

Inhaltsverzeichnis

Abbildungsverzeichnis	7
Tabellenverzeichnis	9
Listingverzeichnis	10
Abkürzungsverzeichnis	11
1 Einleitung	15
1.1 Ausgangssituation	15
1.2 Forschungsstand	16
1.3 Zielsetzung der Studie	16
1.4 Aufbau der Studie	17
1.5 Notation	17
2 Grundlagen von Exploiting Frameworks und Intrusion Detection Systemen	18
2.1 Grundlegende Begriffe	18
2.1.1 Sicherheitslücke (Vulnerability)	18
2.1.2 Exploit	19
2.1.3 Pufferüberlauf (Buffer Overflow)	21
2.1.4 Shellcode	23
2.1.5 Spoofing	24
2.1.6 Denial of Service	25
2.2 Funktionsweise von Exploiting Frameworks	26
2.2.1 Aufgaben	26
2.2.2 Architektur	27
2.2.3 Metasploit Framework (MSF)	28
2.2.3.1 Architektur	29
2.2.3.2 Benutzerschnittstellen	30
2.3 Funktionsweise von Intrusion Detection Systemen (IDS)	32
2.3.1 Definition Intrusion Detection	32
2.3.2 Definition Intrusion Detection System	32
2.3.3 Taxonomie von IDS	32
2.3.4 Komponenten eines IDS	33

2.3.4.1	Netz-basierte Sensoren	33
2.3.4.2	Host-basierte Sensoren	34
2.3.5	Methoden der Angriffserkennung	35
2.3.5.1	Erkennung von Angriffsmustern	35
2.3.5.2	Anomalieerkennung	35
2.3.6	Intrusion Protection Systeme (IPS)	35
2.3.7	Falschmeldungen (False Positives und False Negatives)	35
2.3.8	Sourcefire Snort (IDS/IPS)	36
2.3.8.1	Architektur und Funktionsweise	36
2.3.8.2	Preprozessoren	37
2.3.8.3	Signaturen	38
3	Konzepte zur Verschleierung von Angriffen	40
3.1	Allgemeine Verschleierungs-Techniken	40
3.1.1	Insertion / Injection	40
3.1.2	Evasion	42
3.1.3	Denial of Service	42
3.1.4	Obfuscation	44
3.2	Angriffstechnik der Sicherungsschicht (OSI-Schicht 2)	44
3.3	Angriffstechniken der Netzwerkschicht (OSI-Schicht 3)	45
3.3.1	Ungültige IP-Header Felder	46
3.3.2	IP Optionen	46
3.3.3	Fragmentierung von IP-Paketen	47
3.4	Angriffstechniken der Transportschicht (OSI-Schicht 4)	49
3.4.1	Ungültige TCP-Header Felder	50
3.4.2	TCP Optionen	50
3.4.3	TCP Stream Reassembly	51
3.4.4	TCP Control Block (TCB)	51
3.5	Angriffstechniken der Anwendungsschicht (OSI-Schicht 5-7)	52
3.5.1	Coding Evasion	52
3.5.2	Directory-Traversal Evasion	52
3.5.3	Evasion durch polymorphen Shellcode	52
4	Verschleierung von Angriffen in Exploiting Frameworks	54
4.1	Verschleierung von Angriffen im Metasploit Framework	54
4.1.1	Implementierte Insertion- und Evasion Techniken	55
4.1.2	Implementierte Obfuscation Techniken	55
4.1.2.1	Verschleierung des Angriffscode	55
4.1.2.2	Verschleierung des Shellcode	57
4.1.3	Filterung von erkennbaren Angriffen auf Clientseite (IPS-Filter Plugin)	58

4.2	Verschleierung von Angriffen in Core Impact	59
4.3	Verschleierung von Angriffen in SAINT exploit	59
5	Bewertung von NIDS unter dem Gesichtspunkt von Evasion Techniken	60
5.1	Bewertungsparameter für Network Intrusion Detection Systeme	60
5.2	Entwurf der Testumgebung	65
5.2.1	Anforderungsanalyse	65
5.2.2	Auswahl der zu evaluierenden Network Intrusion Detection Systeme . .	65
5.2.3	Auswahl der Testverfahren	67
5.2.3.1	Tests der Evasion Techniken der Netzwerk- und Transportschicht	68
5.2.3.2	Tests der Obfuscation Techniken der Anwendungsschicht . . .	74
5.2.4	Konfiguration der Testumgebung	81
5.3	Realisierung der Testumgebung	83
5.3.1	Einrichtung der Virtuellen Maschinen in VirtualBox	83
5.3.1.1	Einrichtung des Metasploit Exploiting Frameworks	83
5.3.1.2	Einrichtung der Netzwerkkomponenten (Hub, Router)	84
5.3.1.3	Einrichtung des NIDS Snort	87
5.3.1.4	Einrichtung des NIDS / IPS Untangle	89
5.3.1.5	Einrichtung des NIDS Bro	91
5.3.1.6	Einrichtung des NIDS Securepoint	92
5.3.1.7	Einrichtung der Zielsysteme	92
5.3.2	Integration der Cisco Appliances	92
5.3.2.1	Einrichtung des Cisco 2620 Routers (IP Plus)	93
5.3.2.2	Einrichtung des Cisco 4215 Sensors	94
5.4	Durchführung der Tests	97
5.5	Auswertung der Testergebnisse	98
5.5.1	Auswertung der Protokolldateien	98
5.5.2	Darstellung der Testergebnisse	100
5.5.3	Zusammenfassende Bewertung der NIDS	103
5.5.4	Zusammenfassung	105
6	Ansätze zur verbesserten Erkennung von verschleierten Angriffen	109
6.1	Maschinelles Lernen für Echtzeit-Intrusion-Detection	109
6.2	Verbesserung von NIDS durch Host-basierte Informationen	109
6.3	Verwendung von Grafikprozessoren zur Mustererkennung	110
6.4	Dynamische Taint-Analyse zur Erkennung von Angriffen	111
6.5	Normalisierung von Netzverkehr zur Beseitigung von Mehrdeutigkeiten	112
6.6	Active Mapping	113
7	Zusammenfassung und Fazit	115

Literaturverzeichnis	117
A Bewertungsparameter der evaluierten NIDS	122
B Konfigurationen	129
B.1 Snort Version 2.8.4.1 - Konfigurationsdatei snort.conf	129
B.2 Cisco 4215 IDS Sensor - Konfiguration	133
C Quellcode	135
C.1 Metasploit Framework Obfuscation Test Script (msfauto.sh)	135
C.2 Metasploit IDS Filter Plugin (ids_filter.rb)	145
C.3 Metasploit Exploit ms08_067_netapi Modulinformationen	148
C.4 Metasploit Verschleierungs-Optionen des Moduls ms08_067_netapi	151
Stichwortverzeichnis	153