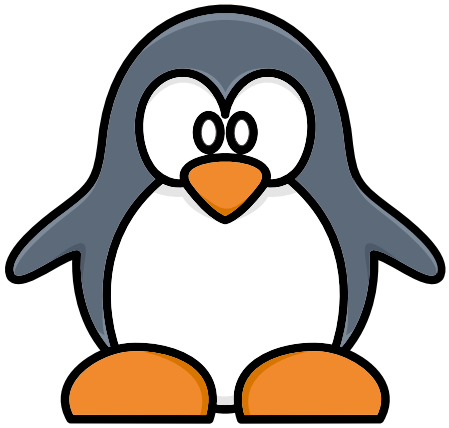
LEARNING LINUX
EXERCISE GUIDE



A PRACTICLE EXERCISE GUIDE

An exercise booklet to help you learn how to use Linux

Written By:

Dan Cannon

INTRODUCTION

Welcome! This worksheet will guide you through various exercises that will help you build foundational Linux skills.

This exercise booklet assumes that you already have a machine running some variation of Linux on it.

You will then need to go to the North Green Github page and download learninglinux using the command

git clone https://github.com/northgreensecurity.com/learninglinux
sudo ./learninglinux

This tool will create a folder in your home directory called learninglinux, folders and files that are created will be within this folder

1 DATA EXERCISES

An important skill for all penetration testers and ethical hackers is an ability to interact with and analyse data.

You'll practice using powerful tools like grep, cut, sort, and uniq to search through and manipulate text data. By the end of this section, you will be comfortable working with files and extracting useful information quickly.

Exercises:

1) Select option 1 to create the data_exercises folder
change directory to this folder.

2) Identify how many lines are in the fruit_list.txt file

Command:

```
1) cat fruit_list.txt | wc -l
```

3) Use grep to find any occurance of the word cherry in fruit_list.txt

Command:

```
Either:  cat fruit_list.txt | grep cherry
Or:      grep cherry fruit_list.txt
```

4) How many lines does the word cherry occur in in the file fruit_list.txt

Command:

```
Either:  cat fruit_list.txt | grep cherry | wc -l
Or:      grep cherry fruit_list.txt | wc -l
```

1 DATA EXERCISES

5) create a copy of the fruit_list.txt file and change all instances of the word peach to blueberry

Command:

1) cp fruit_list.txt fruit_list2.txt
2) sed -i 's/peach/blueberry/g' fruit_list2.txt

5) Use cut to extract all the first names from names.csv

Command:

Either: cat names.csv | cut -d , -f 1
Or: cut -d , -f 1 names.csv

6) Sort the first names from names.csv in alphabetical order

Command:

Either: cat names.csv | cut -d , -f 1 | sort
Or: cut -d , -f 1 names.csv | sort

7) There are duplicate names in this output. Show only a list of the unique names

Command:

Either: cat names.csv | cut -d , -f 1 | sort | uniq
Or: cut -d , -f 1 names.csv | sort | uniq

2 PRIVILEGES EXERCISES

This section focuses on user permissions and privilege management

By understanding how to work with users and their privileges, you'll be able to effectively control access to system files

Exercises:

1) Select option 2 to create new user accounts and the privilege_exercises folder. Open the users_credentials.txt file to see the accounts created

Command:

1) cat user_credentials.txt

2) Change to user 1 and identify the sudo privileges of this account

Command:

1) su user1
2) sudo -l

3) Can you demonstrate that user1 can run any command as any user?

Command:

1) sudo su
2) sudo cat /etc/shadow

4) Change to user2 and identify the sudo privileges of the account

Command:

1) su user2
2) sudo -l

2 PRIVILEGES EXERCISES

5) Can you demonstrate that user2 is able to run any commands with the root privilege?

Command:

1) cat /etc/shadow
2) sudo cat /etc/shadow

6) Look at the /etc/sudoers file. Do you think user3 needs to enter a password when running sudo nano?

Command:

1) sudo cat /etc/sudoers

7) Change to user3 and demonstrate this by opening the /etc/shadow file

Command:

1) su user3
2) nano /etc/shadow
3) sudo /etc/shadow

3 PERMISSIONS EXERCISES

Understanding file permissions and ownership is crucial to a penetration tester.

This section will help you learn how to inspect and modify file permissions, as well as understand who has access to specific files.

Exercises:

1) Select option 4 to create the permissions folder. Change to this directory for the files in these exercises

2) View the file permissions of the two files in the folder

Command:

1) ls -la

3) Can you read either file?

Command:

1) cat read_only.txt

4) Change the ownership of no_access.txt to your user account (the user kali has been used for this example)

Command:

1) sudo chown kali:kali no_access.txt

3 PERMISSIONS EXERCISES

5) Now that you are the owner of the file can you read no_access.txt

Command:

1) cat no_access.txt

6) Change the permission of the file to give yourself read and write access and all other users read access

Command:

1) chmod 644 no_access.txt
I2) s -la

7) Create an executable file that all users can run. Create the file hello.sh and put the following commands in:
#!/bin/bash
echo "Hello World"

Command:

1) nano hello.sh
<input the above code>
2) chmod +x hello.sh
3) ./hello.sh

3 COMPRESSION EXERCISES

Files come in all sizes and at times it is easier to transmit them in a compressed format. It is important to be able to extract important data from these files

The exercises will walk you through the process of extracting and creating compressed files.

Exercises:

1) Select option 5 to create the compression folder. Change to this directory for the files in these exercises

2) extract the data from compressed1.tar.gz

Command:

1) sudo tar vxzf compressed1.tar.gz
2) sudo cat uncompressed1.txt

3) extract the data from compressed2.zip

Command:

1) sudo unzip compressed2.zip
2) sudo cat home/kali/learninglinux/compression/uncompressed2.txt

4) extract the data from compressed3.gz

Command:

1) sudo gunzip compressed3.gz
2) sudo cat compressed3

4 FILE SEARCHING **EXERCISES**

Being able to locate files quickly is a vital skill in penetration testing.

. In this section, you will practice using commands like find and locate to search for files across the system. These tools allow you to search based on file names, types, or contents, which is essential when you have many files spread across different directories.

Exercises:

1) Select option 6 to create the finding_files folder. Change to this directory and read the find_me.txt file to see the name of files for these exercises

2) find the location of each of the files listed in find_me.txt using the find command

Command:

1) find / -name "file1.txt"
2) find / -name "file2.csv"
3) find / -name "file3.log

3) The locate command can quickly find files by name without traversing the whole filesystem, as it relies on an indexed database, however we will need to update the database with our new files.
Find the location of each file using locate

Command:

1) sudo updatedb
2) locate file1.txt
3) locate file2.csv
4) locate file3.log

4 FILE SEARCHING EXERCISES

You'll note that file1.txt is not identified with locate as the /tmp folder is not indexed

6) find all csv files on the device and grep for file2.csv

Command:

1) find / -type f -name "*.csv" | grep file2

5 TRANSFERING FILES **EXERCISES**

Being able to remotely access other machines and copy files across the network is an important skill

In this section, you will create a virtual machine to remotely connect to and be able to move files from one device to another

Exercises:

1) Select option 7 to create a docker container (a light-weight virtual machine) and make note of the IP address the tool provides.

2) Confirm you can SSH to the docker container

Command:

1) ssh root@<IPADDRESS>

3) Verify that this shell is not your linux machine by viewing the /home directory

Command:

1) ls /home/

4) Create a file on the remote host in the /tmp directory called remote file

Command:

1) echo “Remote file” > /tmp/remote.txt

5 TRANSFERING FILES EXERCISES

Open up another terminal at this point.

5) Create a file on your local host in your /home directory called local

Command:

1) echo "Local file" > /home/<username>/local.txt

6) copy the local file into the /tmp directory on the remote server using the tool scp

Command:

1) scp local.txt root@<IPADDRESS>:/tmp

7) pull the remote file from the docker container into your home directory using the tool scp

Command:

1) scp root@172.19.0.2:/tmp/remote.txt remote.txt

You will now have both the remote.txt and local.txt files in your home directory and in the /tmp directory of the docker container

6 IP ADDRESS & ROUTING EXERCISES

Understanding IP addresses and networking is a key skill to communicate in a network.

In this section, you will disable the features that give you an automatic IP address and configure your device to talk to the network

Note: If you are using a virtual machine, it is recommended that you put it in "bridged" mode

Exercises:

1) Identify your computer's IP address and routing information and make a note of it

Command:

1) ip a
2) ip route

2) Confirm you have internet access by pinging 8.8.8.8

Command:

ping 8.8.8.8

3) Disable DHCP, delete DNS serververs, remove the IP address the device has and remove any routing information. For the commands below it is assumed the interface name is eth0

Command:

1) sudo dhclient -r eth0
2) sudo ip addr flush dev eth0
3) sudo ip route flush dev eth0
4) sudo sed -i '/^nameserver/d' /etc/resolv.conf

6 IP ADDRESS & ROUTING EXERCISES

5) Confirm you have no internet access by pinging 8.8.8.8 again

Command:

1) ping 8.8.8.8

6) set a static IP address on your network range. (choose a random high number such as x.x.x.201 where x.x.x are your network address - we will use 192.168.1. in this example) and set your default gateway

Command:

1) sudo ip addr add 192.168.1.201/24 dev eth0
2) sudo ip route add default via 192.168.1.1
3) ip a
4) ip route

7) confirm that you can now ping an internet accessible IP address but cannot resolve URLs

Command:

1) ping 8.8.8.8
2) ping www.google.com

8) Add Google's DNS server to your system for name resolution and confirm it works

Command:

1) sudo nano /etc/resolv.conf
<add the below line>
2) nameserver 8.8.8.8
3) ping www.google.com

Turning individuals into experts

North Green Security is a leader in penetration testing and cyber security training. Offering a comprehensive range of courses to suit you. We are here to provide guidance and skills that will make you more successful.

Our trainers have over 12 years experience creating and delivering training courses that get results

MORE **ABOUT US**

Website
www.ngsacademy.co.uk

Email
training@northgreensecurity.com

Website
www.northgreensecurity.com

Discord
https://discord.gg/w7K8yVaFbD