Phase 1

Vulnerability Scanning Report

Objective

The Objective of this phase was to perform Vulnerability Scanning using multiple tools like Nmap, Nikto, OpenVAS(Greenbone) which are commonly available in Kali Linux Environment. The Goal is to identify outdated services and identify unwanted/misconfigured ports.

Tools used

- Nmap
- OpenVAS
- Nikto
- Kali Linux

Methodology

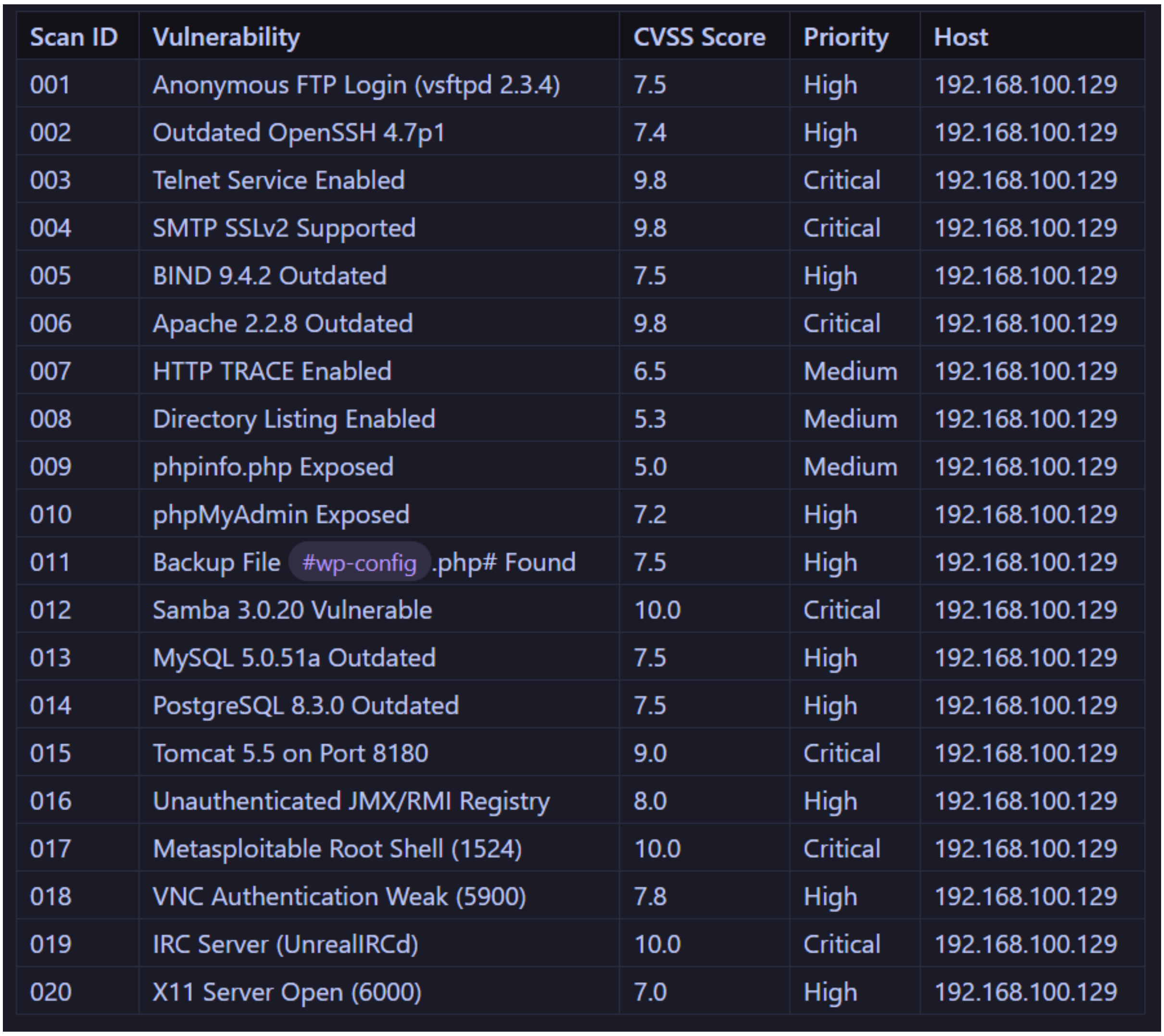
1. **Network scanning using Nmap.**
   A port scan was launched using the command given below:
   Command: nmap -sC -sV <target-ip> -oN nmap_scan.txt
   The scan Results are attached to this document and further ahead a sample extract is provided.
2. **Web Vulnerability Scanning using Nikto**
   Nikto was used to perform the scan on the target.
   Command: nikto -h http://<target-ip>
   The above scan was saved in several formats for demonstration purposes which are attached to this document phase folder.

3. **OpenVAS Vulnerability Scanner.**
   OpenVAS was used to perform Full Vulnerability scan on this Target IP Address. The scan was configured Full and fast. It also resulted in pdf containing full of information about vulnerabilities. This document is also attached.

Findings table

The Below table represents the vulnerabilities present with the appropriate CVSS score and priority.

Vulnerability Assessment Table



Scan ID	Vulnerability	CVSS Score	Priority	Host
001	Anonymous FTP Login (vsftpd 2.3.4)	7.5	High	192.168.100.129
002	Outdated OpenSSH 4.7p1	7.4	High	192.168.100.129
003	Telnet Service Enabled	9.8	Critical	192.168.100.129
004	SMTP SSLv2 Supported	9.8	Critical	192.168.100.129
005	BIND 9.4.2 Outdated	7.5	High	192.168.100.129
006	Apache 2.2.8 Outdated	9.8	Critical	192.168.100.129
007	HTTP TRACE Enabled	6.5	Medium	192.168.100.129
008	Directory Listing Enabled	5.3	Medium	192.168.100.129
009	phpinfo.php Exposed	5.0	Medium	192.168.100.129
010	phpMyAdmin Exposed	7.2	High	192.168.100.129
011	Backup File #wp-config.php# Found	7.5	High	192.168.100.129
012	Samba 3.0.20 Vulnerable	10.0	Critical	192.168.100.129
013	MySQL 5.0.51a Outdated	7.5	High	192.168.100.129
014	PostgreSQL 8.3.0 Outdated	7.5	High	192.168.100.129
015	Tomcat 5.5 on Port 8180	9.0	Critical	192.168.100.129
016	Unauthenticated JMX/RMI Registry	8.0	High	192.168.100.129
017	Metasploitable Root Shell (1524)	10.0	Critical	192.168.100.129
018	VNC Authentication Weak (5900)	7.8	High	192.168.100.129
019	IRC Server (UnrealIRCd)	10.0	Critical	192.168.100.129
020	X11 Server Open (6000)	7.0	High	192.168.100.129

Critical Vulnerabilities

CVE-2010-2861 – Apache 2.2.8 Directory Traversal

- **Description:** The Apache running in the target machine contains Directory traversal vulnerability which allows unrestricted access of server files.
- **Impact:** Exposure of config-files, credentials, or unauthorized web content.
- **Remediation:** Update Apache to the Latest Version Available to Resolve the issue.

Escalation:

Subject: Apache Vulnerability found (Critical).

Hi Team,

During the vulnerability scanning performed on the Target VM, we found a Critical Vulnerability related to the Apache web server running in the target. It allows unrestricted Directory Traversal, exposing server files, Configuration files, Other sensitive Information. I recommend to update the Apache to the latest version available to resolve this issue as soon as possible.

Thanks,
Aniket