Lab 8. Perform network vulnerability scan using Nikto.

Target web server for testing (e.g., a local DVWA instance or Metasploitable).

Step 1: Install Nikto

1. Verify if Nikto is installed:
2. nikto -Version
3. If not installed:
4. sudo apt update
5. sudo apt install nikto

Step 2: Identify Target

1. Get the IP address of your test environment:
2. ifconfig
3. Verify the target is reachable:
4. ping <target_ip>

Step 3: Perform a Basic Scan

1. Run a basic vulnerability scan against the target web server:
2. nikto -h <target_ip>
   - Replace <target_ip> with the IP address of your target system.
3. Screenshot: Show the scan in progress or its results.

Step 4: Perform Advanced Scans

Scan a Specific Port

To scan a specific port (e.g., 8080):

nikto -h <target_ip> -p 8080

Save Results to a File

Save scan results in a text or HTML file:

nikto -h <target_ip> -o results.html -Format html

Use SSL

To scan an HTTPS server:

nikto -h <target_ip> -ssl

Use Plugins

To run specific plugins:

nikto -h <target_ip> -Plugins <plugin_name>

Example:

nikto -h <target_ip> -Plugins all

Step 5: Interpret the Results

1. **Review the identified vulnerabilities:**
   - Missing security headers (e.g., X-Frame-Options, Content-Security-Policy).
   - Outdated software or libraries.
   - Directory listings enabled.
   - Open or misconfigured ports.
2. **Prioritize remediation based on criticality:**
   - Patching outdated software.
   - Implementing proper access control.
   - Disabling unnecessary services or ports.

Step 6: Mitigation Recommendations

1. Update Software: Ensure all web server components are up-to-date.
2. Use Secure Headers: Add headers like Strict-Transport-Security and X-Content-Type-Options.
3. Encrypt Traffic: Use SSL/TLS for all communications.
4. Restrict Access: Use firewalls and network policies to limit exposure.