

Inhaltsverzeichnis

Danksagung.....	19
Die Autoren.....	21
Geleitwort.....	25
 Vorwort.....	 27
Zielpublikum.....	28
Voraussetzungen.....	29
Der Aufbau dieses Buches.....	30
Hinweis zu IP-Adressen.....	32
Begleitwebsite.....	33
Unterstützung für wohltätige Organisationen.....	33
Rural Technology Fund.....	33
Hackers for Charity.....	33
Kiva 34	
Hope for the Warriors®.....	34
Autism Speaks.....	34
Kontakt.....	35
 1. Network Security Monitoring in der Praxis.....	 37
1.1 Kernbegriffe des Network Security Monitoring.....	39
1.1.1 Schützenswerte Güter.....	39
1.1.2 Angreifer.....	39
1.1.3 Schwachstelle.....	40
1.1.4 Exploit.....	40
1.1.5 Risiko.....	40

1.1.6	Anomalie.....	40
1.1.7	Zwischenfall.....	41
1.2	Intrusion Detection	41
1.3	Network Security Monitoring	42
1.4	Schwachstellen- und bedrohungsorientierte Verteidigung im Vergleich..	45
1.5	Der NSM-Zyklus: Erfassung, Erkennung und Analyse.....	46
1.5.1	Erfassung.....	47
1.5.2	Erkennung	47
1.5.3	Analyse	48
1.6	Kritik an NSM	48
1.7	Die Analytiker	49
1.7.1	Wichtige Fähigkeiten.....	50
1.7.2	Einteilung von Analytikern	52
1.7.3	Messen des Erfolgs.....	53
1.8	Security Onion	57
1.8.1	Installation.....	57
1.8.2	Security Onion aktualisieren.....	59
1.8.3	NSM-Dienste einrichten.....	59
1.8.4	Security Onion testen	60
1.9	Zusammenfassung.....	62

Teil 1: Erfassung **63**

2. Die Datenerfassung planen	65
2.1 Applied Collection Framework (ACF)	66
2.1.1 Bedrohungen identifizieren.....	67
2.1.2 Das Risiko quantifizieren	69
2.1.3 Datenquellen identifizieren.....	70
2.1.4 Die Erfassung eingrenzen.....	70

2.2	Fallstudie: Onlinehändler	73
2.2.1	Bedrohungen der Organisation identifizieren	74
2.2.2	Das Risiko quantifizieren	75
2.2.3	Datenquellen identifizieren	77
2.2.4	Die Erfassung eingrenzen	81
2.3	Zusammenfassung	83
3.	Sensoren	85
3.1	NSM-Datentypen	86
3.1.1	Paketdaten (FPC)	86
3.1.2	Sitzungsdaten	86
3.1.3	Statistische Daten	87
3.1.4	Paketstringdaten (PSTR)	87
3.1.5	Protokolldaten	87
3.1.6	Alarmdaten	87
3.2	Sensortypen	89
3.2.1	Nur Erfassung	89
3.2.2	Halbzyklus	89
3.2.3	Vollzyklus	89
3.3	Sensorhardware	90
3.3.1	CPU	91
3.3.2	Arbeitsspeicher	92
3.3.3	Festplattenplatz	93
3.3.4	Netzwerkschnittstellen	96
3.3.5	Lastenausgleich: Anforderungen für Socketpuffer	98
3.3.6	SPAN-Ports und Netzwerk-Taps im Vergleich	99
3.4	Das Betriebssystem des Sensors	104

3.5	Platzierung von Sensoren	104
3.5.1	Die richtigen Ressourcen nutzen	105
3.5.2	Ein- und Austrittspunkte	105
3.5.3	Sichtbarkeit interner IP-Adressen	107
3.5.4	Nähe zu kritischen Elementen	110
3.5.5	Sichtfelddiagramme der Sensoren aufstellen	111
3.6	Den Sensor absichern	113
3.6.1	Betriebssystem- und Softwareaktualisierungen	114
3.6.2	Das Betriebssystem absichern	114
3.6.3	Eingeschränkter Internetzugriff	115
3.6.4	Minimale Softwareinstallation	115
3.6.5	VLAN-Segmentierung	115
3.6.6	Host-IDS	116
3.6.7	Zwei-Faktor-Authentifizierung	116
3.6.8	Netzwerk-IDS	116
3.7	Zusammenfassung	117
4.	Sitzungsdaten	119
4.1	Flussdatensätze	120
4.1.1	NetFlow	124
4.1.2	IPFIX	125
4.1.3	Andere Flusstypen	125
4.2	Sitzungsdaten erfassen	126
4.2.1	Hardwareseitige Generierung	126
4.2.2	Softwareseitige Generierung	127
4.3	Flussdaten mit SiLK erfassen und analysieren	128
4.3.1	Das Packsystem von SiLK	129
4.3.2	Flusstypen in SiLK	130
4.3.3	Die Analysesuited von SiLK	131

4.3.4	SiLK in Security Onion installieren	132
4.3.5	Flussdaten mit Rwfiler filtern	132
4.3.6	Verketteten von Analysetools.....	134
4.3.7	Zusätzliche Werkzeuge und Dokumentation	138
4.4	Flussdaten mit Argus erfassen und analysieren	138
4.4.1	Architektur.....	139
4.4.2	Merkmale.....	139
4.4.3	Grundlegender Datenabruf	140
4.4.4	Weitere Informationen über Argus	142
4.5	Überlegungen zur Speicherung von Sitzungsdaten.....	142
4.6	Zusammenfassung.....	144
5.	FPC-Daten.....	145
5.1	Dumpcap	147
5.2	Daemonlogger	149
5.3	Netsniff-NG	150
5.4	Das passende FPC-Erfassungswerkzeug auswählen	152
5.5	Die FPC-Datenerfassung planen.....	153
5.5.1	Speicherplatz.....	153
5.5.2	Den Durchsatz an der Sensorschnittstelle mit Netsniff-NG und lfpps berechnen	155
5.5.3	Den Durchsatz an der Sensorschnittstelle mithilfe von Sitzungsdaten berechnen	156
5.6	Den Speicherbedarf für FPC-Daten senken	159
5.6.1	Dienste ausschließen.....	159
5.6.2	Kommunikation zwischen bestimmten Hosts ausschließen	161
5.7	Die Aufbewahrung der FPC-Daten verwalten.....	163
5.7.1	Aufbewahrung nach Zeit	164
5.7.2	Aufbewahrung nach Umfang.....	164
5.8	Zusammenfassung.....	169

6. Paketstringdaten.....	171
6.1 Was sind Paketstringdaten?.....	172
6.2 PSTR-Datenerfassung	174
6.2.1 PSTR-Daten manuell generieren	176
6.2.2 URLsnarf	177
6.2.3 Http pry.....	178
6.2.4 Justniffer	181
6.3 PSTR-Daten anzeigen.....	186
6.3.1 Logstash	186
6.3.2 Roh textzerlegung mit BASH-Tools.....	195
6.4 Zusammenfassung.....	198

Teil 2: Erkennung 199

7. Erkennungsmechanismen, Einbruchsindikatoren und Signaturen.....	201
7.1 Erkennungsmechanismen.....	201
7.2 Einbruchsindikatoren und Signaturen.....	203
7.2.1 Host- und Netzwerkindikatoren	204
7.2.2 Statische Indikatoren	205
7.2.3 Variable Indikatoren.....	208
7.2.4 Evolution von Indikatoren und Signaturen	210
7.2.5 Signaturen optimieren	212
7.2.6 Entscheidende Kontextinformationen für Indikatoren und Signaturen ..	214
7.3 Indikatoren und Signaturen verwalten	216
7.3.1 Einfache Verwaltung von Indikatoren und Signaturen mit CSV-Dateien ..	217
7.3.2 Masterliste der Indikatoren und Signaturen.....	218
7.3.3 Revisionstabelle für Indikatoren und Signaturen	221

7.4	Frameworks für Indikatoren und Signaturen	223
7.4.1	OpenIOC	223
7.4.2	STIX	226
7.5	Zusammenfassung.....	228
8.	Reputationsgestützte Erkennung	229
8.1	Öffentliche Reputationslisten.....	230
8.1.1	Gängige öffentliche Reputationslisten	231
8.1.2	Häufig auftretende Probleme bei der Verwendung öffentlicher Reputationslisten.....	236
8.2	Automatisieren der reputationsgestützten Erkennung.....	239
8.2.1	Manuelles Abrufen und Erkennen mit BASH-Skripten.....	239
8.2.2	Collective Intelligence Framework (CIF).....	245
8.2.3	Reputationsgestützte IP-Adressenerkennung mit Snort	249
8.2.4	Reputationsgestützte IP-Adressenerkennung mit Suricata	251
8.2.5	Reputationserkennung mit Bro	254
8.3	Zusammenfassung.....	258
9.	Signaturgestützte Erkennung mit Snort und Suricata	261
9.1	Snort.....	262
9.1.1	Die Architektur von Snort.....	263
9.2	Suricata	265
9.2.1	Die Architektur von Suricata	266
9.3	IDS-Engines in Security Onion austauschen.....	268
9.4	Snort und Suricata initialisieren.....	269
9.5	Snort und Suricata konfigurieren	272
9.5.1	Variablen.....	273
9.5.2	Regelsätze definieren	277
9.5.3	Alarmausgabe.....	284

9.5.4	Snort-Präprozessoren	287
9.5.5	Zusätzliche Befehlszeilenargumente für den NIDS-Modus.....	288
9.6	IDS-Regeln	290
9.6.1	Aufbau von Regeln	290
9.6.2	Optimierung von Regeln	308
9.7	Snort- und Suricata-Alarme anzeigen.....	316
9.7.1	Snorby	317
9.7.2	Sguil	318
9.8	Zusammenfassung.....	318
10.	Bro.....	319
10.1	Grundprinzipien von Bro	320
10.2	# ausführen.....	322
10.3	Bro-Protokolle.....	322
10.4	Eigene Erkennungswerkzeuge mit Bro erstellen	327
10.4.1	Dateien extrahieren	328
10.4.2	Selektive Dateixtraktion.....	330
10.4.3	Dateien aus laufendem Netzwerkverkehr entnehmen.....	332
10.4.4	Bro-Code verpacken.....	335
10.4.5	Konfigurationsoptionen hinzufügen.....	335
10.4.6	Darknet-Überwachung mit Bro.....	338
10.4.7	Das Darknet-Skript erweitern.....	346
10.4.8	Die Standardverarbeitung von Benachrichtigungen aufheben	346
10.4.9	Benachrichtigungen unterbinden, E-Mails senden und Alarme auslösen – auf die einfache Weise	351
10.4.10	Den Bro-Protokollen neue Felder hinzufügen.....	352
10.5	Zuammenfassung	356

11. Anomaliegestützte Erkennung anhand von statistischen Daten.....	357
11.1 Kommunikationsintensive Hosts mit SiLK finden	358
11.2 Diensterkennung mit SiLK.....	362
11.3 Weitere Erkennungsmöglichkeiten mithilfe von Statistiken	368
11.4 Statistiken mit Gnuplot grafisch darstellen	371
11.5 Statistiken mit Google Charts grafisch darstellen	375
11.6 Statistiken mit Afterglow grafisch darstellen.....	380
11.7 Zusammenfassung.....	386
12. Frühwarn-Honeypots zur Erkennung	387
12.1 Frühwarn-Honeypots	388
12.2 Arten von Honeypots	389
12.3 Architektur von Frühwarn-Honeypots.....	390
12.3.1 Phase 1: Die zu simulierenden Geräte und Dienste bestimmen.....	391
12.3.2 Phase 2: Die Platzierung der Honeypots bestimmen.....	391
12.3.3 Phase 3: Alarmierung und Protokollierung entwickeln.....	393
12.4 Honeypotplattformen.....	394
12.4.1 Honeyd	395
12.4.2 Der SSH-Honeypot Kippo.....	399
12.4.3 Tom's Honeypot	404
12.4.4 Honeydocs	407
12.5 Zusammenfassung.....	410

Teil 3: Analyse**411**

13. Paketanalyse	413
13.1 Gestatten: das Paket!.....	414
13.2 Paketmathematik.....	416
13.2.1 Hexdarstellung von Bytes	416
13.2.2 Hexwerte ins Binär- und Dezimalformat umwandeln.....	418
13.2.3 Bytes zählen	419
13.3 Pakete zerlegen	422
13.4 Tcpdump für die NSM-Analyse	428
13.5 Tshark für die Paketanalyse	432
13.6 Wireshark für die NSM-Analyse.....	437
13.6.1 Pakete erfassen	437
13.6.2 Das Format der Zeitanzeige ändern.....	439
13.6.3 Übersicht über die Paketerfassung	440
13.6.4 Protokollhierarchie	441
13.6.5 Endpunkte und Konversationen	442
13.6.6 Streams verfolgen	443
13.6.7 E/A-Diagramm	444
13.6.8 Objekte exportieren	446
13.6.9 Benutzerdefinierte Spalten hinzufügen.....	447
13.6.10 Zerlegungsoptionen für Protokolle einrichten	449
13.6.11 Erfassungs- und Anzeigefilter	450
13.7 Paketfilter	451
13.7.1 Berkeley-Paketfilter (BPF)	451
13.7.2 Anzeigefilter von Wireshark	456
13.8 Zusammenfassung.....	461

14. Aufklärung über Freund und Feind.....	463
14.1 Der Aufklärungszyklus für NSM	463
14.1.1 Definition der Anforderungen	464
14.1.2 Planung.....	465
14.1.3 Erfassung.....	466
14.1.4 Verarbeitung	466
14.1.5 Analyse	467
14.1.6 Weitergabe	467
14.2 Aufklärung über eigene Elemente	467
14.2.1 Anamnese und physische Untersuchung von Netzwerkelementen	468
14.2.2 Ein Bestandsmodell des Netzwerks aufstellen.....	469
14.2.3 PRADS (Passive Real-Time Asset Detection System)	473
14.3 Aufklärung über Bedrohungen.....	480
14.3.1 Recherche über gegnerische Hosts	482
14.3.2 Recherche über schädliche Dateien	492
14.4 Zusammenfassung.....	500
15. Der Analysevorgang	501
15.1 Analysemethoden	502
15.1.1 Relationale Untersuchung.....	502
15.1.2 Differenzielle Diagnose	509
15.1.3 Umsetzen der Analysemethoden	517
15.2 Empfohlene Vorgehensweisen für die Analyse.....	518
15.2.1 Bei Paketen können Sie sich auf nichts verlassen.....	518
15.2.2 Machen Sie sich klar, wie die Daten abstrahiert werden	518
15.2.3 Vier Augen sehen mehr als zwei.....	519
15.2.4 Laden Sie einen Angreifer niemals zum Tanz ein	519
15.2.5 Pakete sind von Natur aus gut	520

15.2.6	Wireshark macht so wenig einen Analytiker wie ein Teleskop einen Astronomen.....	520
15.2.7	Klassifizierung hilft	521
15.2.8	Die Zehnerregel.....	522
15.2.9	Wenn Sie Hufe klappern hören, halten Sie nach Pferden Ausschau – nicht nach Zebras	523
15.3	Morbidität und Mortalität von Zwischenfällen	523
15.3.1	M&M in der Medizin.....	524
15.3.2	M&M in der Informationssicherheit	524
15.4	Zusammenfassung.....	530
A.	Steuerskripte für Security Onion	531
A.1	Befehle auf oberster Ebene.....	531
A.2	Befehle zur Serversteuerung.....	532
A.3	Befehle zur Sensorsteuerung.....	535
B.	Wichtige Dateien und Verzeichnisse von Security Onion	539
B.1	Anwendungsverzeichnisse und Konfigurationsdateien	539
B.2	Verzeichnisse für Sensordaten	541
C.	Paketheader	543
D.	Umrechnungstabelle Dezimalzahlen/Hex/ASCII.....	549
	Stichwortverzeichnis	551