

Table of Contents

Instructions.....	3
Quick Start.....	3
Upgrading from Older Versions.....	3
Version Information.....	4
About this Project.....	4
Local Support.....	4
Community Support.....	4
Print Edition.....	4
Restrictions.....	5
Acknowledgments.....	6
Primary Designers and Developers.....	6
Foreword	8
Introduction.....	14
Note.....	14
Purpose.....	15
Document Scope.....	15
Liability.....	15
Test Results.....	16
Certification and Accreditation.....	17
Certifications for Professionals.....	18
OPST.....	18
OPSA.....	18
OPSE.....	18
OWSE.....	18
CTA.....	18
Certifications for Organizations.....	20
Security Test Audit Report.....	20
ISECOM Licensed Auditors.....	20
OSSTMM Seal of Approval.....	20
Chapter 1 – What You Need to Know.....	22
1.1 Security.....	25
1.2 Controls.....	26
Interactive Controls.....	27
Process Controls.....	27
The Bad Lock Example.....	28
1.3 Information Assurance Objectives.....	29
1.4 Limitations.....	29
Limitations Mapping.....	31
Justification for Limitations.....	32
Managing Limitations.....	32
1.5 Actual Security.....	33
1.6 Compliance.....	33
Chapter 2 – What You Need to Do.....	35
2.1 Defining a Security Test.....	35
2.2 Scope.....	36
Channels.....	37
2.3 Common Test Types.....	38
2.4 Rules Of Engagement.....	40
A. Sales and Marketing.....	40
B. Assessment / Estimate Delivery.....	40
C. Contracts and Negotiations.....	40
D. Scope Definition.....	41
E. Test Plan.....	41
F. Test Process.....	41



OSSTMM 3 – The Open Source Security Testing Methodology Manual

G. Reporting.....	42
2.5 The Operational Security Testing Process.....	43
2.6 Four Point Process.....	45
2.7 The Trifecta.....	46
1. How do current operations work?.....	46
2. How do they work differently from how management thinks they work?.....	46
3. How do they need to work?.....	46
Combining the Trifecta and the 4 Point Process.....	47
2.8 Error Handling.....	48
Working with Test Errors.....	51
2.9 Disclosure.....	52
Disclosure Rights.....	52
Responsibilities.....	52
Chapter 3 – Security Analysis.....	54
Analyzing the Security of Everything.....	54
3.1 Critical Security Thinking.....	55
The Six Step Analysis Technique.....	55
Fallacies as Qualifiers.....	56
3.2 Recognize the OpSec Model.....	57
3.3 Look for Pattern Matching as a Sign for Errors.....	57
3.4 Characterizing the Results.....	58
3.5 Look for Signs of Intuition.....	59
3.6 Transparent Reporting.....	59
Chapter 4 – Operational Security Metrics.....	62
4.1 Getting to Know the Rav.....	63
What is a Rav Like?.....	63
Eight Fundamental Security Questions.....	65
4.2 How to Make a Rav.....	67
Combining Channels and Vectors.....	68
Rav Calculator.....	69
4.3 Applying Test Results to Ravs.....	70
Operational Security.....	70
Controls.....	72
Limitations.....	76
4.4 The Operational Security Formula.....	80
Porosity.....	80
4.5 The Controls Formula.....	81
Missing Controls.....	81
True Controls.....	82
Full Controls.....	82
4.6 The Limitations Formula.....	83
Security Limitations Base.....	83
4.7 The Actual Security Formula.....	84
Actual Security Delta.....	84
True Protection.....	84
Actual Security.....	84
Chapter 5 – Trust Analysis.....	86
5.1 Understanding Trust.....	86
5.2 Fallacies in Trust.....	88
5.3 The Ten Trust Properties.....	89
5.4 The Trust Rules.....	90
Example Trust Rules.....	91
5.5 Applying Trust Rules to Security Testing.....	93
Chapter 6 – Modules.....	95
6.1 Methodology Flow.....	96
The Memory of Operations.....	97
6.2 The Test Modules.....	98
A. Induction Phase.....	99
B. Interaction Phase.....	100
C. Inquest Phase.....	101



OSSTMM 3 – The Open Source Security Testing Methodology Manual

D. Intervention Phase.....	102
6.3 One Methodology.....	103
Chapter 7 - Human Security Testing.....	105
Considerations.....	105
7.1 Posture Review.....	106
7.2 Logistics.....	107
7.3 Active Detection Verification.....	107
7.4 Visibility Audit.....	109
7.5 Access Verification	109
7.6 Trust Verification	110
7.7 Controls Verification	111
7.8 Process Verification.....	112
7.9 Training Verification.....	113
7.10 Property Validation.....	114
7.11 Segregation Review.....	115
7.12 Exposure Verification.....	116
7.13 Competitive Intelligence Scouting.....	116
7.14 Quarantine Verification.....	117
7.15 Privileges Audit.....	117
7.16 Service Continuity.....	118
7.17 End Survey.....	118
Chapter 8 - Physical Security Testing.....	120
Considerations.....	120
8.1 Posture Review.....	121
8.2 Logistics.....	123
8.3 Active Detection Verification.....	124
8.4 Visibility Audit.....	124
8.5 Access Verification	125
8.6 Trust Verification	126
8.7 Controls Verification	127
8.8 Process Verification.....	128
8.9 Configuration Verification.....	128
8.10 Property Validation.....	129
8.11 Segregation Review.....	130
8.12 Exposure Verification.....	130
8.13 Competitive Intelligence Scouting.....	132
8.14 Quarantine Verification.....	133
8.15 Privileges Audit.....	134
8.16 Survivability Validation.....	135
8.17 Alert and Log Review.....	135
Chapter 9 - Wireless Security Testing.....	137
Considerations.....	137
9.1 Posture Review.....	138
9.2 Logistics.....	139
9.3 Active Detection Verification.....	139
9.4 Visibility Audit.....	140
9.5 Access Verification	141
9.6 Trust Verification	142
9.7 Controls Verification	142
9.8 Process Verification.....	144
9.9 Configuration Verification.....	144
9.10 Property Validation.....	145
9.11 Segregation Review.....	145
9.12 Exposure Verification.....	146
9.13 Competitive Intelligence Scouting.....	146
9.14 Quarantine Verification.....	147
9.15 Privileges Audit.....	147
9.16 Survivability Validation.....	148
9.17 Alert and Log Review.....	148
Chapter 10 - Telecommunications Security Testing.....	150
Considerations.....	150
10.1 Posture Review.....	151
10.2 Logistics.....	153
10.3 Active Detection Verification.....	154
10.4 Visibility Audit.....	155
10.5 Access Verification	156
10.6 Trust Verification	157



OSSTMM 3 – The Open Source Security Testing Methodology Manual

10.7 Controls Verification.....	158
10.8 Process Verification.....	159
10.9 Configuration Verification.....	160
10.10 Property Validation.....	161
10.11 Segregation Review.....	161
10.12 Exposure Verification.....	162
10.13 Competitive Intelligence Scouting.....	163
10.14 Quarantine Verification.....	163
10.15 Privileges Audit.....	164
10.16 Survivability Validation.....	164
10.17 Alert and Log Review.....	165
Chapter 11 - Data Networks Security Testing.....	167
Considerations.....	167
11.1 Posture Review.....	168
11.2 Logistics.....	169
11.3 Active Detection Verification.....	170
11.4 Visibility Audit.....	171
11.5 Access Verification	173
11.6 Trust Verification	174
11.7 Controls Verification.....	175
11.8 Process Verification.....	176
11.9 Configuration Verification.....	177
11.10 Property Validation.....	177
11.11 Segregation Review.....	179
11.12 Exposure Verification.....	179
11.13 Competitive Intelligence Scouting.....	181
11.14 Quarantine Verification.....	182
11.15 Privileges Audit.....	183
11.16 Survivability Validation.....	184
11.17 Alert and Log Review.....	184
Chapter 12 - Compliance.....	186
Regulations.....	187
Chapter 13 – Related Projects.....	194
13.1 Source Code Analysis Risk Evaluation.....	194
13.2 Home Security Methodology and Vacation Guide.....	194
13.3 Hacker Highschool.....	195
13.4 The Bad People Project.....	195
13.5 Business Integrity Testing.....	195
13.6 Security Operations Maturity Architecture.....	195
Chapter 14 – Making the STAR.....	197
Chapter 15 - License.....	208
The Open Methodology License 3.....	208

