**ISHWIN KUMAR**

**ASSIGNMENT**

**OverTheWire Bandit Game**

***LEVEL 0:***

*Command: ssh bandit0@bandit.labs.overthewire.org -p 2220*

*Then I entered the password which is Bandit0. SSh helps you connect you to another server over the internet.*

***LEVEL 0-1:***

*Command:*

*ls -la(to list all the files)*

*cat readme (to find password of the next level from readme file)*

*ssh bandit1@localhost (to enter the next level)*

***LEVEL 1-2:***

*ls (to find the '-' file)*

*cat ./- (to find the password for nxt level)*

*ssh bandit2@localhost (to enter 2nd level)*

***LEVEL 2-3:***

*ls (to find the '-' file)*

*cat 'spaces in this filename' (to find the password for nxt level)(here we enclosed in quotes)*

*ssh bandit3@localhost (to enter 3rd level)*

***LEVEL 3-4:***

*ls (to find the inhere directory)*

*cd inhere (we use cd to traverse the directory)*

*ls -al (to show all files)*

*cat .hidden (to find the password for nxt level in the hidden file)*

*ssh bandit4@localhost (to enter 4th level)*

***LEVEL 4-5:***

*ls (we find directory inhere)*

*cd inhere/ (traverse this directory to find files)*

*ls (list all files)*

*file ./\* (to find which file contains most readable text)*

*that is file 07*

*cat ./-file07 (to find pswd)*

*ssh bandit5@localhost (to enter 5th level)*

***LEVEL 5-6:***

*ls (we find directory inhere)*

*cd inhere/ (traverse this directory to find files)*

*ls (list all files)*

*file . -size 1033c (to find file with size of 1033 bytes)*

*cat .maybehere07/.file02 (to find pswd)*

*ssh bandit6@localhost*

***LEVEL 6-7:***

*We are told that next pswd is somewhere on server.*

*We are hinted that user of file is bandit07 and is part of group bandit06*

*find -user bandit7 -group bandit6 -size 33c.*

*From this we know that bandit07 contains credentials.*

*cat /var/lib/dpkg/info/bandit7.password (reads pswd)*

*ssh bandit7@localhost (enter nxt level)*

***LEVEL 7-8:***

*ls (pswd for next level is stored in data.txt)*

*cat data.txt (pswd is next to the word millionth in this file)g*

*grep millionth (to find millionth word)*

*we get the password*

*ssh bandit8@localhost (enter nxt level)*

***LEVEL 7-8:***

*ls (pswd for next level is stored in data.txt)*

*cat data.txt (pswd is next to the word millionth in this file)g*

*grep millionth (to find millionth word)*

*we get the password*

*ssh bandit8@localhost (enter nxt level)*

***LEVEL 8-9:***

*pswd is stored inside data.txt. It is hinted that the password is the only line of text that occurs only once. Srt command to sort the text inside the data.txt file was used.The file had multiple repeating words so uniq was used.*

*Commands: ls, cat data.txt | sort |uniq -u*

*ssh bandit9@localhost.txt*

***LEVEL 9-10:***

*Pswd is followed by '=' cahracetrs.*

*Commands:*

*ls*

*strings data.txt | grep =*

*(we get the pswd)*

*ssh bandit10@localhost*

***LEVEL 10-11:***

*Pswd is encrypted in base64. Using the base64 decode command we get the pswd.*

*Commands:*

*ls*

*cat data.txt | base64 --decode*

*ssh bandit11@localhost*

***LEVEL 11-12:***

*Pswd has changed the format of letters in such a way that all the lowercase and uppercase letters have been rotated by 13 positions. This is what happens in ROT 13 encryption. We use the 'tr' command to convert.*

*ls*

*cat data.txt | tr a-zA-Z n-za-mN-ZA-M*

*ssh bandit12@localhost*