



The need for Security Testing

An Introduction to the OSSTMM 3.0

Charles W. Fullerton
OPST, CISSP, CSS1, CCNP, CCDA, CNA, A+
Founder, CEO
Charles W. Fullerton Institute of Analysis
www.cia-sec.com

The need for Security Testing

There are a number of myths that companies use to discredit the need for Security testing. This whitepaper will address and discount some of those myths. This paper will describe the different types of Security testing available to companies and finally introduce the OSSTMM version 3.0.

Myth # 1

“We don’t need a Security Policy. We’re only a small business.” This is one of the most common myths in Information Security. The Fact is that EVERYONE needs a Security Policy. There are entire books written on how to create a Security Policy. That is beyond the scope of this whitepaper. However, Security Testing is a very important part of that Security Policy.

Myth # 2

“There’s no ROI in Security Testing.” This is another common misconception. Return on Investment can happen in 2 ways: Passive and Active. Two of the well-known passive ways to provide limited ROI include protection from Lawsuit liability and protection from data theft. However, a third passive ROI is in the form of assistance in the navigation of political issues. By performing a quality 3rd party Security Test, you can verify the need for resources, justify a budget request, or even assist management in understanding the methodologies and technologies used in Security.

On the Active side of ROI, Security Testing can point out areas for improvement that can improve efficiency and reduce downtime, allowing for the maximum throughput of information allowed by the technology and processes utilized.

Myth # 3

“The only way to totally secure the network is to unplug it!” This comment is usually spoken as sarcastic as it sounds when you read it. While this may be true in fact, it is definitely not realistic. The best way to secure your organization is to find it’s “Perfect Security.” Perfect Security is computed by performing a Posture Assessment and comparing it to your organization’s Security Policy, and it’s Business, Legal, and Industry justifications.

Myth #4

“We know you can get in if you try to trick our people. What we want is a real test of what a hacker or a script-kiddie would do.” Fact is, this is exactly what a hacker could do to attempt to gain access or information from an organization. Social Engineering is an important part of a Security Test. A social engineering test can point

out areas where security awareness training may be needed. A colleague of mine once said, *“Until companies realize that their people can be their biggest asset or biggest liability in securing their network, attackers will always have the Social Engineering Trump Card.”* – Chuck Herrin, Penetration Tester – Jefferson Wells International

Myth #5

“The Internet isn’t safe! We must immediately purchase this new hyped up product to save our business!” Ok, I’ll admit this is a bit melodramatic. However, one of the biggest problems in the Security industry today is the use of emotion to sell their wares. In my opinion, the use of fear, uncertainty and doubt, is method of sales used by people who don’t understand security and are more interested in making money than helping to secure their customers. Security will not be an accepted part of Information Technology until it becomes a business decision and not an emotional one.

Types of Security Testing

According to the Open Source Security Testing Methodology Manual (OSSTMM www.isecom.org), there are seven main types of security testing. They are:

- Vulnerability Scanning
- Security Scanning
- Penetration Testing
- Risk Assessment
- Security Auditing
- Ethical Hacking
- Posture Assessment & Security Testing

Vulnerability Scanning is using automated software to scan one or more systems against known vulnerability signatures. Examples of this software are Nessus, Sara, and ISS.

Security Scanning is a Vulnerability Scan plus Manual verification. The Security Analyst will then identify network weaknesses and perform a customized professional analysis.

Penetration Testing takes a snapshot of the security on one machine, the “trophy”. The Tester will attempt to gain access to the trophy and prove his access, usually, by saving a file on the machine. It is a controlled and coordinated test with the client to ensure that no laws are broken during the test.

Risk Assessment involves a security analysis of interviews compiled with research of business, legal, and industry justifications.

Security Auditing involves hands on internal inspection of Operating Systems and Applications, often via line-by-line inspection of the code.

Ethical Hacking is basically a number of Penetration Tests on a number of systems on a network segment.

Posture Assessment and Security Testing combine Security Scanning, Ethical Hacking and Risk Assessments to show an overall Security Posture of the organization. It needs a methodology to follow. An excellent example of this would be the OSSTMM.

OSSTMM 3.0

The Open Source Security Testing Methodology Manual was the brainchild of Pete Herzog and the Institute for Security and Open Methodologies (ISECOM). The OSSTMM covers all aspects of a security test, from how to market, to client negotiations and contracting, to how to report your findings. The goal of the OSSTMM is to create a level playing field for all testers using the methodology, while providing a guide for performing a thorough test for clients. It doesn't matter if your company is a large conglomerate or a small start-up consultancy. If you follow the OSSTMM, the report should be compatible with other OSSTMM reports. ISECOM can also verify the accuracy of reports for auditing purposes.

One of the most important parts of the OSSTMM is its "Rules of Engagement". These rules are what keep all tests equal. The rules are grouped into 9 sections.

- Sales and Marketing
- Assessment/Estimate Delivery
- Contract and Negotiations
- Scope
- Providing the Test Plan
- Providing the Rules of Engagement to the Client
- Testing
- Reporting
- Report Delivery

Rule number 1 of the OSSTMM is that the use of fear, uncertainty and doubt may not be used in the sales and marketing for the purpose of selling tests. This one rule makes the decision of an OSSTMM test a business decision and not an emotional one. Another rule dictates that the test plan must include the time the test will take. This must include both calendar time and man-hours. However, the question can be raised; "How do we keep everyone computing the time it takes the same way?"

The OSSTMM also provides a "Rule of Thumb" for scheduling tests. If this rule is strictly followed, a tester can be reasonably accurate in computing how long an OSSTMM Security Test will take. While this rule can be quite complicated to initially understand, with a little practice, a tester can constantly and efficiently schedule OSSTMM tests.

Since the OSSTMM is an international document, it considers a number of laws from numerous countries. From the USA the OSSTMM is compliant with many recent security and privacy regulations including; GLBA, HIPAA, SOX, Clinger-Cohen, COPPA and even California's SB1386. It also considers international best practices and the human right to privacy. Some of these include; OCTAVE, ISO 17799, CHECK, CVE, and many NIST and GAO regulations.

The 6 testing sections of the OSSTMM include:

- Information Security
- Process Security
- Internet Technology Security
- Communications Security
- Wireless Security
- Physical Security

There are 6 testing sections of the OSSTMM. The Information Security section is where an initial Risk Assessment is performed. All pertinent documentation is compiled and analyzed to compute “Perfect Security”. This level of Perfect Security then becomes the benchmark for the rest of the test. Throughout the other five sections, all testing results are reviewed against this benchmark and the final report includes a gap analysis providing solutions to all outstanding vulnerabilities.

The section on Process Security addresses Social Engineering. Through Request, Guided Suggestion, and Trusted Persons testing the tester can gauge the security awareness of your personnel.

The Internet Technology Security Testing section contains what most people view as a security test. Various scans and exploit research will point out any software and configuration vulnerabilities along with comparing the business justifications with what is actually being deployed.

Communications Security Testing involves testing Fax, Voicemail and Voice systems. These systems have been known to be exploited causing their victims to run up costly bills. Most of these exploits will go unknown without being tested.

Wireless Technology has been gaining in use rapidly over the last few years. The Wireless Security Testing section was created to address the gaping exploits that can be found due to misconfigurations by engineers with limited knowledge of the recent technology.

Finally there is the Physical Security Testing section. This section checks areas such as physical access control and the environmental and political situations surrounding the site. An example of this may be, if your data center has been placed in the flight path of an airport runway. What is the risk of having an airliner engine jump into your server rack? If you have a redundant data center, then the risk may be assumable. Another risk is having your call center located in a flood plain.

In each section of the OSSTMM, every item noted will be assigned a value. These values will then be computed to determine the section’s Risk Assessment Value (RAV). RAV’s are used to measure security in a consistent repeatable manner regardless of tester. RAV’s can provide one standard measure across many different industries but more importantly; they can be used to show management statistically how much risk must be attended to.

The OSSTMM doesn’t forget the IT department either. At least 3 days after the final report is delivered, the OSSTMM calls for a workshop with the engineers to address each reported item found. This ensures that the engineers understand the problems and how to fix them properly.

Conclusion

Testing is a very important part of implementing security within an organization. The OSSTMM provides an auditable, quantifiable, thorough, and accredited test that is compliant with many nations' and local laws as well as the human right to privacy. It demonstrates "due diligence" and compliance with industry regulations. On top of all this, testing can point out areas of needed improvement that can optimize throughput of information, reducing downtime and insuring optimal use of funds for the organization.

About the Author

Chuck Fullerton has worked in the IT and Security fields for over 15 years. After serving in South Korea with the U.S. Army, Chuck has worked with many different industries such as, manufacturing, education, finance, healthcare, law enforcement and telecommunications. His philosophy on security is that "everyone has a responsibility to maintain a level of security for themselves on the Internet. People must learn how to secure the equipment under their control." Chuck started the Charles W. Fullerton Institute of Analysis to do just that.

CIA's motto is "We Care about Your Security." CIA is committed to providing ethical, objective OSSTMM testing to its customers. CIA also provides Security Awareness training and will open its Honeynet Project to clients starting towards the end of 2004. Chuck can be reached via email at chuck@cia-sec.com.