OSSTMM 2.2.

Open-Source Security Testing Methodology Manual

Created by Pete Herzog

CURRENT VERSION:	OSSTMM 2.2
NOTES:	With this version the OSSTMM includes more of the 3.0 methodology.
FIXES:	This version includes updatedrules of engagement and rules for OSSTMM certified audits. Additional fixes include RAVs and Error Types.
DATE OF CURRENT VERSION:	Tuesday, December 13, 2006
DATE OF ORIGINAL VERSION:	Monday, December 18, 2000

Restrictions

This research document is free to read, apply and distribute under the Creative Commons 2.5 Attribution-NonCommercial-NoDerivs license. This document may not be altered, sold, or distributed commercially either by itself or as part of a collection. Application of this methodology for personal, private, or commercial (for profit) services use is free and addressed in the Open Methodology License at the end of this manual or at www.isecom.org/oml. The application of this methodology in whole or part into commercial (for profit) tools, software, and knowledge-ware is subject to licensing restrictions through ISECOM. Any and all licensing or commercialization requests can go through ISECOM: info@isecom.org.

Summary

ISECOM, the Institute for Security and Open Methodologies, registered in New York of the United States of America and in Catalunya, Spain as a Non-Profit Organization, is releasing the next update of the Open Source Security Testing Methodology Manual. This manual has been developed for free use and free dissemination under the auspices of the international, open-source community. This manual is designed to exceed international legislation and regulations regarding security as well as those from many participating organizations to assure compliancy. Financing for this manual and all ISECOM projects has been provided independent of commercial and governmental influence through ISECOM partnerships, subscriptions, certifications, licensing, and case-study-based research.

To be most clear, any security test which does not follow a scientific methodology has little to no measurable value; therefore no clear direction can be taken through analysis and no clear result can be formed. The specific guidelines in this manual provide the basis for audits and tools towards a formal scientific method to operational security auditing, the metrics to quantify security within any channel, the rules of engagement for auditors to assure unbiased and logical analysis, and a standard for providing certified security audit reports.

Furthermore, your evaluation of this document, suggestions for improvements, and results of its application for further study are required for further development. Contact us at osstmm@isecom.org or visit us at www.isecom.org to offer research support, review, and editing assistance.

Contributors

Those who have contributed to this manual in consistent, valuable ways have been listed here although many more people should receive our thanks. Each person here receives recognition for the type of contribution although not as to what was contributed. The use of contribution obscurity in this document is for the prevention of biases and to promote fresh ideas. If you are interested in contributing, please see the ISECOM website for more information.

CREATED BY:	Pete Herzog	pete<a>isecom.org
DEVELOPERS:	Marta Barceló	marta<atisecom.org
	Robert E. Lee	robert<a>isecom.org
	Nick Mayencourt	nick<a>isecom.org
	Richard Feist	richard<a>isecom.org
	Raoul Chiesa	raoul<a>isecom.org
	Kim Truett	kim<a>isecom.org
	Colby Clark	colby.Clark<a>cox.net
	Nigel Hedges	Nigel.Hedges<at>isecom.org
	Tom O'Connor	tom91<a>elivefree.net
	Andrea Barisani	lcars<a>infis.univ.trieste.it
	Gary Axten	gary.axten<a>lineone.net
	Marco Ivaldi	raptor<a>mediaservice.net
	Fabrizio Sensibile	fabrizio<a>mediaservice.net
	Jack Louis	jack<a>rapturesecurity.com
	Ty Miller	tmiller<a>purehacking.com
	Dru Lavigne	dru<at>isecom.org
	Felix Schallock	felix.schallock<a>e-security-net.de
	Anton Chuvakin	anton<a>chuvakin.org
	Efrain Torres	et<a>cyberspace.org
	Rogelio M. Azorín	rma<at>isecb.com
	Rob J. Meijer	rmeijer<a>xs4all.nl
	Clemens Wittinger	cwr<at>atsec.com
	Sean Cocat	scocat<at>remingtonltd.com
	Jaume Abella	jaumea<a>salleURL.edu
	John Thomas	sregney<a>gedas.es
	Regney	klee<a>de.ibm.com
	Peter Klee	martin.pivetta<a>itatwork.com
	Martin Pivetta	dfernandez<a>isecauditors.com
	Daniel Fdez. Bleda	cdupuis<a>cccure.org
	Clément Dupuis	jwr<a>rittinghouse.homeip.net
	John Rittinghouse	buytaert<a>stone-it be
	Kris Buytaert	Chris.Griffin<a>anthem.com
	Chris Griffin	

Foreword

In previous versions of the OSSTMM a primary focus was on *what* we do as security testers. Due to the success of those releases and the OSSTMM's growing approval amongst the IT security community, I have had the continued pleasure to expand upon the OSSTMM. To help deliver this methodology, I created the OSSTMM Professional Security Tester (OPST) and Analyst (OPSA) certifications. I've had the pleasure to teach these now on a number of occasions, and it has been during some of these classes that I have observed a growing requirement to define *why* we do security testing.

When dealing with security and risk management, many think of these in terms of odds and predictability. They ask: What are the odds that an incident, threat or attack will occur? Just how predictable is it that this event will occur? And while it is true that some defenses are proactive enough to address unknown and unpredictable attacks, most organizations depend on defenses that are strengthened by a database of known attacks. So, a penetration tester knows that to counteract these he/she must also have a database of known up-to-date attacks. This aids in the swiftness and effectiveness of each attempt. Time and time again, a certain set of "ethical hacks" will prove successful, so the tester will savor these jewels from his/her database of attacks, and log the success ratios. Armed with this information the penetration tester will attempt to exploit a customer's network until one of the attacks succeeds. This technique is well and good, however in practice the client's organization becomes a casino and the penetration testers are playing against the client's set odds-much like the gambler is at the mercy of the odds set by the house.

Methodical security testing is different from penetration testing. It relies on a combination of creativeness, expansive knowledge bases of best practices as well as known threats, and the breadth of the target organization's security presence (or points of risk) to "cheat" at the casino, thus making our own odds. We do this by exploiting predictability and best practices to the most thorough extent possible. In other words, we test all extremes of everything considered predictable and fully utilize best practices to test against the worst-case scenarios that may not be as predictable. For organizations truly committed to reduce as much risk as possible, it almost goes without saying that it is our duty as security testers to explore the breadth and depth of risk and to properly identify this throughout the target of the test.

The types of questions we must continually ask ourselves in the testing process are: Which assets can I access at what time to force the maximum security risk? Under what circumstances do I find the most weaknesses? When am I most likely to put *confidentiality*, *integrity* and *availability* to the test? By remaining methodical and persistent, the accumulative effect of these tests will paint an accurate picture for us of the risks, weaknesses, information leaks, and vulnerabilities. This will assist us greatly with any business justifications for safeguards, as well as satisfying any regulative/legislative requirements through due care and diligence.

The following points will aid you well as you set out to create and deliver your high standard security tests:

- ***When* to test is as important as *what* and *why* to test.**

Waiting to make the test, waiting to report the problems, and waiting to address problems are all mistakes. As you left your house to go on vacation, did you wait until you returned to test if you actually locked the doors? Of course not. You locked the door and rattled the knob to make sure it was locked. Waiting until you return to test would also require going through the house to see what's missing, and you don't need reminding that an audit takes much longer than a security test.

- ***Do* sweat the small stuff, because it's all small stuff.**

Testing is in the details and often it is the smallest details that lead to the biggest security breaches. In addition, it is the accumulation of the small stuff, which individually may not represent much risk but when aggregated, may also lead to a security breach.

- ***Do* make more with less.**

As budgets for security defense remain small, the security tester needs to operate with efficiency and creativity to do more in less time. If inefficient security testing becomes too costly it is tempting for an organization to see security testing as an extraneous cost. This is unfortunate because the risks associated from not conducting security testing still remains unknown. Therefore, as we balance thoroughness with efficiency in our security tests, the results will time and time again speak for themselves - many more organizations will view security testing as a cost justified weapon in their defensive posture.

- **Don't underestimate the importance of the Security Policy *in any form*.**

This policy is the company's official declaration of what they want to accomplish. Very few people ever arrive somewhere without first having intended to get there. A security policy is all about that intention, and the organization's goal of security within it. The security policy for an organization is often very complex with multiple persons tasked to develop and maintain it. Mistakes due to policy in one section will often form a negative flow-on effect that will impact other sections. It only takes a few termites in a wall to lead to infestation of the whole house. For example, if a policy is not in place to specify controls that check people who leave with boxes or equipment, then information leakage may occur. Security Policy specifies many more controls that have a direct effect on standards and procedures, such as what egression rules exist on the screening router, or what e-mails one may forward out from inside the company.

- **What they get is all about *how* you give it.**

Despite all attempts at thoroughness and efficiency, one of the largest factors about determining the success of a security posture is still based on economics. This is all handled far away from the tester's toolbox, and requires a certain level of project management skill, perceptiveness about your client, and good communication skills. Has enough time for the test been budgeted? Will there be enough in the budget for fixing discovered vulnerabilities? What types of risk will senior management accept or feel is unworthy of budgeting? The end result of the security test will be some form of deliverable to your client or client's management – and all these economic factors should have been worked out before hand. After all, what's the difference between a good and a bad security test if the report is ignored?

Table of Contents

Introduction

This manual is a combination of ambition, study, and years of experience. The individual tests themselves are not particularly revolutionary, but the methodology as a whole does represent the benchmark for the security testing profession. And through the thoroughness of its application you will find a revolutionary approach to testing security.

The objective of this manual is to create one accepted method for performing a thorough security test. Details such as the credentials of the security tester, the size of the security firm, financing, or vendor backing will impact the scale and complexity of our test – but any network or security expert who meets the outline requirements in this manual will have completed a successful security profile. You will find no recommendation to follow the methodology like a flowchart. It is a series of steps that must be visited and revisited (often) during the making of a thorough test. The methodology chart provided is the optimal way of addressing this with pairs of testers however any number of testers are able to follow the methodology in tandem. What is most important in this methodology is that the various tests are assessed and performed where applicable until the expected results are met within a given time frame. Only then will the tester have addressed the test according to the OSSTMM model. Only then will the report be - at the very least - called thorough.

Some security testers believe that a security test is simply a “point in time” view of a defensive posture and present the output from their tests as a “security snapshot”. They call it a snapshot because at that time the known vulnerabilities, the known weaknesses, and the known configurations have not changed. But is this snapshot enough? The methodology proposed in this manual will provide more than a snapshot. Risk Assessment Values (RAVs) will enhance these snapshots with the dimensions of frequency and a timing context to the security tests. The snapshot then becomes a profile, encompassing a range of variables over a period of time before degrading below an acceptable risk level. In the 2.5 revision of the OSSTMM we have evolved the definition and application of RAVs to more accurately quantify this risk level. The RAVs provide specific tests with specific time periods that become cyclic in nature and minimize the amount of risk one takes in any defensive posture.

Some may ask: “Is it worth having a standard methodology for testing security?” Well, the quality of output and results of a security test is hard to gauge without one. Many variables affect the outcome of a test, including the personal style and bias of a tester. Precisely because of all these variables it is important to define the right way to test based on best practices and a worldwide consensus. If you can reduce the amount of bias in testing, you will reduce many false assumptions and you will avoid mediocre results. You’ll have the correct balanced judgment of risk, value, and the business justification of the target being tested. By limiting and guiding our biases, it makes good security testers great and provides novices with the proper methodology to conduct the right tests in the right areas.

The end result is that as security testers we participate and form a larger plan. We’re using and contributing to an open-source and standardized methodology that everyone can access. Everyone can open, dissect, add to, suggest and contribute to the OSSTMM, where all constructive criticism will continue to develop and evolve the methodology. It just might be the most valuable contribution anyone can make to professional security testing.

We welcome your feedback.

Pete Herzog, Managing Director, ISECOM

Document Scope

The scope of this document is all components of a complete and thorough security audit, the calculated metrics from the tests, concepts for security test project planning, and the rules of engagement which cover the ethical and proper manner to market, perform, and deliver this test properly and legally. This manual makes no assumptions based on the target size or location. You can apply it to anything which needs to be tested for operational security.

Purpose

The primary purpose of this manual is to provide a scientific methodology for the accurate characterization of security through examination and correlation in a consistent and reliable way. This manual is adaptable to most IS audits, penetration tests, ethical hacking, security assessments, vulnerability assessments, red-teaming, blue-teaming, posture assessments, war games, and security audits.

The secondary purpose is to provide guidelines which when followed will allow the auditor to perform a certified OSSTMM audit. These guidelines exist to assure the following:

1. The test has been conducted thoroughly.
2. The test includes all necessary channels.
3. The posture for the test includes compliance to the highest of civil rights.
4. The results are measurable in a quantifiable means.
5. The results received are consistent and repeatable.
6. The results contain only facts as derived from the tests themselves.

The ultimate goal is to set a standard in a security testing methodology which when used results in meeting factual, practical, and operational security requirements. The indirect result is creating a discipline that can act as a central point in all security tests regardless of the size of the organization, technology, or protection.

Accreditation

To make an OSSTMM certified test for which one can receive accreditation for the operational security of the target, an OSSTMM Audit Report is required to be signed by the tester(s) or analyst(s) and meet the reporting requirements in this manual. This report along with an anonymized version of the security audit report submitted to ISECOM for review will provide for official OSSTMM certification. Therefore a certifiable test and an accredited report does not need to show that this entire manual or any specific subsections were followed. It need only show both what was and was not tested to be applicable for certification.

A certified OSSTMM Audit provides the following benefits:

- Serves as proof of a factual test.
- Makes auditors responsible for the test.
- Makes a clear statement to the client.
- Provides a more convenient overview than an executive summary.
- Provides a valid checklist for the tester.
- Provides clearly calculated and understandable metrics.

Certification

This manual is open. No specific certification is required to use this manual to make an OSSTMM audit. Certification is provided as a means of independent validation and not as a requirement for applying this manual.

Anyone using this methodology for security testing and analysis is said to be performing an OSSTMM audit and is referred to as an OSSTMM Auditor requiring that the act of testing and analysis based on the methodology within this manual.

Professional Certifications

OPST / OPSA / OPSE / OWSE

Individual certification is available through ISECOM for the applied skills recognized for professional security testing and analysis ability and meeting the methodical process with high ethical standards as outlined in the OSSTMM Rules of Engagement. The OPST (OSSTMM Professional Security Tester), the OPSA (OSSTMM Professional Security Analyst), the OSSTMM Professional Security Expert (OPSE), and OSSTMM Wireless Security Expert are the official certifications for OSSTMM Auditors providing the knowledge as skills required to properly apply the OSSTMM or any security test in a scientific manner. More information is available on the ISECOM website.

Certifications of Compliance

Organizations

OSSTMM certification is available for organizations or parts of organizations which maintain a quarterly RAV level of a minimum of 95% and validate with an annual, OSSTMM audit from a third-party auditor. Validation of security tests or quarterly metrics are subject to the ISECOM verification requirements to assure consistency and integrity.

Products and Services

OSSTMM evaluation seals are available for solutions such as products, services, and business processes. This seal defines the operational state of security, privacy, and legislative governance. This serves primarily as clear overview of functions, security limitations, and the delta, also known as the “catalytic effects” incited on the scope. The products, services, and processes so evaluated will then carry this visible certification seal and its RAV score. This will allow a purchaser to see precisely the amount and type of change in security that the evaluated solutions present. It removes the guess work from procurement and allows for one to find and compare alternative solutions.

Intended Audience

This manual is written as a security research document. It is designed for the most optimum and practical method of factual security verification and metrics on a professional level.

End Result

The ultimate goal is to set a standard in testing methodology which when used in security testing results in meeting practical and operational security requirements for testing the security presence. The indirect result is creating a discipline that can act as a central point in all security tests regardless of the size of the organization, technology, or defences.

Analysis

The scope of this document does not include direct analysis however analysis of some form is implied by the use of "Expected Results" within the methodology. Some analysis must be done to assure at least these expected results are met.

Terms and Definitions

Security Test Type

"Security Testing" is an umbrella term to encompass all forms and styles of security tests from the intrusion to the hands-on audit. The application of the methodology from this manual will not deter from the chosen type of testing.

However, as a standard, this methodology is not to be followed "off-the-shelf". Practical implementation of this methodology requires defining individual testing practices to meet the requirements defined here. This means that even when following this methodology, your application of it, your technique, will reflect the type of test you have chosen to do. Test types may be but aren't limited to one of six common types.

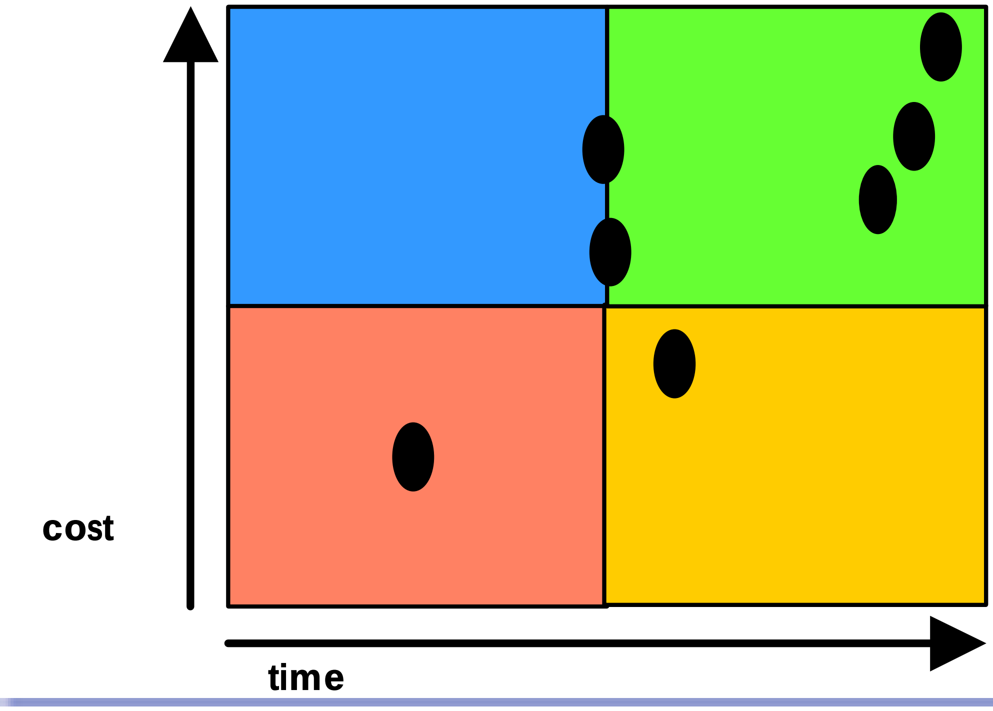
1	**Blind**	The auditor engages the target with no prior knowledge of its defenses, assets, or channels. The target is prepared for the audit knowing in advance all the details of the audit. A blind audit primarily tests the skills of the auditor. The breadth and depth of a blind audit can only be as vast as the auditor's applicable knowledge and efficiency allows.
2	**Double Blind**	This is also known as a black box audit. The auditor engages the target with no prior knowledge of its defenses, assets, or channels. The target is not notified in advance of the scope of the audit, the channels tested, or the test vectors. A double blind audit tests the skills of the auditor and the preparedness of the target to unknown variables of agitation. The breadth and depth of a blind audit can only be as vast as the auditor's applicable knowledge and efficiency allows.
3	**Gray Box**	The auditor engages the target with limited knowledge of its defenses and assets and full knowledge of channels. The target is prepared for the audit knowing in advance all the details of the audit. A gray box audit tests the skills of the auditor and the preparedness of the target to unknown variables of agitation. The nature of the test is efficiency. The breadth and depth depends upon the quality of the information provided to the auditor before the test as well as the auditor's applicable knowledge.
4	**Double Gray Box**	This is also known as a white box audit. The auditor engages the target with limited knowledge of its defenses and assets and full knowledge of channels.

		The target is notified in advance of the scope and timeframe of the audit but not the channels tested or the test vectors. A double gray box audit tests the skills of the auditor and the target's preparedness to unknown variables of agitation. The nature of the test is efficiency. The breadth and depth depends upon the quality of the information provided to the auditor and the target before the test as well as the auditor's applicable knowledge.
5	**Tandem**	This is also known as a crystal box audit. The auditor and the target are prepared for the audit, both knowing in advance all the details of the audit. A tandem audit tests the protection and controls of the target. However, it cannot test the preparedness of the target to unknown variables of agitation. The true nature of the test is thoroughness as the auditor does have full view of all tests and their responses including those which do no return to the . The breadth and depth depends upon the quality of the information provided to the auditor before the test (transparancy) as well as the auditor's applicable knowledge.
6	**Reversal**	The auditor engages the taget with full knowledge of the target, it's processes, and operational security but the target knows nothing of what, how, or when the auditor will be testing. The true nature of this test is to audit the preparedness of the target to unknown variables and vectors of agitation. The breadth and depth depends upon the quality of the information provided to the auditor and the auditor's applicable knowledge and creativity.

In the event of reporting the audit, it is required to identify exactly the type of audit performed. Too often, audits of different test types are compared to track the delta (deviations) from an established baseline of the security presence. If the precise test type is not available to a third-party reviewer or regulator, the audit itself should be considered a Blind test, which is one with the least merit towards a thorough security test.

Common Terms

Commonly applied terms to security testing may be mapped as such:



1. Vulnerability Scanning refers generally to automated checks for known vulnerabilities against a system or systems in a network.

2. Security Scanning refers generally to vulnerability scans which include manual false positive verification, network weakness identification, and customized, professional analysis.

3. Penetration Testing refers generally to a goal-oriented project of which the goal is the trophy and includes gaining privileged access by pre-conditional means.

4. Risk Assessment refers generally to security analysis through interview and mid-level research which includes business justification, legal justifications, and industry specific justifications.

5. Security Auditing refers generally to a hands-on, privileged security inspection of the OS and Applications of a system or systems within a network or networks.

6. Ethical Hacking refers generally to a penetration test of which the goal is to discover trophies throughout the network within the predetermined project time limit.

7. Security Testing and it's military equivilent, the Posture Assessment, is a project-oriented risk assessment of systems and networks through the application of professional analysis on a security scan where penetration is often used to confirm false positives and false negatives as project time allows.

Glossary

Throughout this manual we refer to words and terms that may be construed with other intents or meanings. The OSSTMM uses the reference of the OUSPG Vulnerability Testing Terminology glossary available at http://www.ee.oulu.fi/research/ouspg/sage/glossary/.

Compliance

Compliance is the alignment with a set of general policies. The type of compliance required depends upon the region and currently ruling government, industry and business types, and supporting legislation. Compliance by word is compulsory however, as with any other threat, a risk assessment must be whether or not to invest in any type of compliance. Often times compliance is not as black and white as it appears to be. The OSSTMM recognizes three types of compliance:

1. Legislation. Compliance with legislation is in accordance to region where the legislation can be enforced. The strength and commitment to the legislation comes from its popularity and previously successful legal arguments and appropriately set and just enforcement measures. Failure to comply to legislation may lead to criminal charges.

2. Regulation. Compliance to regulation is in accordance to the industry or within the group where the regulation can be enforced. Failure to comply with regulations most often leads to dismissal from the group, a loss of privileges, a monetary fine, civil charges, and in some cases where legislation exists to support the regulatory body, criminal charges can be made.

3. Policy. Compliance to policy is in accordance to the business or organization where the regulation can be enforced. Failure to comply with policy most often leads to dismissal from the organization, a loss of privileges, a monetary fine, civil charges, and in some cases where legislation exists to support the policy makers, criminal charges can be made.

The OSSTMM is developed with concern for major legislation and regulations. As not all compliance is created equally, the main focus of the OSSTMM is security. Legislation and regulation that detail the purchasing of specific products, services, often through specially lobbied efforts, may have good intentions, however the OSSTMM cannot directly meet these particular requirements. As legislation and regulation may be audited either under the letter of the law or the spirit of the law, depending upon the auditing body, proof of proper and valid operational protection and controls such that as can be proved by an OSSTMM test may or may not be satisfactory. In cases of a regulation or legislation without priorly tried cases, one cannot know if the letter of the law will trump the spirit of the law either. Unfortunately this is the proof for the case of a risk assessment and whether or not priorly tried judgments of the same issue had acceptable consequences. Therefore, the OSSTMM has also been designed for discovery where elements of special products and services can be determined as to know if an other mandated audit will show compliance. In this way, one can meet both the letter and the spirit of the law whenever possible and the two do not conflict.

The following list is only for legislation which has been verified with the OSSTMM and does not limit the actual scope of regulatory and legislative bodies for which this standard may apply at least in the spirit of the law.

Legislation

The tests in this manual have included in design the remote auditing and testing from the outside to the inside of the following:

Austria

- Austrian Data Protection Act 2000 (Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000)) specifically requirements of §14

United States of America

- U.S. Gramm-Leach-Bliley Act (GLBA)
- U.S. Sarbanes-Oxley Act (SOX)
- California Individual Privacy Senate Bill - SB1386
- USA Government Information Security Reform Act of 2000 section 3534(a)(1)(A)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- OCR HIPAA Privacy TA 164.502E.001, Business Associates [45 CFR §§ 160.103, 164.502(e), 164.514(e)]
- OCR HIPAA Privacy TA 164.514E.001, Health-Related Communications and Marketing [45 CFR §§ 164.501, 164.514(e)]
- OCR HIPAA Privacy TA 164.502B.001, Minimum Necessary [45 CFR §§ 164.502(b), 164.514(d)]
- OCR HIPAA Privacy TA 164.501.002, Payment [45 CFR 164.501]

Germany

- Deutsche Bundesdatenschutzgesetz (BDSG)-- Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes from 20. December 1990, BGBl. I S. 2954, 2955, zuletzt geändert durch das Gesetz zur Neuordnung des Postwesens und der Telekommunikation vom 14. September 1994, BGBl. I S. 2325

Spain

- Spanish LOPD Ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal Art.15 LOPD -. Art. 5,
- LSSICE

Canada

- Corporate Governance
- Provincial Law of Quebec, Canada Act Respecting the Protection of Personal Information in the Private Sector (1993).

United Kingdom

- UK Data Protection Act 1998
- Corporate Governance

Australia

- Privacy Act Amendments of Australia-- Act No. 119 of 1988 as amended, prepared on 2 August 2001 incorporating amendments up to Act No. 55 of 2001. The Privacy Act 1988 (Cth) (the Privacy Act) seeks to balance individual privacy with the public interest in law enforcement and regulatory objectives of government.
- National Privacy Principle (NPP) 6 provides that an individual with a right of access to information held about them by an organization.
- National Privacy Principle (NPP) 4.1 provides that an organization must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure.

Policy

The tests in this manual have included in design the remote auditing and testing from the outside to the inside of the following:

IT Information Library

Infos available at http://www.ogc.gov.uk/index.asp?id=2261 issued by the British Office for Government Commerce (OGC)

Germany: IT Baseline Protection Manual (IT Grundschutzhandbuch)

Issued by Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security (BSI)) available at http://www.bsi.de/gshb/english/menue.htm

German IT Systems

S6.68 (Testing the effectiveness of the management system for the handling of security incidents) and tests S6.67 (Use of detection measures for security incidents)

ISO 17799-2000 (BS 7799)

This manual fully complies with all of the remote auditing and testing requirements of BS7799 (and its International equivalent ISO 17799) for information security testing.

GAO and FISCAM

This manual is in compliance to the control activities found in the US General Accounting Office's (GAO) Federal Information System Control Audit Manual (FISCAM) where they apply to network security.

NIST

This manual has matched compliance through methodology in remote security testing and auditing as per the following National Institute of Standards and Technology (NIST) publications:

- An Introduction to Computer Security: The NIST Handbook, 800-12
- Guidelines on Firewalls and Firewall Policy, 800-41
- Information Technology Security Training Requirements: A Role- and Performance-Based Model, 800-16
- DRAFT Guideline on Network Security Testing, 800-42
- PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does, 800-24
- Risk Management Guide for Information Technology Systems, 800-30
- Intrusion Detection Systems, 800-31

Rules Of Engagement

These rules define the operational guidelines of acceptable and ethical practices in marketing and selling testing, performing testing work, and handling the results of testing engagements. While those who are affiliates, partners, team members, or associates of ISECOM are contractually required to uphold the following rules of engagement, proper use of the OSSTMM also requires adherence to these rules. Failure of any person or organization to meet these rules can be reported directly to ISECOM.

Sales and Marketing

Rules for Sales and Marketing may not all apply under government request for proposals, specifically rule 1.5 in many cases is required by the government office in the response to a request for proposal (RFP).
1.1The use of fear, uncertainty, doubt, and deception may not be used in the sales or marketing presentations, websites, supporting materials, reports, or discussion of security testing for the purpose of selling or providing security tests. This includes but is not limited to using personally unverified crimes, facts, glorified criminal or hacker profiles, and statistics with the motivation of fear to create sales.
1.2 The offering of free services for failure to penetrate or provide trophies from the target is forbidden.
1.3 Public cracking, hacking, and trespass contests to promote security assurance for sales or marketing of security testing or security products are forbidden.
1.4 Performing security tests against any scope without explicit written permission from the appropriate authority is strictly forbidden.
1.5 The use of names of past clients for whom you have provided security testing for is forbidden even upon consent of said client. This does not include consented referrals between divisions, branches, offices, or institutions of the same organization or government.
1.6 It is required to advise clients truthfully and factually in regards to their security and security measures. Ignorance is not an excuse for dishonest consultancy.

Assessment / Estimate Delivery

2.3 Verifying security limitations without explicit written permission is forbidden.
2.4 The security testing of obviously highly insecure and unstable systems, locations, and processes is forbidden until the proper security infrastructure has been put in place.

Contracts and Negotiations

3.1 With or without a Non-Disclosure Agreement contract, the security auditor is required to provide confidentiality and non-disclosure of customer information and test results.
3.2 Contracts should limit liability to the cost of the job, unless malicious activity has been proven.
3.3 Contracts must clearly explain the limits and dangers of the security test as part of the statement of work.
3.4 In the case of remote testing, the contract must include the origin of the auditors by address, telephone number and/or IP address.
3.5 Contracts must contain emergency contact persons and phone numbers.
3.6 The contract must include clear, specific permissions for tests involving survivability failures, denial of service, process testing, and social engineering.
3.7 Contracts must contain the process for future contract and statement of work (SOW) changes.
3.8 Contracts must contain verified conflicts of interest for a factual security test and report.

Scope Definition

4.1 The scope must be clearly defined contractually before verifying vulnerable services.

4.2 The audit must clearly explain the limits of any security tests according to the scope.

Test Plan

5.1 The test plan must include both calendar time and man hours.
5.2 The test plan must include hours of testing.
5.3 The test plan may not contain plans, processes, techniques, or procedures which are outside the area of expertise or competence level gained by training and education of the auditor.

Test Process

6.1 The auditor must respect and maintain the safety, health, welfare, and privacy of the public both within and outside the scope.
6.2 The auditor must always operate within the law of the physical location(s) of the scope.
6.3 Client must provide a signed statement which provides testing permission exempting the auditors from trespass within the scope and damages liability to the cost of the audit service with the exception where malicious activity has been proven.
6.4 No unusual or major target changes allowed by the client during testing.
6.5 To prevent temporary raises in security only for the duration of the test, only notify key people about the testing. It is the client's judgment which discerns who the key people are, however, it is assumed that they will be information and policy gatekeepers, managers of security processes, incident response, and security operations.
6.6 If necessary for privileged testing, the client must provide two, separate, access tokens whether they be logins and passwords, certificates, secure ID numbers, badges, etc. and they should be typical to the users of the privileges being tested (no especially empty or secure accesses).
6.7 When testing includes known privileges, the auditor must first test without privileges (such as in a black box environment) prior to testing again with privileges.
6.8 The auditors are required to know their tools, where the tools came from, how the tools work, and have them tested in a restricted test area before using the tools on the client organization.
6.9 The exploitation of tests which are explicitly to test the denial of a service or process and/or survivability may only be done with explicit permission and only to the scope where no damage is done outside of the scope or the community in which the scope resides.
6.10 Tests involving people may only be performed on those identified in the scope and may not include private persons, customers, partners, associates, or other external entities without written permission from those entities.
6.11 High risk vulnerabilities such as discovered breaches, vulnerabilities with known, high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may put immediate lives at risk, discovered during testing must be reported to the customer with a practical solution as soon as they are found.
6.12 Any form of flood testing where a scope is overwhelmed from a larger and stronger source is forbidden over non-privately owned channels.
6.13 The auditor may not leave the scope in a position of less actual security than it had been provided as.

Reporting

7.1 The auditor must respect the privacy of all individuals and maintain their privacy for all results.
7.2 Results involving people untrained in security or non-security personnel may only be reported in non-identifying or statistical means.
7.3 The auditor and analyst may not sign test results and audit reports for which they were not directly involved in.

7.4 Reports must remain object and without untruths or any personally directed malice.
7.5 Client notifications are required whenever the auditor changes the testing plan, changes the source test venue, has high risk findings, previous to running new, high risk or high traffic tests, if any testing problems have occurred with and with regular, progress updates.
7.6 Where solutions and recommendations are included in the report they must be valid and practical.
7.7 Reports must clearly mark all unknowns and anomalies.
7.8 Reports must clearly state both discovered successful and failed security measures and loss controls.
7.9 Reports must use only quantitative metrics for measuring security. These metrics must be based on facts and void of subjective interpretations.
7.10 The client must be notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.
7.11 All communication channels for delivery of report must be end to end confidential.
7.12 Results and reports may never be used for commercial gain.

Process

The security testing process is a discrete event test of a dynamic, stochastic system. The target is a system, a collection of interacting and co-dependent processes, which is also influenced by the stochastic environment it exists in. Being stochastic means the behavior of events in a system cannot be determined because the next environmental state can only be partially but not fully determined by the previous state. The system contains a finite, possibly extremely large, number of variables and each change in variable presents an event and a change in state. Since the environment is stochastic, there is an element of randomness and there is no means for predetermining with certainty how all the variables will affect the system state. A discrete test examines these states within the dynamic system at particular time intervals. Monitoring operations in a continuous manner, as opposed to a discrete one, would provide far too much information to analyze. Nor may it even be possible. Even continuous tests however, require tracking each state in reference to time in order to be analyzed correctly.

A point of note is the extensive research available on change control for processes to limit the amount of indeterminable events in a stochastic system. The auditor will often attempt to exceed the constraints of change control and present "what if" scenarios which the change control implementors may not have considered. A thorough understanding of change control is essential for any auditor.

Unfortunately, auditors assume security testing is simple and often audit under what is known as the "echo process" which requires agitating and then monitoring emanations from the target for indicators of a particular state (secure or insecure, vulnerable or protected, on or off, left or right). The echo process is of the cause and effect type. The auditor makes the cause and analyzes the effect from the target. This means of testing is very fast but is also highly prone to errors, some of which may be devastating to the target. While the Rules of Engagement can help minimize damage to the target in the echo process, it cannot help minimize the errors. We categorized these errors as:

Error Types

1	False Positive	The target response indicates a particular state as true although in reality the state is not true. A false positive often occurs when the auditor's expectations or assumptions of what indicates a particular state does not hold to real-world conditions which are rarely black and white.
2	False Negative	The target response indicates a particular state as not true although in reality the state is true. A false negative often occurs when the auditor's expectations or assumptions about the target does not hold to real-world conditions, the tools are the wrong type for the test, the tools are misused, or the auditor lacks experience. A false negative can be dangerous as it is a misdiagnoses of a secure state when it does not exist.
3	Gray Positive	The target response indicates a particular state as true however the target is designed to respond to any cause with this state whether it is or not. This type of security through obscurity may be dangerous as the illusion cannot be guaranteed to work the same for all stimuli.
4	Gray Negative	The target response indicates a particular state as not true however the target is designed to respond to any cause with this

		state whether it is or not. This type of security through obscurity may be dangerous as the illusion cannot be guaranteed to work the same for all stimuli.
5	Specter	The target response indicates a particular state as either true or false although in reality the state cannot be known. A specter often occurs when the auditor's receives a response from an external stimulus that is perceived to be from the target. A specter may be either intentional of the target, an anomaly from within the channel, or the result of carelessness and/or inexperience from the auditor. One of the most common problems in the echo process is the assumption that the response is a result of the test. Cause and effect testing in the real world cannot achieve consistently reliable results since neither the cause nor the effect can be properly isolated.
6	Indiscretion	The target response indicates a particular state as either true or false but only during a particular time. That time may or may not follow a pattern and if can't be verified at a time when the state changes, it may cause the auditor to not comprehend the other state. An auditor may also determine that this is an anomaly or a problem with testing equipment especially if the auditor failed to calibrate the equipment prior to the test and perform appropriate logistics and controls. An indiscretion can be dangerous as it may lead to a false reporting of the state of security.
7	Entropy Error	The target response cannot accurately indicate a particular state as either true or false due to a high noise to signal ratio. Akin to the idea of losing a flashlight beam in the sunlight, the auditor cannot properly determine state until the noise is reduced. This type of environmentally caused error rarely exists in the lab however is a normal occurrence outside of the lab in an uncontrolled environment. Entropy can be dangerous if its effects cannot be countered.
8	Falsification	The target response indicates a particular state as either true or false although in reality the state is dependent upon largely unknown variables due to target bias. This type of security through obscurity may be dangerous as the bias will shift when tests come from different vectors or employ different techniques. It is also likely that the target is not aware of the bias.
9	Sampling Error	The target is a biased sample of a larger system or a larger number of possible states. This error normally occurs when an authority influences the operational state of the target for the duration of the test. This may be through specific time constraints on the test or a bias of testing only that which is designated as “important” within a system. This type of error will cause a misrepresentation of the overall operational security.

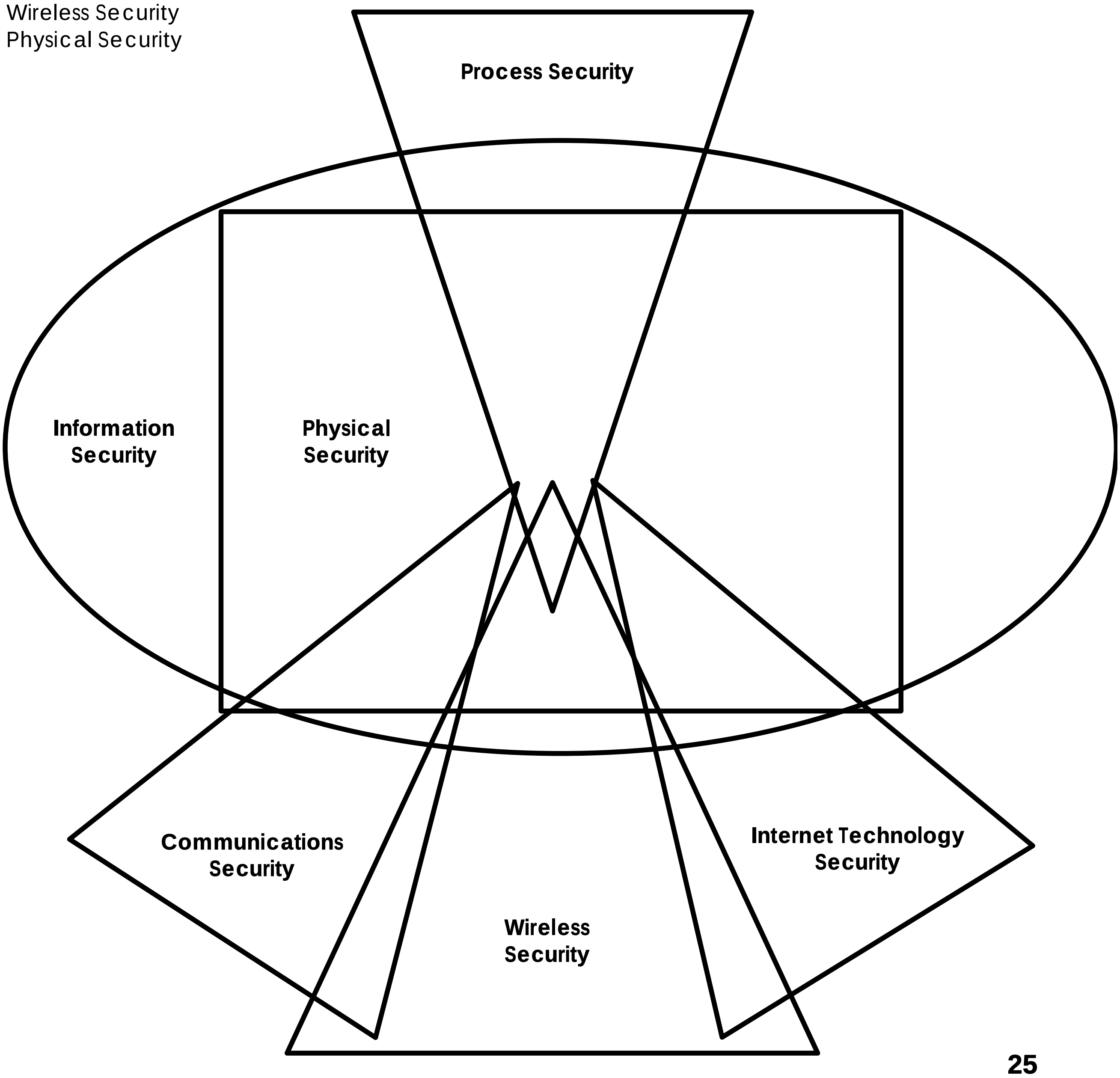
10	Constraint	The limitations of human senses or equipment capabilities indicates a particular state as either true o false although the actual state is unknown. This error is not caused by poor judgment or wrong equipment choices rather it is a failure to recognize imposed constraints or limitations.
11	Propagation	The auditor does not make a particular test or has a bias to ignore a particular result due to an presumed outcome. This is often a blinding from experience or a confirmational bias. The test may be repeated many times or the tools and equipment may be modified to have the desired outcome. As the name implies, a process which receives no feedback and the errors remain unknown or ignored will propagate further errors as the testing continues. Propagation errors may be dangerous because the errors propagated from early in testing may not be visible during an analysis of conclusions. Furthermore, a study of the entire test process is required to discover propagation errors.
12	Human Error	The errors caused by lack of ability, experience, or comprehension, is not one of bias and is always a factor and always present regardless of methodology or technique. Where an experienced auditor may make propagation errors, one without experience is more likely not to recognize human error, something which experiences teaches us to recognize and compensate for. Statistically, there is an indirect relationship between experience and human error. The less experience an auditor has, the greater the amount of human error an audit will contain.

The Security Map

The security map is a visual display of the security presence. The security presence is the environment of a security test and is comprised of six sections which are the sections of this manual. The sections each overlap and contain elements of all other sections. Proper testing of any one section must include the elements of all other sections, direct or indirect.

The sections in this manual are:

1. Information Security
2. Process Security
3. Internet Technology Security
4. Communications Security
5. Wireless Security
6. Physical Security



Security Map Module List

The module list of the security map are the primary elements of each section. Each module must further include all of the Security Dimensions which are integrated into tasks to be completed. To be said to perform an OSSTMM security test of a particular Section, all the modules of that section must be tested and of that which the infrastructure does not exist for said Module and cannot be verified, will be determined as NOT APPLICABLE in the OSSTMM Data Sheet inclusive with the final report.

1. **Information Security Testing**
   1. Posture Assessment
   2. Information Integrity Review
   3. Intelligence Survey
   4. Internet Document Grinding
   5. Human Resources Review
   6. Competitive Intelligence Scouting
   7. Privacy Controls Review
   8. Information Controls Review

2. **Process Security Testing**
   1. Posture Review
   2. Request Testing
   3. Reverse Request Testing
   4. Guided Suggestion Testing
   5. Trusted Persons Testing

3. **Internet Technology Security Testing**
   1. Logistics and Controls
   2. Posture Review
   3. Intrusion Detection Review
   4. Network Surveying
   5. System Services Identification
   6. Competitive Intelligence Scouting
   7. Privacy Review
   8. Document Grinding
   9. Internet Application Testing
   10. Exploit Research and Verification
   11. Routing
   12. Trusted Systems Testing
   13. Access Control Testing
   14. Password Cracking
   15. Containment Measures Testing
   16. Survivability Review
   17. Denial of Service Testing
   18. Security Policy Review
   19. Alert and Log Review

4. **Communications Security Testing**
   1. Posture Review
   2. PBX Review
   3. Voicemail Testing

4. FAX Testing
5. Modem Survey
6. Remote Access Control Testing
7. Voice over IP Testing
8. X.25 Packet Switched Networks Testing

5. Wireless Security Testing

1. Posture Review
2. Electromagnetic Radiation (EMR) Testing
3. 802.11 Wireless Networks Testing
4. Bluetooth Networks Testing
5. Wireless Input Device Testing
6. Wireless Handheld Testing
7. Cordless Communications Testing
8. Wireless Surveillance Device Testing
9. Wireless Transaction Device Testing
10. RFID Testing
11. Infrared Testing
12. Privacy Review

6. Physical Security Testing

1. Posture Review
2. Access Controls Testing
3. Perimeter Review
4. Monitoring Review
5. Alarm Response Review
6. Location Review
7. Environment Review

Risk Assessment

Risk assessment is maintained by both the tester and the analyst for all data gathered to support a valid assessment through non-privileged testing. This implies that if too little or improper data has been gathered then it may not be possible to provide a valid risk assesment and the tester should therefore rely on best practices, the client's industry regulations, the client's business justifications, the client's security policy, and the legal issues for the client and the client's regions for doing business.

Risk Evaluation

The OSSTMM requires that risk means that limits in the security presence will have a detrimental effect on people, culture information, processes, business, image, intellectual property, legal rights, or intellectual capital. This manual maintains four dimensions in testing for a minimal risk state environment:

1. **Safety**

   All tests must exercise concern for worst case scenarios at the greatest expenses. This requires the tester to hold above all else the regard for human safety in physical and emotional health and occupation.

2. **Privacy**

   All tests must exercise regard for the right to personal privacy regardless of the regional law. The ethics and understanding for privacy are often more advanced then current legislation.

3. **Practicality**

   All tests must be engineered for the most minimal complexity, maximum viability, and deepest clarity.

4. **Usability**

   All tests must stay within the frame of usable security. That which is most secure is the least welcoming and forgiving. The tests within this manual are performed to seek a usable level of security (also known as practical security).

Perfect Security

In risk assessment, the OSSTMM applies the technique of "Perfect Security". In Perfect Security, the tester and analyst guage the client as to what would be perfect security. This is countered with the Posture Review, which is best practices, the client's industry regulations, the client's business justifications, the client's security policy, and the legal issues for the client and the client's regions for doing business. The result is Perfect Security for that client. The tester and analyst then provide a gap analysis between the current state of security with Perfect Security.

Simple best practices as defined as a theoretical towards Perfect Security:

Internet Gateway and Services

- No unencrypted remote access.
- No unauthenticated remote access.
- Restrictions deny all and allow specifically.
- Monitor it all and log it.
- Decentralize.
- Limit Inter-system trust.
- Quarantine all inputs and validate them.
- Install only the applications / daemons necessary.
- Layer the security.
- Invisible is best- show nothing except the service itself.
- Simplicity prevents configuration errors.

Mobile Computing

- Quarantine all incoming network and Internet traffic.
- No unencrypted remote access.
- No unauthenticated remote access.
- Encrypt accordingly.
- Install only the applications / daemons necessary.
- Invisible is best- no running services.
- BIOS passwords required.
- Security training for best practices and recognizing security issues is required for users and helpdesks.

Applications

- Usability of security features should be a strength.
- Assure business justifications for all inputs and outputs in the application.
- Quarantine and validate all inputs.
- Limit trusts (to systems and users).
- Encrypt data.
- Hash the components.
- All actions occur on the server side.
- Layer the security.
- Invisible is best- show only the service itself.
- Trigger it to alarm.

People

- Decentralized authority.
- Personal responsibility.
- Personal security and privacy controls.
- Accessible only through gateway personnel.
- Trained in defined legalities and ethics from security policies.
- Limited, need-to-know access to information and infrastructure.

Security Metrics

The completion of a thorough security audit has the advantage of providing accurate metrics on the state of security. The less thorough the audit means a less accurate overall metric. Alternately, lesser skilled auditors and lesser experienced analysts will also adversely affect the quality of the metric. Therefore, a successful metric of security requires an audit which can be described as testing (measuring) from the appropriate vectors required while accounting for inaccuracies and misrepresentations in the test data and skills or experience of the security professionals performing the audit. Faults in these requirements will result in lower quality measurements and false security determinations.

This methodology refers to metrics as Risk Assessment Values (RAVs). While not a risk assessment in itself, an audit with this methodology and the RAVs will provide the factual basis for a more accurate and more complete risk assessment.

Applying Risk Assessment Values

This methodology will define and quantify three areas within the scope which together create the big picture defined as Actual Security as its relevance to the current and real state of security. The big picture approach is to calculate separately as a hash, each of the areas: Operations, Controls, and Limitations. The 3 hashes are combined to form the fourth hash, Actual Security, to provide the big picture type overview and a final metric for comparisons. Since RAVs are the hash of relevant security information, they are infinitely scalable. This allows for comparable values between two or more scopes regardless of the target, vector, test type, or index where the index is the method of how individual targets are calculated. This means with RAVs that the security between a single target can be realistically compared with 10,000 targets.

One important rule to applying these metrics is that Actual Security can only be calculated per scope. A change in channel, vector, or index is a new scope and a new calculation for Actual Security. However, multiple scopes can be calculated together to create one Actual Security that represents a fuller vision of operational security. For example, the audit will be made of internet-facing servers from both the internet side and from within the perimeter network which they reside. That is 2 vectors. The first vector is indexed by IP address and contains 50 targets. The second vector is indexed by MAC address and is 100 targets. Once each audit is completed and metrics are counted for each of the 3 areas, they can be combined into one calculation of 150 targets and the sums of each area. This will give a final Actual Security metric which is much more complete for that perimeter network then either would be alone.

Actual Security

Value Types	Descriptions
Operations	The lack of security one must have to be interactive, useful, public, open, or available. For example, limiting how a person buys goods or services from a store over a particular channel, such as 1 door for going in and out, is a method of security within the store's operations. Operations are defined by visibility, trusts, and accesses.

Controls	Impact and loss reduction controls. The assurance that the physical and information assets as well as the channels themselves are protected from various types of invalid interactions as defined by the channel. For example, insuring the store in the case of fire is a control that does not prevent the inventory from getting damaged or stolen but will pay out equivalent value for the loss. There are 10 controls. The first five controls are Class A which control interactions. The five class B controls are relevant to controlling procedures.
Limitations	This is the current state of perceived and known limits for channels, operations, and controls as verified within the audit. For example, an old lock that is rusted and crumbling used to secure the gates of the store at closing time has an imposed security limitation where it is at a fraction of the protection strength necessary to delay or withstand an attack. Determining that it is old and weak through visual verification in this case is referred to as an identified limitation. Determining it is old and weak by breaking it using 100 kg of force when a successful deterrent requires 1000 kg of force shows a verified limitation.

Operational Security

To measure the security of operations (OPSEC) requires the measurements of visibility, trust, and access from the scope. The number of targets in the scope that can be determined to exist by direct interaction, indirect interaction, or passive emanations is its visibility. As visibility is determined, its value represents the number of targets in the scope. Trust is any non-authenticated interaction to any of the targets. Access is the number of interaction points with each target. The sum of all three is the OPSEC Delta, which is the total number of openings within operations and represents the total amount of operational security decreased within the target.

Calculating OPSEC

OPSEC Categories	**Descriptions**
Visibility	The number of targets in the scope according to the scope. Count all targets by index only once and maintain the index consistently for all targets. It is generally unrealistic to have more targets visible then are targets in the defined scope however it may be possible due to vector bleeds where a target which is normally not visible from one vector is visible due to a misconfiguration or anomaly. A HUMSEC audit employs 50 people however only 38 of them are interactive from the test vector and channel. This would make a visibility of 38.
Trust	Count only each target allowing for unauthenticated interaction according to the scope. A HUMSEC audit may reveal that the help desk employees grant password resets for all calls coming from internal phones without requesting identifying or authorizing information. Within this context, each help desk employee who does this is counted as a Trust for this scope. However, the same cannot be held true for external calls as in that different scope, the one with the external to internal vector, these same help desk employees are not counted as trusts.

Access	This is different from visibility where one is determining the number of existing targets. Here the auditor must count each Access per unique interaction point per unique probe. In a PHYSSEC audit, a building with 2 doors and 5 windows which all open has an Access of 7. If all the doors and windows cannot be opened then it is an Access of 0 as these are not points where one can gain entry. For a COMSEC audit of data networks, the auditor counts each port response as an Access regardless how many different ways the auditor can probe that port. However, if a service is not hosted at that port (daemon or an application) then all replies come from the IP Stack. Therefore a server that responds with a SYN/ACK and service interactivity to 1 of the TCP ports scanned and with a RST to the rest is not said to have an access count of 65536 (including port 0) since 66535 of the ports respond with the same response of RST which is from the kernel. To simplify, count uniquely only ports with service responses and IP Stack responses only when the probe initiates service interactivity. A good example of a service activity over the IP Stack is an ICMP echo response (PING reply). With HUMSEC audits, this is much more simplified. A person who responds to a query counts as an access with all types of queries (all the different questions you may ask or statements made count as the same type of response on the same channel). Therefore a person can only be an Access of 1 per channel and vector. Only a person who completely ignores the request by not acknowledging the channel is not counted.
OPSEC Delta	Visibility + Trust + Access The negative change in OPSEC protection.

Controls

Controls are the 10 loss protection categories in two categories, Class A (interactive) and Class B (process). The Class A categories are authentication, indemnification, subjugation, continuity, and resilience. The Class B categories are non-repudiation, confidentiality, privacy, integrity, and alarm.

Class A

- Authentication is the control of interaction requiring having both credentials and authorization where identification is required for obtaining both.
- Indemnification is the control over the value of assets by law and/or insurance to recoup the real and current value of the loss.
- Subjugation is the locally sourced control over the protection and restrictions of interactions by the asset responsible.
- Continuity is the control over processes to maintain access to assets in the events of corruption or failure.
- Resilience is the control over security mechanisms to provide protection to assets in the events of corruption or failure.

Class B

- Non-repudiation prevents the source from denying its role in any interactivity regardless whether or not access was obtained.
- Confidentiality is the control for assuring an asset displayed or exchanged between parties can be known outside of those parties.

- Privacy is the control for the method of how an asset displayed or exchanged between parties can be known outside of those parties.
- Integrity is the control of methods and assets from undisclosed changes.
- Alarm is the control of notification that OPSEC or any controls have failed, been compromised, or circumvented.

Calculating Controls

Loss Controls Categories	Descriptions
Authentication	Count each instance of authentication required to gain access. This requires that authorization and identification make up the process for the proper use of the authentication mechanism. In a PHYSSEC audit, if both a special ID card and a thumb print scan is required to gain access then add two for authentication. However if access just requires one or the other then only count one.
Indemnification	Count each instance of methods used to exact liability and insure compensation for all assets within the scope. A basic PHYSSEC example is a warning sign threatening to prosecute trespassers. Another common example is property insurance. In a scope of 200 computers, a blanket insurance policy against theft applies to all 200 and therefore is a count of 200. However, do not confuse the method with the flaw in the method. A threat to prosecute without the ability or will to prosecute is still an indemnification method however with a limitation.
Subjugation	Count each instance for access or trust in the scope which strictly does not allow for controls to follow user discretion or originate outside of itself. This is different from being a security limitation in the target since it applies to the design or implementation of controls. In a COMSEC data networks audit, if a login can be made in HTTP as well as HTTPS but requires the user to make that distinction then it fails to count toward Subjugation. However, if the implementation requires the secured mode by default such as a PKI-based internal messaging system then it does meet the requirement of the Subjugation control for that scope. More simply, in HUMSEC, a non-repudiation process where the person must sign a register and provide an identification number to receive a document is under Subjugation controls when the provider of the document records the identification number rather than having the receiver do so to eliminate the recording of a false number with a false name.
Continuity	Count each instance for access or trust in the scope which assures that no interruption in interaction over the channel and vector can be caused even under situations of total failure. Continuity is the umbrella term for characteristics such as survivability, load balancing, and redundancy. In a PHYSSEC audit, it is discovered that if an entry way into a store becomes blocked no alternate entry way is possible and customers cannot enter therefore the access does not

	have Continuity. In a COMSEC data networks audit, if a web server service fails from high-load then an alternate web server provides redundancy so no interactions are lost. This access does have Continuity.
Resistance	Count each instance for access or trust in the scope that does not fail open and without protection or provide new accesses upon a security failure. In common language, it is said to “fail securely”. In a PHYSSEC audit, if a guard controlling authentication to access a door is removed in any way, the door must not remain open or else it does not have Resistance. In a COMSEC data networks audit, if a web service requiring a login or password loses communication with its authentication database, then all access should be denied rather than permitted to have Resistance.
Non-repudiation	Count each instance for the access or trust that provides a non-repudiation mechanism for each interaction to provide assurance that the particular interaction did occur at a particular time between the identified parties. Non-repudiation depends upon identification and authorization to be properly established for it to be properly applied without limitations. In a PHYSSEC audit, the Non-repudiation control exists if the entrance to a building requires a camera with a biometric face scan to gain entry and each time it is used, the time of entry is recorded with the ID. However, if a key-card is used instead, the Non-repudiation control, requires a synchronized, time-coded camera to assure the record of the card-users identity to avoid being a flawed implementation. If the door is tried without the key card, not having the synchronized camera monitoring the door would mean that not all interactions with the entryway have the Non-repudiation control and therefore does not count for this control. In a COMSEC data networks audit, there may be multiple log files for non-repudiation. A port scan has interactions at the IP Stack and go into one log while interaction with the web service would log to another file. However, as the web service may not log the interactions from the POST method, the control is still counted however so is the security limitation.
Confidentiality	Count each instance for access or trust in the scope that provides the means to maintain the content of interactions undisclosed between the interacting parties. A typical tool for Confidentiality is encryption. Additionally, obfuscation of the content of an interaction is also a type of confidentiality albeit a flawed one. In HUMSEC, however, a method of Confidentiality may include whispering or using hand signals.
Privacy	Count each instance for access or trust in the scope that provides the means to maintain the method of interactions undisclosed between the interacting parties. While “being private” is a common expression, the phrase is a bad example of what privacy is as a loss control because it includes elements of confidentiality. As a loss control, when something is done “in private” it means that only “the doing” is private but the content of the interaction may not be. A typical tool for Privacy is opaquing the interaction, having the interaction take place

	outside of the Visibility of third parties. Confusion of the means of interaction as obfuscation is another method of applying the Privacy control. In HUMSEC, a method of Privacy may be simply taking the interaction into a closed room away from other people. In movies, we see techniques to create the Privacy control such as setting two of the same suitcases set side by side, some type of incident to create confusion takes place and the two people switch the suitcases in seemingly plain view.
Integrity	Count each instance for access or trust in the scope which can assure that the interaction process and access to assets has finality and cannot be corrupted, hanged, continued, redirected, or reversed without it being known to the parties involved. Integrity is a change control process. In COMSEC data networks, encryption or a file hash can provide the Integrity control over the change of the file in transit. In HUMSEC, segregation of duties and other corruption-reduction mechanism provide Integrity control. Assuring integrity in personnel requires that two or more people are required for a single process to assure oversight of that process. This includes that no master access to the whole process exists. This can be no person with full access and no master key to all doors.
Alarm	Count each instance for access or trust which has a record or makes a notification when unauthorized and unintended porosity increases for the vector or restrictions and controls are compromised or corrupted. In COMSEC data networks, count each server and service which a network-based intrusion detection system monitors. Or count each service that maintains a monitored log of interaction. Access logs count even if they are not used to send a notification alert immediately unless they are never monitored. However, logs which are not designed to be used for such notifications, such as a counter of packets sent and received, does not classify as an alarm as there is too little data stored for such use.
Controls Delta	Sum (all controls) *.1 The positive change over OPSEC protection. The 10 loss controls combined balance the value of 1 OPSEC loss (access, visibility, or trust).

Security Limitations

The state of security in regard to known flaws and protection restrictions within the scope are calculated as Limitations. To give appropriate values to each limitation type, they must be categorized and classified. While any classification name or number can be used, this methodology attempts to name them according to their effects on OPSEC and Controls and does not regard them in a hierarchal format of severity. Five classifications are designated to represent all types of limitations.

1. Vulnerability is a flaw or error that denies access to assets for authorized people or processes, allows for privileged access to assets to unauthorized people or processes, or allows unauthorized people or processes to hide assets or themselves within the scope.

2. Weakness is a flaw or error that disrupts, reduces, abuses, or nullifies specifically the effects of the interactivity controls authentication, indemnification, resistance, subjugation, and continuity.
3. Concern is a flaw or error that disrupts, reduces, abuses, or nullifies the effects of the flow or execution of process controls non-repudiation, confidentiality, privacy, integrity, and alarm.
4. Exposure is an unjustifiable action, flaw, or error that provides direct or indirect visibility of targets or assets within the chosen scope channel of the security presence.
5. Anomaly is any unidentifiable or unknown element which cannot be accounted for in normal operations.

The concept that limitations are only limitations if they have no justification in business or otherwise is false. A limitation is a limitation if it behaves in one of the limiting factors as described here. A justification for a limitation is a risk decision and one that is either met with a control of some kind even if that control is merely acceptance. Risk decisions that accept the limitations as they are often come down to: the damage a limitation can do does not justify the cost to fix or control the limitation, the limitation must be so according to legislation, regulations, or policy, or a conclusion that the threat does not exist or is likely for the particular limitation. Risk justifications do not enter in the RAV metrics and all limitations should be counted as discovered regardless if best practice, common practice, or legal practice denotes it as not an acceptable risk. For the metric to be a true representation of the operational security of the scope, for the ability of future risk assessments to be performed with the metric as a basis, and for proper controls to be used to offset even those risks deemed necessary for legislative reasons, the auditor must report the operational security state as it is.

Another concept that must be taken into consideration is one of managing flaws and errors in an audit. An audit will often uncover more than one flaw per target. The auditor is to report the flaws per target and not the weak targets. These flaws may be in the protection measures and controls themselves diminishing actual security. Each flaw is to be rated as to what occurs when the flaw is invoked even if that must be theoretical or of limited execution to restrict actual damages. Theoretical categorization, where operation could not take place, is a slippery slope and should really only be limited in the case of a medium to high risk of actual damages or where recovery from damage is difficult or requires a long time period. When categorizing the flaws, each flaw should be examined and calculated in specific terms of operation at its most basic components. However, the auditor should be sure never to report a “flaw within a flaw” where the flaws share the same component and same operational effect.

Calculating Flaws

These are examples of how to correctly classify flaws in PHYSSEC audits.

There is only one operational door into the front of the store (weakness). It is made of standard glass (vulnerability) which has a small crack along the side of it (vulnerability).[1] The lock mechanism requires a standard key of normal complexity which can only be opened by someone with 1-2 years of locksmith skills. The lock is old and brittle however and may not survive repeated hits with a hammer (unverified weakness). The alarm system for the door only triggers when the door is forced and when the lock is turned (concern). From the doorway, one can see the cashier and count the amount of money exchanged (exposure) and when money is being prepared to be dropped in the safe (exposure) .[2]

[1] This is an example of a flaw within a flaw where the glass is the most basic component and the flaw is the same result (access through force).

[2] This is also a flaw within a flaw and although it's the same basic component as #1, but the operational effect is one of viewing assets instead of access through force. Here we count both exposures because the problem is both the visibility through the glass of assets and visibility of a process, the safe drop.

Calculating Security Limitations

Limitations Categories	Auditing and Examples
Vulnerability	Count separately each flaw or error that that defies protections whereby a person or process can access, deny access to others, or hide itself or assets within the scope. In PHYSSEC, a vulnerability can be such things as a simple glass door, a metal gate corroded by the weather, a door that can be sealed by wedging coins into the gap between it and its frame, electronic equipment outdoors not sealed from pests such as ants or mice, a bootable cd-rom drive on a PC, or a process that allows an employee to take a trashcan large enough to hide or transport assets out of the scope. In HUMSEC, a vulnerability can be a cultural bias that does not allow an employee to question others who do not look like they belong there or a lack of training which leaves a new secretary to give out business information classified for internal use only to a caller. In COMSEC data security, a vulnerability can be such things as a flaw in software that allows an attacker to overwrite memory space to gain access, a computation flaw that allows an attacker to lock the CPU into 100% usage, or an operating system that allows enough data to be copied onto the disk until it itself can't operate anymore. In COMSEC telecommunications, a vulnerability can be a flaw in the pay phone system that allows sounds through the receiver mimic coin drops, a telephone box that allows anyone to access anyone else's phone line, a voice mail system that provides messages from any phone anywhere, or a FAX machine that can be polled remotely to resend the last thing in memory to the caller's number. In SPECSEC, a vulnerability can be hardware which can be overloaded and burnt out by higher powered versions of the same frequency or a near frequency, a standard receiver without special configuration which can access the data in the signal, a receiver which can be forced to accept a third-party signal in place of the intended one, or a wireless access point dropping connections from a nearby microwave oven.
Weakness	Count each flaw or error in the controls for interactivity: authentication, indemnification, resistance, subjugation, and continuity. In PHYSSEC, a weakness can be such things as a door lock that opens when a card is wedged between it and the door frame, a back-up generator with no fuel, or insurance that doesn't cover flood damage in a flood zone. In HUMSEC, a weakness can be a process failure of a second guard to take the post of the guard who runs after an intruder or a cultural climate within a company for allowing friends into posted restricted spaces. In COMSEC data security, a weakness can be such things as login that allows unlimited attempts or a web farm with round-robin DNS for load balancing although each system has also a unique name for direct linking.

	In COMSEC telecommunications, a weakness can be a flaw in the PBX that has still the default administration passwords or a modem bank for remote access dial-in which does not log the caller numbers, time, and duration. In SPECSEC, a weakness can be a wireless access point authenticating users based on MAC addresses or a RFID security tag that no longer receives signals and therefore fails "open" after receiving a signal from a high power source.
Concern	Count each flaw or error in process controls: non-repudiation, confidentiality, privacy, integrity, and alarm. In PHYSSEC, a concern can be such things as a door lock mechanism whose operation controls and key types are public, a back-up generator with no power meter or fuel gage, an equipment process that does not require the employee to sign-out materials when received, or a fire alarm not loud enough to be heard by machine workers with ear plugs. In HUMSEC, a concern can be a process failure of a guard who maintains the same schedule and routine or a cultural climate within a company that allows employees to use public meeting rooms for internal business. In COMSEC data security, a concern can be the use of locally generated web server certificates for HTTPS or log files which record only the transaction participants and not the correct date and time of the transaction. In COMSEC telecommunications, a concern can be the use of a FAX machine for sending private information or a voice mail system that uses touch tones for entering a PIN or password. In SPECSEC, a concern can be a wireless access point using weak data encryption or an infrared door opener that cannot read th sender in the rain.
Exposure	Count each unjustifiable action, flaw, or error that provides direct or indirect visibility of targets or assets within the chosen scope channel of the security presence. In PHYSSEC, an exposure can be such things as a window which allows one to view assets and processes or an available power meter that shows how much energy a building uses and its fluctuation over time. In HUMSEC, an exposure can be a guard who allows all visitors to view the sign-in sheet with all the other visitors listed on it or a company operator who informs callers that a particular person is out sick or on vacation. In COMSEC data security, an exposure can be a descriptive and valid banner about a service (disinformation banners are not exposures) or a ICMP echo reply from a host. In COMSEC telecommunications, an exposure can be an automated company directory sorted by alphabet allowing anyone to cycle through all persons and numbers or a FAX machine that stores the last dialed numbers. In SPECSEC, an exposure can be a signal that disrupts other machinery announcing its activity or an infrared device whose operation is visible by standard video cameras with night capability.

Anomaly	Count each unidentifiable or unknown element which cannot be accounted for in normal operations, generally when the source or destination of the element cannot be understood. An anomaly may be an earl sign of a security problem. Since unknowns are elements which cannot be controlled for, a proper audit requires noting any and all anomalies. In PHYSSEC, an anomaly can be dead birds discovered on the roof of a building around communications equipment. In HUMSEC, an anomaly can be questions a guard asks which may seem irrelevant to either the job or standard small talk. In COMSEC data security, an anomaly can be correct responses to a probe from a different IP address than was probed or expected. In COMSEC telecommunications, an anomaly can be a modem response from a number that has no modem. In SPECSEC, an anomaly can be a powerful and probably local signal that appears once momentarily but not long enough to locate the source.

Actual Security

To measure the current state of operations with applied controls and discovered limitations, a final calculation is required to define Actual Security. As implied by its name this is the whole security value which combines the three values of operational security, controls, and limitations to show the actual state of security.

The purpose of Actual Security is to condense the three combined values into a simple metric value percentile that can be used to rate operational security effectiveness and provide a method of comparison, scoring, and rating. This big picture approach is effective because it does not simply show how one is prepared for threats but how effective one's preparations are against threats.

Security Limitations Categories	**Descriptions**
Actual Delta	The actual security delta is the sum of Op Sec Delta and Loss Controls Delta and subtracting the Security Limitations Delta. The Actual Delta is useful for comparing products and solutions by previously estimating the change (delta) the product or solution would make in the scope.
Actual Security (Total)	Actual security is the true (actual) state of security provided as a hash of all three sections and represented in a percentage where 100% represents a balance of controls for interaction points to assets with no limitations.

Sections and Modules

The methodology is broken down into *sections*, *modules* and *tasks*. The sections are specific points in the security map that overlap with each other and begin to dissect a whole that is much less than the sum of its parts. The modules are the flow of the methodology from one security presence point to the other. Each module has an input and an output. The input is the information used in performing each task. The output is the result of completed tasks. Output may or may not be analyzed data (also known as intelligence) to serve as an input for another module. It may even be the case that the same output serves as the input for more than one module or section.

Some tasks yield no output; this means that modules will exist for which there is no input. Modules which have no input can be ignored during testing. Ignored modules do not necessarily indicate an inferior test; rather they may indicate superior security.

Modules that have no output as the result can mean one of five things:

1. The channel had been obstructed in some way during the performing of the tasks.
2. The tasks were not properly performed.
3. The tasks were not applicable.
4. The task result data has been improperly analyzed.
5. The task reveals superior security.

It is vital that impartiality exists in performing the tasks of each module. Searching for something you have no intention of finding may lead to you finding exactly what you want. In this methodology, each module begins as an input and output exactly for the reason of keeping bias low. Each module gives a direction of what should be revealed to move further down the flow.

Time is relative. Larger test environments mean more time spent at each section, module and task. The amount of time allowed before returning with output data depends on the tester, the test environment, and the scope of the testing. Proper testing is a balance of time and energy where time is money and energy is the limit of man and machine power.

Identifying tasks that can be seen as “less than vital” and thereby “safely” trimmed from testing is vital when defining test modules for a target system, where project scope or restraints require. These omitted tasks however should be clearly documented and agreed prior to testing.

With the provision of testing as a service, it is highly important to identify to the commissioning party exactly what *has not or will not* be tested, thereby managing expectations and potentially inappropriate faith in the security of a system.

Test Modules and Tasks

Module Example

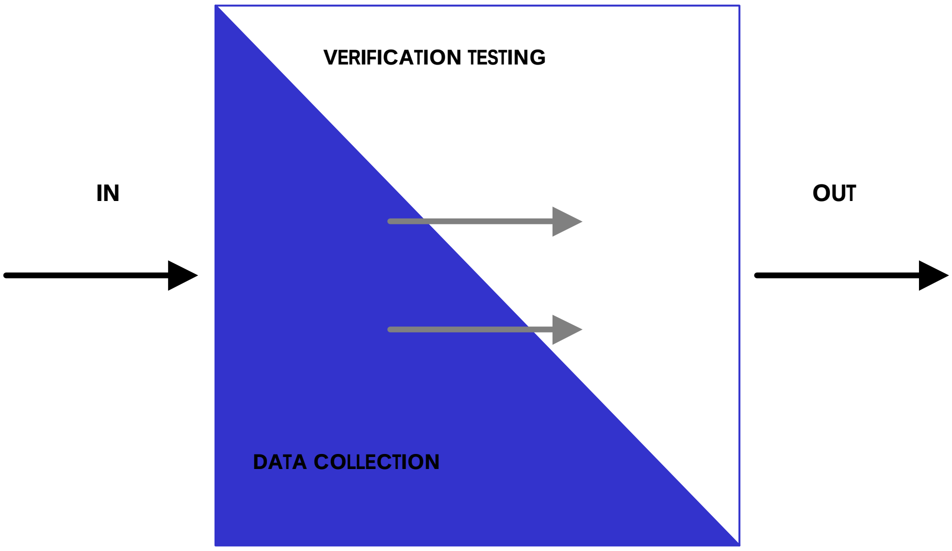
Module Name
Description of the module.

Expected Results:	Item Idea Concept Map

Group task description.

Task 1
Task 2

Methodology



The methodology flows from the initial module to the completion of the final module. The methodology allows for a separation between data collection and verification testing of and on that collected data. The flow may also determine the precise points of when to extract and when to insert this data.

In defining the methodology of testing, it is important to not constrict the creativity of the tester by introducing standards so formal and unrelenting that the quality of the test suffers. Additionally, it is important to leave tasks open to some interpretation where exact definition will cause the methodology to suffer when new technology is introduced.

Each module has a relationship to the one before it and the one after it. Each section has inter-relational aspects to other modules and some inter-relate with all the other sections. Overall, security testing begins with an input that is ultimately the addresses of the systems to be tested. Security testing ends with the beginning of the analysis phase and the construction of the final report. This methodology does not affect the form, size, style, or content of the final report nor does it specify how the data is to be analyzed. That is left to the security tester or organization.

Sections are the whole security model divided into manageable, testable slices. Modules are the test variables in sections. The module requires an input to perform the tasks of the module and the modules of other sections. Tasks are the security tests to perform depending upon the input for the module. The results of the tasks may be immediately analyzed to act as a processed result or left raw. Either way, they are considered the output of the module. This output is often the input for a following module or in certain cases such as newly discovered hosts, may be the input for a previous module.

The whole security model can be broken up into manageable sections for testing. Each Section can in turn be viewed as a collection of test modules, with each module being broken up into sets of tasks.

Section A – Information Security

Modules

1. Competitive Intelligence Review

CI Scouting is the scavenged information from an Internet presence that can be analysed as business intelligence. Different than the straight-out intellectual property theft found in industrial espionage or hacking, CI tends to be non-invasive and much more subtle. It is a good example of how the Internet presence extends far beyond the hosts in the DMZ. Using CI in a penetration test gives business value to the components and can help in finding business justifications for implementing various services.

Expected Results:	A measurement of the organization's network business justifications Size and scope of the Internet presence A measurement of the security policy to future network plans

Tasks to perform for a thorough Competitive Intelligence Scouting:

1. Map and measure the directory structure of the web servers
2. Map the measure the directory structure of the FTP servers
3. Examine the WHOIS database for business services relating to registered host names
4. Determine the IT cost of the Internet infrastructure based on OS, Applications, and Hardware.
5. Determine the cost of support infrastructure based on regional salary requirements for IT professionals, job postings, number of personnel, published resumes, and responsibilities.
6. Measure the buzz (feedback) of the organization based on newsgroups, web boards, and industry feedback sites
7. Record the number of products being sold electronically (for download)
8. Record the number of products found in P2P sources, wares sites, available cracks up to specific versions, and documentation both internal and third party about the products

2. Privacy Review

The privacy review is the focal point of the legal and ethical storage, transmission, and control of data based on employee and customer privacy. The use of this data is a concern to many private persons and legislation is unveiling specific rules regarding privacy. Although some of these laws are local, all of them apply to the Internet and therefore affect security testers internationally.

Expected Results:	List any disclosures List compliance failures between public policy and actual practice List systems involved in data gathering List data gathering techniques List data gathered

Tasks to perform for a thorough Privacy Policy review:

1. Compare publicly accessible policy to actual practice
2. Compare actual practice to regional fraud and privacy laws or compliancy
3. Identify database type and size for storing data
4. Identify data collected by the organization
5. Identify storage location of data
6. Identify cookie types
7. Identify cookie expiration times
8. Identify information stored in cookie
9. Verify cookie encryption methods
10. Identify server location of web bug(s)
11. Identify web bug data gathered and returned to server

3. Document Grinding

The module here is important in the verification of much of the tested information and pertains to many levels of what is considered information security. The amount of time granted to the researching and extraction of information is dependent upon the size of the organisation, the scope of the project, and the length of time planned for the testing. More time however, does not always mean more information but it can eventually lead to key pieces of the security puzzle.

Expected Results:	A profile of the organization A profile of the employees A profile of the organization's network A profile of the organization’s technologies A profile of the organization’s partners, alliances, and strategies

Tasks to perform for a thorough Document Grind:

1. Examine web databases and caches concerning the target organization and key people.
2. Investigate key persons via personal homepages, published resumes, organizational affiliations, directory enquiries, companies house data, and electoral register.
3. Compile e-mail addresses from within the organization and personal e-mail addresses from key people.
4. Search job databases for skill sets technology hires need to possess in the target organization.
5. Search newsgroups for references to and submissions from within the organization and key people.
6. Search documents for hidden codes or revision data.
7. Examine P2P networks for references to and submissions from within the organization and key people.

Section B – Process Security

Modules

1. Request Testing

This is a method of gaining access priviledges to an organization and its assets by querying gateway personnel over communications medium such as telephone, e-mail, chat, bulletin boards, etc. from a fraudulent "priviledged" position. Gateway personnel are those who themselves have the authority to grant access priviledges to others.

Expected Results:	List of access code methods List of valid codes Names of gateway persons Methods of obtaining this information List of information obtained

Tasks to perform for a thorough Request test:

1. Select a gateway person from information already gained about personnel
2. Examine the contact methods for gateway person from the target organisation
3. Gather information about gateway person (position, habits, preferences)
4. Contact gateway person and request information from an authority or priviledged position
5. Gather information from gateway person
6. Enumerate amount of priviledged information disclosed.

2. Guided Suggestion Testing

This is a method of enumeration and priviledged access points enumeration to an organization and its assets by inviting internal personnel over communications medium such as telephone, e-mail, chat, bulletin boards, etc. to an outside location from a fraudulent "priviledged" position. This invitation technique requires a "location" for the person to be invited to such as a web page, e-mail account,

Expected Results:	List of access points List of internal IP addresses Methods of obtaining this information List of information obtained

Tasks to perform for a thorough Guided Suggestion test:

1. Select a person or persons from information already gained about personnel
2. Examine the contact methods for the people from the target organisation
3. Invite the people to use / visit the location
4. Gather information from the visitors
5. Enumerate the type and amount of priviledged information disclosed.

3. Trusted Persons Testing

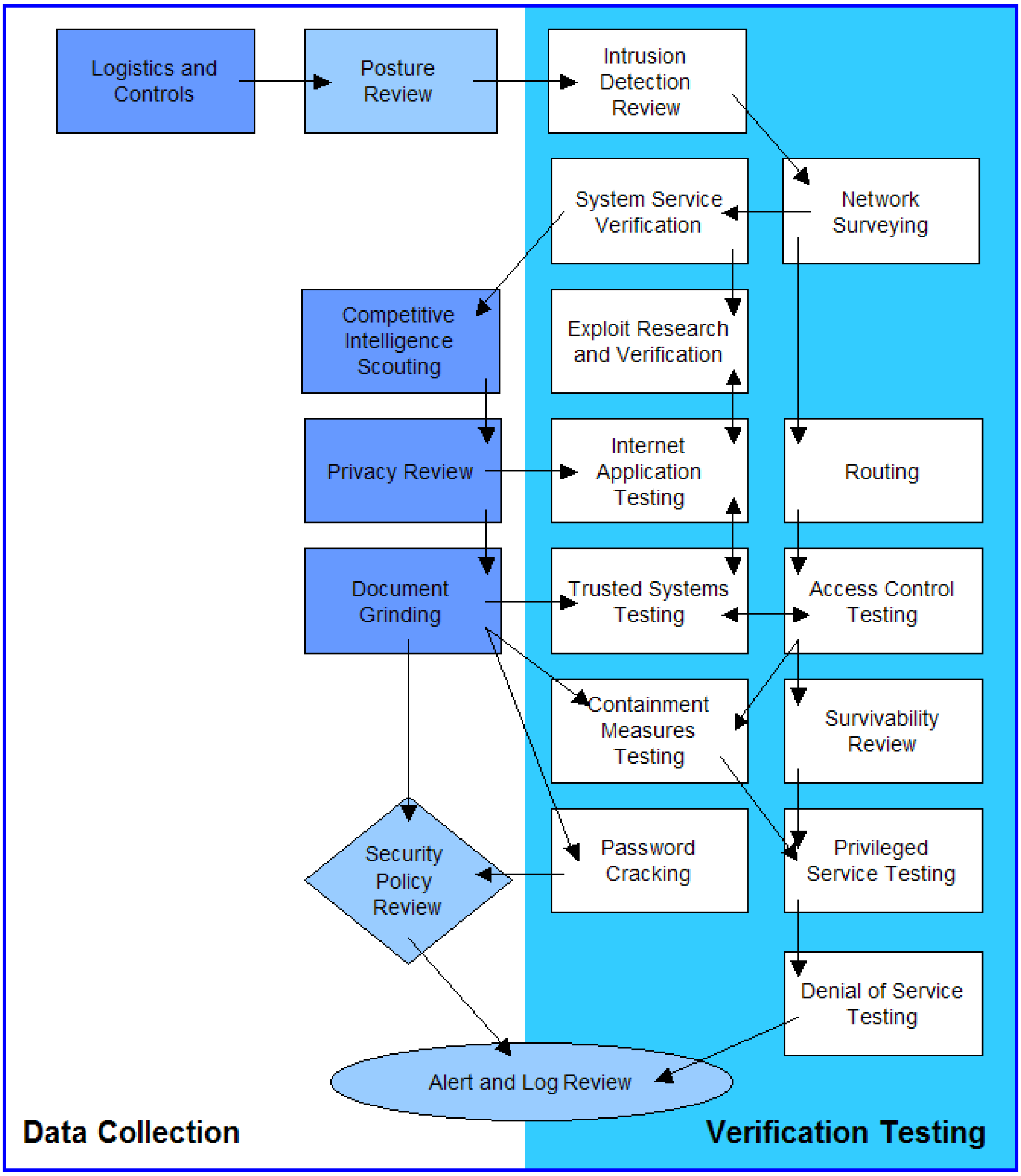
This is a method of using a trusted position of such as that of an employee, vendor, partner, or daughter company employee to subvert the internal person into disclosing information concerning the target organization. This module may be performed through any communication means or in person.

Expected Results:	List of trusted persons List of trusted positions Methods of obtaining this information List of information obtained

Tasks to perform for a thorough Trusted Persons test:

1. Select a person or persons from information already gained about personnel
2. Examine the contact methods for the people from the target organisation
3. Contact the internal person from a position of trust
4. Gather information from the internal person
5. Enumerate the type and amount of priviledged information disclosed.

Section C – Internet Technology Security



Modules

1. Network Surveying

A network survey serves often as an introduction to the systems to be tested. It is best defined as a combination of data collection, information gathering, and policy control. Although it is often advisable from a legal standpoint to define contractually exactly which systems to test if you are a third-party auditor or even if you are the system administrator, you may not be able to start with concrete system names or IP addresses. In this case you must survey and analyze. The point of this exercise is to find the number of reachable systems to be tested without exceeding the legal limits of what you may test. Therefore the network survey is just one way to begin a test; another way is to be given the IP range to test. In this module, no intrusion is being performed directly on the systems except in places considered a quasi-public domain.

In legal terms, the quasi-public domain is a store that invites you in to make purchases. The store can control your access and can deny certain individuals entry but for the most part is open to the general public (even if it monitors them). This is the parallel to an e-business or web site.

Although not truly a module in the methodology, the network survey is a starting point. Often more hosts are detected during actual testing. Please bear in mind that the hosts discovered later may be inserted in the testing as a subset of the defined testing and often only with permission or collaboration with the target organization's internal security team.

Expected Results:	Domain Names Server Names IP Addresses Network Map ISP / ASP information System and Service Owners Possible test limitations

Tasks to perform for a thorough network survey include:

Name server responses.

- Examine Domain registry information for servers.
- Find IP block owned.
- Question the primary, secondary, and ISP name servers for hosts and sub domains.

Examine the outer wall of the network.

- Use multiple traces to the gateway to define the outer network layer and routers.

Examine tracks from the target organization.

- Search web logs and intrusion logs for system trails from the target network.
- Search board and newsgroup postings for server trails back to the target network.

Information Leaks

- Examine target web server source code and scripts for application servers and internal links.
- Examine e-mail headers, bounced mails, and read receipts for the server trails.
- Search newsgroups for posted information from the target.
- Search job databases and newspapers for IT positions within the organization relating to hardware and software.
- Search P2P services for connections into the target network and data concerning the organization.

2. Port Scanning

Port scanning is the invasive probing of system ports on the transport and network level. Included here is also the validation of system reception to tunneled, encapsulated, or routing protocols. This module is to enumerate live or accessible Internet services as well as penetrating the firewall to find additional live systems. The small sample of protocols here is for clarity of definition. Many protocols are not listed here. Testing for different protocols will depend on the system type and services it offers. For a more complete list of protocols, see the Test References section.

Each Internet enabled system has 65,536 TCP and UDP possible ports (incl. Port 0). However, it is not always necessary to test every port for every system. This is left to the discretion of the test team. Port numbers that are important for testing according to the service are listed with the task. Additional port numbers for scanning should be taken from the Consensus Intrusion Database Project Site.

Expected Results:	Open, closed or filtered ports IP addresses of live systems Internal system network addressing List of discovered tunneled and encapsulated protocols List of discovered routing protocols supported Active services Network Map

Tasks to perform for a thorough Port Scan:

Error Checking

- Check the route to the target network for packet loss
- Measure the rate of packet round-trip time
- Measure the rate of packet acceptance and response on the target network
- Measure the amount of packet loss or connection denials at the target network

Enumerate Systems

- Collect broadcast responses from the network
- Probe past the firewall with strategically set packet TTLs (Firewalking) for all IP addresses.
- Use ICMP and reverse name lookups to determine the existence of all the machines in a network.
- Use a TCP source port 80 and ACK on ports 3100-3150, 10001-10050, 33500-33550, and 50 random ports above 35000 for all hosts in the network.
- Use TCP fragments in reverse order with FIN, NULL, and XMAS scans on ports 21, 22, 25, 80, and 443 for all hosts in the network.
- Use a TCP SYN on ports 21, 22, 25, 80, and 443 for all hosts in the network.
- Use DNS connect attempts on all hosts in the network.
- Use FTP and Proxies to bounce scans to the inside of the DMZ for ports 22, 81, 111, 132, 137, and 161 for all hosts on the network.

Enumerating Ports

- Use TCP SYN (Half-Open) scans to enumerate ports as being open, closed, or filtered on the default TCP testing ports in Appendix B for all the hosts in the network.

- Use TCP fragments in reverse order to enumerate ports and services for the subset of ports on the default Packet Fragment testing ports in Appendix B for all hosts in the network.
- Use UDP scans to enumerate ports as being open or closed on the default UDP testing ports in Appendix B if UDP is NOT being filtered already. [Recommended: first test the packet filtering with a very small subset of UDP ports.]

Verifying Various Protocol Response

- Verify and examine the use of traffic and routing protocols.
- Verify and examine the use of non-standard protocols.
- Verify and examine the use of encrypted protocols.

Verifying Packet Level Response

- Identify TCP sequence predictability.
- Identify TCP ISN sequence numbers predictability.
- Identify IPID Sequence Generation predicatbility.
- Identify system up-time.

3. Services Identification

This is the active examination of the application listening behind the service. In certain cases more than one application exists behind a service where one application is the listener and the others are considered components of the listening application. A good example of this is PERL installed for use in a Web application. In that case the listening service is the HTTP daemon and the component is PERL.

Expected Results:	Service Types Service Application Type and Patch Level Network Map

Tasks to perform for a thorough service probe:

- Match each open port to a service and protocol.
- Identify server uptime to latest patch releases.
- Identify the application behind the service and the patch level using banners or fingerprinting.
- Verify the application to the system and the version.
- Locate and identify service remapping or system redirects.
- Identify the components of the listening service.
- Use UDP-based service and trojan requests to all the systems in the network.

4. System Identification

System fingerprinting is the active probing of a system for responses that can distinguish its operating system and version level.

Expected Results:	OS Type Patch Level System Type System enumeration Internal system network addressing

Tasks to perform for a thorough System Identification:

- Examine system responses to determine operating system type and patch level.
- Examine application responses to determine operating system type and patch level.
- Verify the TCP sequence number prediction for each live host on the network.
- Search job postings for server and application information from the target.
- Search tech bulletin boards and newsgroups for server and application information from the target.
- Match information gathered to system responses for more accurate results.

5. Vulnerability Research and Verification

The focus of this module is in the identification, understanding, and verification of weaknesses, misconfigurations and vulnerabilities within a host or network.

Research involved in finding vulnerabilities is necessary up until the delivery of the report. This involves searching online databases and mailing lists specific to the systems and network being tested. Do not confine yourself to the web, consider using IRC, Newsgroups, and underground FTP sites.

Testing for vulnerabilities using automated tools is an efficient way to determine existing holes and system patch level. Although many automated scanners are currently on the market and in the underground, it is important for the tester to identify and incorporate the current underground scripts/exploits into this testing. However, manual verification is necessary for eliminating false positives, expanding the hacking scope, and discovering the data flow in and out of the network. Manual testing refers to a person or persons at the computer using creativity, experience, and ingenuity to test the target network.

Expected Results:	Type of application or service by vulnerability Patch levels of systems and applications List of possible denial of service vulnerabilities List of areas secured by obscurity or visible access List of actual vulnerabilities minus false positives List of Internal or DMZ systems List of mail, server, and other naming conventions Network map

Tasks to perform for thorough Vulnerability Research and Verification:

- Integrate the currently popular scanners, hacking tools, and exploits into the tests.
- Measure the target organization against the currently popular scanning tools.
- Attempt to determine vulnerability by system and application type.
- Attempt to match vulnerabilities to services.
- Attempt to determine application type and service by vulnerability.
- Perform redundant testing with at least 2 automated vulnerability scanners.
- Identify all vulnerabilities according to applications.
- Identify all vulnerabilities according to operating systems.
- Identify all vulnerabilities from similar or like systems that may also affect the target systems.
- Verify all vulnerabilities found during the exploit research phase for false positives and false negatives.
- Verify all positives (be aware of your contract if you are attempting to intrude or might cause a denial of service).

6. Internet Application Testing

An Internet application test employs different software testing techniques to find "security bugs" in server/client applications of the system from the Internet. In this module, we refer the server/client applications to those proprietarily developed by the system owners serving dedicate business purposes and the applications can be developed with any programming languages and technologies. E.g. web application for business transactions is a target in this module. "Black box" and/or "White box" testing can be used in this module.

Expected Results:	List of applications List of application components List of application vulnerabilities List of application system trusts

Tasks to perform for a thorough Internet Application test:

Re-Engineering

- Decompose or deconstruct the binary codes, if accessible.
- Determines the protocol specification of the server/client application.
- Guess program logic from the error/debug messages in the application outputs and program behaviors/performance.

Authentication

- Find possible brute force password guessing access points in the applications.
- Find a valid login credentials with password grinding, if possible.
- Bypass authentication system with spoofed tokens.
- Bypass authentication system with replay authentication information.
- Determine the application logic to maintain the authentication sessions - number of (consecutive) failure logins allowed, login timeout, etc.
- Determine the limitations of access control in the applications - access permissions, login session duration, idle duration.

Session Management

- Determine the session management information - number of concurrent sessions, IP-based authentication, role-based authentication, identity-based authentication, cookie usage, session ID in URL encoding string, session ID in hidden HTML field variables, etc.
- Guess the session ID sequence and format
- Determine the session ID is maintained with IP address information; check if the same session information can be retried and reused in another machine.
- Determine the session management limitations - bandwidth usages, file download/upload limitations, transaction limitations, etc.
- Gather excessive information with direct URL, direct instruction, action sequence jumping and/or pages skipping.
- Gather sensitive information with Man-In-the-Middle attacks.
- Inject excess/bogus information with Session-Hijacking techniques.
- Replay gathered information to fool the applications.

Input Manipulation

- Find the limitations of the defined variables and protocol payload - data length, data type, construct format, etc.
- Use exceptionally long character-strings to find buffer overflows vulnerability in the applications.
- Concatenate commands in the input strings of the applications.
- Inject SQL language in the input strings of database-tired web applications.
- Examine "Cross-Site Scripting" in the web applications of the system.
- Examine unauthorized directory/file access with path/directory traversal in the input strings of the applications.
- Use specific URL-encoded strings and/or Unicode-encoded strings to bypass input validation mechanisms of the applications.
- Execute remote commands through "Server Side Include".
- Manipulate the session/persistent cookies to fool or modify the logic in the server-side web applications.
- Manipulate the (hidden) field variable in the HTML forms to fool or modify the logic in the server-side web applications.
- Manipulate the "Referer", "Host", etc. HTTP Protocol variables to fool or modify the logic in the server-side web applications.
- Use illogical/illegal input to test the application error-handling routines and to find useful debug/error messages from the applications.

Output Manipulation

- Retrieve valuable information stored in the cookies
- Retrieve valuable information from the client application cache.
- Retrieve valuable information stored in the serialized objects.
- Retrieve valuable information stored in the temporary files and objects.

Information Leakage

- Find useful information in hidden field variables of the HTML forms and comments in the HTML documents.
- Examine the information contained in the application banners, usage instructions, welcome messages, farewell messages, application help messages, debug/error messages, etc.

7. Router Testing

The Screening Router is a defence often found on a network that restricts the flow of traffic between the enterprise network and the Internet. It operates on a security policy and uses ACLs (Access Control Lists) to accept or deny packets. This module is designed to assure that only that which should be expressly permitted be allowed into the network; all else should be denied. The screen may also be designed to restrict the outflow of certain types of traffic as well. Routers are becoming more and more complex and some may have features unknown to the tester and often the target organization. The tester's role is in part to determine the role of the router in the DMZ.

Expected Results:	Router type and features implemented Information on the router as a service and a system Outline of the network security policy by the ACL List of the types of packets which may enter the network Map of router responses to various traffic types List of live systems found

Tasks to perform for a thorough router ACL Test:

Router and feature identification

- Verify the router type with information collected from intelligence gathering.
- Verify if the router is providing network address translation (NAT)
- Verify the penetrations from strategically determined packet TTL settings (Firewalking) completed in the Port Scanning module.

Verifying router ACL configuration

- Test the ACL against the written security policy or against the "Deny All" rule.
- Verify that the router is egress filtering local network traffic
- Verify that the router is performing address spoof detection
- Verify the penetrations from inverse scanning completed in the Port Scanning module.
- Test the router outbound capabilities from the inside.
- Measure the ability of the router to handle very small packet fragments
- Measure the ability of the router to handle over-sized packets
- Measure the ability of the router to handle overlapped fragments such as that used in the TEARDROP attack

8. Trusted Systems Testing

The purpose of testing system trusts is to affect the Internet presence by posing as a trusted entity of the network. The testing scenario is often more theory than fact and does more than blur the line between vulnerability testing and Firewall/ACL testing, it is the line.

Expected Results:	Map of systems dependent upon other systems Map of applications with dependencies to other systems Types of vulnerabilities which affect the trusting systems and applications

Tasks to perform for a thorough Trusted Systems test:

- Verify possible relationships determined from intelligence gathering, application testing, and services testing.
- Test the relationships between various systems through spoofing or event triggering.
- Verify which systems can be spoofed.
- Verify which applications can be spoofed.

9. Firewall Testing

The firewall controls the flow of traffic between the enterprise network, the DMZ, and the Internet. It operates on a security policy and uses ACLs (Access Control Lists). This module is designed to assure that only that which should be expressly permitted be allowed into the network, all else should be denied. Additionlly, the tester is to understand the configuration of the firewall and the mapping it provides through to the servers and services behind it.

Reviewing the server logs is needed to verify the tests performed on the Internet presence especially in cases where results of the tests are not immediately visible to the tester. Many unknowns are left to the analyst who has not reviewed the logs.

Expected Results:	Information on the firewall as a service and a system Information on the features implemented on the firewall Outline of the network security policy by the ACL List of the types of packets which may enter the network List of the types of protocols with access inside the network List of live systems found List of packets which entered the network by port number List of protocols which entered the network List of unmonitored paths into the network

Tasks to perform for a thorough router ACL Test:

Firewall and features identification

- Verify the router type with information collected from intelligence gathering.
- Verify if the router is providing network address translation (NAT)
- Verify the penetrations from strategically determined packet TTL settings (Firewalking) completed in the Port Scanning module.

Verifying firewall ACL configuration

- Test the ACL against the written security policy or against the "Deny All" rule.
- Verify that the firewall is egress filtering local network traffic
- Verify that the firewall is performing address spoof detection
- Verify the penetrations from inverse scanning completed in the Port Scanning module.
- Test the firewall outbound capabilities from the inside.
- Determine the success of various packet response fingerprinting methods through the firewall
- Verify the viability of SYN stealth scanning through the firewall for enumeration
- Measure the use of scanning with specific source ports through the firewall for enumeration
- Measure the ability of the firewall to handle overlapped fragments such as that used in the TEARDROP attack
- Measure the ability of the firewall to handle tiny fragmented packets
- Test the firewall’s ability to manage an ongoing series of SYN packets coming in (flooding).
- Test the firewall’s response to packets with the RST flag set.
- Test the firewall’s management of standard UDP packets.

- Verify the firewall's ability to screen enumeration techniques using ACK packets.
- Verify the firewall's ability to screen enumeration techniques using FIN packets.
- Verify the firewall's ability to screen enumeration techniques using NULL packets.
- Verify the firewall's ability to screen enumeration techniques measuring the packet window size (WIN).
- Verify the firewall's ability to screen enumeration techniques using all flags set (XMAS).
- Verify the firewall's ability to screen enumeration techniques using IPIDs.
- Verify the firewall's ability to screen enumeration techniques using encapsulated protocols.
- Measure the robustness of firewall and it's susceptibility to denial of service attacks with sustained TCP connections.
- Measure the robustness of firewall and it's susceptibility to denial of service attacks with temporal TCP connections.
- Measure the robustness of firewall and it's susceptibility to denial of service attacks with streaming UDP.
- Measure the firewall's response to all types of ICMP packets.

Reviewing firewall logs

- Test the firewall logging process.
- Verify TCP and UDP scanning to server logs.
- Verify automated vulnerability scans.
- Verify services' logging deficiencies.

10. Intrusion Detection System Testing

This test is focused on the performance and sensitivity of an IDS. Much of this testing cannot be properly achieved without access to the IDS logs. Some of these tests are also subject to attacker bandwidth, hop distance, and latency that will affect the outcome of these tests. Reviewing the server logs is needed to verify the tests performed on the Internet presence especially in cases where results of the tests are not immediately visible to the tester. Many unknowns are left to the analyst who has not reviewed the logs and alerts.

Expected Results:	Type of IDS Note of IDS performance under heavy load Type of packets dropped or not scanned by the IDS Type of protocols dropped or not scanned by the IDS Note of reaction time and type of the IDS Note of IDS sensitivity Rule map of IDS List of IDS false positives List of IDS missed alarms List of unmonitored paths into the network

Tasks to perform for a thorough IDS Test:

IDS and features identification

- Verify the IDS type with information collected from intelligence gathering.
- Determine its sphere of protection or influence.
- Test the IDS for alarm states.
- Test the signature sensitivity settings over 1 minute, 5 minutes, 60 minutes, and 24 hours.

Testing IDS configuration

- Test the IDS for configured reactions to multiple, varied attacks (flood and swarm).
- Test the IDS for configured reactions to obfuscated URLs and obfuscated exploit payloads.
- Test the IDS for configured reactions to speed adjustments in packet sending.
- Test the IDS for configured reactions to random speed adjustments during an attack.
- Test the IDS for configured reactions to random protocol adjustments during an attack.
- Test the IDS for configured reactions to random source adjustments during an attack.
- Test the IDS for configured reactions to source port adjustments.
- Test the IDS for the ability to handle fragmented packets.
- Test the IDS for the ability to handle specific system method attacks.
- Test the effect and reactions of the IDS against a single IP address versus various addresses.

Reviewing IDS logs and alerts

- Match IDS alerts to vulnerability scans.
- Match IDS alerts to password cracking.
- Match IDS alerts to trusted system tests.

11. Containment Measures Testing

The containment measures dictate the handling of traversable, malicious programs and eggressions. The identification of the security mechanisms and the response policy need to be targetted. It may be necessary to request first a new test mail account or desktop system that the administrator can monitor.

Expected Results:	Define Anti-Trojan Capabilities Define Anti-Virus Capabilities Identify Desktop Containment Measures Identify Desktop Containment Weaknesses List containment resources

Tasks to perform for a thorough CM test:

- Measure the minimum resources that need to be available to this subsystem in order for it to perform its task.
- Verify the resources available to this subsystem that it does not need to perform its tasks, and what resources are shielded from use by this subsystem.
- Verify the detection measures present for the detection of attempted access to the shielded resources.
- Verify unneeded resources
- Verify the features of the containment system.
- Verify detection measures are present for detection of 'unusual' access to the 'needed' resources
    - Measure the response and process against the “sap 27”
    - Measure the configuration of the system.

12. Password Cracking

Password cracking is the process of validating password strength through the use of automated password recovery tools that expose either the application of weak cryptographic algorithms, incorrect implementation of cryptographic algorithms, or weak passwords due to human factors. This module should not be confused with password recovery via sniffing clear text channels, which may be a more simple means of subverting system security, but only due to unencrypted authentication mechanisms, not password weakness itself. [Note: This module could include manual password guessing techniques, which exploits default username and password combinations in applications or operating systems (e.g. Username: System Password: Test), or easy-to-guess passwords resulting from user error (e.g. Username: joe Password: joe). This may be a means of obtaining access to a system initially, perhaps even administrator or root access, but only due to educated guessing. Beyond manual password guessing with simple or default combinations, brute forcing passwords for such applications as Telnet, using scripts or custom programs, is almost not feasible due to prompt timeout values, even with multi-connection (i.e. simulated threading) brute force applications.]

Once gaining administrator or root privileges on a computer system, password cracking may assist in obtaining access to additional systems or applications (thanks to users with matching passwords on multiple systems) and is a valid technique that can be used for system leverage throughout a security test. Thorough or corporate-wide password cracking can also be performed as a simple after-action exercise and may highlight the need for stronger encryption algorithms for key systems storing passwords, as well as highlight a need for enforcing the use of stronger user passwords through stricter policy, automatic generation, or pluggable authentication modules (PAMs).

Expected Results:	Password file cracked or uncracked List of login IDs with user or system passwords List of systems vulnerable to crack attacks List of documents or files vulnerable to crack attacks List of systems with user or system login IDs using the same passwords

Tasks to perform for a thorough Password Cracking verification:

- Obtain the password file from the system that stores usernames and passwords
  - For Unix systems, this will be either /etc/passwd or /etc/shadow
  - For Unix systems that happen to perform SMB authentication, you can find NT passwords in /etc/smbpasswd
  - For NT systems, this will be /winnt/repair/Sam._ (or other, more difficult to obtain variants)
- Run an automated dictionary attack on the password file
- Run a brute force attack on the password file as time and processing cycles allow
- Use obtained passwords or their variations to access additional systems or applications
- Run automated password crackers on encrypted files that are encountered (such as PDFs or Word documents) in an attempt to gather more intelligence and highlight the need for stronger document or file system encryption.

13. Denial of Service Testing

Denial of Service (DoS) is a situation where a circumstance, either intentionally or accidentally, prevents the system from functioning as intended. In certain cases, the system may be functioning exactly as designed however it was never intended to handle the load, scope, or parameters being imposed upon it.

It is very important that DoS testing receives additional support from the organization and is closely monitored. Flood and Distributed (DDoS) attacks are specifically not tested and forbidden to be tested as per this manual. Well resourced floods and DDoS attacks will ALWAYS cause certain problems and often not just to the target but also to all routers and systems between the tester and the target.

Expected Results:	List weak points in the Internet presence including single points of failure Establish a baseline for normal use List system behaviors to heavy use List DoS vulnerable systems

Tasks to perform for a thorough DoS test:

- Verify that administrative accounts and system files and resources are secured properly and all access is granted with "Least Privilege".
- Check the exposure restrictions of systems to non-trusted networks
- Verify that baselines are established for normal system activity
- Verify what procedures are in place to respond to irregular activity.
- Verify the response to SIMULATED negative information (propaganda) attacks.
- Test heavy server and network loads.

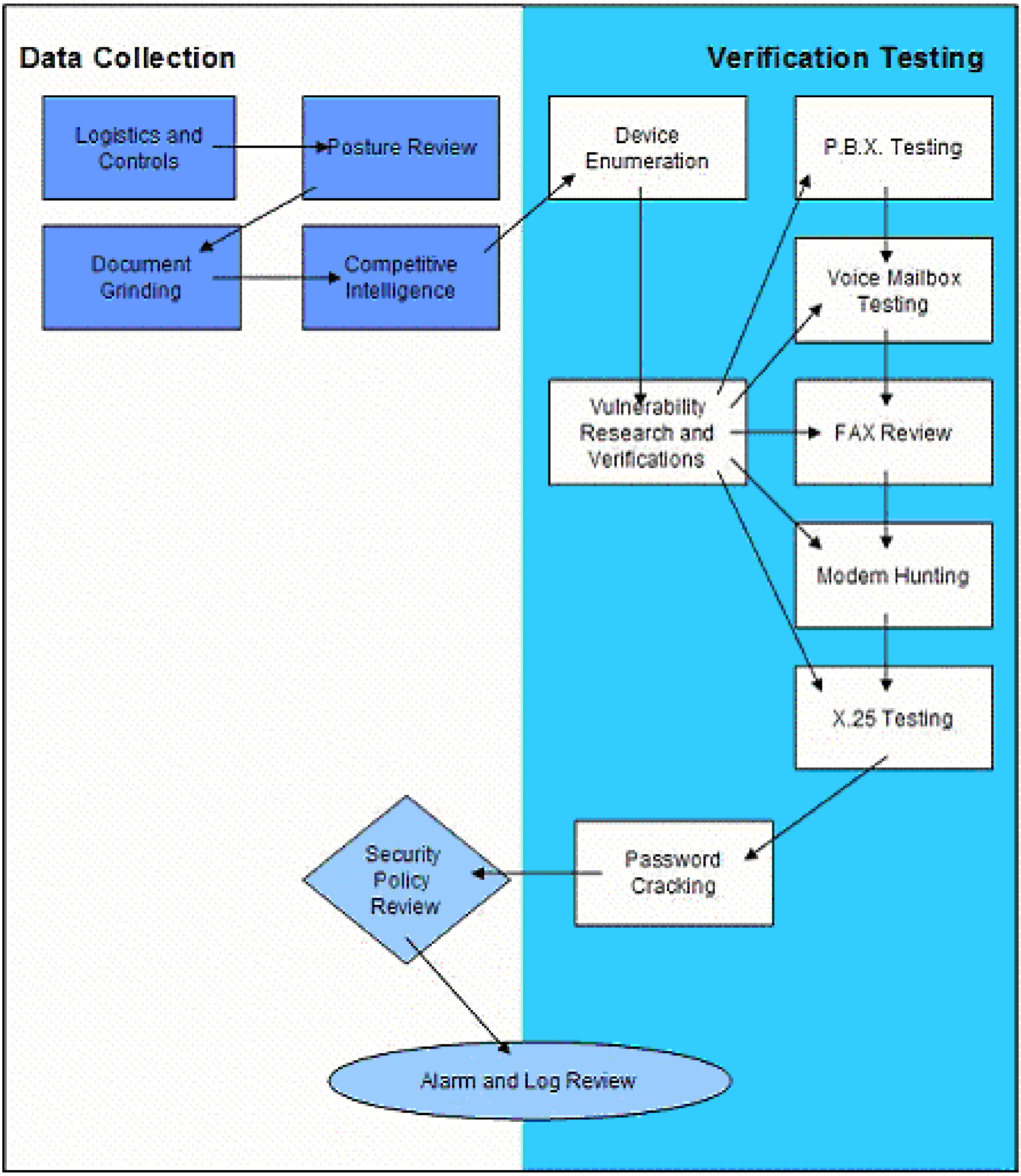
14. Security Policy Review

The security policy noted here is the written human-readable policy document outlining the mitigated risks an organisation will handle with the use of specific types of technologies. This security policy may also be a human readable form of the ACLs. There are two functions to be performed: first, the testing of the written against the actual state of the Internet presence and other non internet related connections; and second, to assure that the policy exists within the business justifications of the organisation, local, federal and international legal statutes, with particular respect to employer's and employee's rights and resposibilities and personal privacy ethics.
These tasks require that the testing and verification of vulnerabilities is completely done and that all other technical reviews have been performed. Unless this is done you can't compare your results with the policy that should be met by measures taken to protect the operating environment.

Tasks to perform for a thorough Security Policy review:

1. Measure the security policy points against the actual state of the Internet presence.
2. *Approval from Management* -- Look for any sign (e.g. signature) that reveals that the policy is approved by management. Without this approval the policy is useless because staff is not required to meet the rules outlined within. From a formal point of view you could stop investigating the policy if it is not approved by management. However, testing should continue to determine how effective the security measures are on the actual state of the internet presence.
3. Ensure that documentation is kept, either electronically or otherwise, that the policy has been read and accepted by people before they are able to gain any access to the computer systems.
4. Identify incident handling procedures, to ensure that breaches are handled by the correct individual(s) and that they are reported in an appropriate manner.
5. *Inbound connections* -- Check out any risks mentioned on behalf of the Internet inbound connections (internet->DMZ, internet -> internal net) and measures which may be required to be implemented to reduce or eliminate those risks. These risks could be allowed on incoming connections, typically SMTP, POP3,HTTP, HTTPS, FTP, VPNs and the corresponding measures as authentication schemes, encryption and ACL. Specifically, rules that deny any stateful access to the internal net are often not met by the implementation.
6. *Outbound connections* -- Outbound connections could be between internal net and DMZ, as well as between internal net and the Internet. Look for any outbound rules that do not correspond to the implementation. Outbound connections could be used to inject malicious code or reveal internal specifics.
7. *Security measures* **--** Rules that require the implementation of security measures should be met. Those could be the use of AVS, IDS, firewalls, DMZs, routers and their proper configuration/implementation according to the outlined risks to be met.
8. Measure the security policy points against the actual state of non-Internet connections.
9. *Modems* -- There should be a rule indicating that the use of modems that are not specially secured is forbidden or at least only allowed if the modems are disconnected when not in use, and configured to disallow dial- in. Check whether a corresponding rule exists and whether the implementation follows the requirements.
10. *Fax machines* -- There should be a rule indicating that the use of fax machines which can allow access from the outside to the memory of the machines is forbidden or at least only allowed if the machines are powered down when not in use. Check whether a corresponding rule exists and whether the implementation follows the requirements.
11. *PBX* -- There should be a rule indicating that the remote administration of the PBX system is forbidden or at least only allowed if the machines are powered down when not in use. Check whether a corresponding rule exists and whether the implementation follows the requirements.
12. Measure the security policy against containment measures and social engineering tests based on the organization's employees' misuse of the Internet according to business justification and best security practices.

Section D – Communications Security



Modules

1. PBX Testing

This is a method of gaining access priviledges to the telephone exchange of a target organization.

Expected Results:	Find PBX Systems that are allowing remote administration List systems allowing world access to the maintenance terminal List all listening and interactive telephony systems.

Tasks to perform for a thorough PBX test:

- Review call detail logs for signs of abuse.
- Ensure administrative accounts don't have default, or easily guessed, passwords.
- Verify that OS is up-to-date and patched.
- Check for remote maintenance access to system.
- Test dial-in authentications.
- Verify remote dial-in authentication.

2. Voicemail Testing

This is a method of gaining access priviledges to the voicemail systems of the target organization and internal personnel.

Expected Results:	List of voice mailboxes that are world accessible List of voicemail dial-in codes and PINs

Tasks to perform for a thorough Voicemail test:

- Verify PIN size and frequency of change
- Identify user and organizational information
- Check for remote maintenance access to system.
- Test dial-in authentications.
- Verify remote dial-in authentication.

3. FAX Review

This is a method of enumerating FAX machines and gaining access priviledges to the systems which may host them.

Expected Results:	List of FAX systems List of FAX systems types and possible operating programs Map of FAX usage protocol within the organization

Tasks to perform for a thorough FAX review:

- Ensure administrative accounts don't have default, or easily guessed, passwords.
- Make sure OS is up to date and patched.
- Check for remote maintenance access to system.
- Test dial-in authentications.
- Verify remote dial-in authentication.

4. Modem Testing

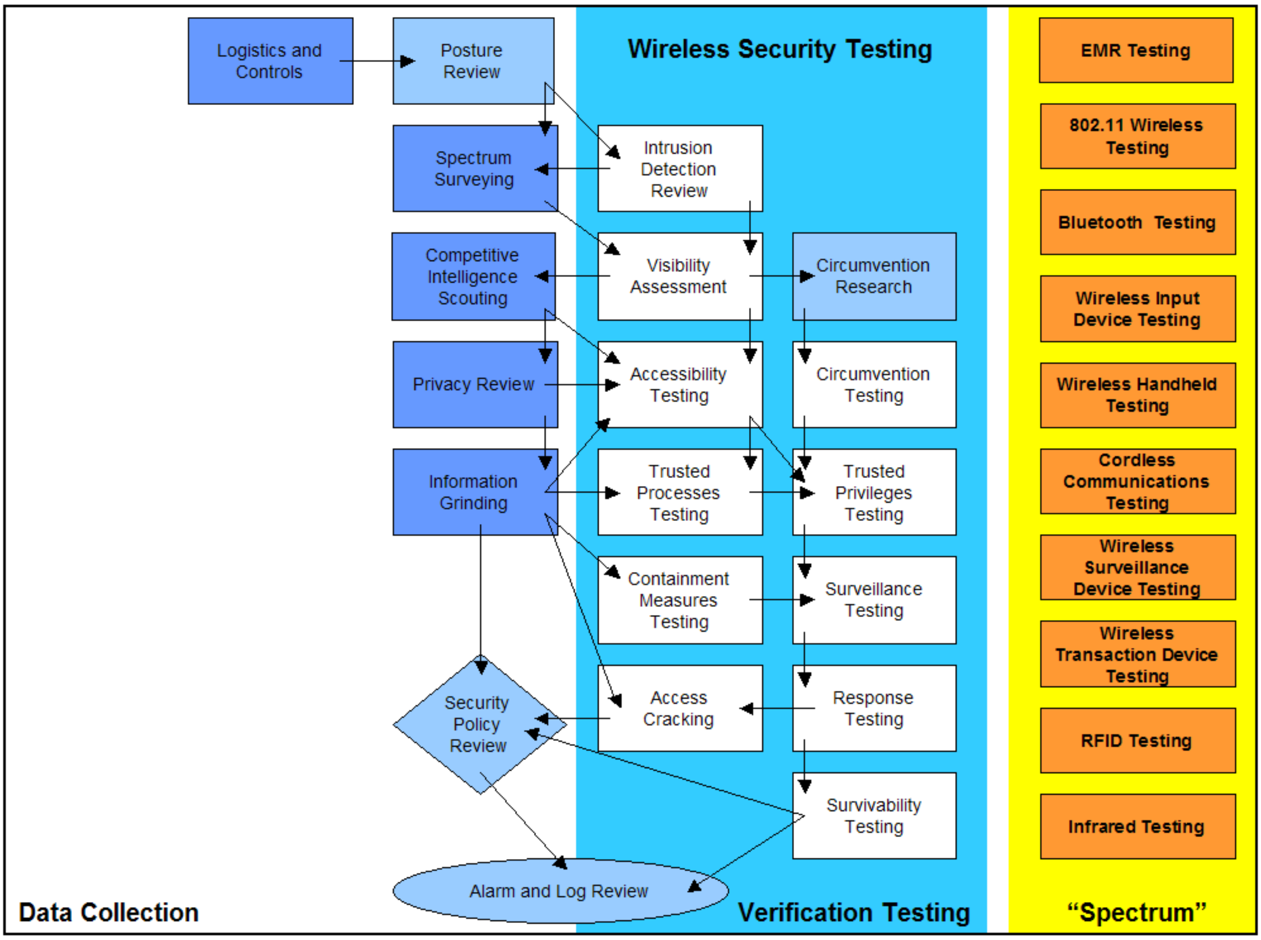
This is a method of enumerating modems and gaining access priviledges to the modem-enabled systems of a target organization.

Expected Results:	List of systems with listening modems List of modem types and operating programs List of modem authentication schemes List of modem logins and passwords Map of modem usage protocol within the organization

Tasks to perform for a thorough Modem test:

- Scan the exchange for modems
- Ensure accounts don't have default, or easily guessed, passwords.
- Make sure OS and modem application is up-to-date and patched.
- Check for remote maintenance access to system.
- Test dial-in authentications.
- Verify remote dial-in authentication.

Section E – Wireless Security



Modules

1. Electromagnetic Radiation (EMR) Testing

This is a method of testing Emissions Security (Emsec), and it pertains to remotely testing the electromagnetic radiation that is emitted from Information Technology devices. Electromagnetic radiation can be captured from devices, such as CRTs, LCDs, printers, modems, cell phones, and so on and used to recreate the data that is displayed on the screen, printed, transmitted… Exploiting this vulnerability is known as Van Eck phreaking.

Equipment for testing or exploiting this vulnerability can prohibitively expensive. However, there are some low cost solutions that incorporate a television receiver, a VCR tuner, synchronization equipment, and other parts. The main cost associated with this form of testing is the time involved. It can require a qualified person to sit for hours trying to find the EMR from the right source. Therefore, this form of testing is usually reserved for highly secure installations where protecting intellectual property is absolutely vital. Additionally, being as it is a given that this data can be obtained from any device that is known to emit EMR, it is best to test for this in implementations that are specifically designed to protect against it.

Protecting against this type of intrusion is usually done by purchasing “Tempest” rated equipment and placing the machines and all peripherals within a shielded room of some sort, such as a Faraday Cage and using only fiber, filtered, or coiled connections to all internal devices between each other and from the outside. Therefore, such protection can be cost prohibitive.

For low budget protection against this type of intrusion, PGP Security has a “Tempest" surveillance prevention option in its secure viewer (used when viewing encrypted text files). This is basically a low-contrast window in which text is viewed. It would probably obfuscate the text if viewed from a van. Also, white noise can be generated to make it much more difficult for intruders to get clean data.

*Note – It is a common myth that CRTs are the biggest culprit in leaking information through EMR. This is not true. They do emit a significant amount of EMR, but it is powerful, nor as easily readable as that emitted by modems and printers. Moreover, to obtain usable data from CRTs, a highly trained individual would have to filter, reassemble, and organize the data. To obtain usable data from a modem or printer, you simply have to intercept it.

Evaluate Business Needs, Practices, Policies and Locations of Sensitive Areas

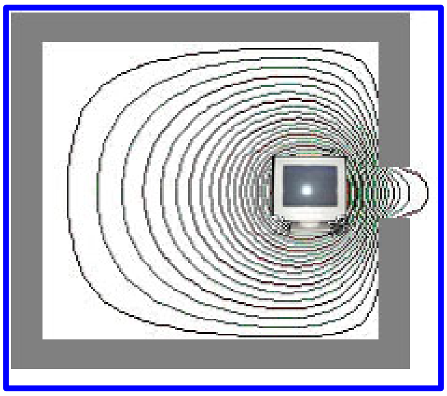
1. Verify that the organization has an adequate security policy in place to address EMR.

Evaluate Hardware and Placement

2. Verify that all Information Technology devices that must be protected are located in a suitable Faraday Cage or metal-shielded room.

Evaluate and Test Wiring and Emissions

3. Verify that all wiring feeds into and out of the shielded room are made of fiber, where possible.



2. [802.11] Wireless Networks Testing

This is a method for testing access to 802.11 WLANs, which are becoming increasingly popular. However, some fairly alarming security problems are common when implementing these technologies. This is mainly because these networks are very quickly and easily thrown together, but security measures are not part of the default setup. There are some basic things that can be done to improve security and some more drastic measures that can be taken to make WLANs fairly secure.

802.11 Specifications:

Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Default encryption	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited Key management.
Operating Range	About 150 feet indoors and 1500 feet outdoors.

Implementations:

802.11a
- Operates in the 5GHz frequency range
- Not compatible with 802.llb or 802.11g hardware
- Maximum speed of 54Mbps

802.11b
- Operates in the 2.4GHz frequency range
- Currently the most widely deployed standard
- Maximum speed of 11Mbps

802.11g
- Operates in the 2.4 GHz frequency range
- Maximum speed of 54Mbps standard
- Expected to be backward compatible with the 802.11b hardware

Evaluate Business Needs, Practices, and Policies:

1. Verify that the organization has an adequate security policy that addresses the use of wireless technology, including the use of 802.11.

Evaluate Hardware, Firmware, and Updates.

2. Perform a complete inventory of all wireless devices on the network.

Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

3. Determine the level of physical access controls to access points and devices controlling them (keyed locks, card badge readers, cameras...).

Evaluate Administrative Access to Wireless Devices:

4. Determine if access points are turned off during portions of the day when they will not be in use.

Evaluate Configuration, Authentication and Encryption of Wireless Networks:

5. Verify that the access point’s default Service Set Identifier (SSID) has been changed.

Evaluate Wireless Clients:

6. Verify that all wireless clients have antivirus software installed.

3. Bluetooth Network Testing

This is a method for testing Bluetooth ad-hoc networks (piconets), which are popular for small, low bandwidth intensive wireless personal area networks (PANs). As with other wireless methods, there are inherent vulnerabilities that pose significant security problems.

Bluetooth Specifications:

Physical Layer	Frequency Hopping Spread Spectrum (FHSS)
Frequency Band	2.4 – 2.45 GHz (ISM band)
Hop Frequency	1,600 hops per second
Raw Data Rate	1Mbps
Throughput	Up to 720 Kbps
Data and Network Security	• Three modes of security (none, link-level, and service-level) • Two levels of device trust and three levels of service security. • Stream encryption algorithm for confidentiality and authentication. • PIN derived keys and limited key management.
Operating Range	About 10 meters (30 feet); can be extended to 100 meters (328 feet).

Evaluate Business Needs, Practices, and Policies:

1. Verify that there is an organizational security policy that addresses the use of wireless technology, including Bluetooth technology.

Evaluate Hardware, Firmware, and Updates.

2. Perform a complete inventory of all Bluetooth enabled wireless devices.

Test for Common Vulnerabilities (especially in the Red-M 1050AP):

3. Perform brute force attack against Bluetooth access point to discern the strength of password. Verify that passwords contain numbers and special characters. Bluetooth Access Points use case insensitive passwords, which makes it easier for attackers to conduct a brute force guessing attack due to the smaller space of possible passwords.

Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

4. Verify the actual perimeter of the Bluetooth network.

Evaluate Device Configuration (Authentication, Passwords, Encryption...):

5. Verify that Bluetooth devices are set to the lowest possible power setting to maintain sufficient operation that will keep transmissions within the secure boundaries of the organization.

4. Wireless Input Device Testing

This section deals with wireless input devices, such as mice and keyboards. These devices are becoming very popular, but present profound vulnerabilities and compromises in privacy and security.

Evaluate Business Needs, Practices, and Policies:

1. Analyze organizational security policy that addresses the use of wireless technology, such as wireless input devices.

Evaluate Hardware, Firmware, and Updates:

2. Perform a complete inventory of all wireless input devices on the network.

Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

3. Perform a site survey to measure and establish the service range of the wireless input devices for the organization.

5. Wireless Handheld Security Testing

Due to the incredible variety and ubiquity of handheld wireless devices, it is nearly impossible to address each type. This section is intended to incorporate all wireless devices in aggregate. There are basic measures that should be taken and tested across all wireless devices. The following steps provide a method of testing for security on all devices.

The most significant aspect in testing these devices lies not in the actual configuration of the device, but in the education of the user. Most of these steps test user knowledge regarding the most secure use of the device.

Evaluate Business Needs, Practices, and Policies:

1. Verify that there is an organizational security policy that addresses the use of all handheld devices.

Evaluate Hardware, Firmware, and Updates:

2. Perform a complete inventory of all wireless devices on the network.

Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

3. Verify that there is external boundary protection around the perimeter of the buildings, or wireless networks.

Evaluate Device Configuration (Authentication, Passwords, Encryption...):

4. Verify that the devices use robust encryption to protect sensitive files and applications.

6. Cordless Communications Testing

This is a method of testing cordless communications communication devices which may exceed the physical and monitored boundaries of an organization. This includes testing for interference between similar or differing wireless communication types within the organization and with neighboring organizations.

Evaluate Business Needs, Practices, and Policies:

1. Verify that the organization has an adequate security policy that addresses the use of cordless communication technology.

Evaluate Hardware, Firmware, and Configuration:

2. Perform an inventory of all cordless communication devices.

Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

3. Verify the distance in which the cordless communication extends beyond the physical boundaries of the organization.

7. Wireless Surveillance Device Testing

This section pertains to the wireless surveillance devices that have recently begun to replace wired surveillance devices – such as cameras, microphones, etc. These devices enable companies to install monitoring equipment in areas where it was previously not feasible and at a lower cost. This monitoring equipment is often completely hidden, either by its very small size or by being disguised in another object, like a fire alarm, picture, or clock. Being as most of this equipment is wireless, it is more susceptible to interference, jamming, monitoring, and playback than its wired counterpart. Also, the security tester may be the last line of defense to ensure that this equipment is installed and operated appropriately.

Evaluate Business Needs, Practices, and Policies:

1. Verify that there is a company policy that effectively addresses wireless surveillance equipment.

Evaluate Devices and Placement:

2. Verify that the surveillance equipment is truly disguised or not visible, if that is the intent of the equipment.

Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

3. Verify the actual perimeter of the wireless surveillance device transmissions.

8. Wireless Transaction Device Testing

This section covers the wireless transaction devices that are in place in many stores. This equipment is currently being used to provide uplinks for cash registers and other point of sale devices, throughout the retail industries. This technology has proven to be a tremendous benefit and business enabler to companies, but is sometimes installed without thought to security and protection of confidential information.

Evaluate Business Needs, Practices, and Policies:

1. Verify that there is a company policy that effectively addresses wireless transaction equipment.

Evaluate Hardware, Firmware, and Updates:

2. Perform a full inventory of all wireless transaction devices.

Evaluate Device Configuration:

3. Verify that that the data being sent is encrypted and the level of encryption being used.

Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

4. Determine the ability of unintended third to intercept transmitted data.

9. RFID Testing

RFID (Radio Frequency Identifier) tags are composed of an integrated circuit (IC), which is sometimes half the size of a grain of sand, and an antenna – usually a coil of wires. Information is stored on the IC and transmitted via the antenna. RFID tags can either be passive (no battery, it uses energy from tag-reader's RF transmission) or active (self-powered by battery). The data transmission speed and range depends on power output, antenna size, receiver sensitivity, frequency, and interference. TFID tags can be read-only, read-write, or a combination of the two, where some data is read-only (such as the serial number) and other data is changeable for later encoding or updates.

Additionally, RFID tags do not require line of sight to be read and can function under a variety of environmental conditions – some tags are water resistant and washable. Each tag contains a 64 bit unique identifier and varying amounts of memory – many have 1024 bits. Therefore, they provide a high level of functionality and data integrity.

Some tags provide security measures. Most tags that use encryption have a 40-bit hidden encryption key. Some RFID transponders integrate a digital signature encryption protocol that includes a challenge/response authentication. Depending on the design of the RFID tag and the transponder, the authentication can be either one sided or two sided.

The exact frequencies used in RFID systems may therefore vary by country or region, however, RFID systems typically utilize the following frequency ranges:

- Low frequency: 30 to 300 kHz frequency range, primarily the 125 kHz band;
- High frequency: 13.56 MHz frequency range;
- Hltra-high frequency (UHF): 300 MHz to 1 GHz frequency range; and
- Microwave frequency: frequency range above 1 GHz, primarily the 2.45 GHz and 5.8 GHz
- bands.

RFID tags are absolutely invaluable to logistics, but feared and doubted by privacy advocates, because of the quality and quantity of information that they provide. Therefore, steps need to be taken to ensure that full logistics needs are not impaired, while privacy constraints are not trampled upon.

There is impending legislation that could affect the way companies use RFID tags, and it is best to take a proactive, forward-thinking approach for best practices. To do this, verify that RFID tags can be read at every step along the logistics path, but are deactivated at their final destination (such as point-of-sale) and that they cannot be reactivated by any means. Deactivation at the final destination helps protect against future legislation, as well as against malicious intent.

However, it also needs to be ensured that RFID tags cannot be deactivated by those attempting to steal the items. Therefore, RFID tag deactivation should only be performed at cash registers or at other specific places to meet business needs.

Evaluate Business Needs, Practices, and Policies:

1. Verify that the organization has an adequate security policy that addresses the use of wireless RFIDs.

Evaluate RFID Attributes (Authentication, Encryption, Properties…):

2. Verify that serial number on ID tag cannot be changed.

Evaluate Placement, Scanners, and Tracking Equipment:

3. For complete tracking of tagged products in a warehouse or other storage environment, ensure that RFID tag readers are in place at all entrances and exits, not just at main freight arrival and departure locations. This will help to reduce shrinkage caused by employee theft.

Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

4. Verify that RFID tag and reader transmissions do not interfere with wireless networks and communications equipment.

10. Infrared Systems Testing

This is a method of testing infrared communications communication devices which may exceed the physical and monitored boundaries of an organization.
Infrared communication is much less accessible from the outside an organization, compared to 802.11 or Bluetooth. However, security on infrared devices tends to be frequently overlooked, due to its relative inaccessibility.

Evaluate Business Needs, Practices, Policies and Locations of Sensitive Areas:

1. Verify that the organization has an adequate security policy that addresses the use of wireless technology, such as infrared devices.

Evaluate Hardware, Firmware, and Updates:

2. Perform a complete audit of all infrared enabled devices.

Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

3. Verify the distance that the infrared communication extends beyond the physical boundaries of the organization.

Evaluate Device Configuration (Authentication, Passwords, Encryption..):

4. Verify authentication-method of the clients.

11. Privacy Review

The privacy of wireless communication devices may exceed the physical and monitored boundaries of an organization. The privacy review is the focal point of the legal and ethical storage, transmission, and control of data based on employee and customer privacy. The use of this data is a concern to many private persons and legislation is unveiling specific rules regarding privacy. Although some of these laws are local, all of them apply to the Internet and therefore affect security testers internationally.

Expected Results:	List any disclosures List compliance failures between public policy and actual practice List wireless communication involved in data gathering List data gathering techniques List data gathered

1. Verify authentication-method of the clients
2. Verify that appropriately strong passwords are in use
3. Verify that that there is a password expiration policy
4. Verify that encryption is used and properly configured
5. Verify that clients can't be forced to fall-back to none-encrypted mode
6. Compare publicly accessible policy to actual practice
7. Compare actual practice to regional fraud and privacy laws or compliancy
8. Identify database type and size for storing data
9. Identify data collected by the organization
10. Identify storage location of data
11. Identify data expiration times

Section F – Physical Security

Modules

1. Perimeter Review

This is a method of testing the physical security of an organization and its assets by reviewing is its physical perimeter security measures.

Expected Results:	Map of physical perimeter Types of physical protective measures List of unprotected / weakly protected areas

Tasks to perform for a thorough Perimiter review:

- Map physical perimeter
- Map physical protective measures (fences, gates, lights, etc)
- Map physical access routes / methods
- Map unmonitored areas

2. Monitoring Review

This is a method of discovering monitored access points to an organization and its assets through discovery of guard and electronic monitoring.

Expected Results:	List of monitored access points Types of monitoring List of unmonitored standard and priviledged access points List of alarm triggers

Tasks to perform for a thorough Monitoring review:

- Enumerate monitoring devices
- Map guarded locations and routes traveled
- Map unmonitored areas to monitored areas
- Test monitoring devices for limitations and weaknesses
- Test monitoring devices for denial of service attacks

3. Access Controls Testing

This is a method of testing access priviledges to an organization and its assets through physical access points.

Expected Results:	List of physical access points Types of authentication Types of alarm systems List of alarm triggers

Tasks to perform for a thorough Access Controls test::

- Enumerate access control areas
- Examine access control devices and types
- Examine alarm types
- Determine the level of complexity in an access control device
- Determine the level of privacy in an access control device
- Test access control devices for vulnerabilites and weakneses
- Test access control devices against Denial of Service

4. Alarm Response Review

This is a method of discovering alarm procedure and equipment in an organization through discovery of guard and electronic monitoring.

Expected Results:	List of alarm types List of alarm triggers Map of alarm procedure List of persons involved in alarm procedure List of containment measures and safety precautions triggered by alarm

Tasks to perform for a thorough Alarm Response review:

- Enumerate alarm devices
- Map alarm trigger procedures
- Map alarm activated security reflexes
- Discover persons involved in an alarm procedure
- Test alarm escalation
- Test alarm enablement and disablement
- Test alarm devices for limitations and weaknesses
- Test alarm devices for denial of service attacks
- Test alarm procedures for Denial of Service attacks

5. Location Review

This is a method of gaining access to an organization or its assets through weaknesses in its location and protection from outside elements.

Expected Results:	Map of physical locations of assets List of physical location access points List of vulnerable access points in location List of external 3rd parties accessing locations

Tasks to perform for a thorough Location review:

- Enumerate visible areas into the organization (line of sight)
- Enumerate audible areas into the organization (laser or electronic ear)
- Test location areas for vulnerabilities and weaknesses to supply delivery
- List supply delivery persons and organizations
- List cleaning staff and organisations
- List hours and days in delivery cycles
- List hours and days in visitor cycles

6. Environment Review

This is a method of gaining access to or harming an organization or its assets through weaknesses in its environment.

Expected Results:	Map of physical locations of assets List of vulnerable locations List of local laws, customs, and ethics List of operational laws, customs, and ethics

Tasks to perform for a thorough Environment review:

- Examine natural disaster conditions for the region
- Examine political environmental conditions
- Examine back-up and recovery procedures
- Identify weaknesses and vulnerabilities in back-up and recovery procedures
- Identify Denial of Service attacks in back-up and recovery procedures
- Examine physical and electronic handicaps in various weather patterns
- Compare operational procedures with regional laws, customs, and ethics

Report Requirements Templates

The following templates are an small example of the report requirements as per what should be displayed in a report to qualify for a certified OSSTMM compliancy stamp. Restrictions of applicability and scope apply.

Network Profile Template

IP ranges to be tested and details of these ranges

Domain information and configurations

Zone Transfer Highlights

SERVER LIST

IP Address	Domain Name(s)	Operating System

Server Information Template

IP Address	domain name

Port	Protocol	Service	Service Details

BANNER(S):

Port	Protocol	Banner

TCP SEQUENCING:

TCP Sequence Prediction
TCP ISN Seq. Numbers
IPID Sequence Generation
Uptime

CONCERNS AND VULNERABILITIES:

Concern or Vulnerability
Example
Solution

Firewall Analysis Template

fingerprinting

This test is to determine the success of various packet response fingerprinting methods through the firewall.

Method	Result

stealth

This determines the viability of SYN stealth scanning through the firewall for enumeration.

Result

source port control

This test measures the use of scanning with specific source ports through the firewall for enumeration.

Protocol	Source	Result
UDP	53	
UDP	161	
TCP	53	
TCP	69	

overlap

This test measures the ability of the firewall to handle overlapped fragments such as that used in the TEARDROP attack.

Protocol	Result

fragments

This test measures the ability of the firewall to handle tiny fragmented packets.

IP	Result

syn flood

This tests the firewall's ability to manage an ongoing series of SYN packets coming in.

IP	Result

rst flag

This test exacts the firewall's response to packets with the RST flag set.

IP	Result

udp

This tests the firewall's management of standard UDP packets.

IP	Result

ack

This test is to discover the firewall's ability to screen enumeration techniques using ACK packets.

IP	Result

fin

This test is to discover the firewall's ability to screen enumeration techniques using FIN packets.

IP	Result

null

This test is to discover the firewall's ability to screen enumeration techniques using NULL packets.

IP	Result

win

This test is to discover the firewall's ability to screen enumeration techniques using WIN packets.

IP	Result

xmas

This test is to discover the firewall's ability to screen enumeration techniques using packets with all flags set.

IP	Result

Advanced Firewall Testing Template

Sustained TCP Connections

This test is to measure the robustness of firewall and it's susceptibility to denial of service attacks.

connection	description	max connects	max idle time

Fleeting TCP Connections

This test is to measure the robustness of firewall and it's susceptibility to denial of service attacks.

connection	description	max connects	max idle time

Streaming UDP Throughput

This test is to measure the robustness of firewall and it's susceptibility to denial of service attacks.

connection	description	max connects

ICMP Responses

This test is to measure the firewall's response to various types of ICMP packets.

type	type description	response	RTT

Spoof Responses

This test is to measure the firewall's Access Control List rules by IP address.

connection	response description	from	to

Protocol

This test is to discover the firewall's ability to screen packets of various protocols.

Protocol	Result

IDS Test Template

IDS type

This test is to determine the IDS type and sphere of protection or influence.

IDS type	protection range by IP

Flood Attack

This test is to measure the IDS´s response capabilities in the event of many attacks of various priorities coming through at once.

flood type	description of attack	duration	result

Obfuscated URLs

This test addresses the IDS's ability to address disguised URLs for attacking webservers.

encoding type	URL sent	result

Speed Adjustments

This test measures the IDS's sensitivity to scans over definitive time periods.

	packet description	delay	result
1 minute			
5 minutes			
60 minutes			
24 hours			

Behavior Attacks

This test measures the IDS's sensitivity to many scans of a random nature.

	description	result
random speed attack		
random protocol attack		
random source attack		

Method Matching

This test measures the IDS's sensitivity to webserver scans of unknown methods.

	result
HEAD	

POST	
PUT	
DELETE	
PATCH	
PROPFIND	
PROPPATCH	
MKCOL	
COPY	
MOVE	
LOCK	
UNLOCK	

Source Port Control

This test measures the use of scanning with specific source ports through the IDS without alarm.

Protocol	Source	Result
UDP	53	
UDP	161	
TCP	443	
TCP	22	

Spoof Responses

This test is to measure the firewall's Access Control List rules by IP address.

connection	response description	from	to

Fragments

This test measures the ability of the IDS to handle tiny fragmented packets.

Result

Social Engineering Target Template

Target Definition

Name	E-mail	Telephone	Description

Social Engineering Telephone Attack Template

Attack Scenario	
Telephone #	
Person	
Description	
Results	

Attack Scenario	
Telephone #	
Person	
Description	
Results	

Social Engineering E-mail Attack Template

Attack Scenario	
Email	
Person	
Description	
Results	

Attack Scenario	
Email	
Person	
Description	
Results	

Trust Analysis Template

IP Address	Domain Name
Description of Trust	

IP Address	Domain Name
Description of Trust	

IP Address	Domain Name
Description of Trust	

Privacy Review Template

IP Address	Domain Name
Privacy Policy	
Privacy Violations	

IP Address	Domain Name
Privacy Policy	
Privacy Violations	

Containment Measures Review Template

IP Address	Domain Name
Server Anti-virus / Anti-trojan Mechanisms	
Server Response to “SAP 27” and 42.zip	

Desktop Anti-virus / Anti-trojan Mechanisms

Desktop Mail Client Types
Desktop Mail Client Vulnerabilities

Desktop Browser Client Types
Desktop Browser Client Vulnerabilities

E-Mail Spoofing Template

Attempts

Internal Connect

Show the results of a telnet to the mail server and sending a mail from one internal address to another internal address.

Egression

Show the results of sending a mail from one internal address to another internal address using an external, third-party pop server.

External Relaying

Show the results of sending a mail from one external address to another external address using the target mail server.

Internal Relaying

Show the results of sending a mail from one internal address to an external address using the target mail server.

Competitive Intelligence Template

IP Address	
Domain Names	
Similar Domain Names	
Total Content Size	
Number of Documents	
Number of Products	
Product List	
Number of Services	
Services List	
Method of Sales	
Restricted Areas	

Password Cracking Template

Protected File

File name	
File type	
Crack time	
User name	
Password	

Encoded Password File

IP Address	
Service Port	
Service Type	
Protocol	
File name	
File type	
Crack time	
Login Names	
Passwords	

Protected Online Service

IP Address	
Service Port	
Service Type	
Protocol	
Login Names	
Passwords	

Denial of Service Template

System Testing

IP Address	
Service Port	
Service Type	
Protocol	
Test Description	
Test Response	

IP Address	
Service Port	
Service Type	
Protocol	
Test Description	
Test Response	

Process Testing

Process	
Persons	
Location	
Time / Date	
Test Description	
Test Response	

Process	
Persons	
Location	
Time / Date	
Test Description	
Test Response	

Document Grinding Template

Primary Contacts	
Method of Contact	

Organizational Information	
Business Name	
Business Address	
Business Telephone	
Business Fax	
Hierarchy Model	
Office Hierarchy	
Line of Business	
Operations	
Legal Structure	
Year Started	
Company History	
Departments and Responsibilities	
Telecommunications Information	
Noted Business Phone Numbers	

Phone Number Block	
Phone Number Type	
Number of Modems	
Modem Phone Numbers	
Modem Connect Speeds	
Number of Fax Machines	
Fax Phone Numbers	
Unusual Phone Numbers	

Employee Data	
Employee Names and Positions	
Employee Personal Pages	
Employee Information	

Outsourcers	
Web Designers	
Email	
Tech Support	

Firewall	
Intrusion Detection System	

Help Desk	
Partners	
Resellers	
Internet Service Providers	
Application Service Providers	

IP Information	
Domain Names	
Network Blocks	
Network Block Owner	
Records Created	
Records Last Updated	

Internal Network Information	
Number of Network Accounts	
Network Account Standard	
Network Account Creation Standard	
Web Clients Used	

Screen Size	
Security Settings in Browser	

Number of Systems	
System Names Standard	
System Names	
Types of Systems	
Operating Systems	
Services provided	

Email Information	
Email Server Address	
Email Server Type	
Email Clients	
Email System	
Email Address Standard	
E-mail Footer	
Encryption / Standard	
Bounced mails	
SMTP server path	
Automatic Vacation Returns	
Mailing Lists	

Web Information	
Website Address	
Web Server Type	
Server Locations	
Dates Listed	
Date Last Modified	
Web Links Internal	
Web Site Searchability	
Web Links External	
Web Server Directory Tree	
Technologies Used	
Encryption standards	
Web-Enabled Languages	
Form Fields	
Form Variables	
Method of Form Postings	
Keywords Used	

Company contactability	
Meta Tags	
Comments Noted	
e-commerce Capabilities	
Services Offered on Net	
Products Offered on Net	
Features	
Search Engines Identified	
Search Engine Ranking	
Daily/Weekly/Monthly Hits	
Link Popularity	
Link Culture	

File Management Information	
FTP Server Address	
SMB Server Address	
Server Location	
Server Type	
Directory Tree	

Files Sitting	

Name Services	
Primary (Authoritative) Name Server	
Secondary	
Last Update	
Additional Name Servers	

Firewall Information	
Firewall Address	
Firewall Type	
IDS system	

Routing Information	
Router Addresses	
Router Types	
Router Capabilities	

Virtual Private Network Information	
VPN Capabilities	
VPN Type	

Network Services	
Network Services Noted	

Internet Presence Information	
Newsgroup Postings	

Bulletin Board Postings	
Business Wire Postings	
Help Wanted Ads	
P2P Files	
Cracks Found	
Serial Numbers Found	

Competitive Intelligence	
Customer List	
Target Market	
Product List	

Social Engineering Template

Company	
Company Name	
Company Address	
Company Telephone	
Company Fax	
Company Webpage	
Products and Services	
Primary Contacts	
Departments and Responsibilities	
Company Facilities Location	
Company History	
Partners	
Resellers	
Company Regulations	
Company Infosecurity Policy	
Company Traditions	
Company Job Postings	
Temporary Employment Availability	
Typical IT threats	

People	
Employee Information	
Employee Names and Positions	
Employee Place in Hierarchy	
Employee Personal Pages	
Employee Best Contact Methods	
Employee Hobbies	
Employee Internet Traces (Usenet, forums)	
Employee Opinions Expressed	
Employee Friends and Relatives	
Employee History (including Work History)	
Employee Character Traits	
Employee Values and Priorities	
Employee Social Habits	
Employee Speech and Speaking Patterns	
Employee Gestures and Manners	

Equipment	
Equipment Used	
Servers, Number and Type	
Workstations, Number and Type	
Software used (with versions)	
Hostnames Used	
Network Topology	
Anti-virus Capabilities	
Network Protection Facilities Used (with software versions)	
Remote Access Facilities Used (including Dial-up)	
Routers Used (with software versions)	
Physical Access Control Technology Used	
Location of Trash Disposal Facilities	

Legal Penetration Testing Checklist

FEATURES TO CONSIDER	APPLICABLE LAW
PRIVACY AND PROTECTION OF INFORMATION	
Obtaining and Using Personal Information. • Personal information about living people should only be obtained and used if is necessary for the purposes of a security test and it is legally permissible. • Certain conditions may need to be satisfied where personal information is obtained and used; these conditions will vary from country to country and could include: - obtaining the consent from the individual whose information is being obtained and used; - or the information is necessary for the prevention and detection of a crime.	International variations exist in relation to obtaining and processing personal data. There is a level of consistency between countries from the European Community, who have implemented Directive 95/46/EC of the European Parliament and of the Council on the protection of personal data with regard to the processing of personal data and of the free movement of such data (OJ [1995] L281/31). The UK's Data Protection Act 1998, which was partly based upon the Directive 95/46/EC expressly requires that personal data shall only be obtained and processed fairly and lawfully. A range of conditions need to be satisfied to demonstrate compliance with the Data Protection Act.
Copying, Storing, Retention and Destruction of Information. • Information belonging to others should only be copied and retained by the Security Testers where it is relevant and necessary for analysis and reporting purposes; unless such activities are expressly prohibited by the contract or by law. • Information belonging to others should only be kept for as long as is necessary for the purposes of testing and reporting. • Information that was legally obtained and deemed necessary for the purposes of the test should be destroyed in an appropriate manner when it is no longer required.	The legal requirements for handling information vary from country to country. Consistency exists between countries from the European Community who are subject to Directive 95/46/EC. - The UK's Data Protection Act 1998, which was partly based upon the Directive 95/46/EC expressly requires that personal data should not be kept for longer than is necessary and that adequate and appropriate security measures should be used to protect personal information. - Where a US company wishes to share personal information with a company subject to Directive 95/46/EC, the US company must adhere to the safe harbor requirements.
Disclosure of Information. • Information should not be disclosed to unauthorised individuals.	There are various rules that exist to protect information from unauthorised disclosed. These rules may be necessary to protect commercial confidentiality or an individual's privacy.

• The Security Tester should ensure that an individual's privacy rights are respected, where necessary. • A Security Tester must not act in any manner which could result in a breach of confidentiality or contravention of any law or contract.	- The European Community countries have adopted the European Convention of Human Rights in to their national laws. - The UK's Human Rights Act 1998 incorporates the Convention right of privacy, article 8. The Data Protection Act 1998 requires that a minimum level of protection is used. - The United Nations Declaration of Human Rights at article 12, states that every individual has a right to privacy.

INFORMATION AND SYSTEM INTEGRITY	
Unauthorised interference with information systems. • Security Testers must not intentionally cause interference to the operation of their customer's information system, unless they are permitted by law or their customer. • Written consent may be required from the customer prior to performance of the Security Test.	Interference with information systems may be governed by a range of different laws internationally. Although it is a feature that may be incorporated as a contractual term. In the UK it is necessary to closely scrutinise the act of the perpetrator, who may be punished under range of legislation such as the Computer Misuse Act, the Theft Act or the Criminal Damages Act.
Damage and Modification of information or information systems • Security Testers should take care not to alter or damage any information or information systems during testing; except where permissible by law or the contracting party.	The alteration, modification or damage of information by the Security Testers may be a either a criminal or civil offence or both depending on the country. - In the UK, it is governed by the Computer Misuse Act and the Criminal Damages Act.
Unauthorised use of information or information systems. • There should be no unauthorised use of information or systems; except where permissible by law.	Information and the information systems may need to be protected from others for a wide range of reasons; such as maintaining client confidentiality or protecting companies research and development.

COMMUNICATION AND AUTHORISATION	

Notification of intention and actions. • Appropriate notices should be provided to the customer and any others with a legal right to know about the impact of a Security Test; • The Security Testers must provide the customer with the necessary detail of the actions that will be taken as part of the Test; • If any hackers are discovered on the customer's system during the Security Test, then the Testers should inform the customer as soon as it is possible. • All parties that may be effected by the Internet Security Test have been informed of the nature of the Test where legally necessary.	It may be a legal requirement in some countries to receive notification of intentions and actions in relation to the Security Test. In the UK Security Testers may be liable for a variety of reasons if they fail to provide the appropriate notifications. They could breach a contractual requirement, be deemed negligent or infringe legislation such as the Computer Misuse Act 1990.
Notification of Responsibilities • The Security Testers should ensure that their customers are aware of their responsibilities, which include: - taking back ups of information prior to the test; - and informing employees who need to know, for legal or operational purposes.	This is a general due diligence requirement, which may apply internationally.
Authorisation • Written permission may be necessary from the customer before the Security Test is undertaken; • Consent may be required from individuals or organisations other than the customer before the Security Test is performed;	Conducting a Security Test written the appropriate authorisation could be a criminal or civil offence depending on the country or countries of the test. - it is the Computer Misuse Act 1990 in the UK which makes it an offence to access a system without authority.
Suspension of the Security Test • If an intruder is discovered on the customer's information system during the Security Test, then the test should be suspended and the incident reported to the customer. Following suspension, the Security Test should	Any Security Tester needs to act with caution otherwise they could be liable for a range of misdemeanours. In particular care needs to be exercised when intruders are discovered as the Security Tester does not want to be blamed for the actions of the intruder.

only be re-commenced with the agreement of the customer.	

CONTRACT	
Contract formation and terms and conditions • Ensure that contracts are formed in compliance with the law; • The terms and conditions for the provision of Security Testing should be sufficiently detailed to reflect the rights and responsibilities of the tester and customer.	The use of contracts is an internationally accepted practice. There are differences between countries with contract law and these should be addressed if contracting with organisations from other countries. - In the UK guidance on contractual formation can be taken from legislation such as the Supply of Goods and Services Act 1982. This Act provides for the existence of implied terms in contracts such as the implied term that a service will be carried out with reasonable care and skill.
Liability • Ensure appropriate and legally acceptable clauses limiting liability exist in a contract. - For example a clause should exist that states that the Security Tester will not accept responsibility or liability for any damage or loss incurred as a result of the customer's failure to implement the appropriate safeguards to protect the information systems or any connected part of it.	There are international variations with the content of liability clauses. - With issues of liability the UK is subject to legislation such as the Unfair Contract Terms Act 1977.
Contents • It may be necessary to ensure that specific information necessary for the test is included with any contractual documents such as: - a list of all the assigned IP addresses which must be expressed as an individual IP address and as a range.	Providing details of the scope and parameters of the Security Test protects the customer and the Tester.

Test References

The following are key references for use with this manual in testing.

sap 27

The sap or "sucker" 27 are various extensions which are used in the wild for attempting to move trojaned code in through e-mail systems and browsers.

EXT.	DESCRIPTION
.ade	Microsoft Access Project extension
.adp	Microsoft Access Project
.bat	Batch file
.chm	Compiled HTML Help file
.cmd	Microsoft Windows NT Command script
.com	Microsoft MS-DOS program
.cpl	Control Panel extension
.crt	Security Certificate
.eml	Outlook Express Mail
.exe	Program
.hlp	Help file
.hta	HTML program
.inf	Setup Information
.ins	Internet Naming Service
.jpg	JPEG image
.isp	Internet Communication Settings
.js	JScript file
.jse	JScript Encoded Script file
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.msc	Microsoft Common Console document
.msi	Microsoft Windows Installer package
.msp	Microsoft Windows Installer patch
.mst	Microsoft Visual Test source files
.pcd	Photo CD Image, MS Visual compiled script
.pif	Shortcut to MS-DOS program
.reg	Registration entries
.scr	Screen Saver
.sct	Windows Script Component
.shb	Shell Scrap Object
.shs	Shell Scrap Object
.url	HTML page
.vb	VBScript file
.vbe	VBScript Encoded Script file
.vbs	VBScript file
.wav	Sound File
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file

Protocols

An extension of the original OSSTMM Internet protocols list, the OPRP is a single resource for information on Internet and network protocols, transport information, and specifications. This resource is essential to thorough security testing.

See www.isecom.org/oprp.

Open Methodology License (OML)

Copyright (C) 2002 Institute for Security and Open Methodologies (ISECOM).

PREAMBLE

A methodology is a tool that details WHO, WHAT, WHICH, and WHEN. A methodology is intellectual capital that is often protected strongly by commercial institutions. Open methodologies are community activites which bring all ideas into one documented piece of intellectual property which is freely available to everyone.

With respect the GNU General Public License (GPL), this license is similar with the exception for the right for software developers to include the open methodologies which are under this license in commercial software. This makes this license incompatible with the GPL.

The main concern this license covers for open methodology developers is that they will receive proper credit for contribution and development as well as reserving the right to allow only free publication and distribution where the open methodology is not used in any commercially printed material of which any monies are derived from whether in publication or distribution.
Special considerations to the Free Software Foundation and the GNU General Public License for legal concepts and wording.

TERMS AND CONDITIONS

1. The license applies to any methodology or other intellectual tool (ie. matrix, checklist, etc.) which contains a notice placed by the copyright holder saying it is protected under the terms of this Open Methodology License.

2. The Methodology refers to any such methodology or intellectual tool or any such work based on the Methodology. A "work based on the Methodology" means either the Methodology or any derivative work by copyright law which applies to a work containing the Methodology or a portion of it, either verbatim or with modifications and/or translated into another language.

3. All persons may copy and distribute verbatim copies of the Methodology as are received, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and creator or creators of the Methodology; keep intact all the notices that refer to this License and to the absence of any warranty; give any other recipients of the Methodology a copy of this License along with the Methodology, and the location as to where they can receive an original copy of the Methodology from the copyright holder.

4. No persons may sell this Methodology, charge for the distribution of this Methodology, or any medium of which this Methodology is apart of without explicit consent from the copyright holder.

5. All persons may include this Methodology in part or in whole in commercial service offerings, private or internal (non-commercial) use, or for educational purposes without explicit consent from the copyright holder providing the service offerings or personal or internal use comply to points 3 and 4 of this License.

6. No persons may modify or change this Methodology for republication without explicit consent from the copyright holder.

7. All persons may utilize the Methodology or any portion of it to create or enhance commercial or free software, and copy and distribute such software under any terms, provided that they also meet all of these
conditions:

a) Points 3, 4, 5, and 6 of this License are strictly adhered to.

b) Any reduction to or incomplete usage of the Methodology in the software must strictly and explicitly state what parts of the Methodology were utilized in the software and which parts were not.

c) When the software is run, all software using the Methodology must either cause the software, when started running, to print or display an announcement of use of the Methodology including an appropriate copyright notice and a notice of warranty how to view a copy of this License or make clear provisions in another form such as in documentation or delivered open source code.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on any person (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If said person cannot satisfy simultaneously his obligations under this License and any other pertinent obligations, then as a consequence said person may not use, copy, modify, or distribute the Methodology at all. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

9. If the distribution and/or use of the Methodology is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Institute for Security and Open Methodologies may publish revised and/or new versions of the Open Methodology License. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
NO WARRANTY

11. BECAUSE THE METHODOLOGY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE METHODOLOGY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE METHODOLOGY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE IN USE OF THE METHODOLOGY IS WITH YOU. SHOULD THE METHODOLOGY PROVE INCOMPLETE OR INCOMPATIBLE YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY USE AND/OR REDISTRIBUTE THE METHODOLOGY

UNMODIFIED AS PERMITTED HEREIN, BE LIABLE TO ANY PERSONS FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE METHODOLOGY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY ANY PESONS OR THIRD PARTIES OR A FAILURE OF THE METHODOLOGY TO OPERATE WITH ANY OTHER METHODOLOGIES), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.