Bandit 0 Learning: ssh **-p** This is an option that allows the user to enter a specific port the number to ssh into

Bandit 1: Using a – as a filename is standard notation indicating stdin and stdout. Using the command cat does not recognise – as a filename and treats it as a synonym for stdin. We can get around this by prefixing the name with the **full path**. (i.e. Including the ./ or the /home/John/ prior to the – file itself) In addition, you can copy text from the command line: ctrl+insert to copy shift+insert to paste.

Bandit 5: find . -type f -size 1033c ! -executable

find / 🡪 will find every path -group (specific group name) -name (name owner)

gzip, tar are tools for decompressing files. We can use file [filename] to identify the type of file that we are attempting to decompress.

We can use a private key create a ssh connection:

Ssh -I [Which indicates the private key]🡪sshkey.private bandit14@localhost

I am unsure whether localhost is necessary. I have been using the standard version of logging into ssh servers when in a CURRENT ssh session; however, I would time out. Does using localhost establish a ssh connection when in an existing session? It appears so!

Can we use nc? “It is designed to be a reliable ‘back-end’ tool.” Apparently, this works: echo ‘password’ | nc localhost 30000

Level 15 Notes: The next level required utilising the openssl command. The openssl command offers tools to manage private keys? The necessary flags included -ign\_eof which prevents the connection from closing once it is established. The -connect command connects to the server. Localhost:30001 is the appropriate port to connect to. (Don’t forget the the s\_client addition)

Nmap -p 31000-32000 localhost 🡪 used to scan for all open ports within the range of 31000 – 32000

Connect to the port with 🡪 openssl s\_client -ign\_eof -connect localhost:{port number}

By adding the -T option to the beginning of the ssh command, one could ‘force’ a psudo terminal from opening despite the fact that the connection is forcefully closed in the .bashrc file.

Bandit19-> We are given a binary file that was created under the user Bandit20. In addition, the binary file polymorphs the current user into one a Bandit20 user thus giving the current user access to files outside their permissions.

Bandit 20 -> echo “password” | nc -l -p 60000 This command tells the machine to listen to traffic on the port 60000. Once the binary file is executed, the executable sends the new password through this port.

Bandit 21 -> Small lesson to learn, you cannot use the autocorrect feature (i.e. the tab button) when in a directory in which you do not have access to. However, if you have a file that is readable, you can cat the individual file.