Southern
New Hampshire
University

CYB 240 Project One Milestone Template

Andree Salvo
Southern New Hampshire University
CYB 240-13711
Instructor: Brian Remson

Firewall OpenVAS Report

Vulnerability One

- **Identification:** PHP End of Life Detection (Windows), CVSS Score: 10.0, PHP Version: 5.3.1
- **Description:** The system is running on PHP 5.3.1, making it an easy target for attackers to exploit, and it hasn't gotten any security updates since 2014
- **Mitigation:** Upgrading the PHP to a supported version will help keep things aligned and get security updates and patches ASAP.

Vulnerability Two

- **Identification**: Apache Web Server End of Life Detection (Windows), CVSS Score: 10.0, Apache Version: 2.2.14
- **Description:** The server uses Apache 2.2.14 and hasn't received any security updates from its vendor, making it vulnerable to an attacker who could compromise the security of the host.
- **Mitigation:** They need to upgrade Apache to a supported version so it stays protected with the latest security patches and updates.

Windows Server OpenVAS Report

Vulnerability One

- **Identification:** PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Windows), CVSS Score: 7.5, CVEs: CVE-2016-10159, CVE-2016-10160
- **Description:** The installed version was on 5.3.1, and this version was known for bugs that could let an attacker either crash an application or eat up the memory data.
- **Mitigation**: They need to upgrade PHP to 5.6.30 or later since anything below that is still vulnerable to those crash bugs.

Vulnerability Two

- **Identification**: PHP socket_connect() Buffer Overflow Vulnerability (Windows), CVSS Score: 7.5, CVE: CVE-2011-1938
- Description: This vulnerability is running off 5.3.1 and it is prone to stack buffer overflow vulnerability

- **Mitigation**: Upgrading from 5.3.1 to 5.3.7 is the latest version since 5.3.7 is the version where the buffer overflow bug got patched

Ubuntu Server OpenVAS Report

Vulnerability One

- **Identification**: MySQL / MariaDB Weak Password, CVSS Score: 9.0
- **Description**: For this vulnerability, the MYSQL setup is running off root with no password, meaning that anyone can log in and take over. This is high due to security holes.
- **Mitigation**: Setting up a strong root password, changing the password as soon as possible, and locking down whoever can access the MySQL service.

Vulnerability Two

- **Identification**: vsftpd Compromised Source Packages Backdoor Vulnerability, CVSS Score: 7.5
- **Description**: The server uses a backdoored version of vsftpd (2.3.4), and this gives attackers a way to run commands, such as manipulating their part of the system.
- **Mitigation**: They need to uninstall the backdoored version and reinstall a legit copy of vsftpd from a trusted source, and know that it’s verified, so they’re not bringing in another sketchy package.