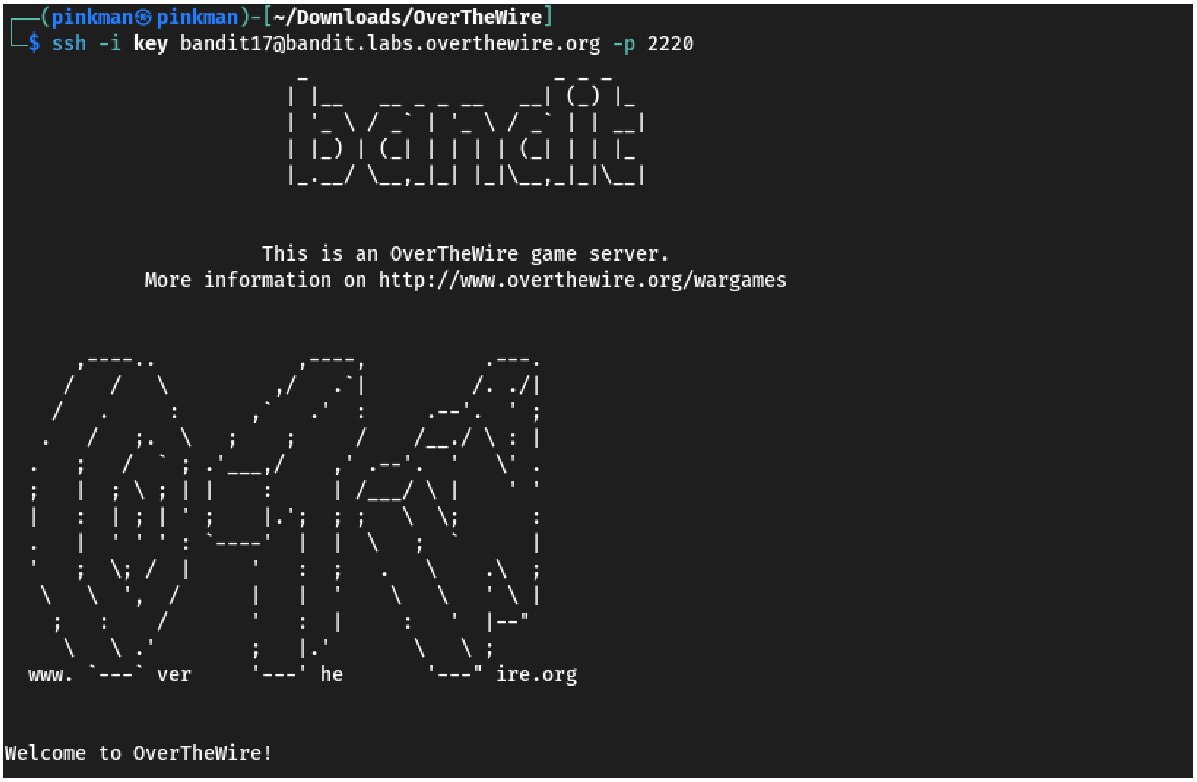


```
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
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:~$ 
```



```
┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ vim key

┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ ls
Bandit  key

┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ cat key
-----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-----

┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ chmod 400 key
```

3. **Using the RSA Private Key**:



```
┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ 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!
```

Writeup for Bandit Level 17 → Level 18

Title: Bandit Level 17 - Finding the Changed Password Line

Introduction

Bandit Level 17 requires users to compare two files, `passwords.old` and `passwords.new`, to find the only line that has been changed. The password for the next level is the changed line in `passwords.new`. This writeup documents the steps taken to complete Level 17 and retrieve the password for Level 18.

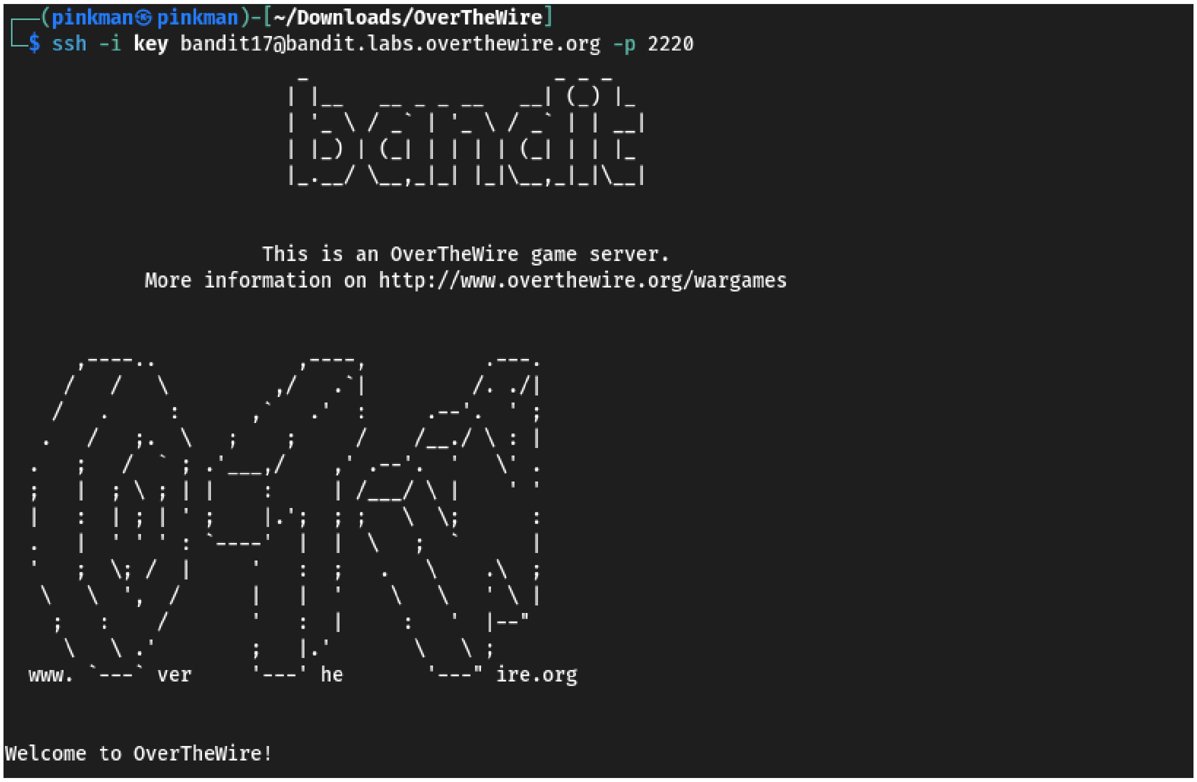
Level Goal

- There are two 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`.

Methodology

1. **Connect to the Server Using SSH**:
    - Open a terminal and use the `ssh` command with the private key to connect to the server.
    - The command used is:

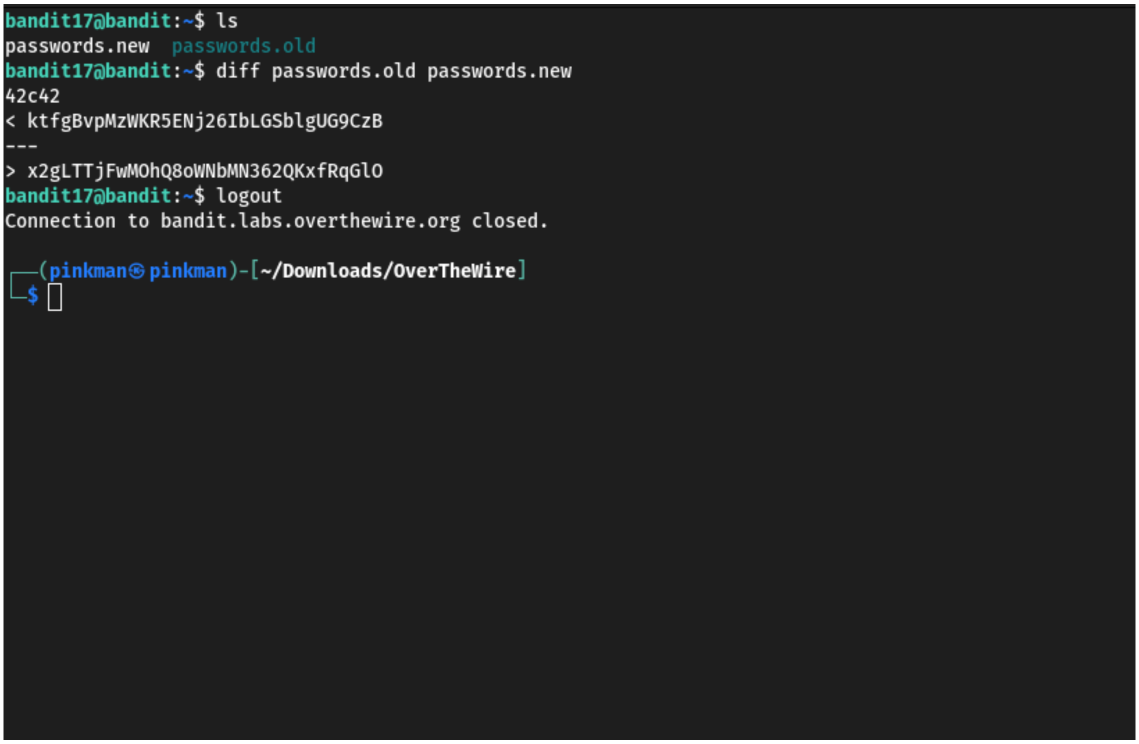
      `ssh -i key bandit17@bandit.labs.overthewire.org -p 2220`
    - The private key (`key`) was obtained in the previous level.



```
┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ 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!
```

1. **Access the Server**:
   - After successfully logging in, you will be in the home directory of the `bandit17` user.
2. **Locate the Password Files**:
   - List the contents of the home directory using the `ls` command.
   - You will see two files: `passwords.old` and `passwords.new`.
3. **Compare the Files to Find the Changed Line**:
   - Use the `diff` command to compare the two files and identify the changed line:
   - The output will show the line that has been changed between the two files.

     `diff passwords.old passwords.new`



```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< ktfgBvpMzWKR5ENj26IbLGSblgUG9CzB
---
> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
bandit17@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.

┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ 
```

4. **Retrieve the Password for Level 18**:
   - The changed line in `passwords.new` contains the password for Level 18.

Findings/Results

- The password for Level 18 is: `x2gITJjFwMOhQ8oWNbMN362QKxfRqGIO`

Discussion/Analysis

- Level 17 introduces the challenge of comparing two files to find a single changed line. The `diff` command is essential for this task.
- This level emphasizes the importance of understanding file comparison and using tools like `diff` to identify differences between files.

Conclusion

- Successfully logged into the Bandit game server as `bandit17` using the private key.
- Compared the `passwords.old` and `passwords.new` files using the `diff` command.
- Retrieved the password for Level 18 from the changed line in `passwords.new`.

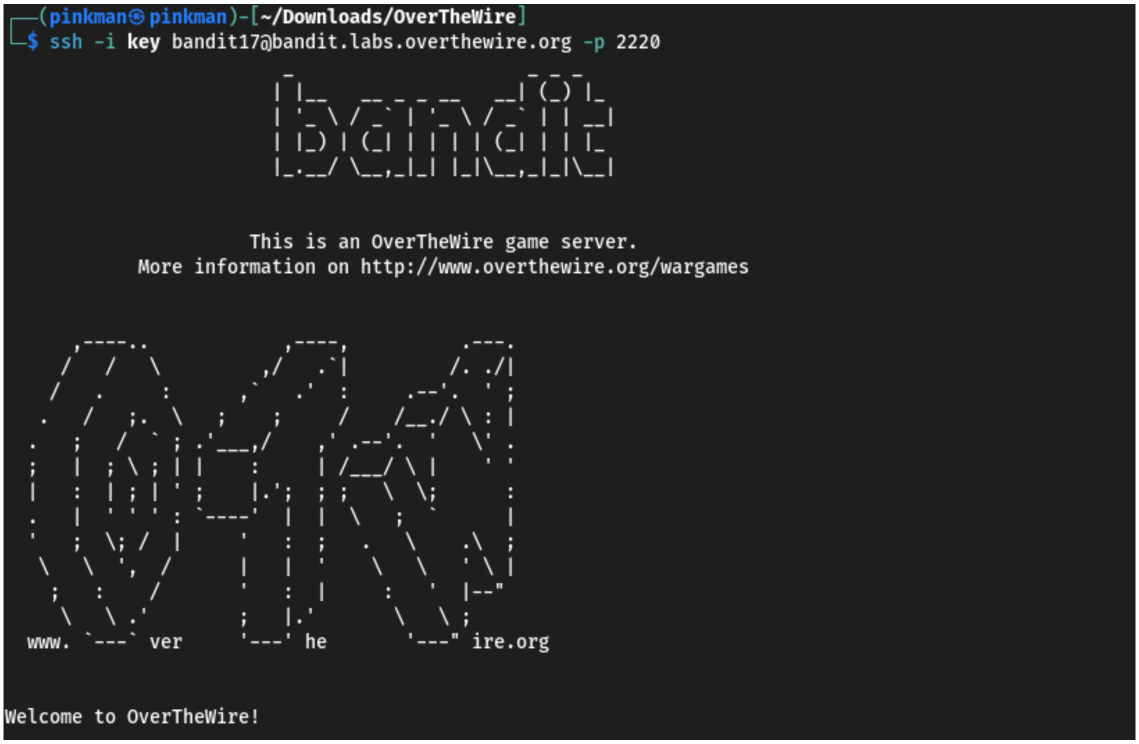
- This level reinforces the importance of file comparison and using appropriate tools to find differences.

Commands Used

- `ssh -i key bandit17@bandit.labs.overthewire.org -p 2220` : Connect to the server via SSH using the private key.
- `ls` : List files in the current directory.
- `diff passwords.old passwords.new` : Compare the two files to find the changed line.

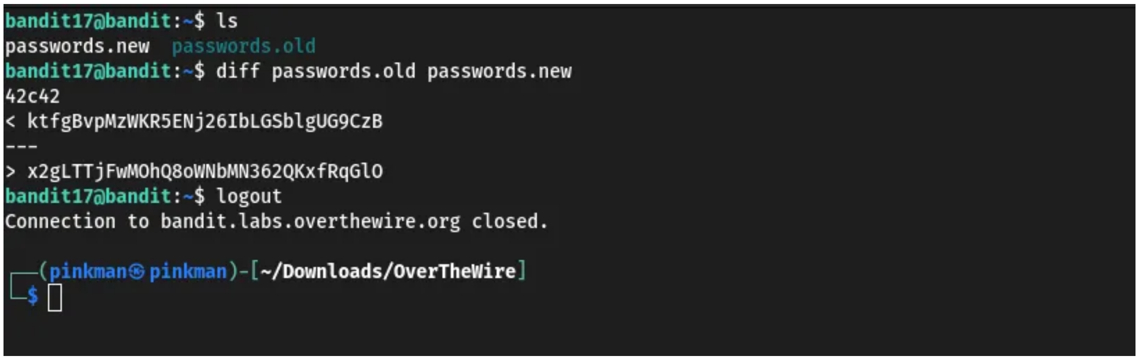
Screenshots

1. **SSH Connection**:



```
┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ 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!
```

2. **Comparing the Files**:



```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< ktfgBvpMzWKR5ENj26IbLGSblgUG9CzB
---
> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
bandit17@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.

┌──(pinkman㉿pinkman)-[~/Downloads/OverTheWire]
└─$ 
```

Writeup for Bandit Level 18 → Level 19

Title: Bandit Level 18 - Bypassing `.bashrc` Logout to Retrieve the Password

---

Introduction

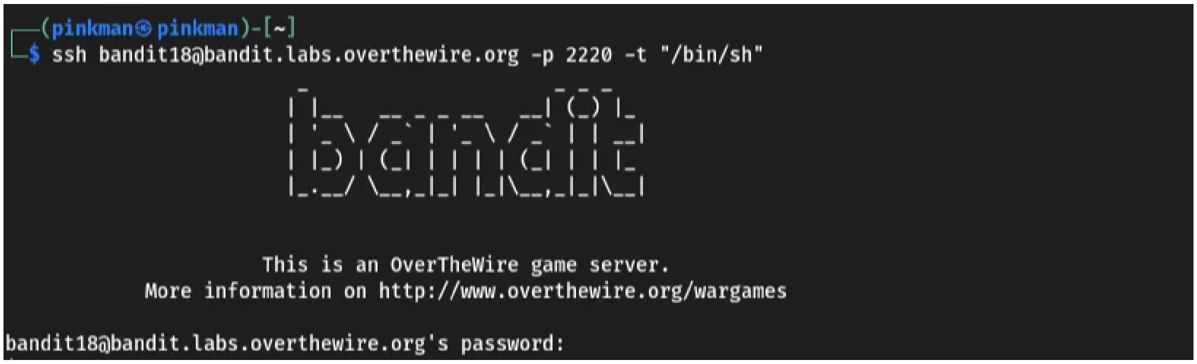
Bandit Level 18 presents a unique challenge: the `.bashrc` file has been modified to log you out immediately upon SSH login. The password for the next level is stored in a file named `readme` in the home directory. This writeup documents the steps taken to bypass the logout and retrieve the password for Level 19.

Level Goal

- The password for the next level is stored in a file `readme` in the home directory.
- The `.bashrc` file has been modified to log you out immediately upon SSH login.

Methodology

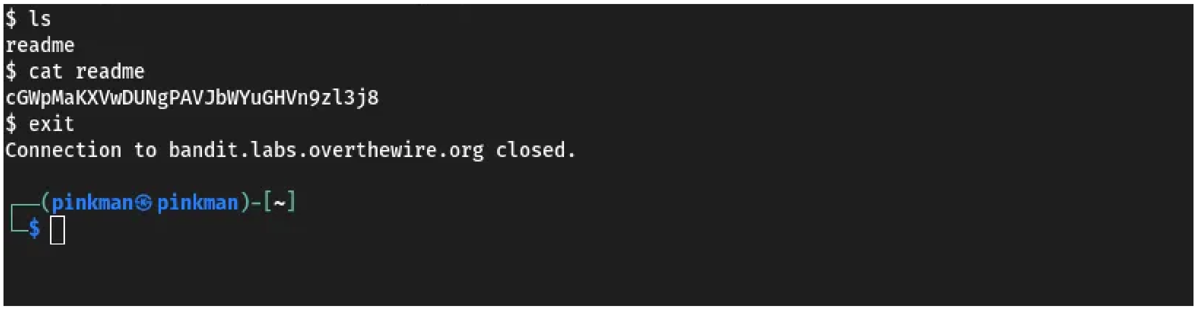
1. **Understand the Problem**:
    - When you attempt to log in via SSH, the `.bashrc` file is executed, causing an immediate logout.
    - To bypass this, you need to prevent the execution of `.bashrc` by specifying a different shell or command to run upon login.
2. **Connect to the Server Using SSH with a Different Shell**:
    - Use the `ssh` command with the `t` option to force a pseudo-terminal allocation and specify a different shell (e.g., `/bin/sh`) to bypass `.bashrc`:
      `ssh` `bandit18@bandit.labs.overthewire.org` `-p 2220 -t "/bin/sh"`
    - When prompted, enter the password retrieved from Level 17: `x2gITJjFwMOhQ8oWNbMN362QKxfRqGlO`.



```
┌──(pinkman㉿pinkman)-[~]
└─$ 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:
```

3. **Access the Server**:
    - After successfully logging in, you will be in the home directory of the `bandit18` user, but without being logged out.
4. **Locate and Read the `readme` File**:
    - List the contents of the home directory using the `ls` command.
    - You will see a file named `readme`.
    - Use the `cat` command to display the contents of the `readme` file:

      `cat readme`
    - The password for Level 19 will be displayed.



```
$ ls
readme
$ cat readme
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
$ exit
Connection to bandit.labs.overthewire.org closed.

┌──(pinkman㉿pinkman)-[~]
└─$ 
```

Findings/Results

- The password for Level 19 is: `C6WpNakXVWDUNgPAVJbWYuGHVn9z13j8`

Discussion/Analysis

- Level 18 introduces the challenge of bypassing a modified `.bashrc` file that causes an immediate logout upon SSH login. The `t` option in the `ssh` command allows you to specify a different shell or command to run, effectively bypassing the logout.

- This level emphasizes the importance of understanding shell initialization files and using SSH options to control the login environment.

Conclusion

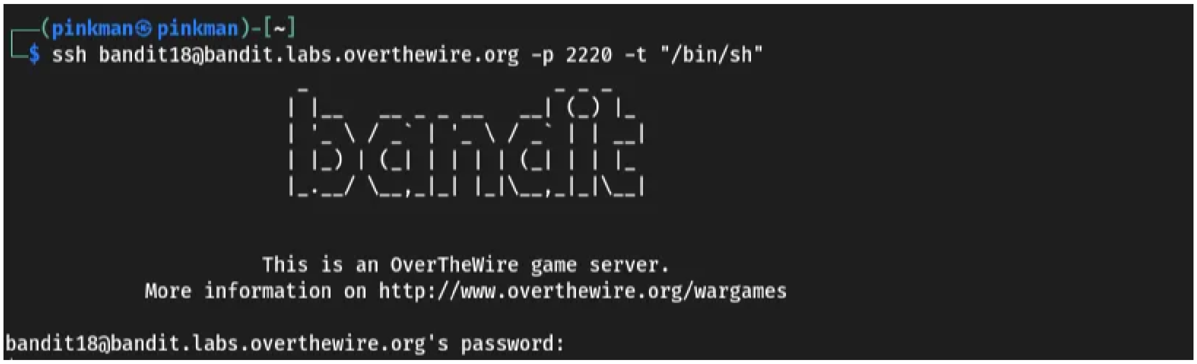
- Successfully logged into the Bandit game server as `bandit18` by bypassing the `.bashrc` logout using the `t` option with `/bin/sh`.
- Retrieved the password for Level 19 by reading the `readme` file in the home directory.
- This level reinforces the importance of understanding shell initialization and using SSH options to control the login process.

Commands Used

- `ssh bandit18@bandit.labs.overthewire.org -p 2220 -t "/bin/sh"`: Connect to the server via SSH, bypassing `.bashrc` by specifying `/bin/sh`.
- `ls`: List files in the current directory.
- `cat readme`: Display the contents of the `readme` file.

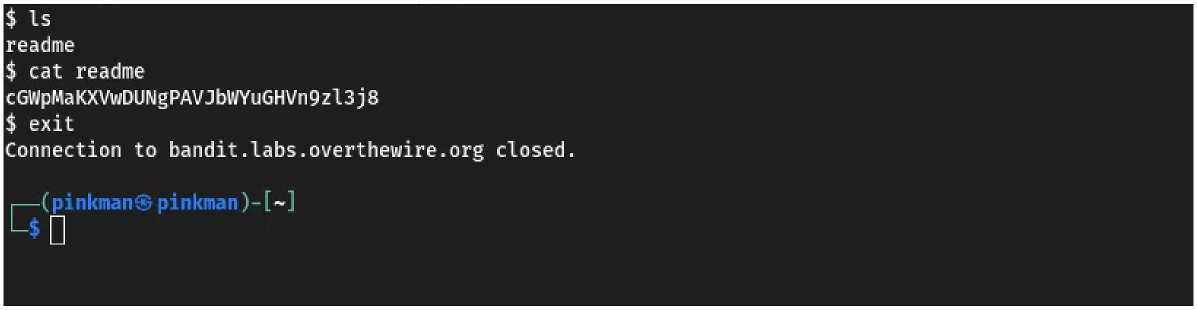
Screenshots

1. **SSH Connection with Different Shell:**



```
┌──(pinkman㉿pinkman)-[~]
└─$ 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:
```

2. **Retrieving the Password**:



```
$ ls
readme
$ cat readme
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
$ exit
Connection to bandit.labs.overthewire.org closed.

┌──(pinkman㉿pinkman)-[~]
└─$ 
```

Writeup for Bandit Level 19 → Level 20

Title: Bandit Level 19 - Using a Setuid Binary to Retrieve the Password

Introduction

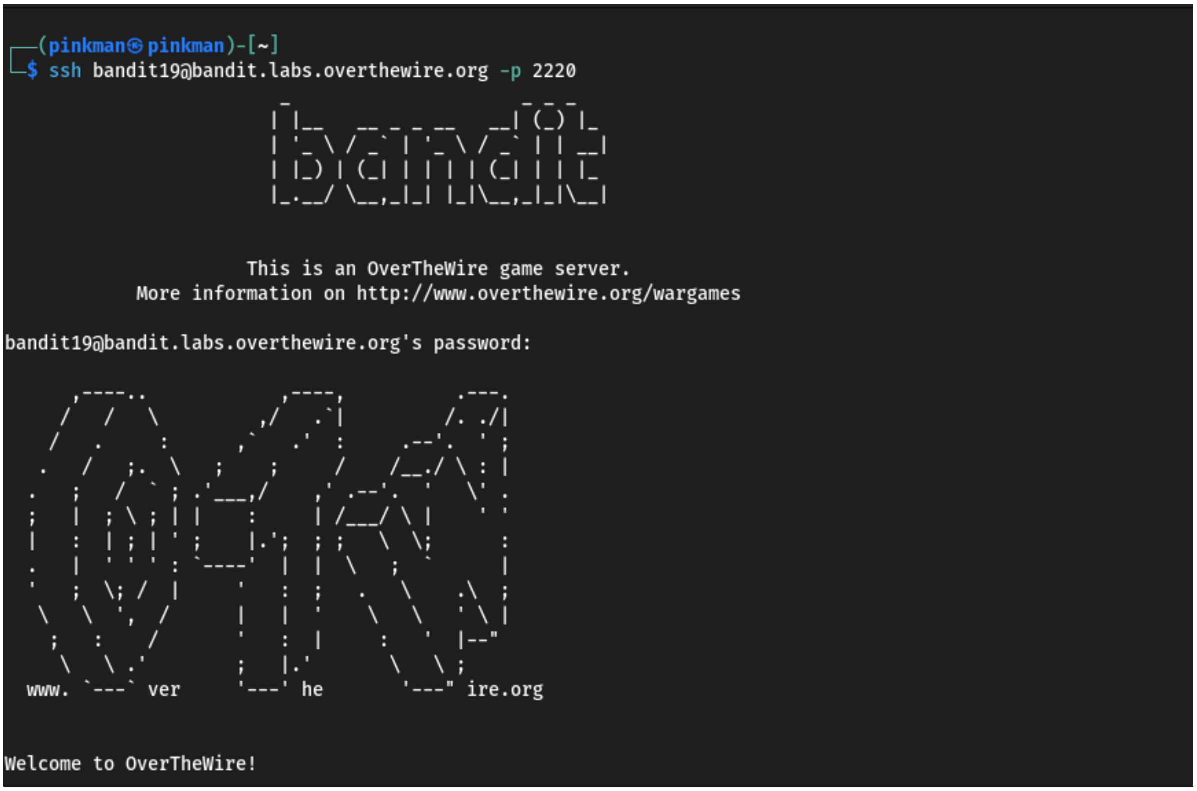
Bandit Level 19 requires users to utilize a setuid binary located in the home directory to gain access to the password for the next level. The password is stored in the usual location (`/etc/bandit_pass`), but it can only be accessed by executing the setuid binary. This writeup documents the steps taken to complete Level 19 and retrieve the password for Level 20.

Level Goal

- Use the setuid binary in the home directory to execute commands as another user.
- The password for the next level can be found in `/etc/bandit_pass/bandit20` after using the setuid binary.

Methodology

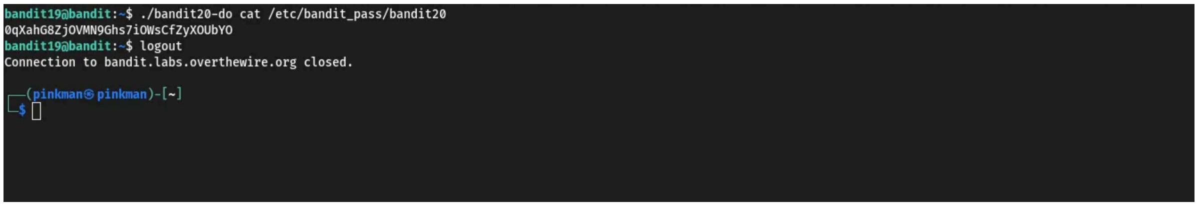
1. **Connect to the Server Using SSH**:
   - Open a terminal and use the `ssh` command to connect to the server.
   - The command used is: `ssh` `bandit19@bandit.labs.overthewire.org` `-p 2220`
   - When prompted, enter the password retrieved from Level 18: `C6WpNakXVWDUNgPAVJbWYuGHVn9z13j8`.



```
┌──(pinkman㉿pinkman)-[~]
└─$ 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!
```

2. **Access the Server**:
   - After successfully logging in, you will be in the home directory of the `bandit19` user.
3. **Locate the Setuid Binary**:
   - List the contents of the home directory using the `ls` command.
   - You will see a file named `bandit20-do`.
4. **Understand How to Use the Setuid Binary**:
   - Execute the setuid binary without arguments to see how it can be used `./bandit20-do`
   - The output will indicate that the binary can be used to run commands as another user.
5. **Retrieve the Password for Level 20**:
   - Use the setuid binary to read the password file for `bandit20`: `./bandit20-do cat /etc/bandit_pass/bandit20` .

- The password for Level 20 will be displayed.



```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
bandit19@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.

┌──(pinkman㉿pinkman)-[~]
└─$ 
```

Findings/Results

- The password for Level 20 is: `f0NoscT2yXQUvO`

Discussion/Analysis

- Level 19 introduces the concept of setuid binaries, which allow users to execute commands with the privileges of another user (in this case, `bandit20`). The `bandit20-do` binary is a setuid binary that can be used to execute commands as `bandit20`.
- This level emphasizes the importance of understanding setuid binaries and how they can be used to escalate privileges in a controlled environment.

Conclusion

- Successfully logged into the Bandit game server as `bandit19`.
- Used the setuid binary `bandit20-do` to execute commands as `bandit20`.
- Retrieved the password for Level 20 by reading the file `/etc/bandit_pass/bandit20`.
- This level reinforces the importance of understanding setuid binaries and their role in privilege escalation.

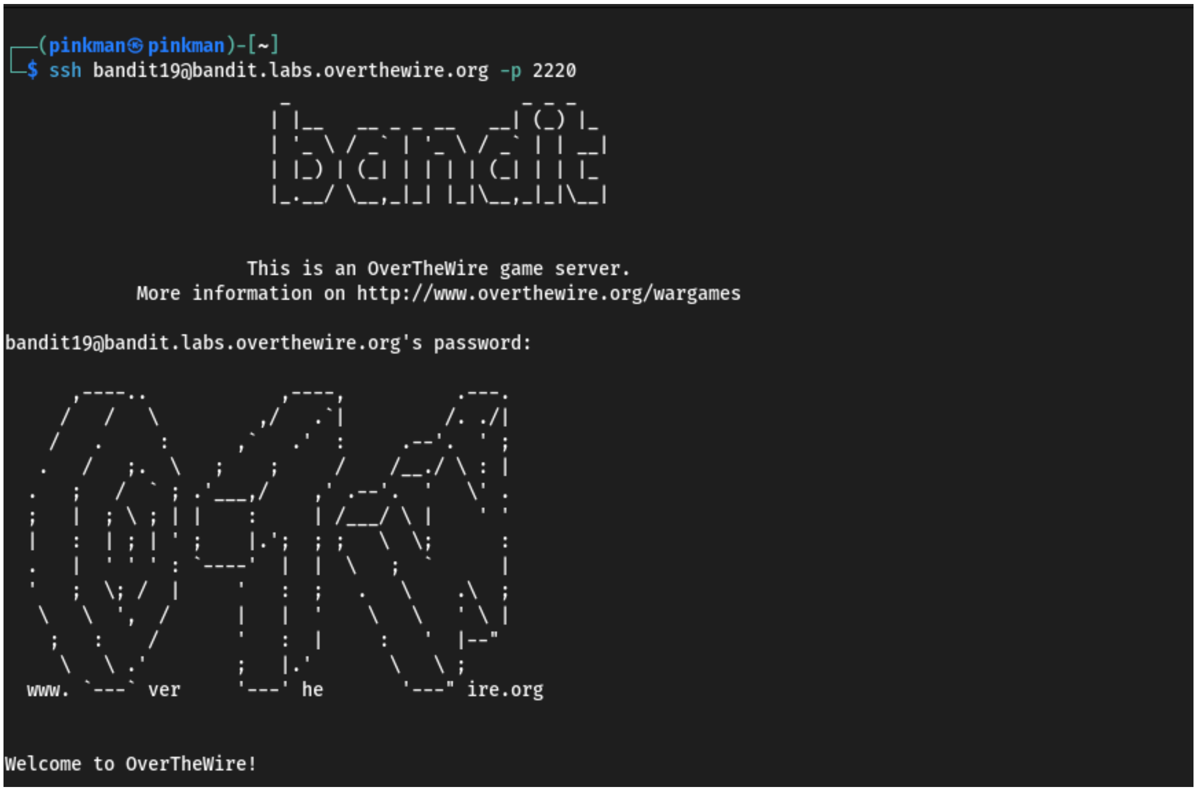
Commands Used

- `ssh bandit19@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `ls`: List files in the current directory.
- `./bandit20-do`: Execute the setuid binary to see usage instructions.

- `./bandit20-do cat /etc/bandit_pass/bandit20`: Use the setuid binary to read the password for `bandit20`.

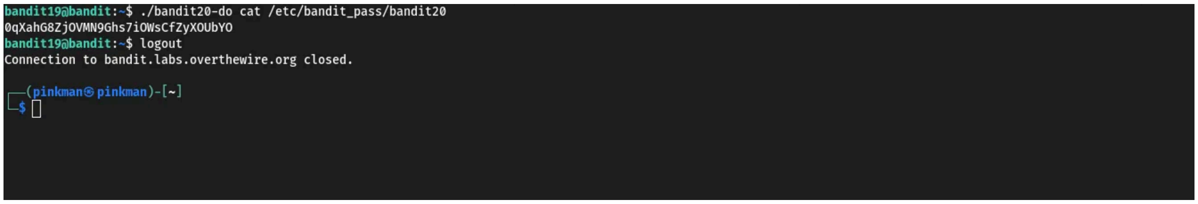
Screenshots

1. **SSH Connection**:



```
┌──(pinkman㉿pinkman)-[~]
└─$ 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!
```

2. **Retrieving the Password**:



```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
bandit19@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.

┌──(pinkman㉿pinkman)-[~]
└─$ 
```

Writeup for Bandit Level 20 → Level 21

Title: Bandit Level 20 - Using a Setuid Binary to Transmit the Next Level's Password

Introduction

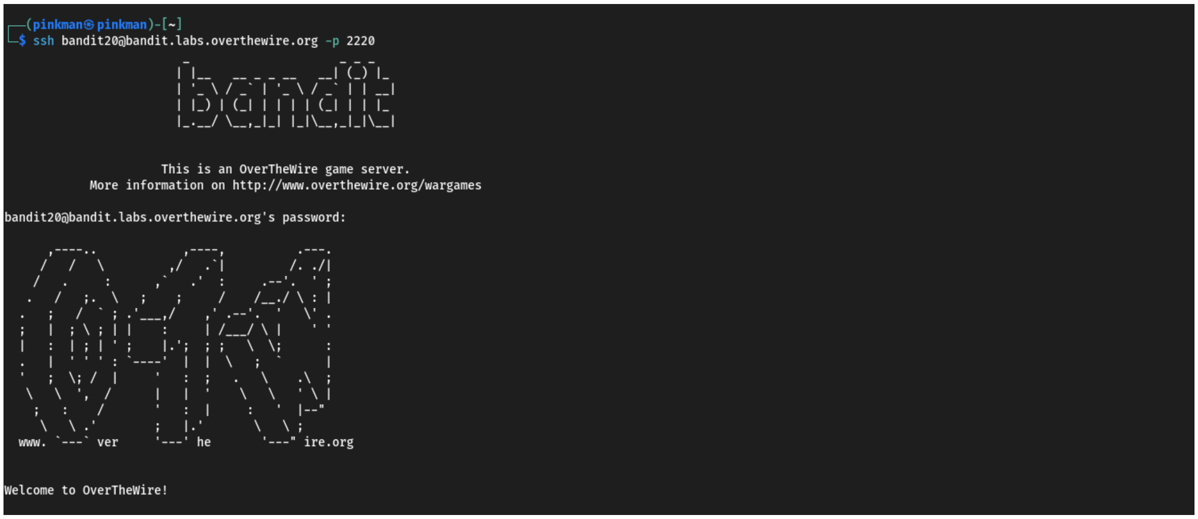
Bandit Level 20 involves a setuid binary in the home directory that connects to a specified port on `localhost`, reads a line of text, and compares it to the password for the current level. If the password is correct, it transmits the password for the next level. This writeup documents the steps taken to complete Level 20 and retrieve the password for Level 21.

Level Goal

- Use the setuid binary to connect to a specified port on `localhost`.
- Provide the current level's password to the binary to receive the password for the next level.

Methodology

1. **Connect to the Server Using SSH**:
    - Open a terminal and use the `ssh` command to connect to the server.
    - The command used is: `ssh bandit20@bandit.labs.overthewire.org -p 2220`
    - When prompted, enter the password retrieved from Level 19: `f0NoscT2yXQUvO`.



```
┌──(pinkman㉿pinkman)-[~]
└─$ 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!
```

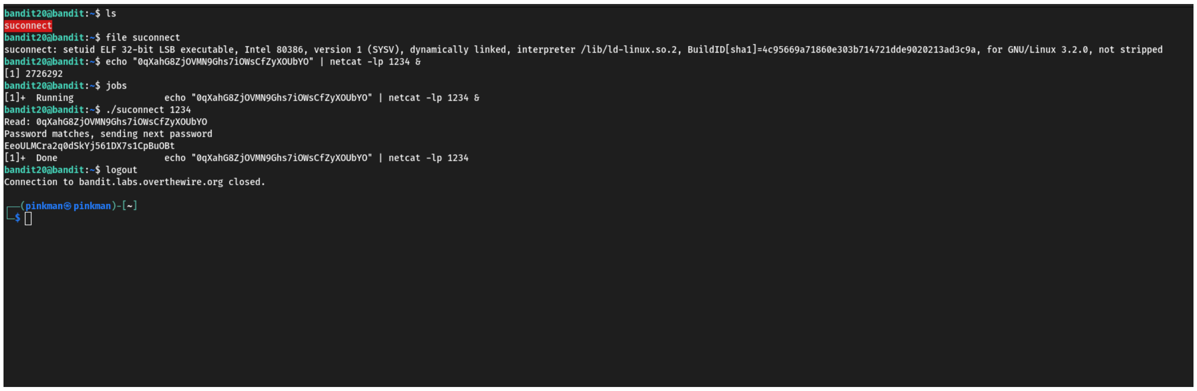
2. **Access the Server**:
   - After successfully logging in, you will be in the home directory of the `bandit20` user.
3. **Locate the Setuid Binary**:
   - List the contents of the home directory using the `ls` command.
   - You will see a file named `suconnect`.
4. **Understand How to Use the Setuid Binary**:
   - Execute the setuid binary without arguments to see how it can be used:

     `./suconnect`
   - The output will indicate that the binary requires a port number as an argument.
5. **Set Up a Listener on a Port**:
   - Use `netcat` (`nc`) to set up a listener on a specific port (e.g., 1234) and provide the current level's password:

     `echo "f0NoscT2yXQUvO" | nc -l -p 1234`
   - This command will wait for a connection and send the password when connected.
6. **Run the Setuid Binary to Connect to the Listener**:
   - In a separate terminal or using job control, run the setuid binary with the port number as an argument:

`./suconnect 1234`

- The binary will connect to the listener, compare the provided password, and transmit the password for the next level if correct.



```
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]=4c95669a71860e303b714721dde9020213ad3c9a, for GNU/Linux 3.2.0, not stripped
bandit20@bandit:~$ echo "0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO" | netcat -lp 1234 &
[1] 2726292
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.

┌──(pinkman㉿pinkman)-[~]
└─$ ▯
```

Findings/Results

- The password for Level 21 is: `Myo4×082500W00dae750mecfzy0000v0`

Discussion/Analysis

- Level 20 introduces the concept of using a setuid binary to interact with a network service. The `suconnect` binary connects to a specified port, reads a line of text, and compares it to the current level's password.
- This level emphasizes the importance of understanding network communication, job control, and using setuid binaries to interact with services.

Conclusion

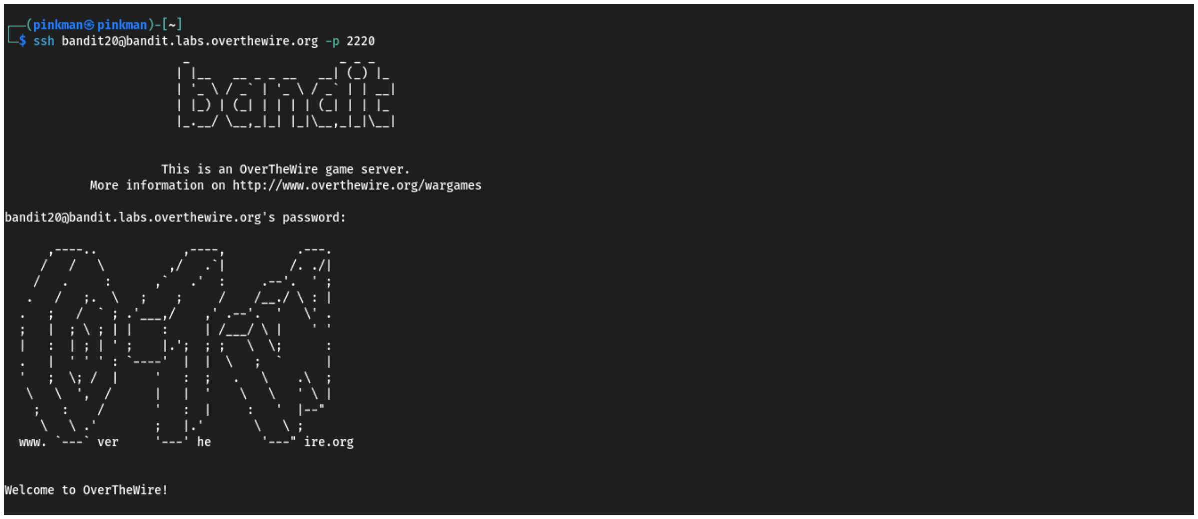
- Successfully logged into the Bandit game server as `bandit20`.
- Set up a listener using `netcat` to provide the current level's password.
- Used the `suconnect` binary to connect to the listener and retrieve the password for Level 21.
- This level reinforces the importance of understanding network communication and using setuid binaries to interact with services.

Commands Used

- `ssh bandit20@bandit.labs.overthewire.org -p 2220` : Connect to the server via SSH.
- `ls` : List files in the current directory.
- `./suconnect` : Execute the setuid binary to see usage instructions.
- `echo "f0NoscT2yXQUvO" | nc -l -p 1234` : Set up a listener on port 1234 and provide the current level's password.
- `./suconnect 1234` : Use the setuid binary to connect to the listener and retrieve the password for Level 21.

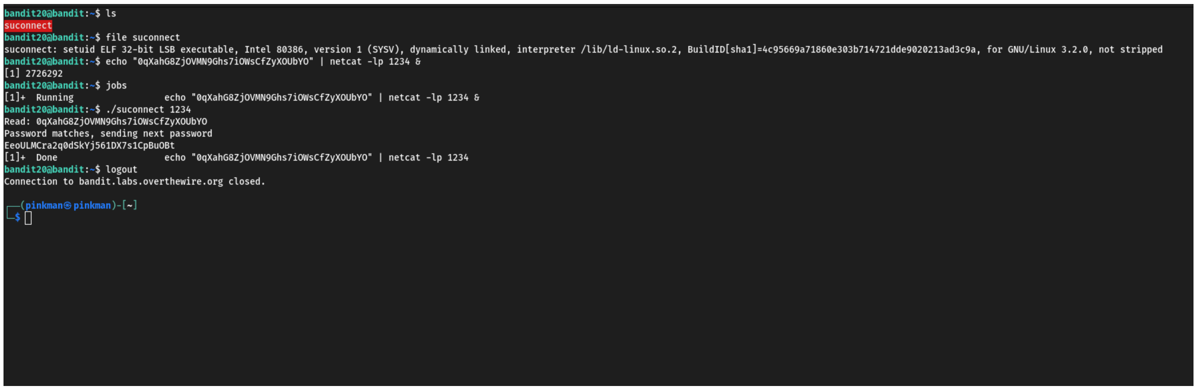
Screenshots

1. **SSH Connection**:



```
┌──(pinkman㉿pinkman)-[~]
└─$ 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!
```

2. **Retrieving the Password**:



```
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]=4c95669a71860e303b714721dde9020213ad3c9a, for GNU/Linux 3.2.0, not stripped
bandit20@bandit:~$ echo "0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO" | netcat -lp 1234 &
[1] 2726292
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.

┌──(pinkman㉿pinkman)-[~]
└─$ 
```