Security Strategies in Web Applications and Social Networking

Lesson 12

Performing a Web Site Vulnerability and Security Assessment

Learning Objective and Key Concepts

Learning Objective

- Explain the value and importance of vulnerability and security assessments for Web applications.

Key Concepts

- Difference between audit, testing, and assessment
- Main steps in security assessments
- Techniques and best practices in security assessments

Web Software Testing, Auditing, and Assessing

- Testing
  - Ensures business requirements are met
  - Operates as expected
  - Integrates well with other software
  - Security testing is typically a subset

Web Software Testing, Auditing, and Assessing (Continued)

- Audit
  - Ensures proper controls are documented as policy
  - Ensures the documented controls are in place
- Security assessment

Security Assessment: What to Test?

- Operating System
- Web Server
- Database Server
- Web Application Software

Security Assessment: Vulnerability Scan

- Uses a variety of tools (open source and commercial)
- Combination of manual and security tools
- Servers vulnerabilities
- Web application vulnerabilities

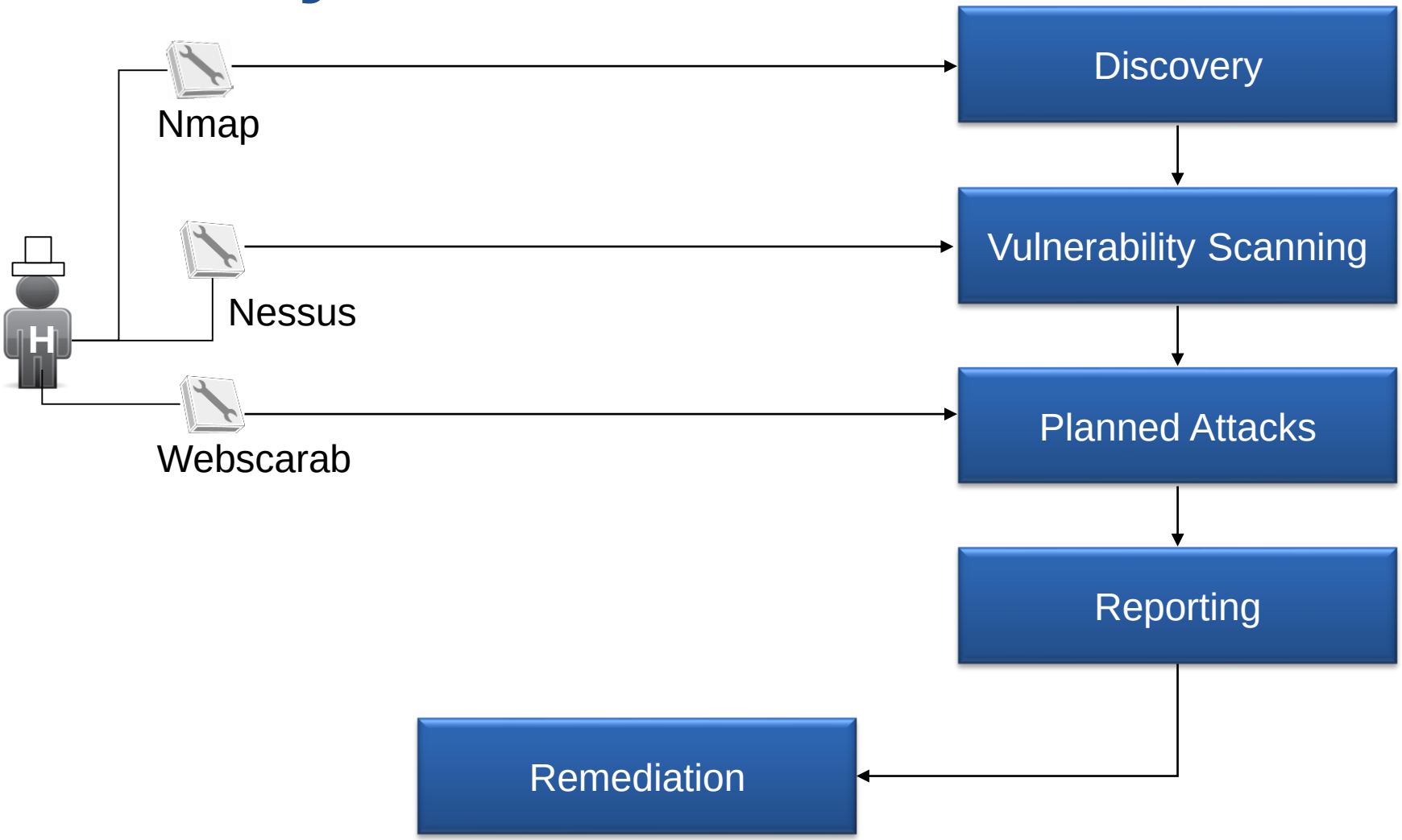
Security Assessment: How to Test?

- Discovery
- Perform a vulnerability scan
- Planned attacks
- Reporting

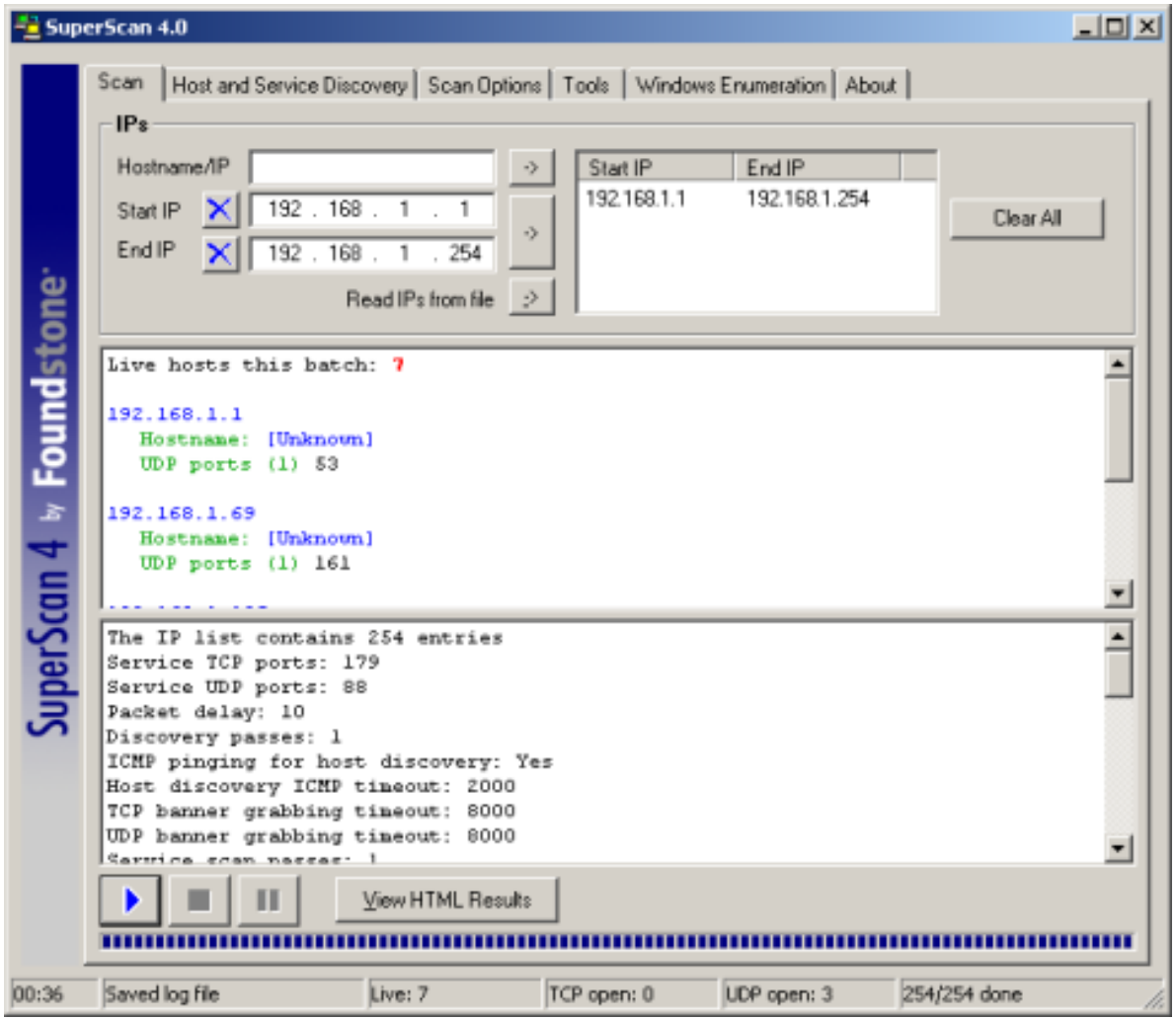
Security Assessment: Discovery

- Fingerprinting
- Ping sweeping
- Operating system detection
- Port scanning

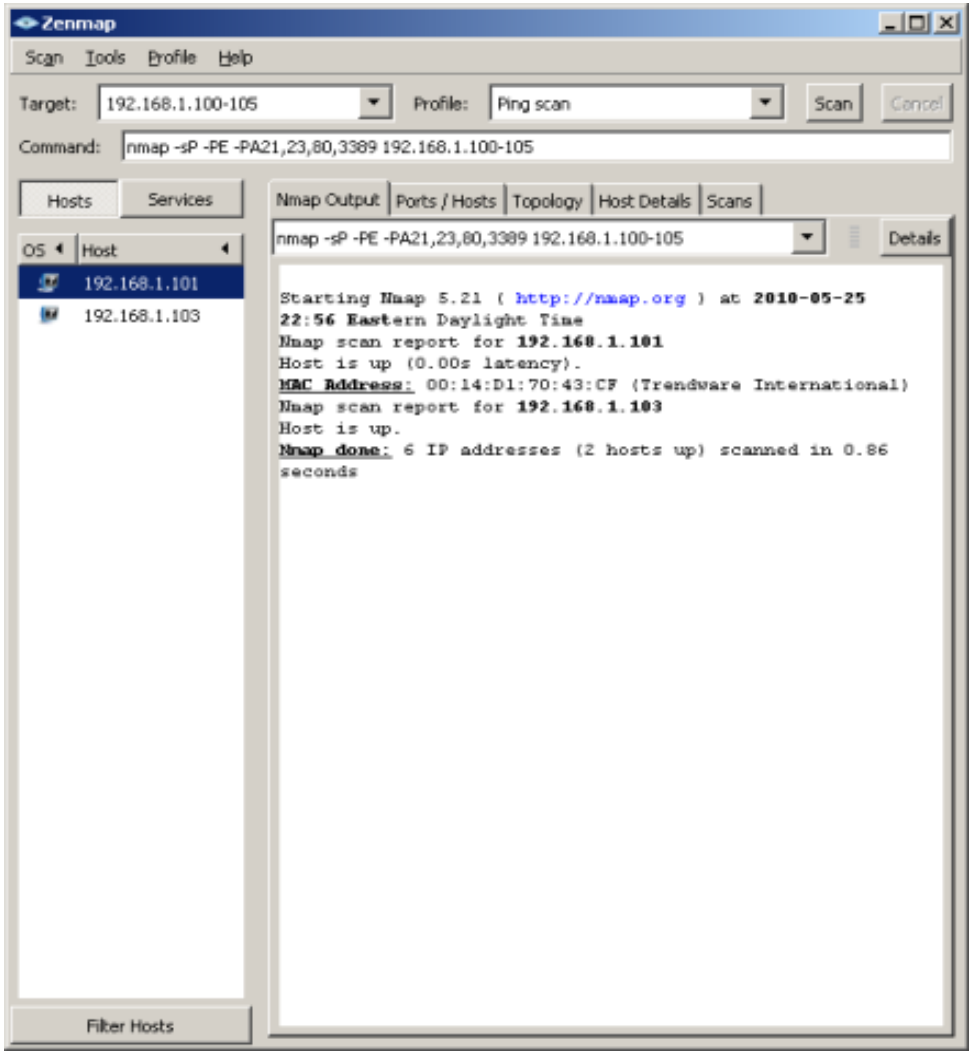
Security Assessment



Example of Ping Sweep Tool



Example of Port Scanning Tool



Nessus Vulnerability Scan

List of hosts

192.168.1.103 — High Severity problem(s) found

[^] Back

192.168.1.103

Scan Time

Start time :	Tue May 25 22:08:52 2010
End time :	Tue May 25 22:12:31 2010

Number of vulnerabilities

Open ports :	10
High :	1
Medium :	1
Low :	41

Remote host information

Operating System :	Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3
NetBIOS name :	ACME-GG9FRPF9CG
DNS name :	acme-gg9frpf9cg.hsd1.ga.comcast.net.

[^] Back to 192.168.1.103

Port general (0/tcp) [-/+]

Nessus Scan Information

Information about this scan :

Nessus version : 4.2.2 (Build 9129)
Plugin feed version : 201005251334
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.1.103
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2010/5/25 22:08
Scan duration : 219 sec

Single Server Web Site Components

Web server OS	The operating system of the hardware server that the components reside on
Web server application	The application that collects, uses, and/or provides data
Web server front end	The Web server software that presents the application to users in the form of HTTP pages
Web site forms	The input fields, or forms, that are used to gather data from users

Security Assessment: When to Test?

- Frequently
- Payment Card Industry Data Security Standard (PCI DSS) requires at least quarterly scans for all merchant levels

Web Security Assessment for PCI DSS Compliance

Organization engages a security company with a Qualified Security Assessor (QSA).

QSA discovery/recommendations

QSA enters discovery phase.

Scanning performed

QSA recommends a SaaS, external organization, or internal process for vulnerability scanning.

Planned attacks performed

Scanning is performed and quarterly scanning schedule is implemented.

QSA submits report to management

Planned attacks are performed by a skilled Web application security engineer by using manual processes and tools.

Remediation begins

QSA compiles a comprehensive report for management and Web security team.

Remediation

Security Assessment: Planned Attacks

- Front-end Web forms and servers
- Back-end database and file servers

Security Assessment: Reporting

- Executive summary
- Summary of findings
- Details of the vulnerability scan
- Details of the security assessment
- Recommended remediation

Remediation

- Management
- System administrator
- Misconfigured servers
- Security updates

Remediation (Continued)

- Firewall or security administrator
- Misconfigured firewalls
- Security patches
- Web developer
- Insecure Web application code

Best Practices

Choose the Right Tools

Test Inside and Out

Think Outside the Box

Research! Research! Research!

Summary

- Web software testing, auditing, and assessing
- Main steps in security assessments
- Techniques and best practices in security assessments
- Web security assessment for PCI DSS compliance

Virtual Lab

- Performing an IT and Web Application Security Assessment

If your educational institution included the Jones & Bartlett labs as part of the course curriculum, use this script to introduce the lab:

"In this lesson, you explored vulnerability and security assessments of Web applications. You learned the difference between audits, tests, and assessments, and you were introduced to the major phases of a security assessment: discovery, vulnerability scanning, planned attacks and penetration testing, and reporting. Finally, you picked up techniques and best practices for performing security assessments.

In the lab for this lesson, you will apply the research you conducted on the Open Web Application Security Project (OWASP), in the Applying OWASP to a Web Security Assessment lab, to analyze the skipfish and RATS reports generated in the Performing Dynamic and Static Quality Control Testing lab. You will identify the security issues identified by both tools and research remediations for them. You also will map your research findings to specific recommendations and best practices suggested by the OWASP and Open SAMM models."