

Thomas Stein

Intrusion Detection System Evasion durch Obfuscation in Exploiting Frameworks

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2009 Diplom.de
ISBN: 9783836636759

Thomas Stein

Intrusion Detection System Evasion durch Obfuscation in Exploiting Frameworks

Thomas Stein

Intrusion Detection System Evasion durch Obfuscation in Exploiting Frameworks

Thomas Stein

Intrusion Detection System Evasion durch Obfuscation in Exploiting Frameworks

ISBN: 978-3-8366-3675-9

Herstellung: Diplomica® Verlag GmbH, Hamburg, 2009

Zugl. Fachhochschule Bonn-Rhein-Sieg, Bonn, Deutschland, Bachelorarbeit, 2009

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden und der Verlag, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

© Diplomica Verlag GmbH

<http://www.diplomica.de>, Hamburg 2009

Inhaltsverzeichnis

Abbildungsverzeichnis	6
Tabellenverzeichnis	8
Listingverzeichnis	9
Abkürzungsverzeichnis	10
1 Einleitung	14
1.1 Ausgangssituation	14
1.2 Forschungsstand	15
1.3 Zielsetzung der Arbeit	15
1.4 Aufbau der Arbeit	16
1.5 Notation	16
2 Grundlagen von Exploiting Frameworks und Intrusion Detection Systemen	17
2.1 Grundlegende Begriffe	17
2.1.1 Sicherheitslücke (Vulnerability)	17
2.1.2 Exploit	18
2.1.3 Pufferüberlauf (Buffer Overflow)	20
2.1.4 Shellcode	22
2.1.5 Spoofing	23
2.1.6 Denial of Service	24
2.2 Funktionsweise von Exploiting Frameworks	25
2.2.1 Aufgaben	25
2.2.2 Architektur	26
2.2.3 Metasploit Framework (MSF)	27
2.2.3.1 Architektur	28
2.2.3.2 Benutzerschnittstellen	29
2.3 Funktionsweise von Intrusion Detection Systemen (IDS)	31
2.3.1 Definition Intrusion Detection	31
2.3.2 Definition Intrusion Detection System	31
2.3.3 Taxonomie von IDS	31
2.3.4 Komponenten eines IDS	32

2.3.4.1	Netz-basierte Sensoren	32
2.3.4.2	Host-basierte Sensoren	33
2.3.5	Methoden der Angriffserkennung	34
2.3.5.1	Erkennung von Angriffsmustern	34
2.3.5.2	Anomalieerkennung	34
2.3.6	Intrusion Protection Systeme (IPS)	34
2.3.7	Falschmeldungen (False Positives und False Negatives)	34
2.3.8	Sourcefire Snort (IDS/IPS)	35
2.3.8.1	Architektur und Funktionsweise	35
2.3.8.2	Preprozessoren	36
2.3.8.3	Signaturen	37
3	Konzepte zur Verschleierung von Angriffen	39
3.1	Allgemeine Verschleierungs-Techniken	39
3.1.1	Insertion / Injection	39
3.1.2	Evasion	41
3.1.3	Denial of Service	41
3.1.4	Obfuscation	43
3.2	Angriffstechnik der Sicherungsschicht (OSI-Schicht 2)	43
3.3	Angriffstechniken der Netzwerkschicht (OSI-Schicht 3)	44
3.3.1	Ungültige IP-Header Felder	45
3.3.2	IP Optionen	45
3.3.3	Fragmentierung von IP-Paketen	46
3.4	Angriffstechniken der Transportschicht (OSI-Schicht 4)	48
3.4.1	Ungültige TCP-Header Felder	49
3.4.2	TCP Optionen	49
3.4.3	TCP Stream Reassembly	50
3.4.4	TCP Control Block (TCB)	50
3.5	Angriffstechniken der Anwendungsschicht (OSI-Schicht 5-7)	51
3.5.1	Coding Evasion	51
3.5.2	Directory-Traversal Evasion	51
3.5.3	Evasion durch polymorphen Shellcode	51
4	Verschleierung von Angriffen in Exploiting Frameworks	53
4.1	Verschleierung von Angriffen im Metasploit Framework	53
4.1.1	Implementierte Insertion- und Evasion Techniken	54
4.1.2	Implementierte Obfuscation Techniken	54
4.1.2.1	Verschleierung des Angriffscodes	54
4.1.2.2	Verschleierung des Shellcode	56
4.1.3	Filterung von erkennbaren Angriffen auf Clientseite (IPS-Filter Plugin)	57

4.2	Verschleierung von Angriffen in Core Impact	58
4.3	Verschleierung von Angriffen in SAINT exploit	58
5	Bewertung von NIDS unter dem Gesichtspunkt von Evasion Techniken	59
5.1	Bewertungsparameter für Network Intrusion Detection Systeme	59
5.2	Entwurf der Testumgebung	64
5.2.1	Anforderungsanalyse	64
5.2.2	Auswahl der zu evaluierenden Network Intrusion Detection Systeme . .	64
5.2.3	Auswahl der Testverfahren	66
5.2.3.1	Tests der Evasion Techniken der Netzwerk- und Transportschicht	67
5.2.3.2	Tests der Obfuscation Techniken der Anwendungsschicht . . .	73
5.2.4	Konfiguration der Testumgebung	80
5.3	Realisierung der Testumgebung	82
5.3.1	Einrichtung der Virtuellen Maschinen in VirtualBox	82
5.3.1.1	Einrichtung des Metasploit Exploiting Frameworks	82
5.3.1.2	Einrichtung der Netzwerkkomponenten (Hub, Router)	83
5.3.1.3	Einrichtung des NIDS Snort	86
5.3.1.4	Einrichtung des NIDS / IPS Untangle	88
5.3.1.5	Einrichtung des NIDS Bro	90
5.3.1.6	Einrichtung des NIDS Securepoint	91
5.3.1.7	Einrichtung der Zielsysteme	91
5.3.2	Integration der Cisco Appliances	91
5.3.2.1	Einrichtung des Cisco 2620 Routers (IP Plus)	92
5.3.2.2	Einrichtung des Cisco 4215 Sensors	93
5.4	Durchführung der Tests	96
5.5	Auswertung der Testergebnisse	97
5.5.1	Auswertung der Protokolldateien	97
5.5.2	Darstellung der Testergebnisse	99
5.5.3	Zusammenfassende Bewertung der NIDS	102
5.5.4	Zusammenfassung	104
6	Ansätze zur verbesserten Erkennung von verschleierte n Angriffen	108
6.1	Maschinelles Lernen für Echtzeit-Intrusion-Detection	108
6.2	Verbesserung von NIDS durch Host-basierte Informationen	108
6.3	Verwendung von Grafikprozessoren zur Mustererkennung	109
6.4	Dynamische Taint-Analyse zur Erkennung von Angriffen	110
6.5	Normalisierung von Netzverkehr zur Beseitigung von Mehrdeutigkeiten	111
6.6	Active Mapping	112
7	Zusammenfassung und Fazit	114

Literaturverzeichnis	116
Anhang	123
A Dokumente	123
A.1 Inhaltsübersicht der DVD	123
A.2 Bewertungsparameter der evaluierten NIDS	124
B Konfigurationen	129
B.1 Snort Version 2.8.4.1 - Konfigurationsdatei snort.conf	129
B.2 Cisco 4215 IDS Sensor - Konfiguration	132
C Quellcode	133
C.1 Metasploit Framework Obfuscation Test Script (msfauto.sh)	133
C.2 Metasploit IDS Filter Plugin (ids_filter.rb)	141
C.3 Metasploit Exploit ms08_067_netapi Modulinformationen	143
C.4 Metasploit Verschleierungs-Optionen des Moduls ms08_067_netapi	145
Stichwortverzeichnis	147

Abbildungsverzeichnis

2.1	Lebenszyklus von Sicherheitslücken (Vulnerability Lifecycle)	20
2.2	Exploiting Framework - Komponenten	26
2.3	Metasploit Framework - Projektlogo	27
2.4	Metasploit Framework - Architektur	28
2.5	Metasploit Framework - Benutzerinterface <code>msfgui</code> nach dem Programmstart . .	30
2.6	Intrusion Detection System - Taxonomie	32
2.7	Snort - Projektlogo	35
2.8	Snort - Architektur	36
2.9	Snort - Aufgaben mehrerer Preprozessoren	37
2.10	Snort - Bestandteile des Snort Regel-Headers	38
3.1	Angriffstechnik - Insertion (des Buchstaben X)	40
3.2	Angriffstechnik - Evasion (des Buchstaben A)	41
3.3	Insertion Angriff auf der Sicherungsschicht (Link Layer)	43
3.4	Internet Protocol (IP) - Internet Datagram Header	44
3.5	Reassembly	46
3.6	Überlappung der Daten von Fragmenten	47
3.7	Transmission Control Protocol (TCP) - TCP Header Format	48
4.1	MSF - Auswahlmöglichkeiten der implementierten Obfuscation Techniken . . .	53
4.2	Core Impact V9 - Erweiterte Modulparameter	58
5.1	Konfiguration der Testumgebung	81
5.2	Untangle - Status der installierten Komponenten	89
5.3	Untangle - Übersicht der vorhandenen Signaturen	90
5.4	Untangle - Status der installierten IPS Komponente	90
5.5	Cisco IPS Device Manager - Signaturübersicht	95
5.6	Cisco IPS Device Manager - Event Viewer	96
5.7	Virtualbox - Übersicht der Virtuellen Maschinen	96
5.8	Testauswertung - Ausführungserfolg der verschleierte Exploits	100
5.9	Testauswertung der verschleierte Angriffe - Ergebnisse der Tests 1-5	105
(a)	Test 01 - DCERPC::fake_bind_multi	105
(b)	Test 02 - DCERPC::fake_bind_multi_append	105
(c)	Test 03 - DCERPC::fake_bind_multi_prepend	105

(d)	Test 04 - DCERPC::max_frag_size	105
(e)	Test 05 - DCERPC::smb_pipeio	105
5.10	Testauswertung der verschleierte Angriffe - Ergebnisse der Tests 6-10	106
(a)	Test 06 - SMB::obscure_trans_pipe_level	106
(b)	Test 07 - SMB::pad_data_level	106
(c)	Test 08 - SMB::pad_file_level	106
(d)	Test 09 - SMB::pipe_evasion	106
(e)	Test 10 - SMB::pipe_read_max_size	106
5.11	Testauswertung der verschleierte Angriffe - Ergebnisse der Tests 11-15	107
(a)	Test 11 - SMB::pipe_read_min_size	107
(b)	Test 12 - SMB::pipe_write_max_size	107
(c)	Test 13 - SMB::pipe_write_min_size	107
(d)	Test 14 - TCP::max_send_size	107
(e)	Test 15 - TCP::send_delay	107
6.1	Gnort - Architektur	109
6.2	Argos - Architektur	110
6.3	Normalisierer - Position im Netz	111

Tabellenverzeichnis

2.1	Metasploit Exploiting Framework - Versionsvergleich	28
2.2	Metasploit Exploiting Framework - Übersicht der Benutzerschnittstellen	30
2.3	IDS - Erkennungsmatrix	35
3.1	Verhalten mehrerer Betriebssysteme bei Überlappungen in Fragmenten	47
4.1	MSF - Implementierte Insertion- und Evasion Techniken	54
4.2	MSF - Implementierte Obfuscation Optionen für das HTTP	55
4.3	MSF - Implementierte Obfuscation Optionen für das SMB Protokoll	55
4.4	MSF - Implementierte Obfuscation Optionen für das DCERPC Protokoll	56
5.1	NIDS - Bewertungsparameter	63
5.2	Intrusion Detection Systeme - Marktübersicht	65
5.3	Evaluationsgegenstand - Liste der zu evaluierenden NIDS	66
5.4	MSF - Modulooptionen des ms08_067_netapi Exploit-Moduls	76
5.5	Metasploit - Paketabhängigkeiten	83
5.6	Testauswertung - Ergebnisse der mittels fragroute verschleierte Angriffe	100
5.7	Testauswertung - Ergebnisse der durch das MSF verschleierte Angriffe	101
5.8	Testauswertung - Kombination mehrerer Obfuscation-Optionen im MSF	102
5.9	NIDS - Bewertungsparameter	104
A.1	NIDS - Bewertungsparameter	128

Listingverzeichnis

2.1	Beispielprogramm in der Programmiersprache C [Burns et al. 2007]	21
2.2	Ausnutzen des Buffer Overflows im Beispielprogramm [Burns et al. 2007]	21
2.3	Deassemblierung - Umwandlung der Opcodes in Assemblercode [Burns et al. 2007]	22
2.4	Linux x86 Shellcode der /bin/bash ausführt in einem C Programm [Burns et al. 2007]	23
2.5	Snort - Test-Regel zur Erkennung von Zugriffen auf FTP-Server	38
4.1	MSF - Enthaltene NOP Generatoren	56
4.2	MSF - Enthaltene Payload Encoder	57
4.3	MSF - Ausschnitt des IPS-Filter Plugin	57
5.1	Fragrouter - Übersicht der Optionen	67
5.2	Fragroute - Übersicht der Optionen	68
5.3	Fragroute - Regeldatei mit IP Fragmentierung (16 Byte Payload Länge)	70
5.4	Ping - ICMP Echo Request mit 128 Byte Daten	70
5.5	Tcpdump - Aufzeichnung des Netzverkehrs: Test 1	71
5.6	RP Filter - Deaktivierung der Quell-Validierung im Kernel	71
5.7	Fragroute - Eintrag in der Routing-Tabelle	71
5.8	Fragroute - Ausgabe der durchgeführten Fragmentierung von IP-Paketen	72
5.9	Tcpdump - Aufzeichnung des Netzverkehrs: Test 2	72
5.10	Tcpdump - Aufzeichnung des Netzverkehrs: Test 3	73
5.11	Tcpdump - Aufzeichnung des Netzverkehrs: Test 4	73
5.12	Metasploit Command Line Interface - Befehl zur Ausgabe aller Exploits	74
5.13	Metasploit Command Line Interface - Ausschnitt der Ausgabe aller Exploits . .	74
5.14	Metasploit Framework - Übersicht der Modulfunktionen	74
5.15	Metasploit Framework Command Line Interface - Aufrufsyntax	75
5.16	Metasploit Framework - Übersicht der Modulooptionen	75
5.17	Metasploit Command Line Interface - Aufruf ohne Verschleierungs-Optionen . .	76
5.18	Metasploit Command Line Interface - Ausgabe der zum Exploit-Modul kompati- blen Payloads	77
5.19	Metasploit Command Line Interface - Übersicht der Modulooptionen nach der Auswahl des Payloads	78
5.20	Übergabeparameter für die Protokollierung auf dem Ziel-IT-System	78
5.21	Metasploit Command Line Interface - Aufruf mit Verschleierungs-Optionen . .	79
5.22	Automatisierungskript - Protokolleintrag	79

5.23	Automatisierungsskript - Funktion zum Aufruf des msfcli	80
5.24	Automatisierungsskript - Aufruf des msfcli mit Verschleierungs-Optionen	81
5.25	Metasploit - Installation der benötigten Softwarepakete	82
5.26	Metasploit - Subversion Checkout	83
5.27	Metasploit - Subversion Checkout	84
5.28	bridge-utils - Konfiguration der Bridge	84
5.29	Aktivierung des Routings im Linux-Kernel	85
5.30	Konfiguration der Netzwerkschnittstellen	85
5.31	Snort - Installation der benötigten Softwarepakete	86
5.32	Snort - Befehle zur Kompilierung des Quellcodes	86
5.33	Snort - Einrichtung der Benutzer und Verzeichnisse	87
5.34	Snort - Ausschnitt der Umgebungsvariablen	88
5.35	Snort - Aufruf mit Konfigurationsparametern	88
5.36	Untangle - Regel: Potentially Bad Traffic (Index of /cgi-bin/ response)	89
5.37	Untangle - Test-Signatur: Erkennung von TCP Netzverkehr	89
5.38	Bro IDS - Quellcode	91
5.39	Bro IDS - Quellcode	91
5.40	Cisco 2620 Router (IP Plus) - IP Audit Optionen	92
5.41	Cisco 2620 Router (IP Plus) - Einrichtung	92
5.42	Cisco 2620 Router (IP Plus) - Ausschnitt der Konsolenausgabe mit Alarmmeldungen	93
5.43	Cisco 4215 Sensor - Fehlermeldung	93
5.44	Cisco 4215 Sensor - Status der Kernkomponenten	94
5.45	Cisco 4215 Sensor - Grundkonfiguration	94
5.46	VM Metasploit - Ausgabe des Automatisierungsskriptes während der Tests	98
5.47	Snort - Logeintrag eines erkannten Angriffs	98
5.48	Tcpdump - Ausgabe der Statistik des aufgezeichneten Netzverkehrs	98
5.49	Windows XP SP3 - Protokolleintrag auf dem Zielsystem	99
5.50	Auswertung der Protokolldateien	99
B.1	Snort Version 2.7.0 Konfigurationsdatei snort.conf	129
B.2	Cisco 4215 IDS Sensor - Konfiguration	132
C.1	Metasploit Framework Obfuscation Test Script (msfauto.sh)	133
C.2	Metasploit IDS Filter Plugin (ids_filter.rb) [Metasploit LLC 2009]	141
C.3	Metasploit Exploit ms08_067_netapi Modulinformationen [Metasploit LLC 2009]	143
C.4	Metasploit Verschleierungs-Optionen des Moduls ms08_067_netapi [Metasploit LLC 2009]	145

Abkürzungsverzeichnis

ASCII	American Standard Code for Information Interchange
ACID	Analysis Console for Intrusion Databases
ARP	Address Resolution Protocol
ACK	Acknowledgment
AUX	Auxiliary
APT	Advanced Paket Manager
Bit	Binary Digit
BSD	Berkeley Software Distribution
BSI	Bundesamt für Sicherheit in der Informationstechnik
BID	Bugtraq Identifier
CGI	Common Gateway Interface
CIDR	Classless Inter-Domain Routing
CVE	Common Vulnerabilities and Exposures
CERT	Computer Emergency Response Team
DB	Datenbank
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
DLL	Dynamic Link Library
DCE	Distributed Computing Environment
EXE	Executable
FE	Front End
FIN	Finish
FP	False positive
FN	Front negative
GPL	GNU General Public License
GUI	Graphical User Interface
GNU	GNU's Not Unix
GTK	GNU Image Manipulation Program Toolkit
HIDS	Host-based Intrusion Detection System
HTML	Hyper Text Markup Language
ICMP	Internet Control Message Protocol