

Intrusion Detection & Response (ID & RS)

Studienarbeit von Uwe Hoffmeister • Christian Klie • Tobias Schmidt



Intrusion Detection & Response

Seminararbeit im SS 2002 (4. Semester Bachelor)

von

Uwe Hoffmeister – 900 1840

Christian Klie – 900 1882

Tobias Schmidt – 900 1883

Intrusion Detection & Response (ID & RS)

Studienarbeit von Uwe Hoffmeister • Christian Klie • Tobias Schmidt

1. Verzeichnisse

1.1. Inhaltsverzeichnis

1.	Verzeichnisse.....	2
1.1.	Inhaltsverzeichnis.....	2
1.2.	Tabellenverzeichnis.....	5
1.3.	Abbildungsverzeichnis.....	5
1.4.	Abkürzungsverzeichnis.....	6
2.	Allgemeine Einführung ins Thema.....	7
3.	Einführung Intrusion Detection Systeme.....	8
3.1.	Motivation für den Einsatz eines Intrusion Detection Systems.....	8
3.1.1.	Bedrohungen für IT Systeme.....	9
3.1.2.	Sicherung von IT Systemen.....	10
3.2.	Typisierung.....	12
3.2.1.	Aufbau eines Intrusion Detection Systems.....	12
3.2.1.1.	Komponente zur Datensammlung.....	13
3.2.1.2.	Datenanalyse.....	14
3.2.1.3.	Ergebnisdarstellung der Auswertung der Auditdaten / Alarmierung.....	15
3.2.2.	Arten von Intrusion Detection Systemen.....	16
3.2.2.1.	Lokale Intrusion Detection Systeme.....	16
3.2.2.2.	Verteilte Intrusion Detection Systeme.....	17
3.2.2.3.	Netzbasierte Intrusion Detection.....	18
3.2.2.4.	Vernetzte Intrusion Detection Systeme.....	19
3.2.3.	Konzepte der Datenauswertung von Intrusion Detection Systemen.....	20
3.2.3.1.	Anomalieerkennung.....	21
3.2.3.2.	Missbrauchserkennung.....	22
3.2.3.3.	Hybrider Einsatz von Anomalie- und Missbrauchserkennung.....	22
3.3.	Zuverlässigkeit von Intrusion Detection Systemen.....	23
3.4.	Maßnahmen und Gegenmaßnahmen eines Intrusion Detection Systems.....	24
3.5.	Auswahlkriterien für ein Intrusion Detection System.....	26
3.6.	Auswahlkriterien für das Intrusion Detection Systems Snort.....	29
3.6.1.	Angriffsszenarien.....	29
3.6.2.	Auditdaten.....	29
3.6.3.	Datenanalyse.....	29
3.6.4.	Architektur.....	30
3.6.5.	Reaktion.....	30
3.6.6.	Benutzerschnittstelle.....	30
3.6.7.	Performanz.....	31
3.6.8.	Dokumentation.....	31

Intrusion Detection & Response (ID & RS)

Studienarbeit von Uwe Hoffmeister • Christian Klie • Tobias Schmidt

3.6.9.	Verfügbarkeit.....	31
3.6.10.	Software/ Hardware.....	31
3.6.11.	Zielumgebung.....	31
3.6.12.	Externe Programme.....	31
4.	Intrusion Detection System Snort.....	32
4.1.	Beschreibung.....	32
4.1.1.	Installation.....	32
4.1.2.	Konfiguration mit Hilfe der grafischen Konsole unter Windows.....	32
4.1.3.	Aufbau von Snort Regeln.....	43
4.1.3.1.	Grundlagen.....	43
4.1.3.2.	Regelköpfe (rule headers).....	44
4.1.3.3.	Options (rule options).....	47
4.1.3.4.	Präprozessoren (preprocessors).....	48
4.1.3.5.	Zusätze.....	50
4.1.3.6.	Ausgaben.....	51
5.	Angriffe.....	54
5.1.	Einleitung.....	54
5.1.1.	Definition.....	54
5.1.2.	Motivation eines Angriffs.....	55
5.1.3.	Sachziele der IT-Sicherheit.....	56
5.2.	Klassifizierung von Angriffsarten.....	58
5.2.1.	Erkundung eines Systems.....	58
5.2.2.	Angriffe auf unterer Systemebene (Protokollebene).....	59
5.2.3.	Angriffe auf oberer Systemebene (Anwendungsebene).....	60
5.2.4.	Angriffe durch interne Wissensträger.....	62
5.2.5.	Denial-of-Service-Angriff.....	63
5.3.	Angriffstools.....	64
5.3.1.	Portscanner: <i>SuperScan</i>	64
5.3.2.	Backdoor: Back Orifice.....	65
5.3.3.	Packet Sniffer: <i>Etherreal</i>	66
5.3.4.	Packet Sniffer: <i>DSniff</i>	67
5.3.5.	Security Scanner: <i>Nessus</i>	69
5.3.6.	Session-Hijacking: <i>Hunt</i>	70
5.4.	Durchführung der Angriffe.....	71
5.4.1.	Portscanner: <i>SuperScan</i>	71
5.4.2.	Backdoor: Back Orifice.....	73
5.4.3.	Network Sniffer: <i>DSniff</i>	77
5.4.4.	Security Scanner: <i>Nessus</i>	79
5.4.5.	Session-Hijacking: <i>Hunt</i>	87
5.5.	Reaktionen des Intrusion Detection Systems.....	89
5.6.	Bewertung der verschiedenen Angriffsmöglichkeiten.....	91
6.	Aktive <i>Gegenangriffe – Reactive Components and Systems</i>	94
6.1.	Einleitung.....	94
6.1.1.	Definitionen.....	96
6.1.2.	Motivation.....	97
6.1.3.	Ziele.....	99

Intrusion Detection & Response (ID & RS)

Studienarbeit von Uwe Hoffmeister • Christian Klie • Tobias Schmidt

6.2.	Software für Gegenangriffe	101
6.2.1.	Anforderungen an Reactive Systeme	102
6.2.2.	Hersteller	103
6.2.3.	Freeware/Shareware	106
6.2.4.	Kommerzielle/Lizenzierte Software.....	108
6.2.5.	Kommerzielle und nichtkommerzielle Software im Vergleich.....	111
6.3.	Gegenangriff.....	113
6.3.1.	Allgemeines	113
6.3.2.	Identifizierung des Angreifers	114
6.3.3.	Ausführung des Gegenangriffs.....	117
6.3.4.	Bewertung von Angriffsmöglichkeiten hinsichtlich der Nutzbarkeit für Reactive Maßnahmen.....	120
6.4.	Ausblick.....	124
7.	Anhang	127
7.1.	Tabellen	127
8.	Literaturverzeichnis	131

Intrusion Detection & Response (ID & RS)

Studienarbeit von Uwe Hoffmeister • Christian Klie • Tobias Schmidt

1.2. Tabellenverzeichnis

Tabelle 1:	Von Snort erkannte Angriffsarten	29
Tabelle 2:	Überblick output moduls	51
Tabelle 3:	Parameterliste XML- Modul	52
Tabelle 4:	Parameterliste des Datenbank- Modul.....	53
Tabelle 5:	Übersicht der Schlüsselworte in Snort	130

1.3. Abbildungsverzeichnis

1.	Lokales Intrusion Detection System.....	16
2.	Verteiltes Intrusion Detection System.....	17
3.	Netzbasieretes Intrusion Detection System.....	18
4.	Programmfenster „General Setup“	33
5.	Programmfenster „IDS Rules“	34
6.	Programmfenster „Logs/Alert – General Setup“	35
7.	Programmfenster „Logs – Log Rotation“	37
8.	Konfiguration WinSnort2HTML.....	38
9.	Beispiel einer HTML- Logdatei	39
10.	Programmfenster „Alarm – Alarm Setup“	40
11.	Programmfenster „Alarm – AlertMail“	41
12.	Programmfenster „Overview“	42
13.	Programmfenster „Superscan“	71
14.	Serversettings in Back Orifice	73
15.	Back Orifice - Serverkonsole	74
16.	PlugIn-Auswahl bei Nessus.....	80
17.	Screenshot Visualroute	116

Intrusion Detection & Response (ID & RS)

Studienarbeit von Uwe Hoffmeister • Christian Klie • Tobias Schmidt

1.4. Abkürzungsverzeichnis

ACK	acknowledgement flag
ASCII	American standard code for information interchange
bzw	beziehungsweise
CDIR	Classes InterDomain Routing
CGI	common gateway interface
CPU	central processing unit
FIN	Final Flag
GRE	Generic Route Encapsulation
HTTP	hypertext transport protocol
HTTPS	hypertext transport protocol secure
ICMP	internet control management protocol
ID	identification
IDS	Intrusion Detection System
IGRP	interior gateway routing protocol
IP	Internet Protocol
IPX	internet packet exchange protocol
IT	Informations Technologie
OSPF	open shortest path first
RIP	routing information protocol
RSH	remote shell
RST	Reset Flag
SMTP	simple mail transfer protocol
SYN	synchronization
TCP	Transfer Control Protocol
UDP	user datagram protocol
URL	uniform resource locator
XML	Extensible Markup Language
z.B.	zum Beispiel

Intrusion Detection & Response (ID & RS)

Studienarbeit von Uwe Hoffmeister • Christian Klie • Tobias Schmidt

2. Allgemeine Einführung ins Thema

Die Sicherheit von IT- Systemen ist in den letzten Jahren zusehends gestiegen. Gründe hierfür liegen zum einen in der globalen Vernetzung von Rechnersystemen und einer immer komplexer werdenden Softwarearchitektur. Als schützenswert erweist sich nicht nur das interne Firmennetz gegenüber Angriffen aus dem eigenen Netz, sondern im zunehmenden Maße auch der Schutz gegen externe Angriffe.

Seitdem IT- Systeme existieren, gibt es Bemühungen, die zum Ziel den Schutz dieser Systeme haben. Allerdings gibt es immer wieder Möglichkeiten, diese Schutzmaßnahmen zu umgehen. Das Interesse an flexiblen und schnell agierenden Systemen zum Schutz von IT- Systemen ist in den letzten Jahren stark gestiegen. Aus diesem Grund, werden Intrusion Detection/ Intrusion Response Systeme entwickelt, um die benötigte Sicherheit zu gewährleisten.

Vorläufer und Basis von Intrusion Detection/ Intrusion Response Systemen sind Auditsysteme, die alle Vorgänge innerhalb eines IT- Systems aufzeichnen und deren Protokolle nachträglich ausgewertet werden. Der Vorteil von Intrusion Detection/ Intrusion Response Systemen liegt in der zeitnahen Auswertung von Auditfiles, um Entscheidungen treffen zu können, die das IT- System sichern.

Diese Arbeit beschäftigt sich mit Intrusion Detection Systemen, Angriffen auf Rechnersysteme und mit einer Möglichkeit zur Intrusion Response/Reactive.