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 widows 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

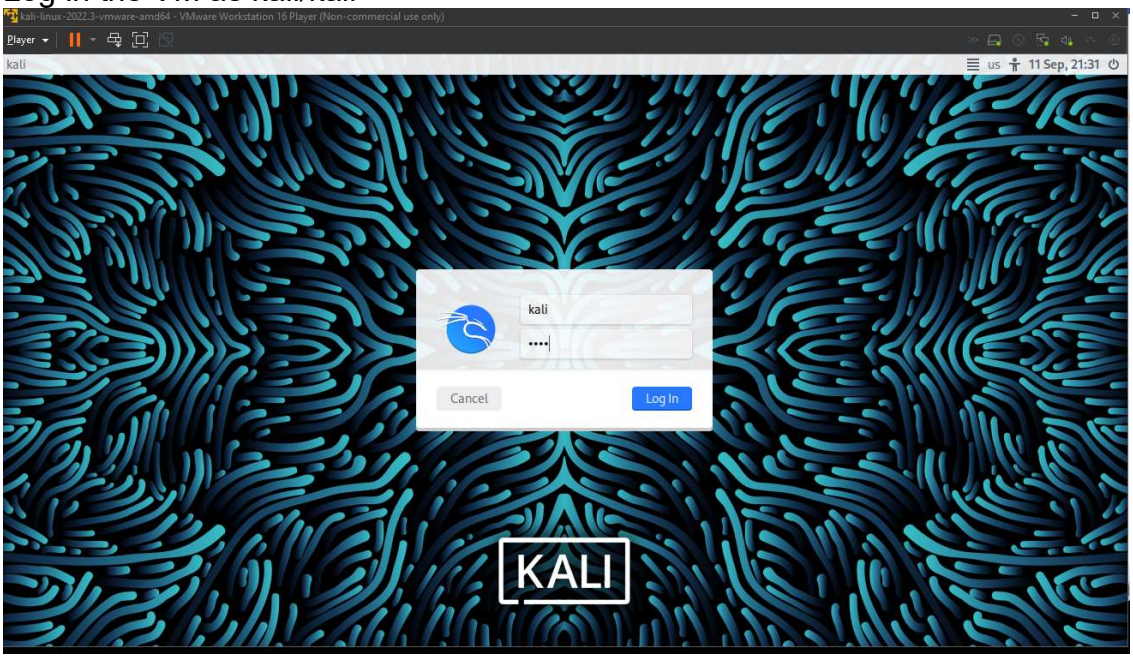
   What possible ports are open to new attacks, and what other users are available, bandit1? Or banidit2? Would a Radius attack affect the login attempt? What impact does it have on the organization if this website goes down?

7. Reporting

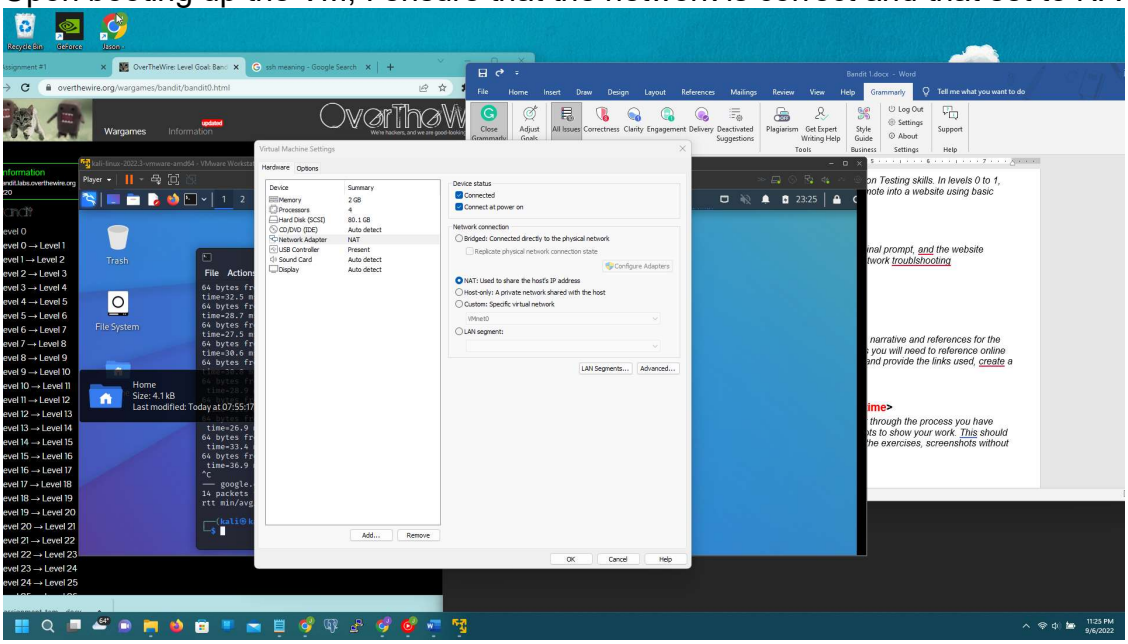
   See the Results section.

Results

1. Log in the VM as kali/kali

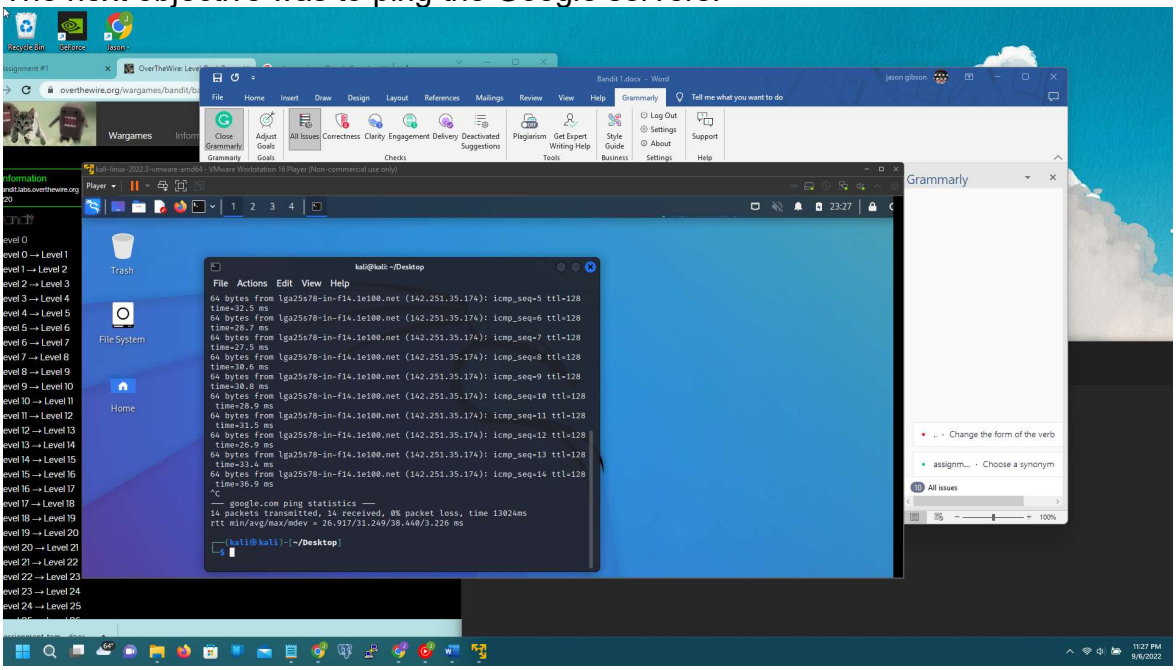


2.
3. Upon booting up the VM, I ensure that the network is correct and that set to NAT



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

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

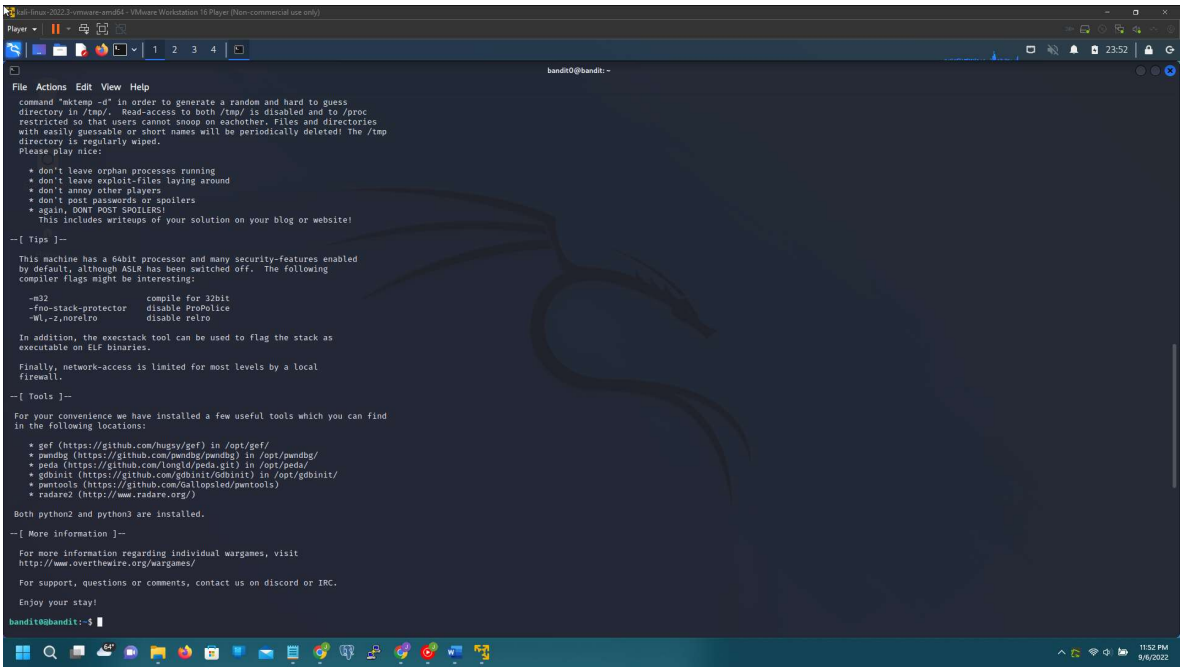


6. Successful pings allow for the next step of SSH into the website. The computer had 14 successes.

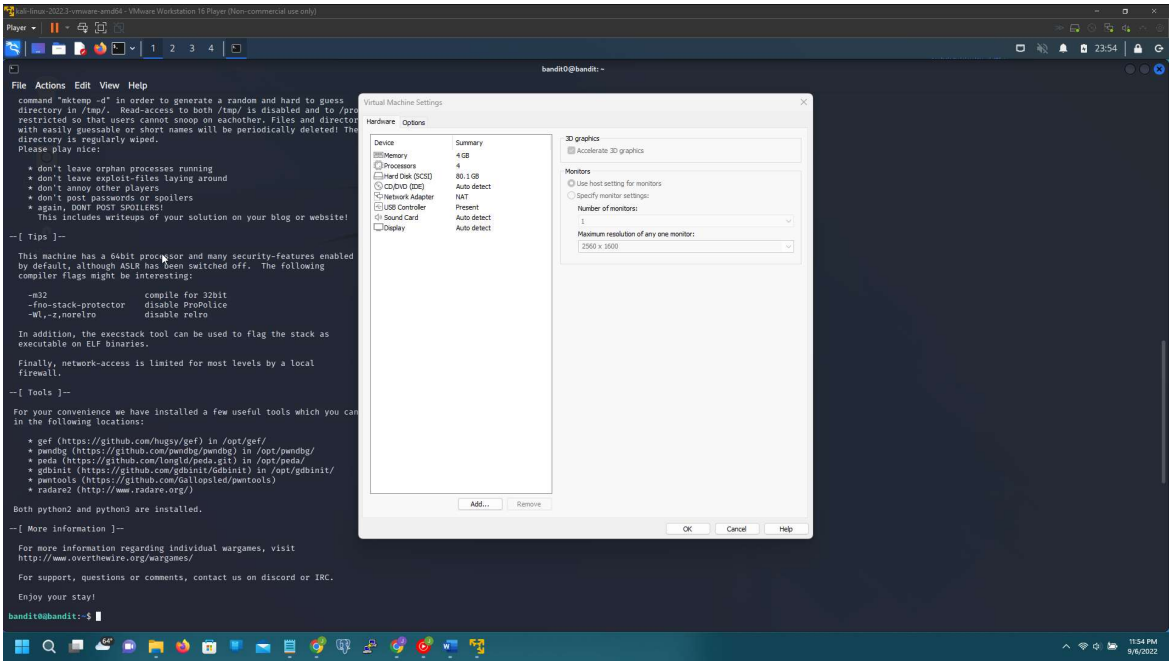
7. Remoting by SSH failed until further research that the @ sign was needed between the username and the website. As noted in reference one, the user connects then to the host. As in further discussions, a password could be used for authentication.

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 to 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.

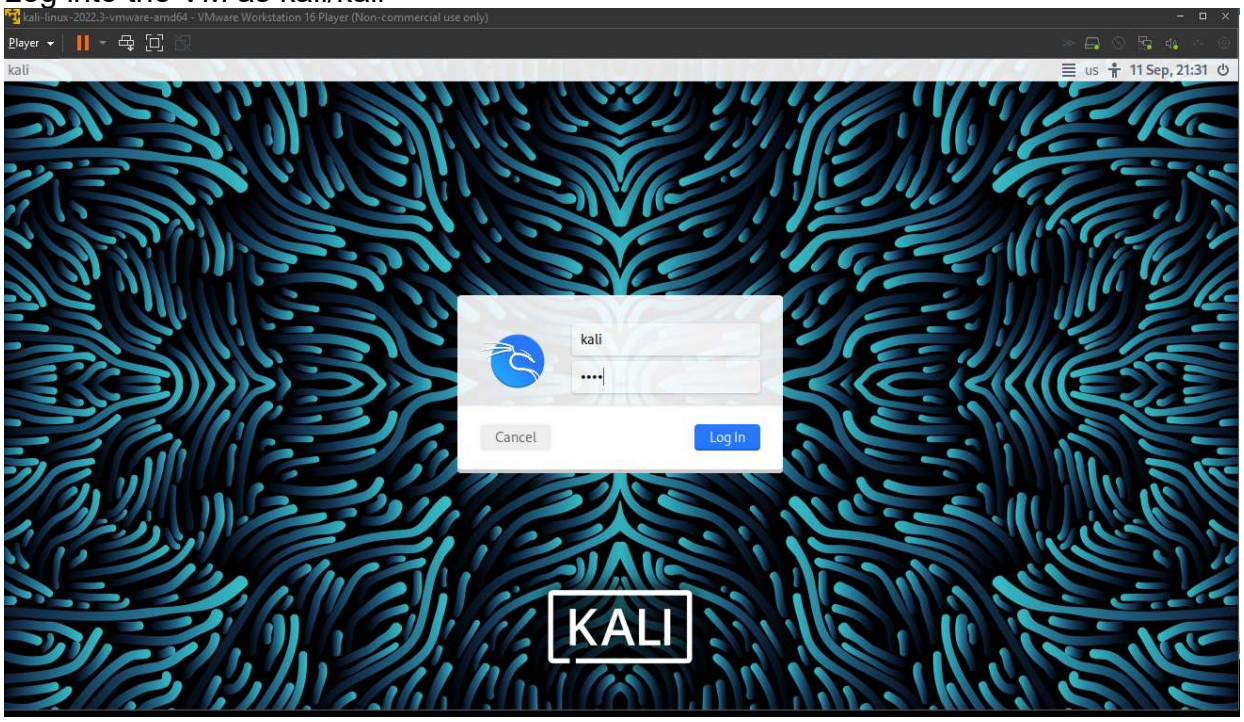
6. Post-Exploitation

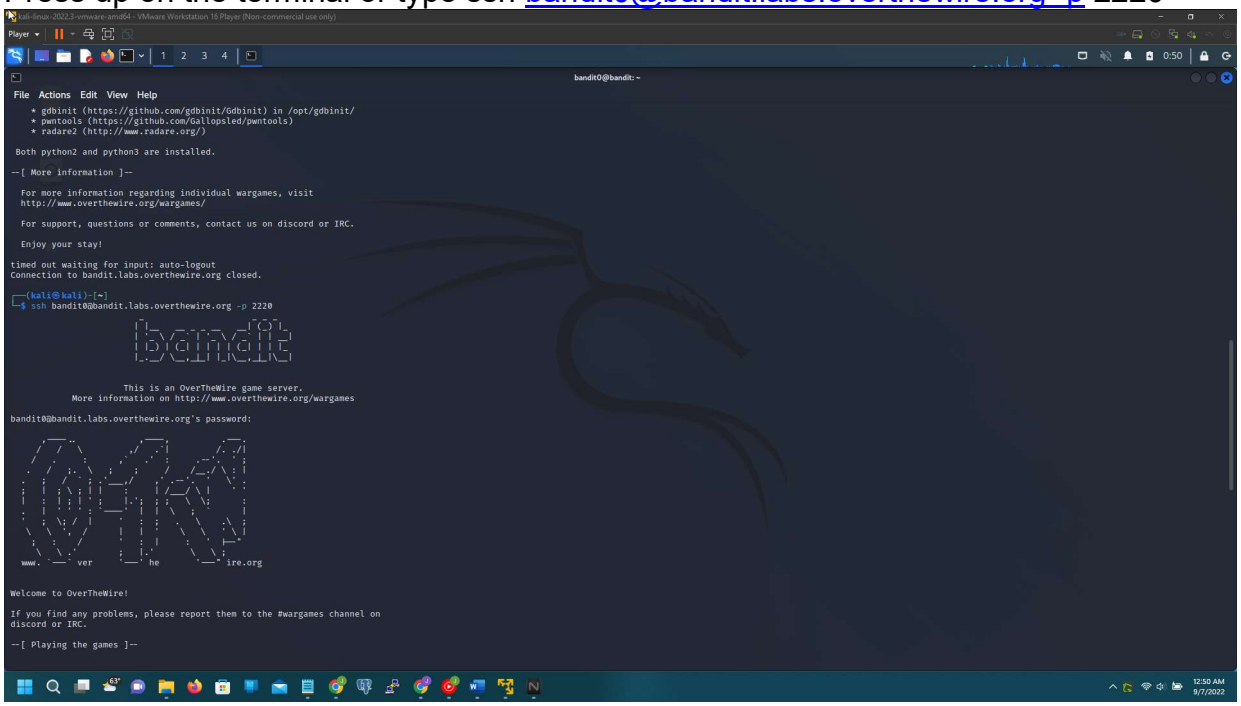
A possible hashed password could exploit the database and cause the user to bypass the SSH system. Elevating the host system to root and executing commands to turn off the server would cause the organization to become disrupted. Changing, elevating, or erasing the user/password altogether would render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

7. Reporting

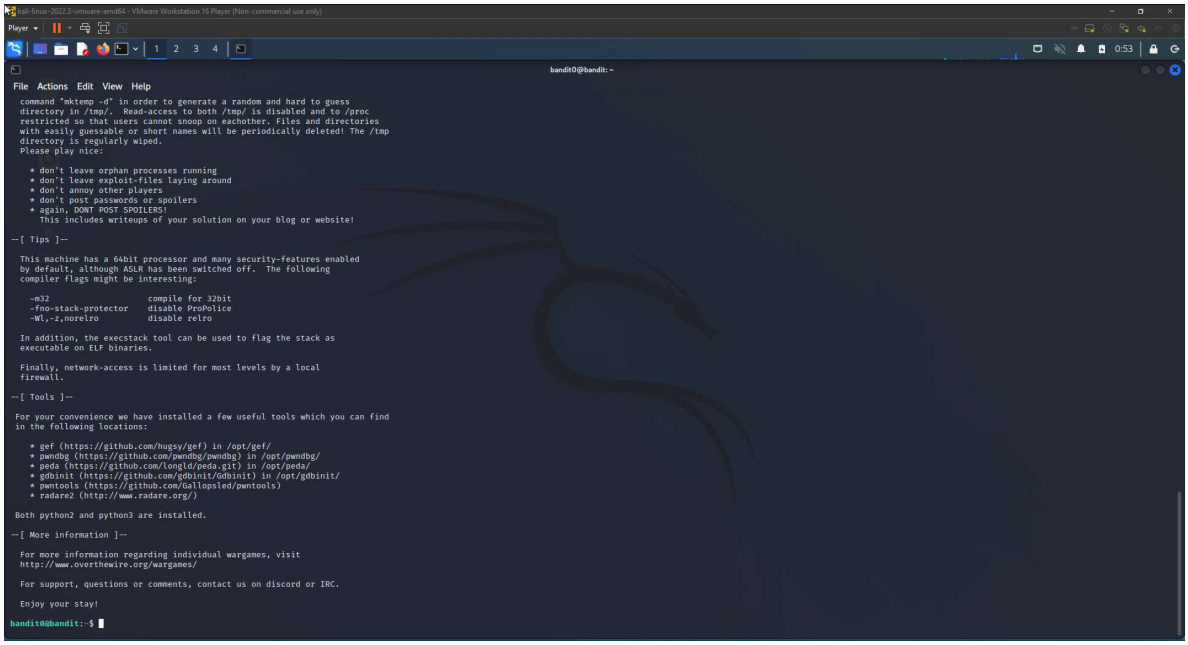
   See Results section

Results

1. Log into the VM as kali/kali
2. 

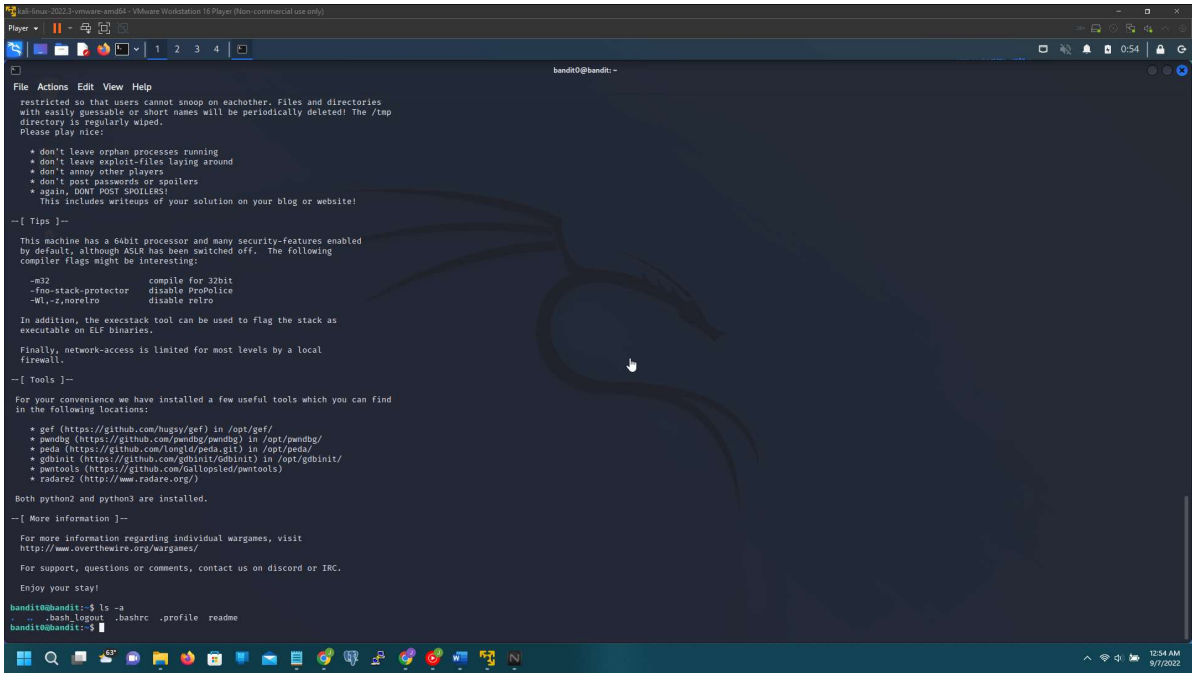
3. Press up on the terminal or type ssh bandit0@bandit.labs.overthewire.org -p 2220
4. 

5. Log in with password bandit0

6. 

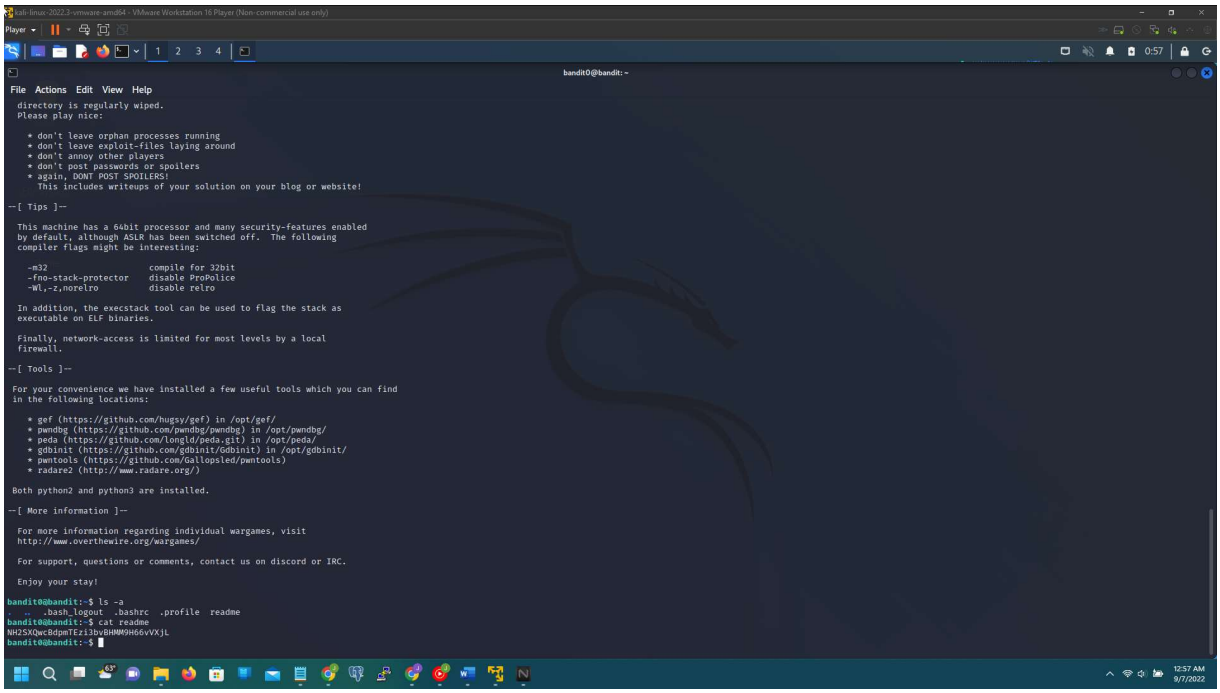
7. The user is now logged in as bandit0@bandit

8. Type ls -a

9. 

10. This displays the ones need, readme.

11. Type cat readme

12. 

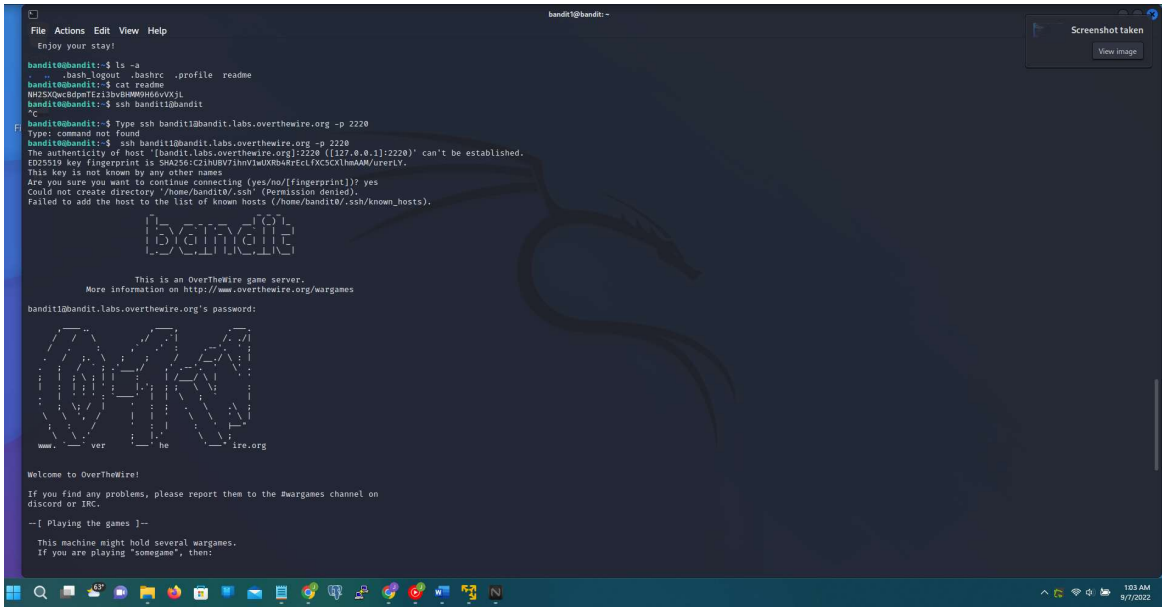
13. The password is: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

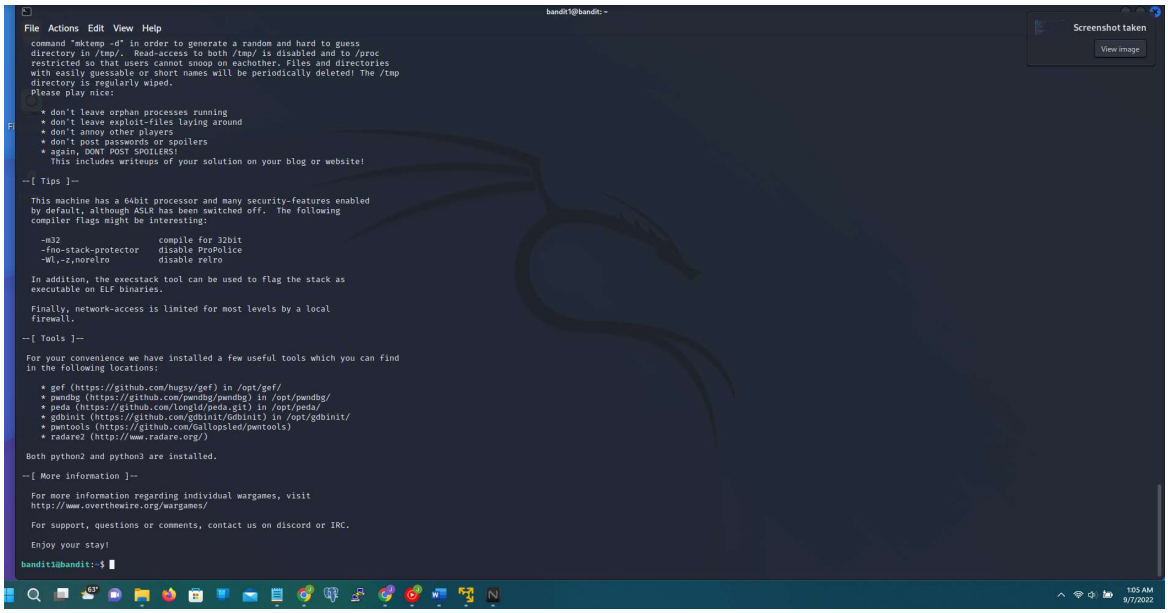
14. Highlight and right click> copy selection

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

16. Select yes

17. Paste the password: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

18. 

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.

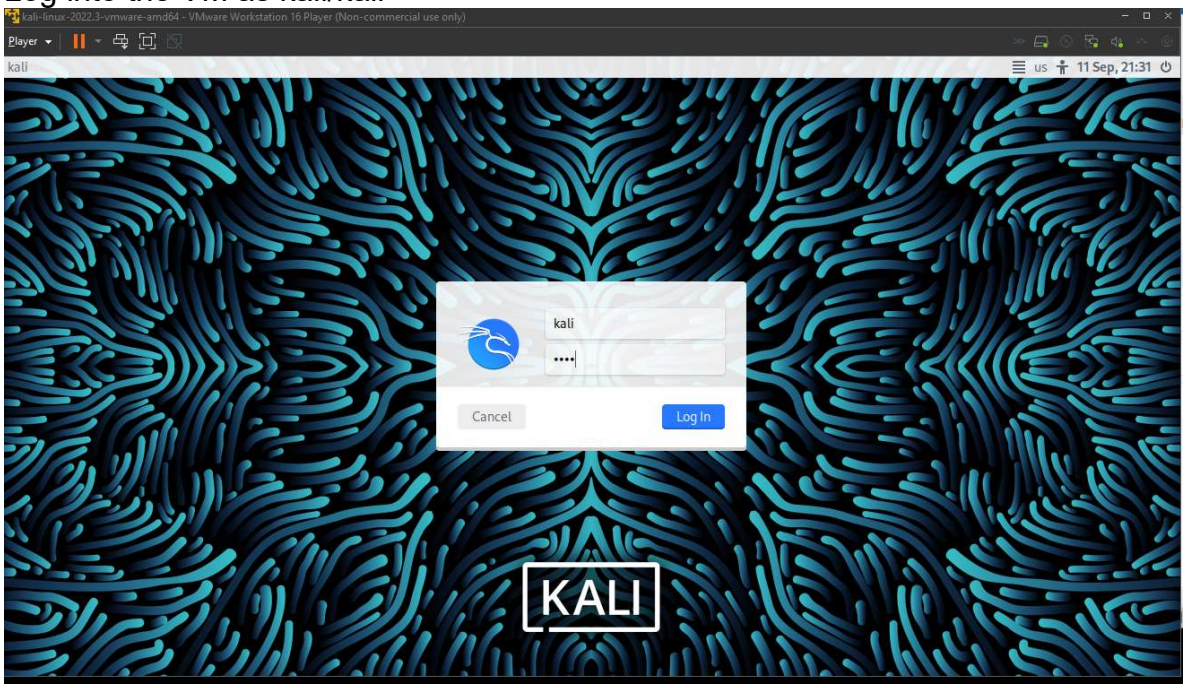
6. Post-Exploitation

   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.

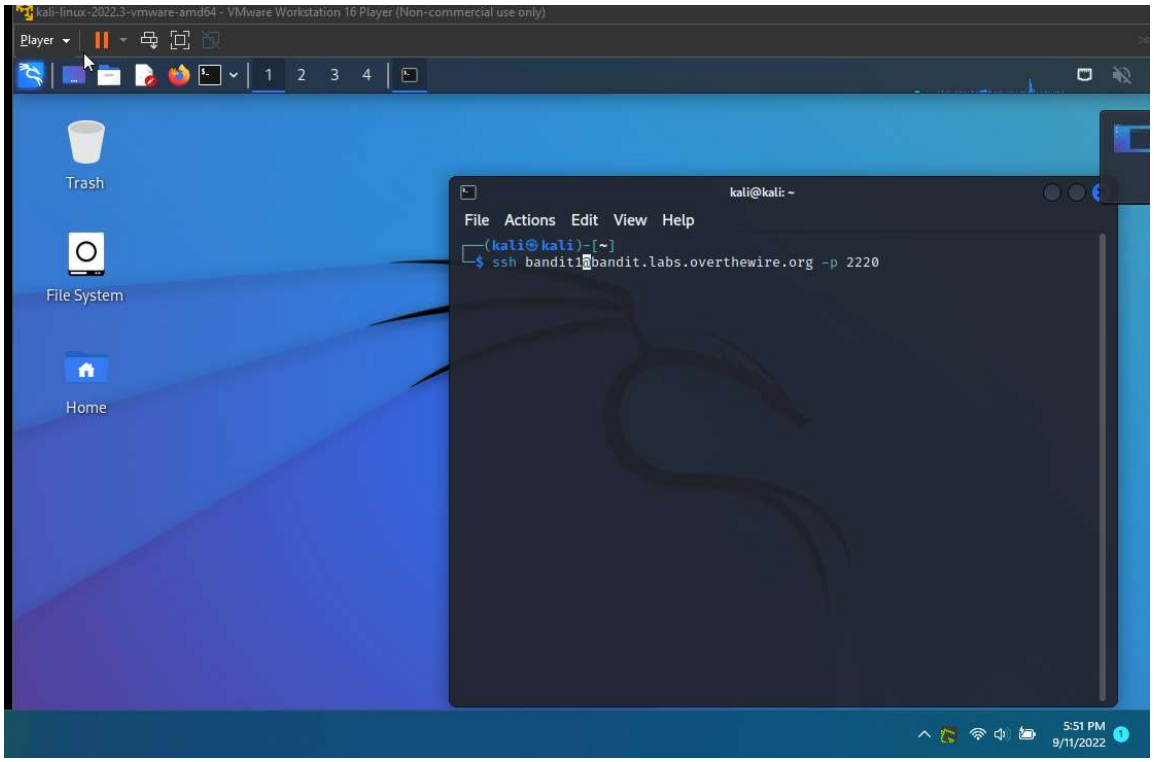
7. Reporting

   See Results section

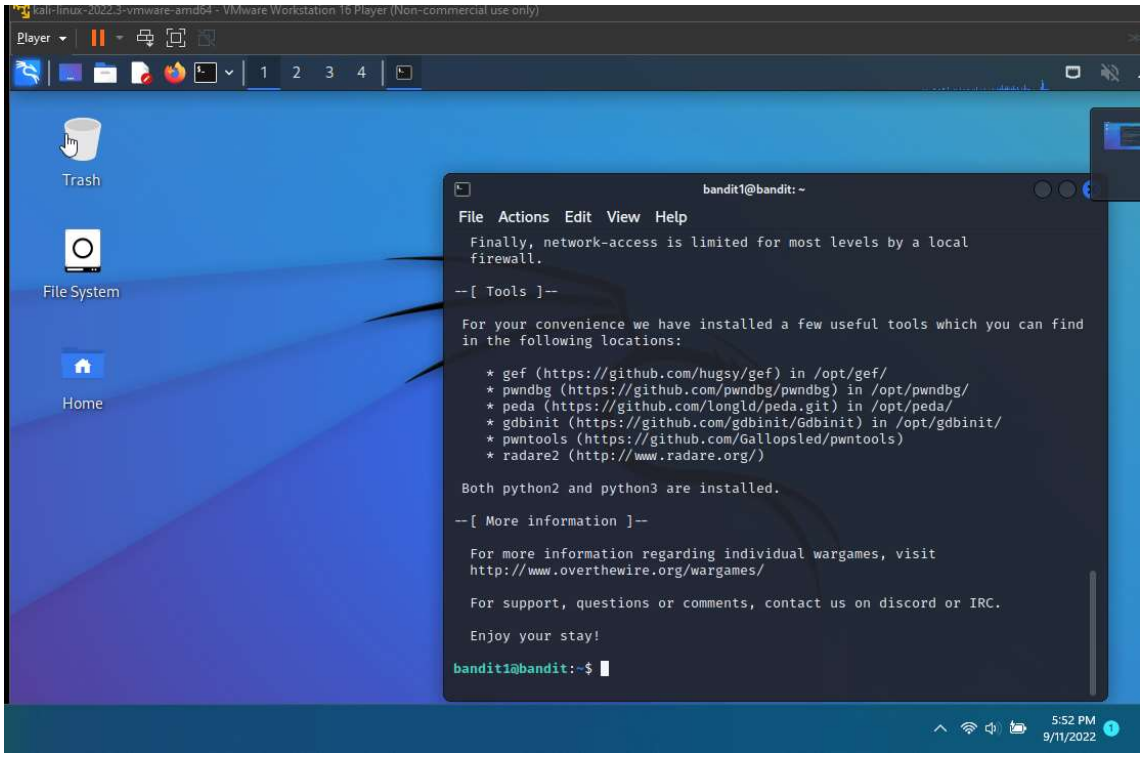
Results

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

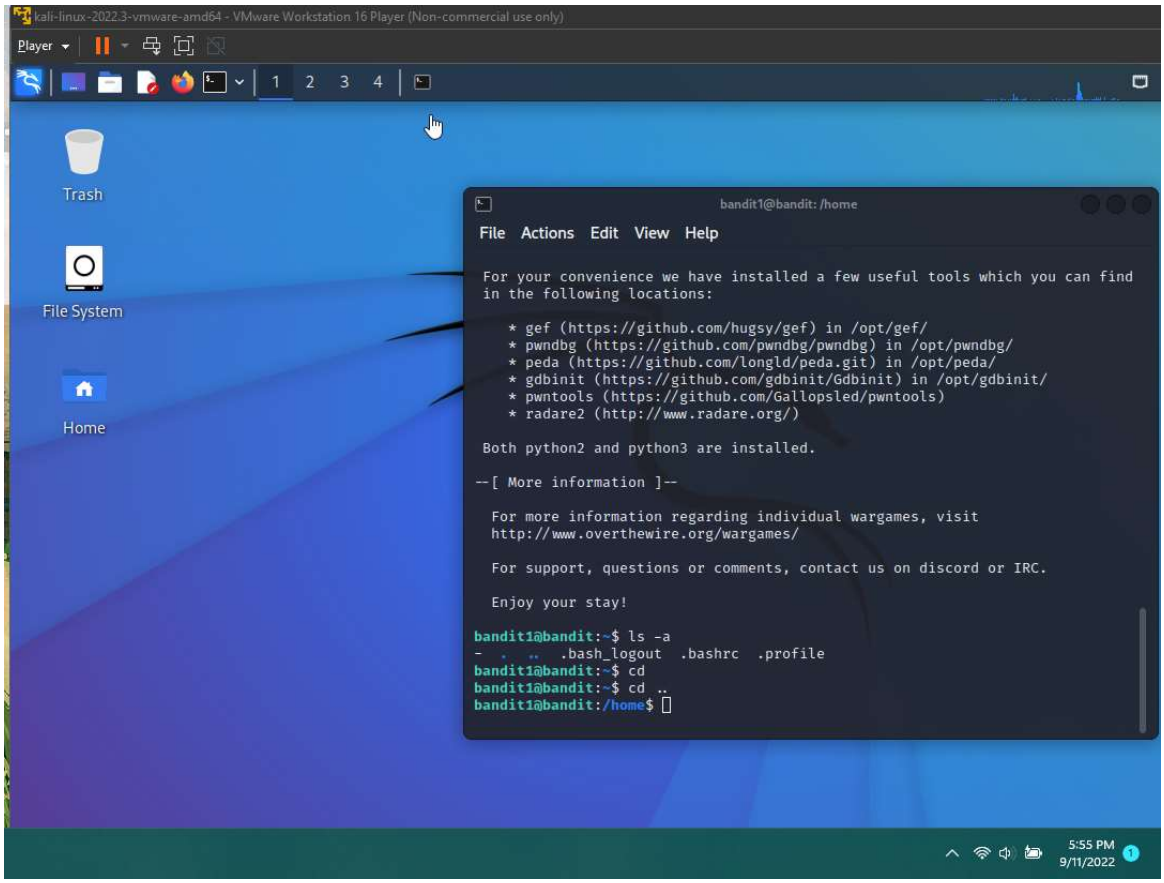
6. 

7. Ls -a to see the directory

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

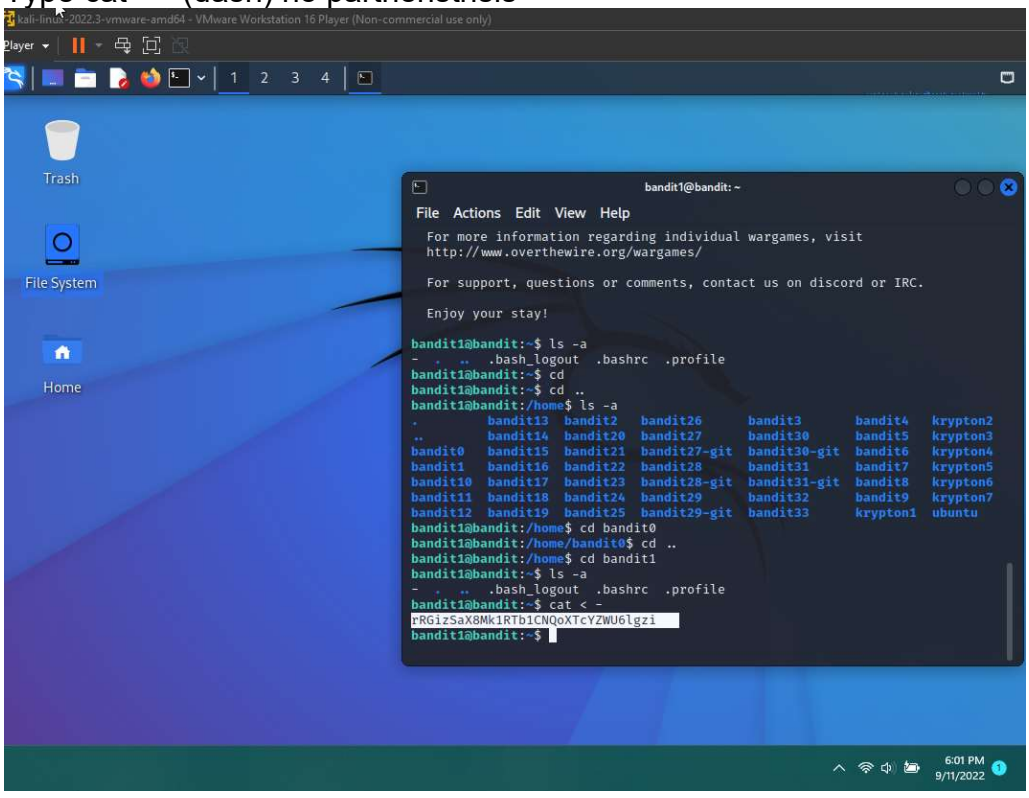
9. Type ls -a file.

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

11. 

12. Ls -a again seen file structure

13. Type cat < - (dash) no parthensthsis

14. 

15. Copy password rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi 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.

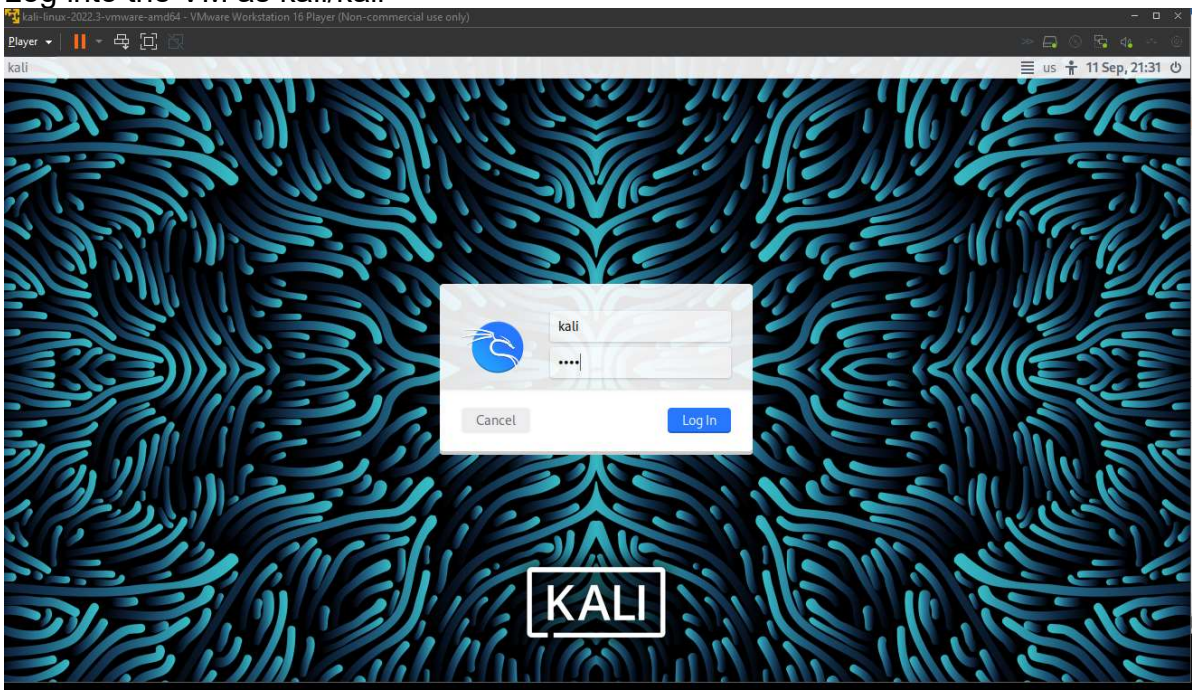
6. Post-Exploitation

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

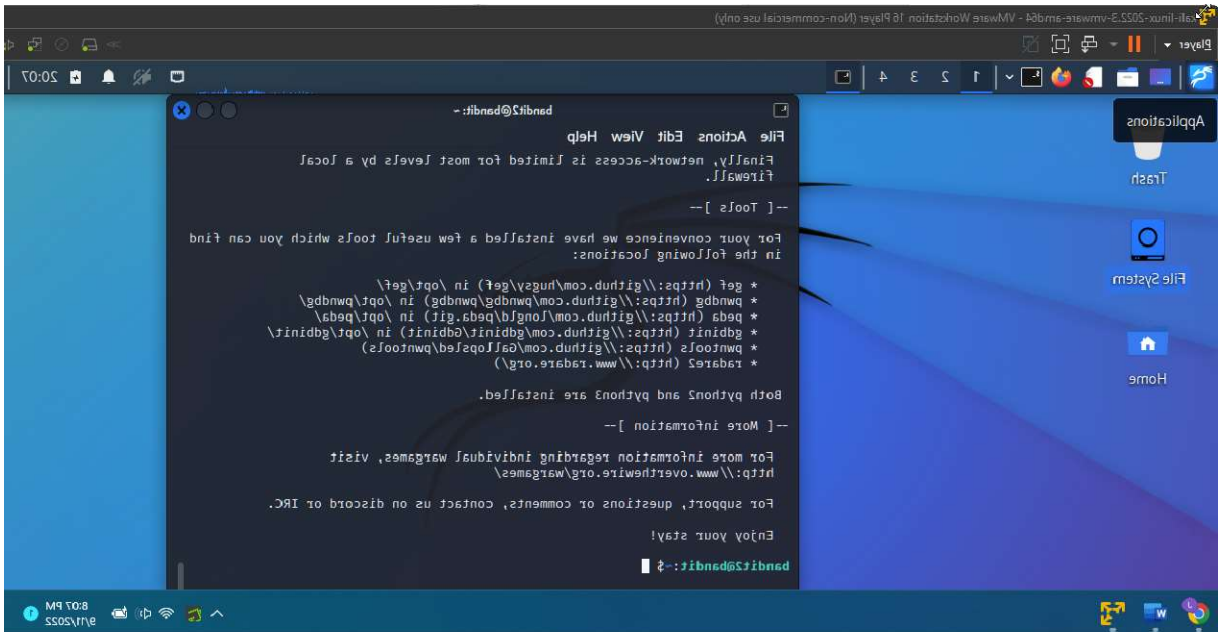
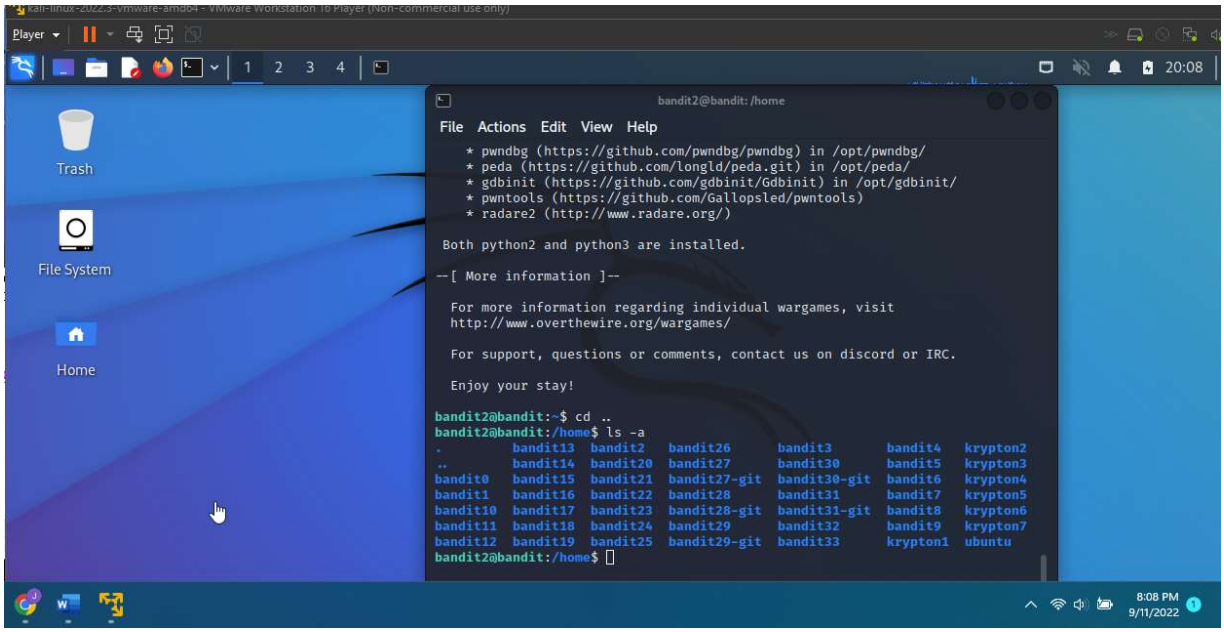
7. Reporting

   See Results section

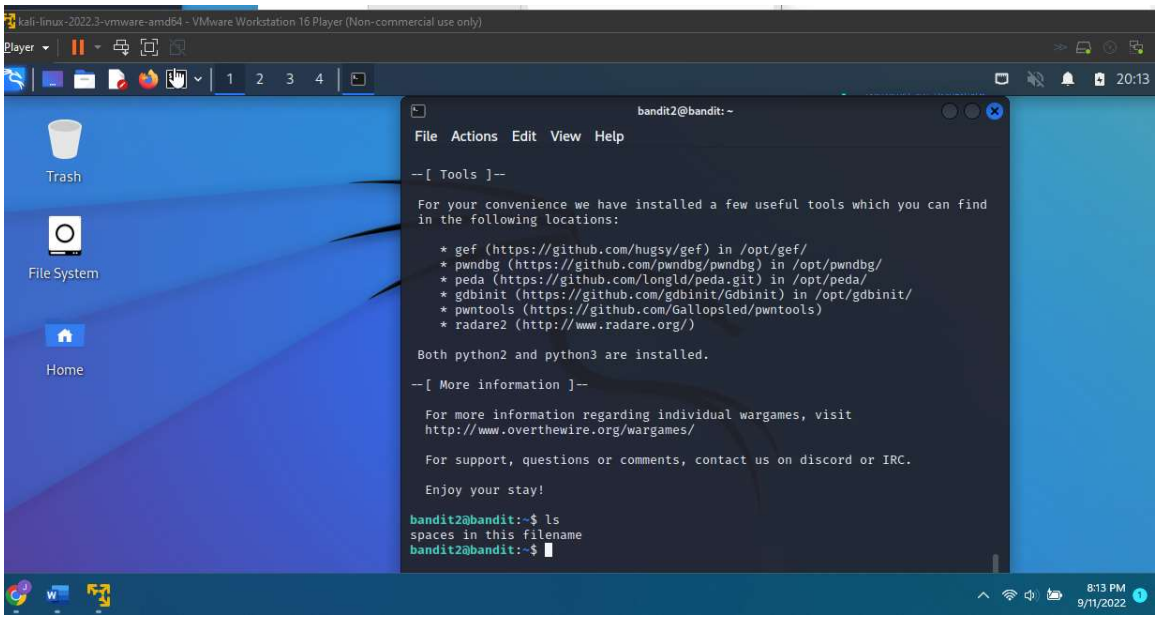
Results

1. Log into the VM as kali/kali
2. 

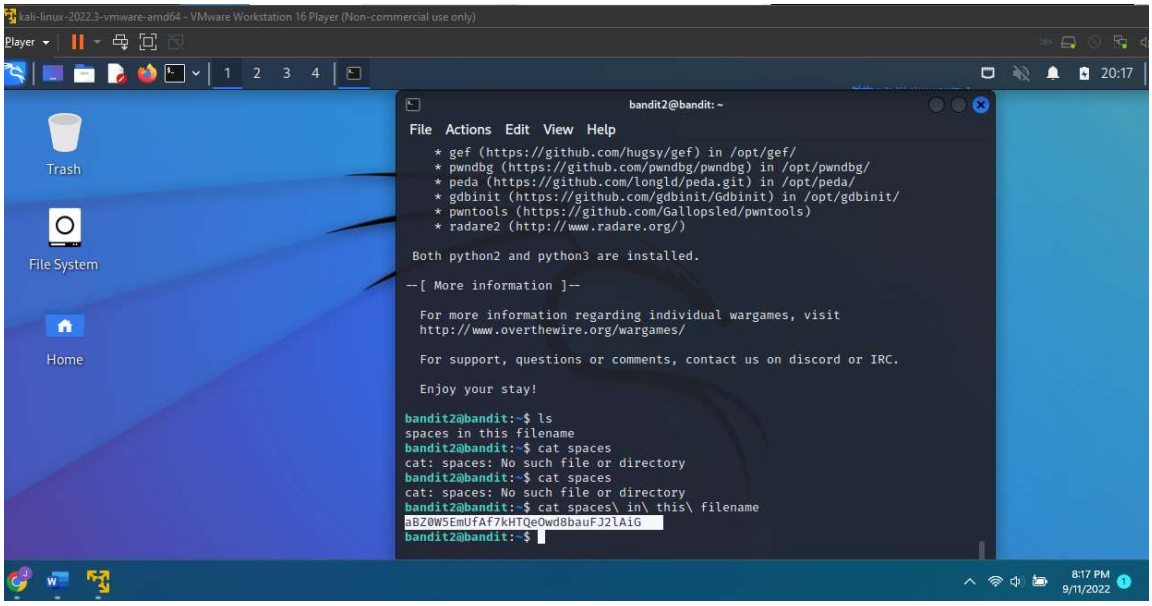
3. Log onto SSH as bandit2@bandit.labs.overthewire.org -p 2220
4. Password rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

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.

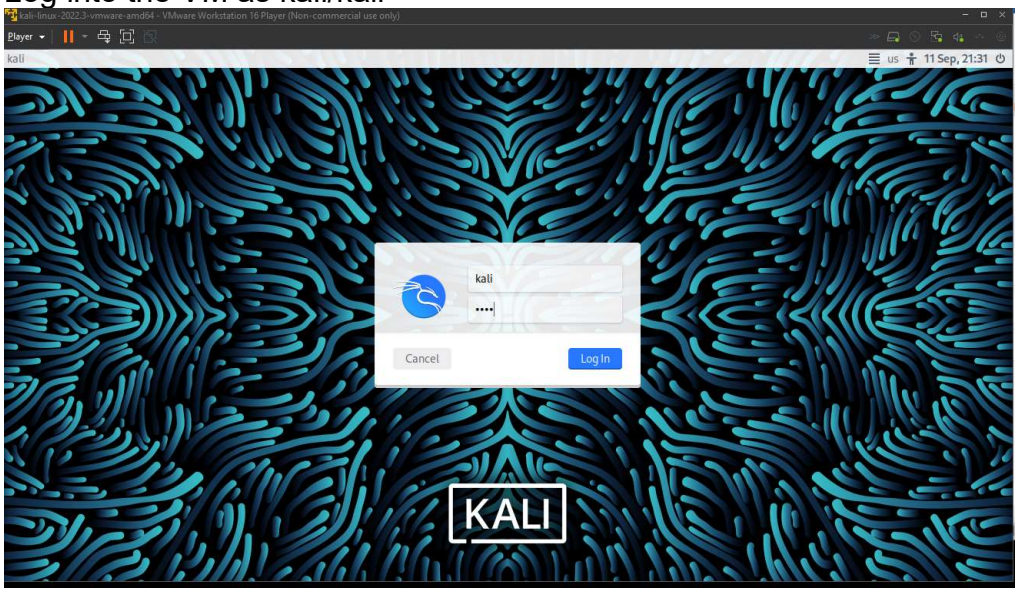
6. Post-Exploitation

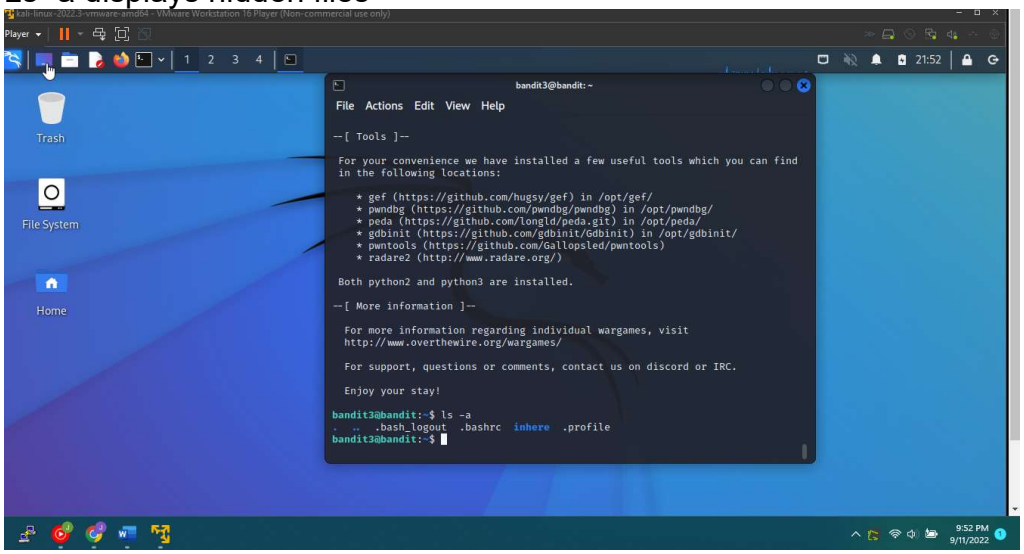
   Recommend using encryption with salting. Also, not allow the password to be easily accessible.

7. Reporting

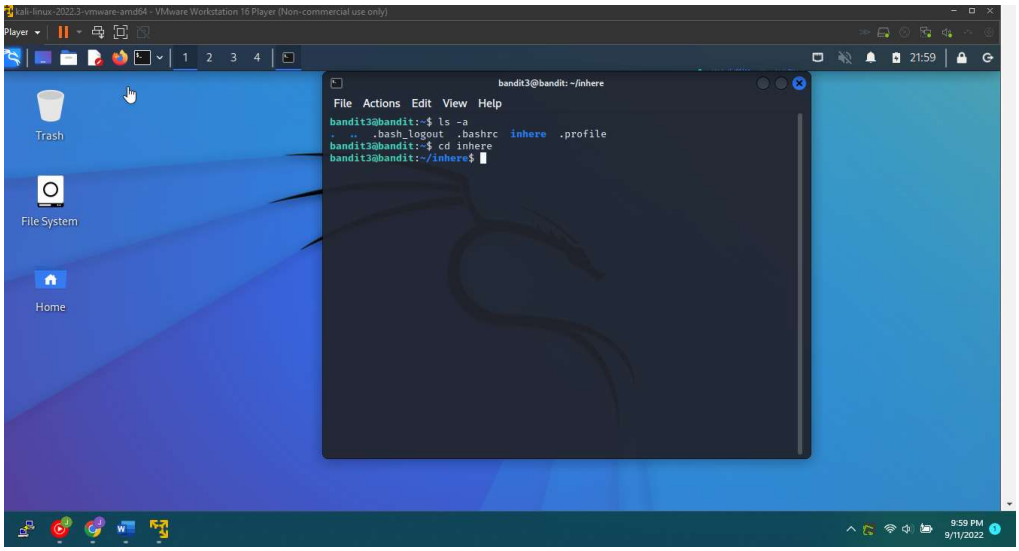
   See Results section

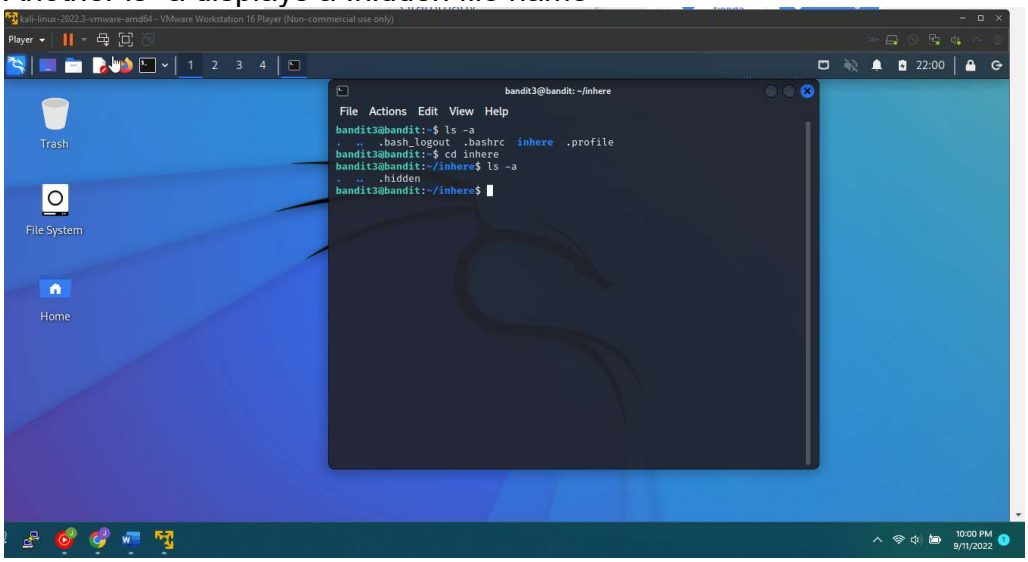
Results

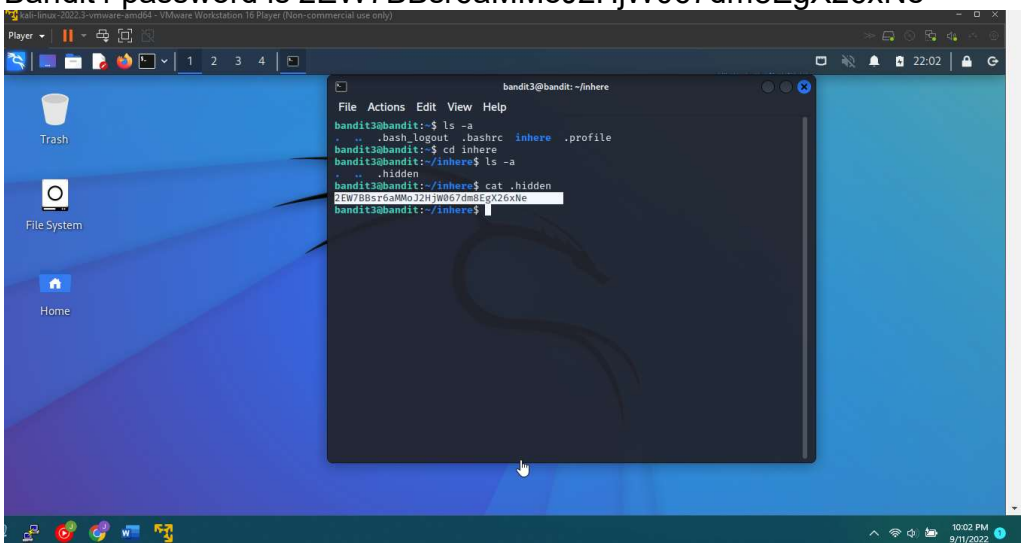
1. Log into the VM as kali/kali
2. 

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

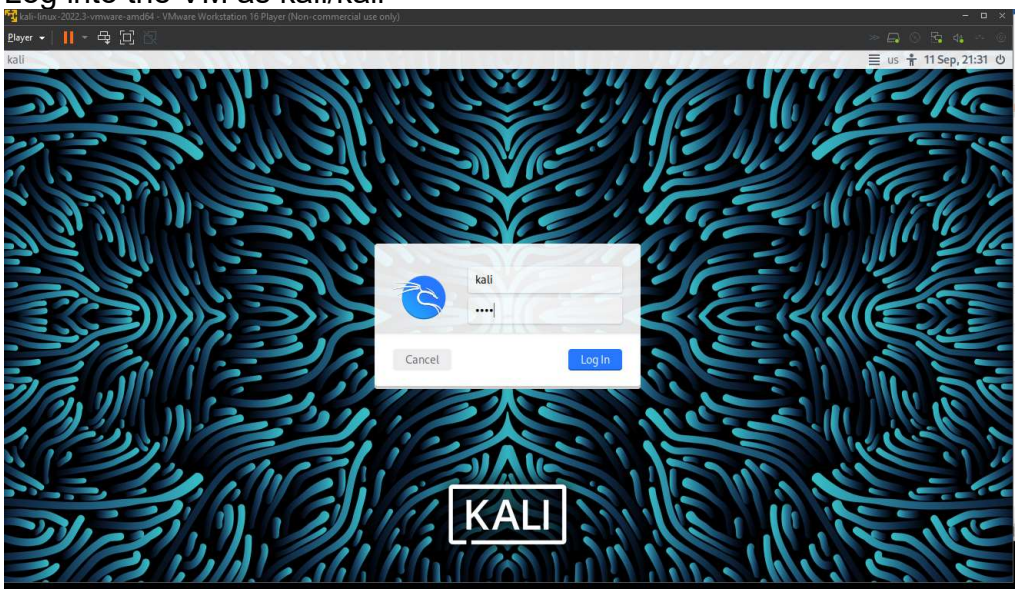
The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 5 to 6, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is hidden in the "inhere" Directory. The ls -a and -ls command finds hidden files and tree folder structure, 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

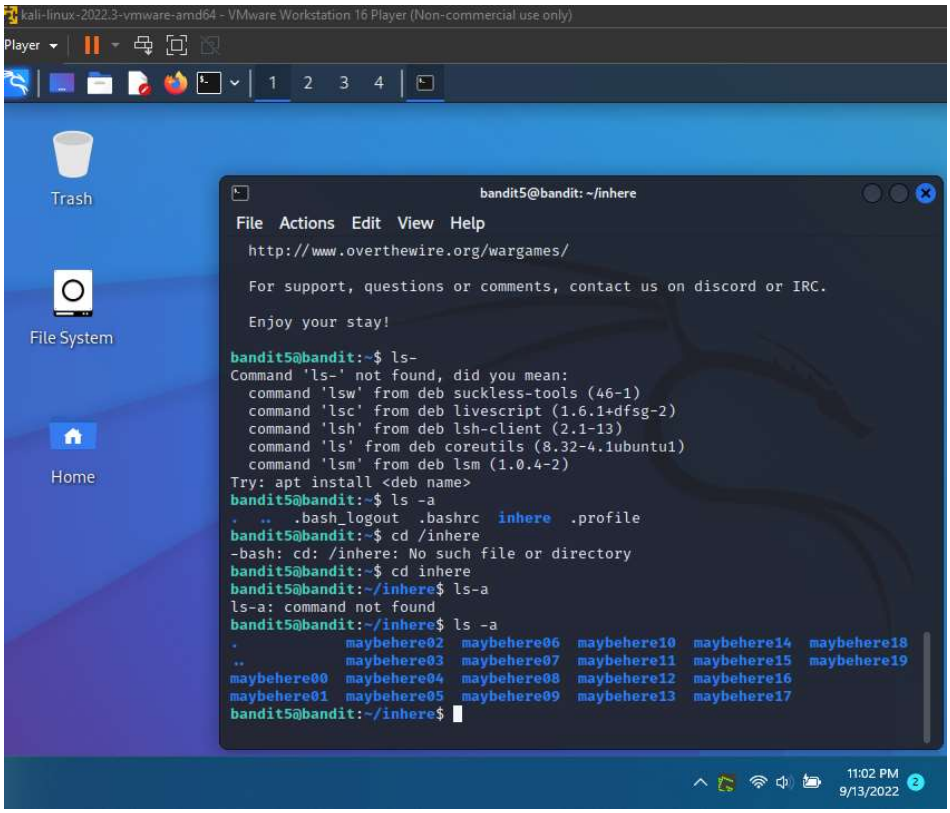
- *The tools needed will be a VM running a Linux distro (Kali).*
- *A terminal prompt.*
- *The Website https://overthewire.org/wargames/bandit/bandit6.html*
- *The following Linux commands ls - list files ls -a list all files including hidden files, cd (change directory), copy, paste, find, cat or read,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

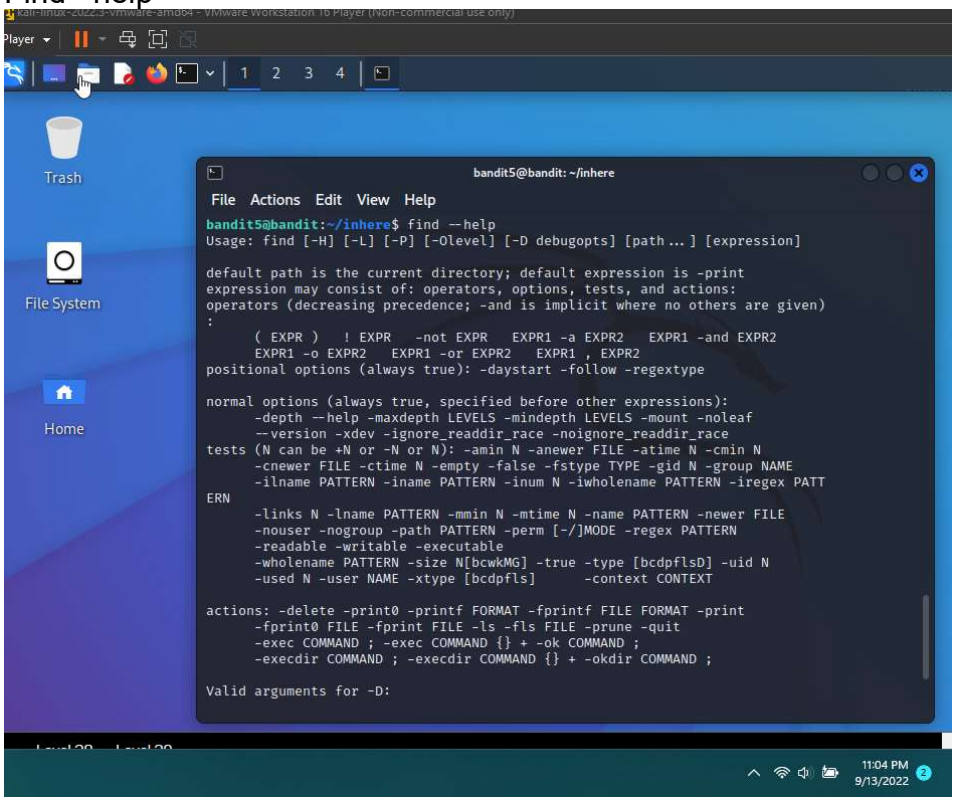
Methodology

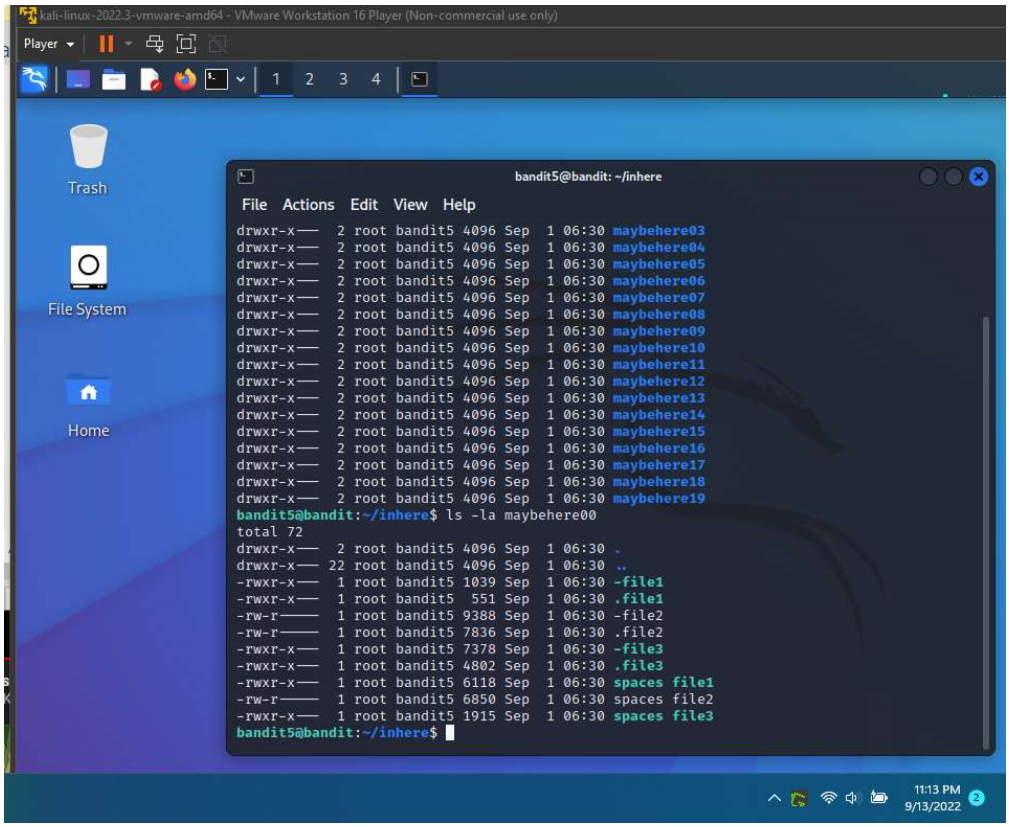
Results

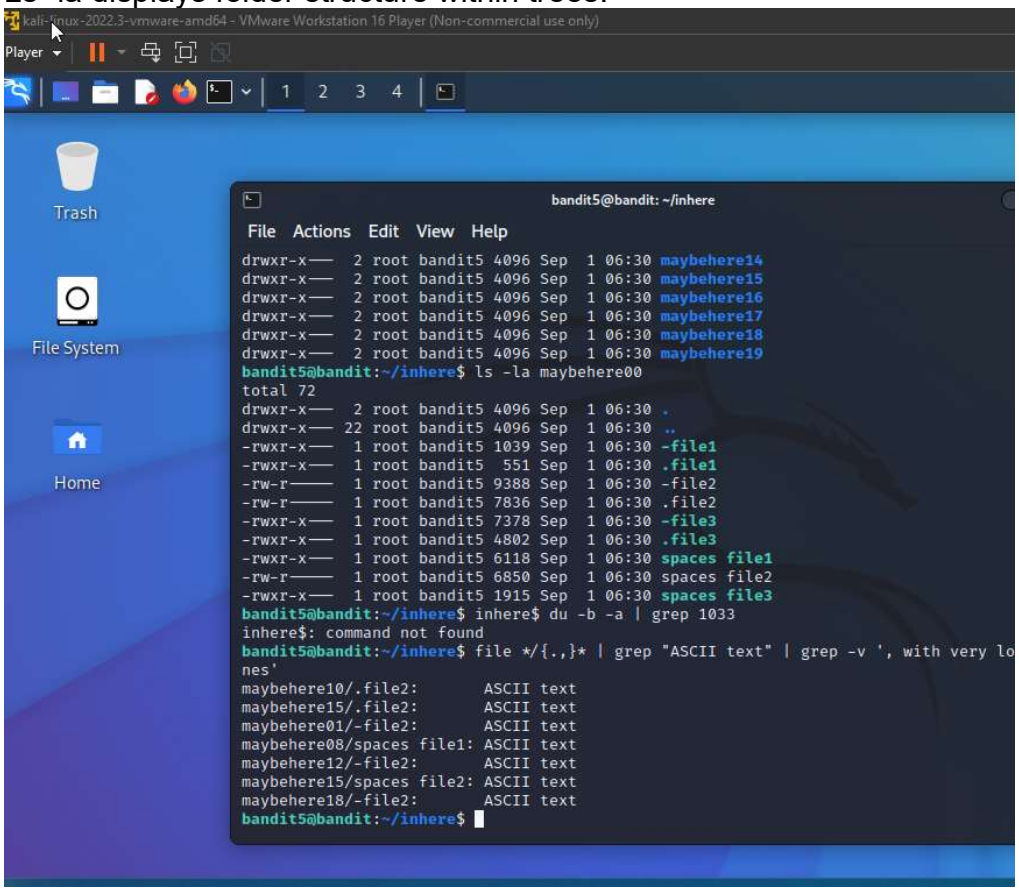
1. Log into the VM as kali/kali
2. 

3. Bandit5 password lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
4. Ls -a displays hidden files

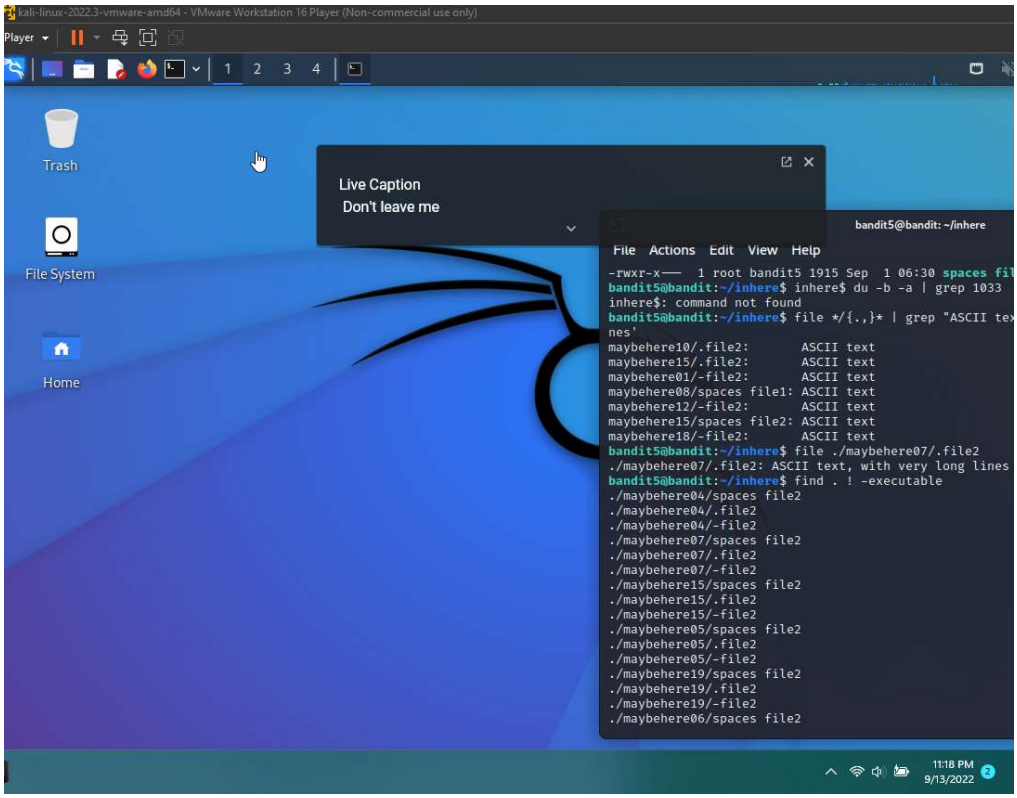
5. 

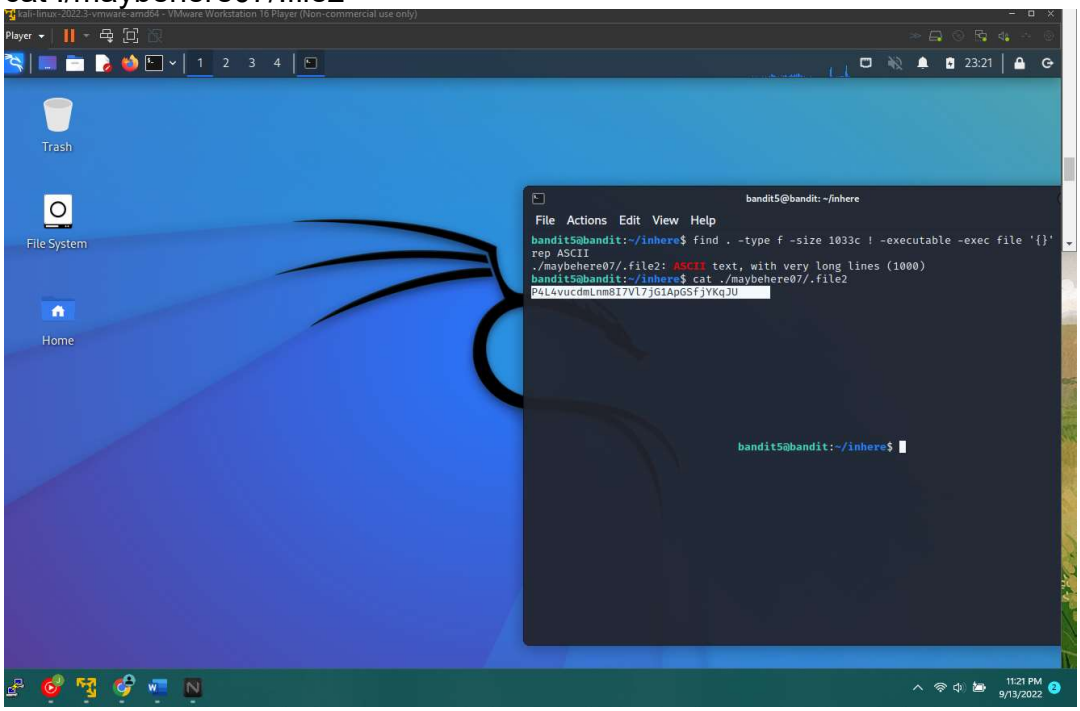
6. Find –help
7. 

8. 

9. Ls -la displays folder structure within trees.
10. 

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

12. 

13. The following commands compare what could be found in file .2, and maybe here has what is looking for.
14. cat ./maybehere07/.file2
15. 

16. Bandit 6 password P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

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

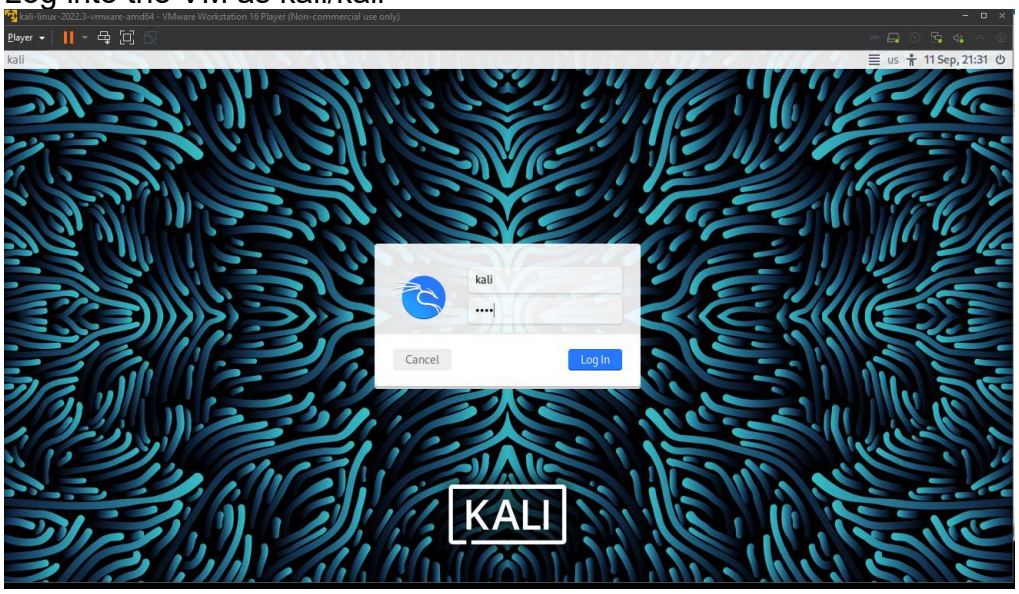
The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 5 to 6, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is hidden in the "inhere" Directory. The ls -a and -ls command finds hidden files and tree folder structure, 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

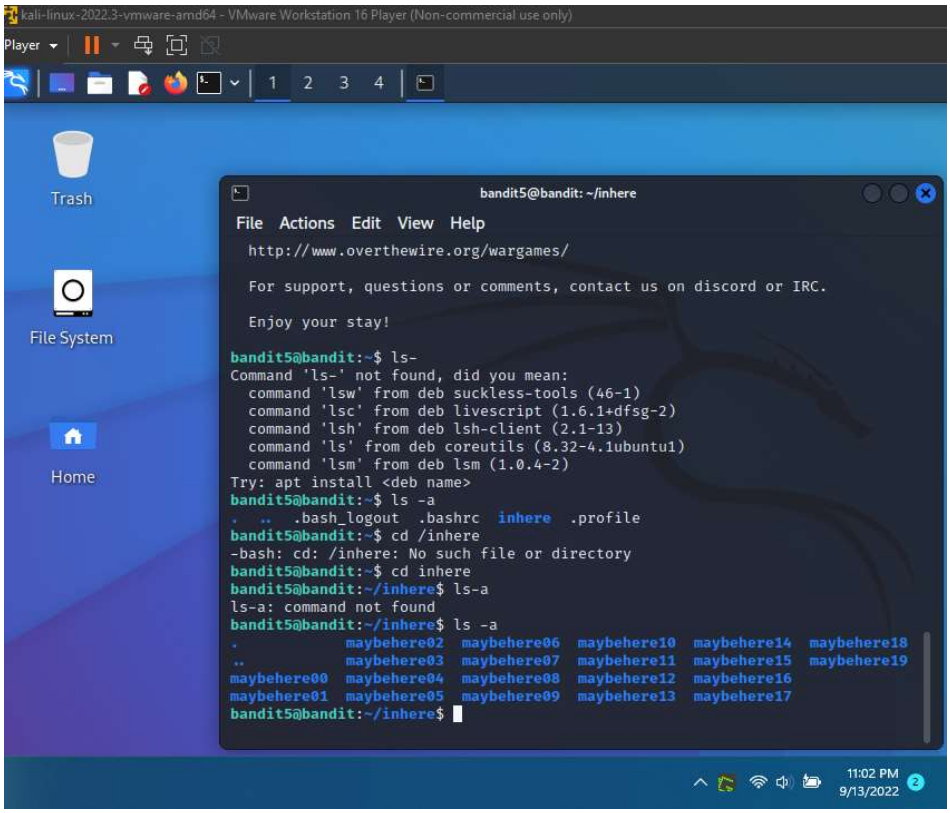
- *The tools needed will be a VM running a Linux distro (Kali).*
- *A terminal prompt.*
- *The Website https://overthewire.org/wargames/bandit/bandit6.html*
- *The following Linux commands ls - list files ls -a list all files including hidden files, cd (change directory), copy, paste, find, cat or read,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

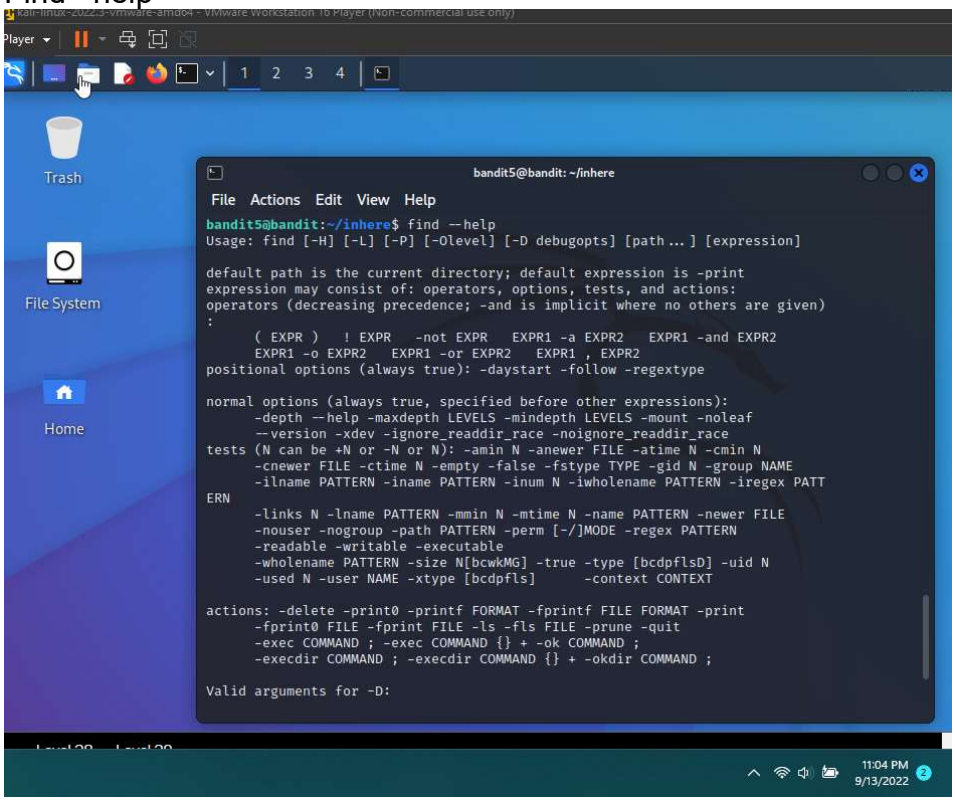
Methodology

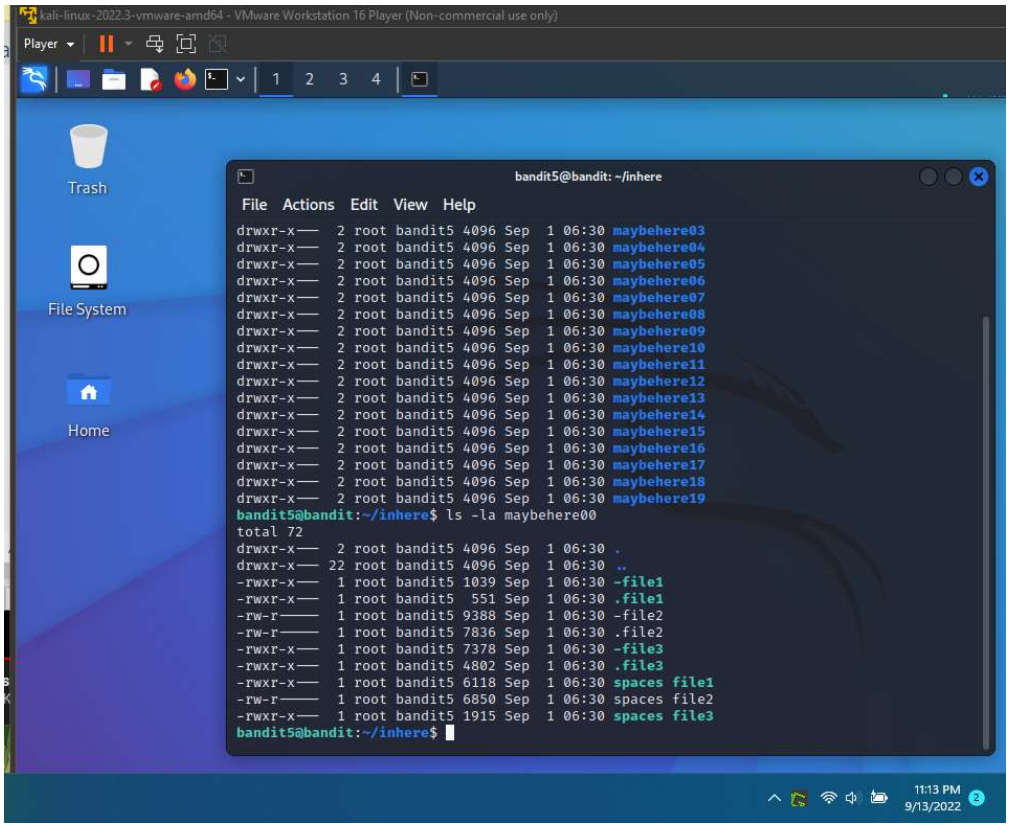
Results

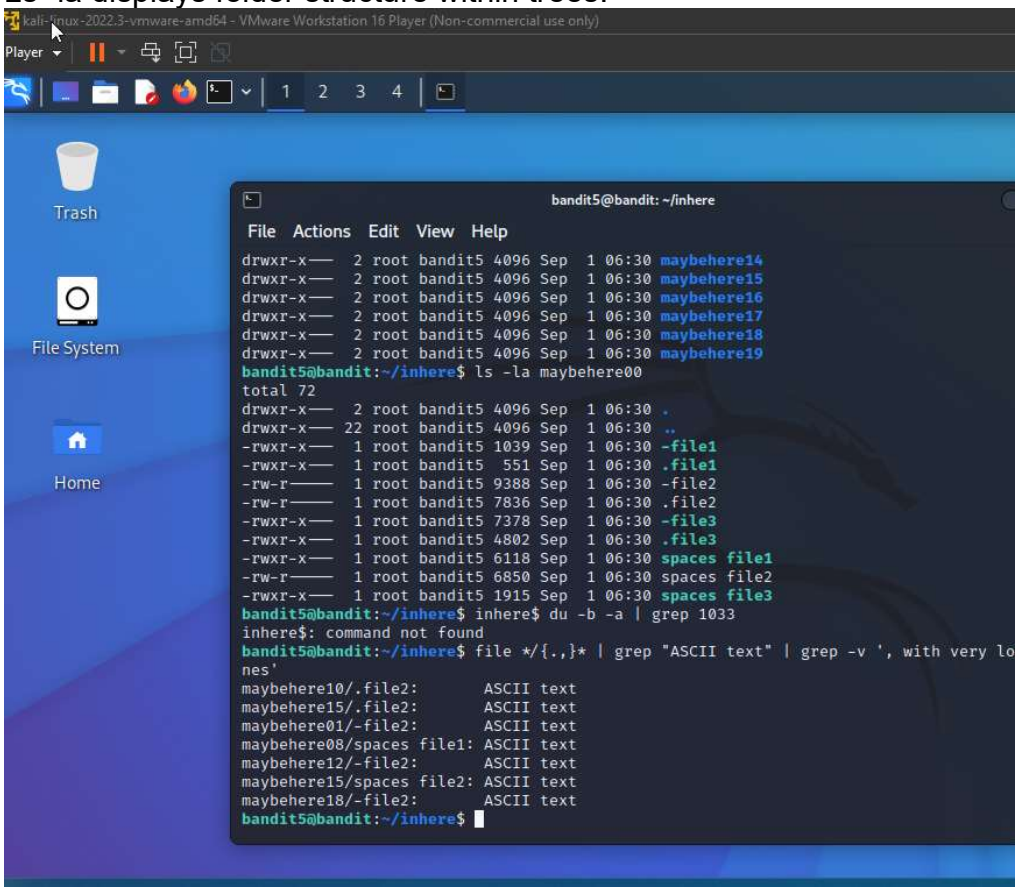
1. Log into the VM as kali/kali
2. 

3. Bandit5 password lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
4. Ls -a displays hidden files

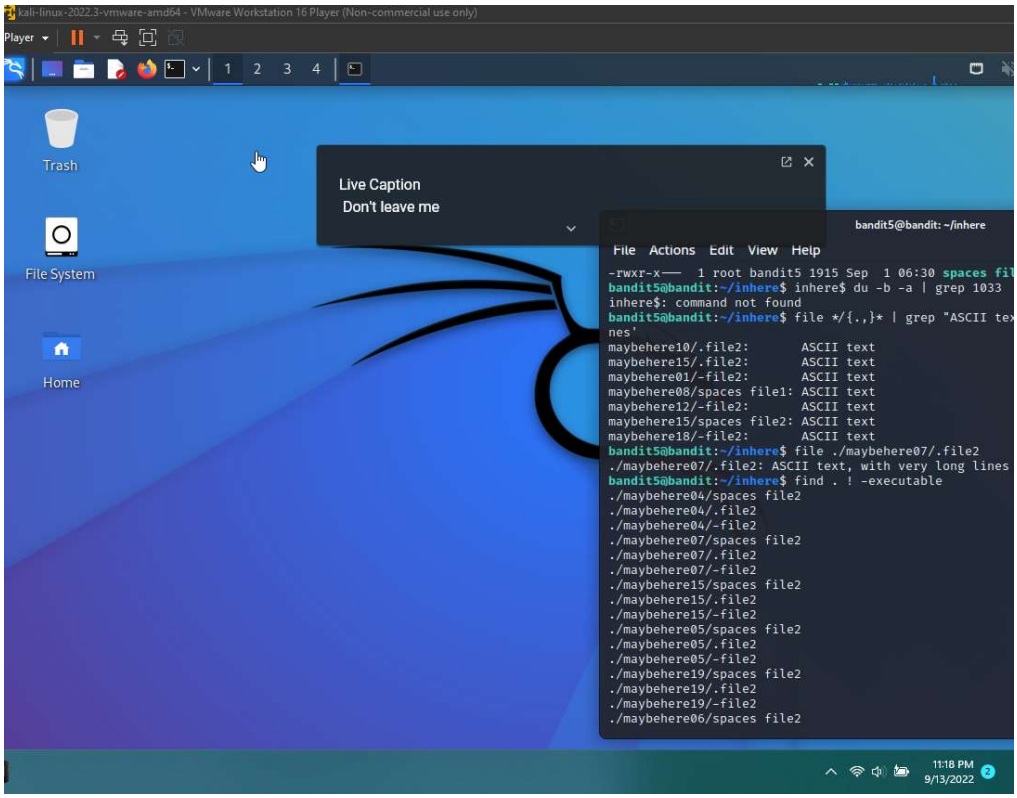
5. 

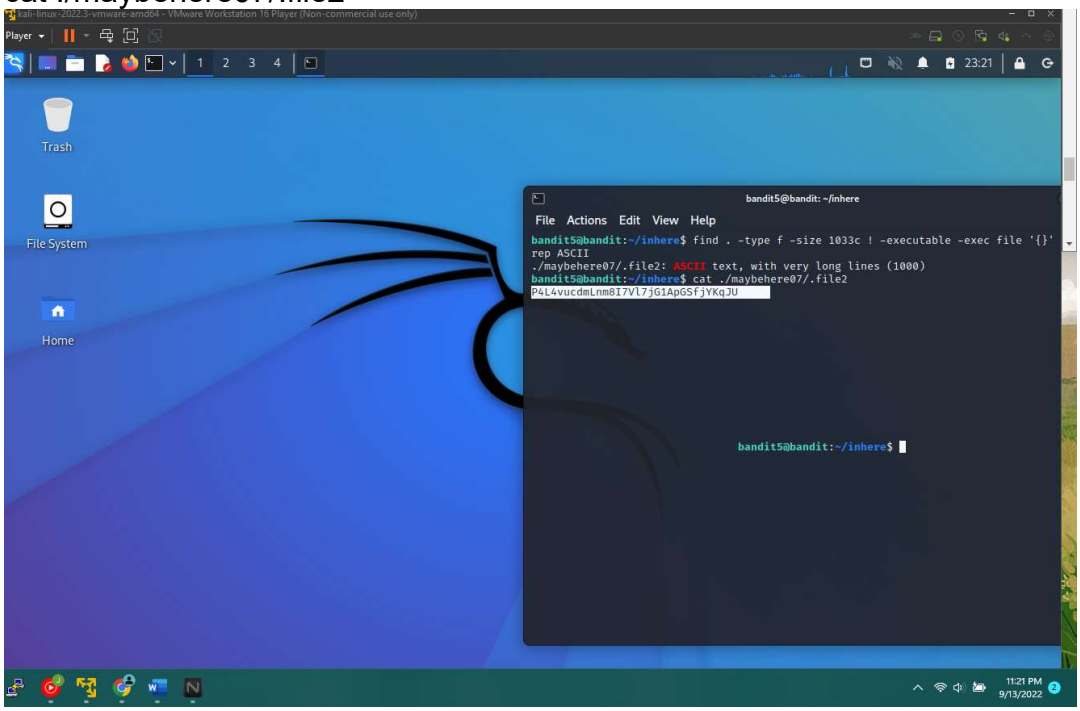
6. Find –help
7. 

8. 

9. Ls -la displays folder structure within trees.
10. 

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

12. 

13. The following commands compare what could be found in file .2, and maybe here has what is looking for.
14. cat ./maybehere07/.file2
15. 

16. Bandit 6 password P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

The College of Saint Rose

ETHICAL HACKING REPORT
ASSIGNMENT # 1 BANDIT 7

JASON GIBSON Gibsonj421@Strose.edu

Scope of the assignment

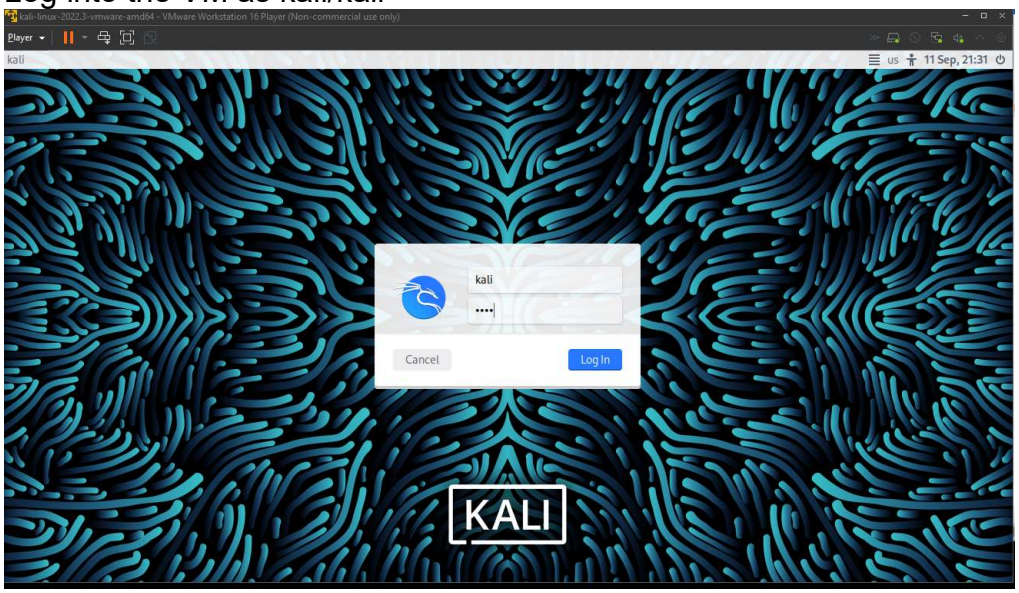
The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 6 to 7, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is hidden Somewhere in the Linux system. The end user will have to discover where. The ls -a and -ls command 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

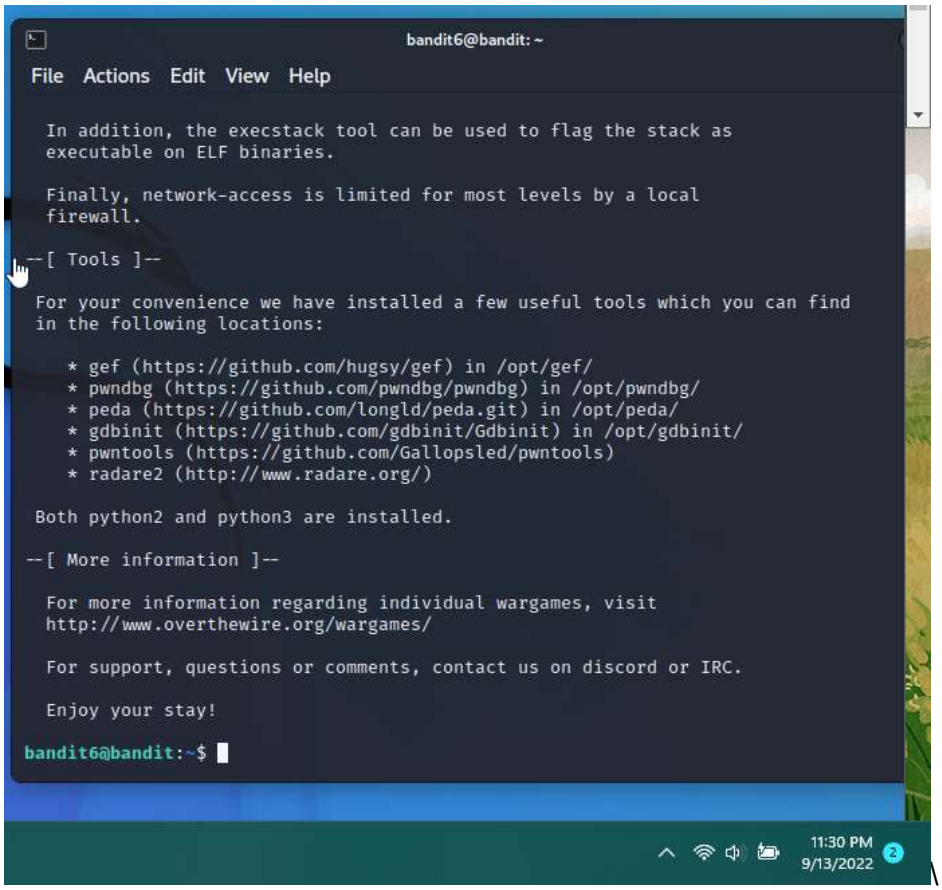
- *The tools needed will be a VM running a Linux distro (Kali).*
- *A terminal prompt.*
- *The Website https://overthewire.org/wargames/bandit/bandit7.html*
- *The following Linux commands ls - list files ls -a, ls la, list all files including hidden files, cd (change directory), copy, paste, find, cat 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

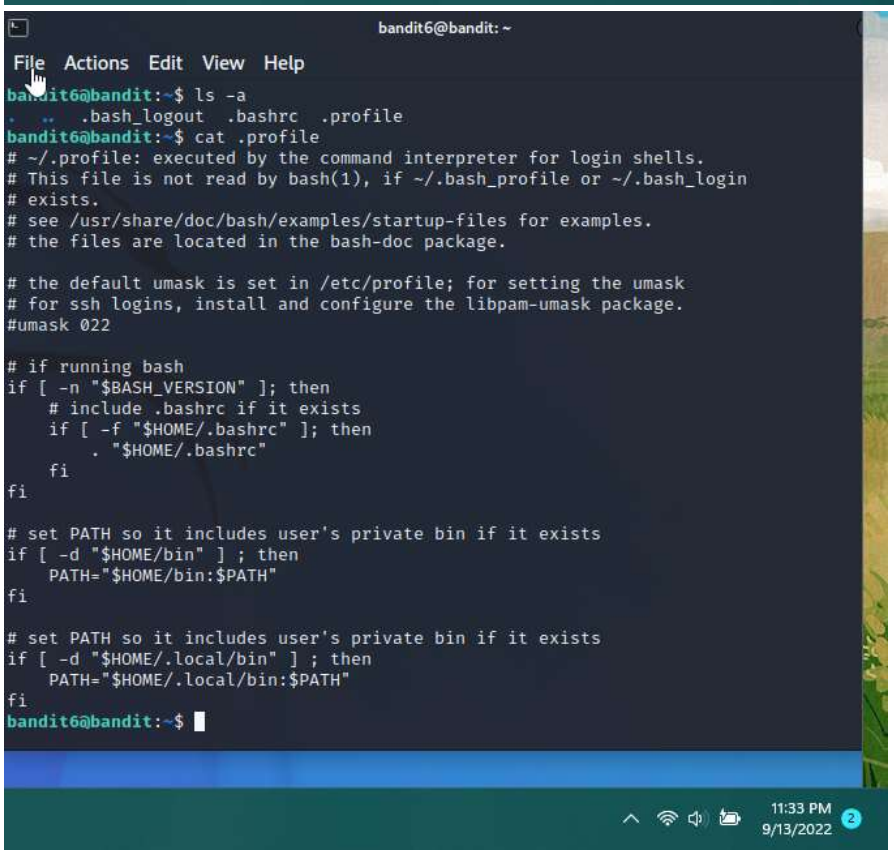
Methodology

Results

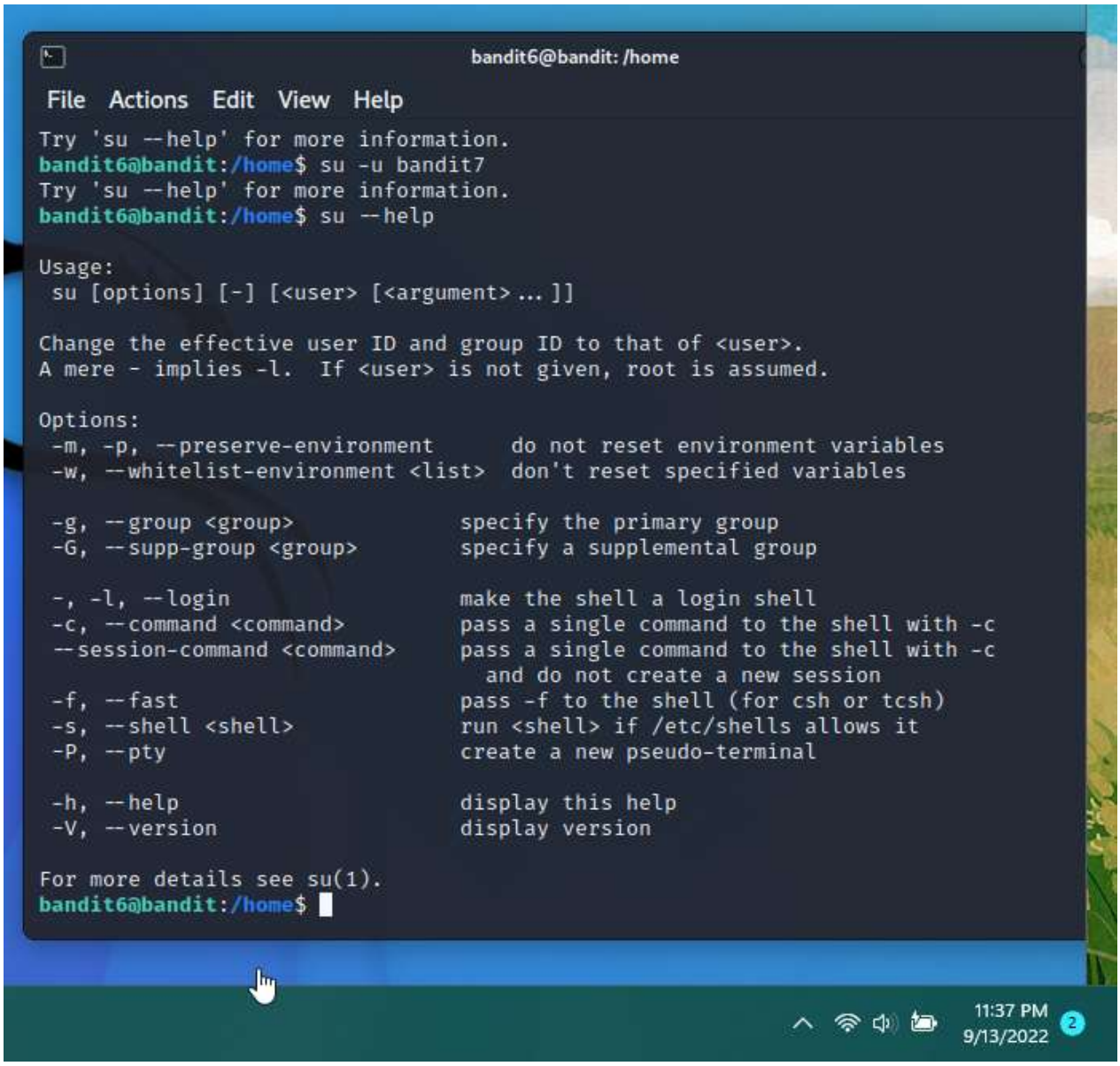
1. Log into the VM as kali/kali
2. 

3. Bandit 6 password P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

4. 

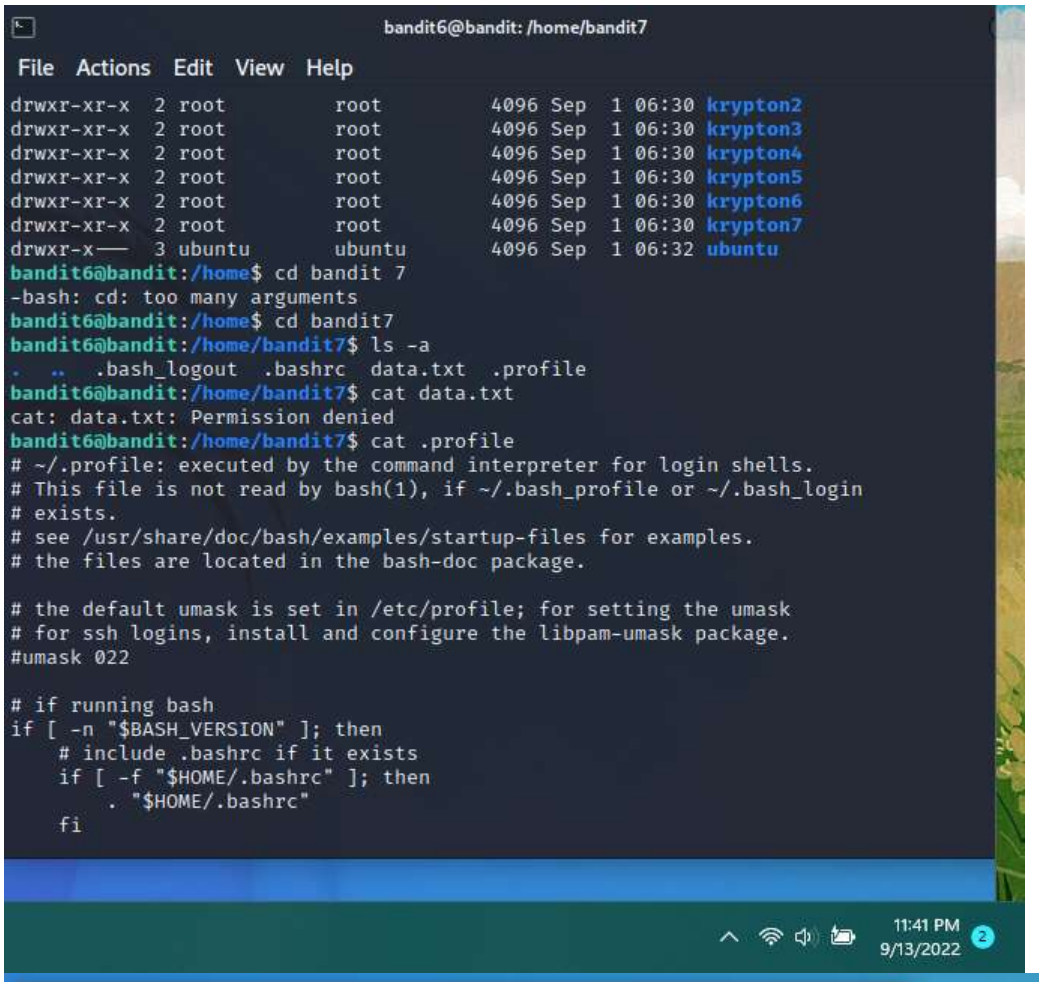
5. 

6. Ls -a cat .profile see info

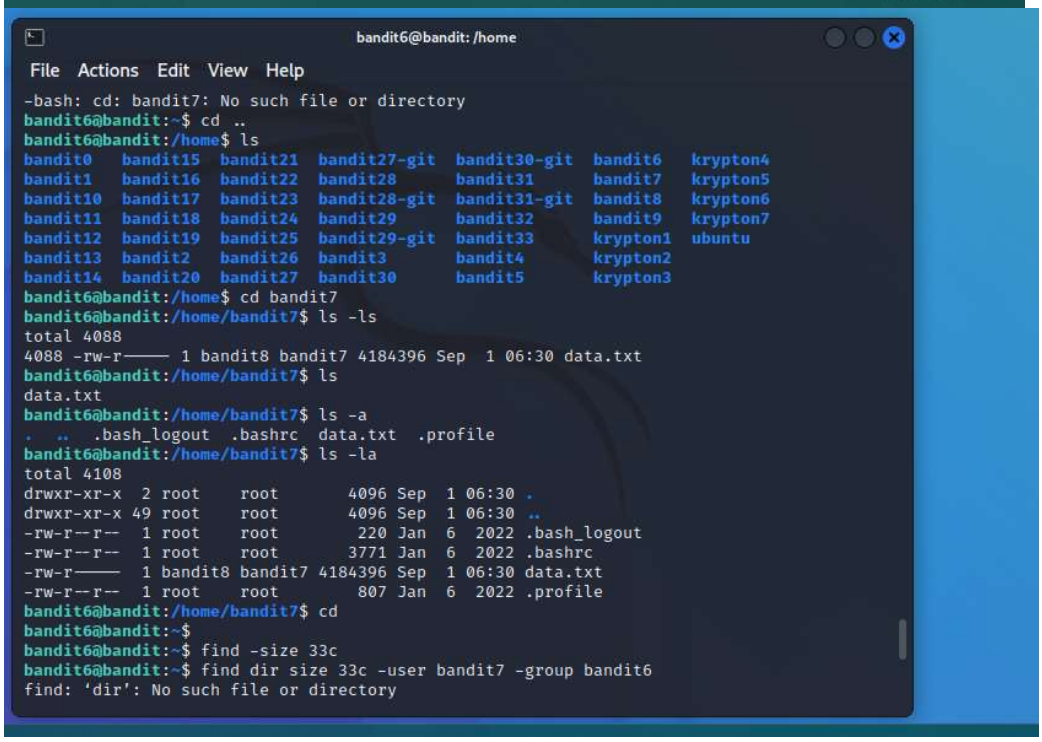
7. 

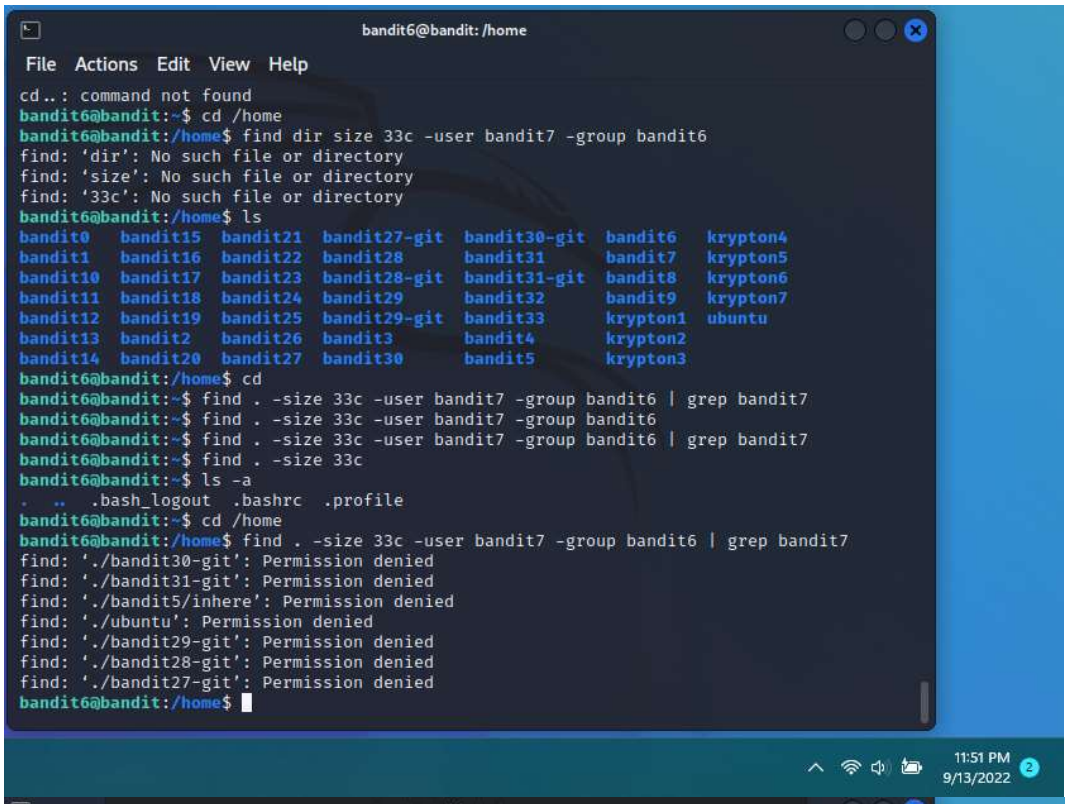
8. Su –help cd .. into home dir

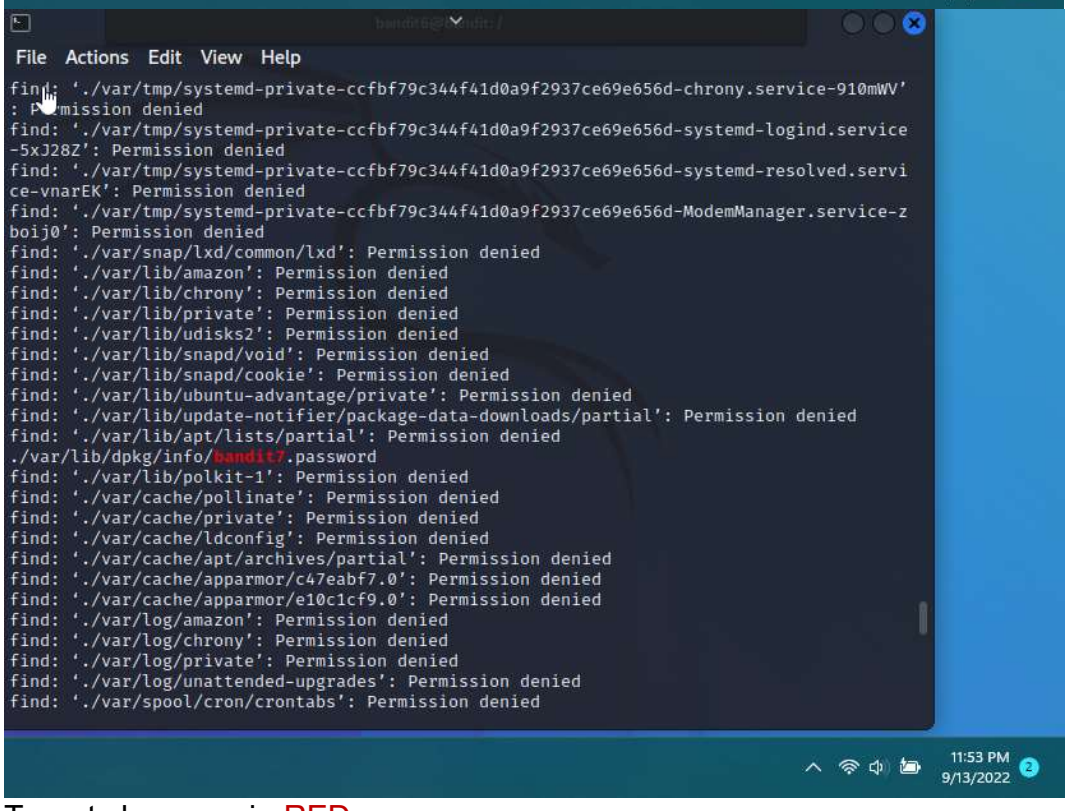
9.


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
11:41 PM
9/13/2022

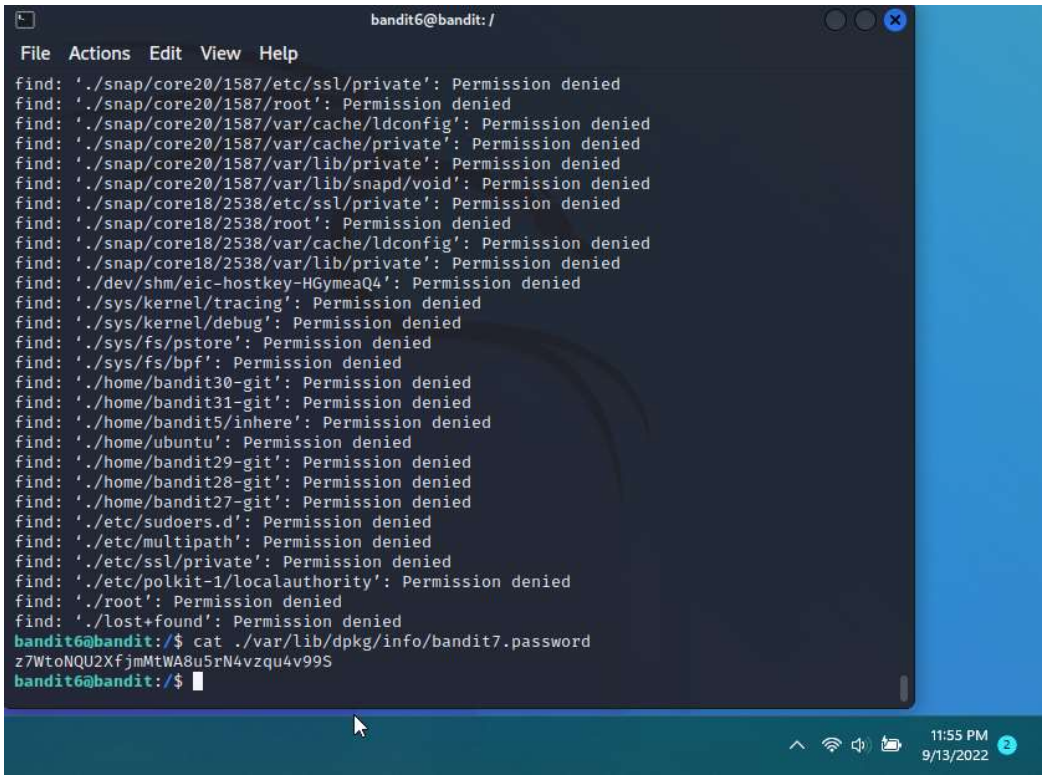
10.


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

11. 

12. 

13. Target shows up in RED

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

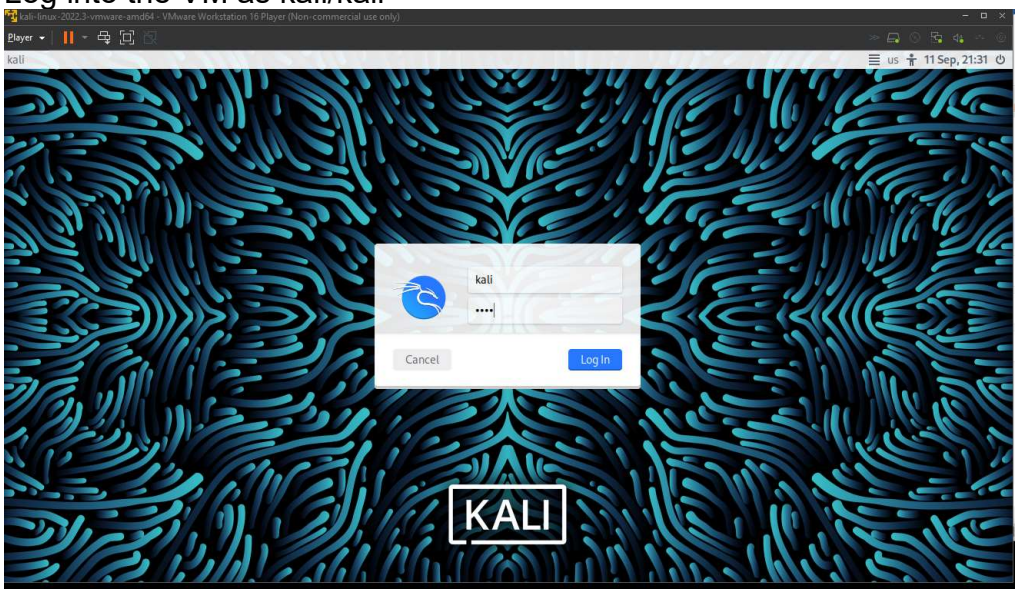
The Over the Wire Exercise Teaches valuable Linux and Penetration Testing skills. In levels 7 to 8, the end user will learn valuable SSH (Secure Shell) and more advanced Linux commands. The file is a hidden millionth string file on the Linux system. The end user will have to discover where. The file 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.*

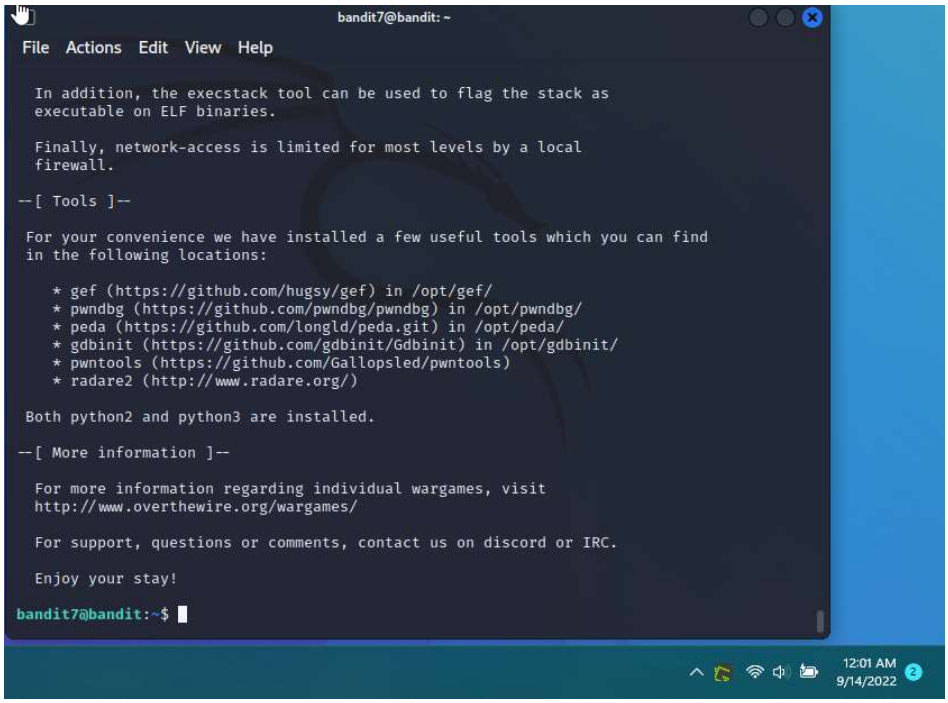
Methodology

Results

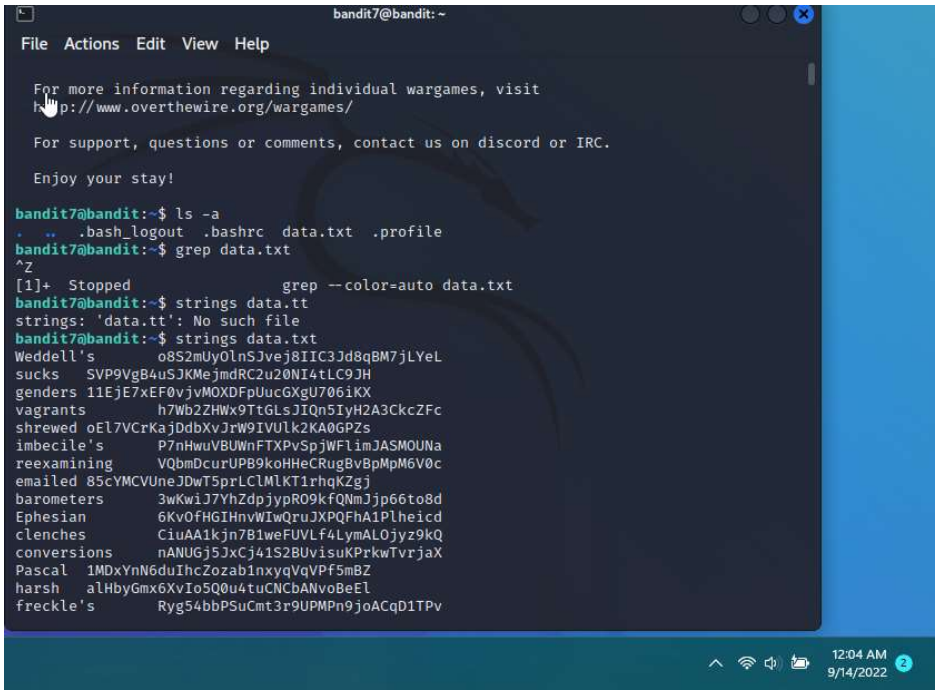
1. Log into the VM as kali/kali
2. 

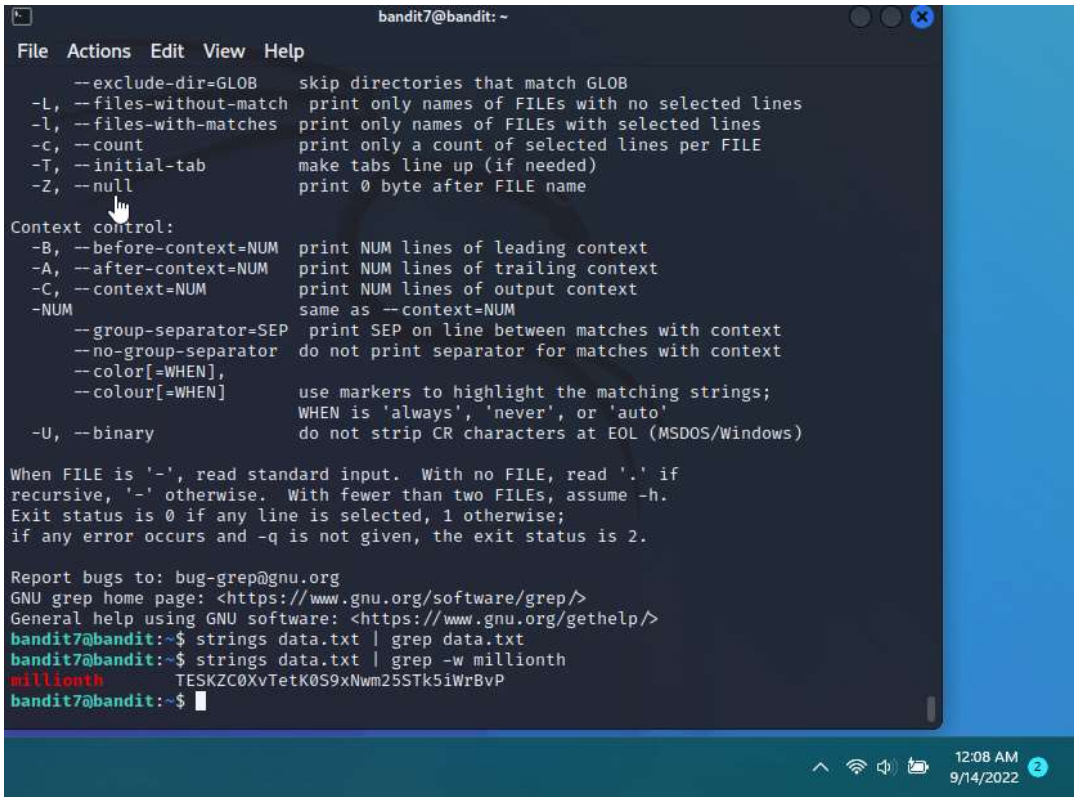
3. Bandit 7 Password z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

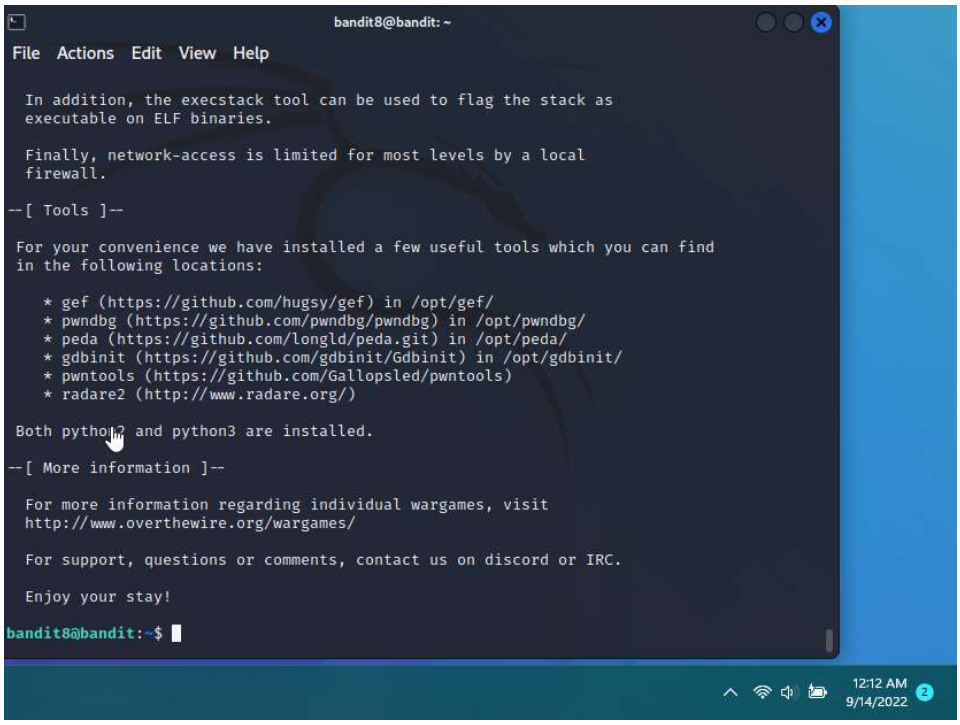
4.


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:~$
12:01 AM
9/14/2022

5.


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 -a
. .. .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 o8S2mUyOlnSJvej8IIC3Jd8qBM7jLYeL
sucks SVP9VgB4uSJKMejmdRC2u20NI4tLC9JH
genders 11EjE7xEF0vjvMOXDFpUucGXgU706iKX
vagrants h7Wb2ZHWx9TtGLsJIQn5IyH2A3CkcZFc
shrewed oEl7VCrKajDdbXvJrW9IVUlk2KA0GPZs
imbecile's P7nHwuVBUWnFTXPvSpjWFlimJASMOUNa
reexamining VQbmDcurUPB9koHHeCRugBvBpMpM6V0c
emailed 85cYMCVUneJDwT5prLClMlkT1rhqKZgj
barometers 3wKwiJ7YhZdpjypRO9kfQNmJjp66to8d
Ephesian 6KvOfHGIHnvWIwQruJXPQFhA1Plheicd
clenches CiuAA1kjn7B1weFUVLf4LymALOjyz9kQ
conversions nANUGj5JxCj41S2BUvisuKPrkwTvrjaX
Pascal 1MDxYnN6duIhcZozab1nxyqVqVPf5mBZ
harsh alHbyGmx6XvIo5Q0u4tuCNCbANvoBeEl
freckle's Ryg54bbPSuCmt3r9UPMPn9joACqD1TPv
12:04 AM
9/14/2022

6. 

7. – help gave the solution
8. Password for millionth TESKZC0XvTetK0S9xNwm25STk5iWrBvP
9. 

The College of Saint Rose

ETHICAL HACKING REPORT
ASSIGNMENT # 1 BANDIT 9

JASON GIBSON Gibsonj421@Strose.edu

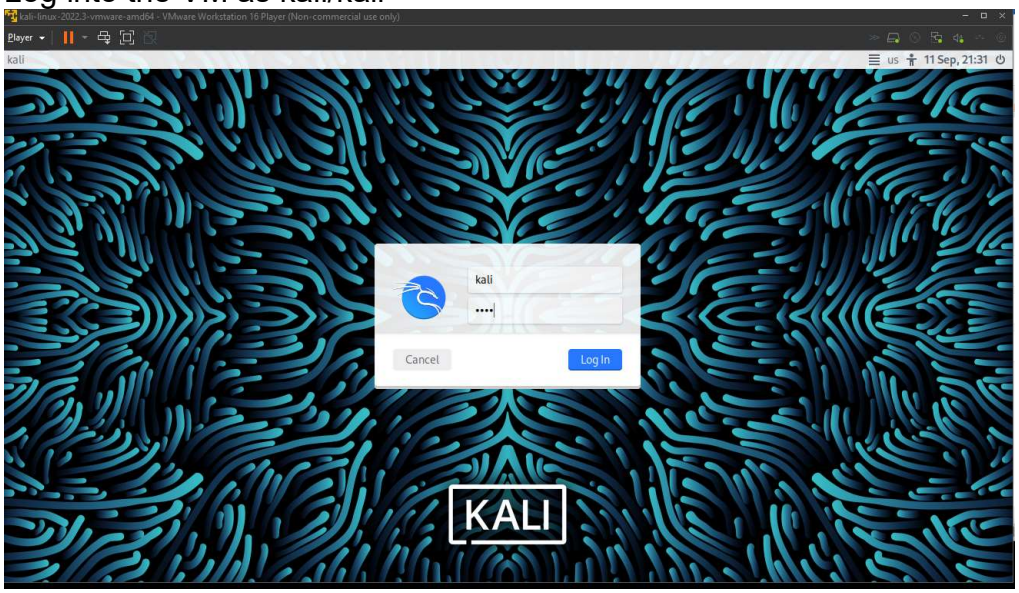
Scope of the assignment

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.*

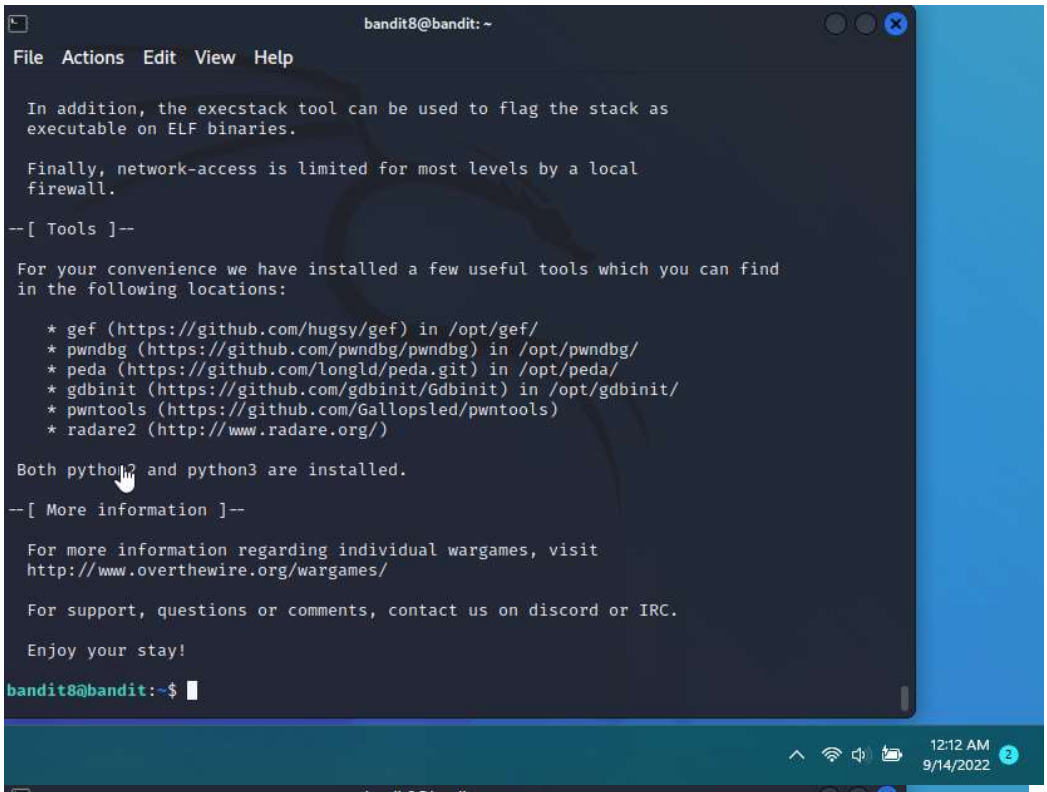
Methodology

Results

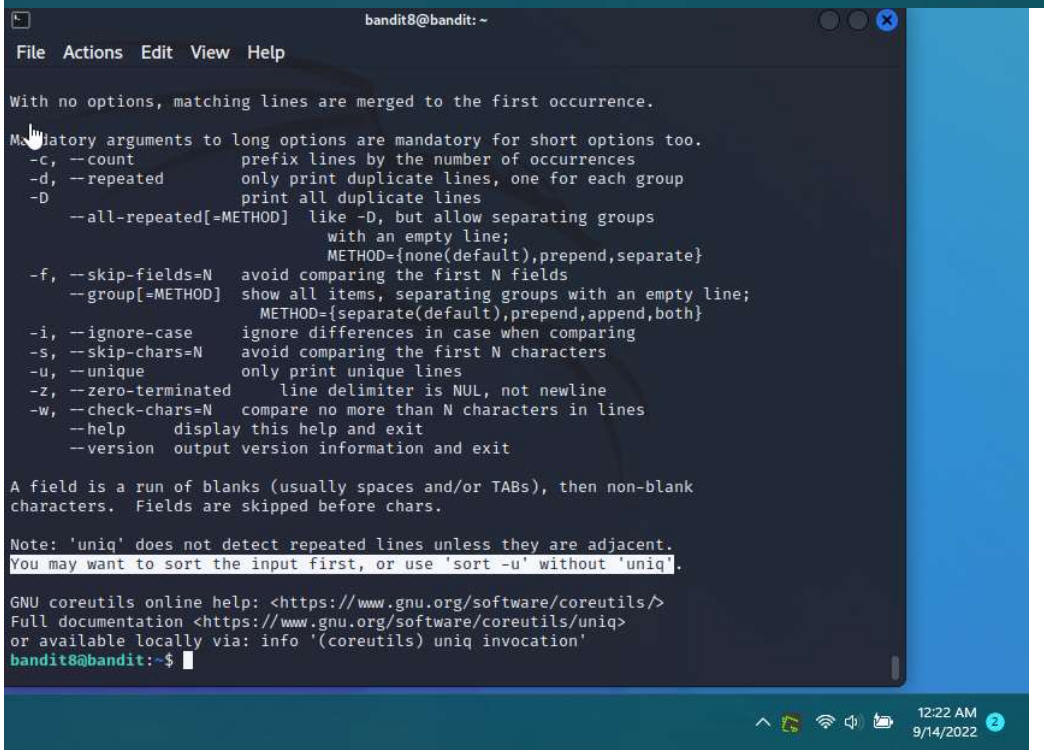
1. Log into the VM as kali/kali
2. 

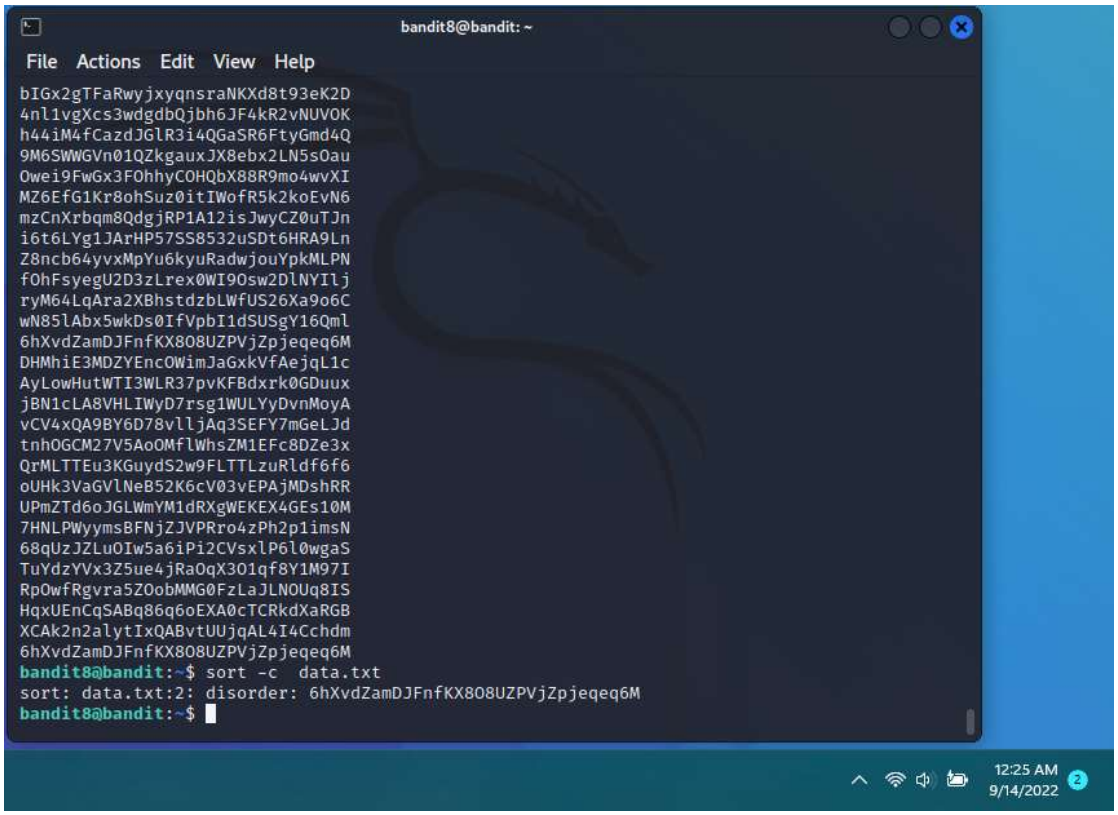
3. Bandit 8 Password TESKZC0XvTetK0S9xNwm25STk5iWrBvP

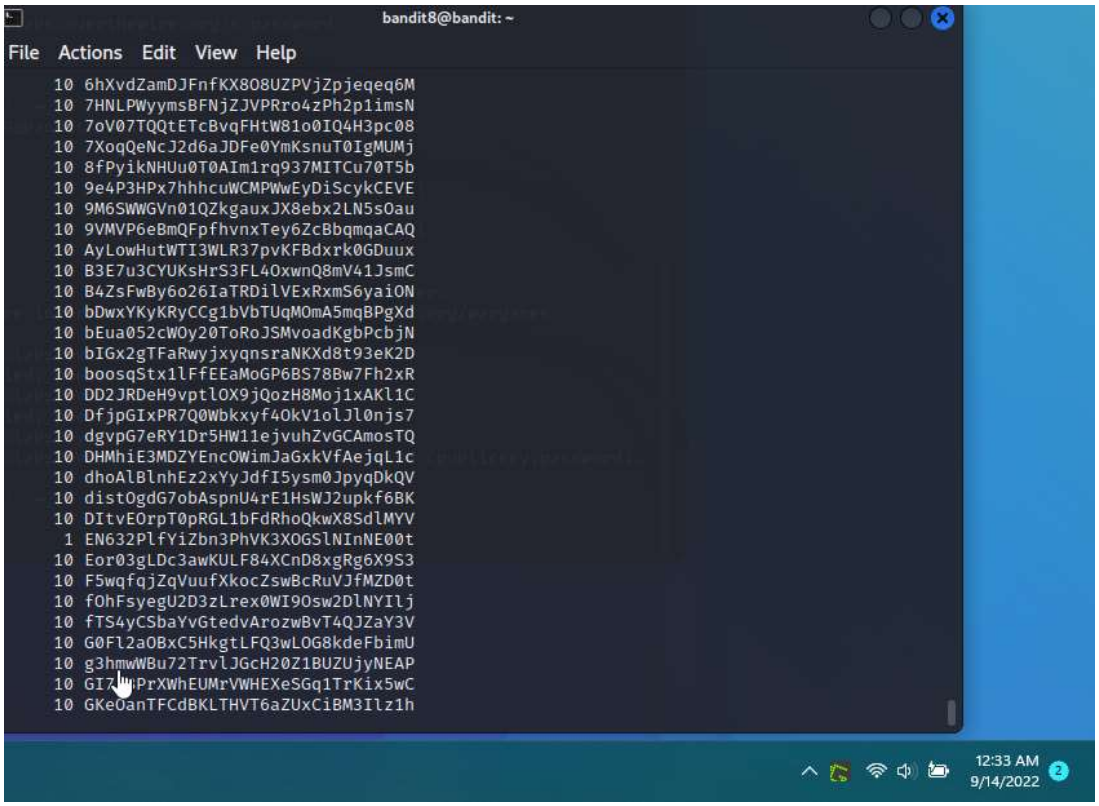
4.


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:~$
12:12 AM
9/14/2022

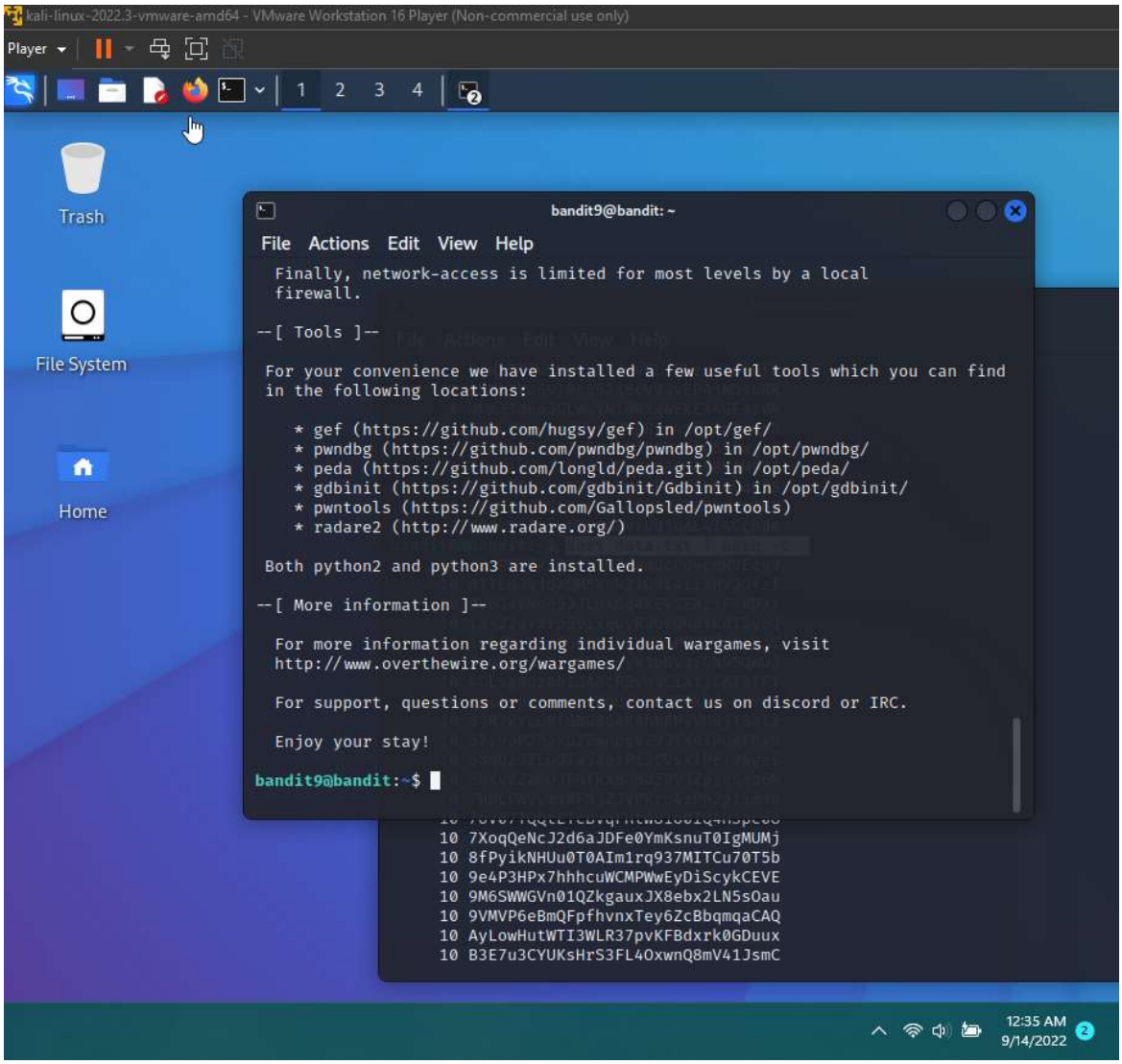
5.


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:~$
12:22 AM
9/14/2022

6. 

7. That was not the currect data
8. 

9. EN632PlfYiZbn3PhVK3XOGSlNInNE00t only occurs once
10. sort data.txt | uniq -c was the command I used.

11. 
kali-linux-2022.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
Trash
File System
Home
bandit9@bandit: ~
File Actions Edit View Help
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!
bandit9@bandit:~$
10 7XoqQeNcJ2d6aJDFe0YmKsnuT0IgMUMj
10 8fPyikNHUu0T0AIm1rq937MITCu70T5b
10 9e4P3HPx7hhhcuWCMPWwEyDiScykCEVE
10 9M6SWWGVn01QZkgauxJX8ebx2LN5sOau
10 9VMVP6eBmQFpfhvnxTey6ZcBbqmqaCAQ
10 AyLowHutWTI3WLR37pvKFBdxrk0GDuux
10 B3E7u3CYUKsHrS3FL4OxwnQ8mV41JsmC
12:35 AM
9/14/2022

The College of Saint Rose

ETHICAL HACKING REPORT
ASSIGNMENT # 1 BANDIT 10

JASON GIBSON Gibsonj421@Strose.edu

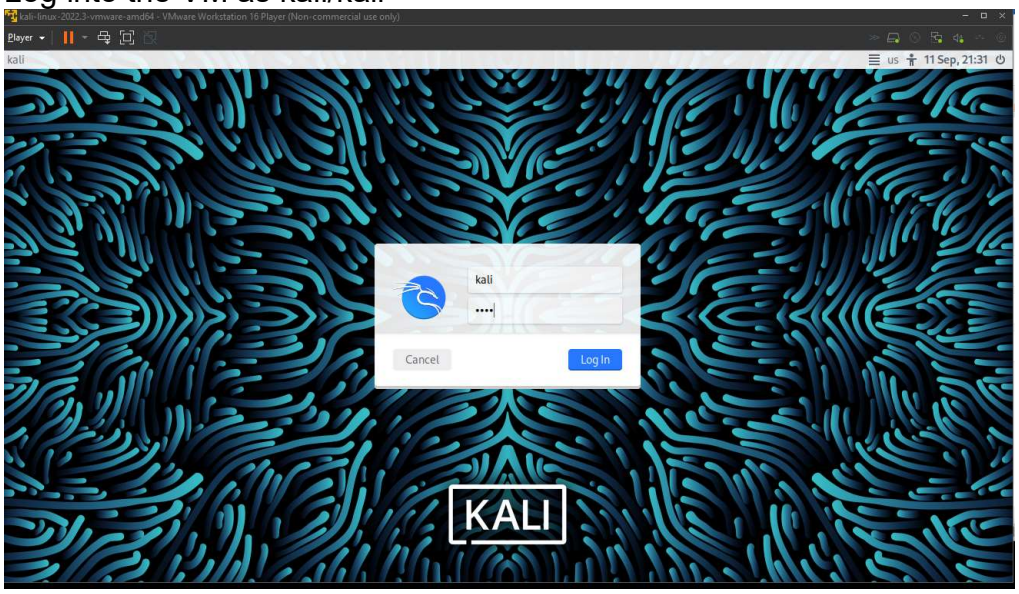
Scope of the assignment

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.

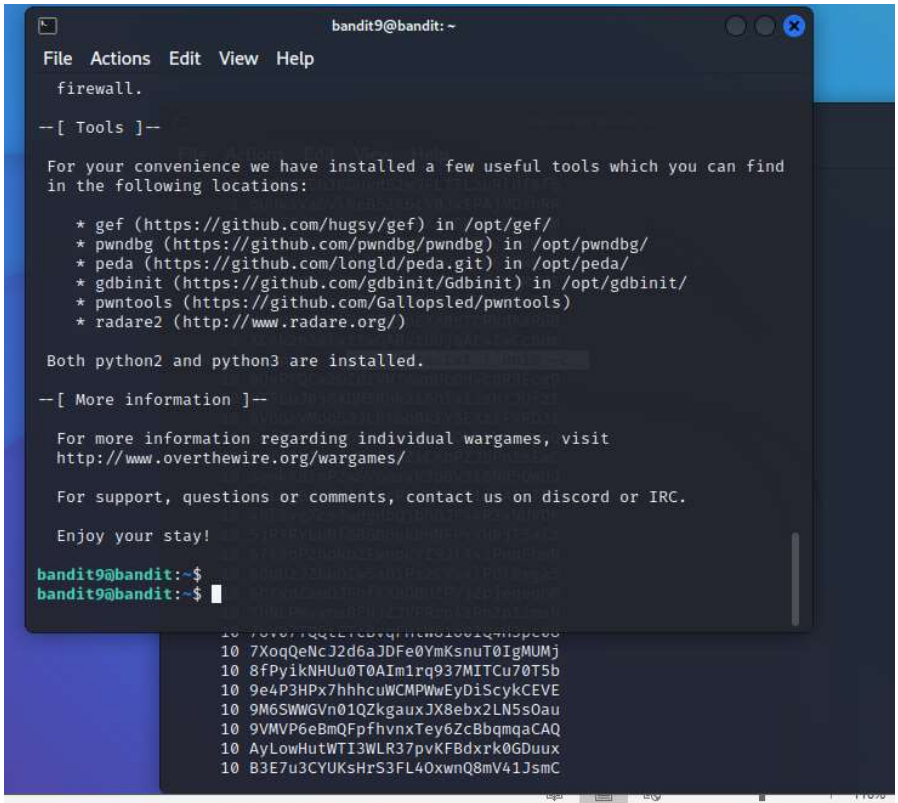
- *The tools needed will be a VM running a Linux distro (Kali).*
- *A terminal prompt.*
- *The Website https://overthewire.org/wargames/bandit/bandit10.html*
- *The following Linux commands ls - list files ls -a, ls la, list all files including hidden files, cd (change directory), copy, paste, uniq,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

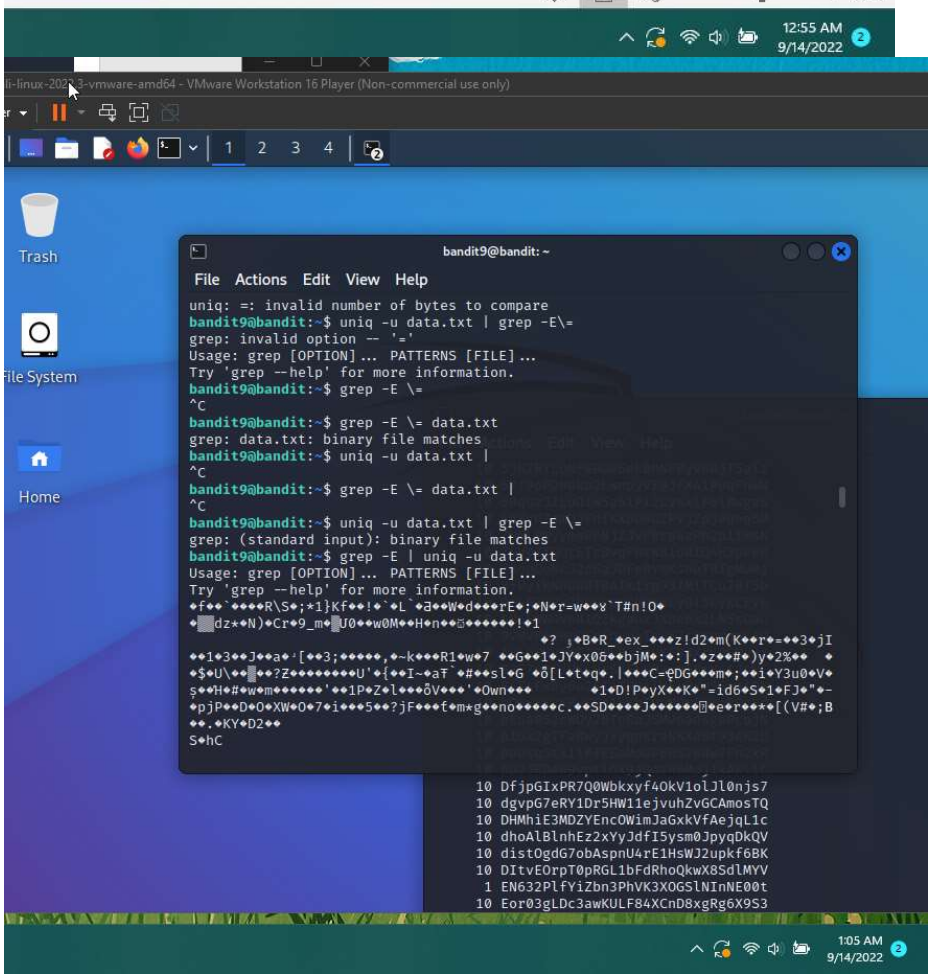
Methodology

Results

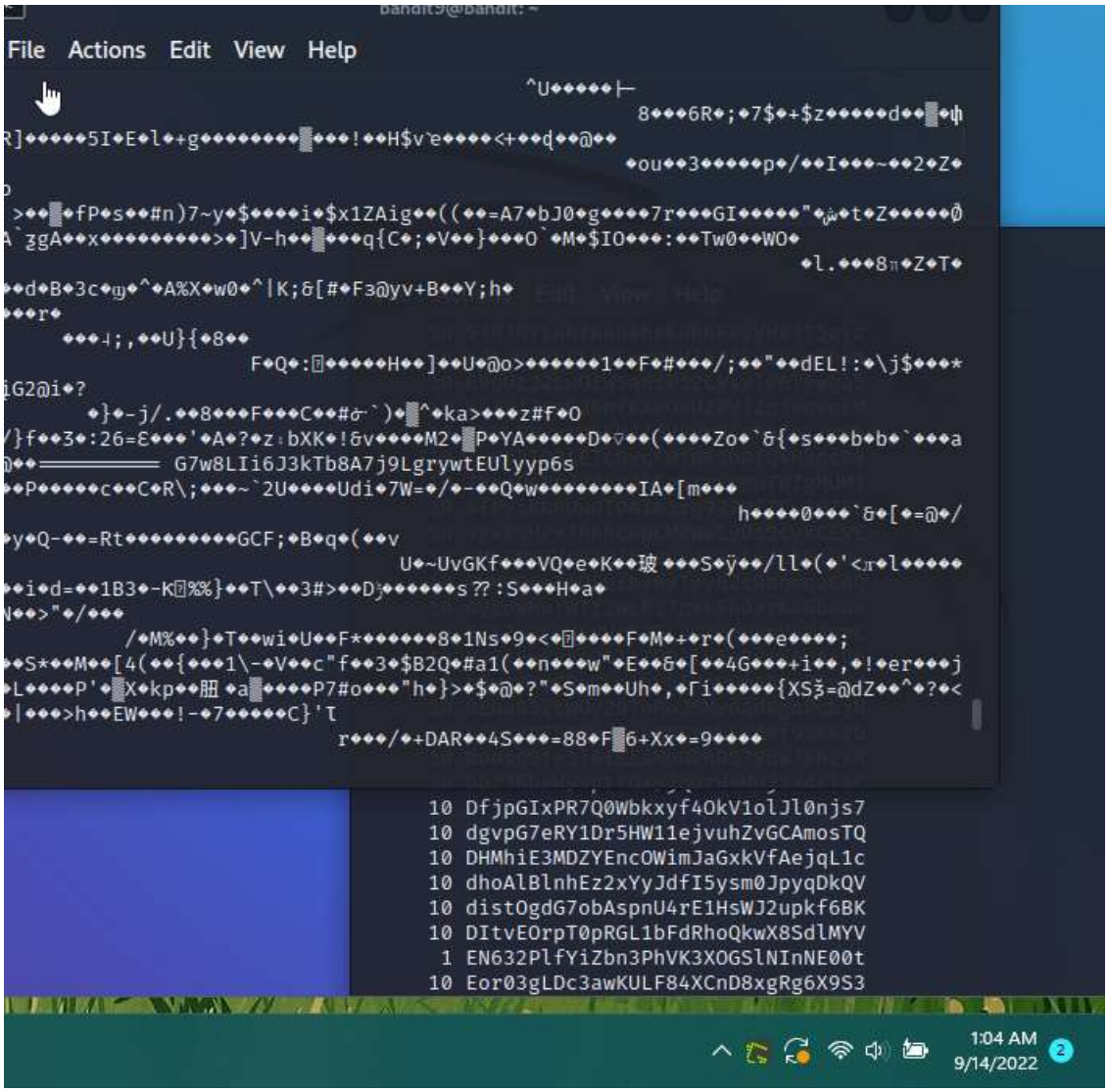
1. Log into the VM as kali/kali
2. 

3. Bandit 9 Password EN632PlfYiZbn3PhVK3XOGSlNInNE00t

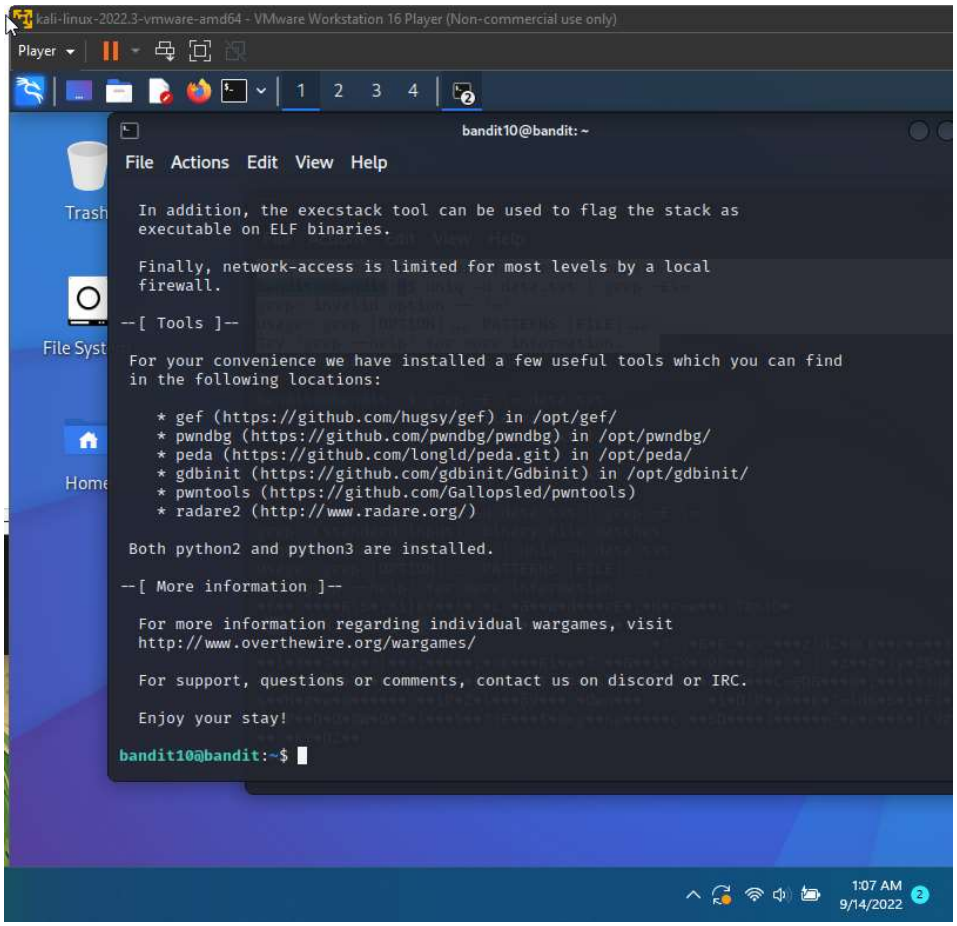


4. 

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.


24.
25. Possible for bandit 10 G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

26. 

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