LAB EXERCISE

2

COMP3134

Introduction to Cyber Security

Week: 2

Objective(s):
Use Information Gathering Techniques to perform network audits and discover network insecurities

Learning Outcome(s):
Recall security fundamental terms and diagrams
Apply and classify network discovery and security auditing techniques

Table of Contents

Contents

Summary

Goal: Use Information Gathering Techniques to perform network audits and discover network insecurities

In Effort To: Recall security fundamental terms and diagrams & Apply and classify network discovery and security auditing techniques

A. Complete Droplet Set-Up

Now that you have successfully created your droplet, it is time to complete the set-up.
There were two options when you created the Droplet

1. One-time password
2. SSH keys

One-Time Password

If you had chosen this option, search your GBC email for an email from Digital Ocean. You should have received an email with your Droplet IP address and a temp password.

Open GitBash and type the command

```
ssh root@IP_ADDRESS
```

When prompted, enter the temp password.
It will ask you to enter a new password, use a Strong Password Generator and create a 20-character password for your droplet with letters, numbers and symbols.
Store this password somewhere safe.

SSH Keys

In case you had chosen this option when creating your droplet, you will fall under one of two categories

1. It is the very first SSH key that you have on your local machine
    a. This is going to be the case if
        i. You're using the lab machines
        ii. You have never created an SSH key before

2. You have already created an SSH key before

Whichever case you fall under, please follow the instructions on the following page

https://help.github.com/en/github/authenticating-to-github/checking-for-existing-ssh-keys

Regain Access to Droplet

Digital Ocean does have an option to regain access to your droplet in case something has gone wrong and you cannot access your droplet
Follow the instructions below in such circumstances
https://www.digitalocean.com/docs/droplets/resources/console/

B. Clone GitHub Repo

Clone course GitHub repo to any location on your local machine
Navigate to the location above and create a folder named **wk2**
Use this local folder created above to create all the files necessary for this Lab Exercise

C. Identifying Server

IP Address Look-Up

If you know a name of an existing domain name, you can use online services to get information about its domain-name registration

Perform a search engine Search with the keyword "whois"
Navigate to any online service site
Perform lookups for 5 distinct domains (not sub-domains)
Create a text file named **whois.txt** and paste the data returned for all 5 queries

Domain Name Look-Up

If you would like to get an IP address of a specific host, you can use online services to accomplish this task

Perform a search engine Search with the keyword "get ip of domain"
Navigate to any online service site
Perform lookups for 5 distinct domains (cannot include domains from above)
Create a text file named **ipinfo.txt** and paste the IP Address and Geolocation data returned for all 5 queries

D. Ensure Server is Running

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network.

Any Host Server Test
Login into your Droplet server using ssh and GitBash
Open GitBash
Type in the following command

```
ssh root@IP_ADDRESS
```

When prompted, enter your droplet password (not needed if using SSH keys)
Once you have successfully connected to your Droplet, install updates and apache2 utilities

```
apt-get update
apt-get install apache2-utils
```

Use the ping tool to determine if a server is up and running

```
ping {host_name}
```

For host_name, use an IP address or any fully qualified domain name (FQDN)
*** search term if you're not familiar with it**

Notice it will continue sending: press ctr+c to stop cycle pre-maturely

To ping for a specified time

```
ping {host_name} -w {time in seconds}
```

Create text file named **ping_1.txt**
Copy and paste the output of at least one of your ping commands above (via GitBash).

Droplet Server Test
Log into your local machine (your desktop or laptop)
Open Command Prompt, Terminal or GitBash (depending on Operating System)
Determine if your Droplet server is up from your local machine
Create text file named **ping_2.txt**
Copy and paste the output of at least one of your ping commands above (via local machine).

E. Path to Destination

Traceroute is command to displaying the route and measuring transit delays of packets across an Internet Protocol network.

Use it to determine how you get form your host to destination host

Install Traceroute (on Remote Host)
To install traceroute on your droplet, type the following command

```
apt-get install traceroute
```

Any Host Server Route Test
Open GitBash window that is connected to your droplet via ssh
Type the command. Replace host_name with any value you desire

```
traceroute {host_name}
```

Create text file named **traceroute_1.txt**
Copy and paste the output of the route your droplet took to go from its host to an external host having the FQDN *host_name* (via GitBash).

Local Host to Droplet Route Test

Log into your local machine (your desktop or laptop)
Open the Command Prompt, Terminal or GitBash (depending on Operating System)
If you are using a windows machine, use the command

```
tracert {host_name}
```

If you are using a Linux machine, use the command

```
traceroute {host_name}
```

If you are on a Mac machine, use the Network Utilities application.
Then click on the Traceroute tab and type in your desired host names

Create text file named **traceroute_2**.txt
Copy and paste the output of the route your local machine took to go from localhost to your droplet host (via local machine).

F. NMAP

Nmap is a powerful network discovery and security auditing utility that is free, open-source, and easy to install. Nmap scans for vulnerabilities on your network, performs inventory checks, and monitors host or service uptime, alongside many other useful features.

Installation of nmap

Open GitBash window that is connected to your droplet via ssh
To install name, execute the following steps

1) Install Nmap
2) Verify Nmap is installed

```
apt-get install nmap
nmap --version
```

Using Nmap

Create a file named **nmap.txt**
Execute the commands stated below and save the command and output to the text file created above. There should be 4 separate outputs in the text file.

To use Nmap to scan 1000 TCP ports, type the following command. Use various host names.

---

nmap {host_name}

To scan a single Port

---

nmap -p {port_number} {host_name}

To scan a range of ports

---

nmap -p {start_port_range}-{end_port_range} {host_name}

To scan 100 most common ports (Fast)

---

nmap -F {host_name}

G. Commit and Upload Changes to GitHub repo

Commit the changes to your repo by:

1. Opening a GitBash window and ensure that it is connected to your local machine
2. Navigate to local repository directory location
3. Add all the files completed in this Lab Exercise
4. Commit the changes
5. Push the changes to your GitHub course repo

Please refer to the instructions in the last section of Lab Exercise 1