**DEPI**

Penetration Test Report for   
metasploitable2

pentester: Mahmoud reda mohamed

Client Name: Eng.Khalid Aymen

Date of Assessment: 12/8/2024

Confidentiality Notice:

This report contains sensitive information. Unauthorized access, distribution,

or copying of this document is strictly prohibited

**Table of Contents**

**1.0 Penetration Test Report 3**

**1.1 Introduction** 3

**1.2 Objective** 3

**2.0 High-Level Summary 4**

**2.1 Recommendations** 5

**3.0 Methodologies 5**

**3.1 Information Gathering** 5

**3.2** Service Enumeration 6

**3.3** Penetration 7

**1.0 Penetration Test Report**

**1.1 Introduction**

This report outlines the findings from a network penetration testing exercise conducted as part of the DEPI initiative. The testing was commissioned by Eng. Khaled Aymen, who tasked our team with assessing the security of the network using a machine obtained from VulnHub. This exercise aimed to identify vulnerabilities and potential security weaknesses within the network infrastructure, providing insights and recommendations to enhance overall security posture..

**1.2 Objective**

The objective of this assessment is to conduct an internal penetration test against a Metasploitable2 machine within the internal home network. The student is tasked with a methodical approach to gain access to the target machine, identify vulnerabilities, and document the findings. This assessment is designed to simulate a real-world penetration test, guiding the student through the entire process from initial reconnaissance to final reporting.

**2.0 High-Level Summary**

Mahmoud Reda was assigned to conduct an internal penetration test on his home network, specifically targeting the Metasploitable2 system. This type of test simulates an attack from within the network, mimicking the actions of a hacker to infiltrate internal systems. The primary objective was to assess the network's security, identify and exploit vulnerabilities, and report the findings to Eng. Khaled Aymen

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the Metasploitable2. When performing the attacks, Mahmoud was able to gain access to the machine, primarily due to outdated patches and poor security configurations. During the testing, Mahmoud had administrative level access to the target machine. Metasploitable2 was successfully exploited and access granted. here is a brief description on how access was obtained are listed below:

* Got in through leveraging an outdated FTP version to obtain administrative access
* Got in through exploiting a file upload vulnerability in Apache Tomcat by uploading a WAR file, which also provided access to the system

**2.1 Recommendations**

Mahmoud recommends patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

**3.0 Methodologies**

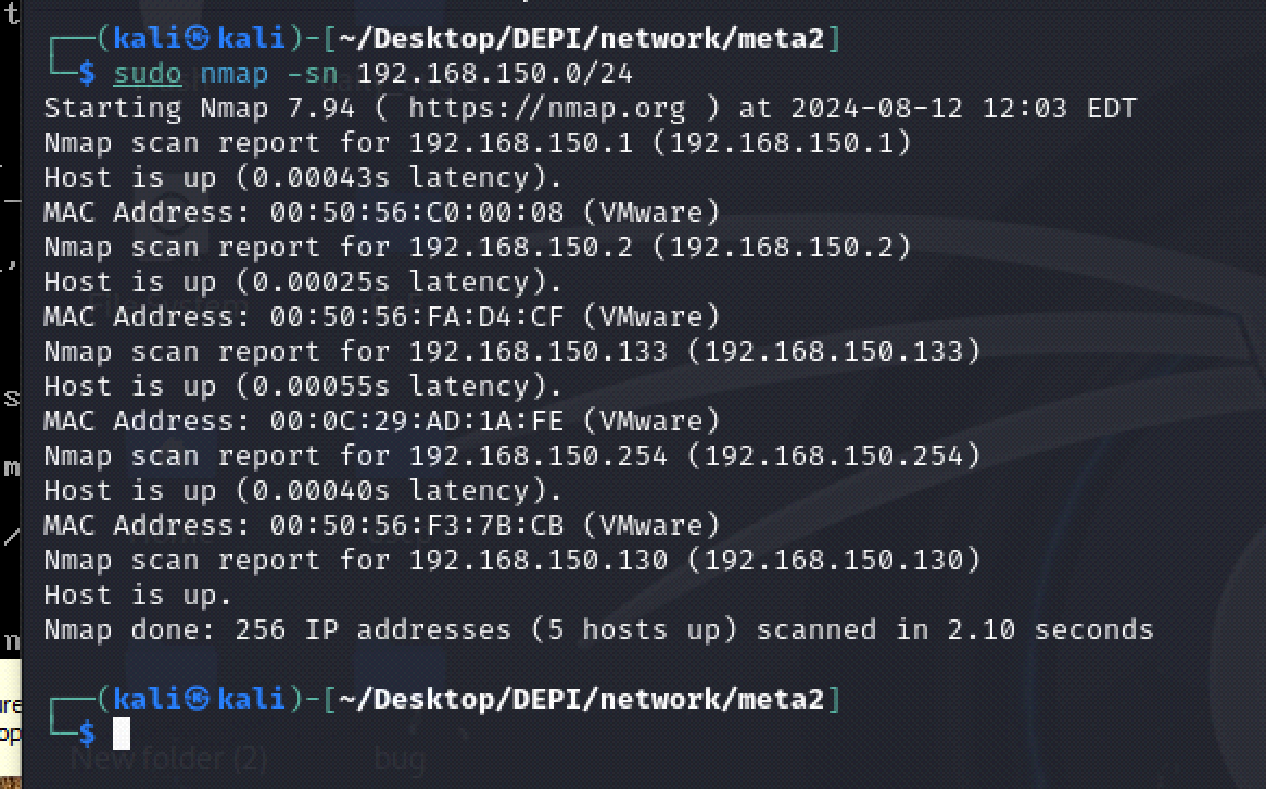
Mahmoud employed a widely recognized penetration testing methodology to effectively evaluate the security of Metasploitable2. Below is a breakdown of how he identified and exploited the machine.

**3.1 Information Gathering**

The information gathering portion of a penetration test focuses on Host discovery. During this penetration test, Mahmoud was tasked with exploiting the home internal network.

**Scope:** 192.168.150.0/24

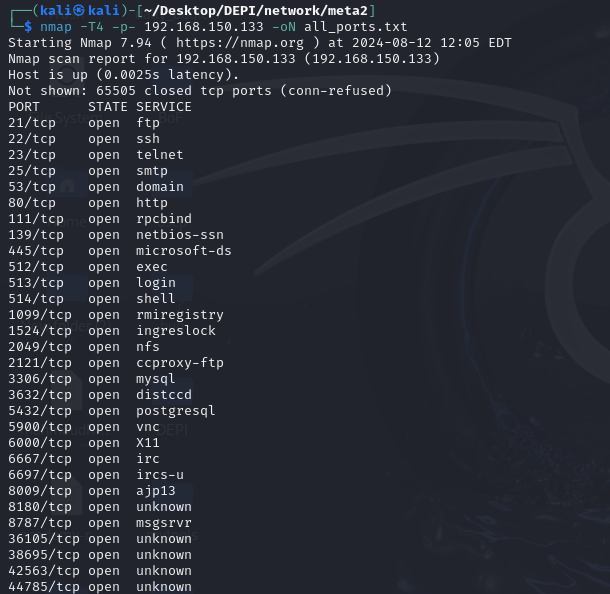
**machine IP:** 192.168.150.133



**3.2 Service Enumeration**

| **Server IP Address** | **Ports Open** |
| --- | --- |
| 192.168.150.133 | **TCP:** 21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,3632,5432,5900,6000,6667,6697,8009,8180,8787,36105,38695,42563,44785 |

**Screenshot Here:**

****

**3.3 Penetration**

| **Vulnerability Exploited:**  VSFTPD v2.3.4 Backdoor Command Execution  **System Vulnerable:** 192.168.150.133  **Vulnerability Explanation**: This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011., a targeted attack was performed on the system which gave Mahmoud full administrative access over the system.  **Vulnerability Fix**: This backdoor was removed on July 3rd 2011 and update the service is a must  **Severity: Critical**  **Screenshot Here:** |
| --- |
| **Vulnerability Exploited:** Remote Code Execution (RCE) through the upload and deployment of a .war file to the Tomcat Web Application Manager.  **System Vulnerable:** 192.168.150.133  **Vulnerability Explanation**: By leveraging the default credentials of Apache Tomcat, we were able to access the Tomcat Web Application Manager. This access allowed us to upload and deploy a .war file, effectively executing arbitrary code on the server. Deploying a .war file requires sufficient privileges, specifically roles such as admin, manager, or manager-script. Upon logging in with the default credentials (tomcat:tomcat), we obtained the necessary privileges to exploit this attack vector.  **Vulnerability Fix**:   * **Remove Default Credentials**: Immediately disable or change the default tomcat:tomcat credentials to a strong, unique username and password combination. * **Restrict Access to the Manager Interface**: Limit access to the Tomcat Web Application Manager by configuring it to be accessible only from trusted IP addresses or networks. * **Regularly Update Tomcat**: Ensure that the Apache Tomcat server is regularly updated to the latest version, applying any security patches promptly.   **Severity: Critical**  **Screenshot Here:** | |