

Name: CHAOYI HUANG

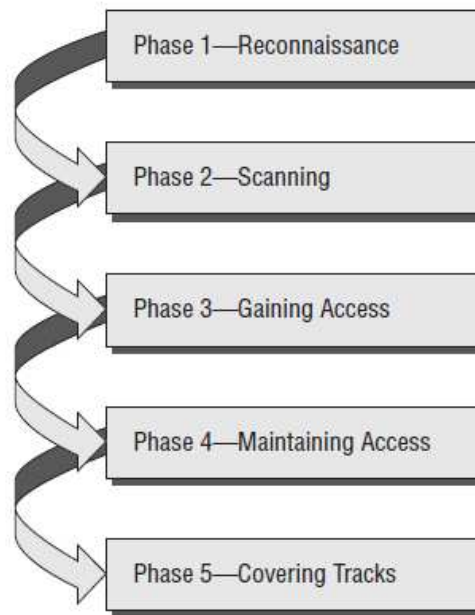
Date: February 13, 2015

Vulnerability Scanning Versus Penetration Test

We suppose that you were an IT administrator in a bank and your boss was asking you about if your company should achieve a vulnerability scanning or a penetration test, how would you answer? You have to know the definitions of Vulnerability Scanning and Penetration Test before you answer your boss's question. Vulnerability Scanning is a process of remotely examining hosts on a network for known, detectable vulnerabilities and misconfigurations. (University of Michigan, 2014) A Penetration Test is the practice of evaluating a chosen entity¹ to ensure the current security controls are performing as expected, and the vulnerability state is known. (Harvard University, n.d.) Normally, people always believe that Vulnerability Scanning and Penetration Test, these two different evaluation activities are alike. Since they have a similar objective that is using technology ways to evaluate the security of IT systems, and they use some similar tools, as well as make some influence with their targets. Even though Vulnerability Scanning and Penetration Testing are alike, but they still have some differences that are Scope, Method, as well as Investment and Return.

¹ For instance, Application, Host, System, Network, Procedure, and Person.

First, Scopes may be used to distinguish Penetration Tests from Vulnerability Test through Depth, Width, and Social Engineering Test. The type of evaluation activities may be identified by Depth. The illustration below shows all typical phases of systems hacking.



People usually divide a typical hacking into five phases, which are Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Covering Tracks. The typical hacking process follows the sequence. (Graves, 2010) Depth means how deep the evaluation activity follows. For example, Vulnerability Scanning's Depth is two that stands for Vulnerability Scanning only simulates the first two phases, which are Reconnaissance and Scanning. However, Penetration Test simulates all phases, so its Depth is five. In addition, Width represents how many kinds of vulnerabilities people are able to find through the evaluation activity. People usually divide vulnerabilities into two parts, which are Known Vulnerabilities and Unknown Vulnerabilities.

Known Vulnerabilities mean some vulnerabilities which have already been found and









































published. In contrast, Unknown Vulnerabilities stand for the other vulnerabilities, which have been found but have not been published, or even have not been found yet. Vulnerability Scanning is only able to find out Known Vulnerabilities, but Penetration Test is able to find out all vulnerabilities. Meanwhile, whether executing Social Engineering Test is a measure to distinguish if the evaluation activity is a penetration test or not. In a social engineering attack, an attacker uses human interaction to obtain or compromise information about an organization or its computer systems. (US-CERT, 2013) Normally, Social Engineering Test only exists during Penetration Test, since it requires the participants with more specific knowledge of Social Engineering. Therefore, Penetration Test's scope is wider than Vulnerability Scanning's.

Second, Penetration Test uses a special achievement method, which is different from Vulnerability Scanning's achievement method with tools, environments, participants, and detection policies. In order to expand the scope of evaluation, Penetration Test usually uses more types of tools. For example, even though you face the same system, you only will use some built-in program from Operating Systems and some Vulnerability Scanners during your vulnerability scanning tasks, yet you probably will use not only those programs, but also Penetration Test frameworks, Denial of Service (DoS) tools, and even Fuzzers² during your penetration test tasks. Moreover, Vulnerability Scanning and Penetration Test usually are run in different kinds of environments, since they make damage with varying degrees to IT systems.

² A fuzzer is a type of exploratory testing tool used for finding weaknesses in a program by scanning its attack surface. (Software Engineering Department of Rochester Institute of Technology, 2013)

Penetration Test contains some dangerous detection methods, such as Denial of Service (DoS) detections, and Fuzzing detections. Those detection methods are similar to real attacks. However, they make the test environment very unstable, so almost no one uses real environments or business environments to achieve Penetration Tests. The participators of Vulnerability Scanning and Penetration Test are different. The participators of Vulnerability Scanning are required to have some basic knowledge about how to use some common commands and Vulnerability Scanners. Nevertheless, the executors of Penetration Test usually are Information Security Professionals, who have more credentials, such as knowledge of Penetration Tests' project management, experience, and certificates³. Meanwhile, even though both of Vulnerability Scanning and Penetration Test have to use Vulnerability Scanners as their tools during the detection phase, yet their Scanning Policies are not the same. Scanning Policies are groups of settings that are used to let scanners execute scanning tasks with indicated methods. The following illustration is a snapshot of editing Scanning Policies in OpenVAS, which is a famous open-source Scanner around the world.

³ For instance, Certified Ethical Hacker (CEH), Licensed Penetration Tester (LPT), Certified Penetration Testing Engineer (CPTe), Certified Penetration Testing Consultant (CPTC), GIAC Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), and GIAC Exploit Researcher and Advanced Penetration Tester (GXPN).

Family  	NVT's selected	Trend 	Select all NVT's	Action
AIX Local Security Checks	0 of 1	 		
Brute force attacks	0 of 11	 		
Buffer overflow	0 of 333	 		
CISCO	0 of 4	 		
CentOS Local Security Checks	0 of 670	 		
Compliance	0 of 3	 		
Credentials	0 of 2	 		
Databases	0 of 52	 		
Debian Local Security Checks	0 of 2205	 		
Default Accounts	0 of 20	 		
Denial of Service	0 of 623	 		
FTP	0 of 143	 		
Fedora Local Security Checks	0 of 3453	 		
Finger abuses	0 of 2	 		
Firewalls	0 of 20	 		

As we have already mentioned before, Vulnerability Scanning usually is executed with real environments or business environments, so the Scanning Policies of Vulnerability Scanning are supposed to be harmless. In contrast, Penetration Test usually uses Full Scanning Policy. Consequently, everything may vary as long as you plan to achieve a Penetration Test.

Third, based on the field of Investment and Return, we still can distinguish the differences between those two different activities through project period, project cost, and the detail level of results. The project period of Penetration Test is longer than the project period of Vulnerability Scanning, due to simulation phases and analysis period. According to Depth, which we have already mentioned before, Penetration Test has to execute three more phases, which are Gaining Access, Maintaining Access, and Covering Tracks, so its project period is supposed to be longer. Moreover, the automatic tools are able to deal with almost all analysis tasks during

Vulnerability Scanning tasks. Nevertheless, Penetration Test has participants do more analysis tasks. For instance, when a vulnerability scanner locates a weak password for an FTP server, Vulnerability Scanning participants will mark it as a vulnerability, yet Penetration Test participants will try to download all data from the FTP server through the weak password and search more significant information from the data. Additionally, Penetration Test charges more money due to human recourse and tools, because it requires more participants to analyze materials and more tools to execute some tasks from the last three phases, which are Gaining Access, Maintaining Access, and Covering Tracks. The result of Penetration Test contains information that is more detailed. The report of vulnerability scanners usually includes some static information, that are assets' information and some vulnerabilities' information which can be found from some famous vulnerabilities databases, such as CVE and Bugtraq. In contrast, Penetration Test's report involves dynamic information, which are able to let readers understand the whole occasion with the weaknesses. Thus, even though Penetration Test has you pay more resource as an investment, you will get your return later.

Finally, Scope and Method are the reasons why the procedures of Vulnerability Scanning and Penetration Test look so different, yet Investment and Return influence the input and output of those two different evaluation activities. In my opinion, if I were the IT administrator of the bank, I would convince my boss to execute those two evaluation activities at the same time, since either one cannot cover all demands.

References

Graves, K. (2010). CEH Certified Ethical Hacker STUDY GUIDE. Indianapolis:
Wiley Publishing, Inc.

Harvard University. (n.d.). Penetration Tests. Retrieved from Harvard University:
<http://isites.harvard.edu/icb/icb.do?keyword=k87162&pageid=icb.page504566>

Software Engineering Department of Rochester Institute of Technology. (2013,
October 7). Web Application Fuzz Testing Tool. Retrieved from Software
Engineering Department of Rochester Institute of Technology:
<http://yogi.se.rit.edu/~swen-331/projects/fuzzer/>

University of Michigan. (2014, October 8). Vulnerability Scanning Services.
Retrieved from Information and Technology Services of University of
Michigan: <http://safecomputing.umich.edu/services/vulnerability-scanning.html>

US-CERT. (2013, February 6). Avoiding Social Engineering and Phishing Attacks.
Retrieved from US-CERT: <https://www.us-cert.gov/ncas/tips/ST04-014>