National University of Computer and Emerging Sciences, Lahore Campus

	Course Name:	**Information Security**	**Course Code:**	**CS3002**
	Program:	**BS (Data Science)**	**Semester:**	**Fall 2024**
	Section:	**7C**	**Total Marks:**	**20**
	Due Date:	**10-Sep-2024**	**Weight:**	
	Exam Type:	**Assignment 1**	**Page(s):**	**2**
Student Name: _____Roll No._____				

Drive link for virtual appliance file:
https://drive.google.com/file/d/1IYorBK2cOOktPiKDvDURmJX_BuQqJOZA/view?ts=66d5b371

1. Prerequisites

Step	Description	Link
Install VirtualBox	Download and install VirtualBox to create and manage virtual machines.	VirtualBox Downloads
Install Extension Pack	Install the VirtualBox extension pack to enable additional features like USB 2.0/3.0 support, VirtualBox RDP, and disk encryption.	
Download Kali Linux VM	Download the Kali Linux virtual machine image, which will be used as the attacking machine in this assignment.	Kali Linux VM Download
Run Updates on Kali Linux VM	After setting up the Kali Linux VM, ensure it is up to date by running sudo apt-get update and sudo apt-get upgrade commands.	
Build a Target VM	Create a second virtual machine (Target Machine) by importing the appliance named "BSCS Spring-2023" provided in the assignment folder.	
Configure Network Settings	Adjust the network settings for both virtual machines to ensure they are on the same network and can communicate with each other.	

Note: Figures and screenshots must be included in your report to illustrate the successful completion of each step. For instance:

- **Figure 1**: Screenshot of the VirtualBox interface after installing and configuring the VMs.
- **Table 1**: Summary of network settings for both VMs, including IP addresses, subnet masks, and gateway information.

---

2. Steps to Complete the Assignment

Step	Description
1. Identify the Target Machine's IP Address	Use the netdiscover command within the Kali Linux VM to identify the IP address of the target machine on the same network.
2. Determine Open Ports and Services	Execute the Nmap tool to scan the target machine's IP address and list open ports and running services. Nmap is available by default in Kali Linux.
3. Identify Vulnerabilities in Web Application	Based on the Nmap scan results, access the web application hosted on the target machine. Attempt to log in using default or discovered credentials.
4. Directory Enumeration Using Dirb	Utilize the dirb utility to perform directory enumeration on the web application. Search for hidden directories or files that may contain sensitive information.
5. Login Using Detected Credentials	Use the username and password obtained during the previous steps to log in to the web application. Document this process with relevant screenshots.

Additional Information:

- **Commands Documentation:** Ensure that every command used (e.g., netdiscover, nmap, dirb) is documented with a brief explanation of its purpose and functionality. Include screenshots that display the execution of the command and its results.
- **Network Configuration:** Present the network configuration in a tabular format similar to the one shown below:

VM	IP Address	Subnet Mask	Default Gateway	Network Adapter
Kali Linux	192.168.0.10	255.255.255.0	192.168.0.1	NAT Network
Target Machine	192.168.0.15	255.255.255.0	192.168.0.1	NAT Network

---

3. Caution

Guideline	Details
Report Format	The assignment must be submitted as a detailed report. Ensure that each step is thoroughly documented, including explanations and justifications for each action.
Inclusion of Figures and Tables	Include screenshots (figures) of each step and summarize configurations or results in tables where appropriate. Use clear and concise labels for all figures and tables.
Visibility of Username	Your username must be clearly visible in all screenshots of the Kali Linux command prompt.
Use of Date Command	Before executing each command, run the date command to timestamp each step. This should be visible in all screenshots.
Academic Integrity	The assignment should be your own work. Plagiarism or copying from fellow students will result in a score of "0" for all parties involved.