Laud Mills

Part A: Open your Kali and Metasploitable2 terminal, write down the commands based on the following instructions. Also attach the screenshots.

1. Find out the IP address, subnet mask and broadcast address of Kali Linux Virtual Machine through command prompt.

Command : ifconfig -a

IP address : 192.168.100.6

Mask : 255.255.255.0

Broadcast address: 192.168.100.255

Screen Capture :

A computer screen with text and numbers

Description automatically generated

1. Find out the IP address of Metasploitable2 Virtual Machine through command prompt.

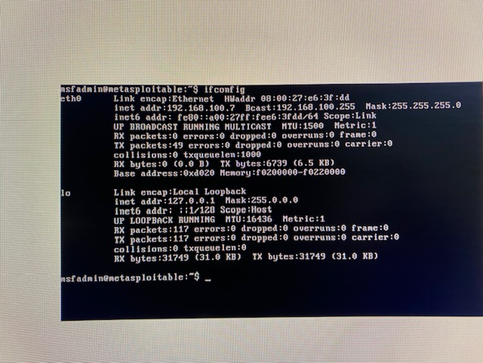
Command : ifconfig

IP address : 192.168.100.7

Mask : 255.255.255.0

Broadcast address: 192.168.100.255

Screen Capture :



1. Check the reachability of Metasploitable2 from Kali Linux by sending ICMP echo request packets.

Command: ping 192.168.100.7 -c 4

Screen Capture:

A computer screen with text and numbers

Description automatically generated

1. Open the Kali Linux browser and write the IP address of Metasploitable2 to access various application of Metasploitable2.
2. List out the purpose of each of the five applications in your own words (1-2 lines are sufficient) that is visible on your Kali browser once you have connected with Metasploitable2.

TWiki is used for remote code execution attacks and provides an environment to create and manage projects.

phpMyAdmin This can be used to MySQL and MariaDB databases in a browser environment. It provides a graphical user interface that makes it user friendly.

Mutillidae provides hands on environment for learners to practice how to exploit and defend against web application vulnerabilities.

DVWA just like the Mutillidae it has learners features for practicing web application security testing.

WebDAV is an extended part of the HTTP protocol that allows interaction with files on a remote web server.

1. Find out default username and password of DVWA on google and login in the system.

Username : admin

Password : password

1. How do you set the security level of DVWA to low? What are the other security levels that you can set?

After logging into DVWA, locate DVWA Security tab on the left. Click on it then select security level from the drop-down options which can be High, Medium and low. Then click on submit. There are 3 options, the other level is medium.

1. Check – whether FTP support is enabled or disabled in DVWA?

Yes FTP is enabled. Checked from the PHP Info tab

1. List out the Hash function supported by DVWA. What is the purpose of a hash function in general?

MD5, SHA-1, SHA-256, bcrypt, crypt, ripemd128 etc. In general Hash functions are used to ensure data integrity.

1. What is the version of OPNSSL? What is the purpose of OpenSSL protocol?

OpenSSL VERSION 0.9.8g OpenSSL is generally used to secure communication on web traffic, emails, VPN within the framework of Confidentiality, Integrity and Availability.

1. Where do you find the user credential (path of the folder) to setup the database?

In the configuration file : /var/www/html/dvwa/config/config.inc.php

Part B: For the following questions, you should go beyond the provided materials and think as a security professional to identify the proper reasons based on real scenario.

1. What information can you determine from the “ifconfig -a” command?

It is used to display all active and inactive network interfaces, IP and MAC addresses, in a system.

1. What are the two most common protocols that web servers use for normal web traffic. Out of two, which protocol is secure & how it provides assurance to the customers that the information is protected during web communication?

They are HTTP and HTTPS. HTTPS is the secure one because it ensures that communication between the web client and server are encrypted.