# Website Scanning Mastery Guide (Day 1-30)

This guide covers tools and commands for web application scanning, organized day-by-day for progressive learning.

---

## Day 1: Whois Lookup

- **Command:** `whois example.com`
- **Purpose:** Retrieve domain registration details.

## Day 2: DNS Resolution

- **Command:** `nslookup example.com`
- **Purpose:** Resolve domain to IP address.

## Day 3: DNS Records Lookup

- **Command:** `dig example.com any`
- **Purpose:** Obtain all DNS records.

## Day 4: Host Availability

- **Command:** `ping example.com`
- **Purpose:** Check if the host is reachable.

## Day 5: Network Path Mapping

- **Command:** `traceroute example.com`
- **Purpose:** Trace the route packets take to reach the host.

## Day 6: Web Port Scan

- **Command:** `nmap -p 80,443 example.com`
- **Purpose:** Scan common web service ports.

## Day 7: Service Version Detection

- **Command:** `nmap -sV example.com`
- **Purpose:** Identify versions of services running on open ports.

## Day 8: Grab Web Page Title

- **Command:** `nmap --script=http-title example.com`

- **Purpose:** Retrieve title of the website.

## Day 9: Enumerate Common Directories

- **Command:** `nmap --script=http-enum example.com`
- **Purpose:** Discover common web directories.

## Day 10: SSL Port Scan

- **Command:** `nmap -p 443 --script=ssl-enum-ciphers example.com`
- **Purpose:** Scan SSL/TLS configurations.

## Day 11: Web Server Vulnerability Scan

- **Command:** `nikto -h example.com`
- **Purpose:** Scan web server for known vulnerabilities.

## Day 12: Directory Brute-force

- **Command:** `gobuster dir -u http://example.com -w wordlist.txt`
- **Purpose:** Discover hidden directories.

## Day 13: WordPress Scan

- **Command:** `wpscan --url example.com`
- **Purpose:** Scan WordPress installations for vulnerabilities.

## Day 14: Technology Detection

- **Command:** `whatweb example.com`
- **Purpose:** Identify technologies used by the site.

## Day 15: Framework Detection

- **Command:** `wappalyzer-cli example.com`
- **Purpose:** Detect web frameworks and CMS.

## Day 16: SSL Scan

- **Command:** `sslscan example.com`
- **Purpose:** Test SSL/TLS configurations.

## Day 17: Detailed TLS Scan

- **Command:** `testssl.sh example.com`
- **Purpose:** Comprehensive TLS/SSL vulnerability scan.

## Day 18: Inspect HTTP Headers

- **Command:** `curl -I https://example.com`
- **Purpose:** Check HTTP headers for security information.

## Day 19: SSL Nikto Scan

- **Command:** `nikto -ssl -h example.com`
- **Purpose:** Scan SSL-enabled web endpoints.

## Day 20: Directory Discovery

- **Command:** `dirb http://example.com wordlist.txt`
- **Purpose:** Brute-force directories on the web server.

## Day 21: Fast Web Fuzzer

- **Command:** `ffuf -u http://example.com/FUZZ -w wordlist.txt`
- **Purpose:** Quickly find hidden resources.

## Day 22: SQL Injection Testing

- **Command:** `sqlmap -u "http://example.com/page?id=1" --batch`
- **Purpose:** Test for SQL injection vulnerabilities.

## Day 23: Subdomain Enumeration

- **Command:** `sublist3r -d example.com`
- **Purpose:** Find subdomains associated with the domain.

## Day 24: Advanced Subdomain Scan

- **Command:** `amass enum -d example.com`
- **Purpose:** Detailed subdomain enumeration.

## Day 25: Save Nikto Reports

- **Command:** `nikto -h example.com -output report.html`
- **Purpose:** Save vulnerability scan report.

## Day 26: Automated Recon Scripts

- **Command:** Custom Bash/Python scripts combining previous tools
- **Purpose:** Automate full website reconnaissance.

## Day 27: Burp Suite Proxy Scan

- **Command:** Use Burp Suite to intercept and scan web traffic
- **Purpose:** Analyze HTTP requests and test for vulnerabilities.

## Day 28: OWASP ZAP Proxy Scan

- **Command:** Use OWASP ZAP to scan website
- **Purpose:** Automated vulnerability testing via proxy.

## Day 29: Analyze HTTP Requests

- **Command:** Capture and analyze traffic with Burp/ZAP or tcpdump
- **Purpose:** Identify vulnerable endpoints and parameters.

## Day 30: Reporting & Documentation

- **Command:** Compile findings and prepare penetration test report
- **Purpose:** Document vulnerabilities and security posture.

---

**Note:** Only scan websites that you are authorized to test. Unauthorized scanning is illegal.