CYBR545- Kali Linux Exercise #1

(Team-based, 100 points)

### Due on Sunday 1/29/2023 @11:49PM Group No.:

### Group members names:

# Introduction and submission:

Read each of the following questions and provide your answers after each question. Keep the format of this file as is and provide group information above. This is a team-based assessment, each group is required to submit one file on eCampus, and each member is expected to submit one peer evaluation for this assessment.

Grading Rubric:

**Notes**:

1. Assume the *target* is a machine that the IP Address: 192.168.1.201.

2. When asked to write output to a file, please always name start the name of your output file with the group name, followed the question’s requirement. For example, if you are in group 10, then your output file for question 1 should be named **Group\_10\_Q1\_Scan.txt**, this is case sensitive. A group will lose 10% of the total grade if the naming criteria is not followed.

1. **Provide a command that can be used to update and upgrade all packages in Kali Linux.**

apt-get update && apt-get upgrade -y

1. **Provide a command to check the IP address of your Kali Linux machine.**

ip addr show" or "ifconfig

1. **Provide a command that can be used to install android sdk on Kali Linux**

apt-get install [package\_name]

1. **Provide a command that explains what “ls” does and its optional parameters.**

man ls

1. **Provide a command to display the current working directory of your Kali Linux.**
2. **Provide a Kali Linux command(s) to conduct a port scan on the target above, if the host is up and running, then display a message stating target is live, optherwise, display a message it is down. Save the results to a file named Scan.txt**

nmap -oN nmap\_scan.txt 192.168.1.100

1. **Provide a command to gather information about a target’s domain, and save the output to a file named Gather.txt**

whois [target\_domain] > Gather.txt

1. **Provide a command to determine the path packets to reach the target IP, and save the results to a file named Route.txt**

traceroute 192.168.1.100 > traceroute.txt

1. **Provide a command that displays the numbers of exploits in the Metasploit framework.**

msfconsole

1. **Create bash script file named users\_scrpit.sh that creates 2 local Kali Linux users. Your bash script should open the attached text file named users.txt and create the Kali Linux users given in the second data column of the attached file. For each username, add the two letter G and your group number. For example, if you are in group 10, then the user named user1 should be user1G10. Submit your file. Submit your script separately with this document.**
2. **Search the web for three Linux vulnerabilities added in the past 3 years.**
   1. **What are the names and references of the selected vulnerabilities?**
   2. **How did you find them? Where?**
3. **Select any vulnerability from the selected in the previous step and answer the questions in the table below.**

|  |  |
| --- | --- |
| **Vulnerability : [provide reference here]** | |
| **Name/ Reference of the vulnerability** |  |
| **Source** |  |
| **Metasploit command to lookup vulnerability** |  |
| **Full name of vulnerability** |  |
| **All platforms affected** |  |
| **Metasploit command to display full vulnerability info** |  |
| **Metasploit command to enable context exploit module** |  |
| **Metasploit command to display the current exploit info** |  |