Information Gathering & Web Enumeration Project

Objective

To perform information gathering and web enumeration on vulnerable web applications hosted on OWASP BWA using tools like Nikto, Nmap, Ping, Nslookup, Host, Google Dorks, WhatWeb, and Dirb.

Tools Used

- OWASP BWA (target VM)
- Kali Linux (attacker machine)
- Nikto
- Nmap
- Ping
- Nslookup
- Host
- Google Dorks
- WhatWeb
- Dirb

Lab Setup

1. Download and run OWASP BWA in VMware/VirtualBox using Bridged Adapter.
2. Find OWASP BWA IP using 'ip a' on BWA terminal.
3. Ensure Kali and OWASP BWA can ping each other.

Project Steps

1. Ping the Target

ping <OWASP-BWA-IP>

Information Gathering & Web Enumeration Project

2. DNS Enumeration

a. Nslookup: nslookup <OWASP-BWA-IP>

b. Host Lookup: host <OWASP-BWA-IP>

3. Nmap Scan

a. Basic Scan: nmap -sS <OWASP-BWA-IP>

b. Aggressive: nmap -A <OWASP-BWA-IP>

c. Vulnerability: nmap --script vuln <OWASP-BWA-IP>

4. WhatWeb Scan

whatweb http://<OWASP-BWA-IP>

5. Directory Brute Forcing (Dirb)

dirb http://<OWASP-BWA-IP>

6. Vulnerability Scan with Nikto

nikto -h http://<OWASP-BWA-IP>

7. Google Dorks (Browser)

Examples:

- site:<target>

- inurl:admin

- intitle:index of

- filetype:php

Deliverables

1. Screenshots of each command and result.

2. Documented observations (open ports, web tech, dirs, vulnerabilities).

3. Final Report (.pdf or .docx):

- Introduction

- Methodology

- Tools Used

- Findings

- Conclusion

Bonus Tips

- Use '-oN result.txt' with Nmap to save results.

- Compare results across tools.

- Add mitigation suggestions or charts if desired.