CYBERSECURITY AUDIT SIMULATION LAB GUIDE

Author: Great Ezenwa | Cybersecurity Analyst

OBJECTIVE

Perform a basic vulnerability assessment of a simulated network environment using Kali Linux tools (Nmap, Nikto, and Burp Suite).

1. Lab Setup (Safe & Isolated)

Requirements:

- Computer with at least 8 GB RAM
- VirtualBox or VMware • Kali Linux ISO
- Target machine (Metasploitable2 or DVWA) Ensure the network uses a Host-Only Adapter for isolation.

2. Network Configuration

Check IPs and confirm connectivity:

```
Sudo netdiscover / ifconfig
ping 192.168.56.128
```

3. Reconnaissance with Nmap

Run the following scan to identify open ports:

- *nmap -sS -sV –p- 192.168.56.128*

```
┌──(wolf㉿kali)-[~]
└─$ nmap -sS -sV -p- 192.168.56.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-23 18:46 EDT
Nmap scan report for 192.168.56.128
Host is up (0.0021s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

4. Web Vulnerability Scan (Nikto)

Nikto analyzes web vulnerabilities such as outdated servers, directory listings, and XSS.

```
nikto -h http://192.168.56.128
```

```
┌──(wolf㉿kali)-[~]
└─$ nikto -h http://192.168.56.128
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.128
+ Target Hostname:    192.168.56.128
+ Target Port:        80
+ Start Time:         2025-10-24 09:18:13 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.moz
illa.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render
 the content of the site in a different fashion to the MIME type. See: https://www.netsparke
r.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is
the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easil
y brute force file names. The following alternatives for 'index' were found: index.php. See:
```

5. Manual Testing with Burp Suite

Configure your browser proxy to 127.0.0.1:8080 and intercept traffic for analysis.

6. Reporting and Recommendations

Category	Finding	Risk Level	Recommendation
Ports	Open SSH, FTP, HTTP, MySQL	High	Restrict access or use firewall

Web Server	Directory Listing Enabled	Low	Disable directory listing
Authentication	Weak login forms	Medium	Enforce strong password policies

7. Ethical and Safety Note

Always perform scans only on systems you own or have explicit permission to test. This guide is for educational and portfolio purposes only