Simulated Vulnerability Scan Results (Nmap + Nikto)

Analyst: Alexander T. Ramos Date: October 05, 2025

Scan Metadata

Scanner: Kali Linux: nmap 7.93, nikto 2.1.6 (simulated)
Target: Metasploitable 2 (192.168.56.101)
Scan Type: TCP SYN scan (-sS), service/version detection (-sV), default scripts (-sC)
Duration: Approx. 00:08:42

Nmap Scan (excerpt)

```
# Nmap 7.93 scan report for 192.168.56.101
Host is up (0.00098s latency).
Not shown: 995 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4 (backdoor)
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)
139/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp open microsoft-ds Samba smbd 3.X
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
- ftp-backdoor: DETECTED (vsftpd backdoor)
- ssl-cert: Subject: /CN=localhost
- smb-os-discovery: OS: Unix (Samba 3.X)
```

Web Application Scan (Nikto excerpt)

```
- Nikto v2.1.6 vhost/Host: 192.168.56.101
+ Target IP: 192.168.56.101
+ Port: 80
+ Server: Apache/2.2.8 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5
+ The X-Frame-Options header is not present
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /admin/: Possible administrative interface found
+ /phpmyadmin/: phpMyAdmin installation possibly found
+ OSVDB-3092: /icons/README: Apache default file found, possible information disclosure
```

Identified Vulnerabilities (sample)

Severity	Title	CVE / Notes
Critical	vsftpd backdoor - remote shell	CVE-2011-2523 - Remote backdoor (public exploit)
High	Apache 2.2.8 path traversal	CVE-2011-3192 / Multiple RCE vectors
High	Samba smbd remote code execution	CVE-2007-2447 (example)
Medium	MySQL weak/default credentials	Verify accounts and credentials
Low	Missing security headers (X-Frame-Options)	Information disclosure

Remediation Recommendations (excerpt)

1. Disable or remove vsftpd service; restrict access or apply vendor patch to remove backdoor.
2. Upgrade Apache to a supported version and apply security patches; restrict HTTP methods and implement security headers.
3. Harden Samba configuration or upgrade; apply vendor patches addressing RCE issues.
4. Enforce strong credentials on MySQL and disable remote root logins; remove default accounts.
5. Re-run credentialed scans after remediation and validate via manual verification steps.

Appendix: Sample Commands Used (for reproduction)

```
nmap -sS -sV -sC -p- 192.168.56.101
nikto -h http://192.168.56.101
nmap -sV --script=ftp-backdoor 192.168.56.101
nmap --script smb-os-discovery 192.168.56.101
```

Note: This document is a simulated scan output for training and portfolio purposes. It does not contain live customer data.