Appendix E

List of Tools: Vulnerability Scanning and Penetration Testing

Introduction

This appendix can be used with reference to Chapters 2, 4 and 5 of the book. Chapter 2 explains how cyberoffences are planned with active attacks wherein an attacker scans the computer network to locate the security hole to get into the system. Chapters 4 and 5 explain different cyberattacks launched either against the organization and/or against an individual. Hence, computer network security is a vital and an important aspect in cybersecurity. VAPT (Vulnerability Assessment and Penetration Testing) is always discussed with reference to computer network (see Section 1.5.18 of Chapter 1 to understand computer network intrusions); however, it is not only limited to network security. VAPT exercise is conducted to understand the weaknesses in operating system, database and application. The reason being that although an attacker can get into the network, if the security is adequately implemented and monitored at OS/database/application level, then it leaves a minimal chance of damage to the system. Along with it, one should not forget about wireless network, available on mobile and cell phones, providing new playground for attackers (see Section 3.8 of Chapter 3).

In this appendix, you will get an overview about PT (penetration testing) and VA (vulnerability assessment). Refer to Ref. #1, Books, Further Reading for more details on this topic. At the end of this appendix, you will come across numerous VAPT tools in Table E.1.

Vulnerability Assessment (VA)

Vulnerability assessment (VA)[1] is a process of identifying, quantifying and prioritizing (i.e., ranking) the vulnerabilities found/observed in the system. Vulnerability assessment is conducted for small businesses to large infrastructures. Vulnerability assessment into BCP/DRP (business continuity planning/disaster recovery planning) is an important step to assess the threats from potential hazards to the organization. Since now IT Systems are the backbone for every business, it is conducted in all the fields. For example, systems for which vulnerability assessments are performed include nuclear power plants, information technology systems, energy supply systems, water supply systems, transportation systems and communication systems.

Many things are common between vulnerability assessment and risk assessment. Vulnerability assessments are usually performed as per the following steps:

1. List assets and resources in a system.
2. Assign quantifiable value and importance to these resources based on criticality.
3. Identify the vulnerabilities or potential threats to each asset/resource.

Mitigate or eliminate the most serious (i.e., top ranked) vulnerabilities for the most valuable resources.

> ☛ The primary difference between PT and VA is: “vulnerabilities are identified under VA” whereas “vulnerabilities are exploited during PT.”

Penetration Testing

Penetration testing (PT),[2] also called as "PenTest," is a method to evaluate the security of a computer system or network by simulating an attack from a malicious source. The attacker is known as a Black Hat Hacker or Cracker (see Boxes 2.1 and 2.2 of Chapter 2). PT involves an analysis of the system for potential vulnerabilities that could result from:

1. Known and unknown hardware or software flaws,
2. poor or improper system configuration, or
3. operational weaknesses and/or technical countermeasures.

The analysis is conducted and security issues that are found are presented to the management displaying the impact and mitigation plan and/or a technical solution. The objective of the penetration testing is to determine the feasibility of an attack and the amount of business impact of a successful exploit.

Types of Penetration Tests

Let us understand different types of PTs.**[3]**

Application Security Testing

With the growth of E-Business, it became essential to offer core business functionality through Web-based applications. Internet-enabled applications provide an organization the global reach, providing access to partners (i.e., customers, vendors, contractors, etc.) inside the Intranet. This feature introduces new security vulnerabilities since security can be compromised as the traffic is allowed to pass the firewall. The objective behind application security testing is to evaluate the controls over the application and its process flow. PT of Web applications refers to a set of services used to detect vulnerabilities and risks, including:

1. Known vulnerabilities in COTS (commercial off the shelf) applications.
2. Technical vulnerabilities such as SQL injection, URL manipulation, cross-site scripting, session hijacking, buffer overflow, click jacking, etc. (see Chapters 4 and 5 to understand all these attacks).
3. Business logic errors such as unauthorized log-ins, personal information modification, unauthorized funds transfer, pricelist modification, etc.

Applications can control the use of resources granted to them and not which resources are granted to them. The applications, in turn, determine the use of these resources by users of the application through application security. Web Application Security Consortium (WASC) and Open Web Application Security Project (OWASP – refer to Box 35.8 on OWASP, Ref. #1, Books, Further Reading) provide updates on the latest threats which impair Web-based applications.

Denial-of-Service Testing

A denial-of-service attack (DoS attack) is an attempt to make a computer resource (i.e., information systems) unavailable to its intended users. (See Section 4.9 of Chapter 4 to understand distinct DoS attacks.) DoS testing is an attempt to exploit specific weaknesses on a system by exhausting the target's resources that will cause it to stop responding to legitimate requests. This testing can be performed using automated tools or manually. Different types of DoS attacks are discussed in Chapter 4 under Section 4.9.3; these can be broadly classified into flooding attacks and software exploits. The determination about the extent of DoS testing to be incorporated into a PT depends on the relative importance of ongoing, continuous availability of the information systems and related processing activities.

Table E.1 VAPT tools

Sr. No.	*Name of the Tool*	*Brief Description*	*Remarks*
1	BackTrack	BackTrack is a Linux distribution used for penetration testing.	For more details on this tool and download, visit: http://www.backtrack-linux.org/
2	CERBERUS INTERNET SCANNER (CIS)	CIS Tools are used for scanning a remote host for many known vulnerabilities including XSS, Web Service checks, FTP, SMTP, POP3, NT, NetBIOS and MS SQL checks.	For more details on this tool and download, visit: http://www.securityfocus.com/tools/676
3	Core Impact	Core Impact (Pro) is comprehensive software solution for assessing the security of: • Web applications. • Network systems. • Endpoint systems and email users. • Wireless networks. • Network devices.	For more details on this tool and download, visit: www.coresecurity.com
4	CyberCop	CyberCop Scanner is a commercial network vulnerability auditing tool.	For more details on this tool and download, visit: http://www.tlic.com/security/intrusion.cfm
5	GFI LANguard	GFI LANguard is a renowned network security scanner. It provides a complete network security overview.	For more details on this tool and download, visit: www.gfi.com/lannetscan
6	HackerShield	HackerShield scans websites for vulnerabilities to improve upon defense and security against attackers.	For more details on this tool and download, visit: http://www.hackershield.com/
7	ISS Internet Scanner	Internet Security Systems Internet Scanner is a leading product of security management solutions for the Internet, protecting digital assets and ensuring safe and uninterrupted E-Business with its industry-leading intrusion detection and vulnerability assessment, remote managed security services, and strategic consulting and education offerings.	For more details on this tool and download, visit: www.iss.net
8	MBSA	Microsoft Baseline Security Analyzer (MBSA) is designed to determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance.	For more details on this tool and download, visit: http://technet.microsoft.com/en-us/security/cc184924
9	Metasploit	Metasploit Framework is the open-source penetration testing framework with the world’s largest database of	For more details on this tool and download, visit: http://www.metasploit.com/

		public, tested exploits.	
10	Nessus	Nessus is a powerful, fast and modular security scanner that tests for many thousands of vulnerabilities. ControlScans' system can also be used to create custom Nessus reports.	For more details on this tool and download, visit: www.nessus.org
11	NetRecon	NetRecon scans multiple OS such as UNIX, Linux, Windows 2000 and NetWare. NetRecon tests the entire network for security vulnerabilities and provides recommendations on how to fix them.	For more details on this tool and download, visit: www.symantec.com
12	Nikto	Nikto is an open-source (GPL) web server scanner which performs comprehensive tests against web servers. It also checks for server configurations such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.	For more details on this tool and download, visit: http://www.cirt.net/nikto2
13	QualysGuard	QualysGuard Vulnerability Management (VM) is an on-demand Software-as-a-Service (SaaS) solution. There is no infrastructure to deploy or manage it. It automates the life cycle of network auditing and vulnerability management across the enterprise, including network discovery and mapping, asset prioritization, vulnerability assessment reporting and remediation tracking according to business risk.	For more details on this tool and download, visit: www.qualys.com
14	Rational AppScan	IBM Rational AppScan automates application security analysis and detects exploitable vulnerabilities, protecting against the threat of cyberattack.	For more details on this tool and download, visit: http://www-01.ibm.com/software/awdtools/appscan/
15	Retina	Retina is unified vulnerability and compliance management solution that integrates assessment, mitigation, protection and reporting into a complete offering.	For more details on this tool and download, visit: http://www.eeye.com/Products/Retina.aspx
16	SAINT	Security Administrator's Integrated Network Product Suit available as: • **SAINTscanner:** The SAINT vulnerability scanner identifies threats across the network including devices, operating systems, desktop applications, Web applications, databases and	For more details on this tool and download, visit: www.saintcorporation.com

		more. - **SAINTexploit:** The penetration testing component is integrated with the SAINT vulnerability scanner. SAINTexploit automates the penetration testing process, examines vulnerabilities discovered by the scanner, exposes where the attacker could breach the network and exploits the vulnerability proving its existence without a doubt. - **SAINTmanager:** The remote management console is for organizations that want to centrally manage multiple scanners and help manage the vulnerability life cycle.	
17	SARA	Security Auditor’s Research Assistant (SARA) is a third-generation network security analysis tool that has been actively updated for over 10 years.	For more details on this tool and download, visit: www.www-arc.com
18	HP WebInspect	HP WebInspect performs web application security testing and assessment for complex web applications, built on emerging Web 2.0 technologies.	For more details on this tool and download, visit: https://www.fortify.com/products/web_inspect.html
19	Wireshark	Wireshark (originally named Ethereal) is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development.	For more details on this tool and download, visit: http://www.wireshark.org/
20	X-scan	X-scan scans the perimeter that consists of Internet facing devices, which attackers usually target. It helps you to detect vulnerabilities and manage remediation to prevent attackers from penetrating the network from the outside.	For more details on this tool and download, visit: http://www.sentry-scan.co.uk/xSCAN.html

In summary penetration testing and vulnerability assessment are important aspects in cybersecurity domain. Unless the security flaws are known, they cannot be fixed. However, one has to have in-depth knowledge about computer networks and related areas to guide and implement the solutions to fix the security holes. Chapter 12 explains career guide path into network security domain under Section 12.3.3. Further, Chapter 12 explains related certifications and aspirants may opt for licensed penetration tester (LPT), which is specialized skill set under network security domain.

References

[1] To know more about vulnerability assessment, visit: http://en.wikipedia.org/wiki/Vulnerability_assessment (7 November 2010).

[2] To know more about penetration testing, visit: http://en.wikipedia.org/wiki/Penetration_test (7 November 2010).

[3] To know more about types of penetration tests, visit: http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1083719,00.html (8 November 2010).

Further Reading

Additional Useful Web References

1. To know more about vulnerability Assessment and Network Security, visit: http://www.vulnerabilityscanning.com (7 November 2010).

2. To know more about penetration testing strategies, visit: http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1083715,00.html (8 November 2010).

3. To know how vulnerability assessment, visit: www.sans.org/reading_room/whitepapers (7 November 2010). This paper belongs to SANS Institute on Vulnerability Assessment.

4. To know about vulnerability assessment, visit: http://iac.dtic.mil/iatac/download/vulnerability_assessment.pdf (7 November 2010). This site is about Information Assurance Tools Report on Vulnerability Assessment.

5. To know *Penetration Testing Methodology and Standards*, visit: http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1083724,00.html (8 November 2010).

Book

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Chapter 35 (Section 35.9), Wiley India, New Delhi.