A logo of a university

Description automatically generated

**PEN TESTTING APPLICATION REPORT**

**SQL INJECTION SIMULATION**

Performed By: Emmanuel Nana Kwame Ninsin

**TABLE OF CONTENTS**

1. INTRODUCTION AND OVERVIEW Pages 3 to 7
   1. Objective ---------------------------------------------------------------------- 3
   2. Scope --------------------------------------------------------------------------- 3
   3. IT Asset Inventory Details
      1. Hardware Specifications
         1. Machine specifications for project ---------------------------3
         2. Recommended Specifications -------------------------------- 4
         3. Minimum Specifications -------------------------------------- 4
      2. Software Specifications
         1. Attacker Specifications --------------------------------------- 4
         2. Victim Specifications ----------------------------------------- 4
      3. Network Configurations
         1. Static IP address of each Virtual Machine ----------------- 5
         2. Description ----------------------------------------------------- 5
   4. Real Life Implications of Project ----------------------------------------- 6
   5. Warnings --------------------------------------------------------------------- 7
2. ENVIRONMENT SETUP Pages 8 to 58
   1. Installing Oracle VirtualBox
      1. Download Guide ------------------------------------------------------- 8
      2. Installation Guide ------------------------------------------------------ 8
   2. Attacker machine setup
      1. Download Guide ------------------------------------------------------ 12
      2. Creating the Virtual Machine ---------------------------------------- 12
      3. Installation Guide and Network Configuration ------------------- 17
      4. Nmap -------------------------------------------------------------------- 29
      5. SQLMap ---------------------------------------------------------------- 29
   3. Victim machine setup
      1. Download Guide ------------------------------------------------------ 30
      2. Creating Virtual Machine -------------------------------------------- 30
      3. Configuration Steps
         1. Giving user Sudo privileges -------------------------------- 35
         2. Network Configuration --------------------------------------- 37
      4. LAMP Stack setup
         1. Installing and Configuring Apache web server ------------ 39
         2. Installing and Configuring MySQL database ------------- 41
         3. Installing and Configuring PHP ----------------------------- 45
      5. DVWA setup ----------------------------------------------------------- 48
      6. Testing Connection within Internal Network --------------------- 53
3. THINGS TO NOTE Pages 59 to 60
   1. Best Practices ---------------------------------------------------------------- 59
   2. Troubleshooting ------------------------------------------------------------- 59
4. EXPERIENCE ------------------------------------------------------------------ 60
5. SOURCES ----------------------------------------------------------------------- 61
6. **INTRODUCTION AND OVERVIEW**
   1. **Objective**

The objective of this penetration testing project is to simulate an attacker’s approach to discovering and exploiting a vulnerable machine on a network. The process begins with the use of Nmap from a Kali Linux attacker machine to perform network reconnaissance and identify a target system, specifically an Ubuntu Server hosting a web application. Once the victim machine is identified, an SQL injection attack will be executed using the SQLMap tool to exploit vulnerabilities in the web application. The goal is to demonstrate how attackers can gain unauthorized access to a database and exfiltrate sensitive data, providing a practical understanding of the risks associated with SQL injection vulnerabilities.

* 1. **Scope**

This report outlines the process of setting up a controlled sandbox environment for penetration testing, consisting of an attacker machine and a DVWA (Damn Vulnerable Web Application). The setup involves configuring a LAMP stack to create a vulnerable web server. Additionally, the report details the installation and configuration of SQLMap on the attacker machine to conduct penetration tests. Nmap will be used for reconnaissance to identify potential targets and open ports within the network. All activities will take place within an internal, isolated network that is disconnected from the internet, ensuring a secure testing environment.

* 1. **IT Asset Management**
     1. Hardware requirements

To undertake this project, a host machine or device must be able to download a hypervisor (must be capable of virtualization). Additionally, it must be capable of running to virtual machines simultaneously for the entire duration of the penetration testing process.

1.3.1.1. *Machine specifications for project*

**Name:** Dell Latitude 5490

**Operating System:** Windows 11 Enterprise, version 23H2

**Processor:** Intel(R) Core™ i7-8650U CPU @1.90GHz 2.11GHz

**Installed RAM:** 16 Gigabytes (15.9 usable)

**System Type:** 64-bit operating system, x64-based processor

**Storage: 1 Terabyte**

1.3.1.2. *Minimum Specifications*

**Processor:** Dual-core processor with hyper-threading (e.g., Intel Core i5 or AMD Ryzen 5)

**RAM:** 8 GB of RAM

**Storage:** 8 GB of RAM

**GPU:** Dedicated GPU (e.g., Nvidia GTX or RTX, AMD Radeon)

1.3.1.3. *Recommended Specifications*

* **Processor:** Quad-core processor with hyper-threading (e.g., Intel Core i7 or AMD Ryzen 7)
* **RAM:** 16 GB of RAM
* **Storage:** 512 GB SSD or larger
* **GPU:** Integrated graphics (e.g., Intel UHD or AMD Vega)
  + 1. Software Requirements

**Oracle VirtualBox**: pen source, cross-platform, virtualization software, enables developers to deliver code faster by running multiple operating systems on a single device.

1.3.2.1. *Attacker Specifications*

(a) **Kali Linux:** an open-source, Debian-based Linux distribution which allows users to perform advanced penetration testing and security auditing.

(b) **Nmap:** an open-source network scanning and host discovery tool.

(c) **SQLMap:** an open-source tool that automatically finds and exploits SQL injection vulnerabilities.

1.3.2.2. *Victim Specifications*

(a) **Ubuntu 20.*04:***A distribution (version) of the Linux operating system. It serves as the operating system of our victim.

(b) **Apache:** a free, open-source web server.

(c) **MySQL:** a widely used relational database management system (RDBMS). It is free and open source.

(d) **PHP:** an open-source server-side scripting language that many devs use for web development. It is also a general-purpose language that you can use to make lots of projects, including Graphical User Interfaces (GUIs).

(e) **DVWA (Damn Vulnerable Web Application):** a pedagogical tool and recipient of attacks. It’s a PHP/MySQL web application intentionally designed to be vulnerable.

* + 1. Network Configurations

1.3.3.1. *Static IP address of each Virtual Machine*

|  |  |
| --- | --- |
| Attacker (Kali Linux)  **IP address:** 192.168.100.10  **Netmask:** 255.255.255.0  **Gateway:** 192.168.100.1 | Victim (Ubuntu 20.04)  **IP address**: 192.168.100.20  **Netmask:** 255.255.255.0  **Gateway:** 192.168.100.1 |

1.3.3.2*. Description*

The goal of this configuration process is to ensure that the two virtual machines can communicate within an internal network devoid of internet access.

Each machine would be given 2 adapters

**Adapter 1**: This would be connected to NAT to give each device an Internet connection for future configurations

**Adapter 2:** This would be connected to the internal network intent through which the devices can communicate with each other.

Adapter 1 would only remain on during the setup and configuration processes. After that, when preparations are made for the SQL injection, Adapter 1 would be disabled, and Adapter 2 would be enabled. This would deprive both devices of an Internet connection but would still allow communication between the two (and only the two) devices through the internal network. This creates an isolated sandbox environment where all our actions are contained within the sandbox

TAKE NOTE, INTERNET CONNECTION MUST REMAIN DISABLED DURING THE ENTIRE DURATION OF THE PENTESTING TESTING EXPERIENCE.

* + 1. Real Life Implications of Project

In a world where we are becoming more and more digitally interconnected, the threat of cyber-attacks continues to loom over all systems, whether it is an individual computer or a server farm. SQL injections are one of the many ways that attackers use to gain access to data. It involves exploiting weakness in a system's SQL commands through which malicious commands can be injected to corrupt the system. This project is a penetrative testing scenario used to exploit a vulnerable system through this means.

This has several implications for companies and individuals including:

1. Data Breaches
2. Financial loss
3. Loss of customer trust
4. System Manipulation and downtime
5. Legal and Compliance issues
6. Escalation of privileges
7. Intellectual Property Theft
8. Black Market Exploits and more

Through this project, the following would be addressed.

• How a technique like SQL injection is used to perform data exfiltration

• How tools like SQLMap are used to make such techniques so much easier using simple commands, documentation and wizards.

• How important is it for programmers to always think of all extremes when writing code, particularly when it involves sensitive data.

• How vulnerable systems are susceptible to such attacks and the importance of patch management and regular system updates.

* + 1. Warning

This project simulates an actual method used to infiltrate a database and gain access to its data.

**DO NOT TRY THESE SKILLS ON ANY COMPUTER, WEBSITE OR SYSTEM UNLESS AUTHORISED TO DO SO BY CONTRACT.**

This should be performed in a sandbox environment if for practice.

I would not be responsible if you did not follow the contents of this warning.

1. **ENVIRONMENT SETUP**
   1. **Installing Oracle VirtualBox**
      1. **Download Guide**

**Download URL:** [**https://www.virtualbox.org/wiki/Downloads**](https://www.virtualbox.org/wiki/Downloads)

* Download the following: package for Windows host: o VirtualBox- VirtualBox-7.1.4-165100-Win.exe • VirtualBox
* Extension Package o Oracle\_VirtualBox\_Extension\_Pack-7.1.0.vbox-extpack
  + 1. **Installation Guide**

**Install Virtual Box**

|  |  |
| --- | --- |
| 1. Double-click the file VirtualBox-7.1.4-165100-Win.exe to start the installation | A screenshot of a computer  Description automatically generated |
| 1. Agree to the terms in the License Agreement and click Next. | A screenshot of a computer  Description automatically generated |
| 1. In the first custom section, you can leave everything as default and click Next | A screenshot of a computer  Description automatically generated |
| 1. Click Yes for the “Network Configuration Warning”. It basically saying that installing the network feature of VirtualBox would reset the network and temporarily disconnect the machine from the internet. | A screenshot of a computer  Description automatically generated |
| 1. Click Yes to download the missing dependencies python core. | A screenshot of a computer  Description automatically generated |
| 1. Click on “Install” to install VirtualBox | A screenshot of a computer  Description automatically generated |
| 1. Uncheck the “Start Oracle VirtualBox 7.1.4” after installation checkbox and click on Finish | A screenshot of a computer  Description automatically generated |
|  |  |

* 1. **Installing Attacker Machine**
     1. **Download Guide**

**Attacker OS:** Kali Linux

**Download URL:** <https://www.kali.org/get-kali/#kali-platforms>

The URL above shows the different Kali Linux platforms. In this case, we would be using Installer Images.

* + 1. **Creating the Virtual Machine**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Open your newly installed VirtualBox software |  | | | | | | |
| 1. When VirtualBox is opened for the first time, a welcome message is displayed. 2. To create a new virtual machine, click on New (As shown by the blue highlight) or go to   Machine 🡪New | | A screenshot of a computer  Description automatically generated | | | | | |
| 1. In the window that pops up, Enter:  * The name of your virtual machine * The folder where you want to store the machine (This can be left as default) * The file path of where your ISO image file is stored  1. Notice that when you change the name to Linux, VirtualBox recognizes it in the Type. Make sure the subtype is Debian and Click Finish. | | | | A screenshot of a computer  Description automatically generated | | | | | |
| 1. In the Hardware section, set: 2. Base memory = 2048MB 3. Processors = 2   Make sure to use enough memory and processors to allow optimal performance | | A screenshot of a computer  Description automatically generated | | | | | |
| 1. Set the Size to be at least 30 GB and check “Pre-allocate Full Size” 2. Click on Finish | | A screenshot of a computer  Description automatically generated | | | | | |
| 1. For a new user a fresh version of Kali would be the only machine created. 2. Click on Settings 3. Or go to Machine 🡪 Settings | | A screenshot of a computer  Description automatically generated | | | | | |
| 1. In settings go to General🡪Advanced 2. Set Shared Clipboard to Bidirectional | | A screenshot of a computer  Description automatically generated | | | | | |
| 1. Still in Settings, Go to network 2. Enable Adapter 1 and set it to NAT 3. This gives the virtual machine internet access | |  | | | | | |
| 1. Go to Storage in Settings and ensure that the Kali Linux virtual machine is listed. 2. Click OK. | |  | | | | | |
| 1. Start the virtual Machine by clicking the green arrow or going to Machine🡪 New | | A screenshot of a computer  Description automatically generated | | | | | |
|  | |  | | | | | |
| * + 1. **Installation Guide and Network Configuration** | | | | | | | |
|  | |  | | | | | |
| 1. Select Graphical Install | |  | | | | | |
| 1. Select English for Language 2. Click Continue | |  | | | | | |
| 1. Select United States for Location 2. Click Continue | |  | | | | | |
| 1. Select American English for Keyboard Configuration 2. Click Continue | |  | | | | | |
| 1. Enter a specific hostname that identifies your system on the network. 2. Click Continue | |  | | | | | |
| 1. Set up a user account by typing a name. 2. Eg: YourName. | |  | | | | | |
| 1. Configure the clock to Eastern time | |  | | | | | |
| 1. For Partition disks, select   “Guided – use entire disk”   1. Click Continue | |  | | | | | |
| 1. Select the disk to partition. 2. Click Continue | |  | | | | | |
| 1. Select “All files in one partition (recommended for new users)” 2. Click Continue | |  | | | | | |
| 1. Select “Finish partitioning and write changes to disk” 2. Click Continue | |  | | | | | |
| 1. Select “Yes” 2. Click Continue | |  | | | | | |
| 1. Leave everything as default unless specific configurations are required. 2. Click Continue | |  | | | | | |
| 1. Install the GRUB boot loader by selecting Yes 2. Click Continue | |  | | | | | |
| 1. Device for boot loader installation 2. Select /dva/sdb… 3. Click Continue | |  | | | | | |
| 1. The installation is complete 2. Click Continue to reboot the machine | |  | | | | | |
| 1. Once Kali is installed, login in by entering the username and password created during the installation process | |  | | | | | |
| 1. Once logged in, click on the terminal emulator to open the terminal | |  | | | | | |
| 1. Ping 8.8.8.8 to check whether an internet connection is available. | |  | | | | | |
| 1. Use ifconfig to check the network details of the machine | |  | | | | | |
| 1. Execute the command   **sudo apt-get install gedit.**   1. Enter your password and press enter 2. Type y and click Enter 3. This installs the gedit text editor | | | |  | |
| 1. Now shutdown the machine with the command   **sudo poweroff** | | | | |  | |
| 1. Now we are going to give the machine its static IP address 2. Make sure the machine is selected and click on Settings 🡪Network | | A screenshot of a computer  Description automatically generated | | | | | |
| 1. Enable the following adapters 2. Adapter 1 = Internal Network with name being “intent” 3. Adapter 2 = NAT 4. Click Okay. | |  | | | | | |
| 1. Start the machine | | A screenshot of a computer  Description automatically generated | | | | | |
| 1. Open the Terminal Emulator and execute the command as shown. 2. This opens the networks file which is responsible for storing all network configurations | |  | | | | | |
| 1. Modify the file with the code shown below | | | | | | | |
| # This file describes the network interfaces available on your system  # and how to activate them. For more information, see interfaces(5).  source /etc/network/interfaces.d/\*  # The loopback network interface auto lo  iface lo inet loopback  auto eth1  iface eth1 inet dhcp  auto eth0  iface eth0 inet static address 192.168.100.10 netmask 255.255.255.0 gateway 192.168.100.1 | | | | |  | |
| 1. Save the file and reboot the machine with the command   Sudo reboot | |  | | | | | |
| 1. Now check the configuration of the network with ifconfig. | |  | | | | | |

* + 1. **Nmap**

Nmap is a network scanning tool used to identify other hosts on the network. This is normally preinstalled on Kali Linux. To check if it is available, execute the command **“nmap -v”** in the Terminal Emulator. This would be the expected result:A screen shot of a computer

Description automatically generated

If is unavailable, install it with this command:

**sudo apt install nmap**

* + 1. **SQLMap**

This tool is used to perform the SQL injection. It is normally preinstalled on Kali Linux. To check if it is available type **“sqlmap” in** Terminal Emulator. This would be the expected result:

If it isunavailable, install it with this command:

**git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev**

Move into the new directory (**cd sqlmap-dev**) and execute:

**python3 sqlmap.py**

* 1. **Victim machine setup**

**2.3.1. Download Guide**

**Download URL:** [**https://old-releases.ubuntu.com/releases/**](https://old-releases.ubuntu.com/releases/)

**Take note** that a slightly older version of ubuntu is required for the project. It should be old enough to be made vulnerable but not too old that it cannot support the components of the LAMP stack or the DVWA. **For this project, Ubuntu 20.04 would be used.**

**2.3.2. Creating the Virtual Machine**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. Open Virtual box and create a new virtual machine by clicking on New (As shown by the blue highlight) or go to   Machine 🡪New |  | | | | | |
| 1. In the window that pops up, Enter:  * The name of your virtual machine * The folder where you want to store the machine (This can be left as default) * The file path of where your ISO image file is stored  1. Notice that when you change the name to Linux, VirtualBox recognizes it in the Type. Make sure the subtype is Ubuntu and Click Finish. 2. Uncheck “Skip Unattended Installation” | |  | | | |
| 1. We will perform an unattended OS install which involves creating a user account 2. Type in a username 3. Create ad confirm a password 4. Specify a hostname 5. Check “Guest Additions” 6. Click Next |  | | |
| Allowing an unattended guest OS install means that virtualbox would handle the installations steps and configurations of your virtual machine. The only issue is that the account it creates does not not have sudo permissions and would have to be configured manually.  Checking guest additions makes the virtual machine more flexible for the user and allows features such as a fully resizable screen. | | | |
| 1. In the Hardware section, set: 2. Base memory = 5000MB 3. Processors = 4   Make sure to use enough memory and processors to allow optimal performance |  | | |
| 1. Set the Size to be at least 25GB 2. Check “Pre-allocate Full Size” (Optional) 3. Click Next and Finish (The Finish window just shows a summary of the VM specifications) |  | | |
| 1. A new ubuntu virtual machine would be created 2. Make sure the machine is selected and click on Settings 3. Or go to Machine 🡪 Settings |  | | |
| 1. In settings go to General🡪Advanced 2. Set Shared Clipboard to Bidirectional |  | | |
| 1. Still in Settings, Go to network 2. Enable Adapter 1 and set it to NAT 3. Enable Adapter 2 and set it to the internal network “intent” 4. Click Okay |  | | |
| Now Start the virtual machine. | | | |
| 1. . Log into your user account | | |  | |
| 1. Select Next for each of the prompts that appear and go to the desktop. | | |  | |

* + 1. **Configuration Steps**
       1. **Giving user Sudo privileges**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Due to the unattended install of the OS, the user account created was not included in the sudeors file/group and therefore does not have sudoers privileges. | | | | | |
| 1. On the desktop go to the application Tray | |  | | | |
| 1. Type Terminal in the search bar and open it | |  | | | |
| To gain sudo privelages, the useraccount must be added to the sudoers file. This can only be done by becoming the root user. It is not advised to remain as root through the entire pen testing eperience so this would only be done to gain sudo privelages. | | | | | |
| 1. To become root, execute the command:   **su -**   1. Type in your account password and press Enter. | | |  | |
| 1. You will notice that the prompt changes, which show that you are now root. |  | | | |
| 1. Use the following command to find the root. | |  | | | |
| 1. The system must reboot for the changes to take place. Shut down the machine with:   **Sudo poweroff**   1. Turn the machine on | | | |  | |
|  | | | |  | |
| * + - 1. **Network Configurations** | | | | | |
| This stage involves gaining the ifconfig command and assigning the static IP address necessary for the project. | | | | | |
| 1. To check if you have root privileges with sudo execute the command   **sudo whoami**   1. This would output the text “root” | |  | | | |
| 1. Now install the net-tools package. This would allow the usage of ifconfig   **sudo apt install net-tools** | |  | | | |
| 1. Execute the ifconfig command. The output is the default network configuration of Ubuntu 2. Keep the terminal open | |  | | | |
| 1. Go to the app tray and type “Settings in the search bar 2. Open the settings | |  | | | |
| 1. Go to the network settings and selet the settings button of Ethernet (enp0s8). 2. This represents Adapter 2 which was set to internal network. | |  | | | |
| 1. Click on the IPv4 tab 2. Select the Manual IPv4 Method 3. Fill in the table with the following data   **IP address**: 192.168.100.20  **Netmask:** 255.255.255.0  **Gateway:** 192.168.100.1   1. Click Apply | |  | | | |
| 1. Back in the Terminal, run the ifconfig command and check the updates. | |  | | | |

* + 1. **LAMP Stack Setup**
       1. **Installing and Configuring Apache web server**

|  |
| --- |
| 1. Update all packages with the commands:   **sudo apt update**  **sudo apt upgrade**   1. Take note, you may have to enter your user account password to progress |
|  |
|  |
| 1. Install Apache with the following command:   **sudo apt install apache2**   1. Type “y” for the following prompt and press Enter. |
|  |
| 1. Start the Apache service by executing the command:   **sudo systemctli enable apache2** |
|  |
| 1. Next, enable the ufw firewall. It would be configured to allow http traffic port 80. |
|  |
| 1. Use the following command   **sudo ufw app list**  to determine the services that would use the firewall |
| A screenshot of a computer  Description automatically generated |
| 1. Use the command   **sudo ufw allow in “Apache”**  To allow http traffic from our server |

|  |
| --- |
|  |
| 1. Use the command   **sudo ufw status**  To check the status of the firewall |
|  |
| 1. To ensure a successful installation, search for a browser and type the this url in the search engine:   [**http://192.168.100.20**](http://192.168.100.20) **(This is the IP address of the server)**  This would take you to the default Apache landing page if all configurations were successful. |
|  |

* + - 1. **Installing and Configuring MySQL database**

|  |
| --- |
| 1. To install mysql, use the commnd   **sudo apt install mysql – server**  Type “y” and press Enter to start the installation |
|  |
| 1. We must now run the mysql\_secure\_installation script to secure the installation process but there is a problem as shown by the warning below by DigitalOcean (Source listed in the sources chapter) 2. **Warning**: As of July 2022, an error will occur when you run the mysql\_secure\_installation script without some further configuration. The reason is that this script will attempt to set a password for the installation’s **root** MySQL account but, by default on Ubuntu installations, this account is not configured to connect using a password. 3. To solve this first open mysql with the command   **sudo mysql** |
|  |
| Run the following command to set root to a password |
|  |
| Exit sql with the “exit” statement; |
|  |
| 1. The secure script can now be run with the command. 2. Type “y” and click enter at the prompt to continue. |
| 1. The script is used to provide security configurations to mysql, one of which involves changing the root password set earlier. Type “y” to change password or any other key to skip and press Enter. 2. For this project the password would remain the same. |
|  |
| 1. If you selected selected yes for the password change, You would be to enter a level of difficulty for your password to adhere to. Select a level as shown below and type and confirm your pasword. If your password does not adhere to the security level, you would be asked to enter a new password. 2. Since we did not change the password for this project this prompt would not show. |
|  |
| 1. Type “y” to accept all the prompts that follow until the script is complete |
|  |
| 1. Once the script is complete, try logging into the database as root with the command   **sudo mysql -u root -p**  **T**ype in your root password and click enter   1. **Take note, the database root account is different from the Ubuntu root account** 2. A successful login would display a message as shown below |
|  |
| 1. Now logout using the comand   **exit**   1. Press enter |
|  |

* + - 1. **Installing and Testing PHP**

|  |
| --- |
| Now comes the point we install php which will be responsible for processing code to display dynamic content. Along with php, we would need php-mysql, a PHP module that allows PHP to communicate with MySQL-based databases. You’ll also need libapache2-mod-php to enable Apache to handle PHP files. Core PHP packages will automatically be installed as dependencies (DigitalOcean 🡪Check sources). |
| 1. To install php and the required modules, use the command:   **sudo apt install php libapache2-mod-php php-mysql**   1. And press Enter 2. Type “y” and press Enter for the prompt that follows |
|  |
| 1. Check the php version with the command:   **php -v**   1. Press and Enter and check the output |
|  |
| 1. Lets test php processing. Create a new file named info php your custom web root folder. Use the command   **sudo nano /var/www/192.168.100.20/info.php**   1. The file is opened in the nano text editor. |
|  |
| 1. Insert the following php code into the file   **<?php**  **phpinfo();**  **?>**   1. and save it with the sequence   **Ctrl + O 🡪 Enter 🡪 Ctrl + X** |
|  |
| 1. Restart the Apache web server with the command   **systemctl restart apache2** |
|  |
| 1. Go to the web browser and access the file with the URL:   **http://192.168.100.20/info.php**   1. The result is shown below |
|  |

* + 1. **DVWA Setup**

|  |
| --- |
| For this project, DVWA would be installed as a package from GitHub |
| 1. First Update all packages |
|  |
| 1. Remove index.html from the Apache root directory (/var/www/html/) |
|  |
| 1. Next install git. This would help us clone or install the DVWA repository from GitHub 2. Type “y” at the prompt and press Enter |
|  |
| 1. Next clone the latest version DVWA package into a temporary folder (in tis case called **tmp**). |
|  |
| 1. Move or copy these files to Apache default web root directory as shown below. |
|  |
| 1. Create a copy of the file **/var/www/html/config/config.inc.php.dist**  and name it **/var/www/html/config/config.inc.php** |
|  |
| 1. We must modify the configuration file with the details of our database, such that the DVWA is able to connect to the database |
|  |
|  |
| 1. In the file look for this section of the file and make the following changes 2. Set db\_user to root 3. Set db\_passwrd to the database root password 4. Save the file and exit gedit. |
|  |
| 1. Restart the mysql Database. |
|  |
| 1. From the checking the php version earlier, we know that the version installed is 7.4 (or whichever version you have installed). Open the file **/etc/php/7.2/apache2/php.ini** 2. Make the following changes  * allow\_url\_include = on – Allows for Remote File Inclusions (RFI) * allow\_url\_fopen = on – Allows for Remote File Inclusions (RFI) * display\_errors = off – (Optional) Hides PHP warning messages to make it less verbose |
|  |
| 1. Use the command show below to the ownership of all files and directories inside /var/www/html (including subdirectories and files) to the www-data user and the www-data group. |
|  |
| 1. Now go to your browser and type the following in the search bar:   **http:// 192.168.100.20**  The output is as shown below |
|  |
| 1. It can be seen above that the gd PHP module is disabled. This is a requirement and must be installed. Install it with the command below. |
|  |
| 1. Restart the Apache |
|  |
| 1. Reload the DVWA Setup page. The PHP module gd field should be enabled now |
|  |
| 1. Close everything and shutdown the machine |
| 1. Move to the bottom of the page and click the “Create/Reset Database”. |
|  |
| 1. If all was configured well you would be taken to a login page. Enter “admin” as your user name and your database root password and click Login.   CONGRATS, THE DVWA HAS BEEN SET UP! |
|  |
|  |
|  |
|  |

* + 1. **Testing Connection within Internal Network**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| At this point both machines have been individually set up for penetration testing but now, we have to see whether they can communicate with each other on the internal network | | | | | | | |
| 1. Open Virtual Box |  | | | | | | |
| 1. Go to Settings🡪Network of the victim machine (Ubuntu Server) 2. Disable the Adapter connected to NAT (Adapter 1) 3. Click OK to apply the changes. | | |  | | | | | | |
| 1. Enable Adapter 2 which should be connected to the internal network intnet 2. Click OK | | |  | | | | | | |
| 1. Go to Settings🡪Network of the attacker machine (Kali Linux) 2. Disable the Adapter connected to NAT (Adapter 2) 3. Click OK to apply the changes | | | |  | | | | |
| 1. Enable Adapter 2 which should be connected to the internal network intnet 2. Click OK | | | |  | | | | |
| 1. Start the Virtual Machines |  | | | |
| 1. Log onto the machines using their respective user accounts |  | | | |
| 1. Open the terminals of the two machines and check that they have no internet access 2. ping the address 8.8.8.8 to check for an internet connection 3. The output should be “Destination Host Unreachable | |  | | | |
| 1. To check whether the two machines can connect, we must ping each IP address 2. For Ubuntu:   **ping 192.168.100.10**   1. For Kali   **ping 192.168.100.20**   1. They should be able to successfully ping 2. Close both terminals and shut down both machines | | |  | | | |

1. **THINGS TO NOTE**

**3.1. Best Practices**

Outlined below are the best practices to consider when setting up a virtual environment.

* 1. Ensure that the operating systems you use can support all the necessary processes that would be performed with it.
  2. Set up a secure host system by making sure your system is up-to-date with the latest security updates. This can be your first line of defense incase of a VM leak (a situation whereby processes in the virtual environment affect the host system)
  3. Make sure your environment is on its own internal network, isolated from the internet,
  4. Document findings and processes.
  5. Take snapshots at every significant step taken to have a restore point if things go wrong. This serves as a backup for data loss
  6. Practice ethical hacking. Always gain permission before trying the skills you use in your virtual environment on another machine or network.

**3.2. Troubleshooting**

Outlined below are the problems I faced and how I was able to solve them.

**Problem 1**: I did not capture screenshots at critical points while working on my DVWA server. Consequently, when complications arose while connecting the database to the application, I had to restore the machine to its initial state, which was the only available restore point.

**Solution:** Created snapshots at every major point in the process

**Problem 2:** The incorrect configuration of Kali Linux adapters prevented the creation of a static IP address. Adapter 1 was set as the NAT adapter and Adapter 2 as the Internal Network adapter, intended for the static IP configuration. However, Kali Linux defaults to selecting enp0 (Adapter 1). Consequently, disabling Adapter 1 in favor of Adapter 2 resulted in Adapter 2 not being recognized

**Solution:** Applied internal network configurations to Adapter 1 and NAT configurations to Adapter 2.

**Problem 3:** When the MySQL database is installed, a security script must be run. As of 2022, certain issues would arise if certain steps were not taken before the script was run. I did not know this until it was too late, leading to those unexpected results.

**Solution:** Restored snapshot and performed critical steps.

**Problem 4:** Incorrect configuration of the PHP file responsible for connecting the DVWA to the database.

**Solution:** Restored the initial state and reconfigured the file.

**Problem 5:** Forgot to set the clipboard of the virtual machine to be bidirectional to copy long lines of code from the documentation to the terminal. This made writing the commands take more time.

**Solution:** Set the clipboard of machines to bidirectional

1. **EXPERIENCE**

While developing the virtual machines, I thoroughly researched each area and formulated a plan to ensure success. Setting up Kali Linux was straightforward, thanks to the clear instructions provided by the IAS Lab 2 manual. However, configuring the DVWA proved more challenging, as there was no single comprehensive resource available; I had to consult multiple websites covering different Ubuntu versions to piece together the required steps. My prior experience made setting up the LAMP stack easier but connecting it to the DVWA posed certain database configuration issues that initially stalled progress. Despite the frustration, I restarted from the beginning and was able to proceed smoothly. This experience was highly valuable, offering practical learning opportunities and fostering extensive research skills.

1. **SOURCES**

* What is Kali Linux

URL: <https://www.kali.org/docs/introduction/what-is-kali-linux/>

* What Is Nmap? A Comprehensive Guide For Network Mapping

URL: <https://www.geeksforgeeks.org/what-is-nmap-a-comprehensive-guide-for-network-mapping/>

* SQL Injection Attacks – How to Use SQLMap to Find Database Vulnerabilities

URL: <https://www.freecodecamp.org/news/how-to-protect-against-sql-injection-attacks/>

* MySQL Tutorial

URL: <https://www.w3schools.com/mysql/>

* What is PHP? The PHP Programming Language Meaning Explained

<URL:https://www.freecodecamp.org/news/what-is-php-the-php-programming-language-meaning-explained/>

* The Best DVWA (Damn Vulnerable Web Application) 2024 Guide

URL: <https://www.stationx.net/dvwa-damn-vulnerable-web-application/>

* How to Install and Configure DVWA Lab on Ubuntu 18.04 server

URL: <https://kifarunix.com/how-to-setup-damn-vulnerable-web-app-lab-on-ubuntu-18-04-server/>

* How To Install Linux, Apache, MySQL, PHP (LAMP) Stack on Ubuntu

URL: <https://www.digitalocean.com/community/tutorials/how-to-install-lamp-stack-on-ubuntu>

* How to Create and Use VirtualBox Snapshots

URL: <https://www.baeldung.com/linux/virtualbox-snapshots>

* Initial Server Setup with Ubuntu 20.04

URL: <https://www.digitalocean.com/community/tutorials/initial-server-setup-with-ubuntu-20-04>

* How to run an Ubuntu Desktop virtual machine using VirtualBox 7

URL: <https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-on-a-virtual-machine-using-virtualbox#1-overview>

* **How to Install DVWA in Ubuntu**

URL: <https://securingninja.com/how-to-install-dvwa-in-ubuntu/>