Root Access Lab

Introduction and/or Background
root is the user name or account that by default has access to all commands and files on a Linux or other Unix-like operating system.

Objectives
In this project/lab the student will:

- Gain familiarity with root access

Equipment/Supplies Needed

- As specified in Lab 0.0.1.
- Linux Installation File: Kali Linux and Metasploitable

Procedure
Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

1. Turn on both the Kali and Metasploitable VMs. Metasploitable is available here.
2. Discover Metasploitable2's IPv4 address.
3. Open a Terminal window on the Kali VM.
4. Open the Metasploit console. The postgresql service should automatically start.
5. Run an nmap service and version scan directly from the msf5 command prompt and **take a screenshot** of the results.
6. Search for vsftp exploits in Metasploit.
7. Load the vsftp exploit module.
8. Set RHOST to Metasploitable2's IPv4 address.

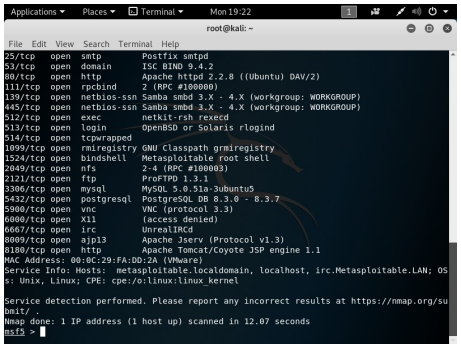
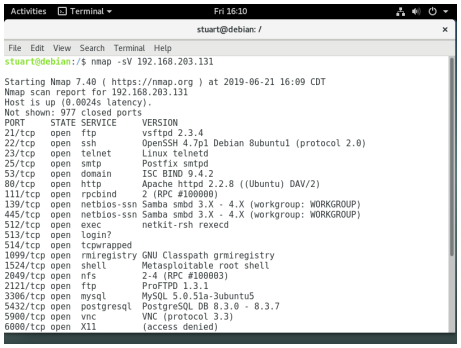
9 Execute the exploit.

10 Enter the whoami command and **take a screenshot**.

11 Enter the exit command to return to the metasploit command prompt.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot showing nmap service and version scan from the msf command prompt (50 points)	 
	Criteria #2: Screenshot showing root access obtained (50 points)