The Ideahamster Organization

Open-Source Security Testing Methodology Manual

Created by Pete Herzog

current version:	osstmm.2.0 release candidate 6	
notes:	*This is a preview release version to for 2.0 and not an update for version 1.5. This version focuses on security testing from the outside to the inside. This has not been peer-reviewed.*	
date of current version:	Tuesday, February 26, 2002	
date of original version:	Monday, December 18, 2000	
created by:	Pete Herzog	
key contributors:	Victor A. Rodriguez Marta Barceló Peter Klee Vincent Ip Waidat Chan Russ Spooner Miguel Angel Dominguez Torres Rich Jankowski Anton Chuvakin Efrain Torres Michael S. Hines	Clément Dupuis Tyler Shields Jose Luis Martin Mas Don Bailey Felix Schallock Miguel Angel de Cara Angel Luis Uruñuela Dru Lavigne Sacha Faust Rob J. Meijer John Pascuzzi
key assistance:	Rafael Ausejo Prieto Nigel Hedges Debbie Evans Daniel R. Walsh Juan Antonio Cerón Jordi Martinez Barrachina	Lluís Vera Drew Simonis Manuel Fernando Muiños Gómez Emily K. Hawthorn Kevin Timm

Those who have been contributed to this manual in consistant, valuable ways have been listed here although many more people do 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.

Table of Contents

Foreword

by Pete Herzog

It began with a simple idea: to make a methodology for security testing open to all. I had no interest in competing with the many hacking books and articles in existence. I knew that this would be important if it worked. I knew it had to work since much of security testing follows a methodology whether or not we sec testers really saw it as anything but a rhythm.

Sure enough, in a moment of inspiration, commuting on a train from Barcelona, I scratched out the few ideas I had for a flow chart on the back of an envelope. It got interesting. At home, I began to map it out further and defined what I had mapped. That became the OSSTMM version 0.9.0. Now as we enter into 2.0 I feel as if this manual has truly become a project. I had over 150 contributions, with 33 people becoming regular team members, and half a million downloads of the meth. From those downloads, I have had many positive comments and constructive criticisms. This manual, through peer review and much support, has become the most thorough and complete security testing document to be found.

The changes to 2.0 have resulted in a very different manual from its successor and I have a feeling once OSSTMM 2.5, the peer-reviewed and official version of 2.0 is released, it will again look very different from this version. But in the end, it should still feel the same—it should feel complete.

The major changes I have implemented resulted from two decisions. The first decision was to integrate security metrics and benchmarking in a way that would allow anyone to evaluate security products based on their ability to test according to the OSSTMM and to measure the risks associated with security within a time cycle. The second decision was to develop this methodology more as to include physical security testing, social engineering, wireless testing, and communications testing.

To act on the first decision, we had to make the RAVs work. We needed a metric for measuring risk and security against time and inaction. Bouncing off the two SPF ("sun protection factor" and "security protection factor") ideas received, we were able to get it to work well. Whether it works well enough remains to be seen in the peer review.

The second decision required much more information and planning which, as you see here, needs more work. I wanted to refine the scope to accommodate this increase which meant only unpriviledged testing and only from the outside to the inside.

Since OSSTMM 1.5 was released the world has had its own security crisis publicized in ways that only tragic events in first-world nations can muster. It became clear to many that something needed to be done about the few who knew how to get around security controls and cause harm. Many reactions caused many new security controls and many new privacy laws to get passed worldwide. In an effort to remain up-to-date, I fought to stay on top of all this legislation but in the end, one thing was clear: most of the ractions and legislation didn't change anything. From a security tester's standpoint, I could see how it is always the same things, whether protecting a network or an airplane, that impedes worthwhile security. It is always an issue of usability and understanding. Those who know the defensive products best knows what they can do and what they can't. Those who understand alarm and monitoring know the limitations of those devices. And those who know people will always find their ways into priviledged and barred entry points. So why aren't these resources properly tested? I think it's because too much of security defense is one-sided and often hollow. Too much trust is put in a machine and too little education into the operators and monitors of these machines. In the end, many of these defenses are then tested in the same one-sided way and never like those who sublimate them.

A great security tester is a bit of a mad scientist that mixes vast knowledge, fantastic creativity, inspired charisma, and scientific methodology. The OSSTMM aspires to be that scientific methodology. At least I am inspired to bring it to that point. In the end, nothing defensive should ever be built and placed without having been tested in the environment it stands in. And that's the kind of world I want to live in.

Introduction

This manual is a definitive standard for unpriviledged security testing in any environment from the outside to the inside. This focus requires that the tester has no special access point or permission different from that which is shared with the general public.

The concept of this manual has and always will be to create one accepted method for performing a thorough security test. Regardless of the credentials of the security tester, the size of the security firm, financing, or vendor backing, any network or security expert who meets the outline requirements in this manual is said to have completed a successful security scattershot. This does not mean one cannot perform a test faster, more in depth, or of a different flavor. The tester following the methodology within this manual is said to have followed the standard model and therefore if nothing else, has been thorough. In doing so, the tester still must report the results of all modules and tasks fulfilled to include OSSTMM certification in a report.

I will define the security scattershot I described previously because I believe a security test is no more than a view of a defensive posture at a single moment in time. At that time, the known vulnerabilities, the known weaknesses, the known configurations have not changed within that minute and therefore is said to be a snapshot. But is this snapshot enough? The methodology proposed in this manual will provide more than a snapshot if followed correctly with no short-cuts as based on the accepted concept of risk assessment and management. The snapshot will be a scattershot-- encompassing a range of variables over various periods of time before degrading below an acceptable risk level. This manual introduces Risk Assessment Values (RAVs) which will aid in the clarification of this scattershot by quantifying the risk level and allowing for specific tests within specific time periods to cycle and minimize the amount of risk one takes in any defensive posture.

Is it worth having a standard methodology for security testing? Security testing is not a product to be standardized and I know of many variables which affect the outcome of a test and stems from the tester. Precisely because of all these variables it is important to define one right way to test based on consensus and best practices worldwide.

In the end, following an open-source, standardized methodology that anyone and everyone can open and dissect and add to and complain about is the most valuable contribution anyone can make to security testing. And if you need a reason to recognize it and admit it exists (whether or not you follow it to the letter) it's because you, your colleagues, and your fellow professionals have helped design it and write it. The rest is about firm size, finance capital, and vendor backing.

Scope

This is a document of security testing methodology; a set of rules and guidelines for all means in which events are tested from the outside to the inside. It is within the scope of this document to provide a standardized approach to a thorough security assessment of each section within the security presence of an organization. Within this standardized approach for thoroughness, we achieve an Open Standard for Security Testing and use it as a baseline for all security testing methodologies known and unknown.

Accreditation

The use of this manual in the conducting of security testing is determined by the reporting of each task and its results even where not applicable in the final report. All final reports which include this information are said to have been conducted in the most thorough and complete manner and may include the following statement and a tamp in the report:

Open Source Security Testing Methodology Manual
Certified
OSSTMM 2.0
Compliant!
www.osstmm.org

This test has been performed in accordance to the **Open Source Security Testing Methodology** available at http://www.osstmm.org/ and hereby stands within best practices of security testing.

All stamps (color and b&w) are available at http://www.osstmm.org/stamps.htm

Intended Audience

This manual is written for the security testing professionals. Terms, skills, and tools mentioned in here may not make much sense to the novice or those not directly involved in security testing.

This manual does not explain how to perform the tests. This manual focuses on what must be tested in what manner and order. Those attempting to circumvent a security posture need to find only one hole. Security testers need to find them all. We are caught between the lesser of two evils and disclosure will at least inform in a structured, useful way those who need to defend themselves. So to disclose with this manual or not is truly a damned if you do and damned if you don't predicament. We choose disclosure. In choosing disclosure we have been sure not to include specific vulnerabilities or problems that can be abused and only offer this standard methodology.

Designers and developers will find this manual useful in building better defense and testing tools. Many of the tests do not currently have a way to automate them. Many of the automated tests do not follow a methodology in an optimal order. This manual will address these issues.

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 defenses.

Analysis

Analysis is not within the scope of this document. The focus of this manual is in the process of test and result.

Risk Assessment

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).

Terms

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

This manual was developed to satisfy the testing and risk assessment for personal data protection and information security in the following bodies of legislation. The tests performed provide the necessary information to analyze for data privacy concerns as per most governmental legislations and organizational best practices due to this manual's thorough testing stance. Although not all country statutes can be detailed herein, this manual has explored the various bodies of law to meet the requirements of strong examples of individual rights and privacy.

Legislation

The tests in this manual are designed for the remote auditing and testing of the following:

United States of America

- 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,

Canada

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

United Kingdom

- UK Data Protection Act 1998

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 organisation.
- National Privacy Principle (NPP) 4.1 provides that an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

Best Practices

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

IS 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.

CASPR

This manual is in full compliance with the best practices and guidelines set forth by document control and peer review from the members of the Commonly Accepted Security Practices and Recomendations (CASPR) of which this manual will fulfill a Best Practices need for Security Testing in Internet Security.

OWASP

This manual is in full compliance with the remote security testing and auditing of web applications as per the Open Web Application Security Project (OWASP).

SCIP

This document uses offensive and defensive market/business intelligence gathering techniques known as Competitive Intelligence as per the Society of Competitive Intelligence Professionals (SCIP) and the technique known as "Scouting" to compare the target organization's market/business positioning to the actual position as seen from other intelligence professionals on the Internet. Another aspect of this manual is to introduce offense measures to conduct market/business intelligence gathering.

SET

This document incorporates the remote auditing test from the SET Secure Electronic Transaction(TM)Compliance Testing Policies and Procedures, Version 4.1, February 22, 2000

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

Best Practice and "Intelligent" Papers

- Breaking into computer networks from the Internet. By roelof@sensepost.com, 2001 Roelof Temmingh & SensePost (Pty) Ltd
- Security Reference Handbook. 2001, Symantec Corporation
- The MH DeskReference Version 1.2. by The Rhino9 Team
- Auditing Your Firewall Setup. Lance Spitzner, 12 December, 2000
- Security of Information Technology. NPG 2810.1, NASA Procedures and Guidelines
- "The 10 Commandments of Counterintelligence". James M. Olson, Studies of Intelligence, Unclassified Edition, Fall-Winter 2001, No.11, published by the CIA's Center for the Study of Intelligence
- "Security and Company Culture". Michael G. McCourt, Workplace Violence Prevention Reporter, December 2001

Process

A security test is performed with two types of attack. A passive attack is often a form of data collection which does not directly influence or trespass upon the target. An intrusive attack however does trespass upon the target and can be monitored, logged, and used to alarm the target.

The process of a security test concentrates on evaluating the following areas which in turn reflect upon the security presence which is the defined environment for security testing.

Visibility

Visibility is what can be seen, logged, or monitored in the security presence both with and without the aid of electronic devices. This includes, but is not limited to, radio waves, light beyond the visible spectrum, communication devices such as telephones, GSM, and e-mail, and network packets such as TCP/IP.

Access

Access is an entry point into the security presence. An access point need not be physical barrier. This can include, but is not limited to, a web page, a window, a network connection, radio waves, or anything in which a location supports the definition of quasi-public or where a computer interacts with another computer within a network. Limiting access means denying all except what is expressly permitted financially and in best practices.

Trust

Trust is a specialized pathway in regards to the security presence. Trust includes the kind and amount of authentication, nonrepudiation, access control, accountability, confidentiality, and integrity between two or more factors within the security presence.

Alarm

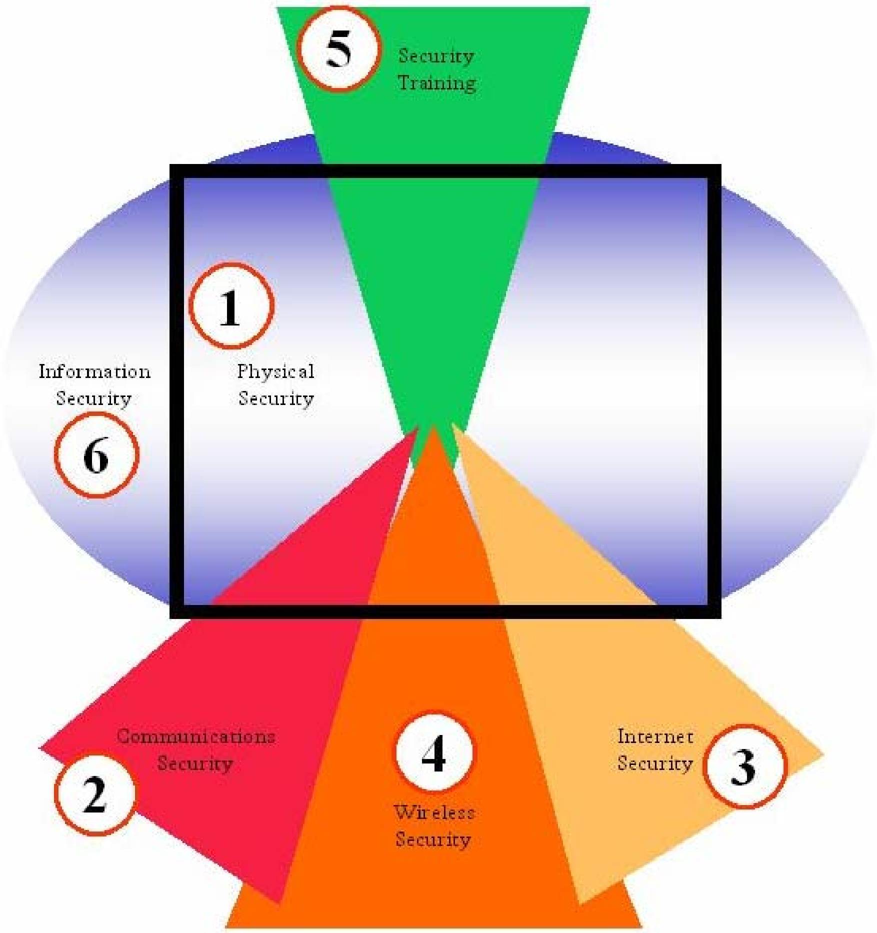
Alarm is the timely and appropriate notification of activities that violate or attempt to violate Visibility, Access, or Trust. In most security breaches, alarm is often the single process which initiates further consequences.

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 in this manual are:

Internet Security
Information Security
Physical Security
Communications Security
Wireless Security
Social Engineering



Module List

Internet Security

- Network Surveying
- Port Scanning
- System Identification
- Services Identification
- Vulnerability Research and Verification
- Internet Application Testing
- Router Testing
- Firewall Testing
- Intrusion Detection System Testing
- Trusted Systems Testing
- Password Cracking
- Denial of Service Testing
- Containment Measures Testing

Information Security

- Document Grinding
- Competitive Intelligence Scouting
- Privacy Review

Social Engineering

- Request Testing
- Guided Suggestion Testing
- Trust Testing

Wireless Security

- Wireless Networks Testing
- Cordless Communications Testing
- Privacy Review
- Infrared Systems Testing

Communications Security

- PBX Testing
- Voicemail Testing
- FAX review
- Modem Testing

Physical Security

- Access Controls Testing
- Perimeter Review
- Monitoring Review
- Alarm Response Testing
- Location Review
- Environment Review

Sections and Modules

The methodology is broken down into *sections*, *modules* and *tasks*. The sections are specific points in the security map which overlap with each other and begin to disect a whole which 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 three things--

- The tasks were not properly performed.
- The tasks were not applicable.
- The tasks revealed superior security.
- The task result data has been improperly analyzed.

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 ommitted 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 innappropriate faith in the security of a system.

Test Modules and Tasks

Module Example

Module Name

tools link

Section Name

RAV cycle

RAV degradation

Description of the module.

Expected Results:	Item Idea Concept Map

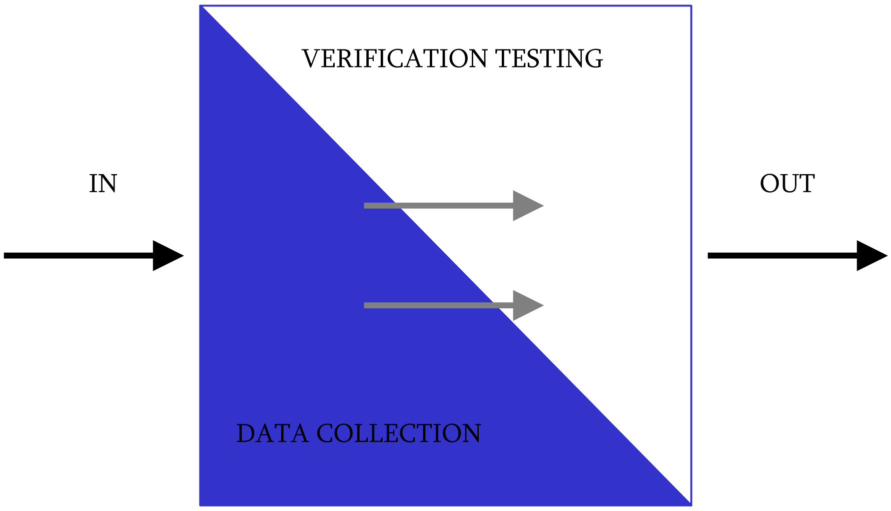
Tasks to perform for a thorough network survey include:

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 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.

Assessing Risk

Integrated with each module are Risk Assessment Values (RAVs) which are defined as the degradation of security (or escalation of risk) over a specific life cycle based on best practices for periodic testing. The association of risk levels with cycles has proven to be an effective procedure for security metrics.

The concept of security metrics in this manual are for:

1. Establish a standard time cycle for testing and retesting to
2. Maintain a measurable level of risk based on
3. The degradation of security (escalation of risk) which occurs naturally, with time and
4. The ability to measure Internet security with consistancy and detail.

Unlike conventional risk management, the RAVs operate purely on the application of security within an organization. They take into consideration the controls such as the processes, politics, and procedures by operating in parallel with the testing methodology. While the testing methodology does examine these controls sometimes in an indirect nature, the actual controls do not interest the tester rather it is the application of these controls that determine the results of a security test. A well written policy which is not followed will have no effect on actual security.

RAVs are determined mathematically by three factors:

1. The degrees of degradation of each separate module from point of optimum health which is noted as a theoretical maximum of 100% for risk management purposes,
2. The cycle which determines the maximum length of time it takes for the degradation to reach zero based on security best practices for regular testing,
3. And various weights based on the process areas of Alarm, Trust, Visibility, and Access.

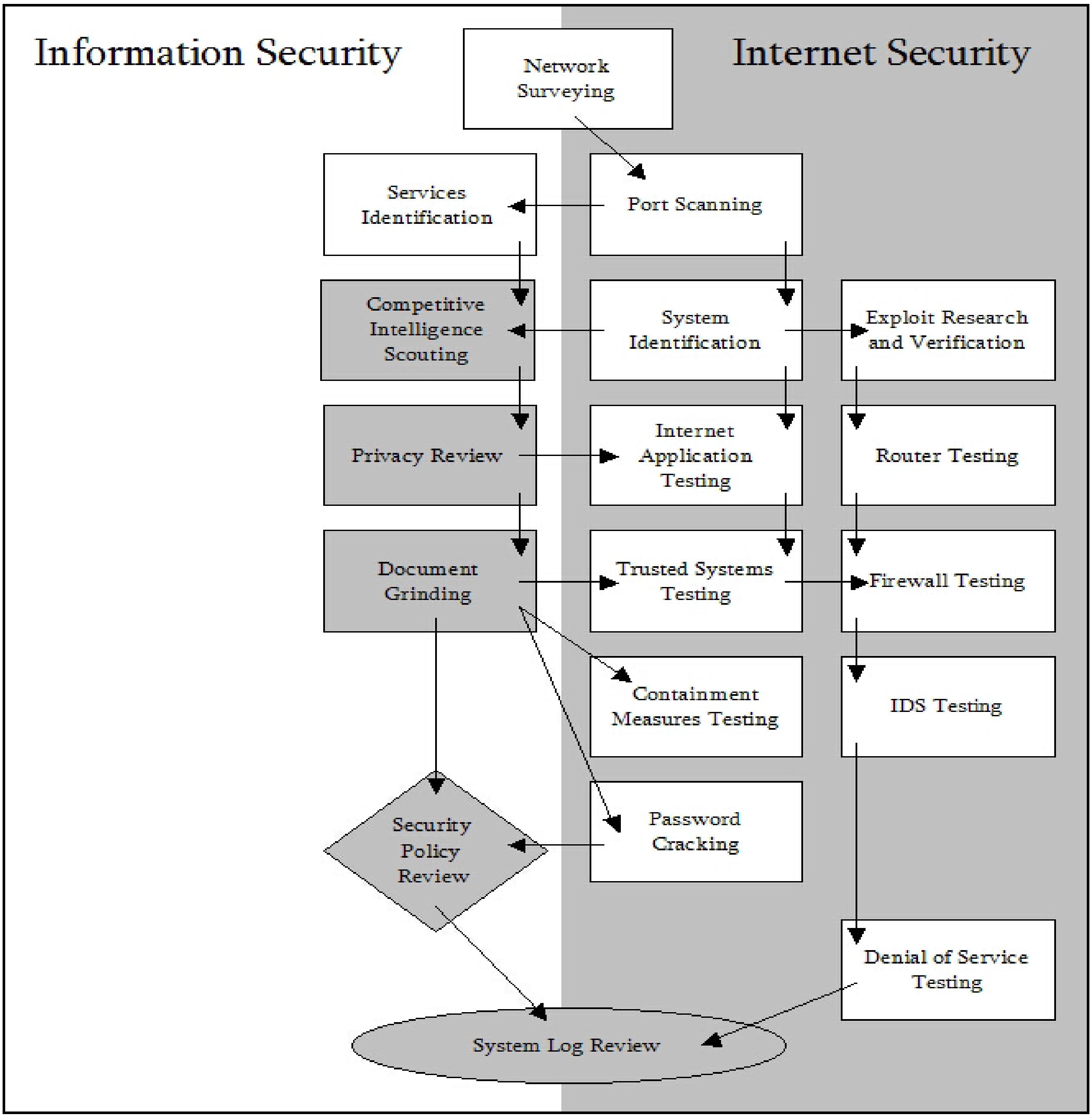
$$\boxed{RA_{var} = \left(1 - \left(\frac{deg/10}{cycl}\right)\right)^{days} \times RA}$$

The RAV is determined, as per current algorythm, is to be the division of the degradation by the cycle.

Section 1 – Internet Security

Internet Presence Points

Security testing is a strategic effort. While there may be different ways and different tools to test many of the same modules, there are few variations in the order in which to test them.



Internet presence points are every point in the Internet where an organization interacts with the Internet. These presence points are developed to offer as modules in the methodology flow. Some of these modules are:

Network Surveying

Internet Security

	tools
30 days	3%

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 times, 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 times 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.

Port Scanning

Internet Security

	tools
7 days	1.7%

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 Appendix F.

Each Internet enabled system has 65,536 TCP and UDP possible ports. 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.

Services Identification

Internet Security

	tools
19 days	3.9%

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.

System Identification

Internet Security

	tools
54 days	2.15%

System fingerprinting is the active probing of a system for responses that can distinguish unique systems to 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.

Vulnerability Research and Verification

Internet Security

	tools
3 days	3.6%

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).

Internet Application Testing

Internet Security

	tools
67 days	5.8%

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.

Router Testing

Internet Security

	tools
34 days	3.2%

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

Trusted Systems Testing

	tools
42 days	4.1%

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.

Firewall Testing

Internet Security

	tools
34 days	2.9%

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.

Intrusion Detection System Testing

Internet Security

	tools
25 days	2.3%

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.

Containment Measures Testing

Internet Security

	tools
96 days	3.9%

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.

Password Cracking

Internet Security

	tools
21 days	7.8%

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.
- Verify password aging.

Denial of Service Testing

Internet Security

	tools
4 days	5.4%

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.

Section 2 - Information Security

Competitive Intelligence Scouting

Information Security

	tools
17 days	7.3%

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 lends 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:

- Map and measure the directory structure of the web servers
- Map the measure the directory structure of the FTP servers
- Examine the WHOIS database for business services relating to registered host names
- Determine the IT cost of the Internet infrastructure based on OS, Applications, and Hardware.
- Determine the cost of support infrastructure based on regional salary requirements for IT professionals, job postings, number of personnel, published resumes, and responsibilities.
- Measure the buzz (feedback) of the organization based on newsgroups, web boards, and industry feedback sites
- Record the number of products being sold electronically (for download)
- 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

Privacy Review

Information Security

	tools
96 days	2.9%

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:

- Compare publicly accessible policy to actual practice
- Compare actual practice to regional fraud and privacy laws or compliancy
- Identify database type and size for storing data
- Identify data collected by the organization
- Identify storage location of data
- Identify cookie types
- Identify cookie expiration times
- Identify information stored in cookie
- Verify cookie encryption methods
- Identify server location of web bug(s)
- Identify web bug data gathered and returned to server

Document Grinding

Information Security

	tools
96 days	8.7%

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:

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

Section 3 – Social Engineering

Request Testing

Social Engineering

	tools
96 days	2.9%

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:

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

Guided Suggestion Testing

Social Engineering

	tools
46 days	8.9%

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:

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

Trusted Persons Testing

Social Engineering

	tools
96 days	6.2%

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:

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

Section 4 – Wireless Security

Wireless Networks Testing

Wireless Security

	tools
28 days	1.3%

This is a method for testing wireless access to LAN and is becoming increasingly popular. However, some fairly alarming problems, security-wise, are common when implementing these technologies.

Expected Results:	The outer-most physical edge of the wireless network The logical boundaries of the wireless network Access points into the network IP-range (and possibly DHCP-server) of the wireless network Exploitable "mobile units" (clients)

Tasks to perform for a thorough Wireless Networks test:

- Verify the distance in which the wireless communication extends beyond the physical boundaries of the organization.
- List equipment needed/tried should be taken (antenna, card, amplifier, etc.)
- Verify authentication-method of the clients
- Verify that encrytion is configured and running - and what keylength used
- Verify that clients can't be forced to fall-back to plaintext-mode
- Verify the IP-range of the network
- Verify the IP-range and reachable from the wireless network, and the protocols involved
- Probe network for possible DoS problems

Cordless Communications Testing

Wireless Security

	tools
60 days	2.8%

This is a method of testing cordless communications communication devices which may exceed the physical and monitored boundaries of an organization.

Expected Results:	The outer-most physical edge of the cordless communications The logical boundaries of the cordless communications List of communication types List of frequencies emanating from the target List of vulnerabilities in the cordless communication present

Tasks to perform for a thorough Cordless Communications test:

- Verify the distance in which the cordless communication extends beyond the physical boundaries of the organization.
- Note equipment needed/tried should be taken (antenna, scanner, amplifier, etc.)
- Verify authentication-method of the clients
- Verify that encryption is used, configured, and type used
- Verify that clients can't be forced to fall-back to non-encrypted mode
- Probe network for possible DoS problems

Privacy Review

Wireless Security

	tools
70 days	2.1%

The privacy of cordless 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

Tasks to perform for a thorough Privacy Review:

- Verify authentication-method of the clients
- Verify that encryption is used is configured and type used
- Verify that clients can't be forced to fall-back to none-encrypted mode
- Compare publicly accessible policy to actual practice
- Compare actual practice to regional fraud and privacy laws or compliancy
- Identify database type and size for storing data
- Identify data collected by the organization
- Identify storage location of data
- Identify data expiration times

Infrared Systems Testing

Wireless Security

	tools
120 days	0.6%

This is a method of testing infrared communications communication devices which may exceed the physical and monitored boundaries of an organization.

Expected Results:	The outer-most physical edge of the infrared communications List of line-of-site areas into the target The logical boundaries of infrared communications List of communication types List of systems and applications emanating from the target

Tasks to perform for a thorough Infrared Systems test:

- Verify the distance in which the infrared communication extends beyond the physical boundaries of the organization.
- Note equipment needed/tried should be taken (antenna, scanner, amplifier, etc.)
- Verify authentication-method of the clients
- Verify that encryption is used, configured, and type used
- Verify that clients can't be forced to fall-back to non-encrypted mode
- Probe network for possible DoS problems

Section 5 – Communications Security

PBX Testing

Communications Security

	tools
180 days	2.9%

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.

Voicemail Testing

Communications Security

	tools
101 days	4.1%

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.

FAX Review

Communications Security

tools	
200 days	1.25%

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.

Modem Testing

Communications Security

tools	
124 days	6.3%

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 6 – Physical Security

Access Controls Testing

Physical Security

	tools
92 days	6.9%

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

Perimeter Review

Physical Security

	tools
12 days	2.45%

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 physical access points Types of monitoring Types of alarm systems List of alarm triggers

Tasks to perform for a thorough Perimiter review:

- Enumerate monitoring devices
- Map monitoring devices
- Map guarded locations and routes traveled
- Map unmonitored areas

Monitoring Review

Physical Security

	tools
122 days	4.1%

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 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

Alarm Response Review

Physical Security

	tools
96 days	8.25%

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

Location Review

Physical Security

	tools
180 days	7.9%

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

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 hours and days in delivery cycles
- List hours and days in visitor cycles

Environment Review

Physical Security

	tools
180 days	9.5%

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 access points List of vulnerable access points 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 template is 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	

Internal System Information	
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	

Security Policy Review

Although no longer a module, the security policy review is still an important, functional part of this manual.

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:

- Measure the security policy points against the actual state of the Internet presence.
  - *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.
  - 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.
  - Identify incident handling procedures, to ensure that breaches are handled by the correct individual(s) and that they are reported in an appropriate manner.
    - *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.
    - *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.
    - *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.
- Measure the security policy points against the actual state of non-Internet connections.
  - *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.
  - *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.
  - *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.
- 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.

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

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

Included with this manual are key references for using 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
.bas	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

Acronym	Stands for	RFC	Protocol ID	Description
AH	IP Authentication Header	RFC 2402	51	Indicates an IPSEC packet, therefore contents will be encrypted
DDP	(Appletalk's) Datagram Delivery Protocol		37	Appletalk's equivalent to IP
EGP	Exterior Gateway Protocol	RFC 904	8	Family of routing protocols used to connect the global Internet
EIGRP	(Cisco's) Enhanced Interior Routing Protocol		88	Cisco's solution for routing IP, IPX, & Appletalk
ESP	IP Encapsulating Security Payload	RFC 2406	50	Used to encrypt the contents of an IPSEC packet
GRE	General Routing Encapsulation	RFC 2784	47	Indicates an encrypted packet, possibly a PPTP packet
ICMP	Internet Message Control Protocol	RFC 950	1	Used to send error messages; also used by Ping utility
ICMPv6	RFC 2463		58	Same as ICMP, but for IP version 6 networks
IDRP	Inter-Domain Routing Protocol	RFC 1745	45	A type of EGP
IGMP	Internet Group Management Protocol	RFC 2236	2	Used during multicasts to allow subscribed users to receive packets
IGP	any Interior Gateway Protocol (e.g. IGRP) RFC 1371		9	Routing protocols used to connect smaller networks
IGRP	Cisco's Interior Gateway Routing Protocol		9	An example of one of Cisco's IGPs
IP	Internet Protocol	RFC 791	0	Provides network addressing on TCP/IP networks
IP-ENCAP IP in IP			4	
IPIP	IP-within-IP Encapsulation Protocol		94	
IPv6	Internet Protocol version 6	RFC 2460	41	Same as IP, but for IP version 6 networks
IPv6-FRAG		RFC 2460	44	
IPv6-NONXT IPv6 no next header		RFC 2460	59	
IPv6-OPTS		RFC 2460	60	
IPv6-ROUTE		RFC 2460	43	
IPX-in-IP			111	
L2TP	Layer 2 Tunneling Protocol	RFC 2661	115	Used in Virtual Private Networks
MOBILE	Minimal Encapsulation within IP	RFC 2004	55	Indicates an IP packet carried within another IP packet
PNNI	PNNI over IP	RFC 2843	102	Used for communication between ATM switches
RSVP	Resource Reservation Setup Protocol	RFC 2750	46	Reserves bandwidth on the Internet for multicasts
SKIP		RFC 2356	57	Allows a mobile user to maintain their IP address securely
SWIPE	IP with encryption		53	
TCP	Transmission Control Protocol	RFC 793	6	Connection oriented transport used in TCP/IP networks
UDP	User Datagram Protocol	RFC 768	17	Connection-less transport used in TCP/IP networks
VRRP	Virtual Router Redundancy Protocol	RFC 2338	112	Provides dynamic default route on static routers

Acronym	Stands For	RFC/ Standard	Port	Description
AARP	Appletalk Address Resolution Protocol	ADPA #C0144LL/A		Since Appletalk addresses are dynamic, ensures there are no address conflicts
AEP	AppleTalk Echo Protocol			Provides functionality similar to Ping
ARP	Address Resolution Protocol	RFC 826		Maps IP addresses to associated MAC address
ATALK	AppleTalk Protocol	ADPA #C0144LL/A		The Appletalk Protocol Suite
ATMP	Ascend Tunnel Management Protocol	RFC 2107	5150	Allows remote users to access a network
BGP4	Border Gateway Protocol	RFC 1772	179	A type of EGP
BO2K	Back Orifice 2000		31337	A dubious set of remote administration tools
BOOTP/DHCP	Bootstrap Protocol	RFC 2132	67 & 68	Allows a client to receive IP addressing info from a server
CATALYST	Synchronization protocol for Cisco Catalyst switches		2836	Synchronization protocol for Cisco Catalyst switches
CDP	Cisco Discovery Protocol			Used by Cisco routers to exchange information
CGMP	Cisco Inter-Process Communication			Allows switches to support multicast traffic
Chargen	Character Generator	RFC 864	19	Rarely used for legitimate purposes
CIPC	Cisco Group Management Protocol			
CSTB	Cisco Spanning Tree BPDU			
DAYTIME		RFC 868	13	Rarely used for legitimate purposes
DBASE	dBASE UNIX		217	
DISCARD		RFC 863	9	
DISL	Dynamic Inter-Switch Link			Used to load balance traffic between switches
DLSRPN	Data Link Switch (DLSw) Read	RFC 1795	2065	Provides communications between Datalink Switches
DLSWPN	Data Link Switch (DLSw) Write	RFC 1795	2067	Provides communications between Datalink Switches
DNS	Domain Name Service Protocol	RFCs 1034 & 1035	53	Used to translate a hostname into its associated IP address
DOOM	DOOM Game		666	
DRP	DEC Routing Protocol		1974	Routing Protocol used by Digital Networks
ECHO		RFC 862	7	Rarely used for legitimate purposes
FINGER	Finger User Information Protocol	RFC 1288	79	Used to gather information about user accounts on Unix systems
FTP	File Transfer Protocol	RFC 959	20 & 21	Used to transfer files between hosts
GARP	General Attribute Registration Protocol	ISO/IEC 15802-3		
GDP	Cisco Gateway Discovery Protocol		1997	Used by Cisco routers to discover routes
GOPHER	Internet Gopher Protocol	RFC 1436	70	Text based tool for browsing non-html content
H.323	Audio/Video Conferencing Standard		1720	Audio/Video Conferencing Standard
HSRP	Cisco Hot Standby Router Protocol	RFC 2281	1985	Used by Cisco routers to create one "virtual" router from many physical routers
HTTP	Hypertext Transfer Protocol	RFC 1945	80	Used to exchange files on the WWW
HTTPS	Secure HTTP	RFC 2660	443	Used to encrypt http content
ICA	(Citrix) Independent Computing Architecture		1494, 1604	Citrix's solution for creating "thin" clients
ICP	Internet Cache Protocol	RFC 2186	3130, 3128	Used on cache servers e.g. Squid

ICQ	I Seek You		4000	Mirabilis' web-based chat service
IDENTD	Auth		113	Used to identify remote users e.g. email client
IMAP4	Interactive Mail Access Protocol	RFC 2061	143	Used to retreive email from email servers
IMAP4-SSL		RFC 2595	585, 993	Encrypts IMAP data
INGRES-N	Network PostScript		134	
IPX	Internet Packet Exchange	RFC 1132	213	Provides network addressing on Netware networks similar in function to IP
IPX-TUNN	Tunneling IPX through IP networks	RFC 1234	213	Tunneling IPX packets through IP networks
IRC	Internet Relay Chat Protocol	RFCs 2810-2813	6667	Text-based conferencing system
ISAKMP	Internet Security Association Key Mgmt Protocol	RFC 2408	500	Used to manage keys for IPSEC
KERBEROS		RFC 1510	88, 749-751, 754	Provides authentication and encryption services
L2F	Cisco Layer Two Forwarding	RFC 2341	1701	Used for dial-up
L2TP	Layer 2 Tunneling Protocol	RFC 2661	1701	Allows many types of packets to use PPP
L3SW	Layer 3 IP and IPX switching			
LDAP	Lightweight Directory Access Protocol	RFC 2251	389, 636, 3268, 3269	Used to maintain directory databases
LPR	Line Printer Remote	RFC 1179	515	Used in Unix printing
MS-SQL	(Microsoft's) SQL Server		1433 & 1434	Used to query and update Microsoft databases
NBP	AppleTalk Name Binding Protocol		2 & 202	Used on Appletalk networks to register names and socket addresses
NBT	NetBIOS-over-TCP	RFCs 1001 & 1002	137-139	Allows Microsoft applications to use TCP/IP
NCP	Netware Core Protocol		524	Manages access to resources on Netware networks
NDS	Netware Directory Services	RFC 2241	353	Database of resources available on a Netware network
Netmeeting			3895221731	Conferencing program from Microsoft
Netshow			1755	Streaming media utility from Microsoft
NetwareIP			43981 & 43982	Novell's version of TCP/IP
NFS	Sun Network File System	RFC 3010	111 & 2049	Used to share files on Unix networks
NHRP	Next Hop Resolution Protocol	RFC 2332		Used to find address of next hop on networks that don't support broadcasts
NLSP	Netware Link State Protocol			Novell's link-state routing protocol
NNTP	Network News Transfer Protocol	RFC 977	119 & 563	Used to transfer Usenet news across the Internet
NOTES	Lotus Notes Protocol		1352	Used on Lotus messaging systems
NOV-PEP	Novell Packet Exchange Protocol.			
NOV-RIP	Novell Routing Information Protocol			Distance-vector routing protocol used on Novell networks
NOV-SAP	Novell Service Advertising Protocol			Used to find resources on Novell networks
NOV-SPX	Novell Sequenced Packet Exchange Protocol			Novell's connection-oriented transport
NTALK/TALK			517, 518	Text-based conferencing system on Unix networks
NTP	Network Time Protocol	RFC 1305	123	Used to synchronize clocks on a network
OSPF	Open Shortest Path First	RFC 2328	89	Link-state routing protocol
POP3	Post Office Protocol	RFC 1939	110 & 995	Used to retreive email from email servers
PORTMAP	SUNRPC PORTMAPPER	RFC 1057	111	Maps RPC service numbers to IP port numbers on NFS and Microsoft

				networks
PPTP	Point to Point Tunneling Protocol	RFC 2637	1723	Used by Microsoft to create virtual private networks
PRINT	Network PostScript		170	
QUOTD	Quote of the Day		17	Rarely used for legitimate purposes
RADIUS	Remote Authentication Dial-in Service	RFC 2868	18121813	Used to authenticate dial-up users
RARP	Reverse Address Resolution Protocol	RFC 903		Used to map MAC address to its associated IP address
RAUDIO	Real Audio		6970-7170	Provides real-time audio streaming
RDP	(Microsoft's) Remote Desktop Protocol		3389	Used by Windows2000 Terminal Services
REXEC	Remote Exec		512	Rarely used for legitimate purposes
RIP	Routing Information Protcol	RFC 2453	520	Distance-vector routing protocol
RLOGIN	Remote login	RFC 1282	513	Rarely used for legitimate purposes
RSYNC	Remote Synchronization		873	Used for file synchronization in Unix networks
RTMP	(AppleTalk's) Routing Table Maintenance Protocol		1 & 201	Appletalk's distance-vector routing protocol
RTP/RTCP Real Time (Control) Protocol		RFC 1889	5004, 5005	Used to transport time-sensitive data, e.g. audio/video
SMB	(Microsoft) Server Message Block		138, 139, 445	Information sharing protocol used on Microsoft networks
SMTP	Simple Mail Transfer Protocol	RFC 2821	25 & 465	Used to deliver email over TCP/IP networks
SNMP	Simple Network Management Protocol	RFC 1157	161 & 1993	Used to remotely monitor networking devices
SNMPTRAP	Simple Network Management Protocol Trap Port	RFC 1215	162	Messages sent by devices monitored by SNMP
SQL*NET	Oracle SQL*NET		1521, 1526, 1575, 1600	Oracle's database
SSH	Secure Shell		22	Used instead of telnet to securely access Unix hosts
SSTB	Shared Spanning Tree BPDU			Used in bridged networks
STP	Spanning Tree Protocol	ISO/IEC 15802-3		Used in bridged networks
SUNRPC	SUN Remote Procedure Call Protocol	RFC 1831	111	Used by NFS and NIS networks
SYBASE	7878, 8001, 8002, 8080, 9000-9002			Allows database access over multiple protocols
SYSLOG			514	Logging facility used by Unix hosts
T.120/3	App sharing/chat/whiteboard standard		1503	Application sharing/chat/whiteboard standard
TACACS		RFC 1492	49	Provides authentication for dial-up users
TAGSWITC (Cisco's) Tag Switching		RFC 2105		Used to provide scalable routing
TELNET		RFC 854	23	Used to access a command shell on a remote host
TFTP	Trivial File Transfer Protocol	RFC 1350	69	File transfer protocol implemented in ROM of diskless workstations and routers
VDOLIVE	VDOLive		7000	Used to provide real-time audio and video
VSI	Virtual Switch Interface			Used by Cisco to allow multiple, independent control planes to control a switch
VTP	(Cisco's) VLAN Trunking Protocol			Cisco's protocol for administering VLANs
WCCP	(Cisco's) Web Cache Coordination Protocol		2048	Cisco's protocol for routers to communicate with Cache Servers
WHOIS		RFC 2167	43	Provides information concerning who has registered which IP addresses

WINS	(Microsoft) Windows Internet Name Service	42137	Used to locate resources on Microsoft networks

X Font Server		7100	Part of the XWindows system used on Unix hosts
X11	X Windows Protocol	6000-6063	Provides a graphical user interface on Unix hosts
XDMCP	X Display Manager Control Protocol	177	Part of the XWindows system used on Unix hosts
ZIP	AppleTalk Zone Information Protocol	6	Used on Appletalk networks to man network names to zones