## **Detailed Penetration Test Report**

### **Project Overview**

For this project, I performed a penetration test on my mother's network. The goal was to identify potential vulnerabilities and assess the security posture of her home network.

### **Step-by-Step Process**

#### **Step 1: Initial Network Scan**

**Command:** sudo nmap 192.168.0.114 -sV -O -p1-65535

* **Description:**
  + **Nmap:** A powerful network scanning tool used to discover hosts and services on a computer network.
  + **sudo:** Grants root privileges necessary for certain Nmap options.
  + **192.168.0.114:** Target IP address.
  + **-sV:** Detects service versions.
  + **-O:** Detects the operating system.
  + **-p1-65535:** Scans all 65,535 ports.
* **Details:**
  + This was a comprehensive stealth scan that took about 25 minutes.
  + The scan provided detailed information about the different services running on the target machine, as well as the open ports.

#### **Step 2: Installing Dirb**

**Command:** sudo apt install dirb

* **Description:**
  + **Dirb:** A web content scanner used to find existing (and often hidden) web objects.
  + **sudo apt install:** Command to install software on Debian-based Linux distributions.
* **Purpose:**
  + Dirb helps in searching for directories and files that might be vulnerable or exposed unintentionally.

#### **Step 3: Running Dirb**

**Command:** dirb http://192.168.0.114

* **Description:**
  + Scans the specified URL for hidden directories and files.
* **Outcome:**
  + Dirb provided a list of directories and files found on the web server at the target IP address.

#### **Step 4: Vulnerability Search**

* **Process:**
  + Dirb continues to search for any vulnerabilities within the discovered directories and files.
  + Analyzes the results for potential security issues.

#### **Step 5: Extended Dirb Search**

**Command:** dirb http://192.168.0.114/cgi-bin/

* **Description:**
  + Targets the common cgi-bin directory, often a source of vulnerabilities due to improperly secured CGI scripts.
* **Outcome:**
  + Generated a report of approximately 2000 words detailing the discovered files and potential vulnerabilities.

#### **Step 6: Exploit Search with Metasploit**

**Tool:** Metasploit Framework

* **Description:**
  + **Metasploit:** A popular penetration testing framework that helps in discovering, testing, and exploiting vulnerabilities.
  + Used to search for known exploits that could be used against the discovered services and vulnerabilities.
* **Process:**
  + Conducted various searches within Metasploit to identify potential exploits applicable to the target system.

#### **Step 7: Preparing Exploit Code**

**Commands:**

* sudo apt install mousepad
* touch 37292.c
* mousepad 37292.c
* **Description:**
  + **Mousepad:** A simple text editor.
  + **touch 37292.c:** Creates a new file named 37292.c.
  + **mousepad 37292.c:** Opens the file in Mousepad for editing.
* **Purpose:**
  + To prepare and edit exploit code for further testing.

#### **Step 8: Storing Findings**

* **Process:**
  + All findings, notes, and codes were stored and edited within Mousepad.

#### **Step 9: Using Unshadow Password**

**Process:**

* **Unshadowing:** Combining password and shadow files to prepare them for cracking.
* Although the password was already known, this step involves using the unshadow command when necessary to crack encrypted passwords.

### **Conclusion**

This penetration test identified several potential vulnerabilities and provided insights into the security posture of the network. The process involved comprehensive scanning, vulnerability detection, and exploitation attempts using various tools like Nmap, Dirb, and Metasploit. The findings were documented and analyzed to enhance the security of the target network. Although I understood the assignment for learning how to perform a basic penetration test, and I was also able to perform basic functions for the test, i’ve also realized that I need to get my mother a VPN since she doesn’t have great security measures in place. So more detailed information on the test was not provided.

**Source**

<https://www.youtube.com/watch?v=B7tTQ272OHE&t=141s>