

The College of Saint Rose

ETHICAL HACKING REPORT

ASSIGNMENT # 1 BANDIT 0

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In level 0, the end user will learn valuable SSH (Secure Shell) and how to remote into a website using essential tools and command lines of Linux

Tools

- *The tools needed will be a VM running a Linux distro (Kali),*
- *A terminal prompt, the website <https://overthewire.org/wargames/bandit/bandit0.html>,*
- *The ICMP for network troubleshooting,*

Methodology

1. Pre-Engagement Interactions

The tools needed to perform the test are Vmware Player workstation 16, Kali Linux kali-Linux-2022.3-VirtualBox-amd64, SSH, the website <https://overthewire.org/wargames/bandit/bandit0.html> and the command line interface.

2. Intelligence Gathering

As part of Zoom and in-class discussion. 1 User was found—bandit0 with a password of bandit0 through SSH and online instructions. Video acceleration helps the VM, and so does increasing the memory. Rebooting also allowed the redraw of the windows for the VM and forced the VM to recreate new sessions.

3. Threat Modeling

A tutorial on how to access the secure website is given on the website. With a bad actor, they could gain access if they need to and elevate privileges.

4. Vulnerability Analysis

SSH is not entirely secure; a password and username are given on the website. A tutorial on how to log in is provided, allowing access.

5. Exploitation

A Brute-force would allow someone access. SSH over the web isn't secure; can the website recover if a DDoS attack occurs?

6. Post-Exploitation

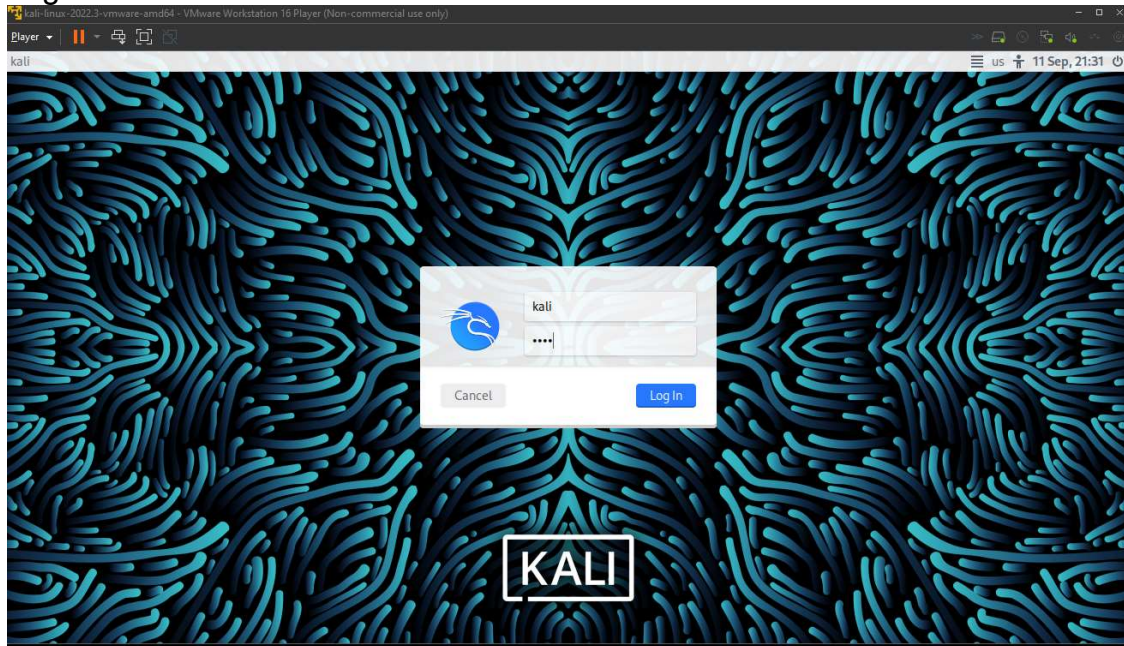
What possible ports are open to new attacks, and what other users are available, bandit1? Or bandit2? Would a Radius attack affect the login attempt? What impact does it have on the organization if this website goes down?

7. Reporting

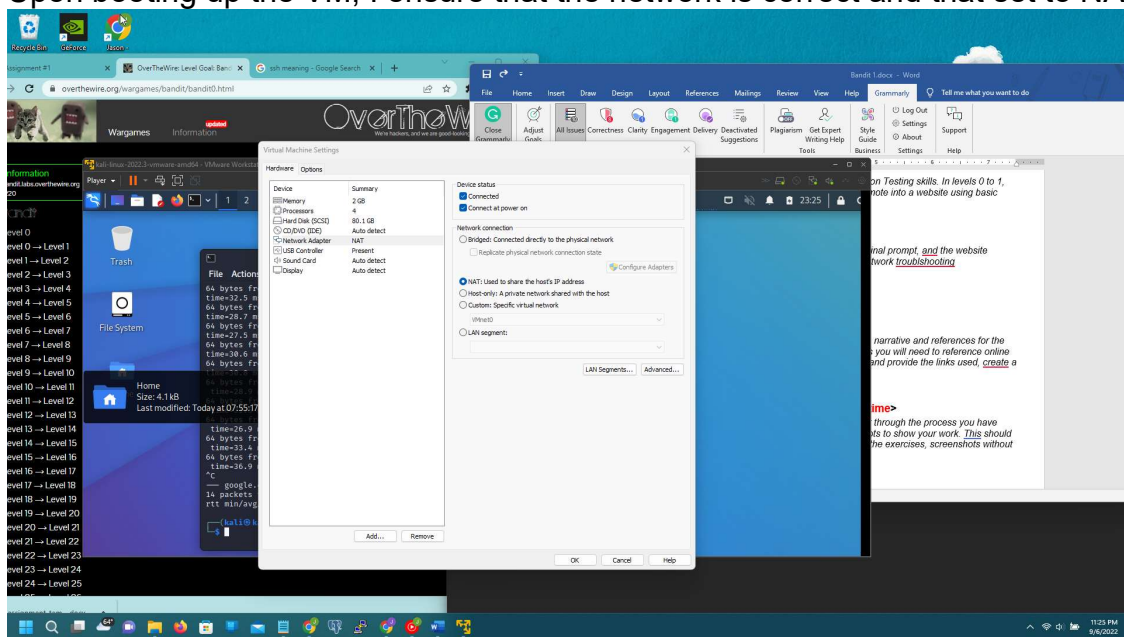
See the Results section.

Results

1. Log in the VM as kali/kali

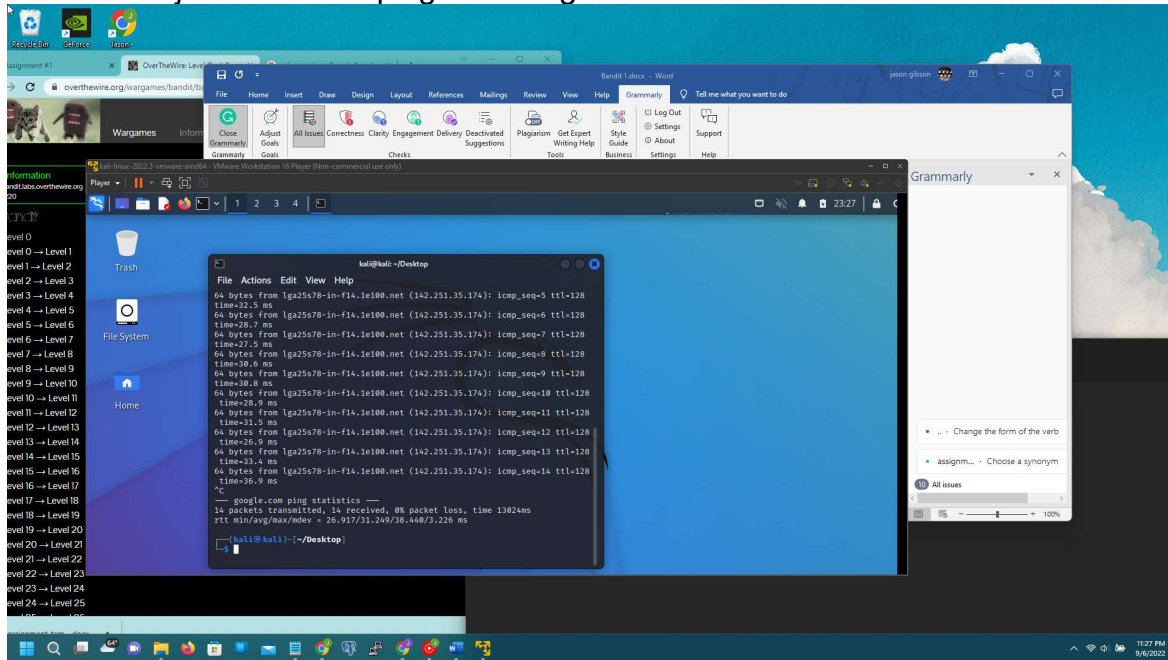


2. Upon booting up the VM, I ensure that the network is correct and that set to NAT

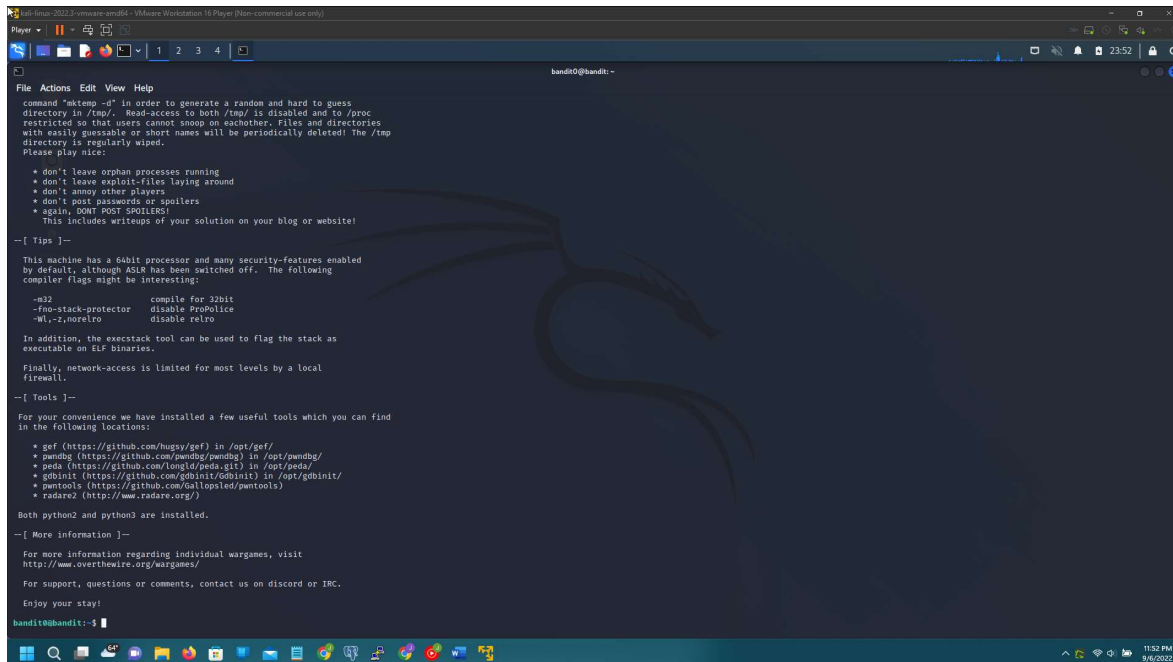


4. After the network is verified, The machine needs to contact the internet.

5. The next objective was to ping the Google servers.

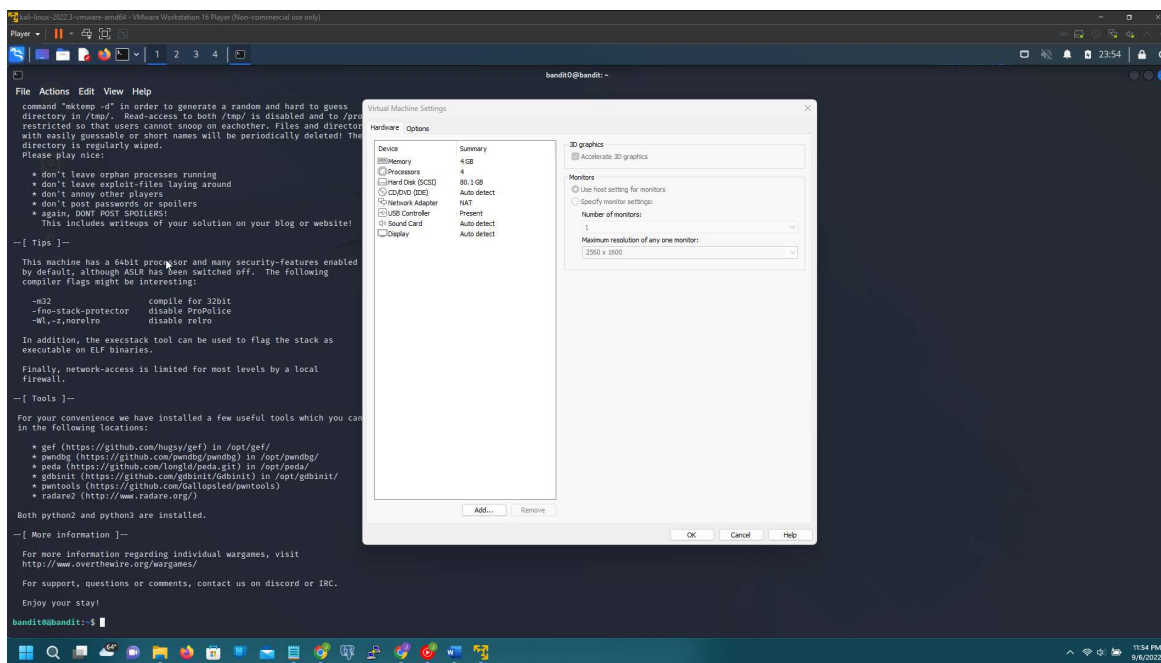


6. Successful pings allow for the next step of SSH into the website. The computer had 14 successes.
7. Remoting by SSH failed until further research that the @ sign was needed between the username and the website. As noted in reference one, the user connects then to the host. As in further discussions, a password could be used for authentication.
8. A prompt asks if you would like to bypass the security because of a lack of a key. Yes or No? Selecting YES allows access. NO denies access. The key is part of the SSH process required when a password is provided, and the key can be exchanged after the first time.
9. Access is given with the password bandit0



10.

11. Fixing the Video setting and adjusting allowing a reboot allows for the VM to refresh



12.

13. The user is logged on as bandit1@bandit

References

1. <https://www.wikihow.com/Use-SSH>
2. http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
3. <https://kirkpatrickprice.com/blog/stages-of-penetration-testing-according-to-ptes/>

The College of Saint Rose

ETHICAL HACKING REPORT

ASSIGNMENT # 1 BANDIT 1

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 0 to 1, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. This will include moving within the file structure and reading and copying/pasting files. The readme file will give the password to proceed to the next exercise.

Tools

- VM running a Linux distro (Kali),
- A terminal prompt, the Website <https://overthewire.org/wargames/bandit/bandit2.html>
- The following Linux commands `ls` - list files `ls -a` list all files including hidden, `cd` change directory `copy` and `paste`, and `cat` to concatenate or read

Methodology

1. Pre-Engagement Interactions

The tools needed to perform the test are VMware Player workstation 16, Kali Linux kali-Linux-2022.3-VirtualBox-amd64, SSH, the Website <https://overthewire.org/wargames/bandit/bandit2.html>, and the command line interface the mouse to be able to copy and paste, enable shared clipboard in VMware.

2. Intelligence Gathering

As part of Zoom and in-class discussion. 1 User was found—bandit1 with a password of NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL. `ls` allows the user to see files; `ls -a` allows the user to view hidden files. The `cat` command will enable the user to read files—`CD` changes Directory. The clipboard must be shared to allow for access to the host and guest OS.

3. Threat Modeling

Brute forcing the password would not be impossible but impracticable. Other vulnerabilities would allow the attacker to bypass SSH and the password authentication process altogether.

4. Vulnerability Analysis

The Website gives access to the commands on its user profile. If an attacker wanted to, they could elevate the rights and gain access or find another piece of junk software and exploit that. The Website gives out its password in plaintext, which isn't good practice. This should be encrypted.

5. Exploitation

A Xmas attack on the server or spoofing who the user is would cause the authentication to be null. Changing the password or changing the file type or the location of the readme file to something unusable would make this an exploit. The passwords should be encrypted and salted.

6. Post-Exploitation

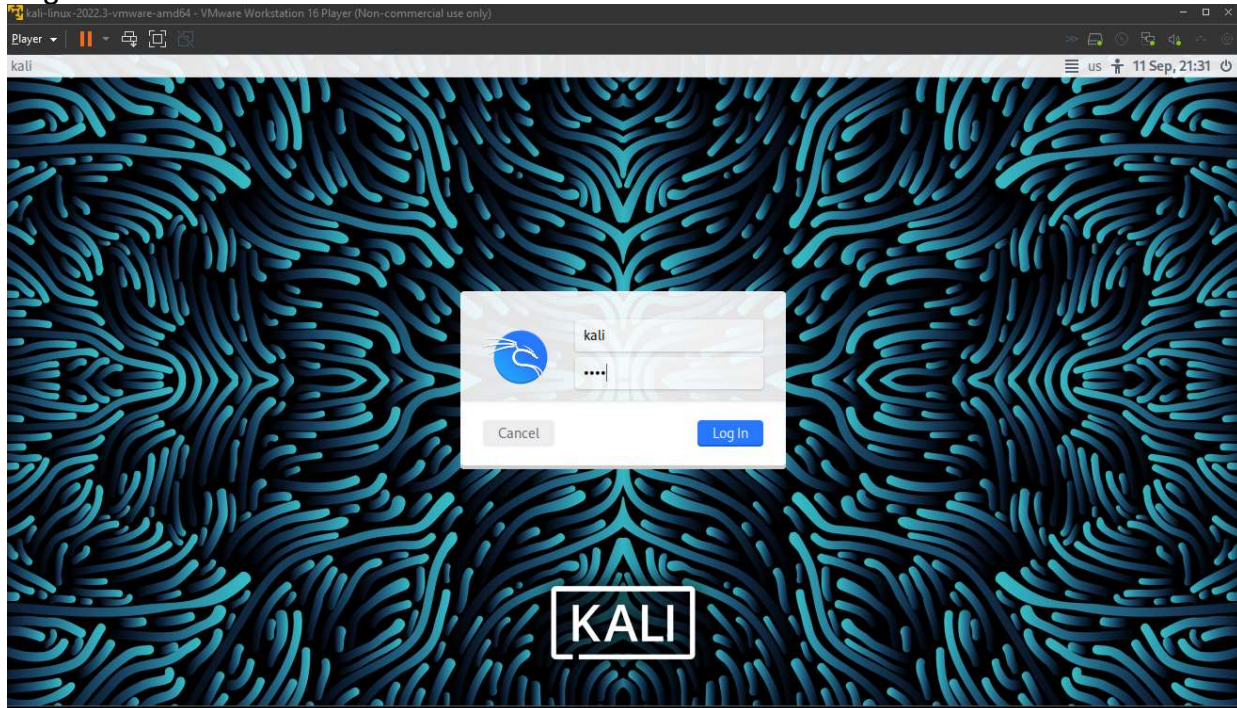
A possible hashed password could exploit the database and cause the user to bypass the SSH system. Elevating the host system to root and executing commands to turn off the server would cause the organization to become disrupted. Changing, elevating, or erasing the user/password altogether would render the site's purpose unusable.

7. Reporting

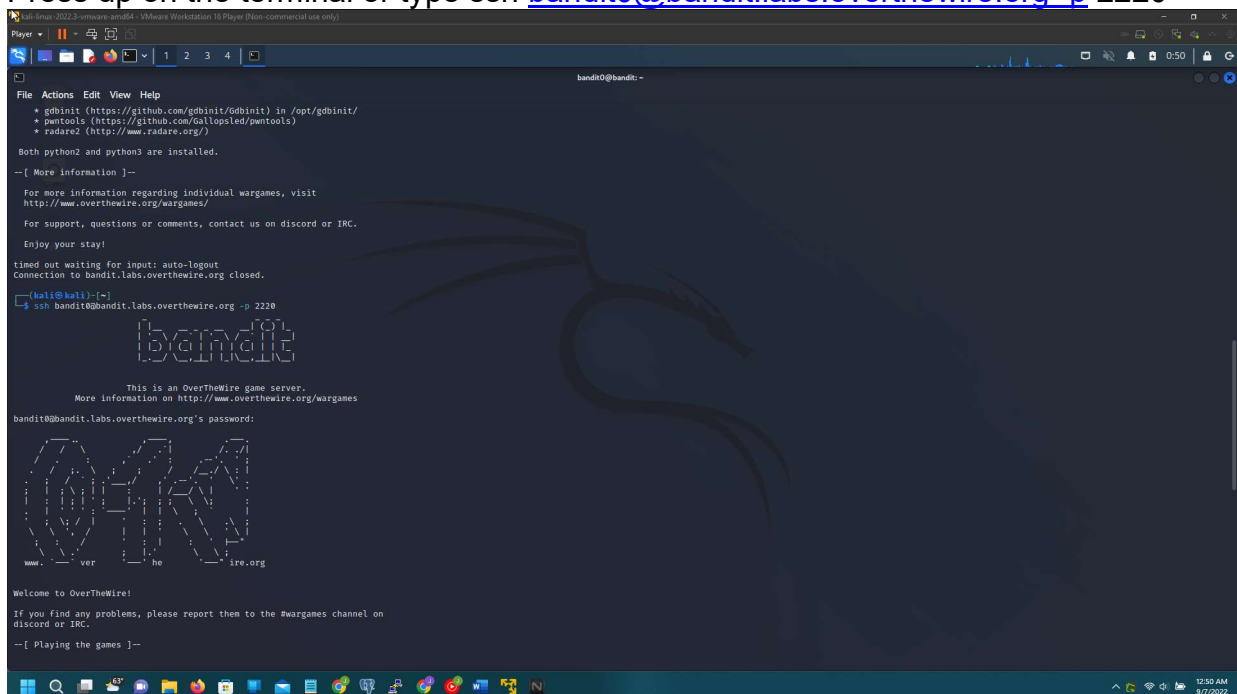
See Results section

Results

1. Log into the VM as kali/kali

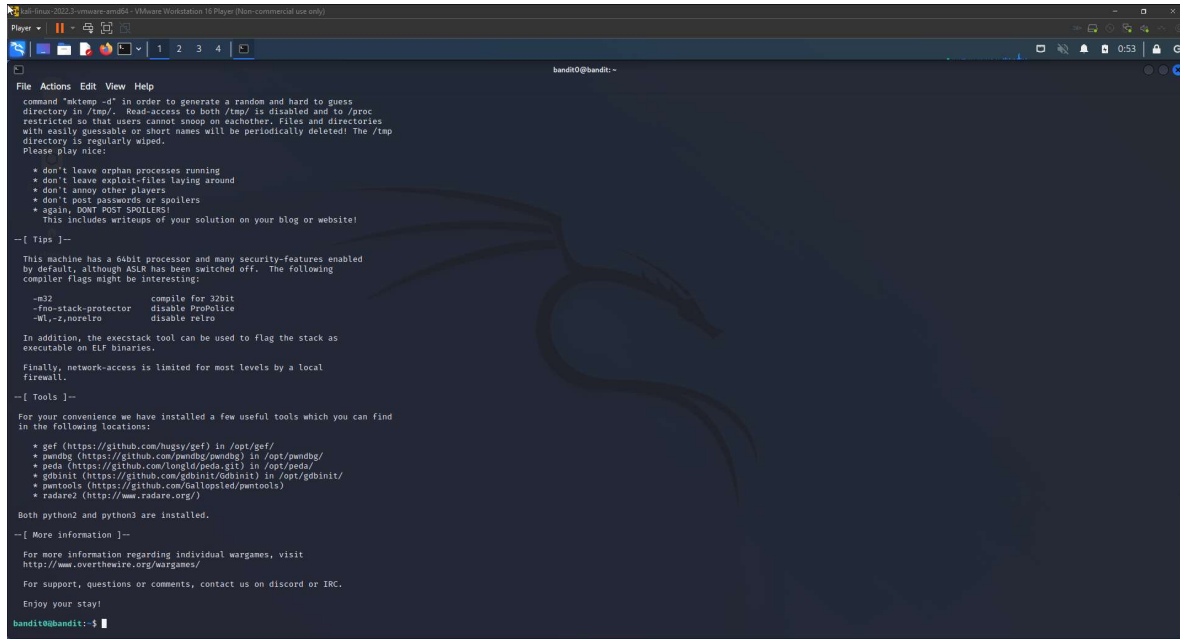


2. Press up on the terminal or type ssh [bandit0@bandit.labs.overthewire.org](https://bandit.labs.overthewire.org) -p 2220



4.

5. Log in with password bandit0

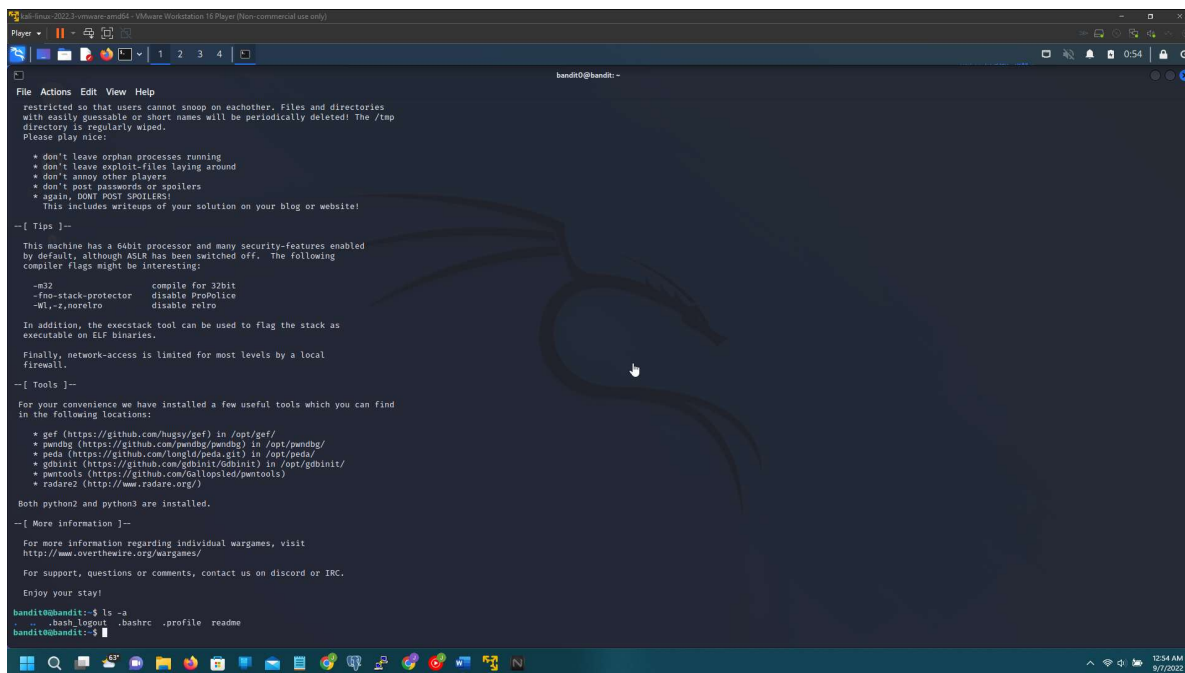


```
bandit0@bandit: ~  
File Actions Edit View Help  
command "mkdir -p" in order to generate a random and hard to guess  
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc  
restricted so that users cannot snoop on eachother. Files and directories  
with easily guessable or short names will be periodically deleted! The /tmp  
directory is regularly wiped.  
Please play nice:  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't post passwords or spoilers  
* again, DON'T POST SPOILERS!  
This includes writeups of your solution on your blog or website!  
--[ Tips ]--  
This machine has a 64bit processor and many security-features enabled  
by default, although ASLR has been switched off. The following  
compiler flags might be interesting:  
-m32 compile for 32bit  
-fno-stack-protector disable ProPolice  
-Wl,-z,norelro disable relro  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
Finally, network-access is limited for most levels by a local  
firewall.  
--[ Tools ]--  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longle/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
Both python2 and python3 are installed.  
--[ More information ]--  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
For support, questions or comments, contact us on discord or IRC.  
Enjoy your stay!  
bandit0@bandit:~$
```

6.

7. The user is now logged in as bandit0@bandit

8. Type ls -a

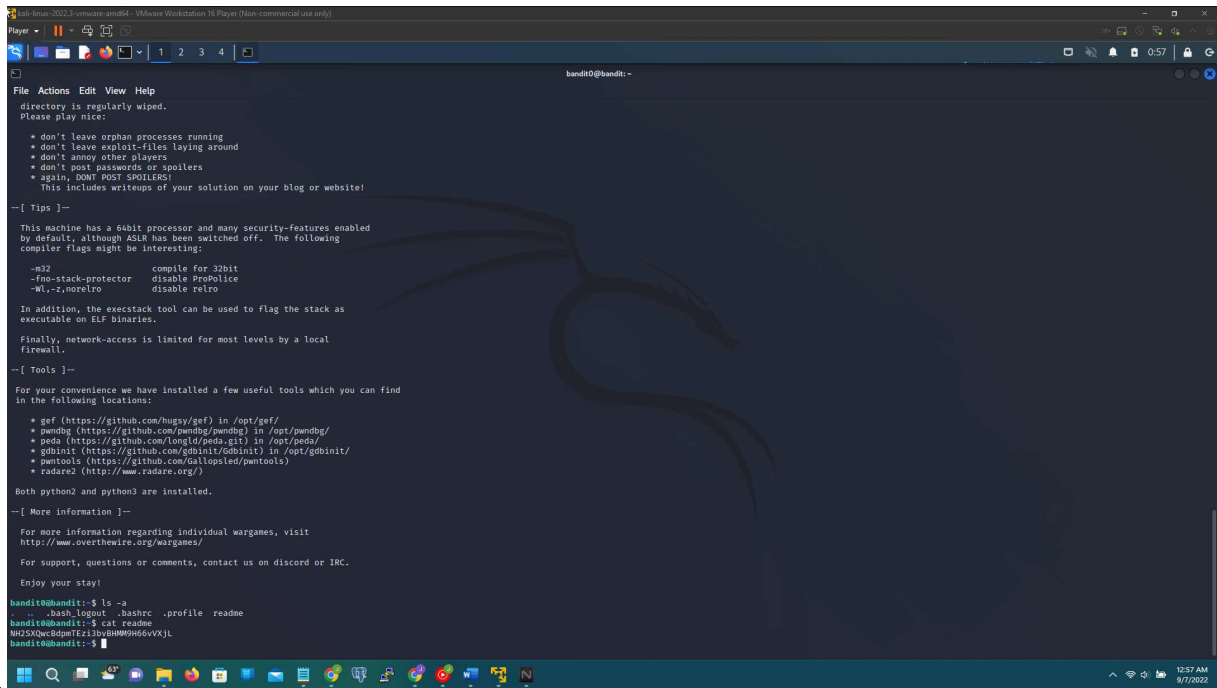


```
bandit0@bandit: ~  
File Actions Edit View Help  
restricted so that users cannot snoop on eachother. Files and directories  
with easily guessable or short names will be periodically deleted! The /tmp  
directory is regularly wiped.  
Please play nice:  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't post passwords or spoilers  
* again, DON'T POST SPOILERS!  
This includes writeups of your solution on your blog or website!  
--[ Tips ]--  
This machine has a 64bit processor and many security-features enabled  
by default, although ASLR has been switched off. The following  
compiler flags might be interesting:  
-m32 compile for 32bit  
-fno-stack-protector disable ProPolice  
-Wl,-z,norelro disable relro  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
Finally, network-access is limited for most levels by a local  
firewall.  
--[ Tools ]--  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longle/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
Both python2 and python3 are installed.  
--[ More information ]--  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
For support, questions or comments, contact us on discord or IRC.  
Enjoy your stay!  
bandit0@bandit:~$ ls -a  
. .bash_logout .bashrc .profile readme  
bandit0@bandit:~$
```

9.

10. This displays the ones need, readme.

11. Type cat readme



```
bandit0@bandit:~  
File Actions Edit View Help  
directory is regularly wiped.  
Please play nice:  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't post passwords or spoilers  
* again, DON'T POST SPOILERS!  
This includes writeups of your solution on your blog or website!  
--[ Tips ]--  
This machine has a 64bit processor and many security-features enabled  
by default, although ASLR has been switched off. The following  
compiler flags might be interesting:  
-m32          compile for 32bit  
-fno-stack-protector  disable ProPolice  
-Wl,-z,norelro  disable relro  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
Finally, network-access is limited for most levels by a local  
firewall.  
--[ Tools ]--  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
* get (https://github.com/hugsy/get) in /opt/get/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools) in /opt/pwntools/  
* radare2 (https://www.radare.org/r) in /opt/radare2/  
Both python2 and python3 are installed.  
--[ More information ]--  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
For support, questions or comments, contact us on discord or IRC.  
Enjoy your stay!  
bandit0@bandit:~$ ls -la  
-bash_logout .bashrc .profile readme  
bandit0@bandit:~$ cat readme  
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL  
bandit0@bandit:~$
```

12.

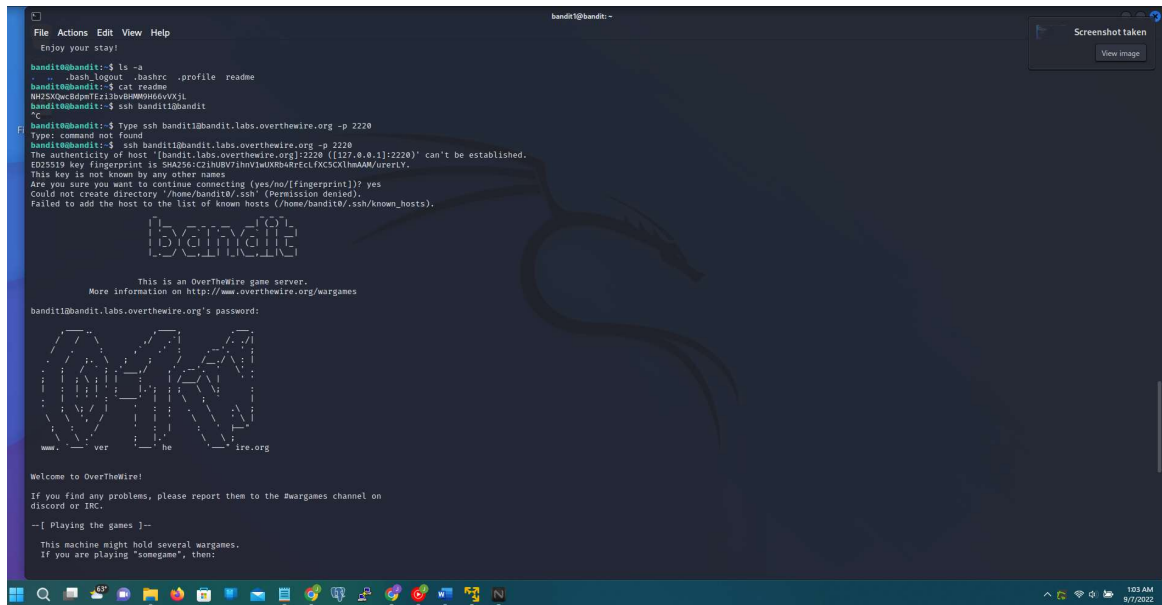
13. The password is: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

14. Highlight and right click> copy selection

15. Type: ssh bandit1@bandit.labs.overthewire.org -p 2220

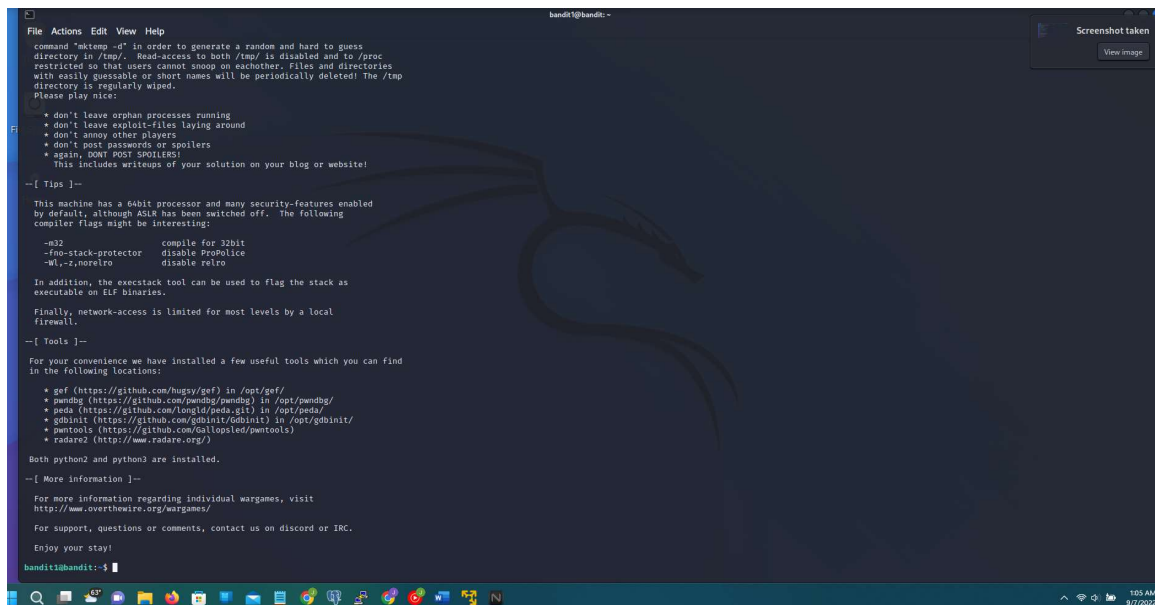
16. Select yes

17. Paste the password: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL



```
bandit0@bandit:~  
File Actions Edit View Help  
Enjoy your stay!  
bandit0@bandit:~$ ls -la  
-bash_logout .bashrc .profile readme  
bandit0@bandit:~$ cat readme  
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL  
bandit0@bandit:~$ ssh bandit1@bandit  
^C  
bandit0@bandit:~$ Type ssh bandit1@bandit.labs.overthewire.org -p 2220  
Type: command not found  
bandit0@bandit:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220  
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]:2220)' can't be established.  
ED25519 key fingerprint is SHA256:C1H0UW7IhV1W0XB4RrECLfKCSCK1hMAAM/urervL.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Could not create directory '/home/bandit0/.ssh' (permission denied).  
Failed to add the host to the list of known hosts (/home/bandit0/.ssh/known_hosts).  
bandit1@bandit.labs.overthewire.org's password:  
Welcome to OverTheWire!  
If you find any problems, please report them to the #wargames channel on  
discord or IRC.  
--[ Playing the games ]--  
This machine might hold several wargames.  
If you are playing "somegame", then:
```

18.



```
bandit1@bandit1:~$  
command "mktemp -d" in order to generate a random and hard to guess  
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc  
restricted so that users cannot snoop on each other, files and directories  
with easily guessable or short names will be periodically deleted! The /tmp  
directory is regularly wiped.  
Please play nice!  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't post passwords or spoilers  
* again, DONT POST SPOILERS!  
This includes writeups of your solution on your blog or website!  
-- [ Tips ] --  
This machine has a 64bit processor and many security-features enabled  
by default, although ASLR has been switched off. The following  
compiler flags might be interesting:  
-m32          compile for 32bit  
-fno-stack-protector  disable ProPolice  
-Wl,-z,norelro  disable relro  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
Finally, network-access is limited for most levels by a local  
firewall.  
-- [ Tools ] --  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/lionel0/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
Both python2 and python3 are installed.  
-- [ More information ] --  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
For support, questions or comments, contact us on discord or IRC.  
Enjoy your stay!  
bandit1@bandit1:~$
```

19.

20. The user is now logged in as bandit1@bandit

References

1. <https://www.wikihow.com/Use-SSH>
2. http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
3. <https://kirkpatrickprice.com/blog/stages-of-penetration-testing-according-to-ptes/>
4. <https://overthewire.org/wargames/bandit/bandit1.html>
5. <https://www.ibm.com/docs/en/i/7.3?topic=security-password-encryption> .

The College of Saint Rose

ETHICAL HACKING REPORT

ASSIGNMENT # 1 BANDIT 2

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 1 to 2, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The user will also have to use google to find out how to use the dashed filename and be able to read a password field from the file extension. The file is in /home dir.

Tools

- A VM running a Linux distro (Kali),
- A terminal prompt, the Website <https://overthewire.org/wargames/bandit/bandit2.html>
- The following Linux commands `ls` - list files `ls -a` list all files including hidden, `cd` change directory `copy` and `paste`, and `cat` to concatenate or read, `cat < -` or `./-` to read the input file
- Google: <https://www.google.com/search?q=dashed+filename>

Methodology

1. Pre-Engagement Interactions

The tools needed to perform the test are Vmware Player workstation 16, Kali Linux kali-Linux-2022.3-VirtualBox-amd64, SSH, the Website <https://overthewire.org/wargames/bandit/bandit2.html>, the command line interface the mouse to be able to copy and paste, enable shared clipboard in VMware. Google : <https://www.google.com/search?q=dashed+filename> the `cat < -` or `./-` to read the input file

2. Intelligence Gathering

A Google search reveals that `cat < dash` will allow reading or `cat reverse < dash` file names.

3. Threat Modeling

Since a tutorial of this example is online, a password is freely given. Access can be easily acquired.

4. Vulnerability Analysis

The Website gives access to the commands on its user profile. If an attacker wanted to, they could elevate the rights and gain access or find another piece of junk software and exploit that. The Website gives out its password in plaintext, which isn't good practice. This should be encrypted. They do not have an up-to-date Linux system that could cause an attacker to expose the database.

5. Exploitation

A brute force or a scripted attack on the SSH service could allow entry. Also, having done the previous exercise, the user can now access and manipulate data on the server if they know how. Using pipes and elevating privileges could allow an attacker access to the server to overwrite data.

6. Post-Exploitation

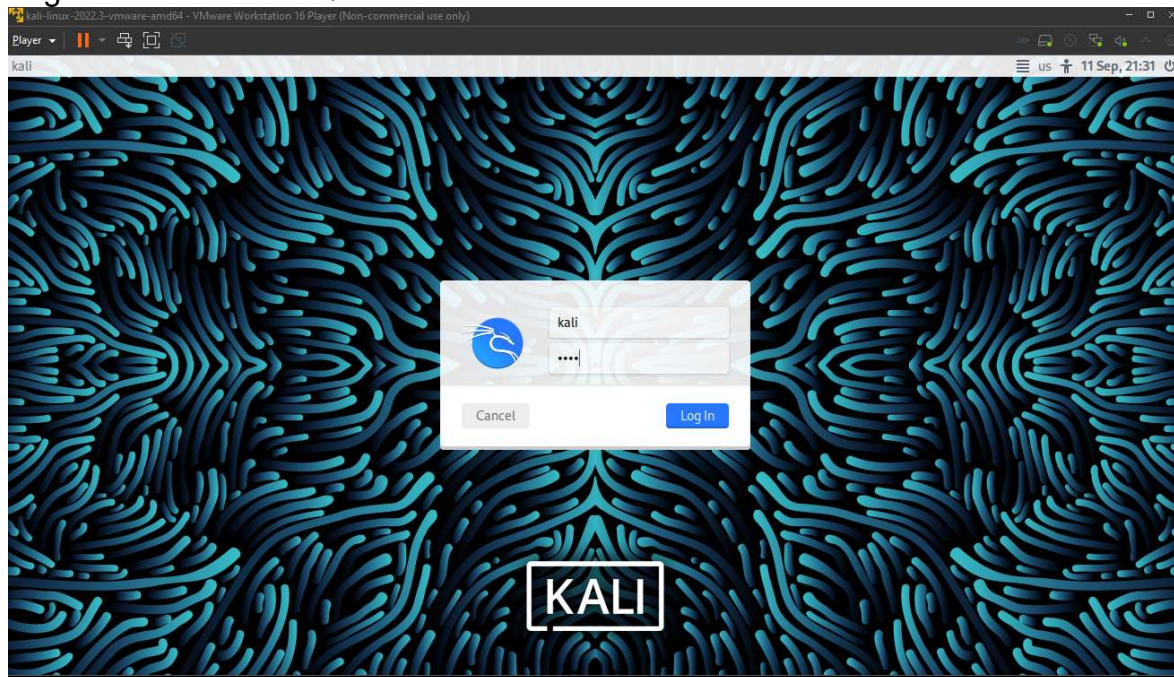
A possible hashed password could exploit the database and cause the user to bypass the SSH system. Elevating the host system to root and executing commands to turn off the server would cause the organization to become disrupted. Changing, elevating, or erasing the user/password altogether would render the site's purpose unusable.

7. Reporting

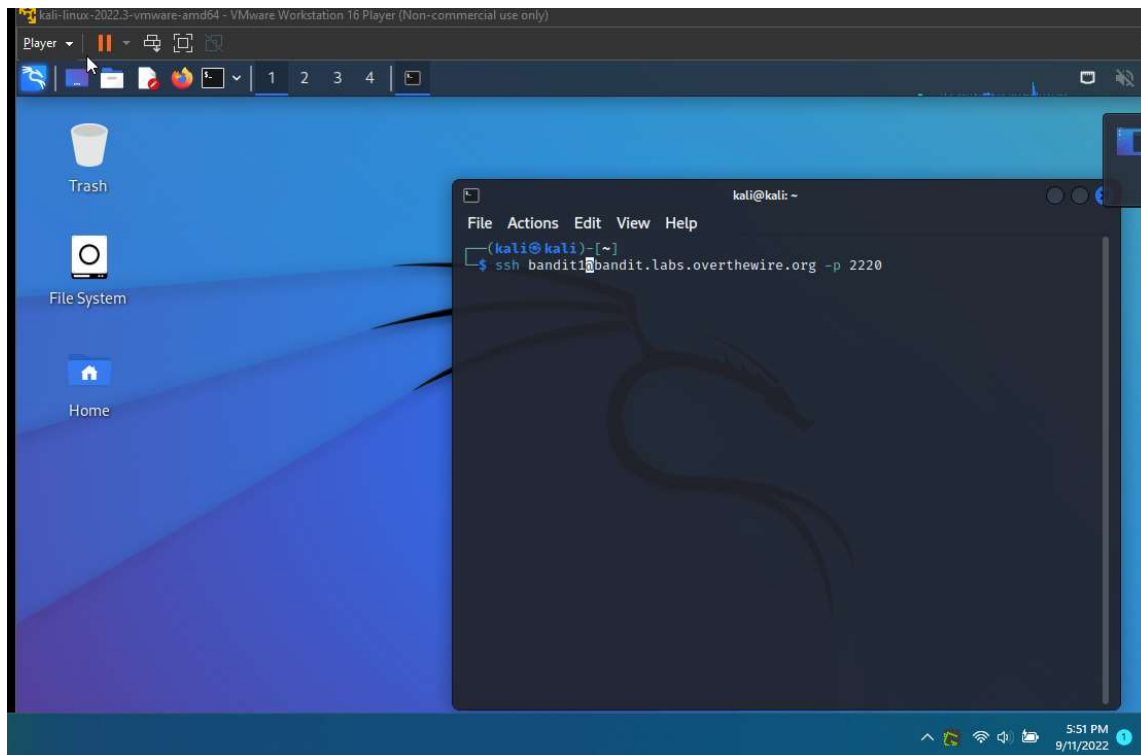
See Results section

Results

1. Log into the VM as kali/kali

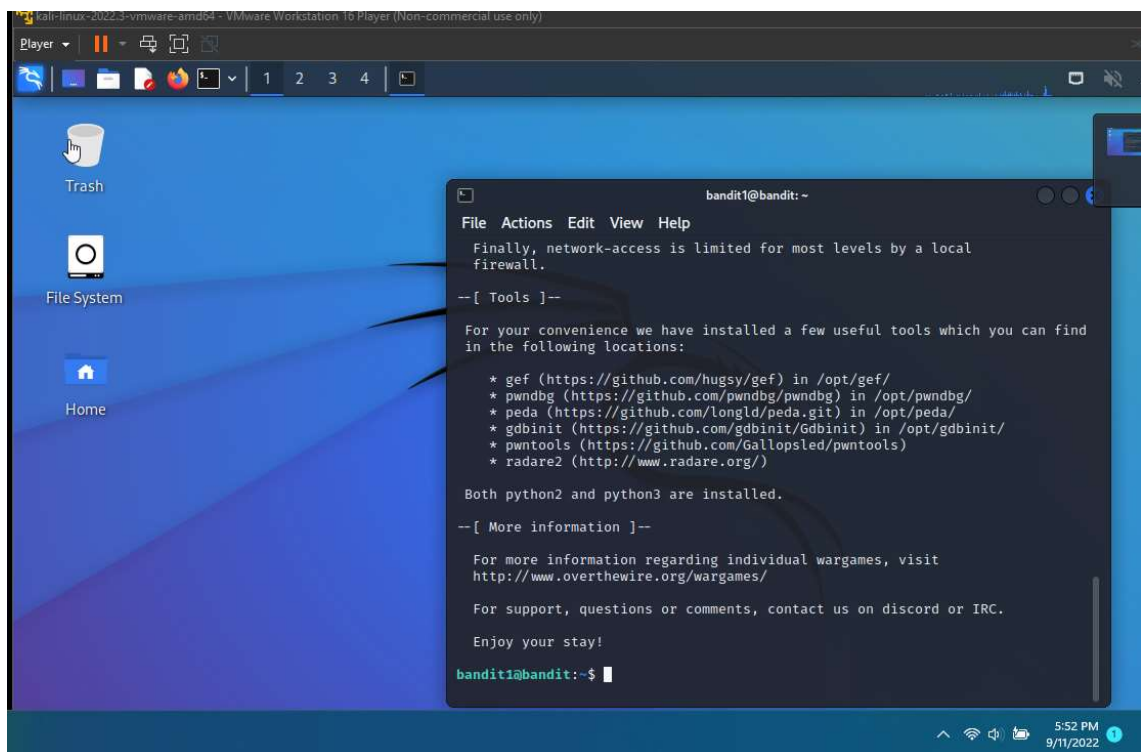


- 2.
3. Press up on the terminal or type ssh bandit1@bandit.labs.overthewire.org -p 2220



4.

5. Log in with password NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL



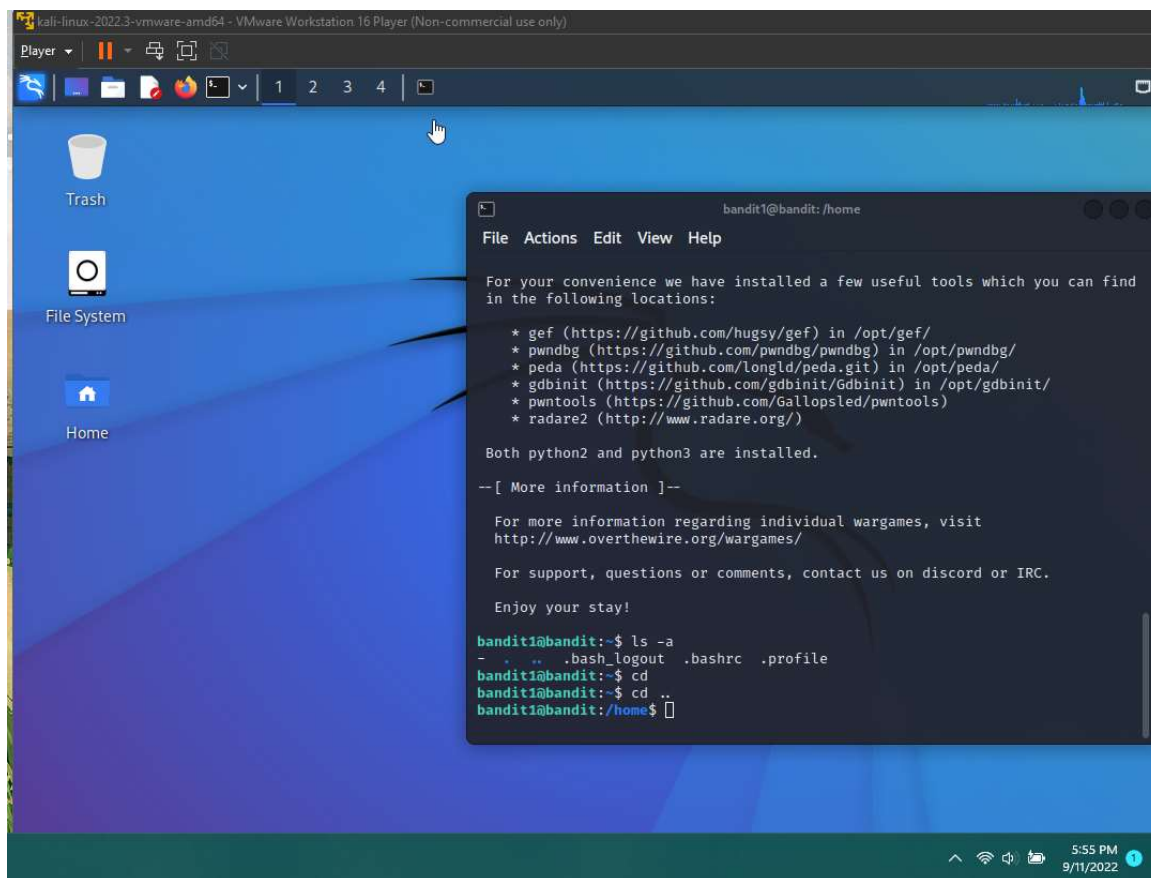
6.

7. Ls -a to see the directory

8. The user is now logged in as bandit0@bandit

9. Type ls -a file.

10. I did not find anything new, so I did cd to change the directory to go to /home



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying a welcome message from the Bandit wargame. The message lists installed tools like gef, pwndbg, peda, gdbinit, pwntools, and radare2. It also mentions that both python2 and python3 are installed. Below the message, the user runs the command `ls -a`, which shows the hidden files `.bash_logout`, `.bashrc`, and `.profile`. The user then runs `cd` to move to the home directory, and finally `cd ..` to move to the parent directory, which is `/home`.

```
bandit1@bandit: /home
File Actions Edit View Help

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

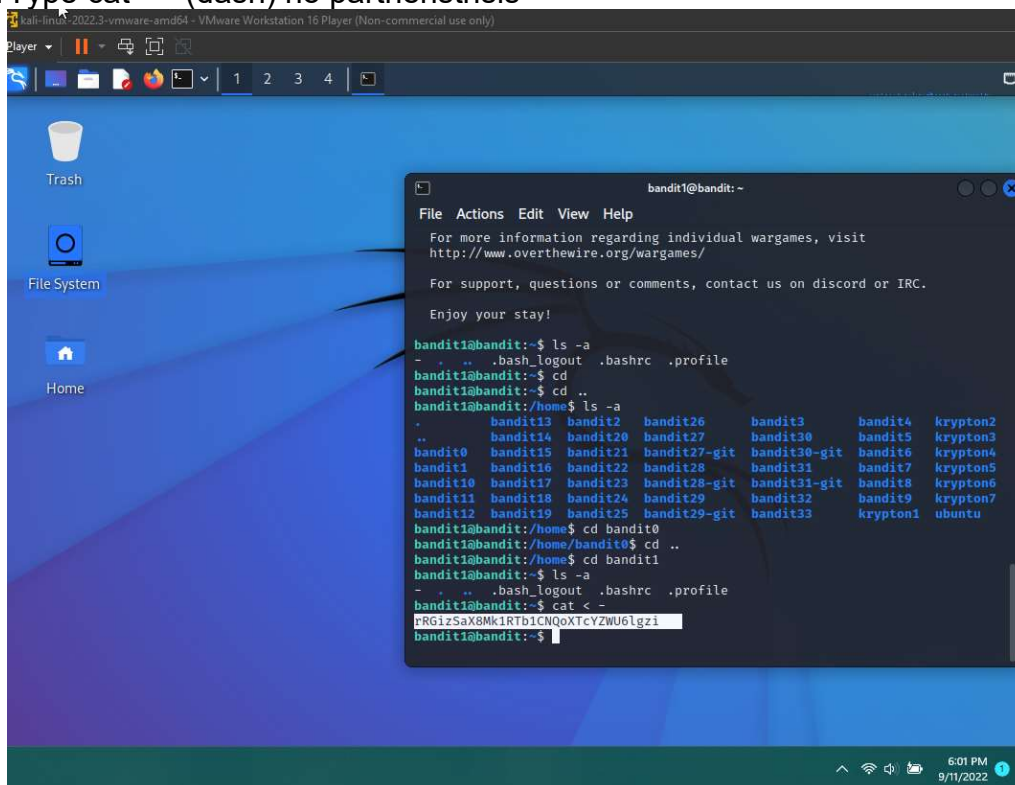
Enjoy your stay!

bandit1@bandit:~$ ls -a
- . .. .bash_logout .bashrc .profile
bandit1@bandit:~$ cd
bandit1@bandit:~$ cd ..
bandit1@bandit:/home$
```

11.

12. Ls -a again seen file structure

13. Type cat < - (dash) no parthensthesis



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying a directory listing of the `/home` directory. The listing shows a grid of directories and files, including `bandit13`, `bandit2`, `bandit26`, `bandit3`, `bandit4`, `krypton2`, `bandit14`, `bandit20`, `bandit27`, `bandit30`, `bandit5`, `krypton3`, `bandit0`, `bandit15`, `bandit21`, `bandit27-git`, `bandit30-git`, `bandit6`, `krypton4`, `bandit1`, `bandit16`, `bandit22`, `bandit28`, `bandit31`, `bandit7`, `krypton5`, `bandit10`, `bandit17`, `bandit23`, `bandit28-git`, `bandit31-git`, `bandit8`, `krypton6`, `bandit11`, `bandit18`, `bandit24`, `bandit29`, `bandit32`, `bandit9`, `krypton7`, `bandit12`, `bandit19`, `bandit25`, `bandit29-git`, `bandit33`, `krypton1`, and `ubuntu`. The user then runs `cd bandit0`, `cd`, `cd bandit1`, and `ls -a`. Finally, the user runs `cat < -`, which outputs the flag `rRGiz5aX8Mk1RTb1CNQoXtCvZWU6lgzi`.

```
bandit1@bandit: ~
File Actions Edit View Help

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit1@bandit:~$ ls -a
- . .. .bash_logout .bashrc .profile
bandit1@bandit:~$ cd
bandit1@bandit:~$ cd ..
bandit1@bandit:/home$ ls -a
. bandit13 bandit2 bandit26 bandit3 bandit4 krypton2
.. bandit14 bandit20 bandit27 bandit30 bandit5 krypton3
bandit0 bandit15 bandit21 bandit27-git bandit30-git bandit6 krypton4
bandit1 bandit16 bandit22 bandit28 bandit31 bandit7 krypton5
bandit10 bandit17 bandit23 bandit28-git bandit31-git bandit8 krypton6
bandit11 bandit18 bandit24 bandit29 bandit32 bandit9 krypton7
bandit12 bandit19 bandit25 bandit29-git bandit33 krypton1 ubuntu
bandit1@bandit:/home$ cd bandit0
bandit1@bandit:/home/bandit0$ cd
bandit1@bandit:/home$ cd bandit1
bandit1@bandit:~$ ls -a
- . .. .bash_logout .bashrc .profile
bandit1@bandit:~$ cat < -
rRGiz5aX8Mk1RTb1CNQoXtCvZWU6lgzi
bandit1@bandit:~$
```

14.

15. Copy password rGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi for bandit3

References

1. <https://stackoverflow.com/questions/42187323/how-to-open-a-dashed-filename-using-terminal>
2. <https://overthewire.org/wargames/bandit/bandit2.html>

The College of Saint Rose

ETHICAL HACKING REPORT

ASSIGNMENT # 1 BANDIT 3

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 2 to 3, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The user will also have to use google to use "spaces in name files". The user will also need to be able to navigate to the home directory. The user will also need to be able to access "spaces in this filename" on the file structure.

Tools

- The tools needed will be a VM running a Linux distro (Kali)
- A terminal prompt
- the Website <https://overthewire.org/wargames/bandit/bandit3.html>
- the following Linux commands `ls` - list files `ls -a` list all files including hidden files, `cd` changedirectory copy, paste, cat or read, and the touch command and `"\"`
- <https://linuxhint.com/reference-filename-with-spaces-linux/>
- <https://medium.com/@theGirlWhoEncrypts/overthewire-bandit-level-2-level-3-2caa934d3c6e>

Methodology

1. Pre-Engagement Interactions

The tools needed to perform the test are Vmware Player workstation 16, Kali Linux kali-Linux-2022.3-VirtualBox-amd64, SSH, the Website

<https://overthewire.org/wargames/bandit/bandit3.html>, the command line interface the mouse to be able to copy and paste, enable shared clipboard in VMware. Google: <https://linuxhint.com/reference-filename-with-spaces-linux/> the touch and `\` commands

2. Intelligence Gathering

A Google search reveals that the touch command allows users to access or read files with spaces in the name. Along with `\` char. Because I was in the home dir, I saw all users instead of the intended file. I need help with that instances.

<https://medium.com/@theGirlWhoEncrypts/overthewire-bandit-level-2-level-3-2caa934d3c6e> was a reference that provided the steps required.

3. Threat Modeling

A user that can travel the structure of the Linux OS could find other files that could be used similarly, such as `/mnt` or the `/bin` dir. Remote Code Execution could allow code to run in those `/dirs`. A user learning this material could now find any file with spaces.

4. Vulnerability Analysis

While putting spaces in the file would stop a novice user from executing the file, any google search would allow the user to see the file and, with `\`'s, will enable them to see and run it.

5. Exploitation

Space's would stop some but not many. A recommendation would be encryption. Using plain text is never a good idea.

6. Post-Exploitation

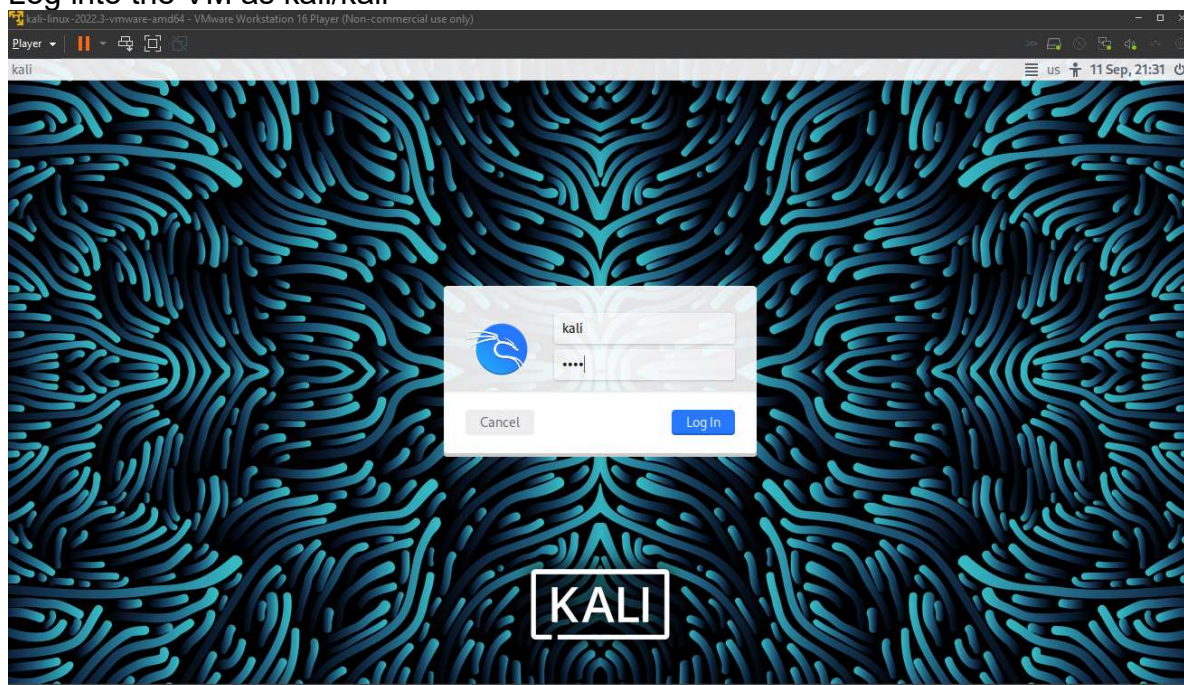
Recommend using encryption with salting. Also, not allow the password to be easily accessible.

7. Reporting

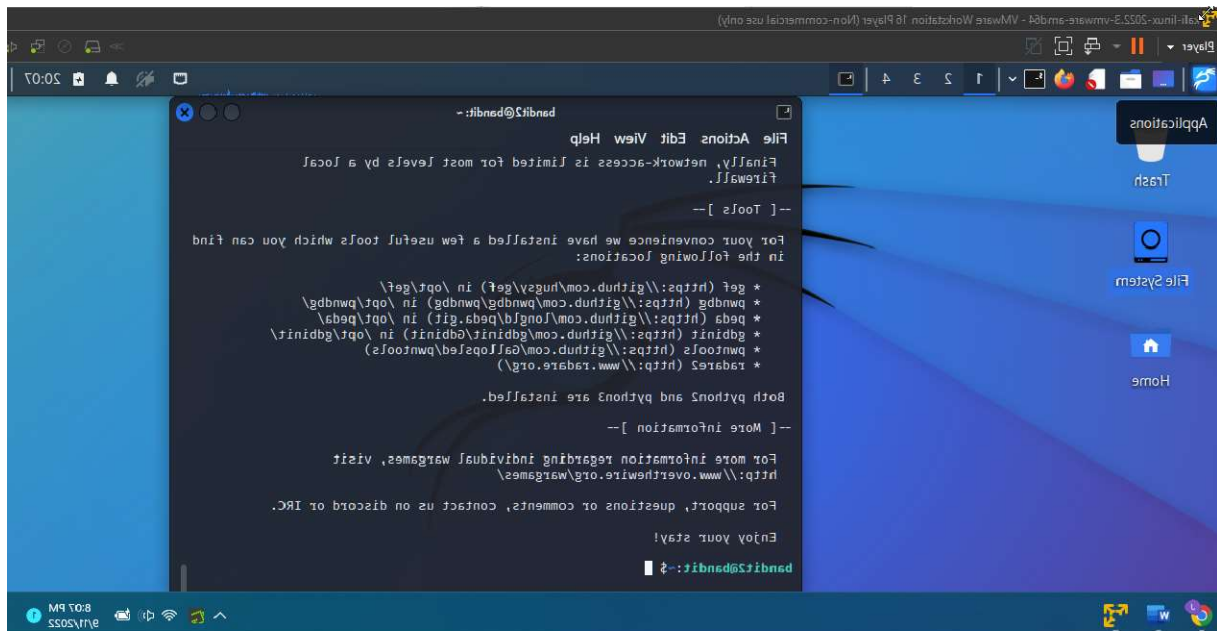
See Results section

Results

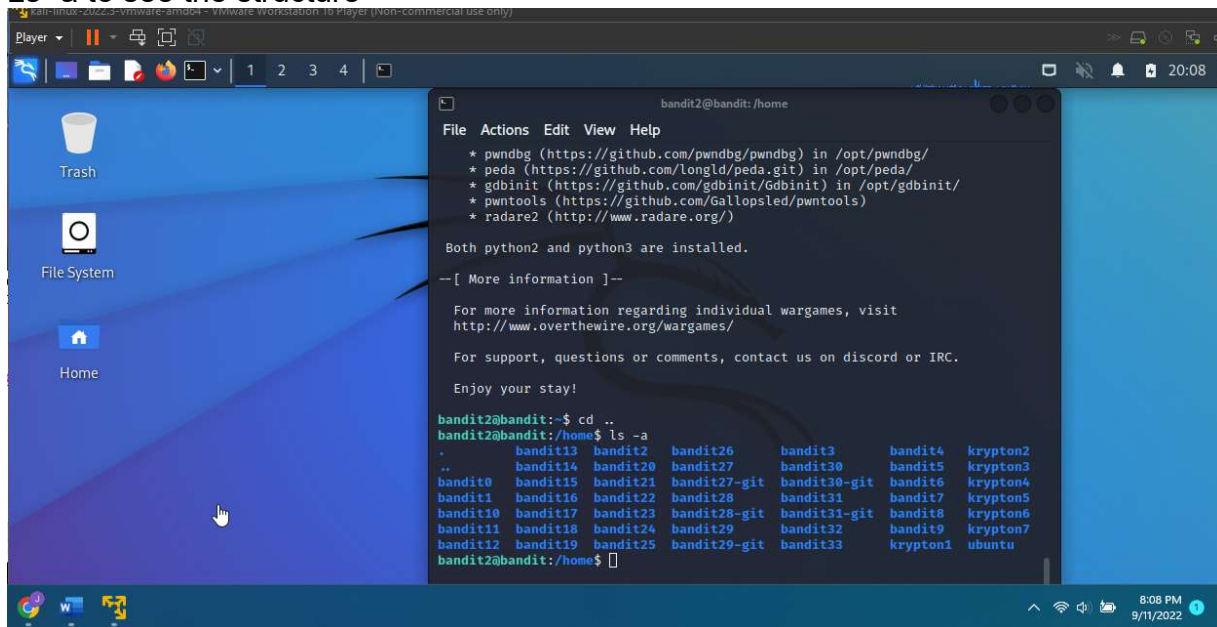
1. Log into the VM as kali/kali



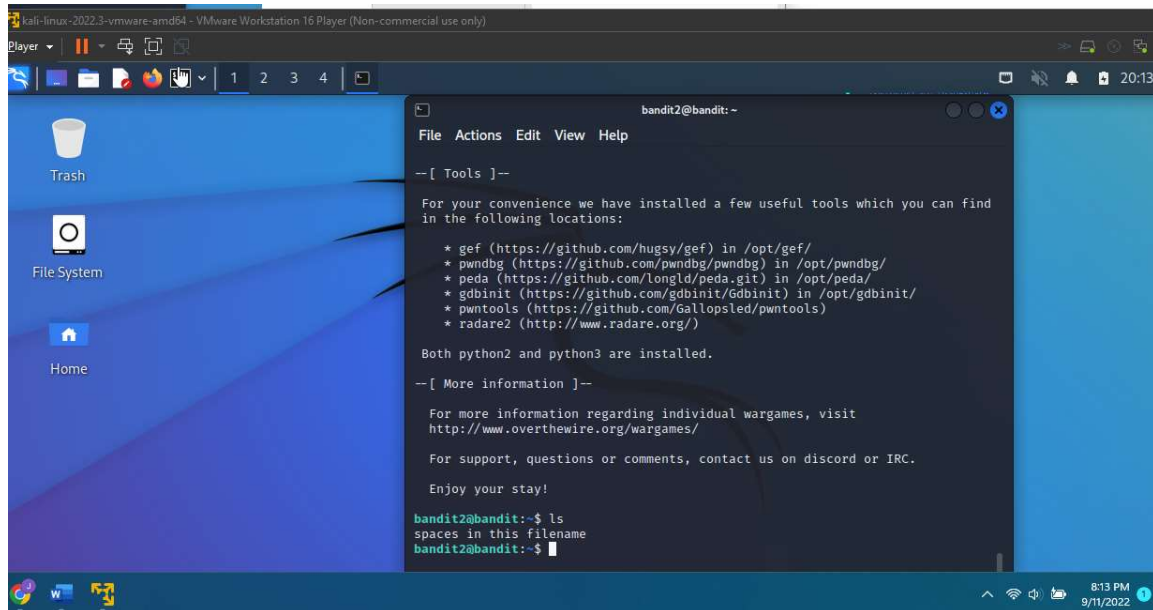
- 2.
3. Log onto SSH as bandit2@bandit.labs.overthewire.org -p 2220
4. Password rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi



- 5.
6. Cd .. to home dir
7. Ls -a to see the structure



- 8.
9. Nothing is shown
10. Close and relog in as bandit2
11. Ls in that dir

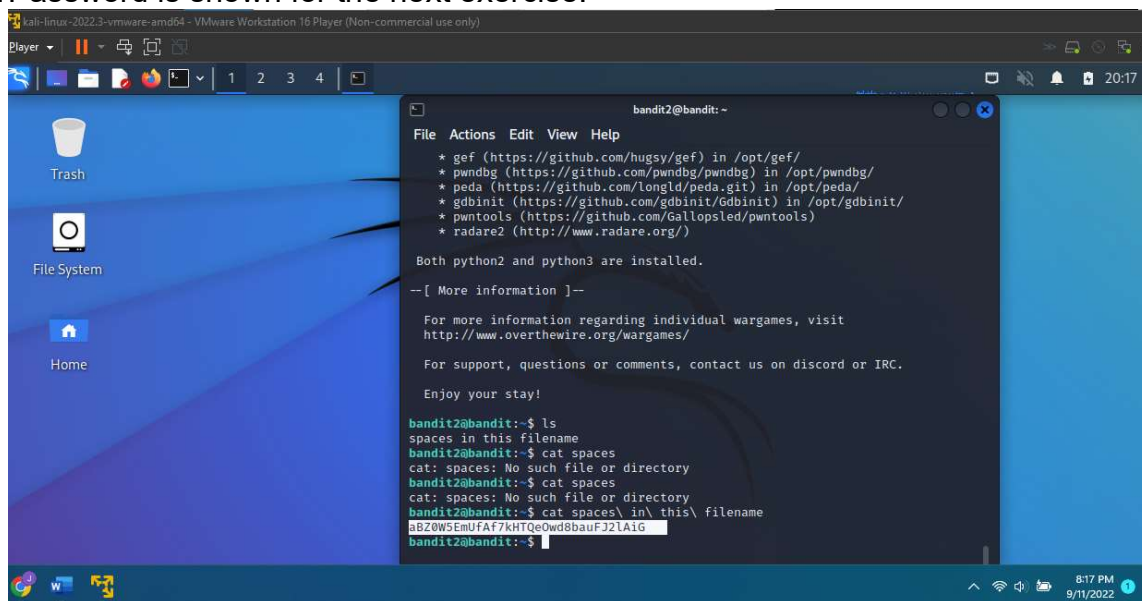


12.

13. File is found

14. Add type cat spaces\ in\ this\ filename to read file or press tab to auto-complete after a few words after spaces.

15. Password is shown for the next exercise.



16.

17. Password is aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG for bandit3

References

1. <https://linuxhint.com/reference-filename-with-spaces-linux/>
2. <https://medium.com/@theGirlWhoEncrypts/overthewire-bandit-level-2-level-3-2caa934d3c6e>

The College of Saint Rose

ETHICAL HACKING REPORT

ASSIGNMENT # 1 BANDIT 4

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 3 to 4, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is hidden in the "inhere" Directory. The ls -a command finds hidden files, and the cat can read a file. Once the file is discovered, the file can be read.

Tools

- The tools needed will be a VM running a Linux distro (Kali).
- A terminal prompt.
- The Website <https://overthewire.org/wargames/bandit/bandit4.html>
- the following Linux commands ls - list files ls -a list all files including hidden files, cd (change directory) copy, paste, cat or read, and the touch command.
- <https://www.javatpoint.com/open-file-in-linux>

Methodology

1. Pre-Engagement Interactions

The tools needed to perform the test are Vmware Player workstation 16, Kali Linux kali-Linux-2022.3-VirtualBox-amd64, SSH, the Website <https://overthewire.org/wargames/bandit/bandit4.html>, the command line interface the mouse to be able to copy and paste, enable shared clipboard in Vmware. The Website <https://linuxhint.com/reference-filename-with-spaces-linux/> the touch, ls -a, cd, and the cat commands

2. Intelligence Gathering

A google search for how to read .hidden files was imperative. <https://www.javatpoint.com/open-file-in-linux> wielded how to use cat to read .hidden files. After navigating to the source file, I determined the password of the file of Bandit4 SSH.

3. Threat Modeling

A user could still travel the root directory of the host to find users and other important files.

4. Vulnerability Analysis

Putting the file in the hidden file structure or system puts the system at risk. The file was still in plain text and easily accessible. A better method would be to encrypt the volume or file and not allow SSH or change passwords often.

5. Exploitation

If a user could follow step 0, they would be able to log onto the target machine.

6. Post-Exploitation

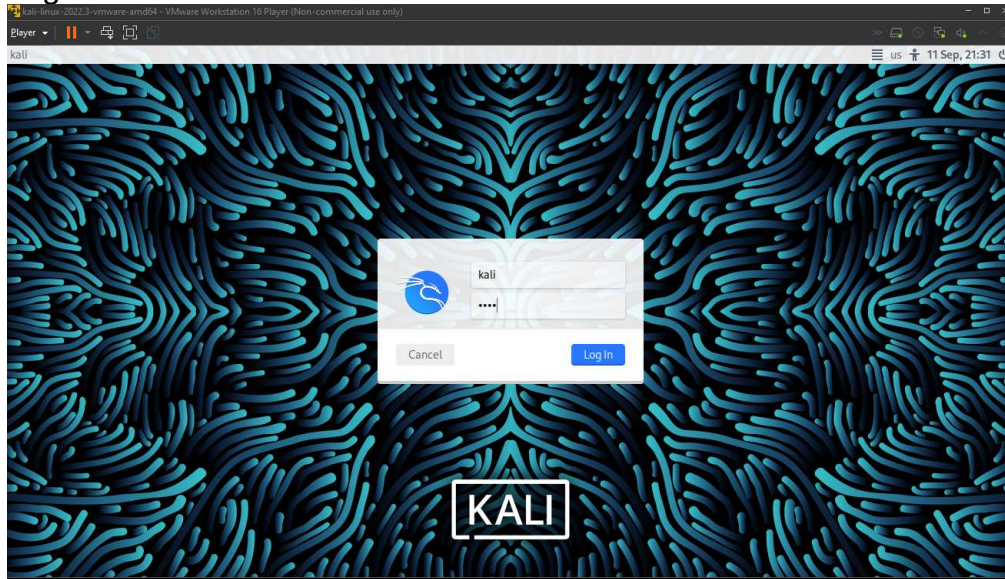
Recommend using encryption with salting. Also, not allow the password to be easily accessible.

7. Reporting

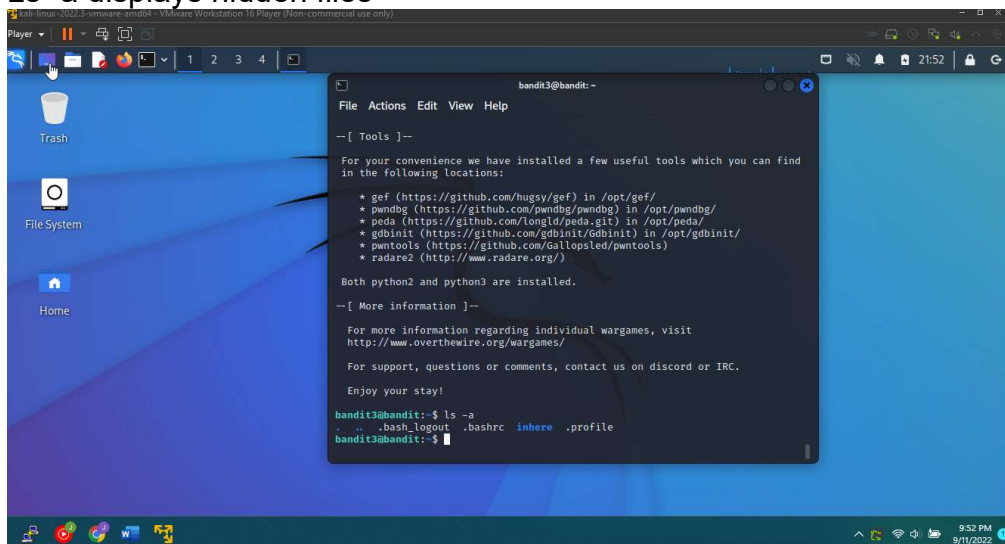
See Results section

Results

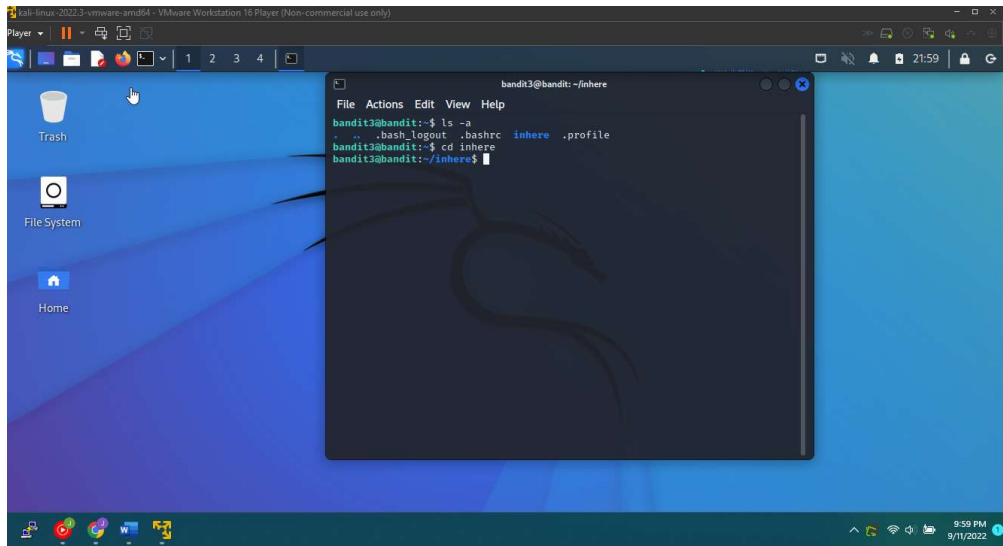
1. Log into the VM as kali/kali



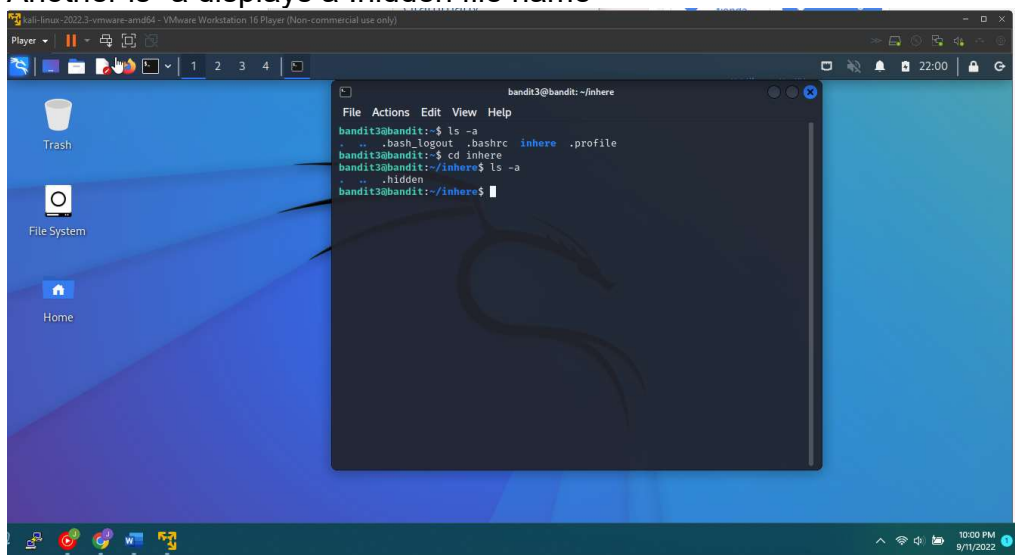
- 2.
3. Log onto SSH as bandit3@bandit.labs.overthewire.org -p 2220
4. Password rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
5. Ls -a displays hidden files



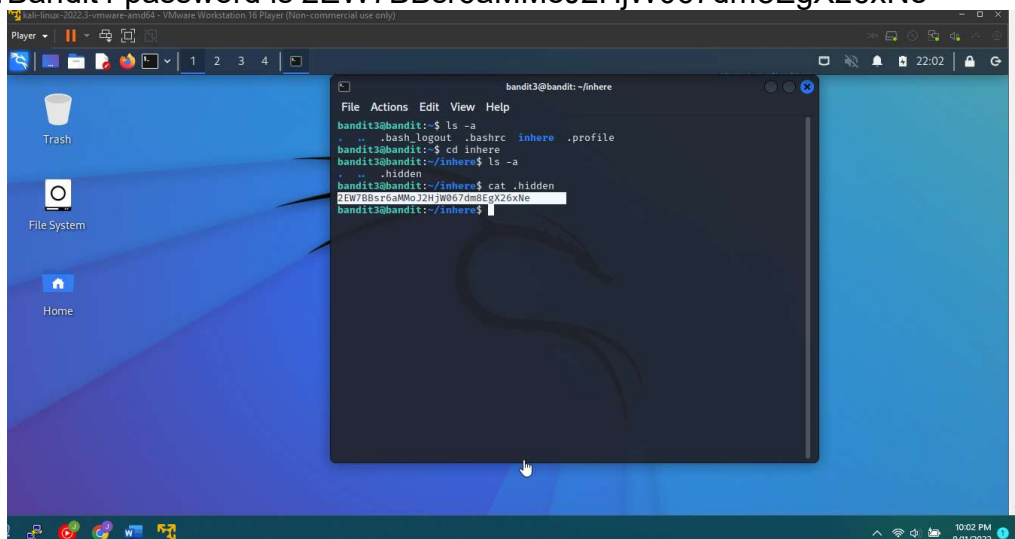
- 6.
7. Cd into the directory /inhere



- 8.
9. Another ls -a displays a .hidden file name



- 10.
11. Cat .hidden reads the file
12. Bandit4 password is 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe



- 13.

References

1. <https://www.javatpoint.com/open-file-in-linux>

The College of Saint Rose

ETHICAL HACKING REPORT
ASSIGNMENT # 1 BANDIT 5

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 5 to 6, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is hidden in the "inhere" Directory. The `ls -a` and `-ls` command finds hidden files and tree folder structure, and the `cat` can read a file. Once the file is discovered, the file can be read. The `grep` command. The `find` and the flags with it like `-type` and `f` for file size.

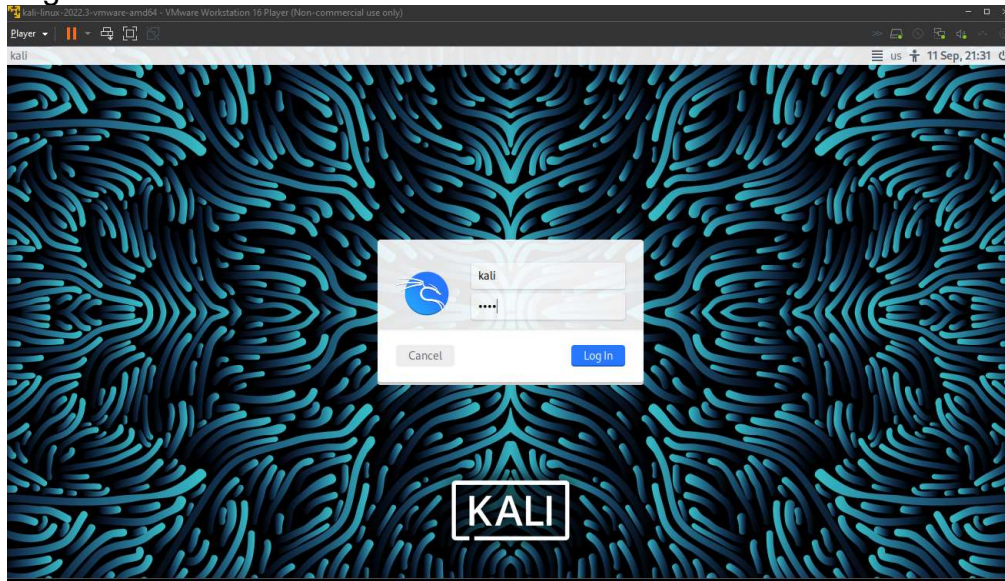
Tools

- The tools needed will be a VM running a Linux distro (Kali).
- A terminal prompt.
- The Website <https://overthewire.org/wargames/bandit/bandit6.html>
- The following Linux commands `ls` - list files `ls -a` list all files including hidden files, `cd` (change directory), `copy`, `paste`, `find`, `cat` or `read`, `grep`, and pipes.
- <https://mayadevbe.me/posts/overthewire/bandit/level6/>

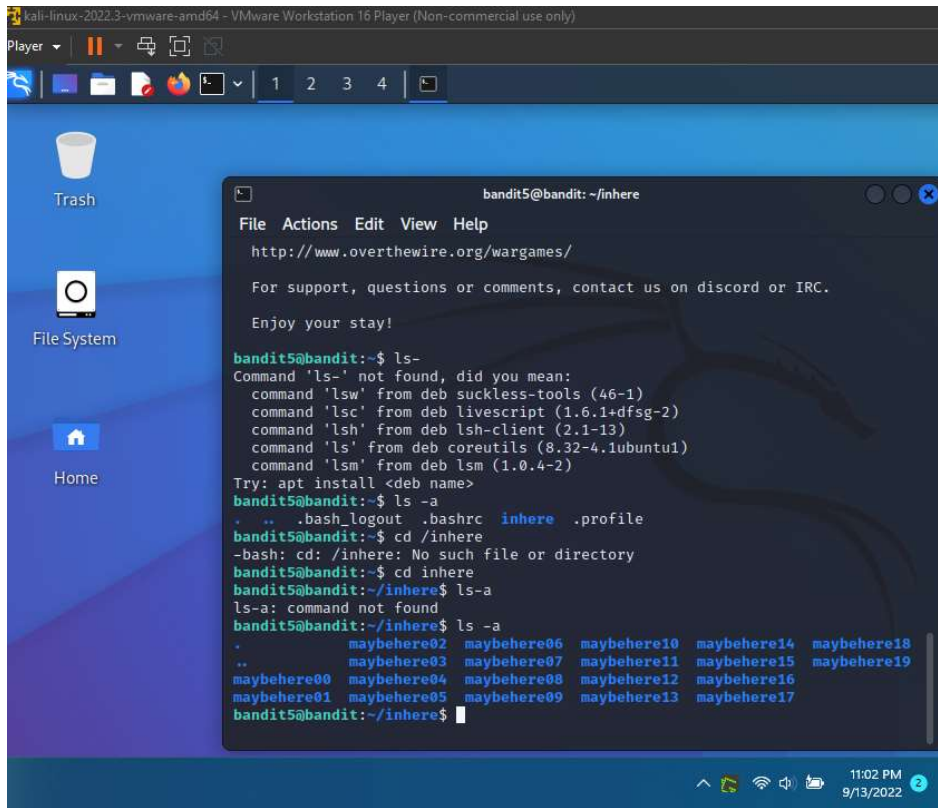
Methodology

Results

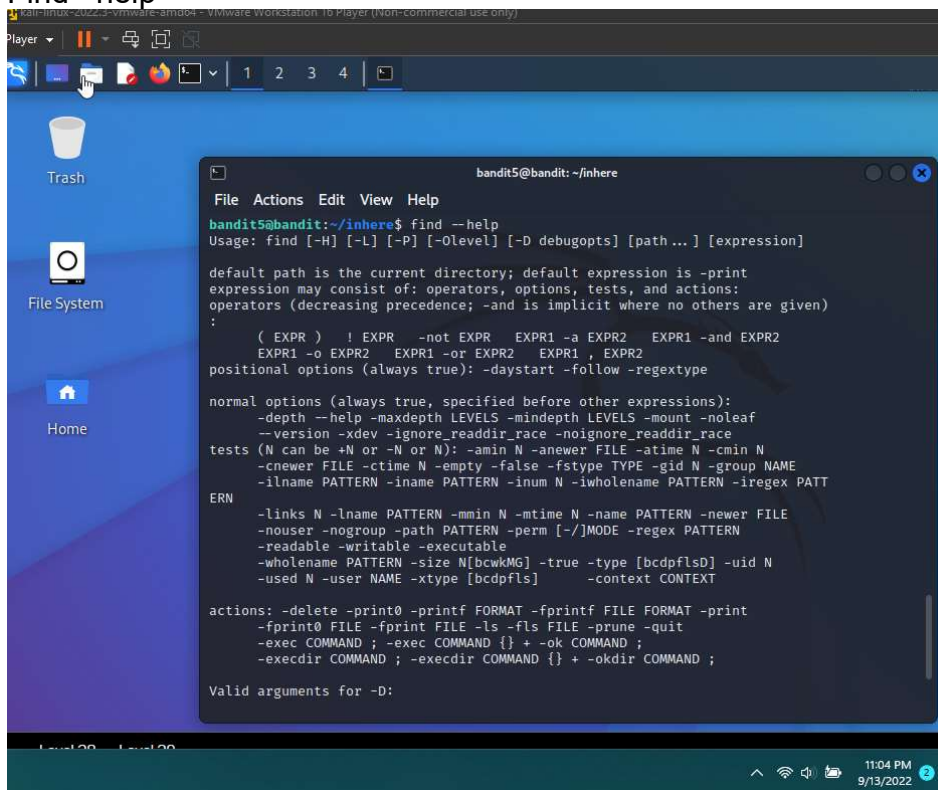
1. Log into the VM as kali/kali



- 2.
3. Bandit5 password `lrlWWI6bB37kxfiCQZqUdOIYfr6eEeqR`
4. `Ls -a` displays hidden files



- 5.
6. Find --help



- 7.

```

bandit5@bandit: ~/inhere
File Actions Edit View Help
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere03
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere04
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere05
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere06
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere07
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere08
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere09
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere10
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere11
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere12
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere13
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere14
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere15
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere16
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere17
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere18
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere19
bandit5@bandit:~/inhere$ ls -la maybehere00
total 72
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 .
drwxr-x-- 22 root bandit5 4096 Sep 1 06:30 ..
-rwxr-x-- 1 root bandit5 1039 Sep 1 06:30 -file1
-rwxr-x-- 1 root bandit5 551 Sep 1 06:30 .file1
-rw-r-- 1 root bandit5 9388 Sep 1 06:30 -file2
-rw-r-- 1 root bandit5 7836 Sep 1 06:30 .file2
-rwxr-x-- 1 root bandit5 7378 Sep 1 06:30 -file3
-rwxr-x-- 1 root bandit5 4802 Sep 1 06:30 .file3
-rwxr-x-- 1 root bandit5 6118 Sep 1 06:30 spaces file1
-rw-r-- 1 root bandit5 6850 Sep 1 06:30 spaces file2
-rwxr-x-- 1 root bandit5 1915 Sep 1 06:30 spaces file3
bandit5@bandit:~/inhere$

```

- 8.
9. Ls -la displays folder structure within trees.

```

bandit5@bandit: ~/inhere
File Actions Edit View Help
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere14
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere15
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere16
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere17
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere18
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 maybehere19
bandit5@bandit:~/inhere$ ls -la maybehere00
total 72
drwxr-x-- 2 root bandit5 4096 Sep 1 06:30 .
drwxr-x-- 22 root bandit5 4096 Sep 1 06:30 ..
-rwxr-x-- 1 root bandit5 1039 Sep 1 06:30 -file1
-rwxr-x-- 1 root bandit5 551 Sep 1 06:30 .file1
-rw-r-- 1 root bandit5 9388 Sep 1 06:30 -file2
-rw-r-- 1 root bandit5 7836 Sep 1 06:30 .file2
-rwxr-x-- 1 root bandit5 7378 Sep 1 06:30 -file3
-rwxr-x-- 1 root bandit5 4802 Sep 1 06:30 .file3
-rwxr-x-- 1 root bandit5 6118 Sep 1 06:30 spaces file1
-rw-r-- 1 root bandit5 6850 Sep 1 06:30 spaces file2
-rwxr-x-- 1 root bandit5 1915 Sep 1 06:30 spaces file3
bandit5@bandit:~/inhere$ du -b -a | grep 1033
inhere$: command not found
bandit5@bandit:~/inhere$ file */{.,}* | grep "ASCII text" | grep -v ', with very long lines'
maybehere10/.file2: ASCII text
maybehere15/.file2: ASCII text
maybehere01/-file2: ASCII text
maybehere08/spaces file1: ASCII text
maybehere12/-file2: ASCII text
maybehere15/spaces file2: ASCII text
maybehere18/-file2: ASCII text
bandit5@bandit:~/inhere$

```

- 10.
11. file */{.,}* | grep "ASCII text" | grep -v ', with very long lines' displays all ASCII Text

***For The Remainder of The This
Exercise***

I Will Scale Down The Detail

The
College
of Saint
Rose

The College of Saint Rose

ETHICAL HACKING REPORT
ASSIGNMENT # 1 BANDIT 6

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 5 to 6, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is hidden in the "inhere" Directory. The `ls -a` and `-ls` command finds hidden files and tree folder structure, and the `cat` can read a file. Once the file is discovered, the file can be read. The `grep` command. The `find` and the flags with it like `-type` and `f` for file size.

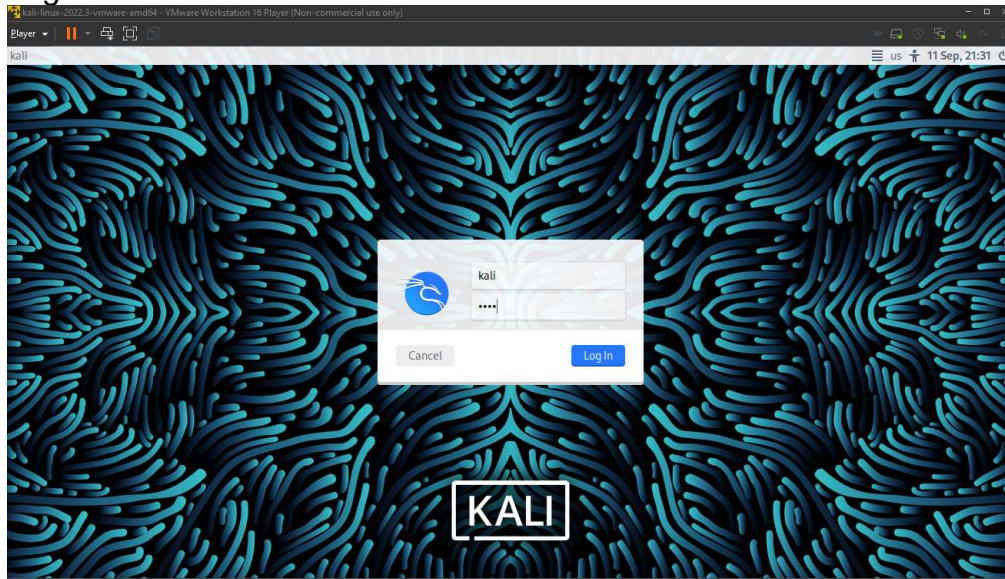
Tools

- The tools needed will be a VM running a Linux distro (Kali).
- A terminal prompt.
- The Website <https://overthewire.org/wargames/bandit/bandit6.html>
- The following Linux commands `ls` - list files `ls -a` list all files including hidden files, `cd` (change directory), `copy`, `paste`, `find`, `cat` or `read`, `grep`, and pipes.
- <https://mayadevbe.me/posts/overthewire/bandit/level6/>

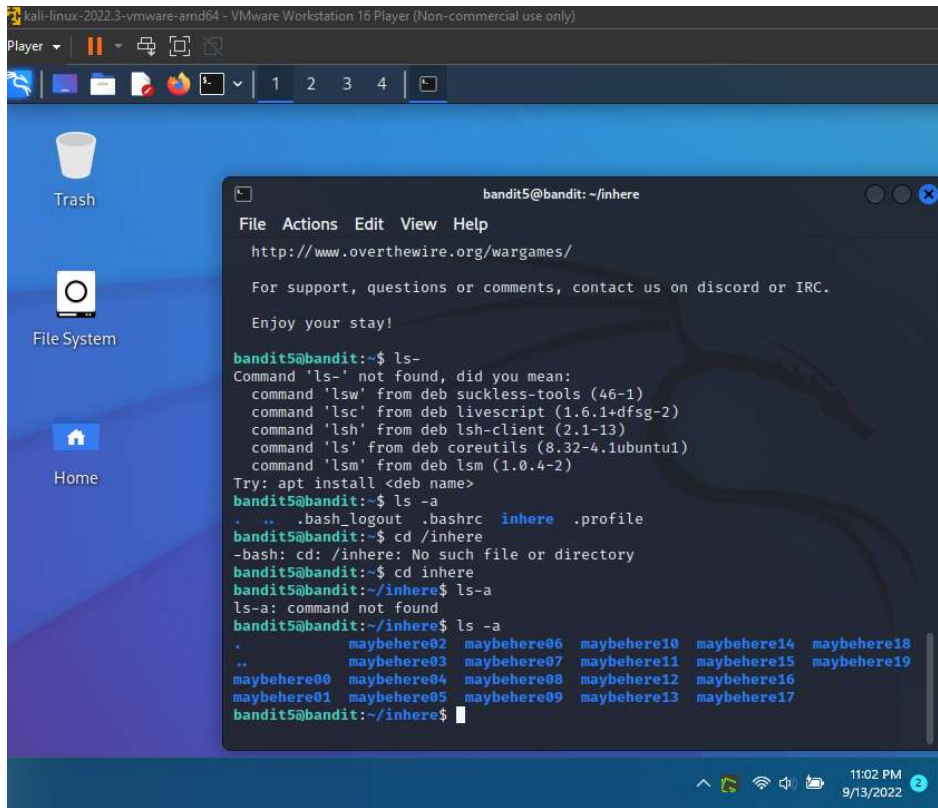
Methodology

Results

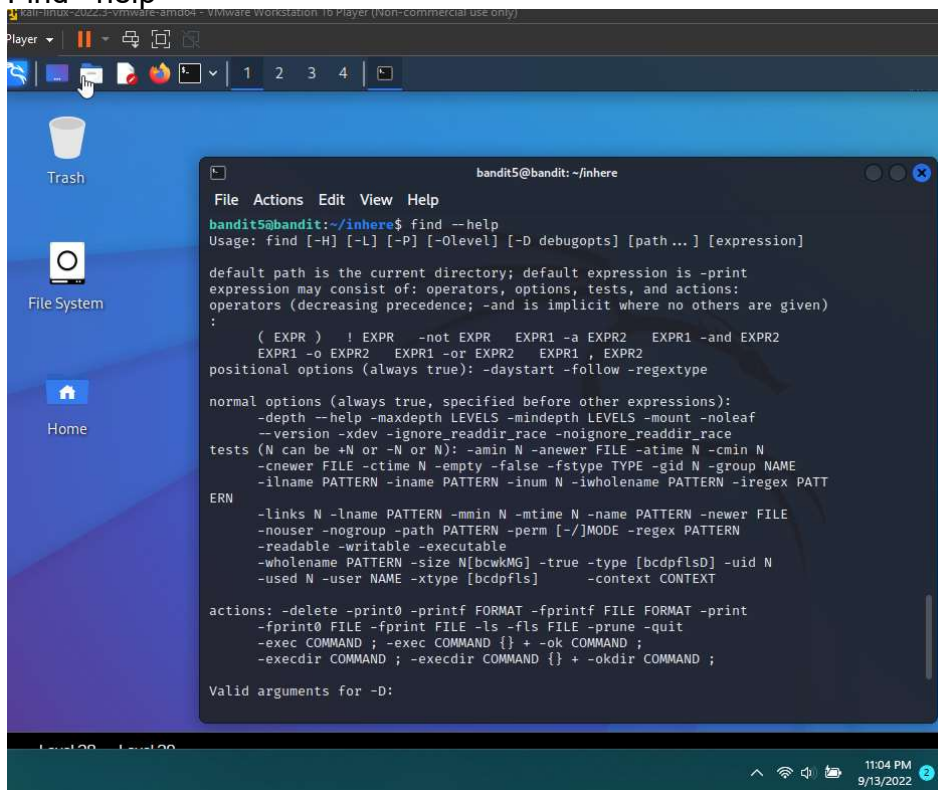
1. Log into the VM as kali/kali



- 2.
3. Bandit5 password `lrlWWl6bB37kxfiCQZqUdOIYfr6eEeqR`
4. `Ls -a` displays hidden files



- 5.
6. Find --help



- 7.

```

kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4

Trash
File System
Home

bandit5@bandit: ~/inhere
File Actions Edit View Help
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh03
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh04
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh05
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh06
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh07
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh08
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh09
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh10
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh11
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh12
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh13
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh14
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh15
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh16
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh17
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh18
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh19
bandit5@bandit:~/inhere$ ls -la maybeh00
total 72
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 .
drwxr-xr-x 22 root bandit5 4096 Sep 1 06:30 ..
-rwxr-xr-x 1 root bandit5 1039 Sep 1 06:30 -file1
-rwxr-xr-x 1 root bandit5 551 Sep 1 06:30 .file1
-rw-r--r-- 1 root bandit5 9388 Sep 1 06:30 -file2
-rw-r--r-- 1 root bandit5 7836 Sep 1 06:30 .file2
-rwxr-xr-x 1 root bandit5 7378 Sep 1 06:30 -file3
-rwxr-xr-x 1 root bandit5 4802 Sep 1 06:30 .file3
-rwxr-xr-x 1 root bandit5 6118 Sep 1 06:30 spaces file1
-rw-r--r-- 1 root bandit5 6850 Sep 1 06:30 spaces file2
-rwxr-xr-x 1 root bandit5 1915 Sep 1 06:30 spaces file3
bandit5@bandit:~/inhere$
11:13 PM
9/13/2022

```

- 8.
9. Ls -la displays folder structure within trees.

```

kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4

Trash
File System
Home

bandit5@bandit: ~/inhere
File Actions Edit View Help
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh14
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh15
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh16
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh17
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh18
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 maybeh19
bandit5@bandit:~/inhere$ ls -la maybeh00
total 72
drwxr-xr-x 2 root bandit5 4096 Sep 1 06:30 .
drwxr-xr-x 22 root bandit5 4096 Sep 1 06:30 ..
-rwxr-xr-x 1 root bandit5 1039 Sep 1 06:30 -file1
-rwxr-xr-x 1 root bandit5 551 Sep 1 06:30 .file1
-rw-r--r-- 1 root bandit5 9388 Sep 1 06:30 -file2
-rw-r--r-- 1 root bandit5 7836 Sep 1 06:30 .file2
-rwxr-xr-x 1 root bandit5 7378 Sep 1 06:30 -file3
-rwxr-xr-x 1 root bandit5 4802 Sep 1 06:30 .file3
-rwxr-xr-x 1 root bandit5 6118 Sep 1 06:30 spaces file1
-rw-r--r-- 1 root bandit5 6850 Sep 1 06:30 spaces file2
-rwxr-xr-x 1 root bandit5 1915 Sep 1 06:30 spaces file3
bandit5@bandit:~/inhere$ du -b -a | grep 1033
inhere$: command not found
bandit5@bandit:~/inhere$ file */{.,}* | grep "ASCII text" | grep -v ', with very long lines'
maybeh10/.file2: ASCII text
maybeh15/.file2: ASCII text
maybeh01/-file2: ASCII text
maybeh08/spaces file1: ASCII text
maybeh12/-file2: ASCII text
maybeh15/spaces file2: ASCII text
maybeh18/-file2: ASCII text
bandit5@bandit:~/inhere$

```

- 10.
11. file */{.,}* | grep "ASCII text" | grep -v ', with very long lines' displays all ASCII Text

The College of Saint Rose

ETHICAL HACKING REPORT
ASSIGNMENT # 1 BANDIT 7

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 6 to 7, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is hidden Somewhere in the Linux system. The end user will have to discover where. The `ls -a` and `-ls` command finds hidden files and tree folder structure, and the `cat` can read a file. Once the file is discovered, the file can be read. The `grep` command: the `find` and the flags like `-type` and `f` for file size.

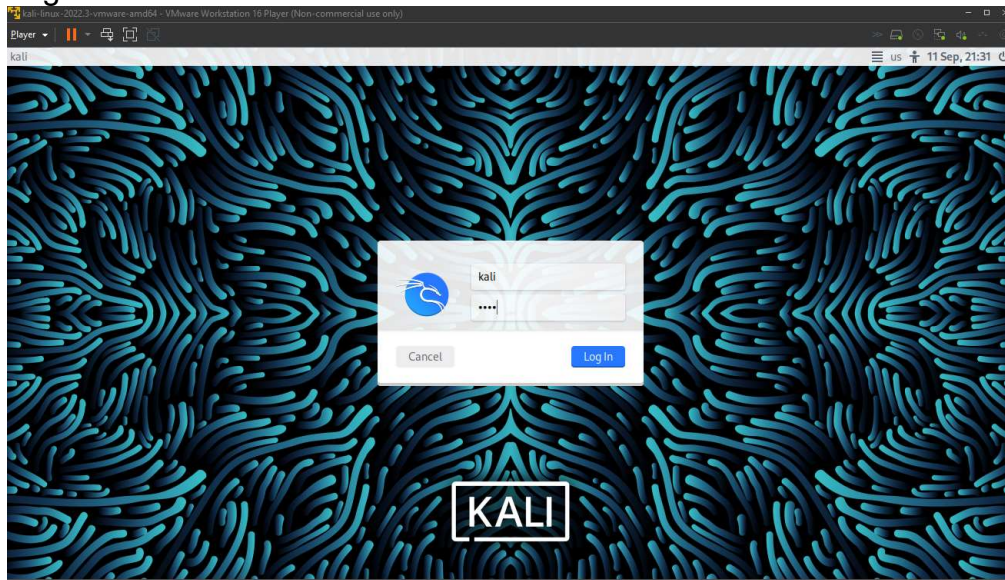
Tools

- The tools needed will be a VM running a Linux distro (Kali).
- A terminal prompt.
- The Website <https://overthewire.org/wargames/bandit/bandit7.html>
- The following Linux commands `ls` - list files `ls -a`, `ls la`, list all files including hidden files, `cd` (change directory), `copy`, `paste`, `find`, `cat` or `read`, `grep`, and `pipes`.
- <https://unix.stackexchange.com/questions/549861/i-want-to-learn-how-to-find-a-file-that-has-the-following-properties-owned-by-a>

Methodology

Results

1. Log into the VM as kali/kali



- 2.
3. Bandit 6 password P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU

```
bandit6@bandit: ~  
File Actions Edit View Help  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit6@bandit:~$
```

4.

```
bandit6@bandit: ~  
File Actions Edit View Help  
bandit6@bandit:~$ ls -a  
. .bash_logout .bashrc .profile  
bandit6@bandit:~$ cat .profile  
# ~/.profile: executed by the command interpreter for login shells.  
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login  
# exists.  
# see /usr/share/doc/bash/examples/startup-files for examples.  
# the files are located in the bash-doc package.  
  
# the default umask is set in /etc/profile; for setting the umask  
# for ssh logins, install and configure the libpam-umask package.  
#umask 022  
  
# if running bash  
if [ -n "$BASH_VERSION" ]; then  
    # include .bashrc if it exists  
    if [ -f "$HOME/.bashrc" ]; then  
        . "$HOME/.bashrc"  
    fi  
fi  
  
# set PATH so it includes user's private bin if it exists  
if [ -d "$HOME/bin" ] ; then  
    PATH="$HOME/bin:$PATH"  
fi  
  
# set PATH so it includes user's private bin if it exists  
if [ -d "$HOME/.local/bin" ] ; then  
    PATH="$HOME/.local/bin:$PATH"  
fi  
bandit6@bandit:~$
```

5.

6. Ls -a cat .profile see info

```
bandit6@bandit: /home
File Actions Edit View Help
Try 'su --help' for more information.
bandit6@bandit:/home$ su -u bandit7
Try 'su --help' for more information.
bandit6@bandit:/home$ su --help

Usage:
  su [options] [-] [<user> [<argument> ... ]]

Change the effective user ID and group ID to that of <user>.
A mere - implies -l. If <user> is not given, root is assumed.

Options:
  -m, -p, --preserve-environment      do not reset environment variables
  -w, --whitelist-environment <list>  don't reset specified variables

  -g, --group <group>                 specify the primary group
  -G, --supp-group <group>            specify a supplemental group

  -, -l, --login                       make the shell a login shell
  -c, --command <command>             pass a single command to the shell with -c
  --session-command <command>         pass a single command to the shell with -c
                                      and do not create a new session
  -f, --fast                           pass -f to the shell (for csh or tcsh)
  -s, --shell <shell>                 run <shell> if /etc/shells allows it
  -P, --pty                             create a new pseudo-terminal

  -h, --help                           display this help
  -V, --version                         display version

For more details see su(1).
bandit6@bandit:/home$
```

- 7.
8. Su -help cd .. into home dir

```

bandit6@bandit: /home/bandit7
File Actions Edit View Help
drwxr-xr-x 2 root root 4096 Sep 1 06:30 krypton2
drwxr-xr-x 2 root root 4096 Sep 1 06:30 krypton3
drwxr-xr-x 2 root root 4096 Sep 1 06:30 krypton4
drwxr-xr-x 2 root root 4096 Sep 1 06:30 krypton5
drwxr-xr-x 2 root root 4096 Sep 1 06:30 krypton6
drwxr-xr-x 2 root root 4096 Sep 1 06:30 krypton7
drwxr-x 3 ubuntu ubuntu 4096 Sep 1 06:32 ubuntu
bandit6@bandit:/home$ cd bandit 7
-bash: cd: too many arguments
bandit6@bandit:/home$ cd bandit7
bandit6@bandit:/home/bandit7$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit6@bandit:/home/bandit7$ cat data.txt
cat: data.txt: Permission denied
bandit6@bandit:/home/bandit7$ cat .profile
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi

```

9.

```

bandit6@bandit: /home
File Actions Edit View Help
-bash: cd: bandit7: No such file or directory
bandit6@bandit:~$ cd ..
bandit6@bandit:/home$ ls
bandit0 bandit15 bandit21 bandit27-git bandit30-git bandit6 krypton4
bandit1 bandit16 bandit22 bandit28 bandit31 bandit7 krypton5
bandit10 bandit17 bandit23 bandit28-git bandit31-git bandit8 krypton6
bandit11 bandit18 bandit24 bandit29 bandit32 bandit9 krypton7
bandit12 bandit19 bandit25 bandit29-git bandit33 krypton1 ubuntu
bandit13 bandit2 bandit26 bandit3 bandit4 krypton2
bandit14 bandit20 bandit27 bandit30 bandit5 krypton3
bandit6@bandit:/home$ cd bandit7
bandit6@bandit:/home/bandit7$ ls -ls
total 4088
4088 -rw-r----- 1 bandit8 bandit7 4184396 Sep 1 06:30 data.txt
bandit6@bandit:/home/bandit7$ ls
data.txt
bandit6@bandit:/home/bandit7$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit6@bandit:/home/bandit7$ ls -la
total 4108
drwxr-xr-x 2 root root 4096 Sep 1 06:30 .
drwxr-xr-x 49 root root 4096 Sep 1 06:30 ..
-rw-r--r-- 1 root root 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 root root 3771 Jan 6 2022 .bashrc
-rw-r----- 1 bandit8 bandit7 4184396 Sep 1 06:30 data.txt
-rw-r--r-- 1 root root 807 Jan 6 2022 .profile
bandit6@bandit:/home/bandit7$ cd
bandit6@bandit:~$
bandit6@bandit:~$ find -size 33c
bandit6@bandit:~$ find dir size 33c -user bandit7 -group bandit6
find: 'dir': No such file or directory

```

10.

```
bandit6@bandit: /home
File Actions Edit View Help
cd..: command not found
bandit6@bandit:~$ cd /home
bandit6@bandit:/home$ find dir size 33c -user bandit7 -group bandit6
find: 'dir': No such file or directory
find: 'size': No such file or directory
find: '33c': No such file or directory
bandit6@bandit:/home$ ls
bandit0  bandit15  bandit21  bandit27-git  bandit30-git  bandit6  krypton4
bandit1  bandit16  bandit22  bandit28      bandit31      bandit7  krypton5
bandit10 bandit17  bandit23  bandit28-git  bandit31-git  bandit8  krypton6
bandit11 bandit18  bandit24  bandit29      bandit32      bandit9  krypton7
bandit12 bandit19  bandit25  bandit29-git  bandit33      krypton1  ubuntu
bandit13 bandit2   bandit26  bandit3       bandit4       krypton2
bandit14 bandit20  bandit27  bandit30      bandit5       krypton3
bandit6@bandit:/home$ cd
bandit6@bandit:~$ find . -size 33c -user bandit7 -group bandit6 | grep bandit7
bandit6@bandit:~$ find . -size 33c -user bandit7 -group bandit6
bandit6@bandit:~$ find . -size 33c -user bandit7 -group bandit6 | grep bandit7
bandit6@bandit:~$ find . -size 33c
bandit6@bandit:~$ ls -la
.  ..  .bash_logout  .bashrc  .profile
bandit6@bandit:~$ cd /home
bandit6@bandit:/home$ find . -size 33c -user bandit7 -group bandit6 | grep bandit7
find: './bandit30-git': Permission denied
find: './bandit31-git': Permission denied
find: './bandit5/inhere': Permission denied
find: './ubuntu': Permission denied
find: './bandit29-git': Permission denied
find: './bandit28-git': Permission denied
find: './bandit27-git': Permission denied
bandit6@bandit:/home$
```

11.

```
bandit6@bandit: /
File Actions Edit View Help
find: './var/tmp/systemd-private-ccfbf79c344f41d0a9f2937ce69e656d-chrony.service-910mWV': Permission denied
find: './var/tmp/systemd-private-ccfbf79c344f41d0a9f2937ce69e656d-systemd-logind.service-5xJ28Z': Permission denied
find: './var/tmp/systemd-private-ccfbf79c344f41d0a9f2937ce69e656d-systemd-resolved.service-vnareK': Permission denied
find: './var/tmp/systemd-private-ccfbf79c344f41d0a9f2937ce69e656d-ModemManager.service-zboij0': Permission denied
find: './var/snap/lxd/common/lxd': Permission denied
find: './var/lib/amazon': Permission denied
find: './var/lib/chrony': Permission denied
find: './var/lib/private': Permission denied
find: './var/lib/udisks2': Permission denied
find: './var/lib/snapd/void': Permission denied
find: './var/lib/snapd/cookie': Permission denied
find: './var/lib/ubuntu-advantage/private': Permission denied
find: './var/lib/update-notifier/package-data-downloads/partial': Permission denied
find: './var/lib/apt/lists/partial': Permission denied
./var/lib/dpkg/info/bandit7.password
find: './var/lib/polkit-1': Permission denied
find: './var/cache/pollinate': Permission denied
find: './var/cache/private': Permission denied
find: './var/cache/ldconfig': Permission denied
find: './var/cache/apt/archives/partial': Permission denied
find: './var/cache/apparmor/c47eabf7.0': Permission denied
find: './var/cache/apparmor/e10c1cf9.0': Permission denied
find: './var/log/amazon': Permission denied
find: './var/log/chrony': Permission denied
find: './var/log/private': Permission denied
find: './var/log/unattended-upgrades': Permission denied
find: './var/spool/cron/crontabs': Permission denied
```

12.

13. Target shows up in RED

```
bandit6@bandit: /
File Actions Edit View Help
find: './snap/core20/1587/etc/ssl/private': Permission denied
find: './snap/core20/1587/root': Permission denied
find: './snap/core20/1587/var/cache/ldconfig': Permission denied
find: './snap/core20/1587/var/cache/private': Permission denied
find: './snap/core20/1587/var/lib/private': Permission denied
find: './snap/core20/1587/var/lib/snapd/void': Permission denied
find: './snap/core18/2538/etc/ssl/private': Permission denied
find: './snap/core18/2538/root': Permission denied
find: './snap/core18/2538/var/cache/ldconfig': Permission denied
find: './snap/core18/2538/var/lib/private': Permission denied
find: './dev/shm/eic-hostkey-HGyneaQ4': Permission denied
find: './sys/kernel/tracing': Permission denied
find: './sys/kernel/debug': Permission denied
find: './sys/fs/pstore': Permission denied
find: './sys/fs/bpf': Permission denied
find: './home/bandit30-git': Permission denied
find: './home/bandit31-git': Permission denied
find: './home/bandit5/inhere': Permission denied
find: './home/ubuntu': Permission denied
find: './home/bandit29-git': Permission denied
find: './home/bandit28-git': Permission denied
find: './home/bandit27-git': Permission denied
find: './etc/sudoers.d': Permission denied
find: './etc/multipath': Permission denied
find: './etc/ssl/private': Permission denied
find: './etc/polkit-1/localauthority': Permission denied
find: './root': Permission denied
find: './lost+found': Permission denied
bandit6@bandit:/$ cat ./var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:/$
```

- 14.
15. Bandit 7 Password z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

The College of Saint Rose

ETHICAL HACKING REPORT
ASSIGNMENT # 1 BANDIT 8

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 7 to 8, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is a hidden millionth string file on the Linux system. The end user will have to discover where. The file is on the main directory; a command finds hidden files, and tree folder structure, A Pipe with strings file name pipe grep and the flag will solve the assignment. Once the file is discovered, the file and filter out the word millionth and will be able to read the password.

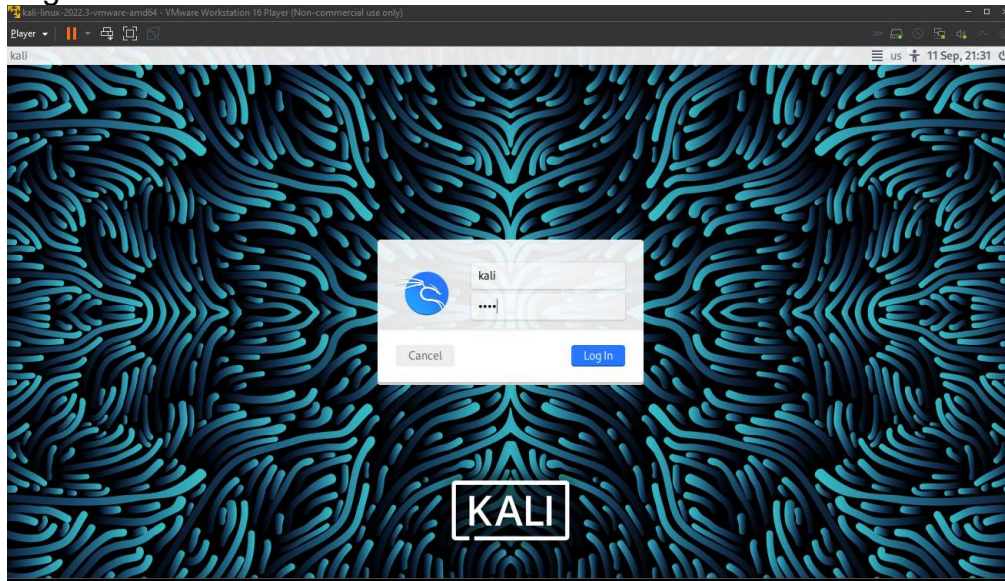
Tools

- The tools needed will be a VM running a Linux distro (Kali).
- A terminal prompt.
- The Website <https://overthewire.org/wargames/bandit/bandit8.html>
- The following Linux commands `ls` - list files `ls -a`, `ls la`, list all files including hidden files, `cd` (change directory), `copy`, `paste`, `find`, `cat` or `read`, `grep`, and pipes and `String`.

Methodology

Results

1. Log into the VM as kali/kali



- 2.
3. Bandit 7 Password z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

```
bandit7@bandit: ~  
File Actions Edit View Help  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit7@bandit:~$
```

4.

```
bandit7@bandit: ~  
File Actions Edit View Help  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit7@bandit:~$ ls -la  
.. .bash_logout .bashrc data.txt .profile  
bandit7@bandit:~$ grep data.txt  
^Z  
[1]+  Stopped                  grep --color=auto data.txt  
bandit7@bandit:~$ strings data.tt  
strings: 'data.tt': No such file  
bandit7@bandit:~$ strings data.txt  
Weddell's      o8S2mUy0lnSjvej8IIC3Jd8qBM7jLYeL  
sucks          SVP9VgB4uSJKMejmdRC2u20NI4tLC9JH  
genders        11EjE7xEf0vjvMOXDFpUucGXgU706iKX  
Vagrants       h7Wb2ZHWx9Tt6LsJIQn5IyH2A3CkcZFc  
shrewed        oEl7VCrKajDdbXvJrW9IVULk2KA0GPZs  
imbecile's     P7nHwuVBuWnFTXpVSpjWFlmJASMOUnA  
reexamining    VQbmDcurUPB9koHHeCRugBvBpMpM6V0c  
emailed        85cYMCVUneJDwT5prLCLmLkT1rhqKZgj  
barometers     3wKwiJ7YhZdpjypR09kfQNmJjp66to8d  
Ephesian       6KvOfHGIHnvWIwQruJXPQFhA1Plheicd  
clenches       CiuAA1kjn7B1weFUVLF4LymAL0jyz9kQ  
conversions    nANUGj5JxCj41S2BUvisuKPrkwTvrjaX  
Pascal         1MDxYnN6duIhcZozab1nxyqVqVPF5mBZ  
harsh          alHbyGmx6XvIo5Q0u4tuCNCbANvoBeEL  
freckle's      Ryg54bbPSuCmt3r9UPMPn9joACqD1TPv
```

5.

```
bandit7@bandit: ~  
File Actions Edit View Help  
--exclude-dir=GLOB      skip directories that match GLOB  
-L, --files-without-match  print only names of FILES with no selected lines  
-l, --files-with-matches  print only names of FILES with selected lines  
-c, --count              print only a count of selected lines per FILE  
-T, --initial-tab        make tabs line up (if needed)  
-Z, --null                print 0 byte after FILE name  
  
Context control:  
-B, --before-context=NUM  print NUM lines of leading context  
-A, --after-context=NUM   print NUM lines of trailing context  
-C, --context=NUM         print NUM lines of output context  
-NUM                      same as --context=NUM  
--group-separator=SEP     print SEP on line between matches with context  
--no-group-separator      do not print separator for matches with context  
--color[=WHEN],           use markers to highlight the matching strings;  
--colour[=WHEN]           WHEN is 'always', 'never', or 'auto'  
-U, --binary              do not strip CR characters at EOL (MSDOS/Windows)  
  
When FILE is '-', read standard input. With no FILE, read '.' if  
recursive, '-' otherwise. With fewer than two FILES, assume -h.  
Exit status is 0 if any line is selected, 1 otherwise;  
if any error occurs and -q is not given, the exit status is 2.  
  
Report bugs to: bug-grep@gnu.org  
GNU grep home page: <https://www.gnu.org/software/grep/>  
General help using GNU software: <https://www.gnu.org/gethelp/>  
bandit7@bandit:~$ strings data.txt | grep data.txt  
bandit7@bandit:~$ strings data.txt | grep -w millionth  
millionth      TESKZC0XvTetK0S9xNwm25STk5iWrBvP  
bandit7@bandit:~$
```

- 6.
7. – help gave the solution
8. Password for millionth TESKZC0XvTetK0S9xNwm25STk5iWrBvP

```
bandit8@bandit: ~  
File Actions Edit View Help  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit8@bandit:~$
```

- 9.

The College of Saint Rose

ETHICAL HACKING REPORT
ASSIGNMENT # 1 BANDIT 9

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

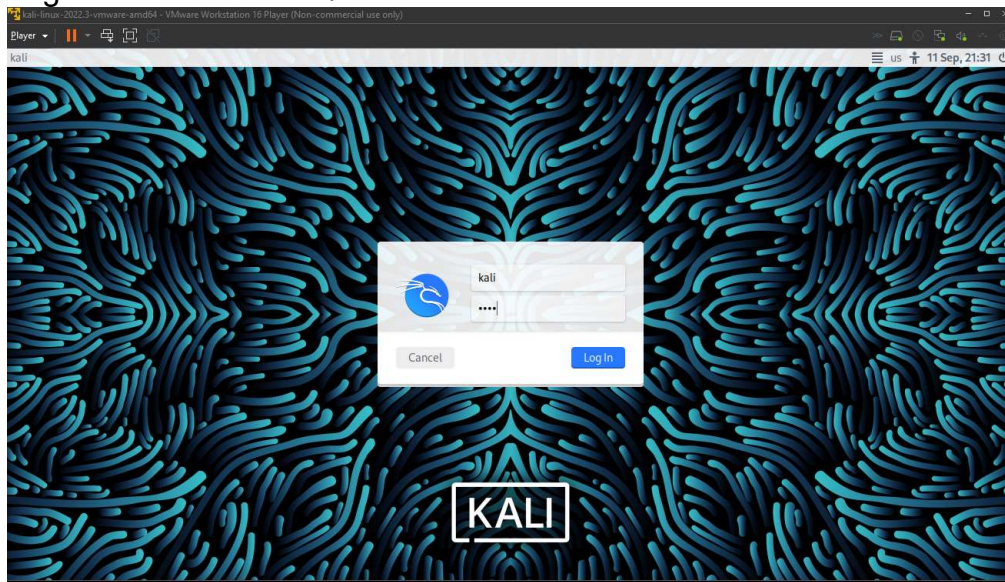
The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 7 to 8, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is located in the data.txt. The user will have to use sort and uniq with pipes to be able to solve the assignment.

- The tools needed will be a VM running a Linux distro (Kali).
- A terminal prompt.
- The Website <https://overthewire.org/wargames/bandit/bandit9.html>
- The following Linux commands ls - list files ls -a, ls la, list all files including hidden files, cd (change directory), copy, paste, uniq, sort -flags.

Methodology

Results

1. Log into the VM as kali/kali



- 2.
3. Bandit 8 Password TESKZC0XvTetK0S9xNwm25STk5iWrBvP

```
bandit8@bandit: ~  
File Actions Edit View Help  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit8@bandit:~$
```

4.

```
bandit8@bandit: ~  
File Actions Edit View Help  
  
With no options, matching lines are merged to the first occurrence.  
  
Mandatory arguments to long options are mandatory for short options too.  
-c, --count          prefix lines by the number of occurrences  
-d, --repeated       only print duplicate lines, one for each group  
-D                  print all duplicate lines  
    --all-repeated[=METHOD] like -D, but allow separating groups  
                           with an empty line;  
                           METHOD={none(default),prepend,separate}  
-f, --skip-fields=N  avoid comparing the first N fields  
    --group[=METHOD] show all items, separating groups with an empty line;  
                           METHOD={separate(default),prepend,append,both}  
-i, --ignore-case    ignore differences in case when comparing  
-s, --skip-chars=N   avoid comparing the first N characters  
-u, --unique         only print unique lines  
-z, --zero-terminated line delimiter is NUL, not newline  
-w, --check-chars=N  compare no more than N characters in lines  
    --help          display this help and exit  
    --version       output version information and exit  
  
A field is a run of blanks (usually spaces and/or TABs), then non-blank  
characters. Fields are skipped before chars.  
  
Note: 'uniq' does not detect repeated lines unless they are adjacent.  
You may want to sort the input first, or use 'sort -u' without 'uniq'.  
  
GNU coreutils online help: <https://www.gnu.org/software/coreutils/>  
Full documentation <https://www.gnu.org/software/coreutils/uniq>  
or available locally via: info '(coreutils) uniq invocation'  
bandit8@bandit:~$
```

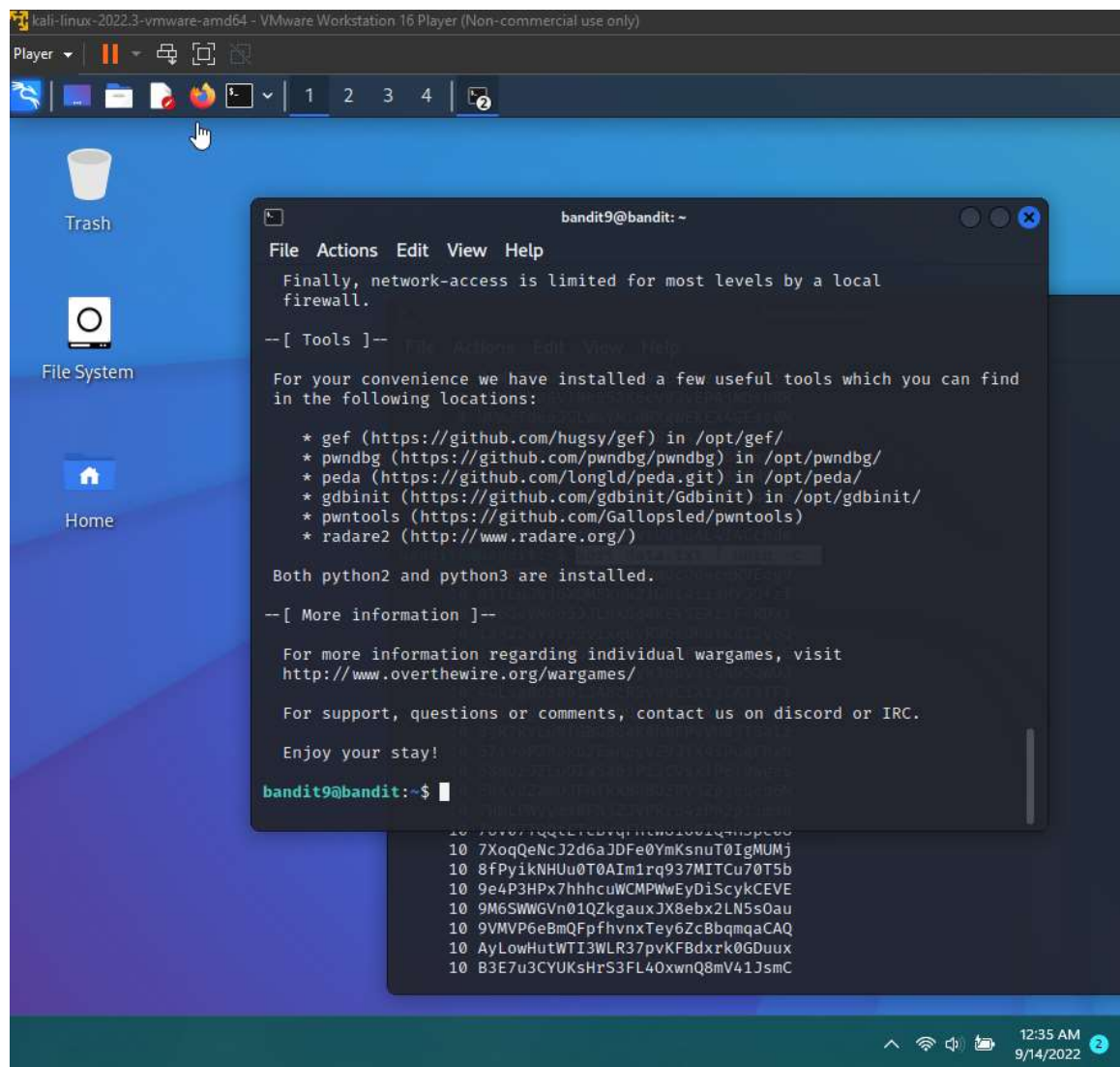
5.

```
bandit8@bandit: ~  
File Actions Edit View Help  
bIGx2gTFaRwyjxyqnsraNKXd8t93eK2D  
4n11vgXcs3wdgdbQjbb6JF4kR2vNUVOK  
h44iM4fCazdJGLR3i4QGaSR6FtyGmd4Q  
9M6SWWGVn01QZkgauxJX8ebx2LN5s0au  
Owei9FwGx3FOhhyCOHQbX88R9mo4wvXI  
MZ6EFg1Kr8ohSuz0itIWofR5k2koEvN6  
mzCnXrbqm8QdgjRP1A12isJwyCZ0uTJn  
i6t6LYg1JArHP57SS8532uSDt6HRA9Ln  
Z8ncb64yvxMpYu6kyuRadwjouYpkMLPN  
f0hFsyegU2D3zLrex0WI90sw2DlNYIlj  
ryM64LqAra2XBhstdzbLWFUS26Xa9o6C  
wn85LAbx5wkDs0IfvPbI1dSUSgY16QmL  
6hXvdZamDJFnfKX808UZPVjZpjeqeq6M  
DHMhiE3MDZYEncOWimJaGxkVfAejqL1c  
AyLowHutWTI3WLR37pvKFBdxrk0GDuux  
jBN1cLA8VHLIWyD7rsgIWULYyDvnMoyA  
vCV4xQA9BY6D78vlljAq3SEFy7mGeLJd  
tnhOGCM27V5AoOmFLWhsZM1EFc8DZe3x  
QrMLTTEu3KGuydS2w9FLTLZuRldf6f6  
oUHk3VaGVlNeB52K6cV03vEPAjMDshRR  
UPmZTd6oJGLWmYm1dRXgWEKEX4GES10M  
7HNLWPyymSBFNjZJVPRro4zPh2p1imsN  
68qUzJZLu0Iw5a6iPi2CVsxlP6l0wgaS  
TuYdzYVx3Z5ue4jRaOqX301qf8Y1M97I  
RpOwFRgvra5Z0obMMG0FzLaJLN0Uq8IS  
HqxUEnCqSABq86q6oEXA0cTCRkdXaRGB  
XCAk2n2alytIxQABvtUujqAL4I4Cchdm  
6hXvdZamDJFnfKX808UZPVjZpjeqeq6M  
bandit8@bandit:~$ sort -c data.txt  
sort: data.txt:2: disorder: 6hXvdZamDJFnfKX808UZPVjZpjeqeq6M  
bandit8@bandit:~$
```

- 6.
7. That was not the correct data

```
bandit8@bandit: ~  
File Actions Edit View Help  
10 6hXvdZamDJFnfKX808UZPVjZpjeqeq6M  
10 7HNLWPyymSBFNjZJVPRro4zPh2p1imsN  
10 7oV07TQQtETcBvqFHTw81o0IQ4H3pc08  
10 7XoQqNeNcJ2d6aJDFe0YmKsnuT0IgMUMj  
10 8fPyikNHUu0T0AIm1rq937MITCu70T5b  
10 9e4P3HPx7hhhcuWCMPPWwEyDiScykCEVE  
10 9M6SWWGVn01QZkgauxJX8ebx2LN5s0au  
10 9VMVP6eBmQFpfhvnXtEy6ZcBbmqqaCAQ  
10 AyLowHutWTI3WLR37pvKFBdxrk0GDuux  
10 B3E7u3CYUKsHrS3FL40xwnQ8mV41JsmC  
10 B4ZsFwBy6o26IaTRDiLVeXrmS6yai0N  
10 bDwxYKyKRyCCg1bVbTuqM0mA5mqBPgXd  
10 bEua052cW0y20ToRoJSMvoadKgbPcbjN  
10 bIGx2gTFaRwyjxyqnsraNKXd8t93eK2D  
10 boosqStx1lFFEEaMoGP6BS78Bw7Fh2xR  
10 DD2JRDeH9vptLOX9jQozH8Moji1xAKl1C  
10 DfjpGIxPR7Q0Wbkxyf40kV1o1Jl0njs7  
10 dgypG7eRY1Dr5HW11ejvuhZvGCAmosTQ  
10 DHMhiE3MDZYEncOWimJaGxkVfAejqL1c  
10 dhoAlBlnhEz2xYyJdfI5ysm0JpyqDkQV  
10 distOgdG7obAspnU4rE1HsWJ2upkf6BK  
10 DItvE0rpT0pRGL1bFdRhoQkwX8SdlMYV  
1 EN632PlfYiZbn3PhVK3XOGSlnInNE00t  
10 Eor03gLDc3awKULF84XCnD8xgRg6X9S3  
10 F5wqfjqZqVuufXkocZswBcRuVjFMZD0t  
10 f0hFsyegU2D3zLrex0WI90sw2DlNYIlj  
10 fTS4yCSbaYvGtedvArozwbVt4QJZaY3V  
10 G0Fl2a0BxC5HkgtLFQ3wLOG8kdeFbimU  
10 g3hmmW8u72TrvlJGcH20Z1BUZUjyNEAP  
10 GI7mPrXWhEUMrVWHEXesGq1TrKix5wC  
10 GKe0anTFCdBKLTHTV6aZUXCiBM3Ilz1h
```

- 8.
9. EN632PlfYiZbn3PhVK3XOGSlnInNE00t only occurs once
10. sort data.txt | uniq -c was the command I used.



11.

The College of Saint Rose

ETHICAL HACKING REPORT
ASSIGNMENT # 1 BANDIT 10

JASON GIBSON

Gibsonj421@Strose.edu

Scope of the assignment

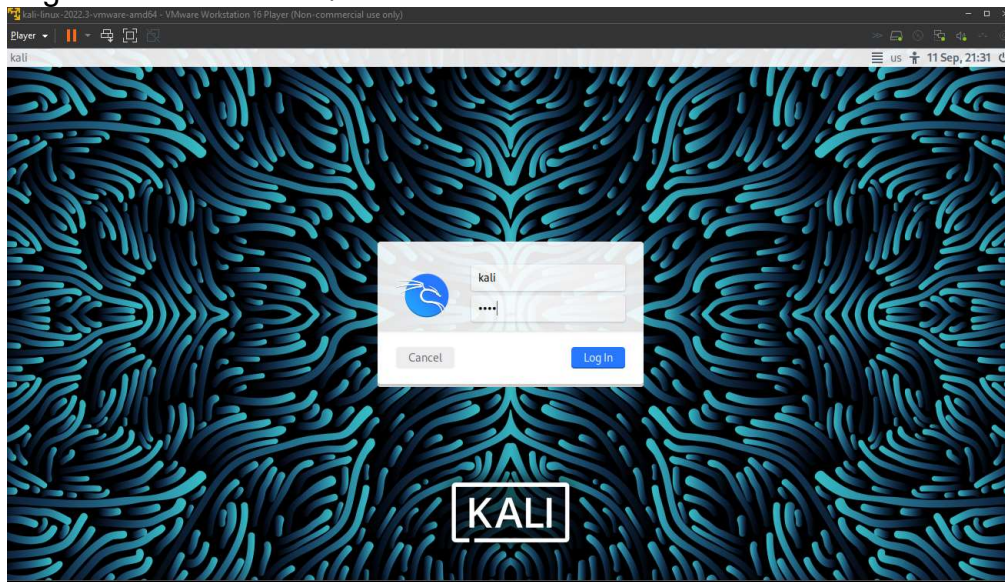
The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 9 to 10, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is located in the data.txt. The user will have to use sort and uniq with pipes to be able to solve the assignment.

- The tools needed will be a VM running a Linux distro (Kali).
- A terminal prompt.
- The Website <https://overthewire.org/wargames/bandit/bandit10.html>
- The following Linux commands ls - list files ls -a, ls la, list all files including hidden files, cd (change directory), copy, paste, uniq, sort -flags.

Methodology

Results

1. Log into the VM as kali/kali



2.

3. Bandit9 Password EN632PlfYiZbn3PhVK3XOGSLnNE00t

```
bandit9@bandit: ~  
File Actions Edit View Help  
firewall.  
--[ Tools ]--  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
Both python2 and python3 are installed.  
--[ More information ]--  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
For support, questions or comments, contact us on discord or IRC.  
Enjoy your stay!  
bandit9@bandit:~$  
bandit9@bandit:~$
```

```
bandit9@bandit: ~  
File Actions Edit View Help  
uniq: -: invalid number of bytes to compare  
bandit9@bandit:~$ uniq -u data.txt | grep -E \  
grep: invalid option -- '='  
Usage: grep [OPTION]... PATTERNS [FILE]...  
Try 'grep --help' for more information.  
bandit9@bandit:~$ grep -E \  
^C  
bandit9@bandit:~$ grep -E \= data.txt  
grep: data.txt: binary file matches  
bandit9@bandit:~$ uniq -u data.txt |  
^C  
bandit9@bandit:~$ grep -E \= data.txt |  
^C  
bandit9@bandit:~$ uniq -u data.txt | grep -E \  
grep: (standard input): binary file matches  
bandit9@bandit:~$ grep -E | uniq -u data.txt  
Usage: grep [OPTION]... PATTERNS [FILE]...  
Try 'grep --help' for more information.  
+f++R[S+;+1}Kf++L`a+W+d++E+;N+r=w++T#n!O+  
+dz+N)Cr9_mU0+w0M+H+n+e+++++!+1  
+?_jB*R_ex_++z!d2+m(K+r+=++3+jI  
++1+3+J+a+[[+3;++++,~k++R1+w+7 ++G++I+JY+x0G++bJm+:.].+z++F+)y+2%+  
+S+U+e++Z+++++U'+{+I~aF ++sL+G +d[L+t+q+.]++C=eDG++m+;+i+Y3u0+V+  
s+H#w+m+++++e+IP+Z+l++dV+++`Own+++ +1D!P+yX++K+=id6+S+1+FJ+ "-  
+pJP+D+O+XW+O+7+i++S++?jF+++f+m+g+no+++++.+SD++++J+++++e+e+r++++[ (V#;B  
+.+.KY+D2+  
S+hC  
10 DfjpGixPR7Q0Wbkxyf40kV1oLjL0njs7  
10 dgvpG7eRY1Dr5HW11ejvuhZvGCAmosTQ  
10 DHMhiE3MDZYEncOWimJaGxkvFAeqL1c  
10 dhoAl8lnhEz2xYyJdfI5ysm0JpyqDkQV  
10 distOgdG7obAspnU4rE1HsWJ2upkf6BK  
10 DItvE0rP0pRGL1bFdrHokQkwX8SdLMYV  
1 EN632PlfYiZbn3PhVK3XOGSLnNE00t  
10 Eor03gLDc3awKULF84XCnD8xgRg6X9S3
```

- 4.
- 5.
6. uniq: -: invalid number of bytes to compare

7. bandit9@bandit:~\$ uniq -u data.txt | grep -E\=
8. grep: invalid option -- '='
9. Usage: grep [OPTION]... PATTERNS [FILE]...
10. Try 'grep --help' for more information.
11. bandit9@bandit:~\$ grep -E \=
12. ^C
13. bandit9@bandit:~\$ grep -E \= data.txt
14. grep: data.txt: binary file matches
15. bandit9@bandit:~\$ uniq -u data.txt |
16. ^C
17. bandit9@bandit:~\$ grep -E \= data.txt |
18. ^C
19. bandit9@bandit:~\$ uniq -u data.txt | grep -E \=
20. grep: (standard input): binary file matches
21. bandit9@bandit:~\$ grep -E | uniq -u data.txt
22. Usage: grep [OPTION]... PATTERNS [FILE]...
- 23.

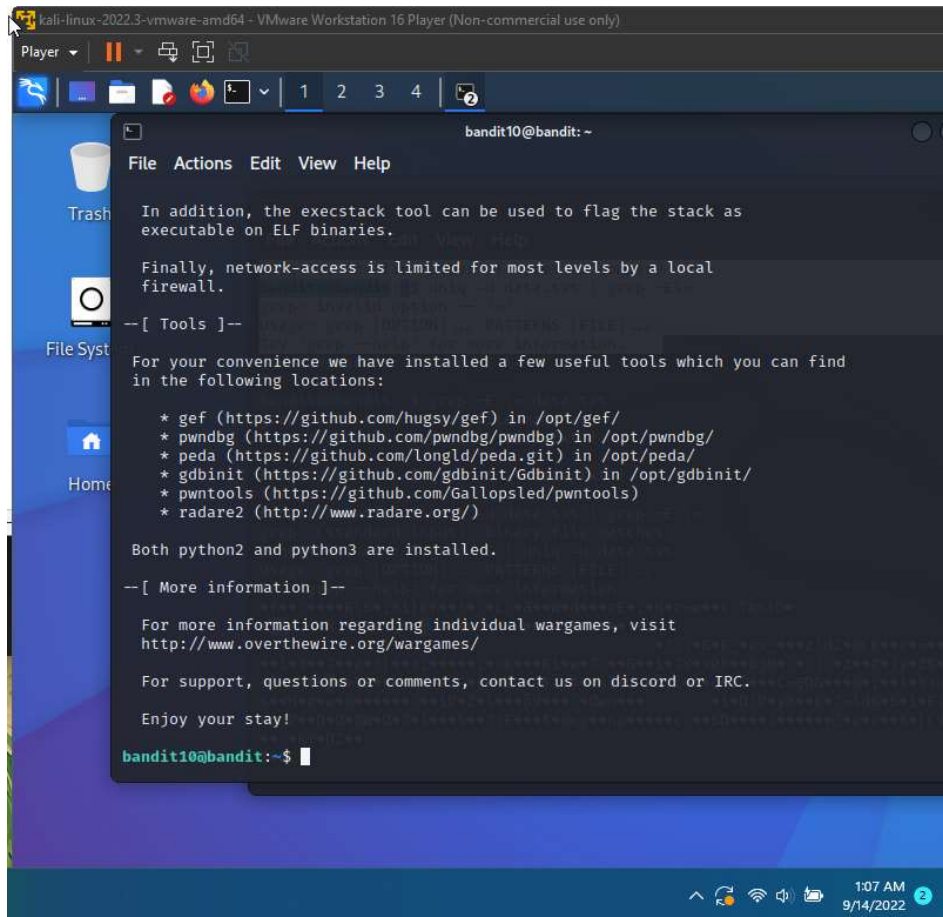
```

File Actions Edit View Help

^U+++++|+
8++++6R+;+7$++$z+++++d+
R]+++++5I+E+!++g+++++!++H$V'e++++<++++d++++
+ou+++3+++++p+/++I++++~+++2+Z+
>++++fP+s++#n)7~y+$++++i+$x1ZAig+((++=A7+bJ0+g++++7r+++GI++++"++t+Z++++0
A`zgA++x+++++>+]V-h++q{C+;+V++}+++O`+M+$IO++++:++Tw0++W0+
+l,+++8++Z+T+
++d+B+3c+uy^+A%X+w0^+|K;6[#+F3@yv+B++Y;h+
++r+
+++;,+U+}{+8+
F+Q+:+++++H++]+U+@o>+++++1++F+#++;/;+""++dEL!+:~j$++++
iG2@i+?
+}+-j/.++B+++F+++C++#+-`)+^+ka>++++z#F+0
/}f+++3+:26=E+++`+A+?+z: bXK+!6v++++M2+P+YA++++D+7++(++++Zo`6{+s++++b+b+`+++a
++++G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
+P++++c++C+R\;++++~2U++++Udi+7W=+/+-++Q+w+++++IA+[m+++
h++++0++++`6+[+=@+/
+Y+Q-++=Rt+++++GCF;+B+q+(++v
U+~UvGKf+++VQ+e+K++玻+++S+ÿ++/ll+(+<+r+l++++
+i+d+=1B3+-K%)+T\++3#>+Dj+++++s ?? :S+++H+a+
N++>"/+++
/+M%++)+T++wi+U++F+++++8+1Ns+9+<+F+M++r+(+++e++++;
+S*++M++[4(++{+++1\--+V++c"++f+++3+$B2Q+#+a1(++n+++w"++E++6+[+++4G+++++i+++,!+er+++j
+L++++P'+X+kp++a++++P7#o++++"h+}>+$@+?"++S+m++Uh+,+Gi++++{XS$=adZ++^+?<
+|++++>h++EW+++!-+7+++++C}'T
r+++/+DAR++4S++++=88+F+6+Xx+=9++++
10 DfjP6IxPR7Q0Wbkxyf40kV1o1Jl0njs7
10 dgvpG7eRY1Dr5HW11ejvuhZvGCAmosTQ
10 DHMhiE3MDZYEncOWimJaGxkVfAejqL1c
10 dhoAlBlnhEz2xYyJdfI5ysm0JpyqDkQV
10 distOgdG7obAspnU4rE1HsWJ2upkf6BK
10 DI tvEOrpT0pRGL1bFdRhoQkwX8SdlMYV
1 EN632PlfYiZbn3PhVK3XOGSLNInNE00t
10 Eor03gLdc3awKULF84XCnD8xgRg6X9S3

```

- 24.
25. Possible for bandit 10 G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s



- 26.
27. Success!
28. Very fun Exerercies.Thank You!