

Contents

1	Network Attacks	1
1.1	Attack Taxonomies	2
1.2	Probes	4
1.2.1	IPSweep and PortSweep	5
1.2.2	NMap	5
1.2.3	MScan	5
1.2.4	SAINT	5
1.2.5	Satan	6
1.3	Privilege Escalation Attacks	6
1.3.1	Buffer Overflow Attacks	7
1.3.2	Misconfiguration Attacks	7
1.3.3	Race-condition Attacks	8
1.3.4	Man-in-the-Middle Attacks	9
1.3.5	Social Engineering Attacks	10
1.4	Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks	11
1.4.1	Detection Approaches for DoS and DDoS Attacks	11
1.4.2	Prevention and Response for DoS and DDoS Attacks	13
1.4.3	Examples of DoS and DDoS Attacks	14
1.5	Worms Attacks	16
1.5.1	Modeling and Analysis of Worm Behaviors	16
1.5.2	Detection and Monitoring of Worm Attacks	17
1.5.3	Worms Containment	18
1.5.4	Examples of Well Known Worm Attacks	19
1.6	Routing Attacks	19
1.6.1	OSPF Attacks	20
1.6.2	BGP Attacks	21
	References	22

2	Detection Approaches	27
2.1	Misuse Detection	27
2.1.1	Pattern Matching	28
2.1.2	Rule-based Techniques	29
2.1.3	State-based Techniques	31
2.1.4	Techniques based on Data Mining	34
2.2	Anomaly Detection	34
2.2.1	Advanced Statistical Models	36
2.2.2	Rule based Techniques	37
2.2.3	Biological Models	39
2.2.4	Learning Models	40
2.3	Specification-based Detection	45
2.4	Hybrid Detection	46
	References	49
3	Data Collection	55
3.1	Data Collection for Host-Based IDSs	55
3.1.1	Audit Logs	56
3.1.2	System Call Sequences	58
3.2	Data Collection for Network-Based IDSs	61
3.2.1	SNMP	61
3.2.2	Packets	62
3.2.3	Limitations of Network-Based IDSs	66
3.3	Data Collection for Application-Based IDSs	67
3.4	Data Collection for Application-Integrated IDSs	68
3.5	Hybrid Data Collection	69
	References	69
4	Theoretical Foundation of Detection	73
4.1	Taxonomy of Anomaly Detection Systems	73
4.2	Fuzzy Logic	75
4.2.1	Fuzzy Logic in Anomaly Detection	77
4.3	Bayes Theory	77
4.3.1	Naive Bayes Classifier	78
4.3.2	Bayes Theory in Anomaly Detection	78
4.4	Artificial Neural Networks	79
4.4.1	Processing Elements	79
4.4.2	Connections	82
4.4.3	Network Architectures	83
4.4.4	Learning Process	84
4.4.5	Artificial Neural Networks in Anomaly Detection	85
4.5	Support Vector Machine (SVM)	86
4.5.1	Support Vector Machine in Anomaly Detection	89
4.6	Evolutionary Computation	89
4.6.1	Evolutionary Computation in Anomaly Detection	91

4.7	Association Rules	92
4.7.1	The Apriori Algorithm	93
4.7.2	Association Rules in Anomaly Detection	93
4.8	Clustering	94
4.8.1	Taxonomy of Clustering Algorithms	95
4.8.2	K-Means Clustering	96
4.8.3	Y-Means Clustering	97
4.8.4	Maximum-Likelihood Estimates	98
4.8.5	Unsupervised Learning of Gaussian Data	100
4.8.6	Clustering Based on Density Distribution Functions	101
4.8.7	Clustering in Anomaly Detection	102
4.9	Signal Processing Techniques Based Models	104
4.10	Comparative Study of Anomaly Detection Techniques	109
	References	110
5	Architecture and Implementation	115
5.1	Centralized	115
5.2	Distributed	115
5.2.1	Intelligent Agents	116
5.2.2	Mobile Agents	123
5.3	Cooperative Intrusion Detection	125
	References	126
6	Alert Management and Correlation	129
6.1	Data Fusion	129
6.2	Alert Correlation	131
6.2.1	Preprocess	132
6.2.2	Correlation Techniques	139
6.2.3	Postprocess	145
6.2.4	Alert Correlation Architectures	150
6.2.5	Validation of Alert Correlation Systems	152
6.3	Cooperative Intrusion Detection	153
6.3.1	Basic Principles of Information Sharing	153
6.3.2	Cooperation Based on Goal-tree Representation of Attack Strategies	154
6.3.3	Cooperative Discovery of Intrusion Chain	154
6.3.4	Abstraction-Based Intrusion Detection	155
6.3.5	Interest-Based Communication and Cooperation	155
6.3.6	Agent-Based Cooperation	156
6.3.7	Secure Communication Using Public-key Encryption	157
	References	157

7	Evaluation Criteria	161
7.1	Accuracy	161
7.1.1	False Positive and Negative	162
7.1.2	Confusion Matrix	163
7.1.3	Precision, Recall, and F-Measure	164
7.1.4	ROC Curves	166
7.1.5	The Base-Rate Fallacy	168
7.2	Performance	171
7.3	Completeness	172
7.4	Timely Response	172
7.5	Adaptation and Cost-Sensitivity	175
7.6	Intrusion Tolerance and Attack Resistance	177
7.6.1	Redundant and Fault Tolerance Design	177
7.6.2	Obstructing Methods	179
7.7	Test, Evaluation and Data Sets	180
	References	182
8	Intrusion Response	185
8.1	Response Type	185
8.1.1	Passive Alerting and Manual Response	185
8.1.2	Active Response	186
8.2	Response Approach	186
8.2.1	Decision Analysis	186
8.2.2	Control Theory	189
8.2.3	Game theory	189
8.2.4	Fuzzy theory	190
8.3	Survivability and Intrusion Tolerance	194
	References	197
A	Examples of Commercial and Open Source IDSs	199
A.1	Bro Intrusion Detection System	199
A.2	Prelude Intrusion Detection System	199
A.3	Snort Intrusion Detection System	200
A.4	Ethereal Application - Network Protocol Analyzer	200
A.5	Multi Router Traffic Grapher (MRTG)	201
A.6	Tamandua Network Intrusion Detection System	202
A.7	Other Commercial IDSs	202
	Index	209

Network Intrusion Detection and Prevention

Concepts and Techniques

Ghorbani, A.A.; Lu, W.; Tavallaee, M.

2010, XVIII, 216 p. 20 illus., Hardcover

ISBN: 978-0-387-88770-8