NebraskaCERT May CSF

A small overview of the OSSTMM: Open Source Security Testing Methodology Manual

by

Aaron Grothe
NEbraskaCERT

Disclaimer

- Any views/opinions or anything else that comes out of my mouth is my opinion and probably no one else's. They do not reflect the views of my employer

Overview

- What is the OSSTMM?
- Points
- Highlights
- A couple of sections and a Module
- How to use OSSTMM
- My Experiences with OSSTMM
- Some issues with OSSTMM
- Resources
- Summary.

What is the OSSTMM?

- The OSSTMM is a framework for doing a security audit
- It is NOT complete
- It has a pretty lively community behind it
- References to the document refer to 2.1 version
- They are used under Fair use as part of reviewing the OSSTMM.

Points

- *When* to test is as important as *what* and *why* to test
- *Do* sweat the small stuff because it is all small stuff
- *Do* make more with less.

Points

- Don't underestimate the importance of the security policy *in any form*
- What they get is all about *how* you give it.

Highlights

- Vuln scanning time/cost graph p. 14
- Security map p. 22.

Modules

- Modules exist for the following sections
  - Information Security
  - Process Security
  - Internet Technology Security
  - Communications Security
  - Wireless Security
  - Physical Security
- Security map Module list p. 23.

Working through a Module

- Pop over to Voicemail section p. 67
- Pop over to IDS section p. 59
  - Testing IDS test template p. 99
- Take a look at Wireless Module p.70.

How to use OSSTMM

- OSSTMM can be used to augment internal security policy
- While some sections are incomplete they are in a lot of ways better than the alternatives
- Tend to be technology driven instead of being driven by policy.

How to use OSSTMM

- Can get training and Certification in the OS-STMM methodology
- Certifications exist
  - OSSTMM Professional Security Tester (OPST)
  - OSSTMM Professional Security Analyst (OPSA).

How to use OSSTMM

- OSSTMM is more than just a book
  - Active mail lists
  - Memberships available to get beta versions of OSSTM. Gold and Silver level
  - Silver is around $50.00 a year.

My Experiences with OSSTMM

- OML License p.127 has raised issues with corporate types. Being under a more popular license like the GFDL, or a creative commons license might be useful
- Rules of Engagement p.18 puts additional restrictions on using OSSTMM. The planks such as do not use FUD are hard to argue with, but are still additional restrictions
- Commercial license is also available.

Some Issues with OSSTMM

- We have a section on RFID and not a PKI section?
- Where be the Cryptography section?
- 3+ years old and only 128 pages.

Resources

- Ideahamster http://www.ideahamster.org
  - Homepage for ISECOM and OSSTMM
- OUSPG Vulnerability Testing Terminology Glossary
  - http://www.ee.oulu.fi/research/ouspg/glossary

Summary

- Version 3.0 is due anytime now
- Being available in a variety of languages offer it the opportunity to become a popular standard
- Mail lists offer some lively discussion
- Can be used to supplement other standards such as OCTAVE.

Summary

- ISECOM is developing other things such as the SPSMM Secure Programming Standards Methodology Manual, JACK of all trades security training supplement (being revised).

Q & A

- Questions???