

Offensive Penetration Testing Module 2 Lesson 2.1

Description: In this lab we will look at basic Linux commands in Kali

Requirements: Just the Kali VM open

Step 1: Have terminal open on Kali (or your favourite Linux box, but we'll probably be using Kali)

Step 2: You can run the command **updatedb** but you'll have to wait a while (it's a big command)

Step 3: Run **locate** command (to find a file, he uses a file called word.txt)

Step 4: If you have or make a file called word.txt, using the **locate** command will tell you where it is

Step 5: The **-c** option can specify what you want to search for (for example .txt files) and it'll tell you how many you have. This won't tell you where they are, just how many you have.

Step 6: The **-i** option mean it's case insensitive. This will bring up location paths of such files.

Step 7: The **-S** option shows how many files and directories you have currently, as per the updated file database.

Step 8: The **-r** command is to look for a specific file. For example the exact word.txt file. If you don't have it, it won't show up

Step 9: **locate -r /word.txt\$** --- like so to look specifically for the word.txt file

- The **-n** option limits the amount of results you get
- For example:

Step 1: **locate "*.py" -n 20** gives you the first 20 results of files with the .py extension

- The **which** command is a useful command in Linux.
- It can help you find a specific app or program

Step 1: For example, when you type **which bash** it'll tell you where the bash shell is.

Step 2: **which python**, whether the python language is installed, and so on

Step 3: Another instructor example is the **-a** option like so

Step 4: **which -a john**

- This will tell you all the places a specific program is installed (in this case john)

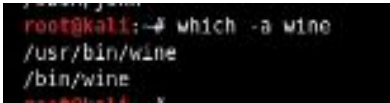
```
root@kali:~# which john
/usr/sbin/john
root@kali:~# which -a john
/usr/sbin/john
/sbin/john
```

- john example

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

-  wine example
- You can also use the **whereis** command instead of **which**

Step 10: The **find** command

- Useful for looking for suid files
- And of course has the same abilities as the **which** and **whereis** commands

Step 1: Example: **find /root/Documents/** gives a list of all the files in that folder

- You can also use **find** to look up a specific file by name

Step 2: **find / -name Start.py** (for example)

Step 3: If you run **find / -name "*.py"** you will get a list of **all** the python files in your computer. All of them.

Step 4: For even more options for the **find** command you can look into the manual pages.

Much better than **which** and **whereis**.

Step 5: **find / -maxdepth 2 -name "*.html"**

- This will only search 2 directories depth for all html files.

Step 6: **find / -maxdepth 4 -name "*.html"** will search 4 directories depth.

- And the **-perm** option is used to find files with specific permissions (for example suid files)

Step 7: **find / -type f -perm 0664** for example

Step 8: **find / -atime 50** finds files that were accessed in the last 50 days

Step 9: **find / -size 50m** finds files that are 50 megabytes

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Offensive Penetration Testing Module 2 Lesson 2.2

Description: In this lab we will look at services you can use in Kali for pentesting

Requirements: Just the Kali VM open

Step 1: Ifconfig to check ip

- First service: ssh

Step 2: ssh 10.211.55.7 (the instructor's test windows box for example, but you can put in your own test ip of the box you want to access, if you have a testing lab.)

Step 3: It will prompt for a password, write in that password

- You should be taken to a ssh shell of that box. You can now access that box, run commands on it, etc etc.
- By default ssh will default to root@whateverip even if the box you're trying to access doesn't have a root user.

Step 4: So use the -l option to specify a username. Or you can type the username@ipordomain in the ssh command

Step 5: ssh username@ip (10.211.55.7 for example) and you will still get the password prompt

Step 6: Type in your password

Step 7: You should get a shell to the box. (a command prompt in this case for the windows box)

Step 8: In this windows box you can type ipconfig to check ip and network info and whoami for finding out what user you're logged in as

Step 9: Type exit to get out of the ssh shell.

- You will be taken back to you kali terminal.

Step 10: You can specify a port with the -p option, in case the box you're accessing or testing does not have their ssh service on port 22 as it is generally the case.

- Another thing about ssh is you don't have to use a password to log in to the box you're accessing. And sometimes you won't get a password if you're testing boxes or doing ctfs and whatnot.
- What you can do is use ssh keys/ certificates to log in with the -i option.
- Generally using an id_rsa key to log in.

Step 11: Like so: ssh username@ip -i id_rsa

Step 12: It might still prompt you for a password, for example if the ssh key was encrypted. But it generally won't if you use an ssh key.

- You can actually generate your own ssh keys with the ssh-keygen command.

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Step 13: Like so: ssh-keygen

- You can also execute commands without logging to the terminal

```
root@kali:~/Desktop/Files# ssh alejandroguinea@10.211.55.7 "ipconfig"
alejandroguinea@10.211.55.7's password:
```

Step 14:

- Like so.
- Example on how you can use that in a pentesting way

Step 15:

```
Default Gateway . . . . . : 10.211.55.1
root@kali:~/Desktop/Files# ssh alejandroguinea@10.211.55.7 "net user alejandroguinea password"
```

- You can change the password without actively being logged in to the ssh shell.
- The -c option compresses the traffic. Useful if you have limited bandwidth or want to stay stealthy.

Step 16:

```
root@kali:~/Desktop/Files# ssh -C 10.211.5.7
```

- Ssh can also be used for port forwarding (something people do a lot in ctf's).

Step 17: Ssh -L port1:host1:port2 host2 for example (-L is local port)

- An example:

Step 18:

```
root@kali:~/Desktop/Files# ssh -L 2222:google.com:80 alejandroguinea@10.211.55.7
alejandroguinea@10.211.55.7's password:
```

- There's also remote port forwarding (the -R option, where you port forward to the box you want to access)
- Local port forwarding is forwarding a port out, so it can be accessed outside the box.
- There is also the scp command.
- Scp is used when you have access to box's ssh and you want to transfer files over.
- For example transfer a file to the box from your local machine.

Step 19:

```
ish.py fuz.py javascript.txt pocC1SSP.py poc.py rvs.php start.py wordlist.txt
p/Files# scp /root/Desktop/Files/javascript.txt alejandroguinea@10.211.55.7:"C:\Users\alejandroguinea\Desktop"
.211.55.7's password:
```

- Command was a little long but basically it's copying the javascript.txt file from the first path to the ssh shell and specifying a target path in which the file will be transferred (the second path)

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Step 20:

```
root@kali:~/Desktop/Files# scp /root/Desktop/Files/javascript.txt alejandroguinea@10.211.55.7:"C:\Users\alejandroguinea\Desktop"
alejandroguinea@10.211.55.7's password:
^Croot@kali:~/Desktop/Files# scp /root/Desktop/Files/javascript.txt alejandroguinea@10.211.55.7:"C:\Users\alejandroguinea\Desktop"
alejandroguinea@10.211.55.7's password:
javascript.txt
root@kali:~/Desktop/Files#
```

- The result of the scp command.
- The command here is:

Step 21: `Scp /root/Desktop/Files/javascript.txt username@ip: "C:\Users\youruser\Desktop"`

Step 22: Type in your password.

- And then you will get the name of the file back. This means its sent successfully to the other box
- You can actually do it backwards too

```
root@kali:~/Desktop/Files# scp -T alejandroguinea@10.211.55.7:"C:\Users\alejandroguinea\Desktop\test.txt" /root/Desktop/Files/
alejandroguinea@10.211.55.7's password:
test.txt
root@kali:~/Desktop/Files#
```

- The command is :

Step 23: `scp -T user@ip: "C:\Users\youruser\Desktop\test.txt"`

`/root/Desktop/Files/`

Step 24: Change the user@ip to whatever username and ip the box you're accessing has.

Step 25: Type in your password

Step 26: And you should get the name of the file back. Transfer complete.

- Another service that is useful is the apache http service
- Here's an example

Step 27:

```
root@kali:~/Desktop/Files# service apache2 start
root@kali:~/Desktop/Files# echo "Hello cybrary students" > /var/www/html/index.html
root@kali:~/Desktop/Files#
```

- Here we start the apache server
- If you go to localhost on your browser you can see the apache starter page.
- The second command sends a message to the index.html page.
- The third service that is useful is the ftp service

Step 28: To connect to the ftp service just type ftp and then the ip address

Step 29: For example `ftp 10.211.55.7`

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

```
Connected to 10.211.55.7.  
220 Microsoft FTP Service  
Name (10.211.55.7:root):
```

•
Step 30: Type in a username to log in as

Step 31: Now it will ask for password. Type in your password.

```
230 User logged in.  
Remote system type is Windows_NT.  
ftp> ls  
200 PORT command successful.  
125 Data connection already open; Transfer starting.  
09-02-19 12:58PM      88116 javascript.txt  
09-02-19 11:35AM          0 test.txt  
226 Transfer complete.  
ftp>
```

- First you should check if ftp supports anonymous log in. Sometimes they do.

Step 32: To log in anonymously just write ftp yourip

Step 33: For the name write anonymous.

Step 34: Then anonymous for the password.

- If it works you should have access to the ftp server as anonymous.
- In the ftp server you can use put or get to get files from the server

Step 35: For example put finish.py will transfer the finish.py from you local box over to the other box.

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Offensive Penetration Testing Module 2 Lesson 2.3

Description: In this lab we will look at managing services in Kali

Requirements: Just the Kali VM open

Step 1: To find service configuration files you go to the etc directory and there you go to the init.d directory

Step 2: Cat etc/init.d/apache2 will give you the info on the apache 2 service configuration such as starting and stopping the service

Step 3: You can also see the status of services with etc/init.d/service status (in place of service write the service you want like ssh for example)

Step 4: To check if it's running write netstat -antp | grep 22
That will look for any services running on port 22 (the ssh)

Step 5: To stop the ssh service write service ssh stop

Step 6: netstat -antp | grep 22 will give nothing now because the ssh service is not running

Step 7: etc/init.d/ssh status will now say the ssh service is inactive .

- Now we need to get a process to start automatically when you open the kali box or restart it. We will use ssh for this example

Step 1: Start the service you

- service ssh start

Step 1: Check the status of the service

- etc/init.d/ssh status (alternatively service ssh status)

Step 1: Now run the update-rc.d command

- update-rc.d ssh enable
- This will enable the ssh service to start by itself when you start or restart Kali. This is called boot persistence.

Step 1: Now disable it

- update-rc.d ssh disable
- Other tools that do the job are rcconf and sysv-rc-conf

Offensive Penetration Testing Module 2 Lesson 2.4

Description: In this lab we will look at bash shell scripts

Requirements: Just the Kali VM open

Step 1: First we print something out

- `echo "Hello cybrary"`
- This will print the string to the command line

Step 2: To remove a file use `rm` file

- For example `rm cybrary.sh` will delete the `cybrary.sh` file (if you have one)
- We will use nano editor to create our bash script

Step 3: Write this at the top of the file once you open nano

- `#!/bin/bash`

Step 4: Next we write the `echo` command from before

- `echo "Hello cybrary"`

Step 5: Save the file and exit

Step 6: To make the file executable use the `chmod` command

- `chmod cybrary.sh 777` will set the file permissions of the `cybrary.sh` file to 777 which will give it executable permission. That is giving all permissions to all users and groups

Step 7: Check the file after running `chmod`

- `ls cybrary.sh`
- The script should now be in green, indicating its an executable file.

Step 8: Because we added the shebang(the `#!/bin/bash`) line to the script now we can just run it as it is

- `./cybrary.sh`
- This will print out the Hello cybrary line.

Next up: While loops

Step 9: Open the `cybrary.sh` file

Step 10: Write `n=1` below the shebang line (`#!/bin/bash`)

Step 11: Now, write this line which will be our loop

- `while [$n -le 5]`

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Step 12: Write do under it

Step 13: Below that write

- echo "Cybrary \$n times!"
- n=\$((n+1))
- done

And there's your loop.

Step 14: Save the file

Step 15: Now we can execute the new script and see if the loop works

- ./cybrary.sh

This is the output of the new while loop

```
root@kali:~/Desktop/Files# ./cybrary.sh
Cybrary 1 times!
Cybrary 2 times!
Cybrary 3 times!
Cybrary 4 times!
Cybrary 5 times!
root@kali:~/Desktop/Files#
```

Next up: For loops

Step 16: Open the cybrary.sh file

Step 17: Write

- for ((counter=0; counter>0; counter--))
- do
- echo -n "\$counter"
- done
- printf "\n"

Step 18: Save the file

Step 19: Execute the script with ./cybrary.sh

Step 20: And here's the output

```
root@kali:~/Desktop/Files# ./cybrary.sh
54321
root@kali:~/Desktop/Files#
```

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Next up: User input

Step 21: Open the cybrary.sh file

Step 22: Write

- echo "Enter your name:"
- read name
- echo "Welcome " \$name "to the Cybrary class"

Step 23: Save the file

Step 24: Execute the script with ./cybrary.sh

Step 25: And here's the output

```
root@kali:~/Desktop/Files# ./cybrary.sh
Enter your name:
Alejandro
Welcome Alejandro to the Cybrary class
root@kali:~/Desktop/Files#
```

Next up: If statements

Step 26: Open the cybrary.sh file

Step 27: Write

- echo "Enter username:"
- read username
- echo "Enter password:"
- read password
- if [[(username== "admin" && password== "secret")]]; then
- echo "valid user"
- else
- echo "invalid user"
- fi

Step 28: Save the file

Step 29: Execute the script with ./cybrary.sh

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Step 30: And here's the output

```
root@kali:~/Desktop/Files# ./cybrary.sh
Enter username
admin
Enter password
secret
valid user
root@kali:~/Desktop/Files#
```

Valid user

```
root@kali:~/Desktop/Files# ./cybrary.sh
Enter username
alejandro
Enter password
secret
invalid user
root@kali:~/Desktop/Files#
```

Invalid user

Next up: Command Line arguments

Step 31: Open the cybrary.sh file

Step 32: Write

- echo "Total arguments :#"
- echo "first argument : \$1"
- echo "second argument: \$2"

Step 33: Save the file

Step 34: Execute the script with ./cybrary.sh

Step 35: And here's the output

```
root@kali:~/Desktop/Files# ./cybrary.sh
Total arguments : 0
1st argument =
2nd argument =
root@kali:~/Desktop/Files# ./cybrary.sh Alejandro Guinea
Total arguments : 2
1st argument = Alejandro
2nd argument = Guinea
root@kali:~/Desktop/Files#
```

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Next up: Tools you can use inside a bash script

Step 36: Open the cybrary.sh file

Step 37: Write

- `if [$# -eq 0]`
- `then`
- `echo "Error: Y0u have to enter a valid ssh server!"`
- `exit 1`
- `else`
- `echo "The DNS used by the server is:"`
- `ssh username@$1 (in this case the instructor alejandroguinea)`
`"ipconfig -all" | grep DNS`
- `fi`

Step 38: Save the file

Step 39: Execute the script with `./cybrary.sh`

Step 40: And here's the output

```
root@kali:~/Desktop/Files# ./cybrary.sh
Error: You have to enter a valid ssh server
root@kali:~/Desktop/Files# ./cybrary.sh 10.211.55.7
The DNS being used by the server is:
alejandroguinea@10.211.55.7's password:
DNS Suffix Search List. . . . . : localdomain
Connection-specific DNS Suffix . : localdomain
DNS Servers . . . . . : 10.211.55.1
```

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Offensive Penetration Testing Module 2 Lesson 2.5

Description:

Objective is to learn how to combine multiple commands in a single line using the terminal of Kali Linux. Please watch the lesson videos to understand the usefulness of doing the same, especially when you have taken control on a remote machine.

We will go on each command one by one and then will put all commands in a single line in the last step on the Terminal.

Requirements:

1. Access to the OSCP Lab / course
2. Kali Linux and its terminal
3. Knowledge on basic Linux commands such as updatedb, cat, wget, locate, find, which, whereis, tr, awk etc.
4. Knowledge on redirection symbols such as `|` [pipe] and `>` [greater than]
5. Complete Lesson 2.4 - Shell and bash Scripts for more details.

Note : Single and Double quotes have been cleaned up in commands given in the example. Nevertheless, please take care of the single and double quotes in the commands if you get error in your terminal if you copy pasted it

Step 1: Use wget to download a list of names from a url
The file will be downloaded to the current directory

```
wget https://raw.githubusercontent.com/dominictarr/random-name/master/first-names.txt
```

Step 2: Use cat command to see the content of the file

```
cat first-names.txt
```

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Step 3: Combine cat command from the previous step with tr command to convert uppercase letters to lowercase

```
cat first-names.txt | tr '[:upper:]' '[:lower:]'
```

Step 4: Combine head command with the commands used in the previous step to filter the top 20 names

```
cat first-names.txt | tr '[:upper:]' '[:lower:]' | head -n 20
```

Step 5 (Optional): If you are using Kali as the guest OS on a MacOS host, Combine **dos2unix** command with the commands from the previous step to remove hidden carriage return from the previous output.

```
cat first-names.txt | tr '[:upper:]' '[:lower:]' | head -n 20 | dos2unix
```

Step 6: Combine awk command with the commands from the previous step to prepend each line with “www.” and append with “.com”.

```
cat first-names.txt | tr '[:upper:]' '[:lower:]' | head -n 20 | dos2unix | awk '$0="www."$0".com"'
```

Step 7: Enclose all of the list in the previous command with backticks as it would execute the list of commands given above, when we use a **for loop** as shown below

```
for i in `cat first-names.txt | tr '[:upper:]' '[:lower:]' | head -n 20 | dos2unix | awk '$0="www."$0".com"'`;do host $i;done
```

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Step 8: Use awk with the line from the previous step to filter the relevant output

```
for i in `cat first-names.txt | tr '[:upper:]' '[:lower:]' | head -n 20 | dos2unix | awk '$0="www."$0".com"'` ;do host $i;done | awk '/has address/{print $4}'
```

Note : please do not misuse the list of IP's as the output shows the list of public IP's

Step 7: Save the list of IP's to a file using > symbol

```
for i in `cat first-names.txt | tr '[:upper:]' '[:lower:]' | head -n 20 | dos2unix | awk '$0="www."$0".com"'` ;do host $i;done | awk '/has address/{print $4}' > ips.txt
```

Lab Questions - Lesson 2.5 -

Question 1: What is executed by the **wget** command ?

Wget helps in downloading files from a given url. For example, we used it to download the list of names.

Question 2: What is the result of executing the **head -n 20** command ?

head -n 20 helps in getting the first 20 lines from a given file or the output.

Question 3: Can you use actually use a **for loop** directly in a terminal ?

Yes we can use for loop directly in the terminal. We have used it as shown in the steps in the Lesson.

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.