

Alexander Geschonneck

Computer-Forensik

Systemeinbrüche erkennen, ermitteln, aufklären



dpunkt.verlag

Inhalt

| | |
|--|-----------|
| Einleitung | 1 |
| Wer sollte dieses Buch lesen? | 2 |
| Was lernt man in diesem Buch? | 4 |
| Was lernt man in diesem Buch nicht? | 4 |
| Wie liest man dieses Buch? | 5 |
| 1 Bedrohungssituation | 9 |
| 1.1 Bedrohung und Wahrscheinlichkeit | 9 |
| 1.2 Risikoverteilung | 10 |
| 1.3 Motivation der Täter | 14 |
| 1.4 Innentäter vs. Außentäter | 19 |
| 1.5 Bestätigung durch die Statistik? | 21 |
| 1.6 Computerkriminalität | 23 |
| 2 Ablauf von Angriffen | 25 |
| 2.1 Typischer Angriffsverlauf | 25 |
| 2.1.1 Footprinting | 25 |
| 2.1.2 Port- und Protokollscan | 26 |
| 2.1.3 Enumeration | 26 |
| 2.1.4 Exploiting/Penetration | 27 |
| 2.1.5 Hintertüren einrichten | 27 |
| 2.1.6 Spuren verwischen | 28 |
| 2.2 Beispiel eines Angriffs | 28 |
| 3 Incident Response als Grundlage der Computer-Forensik | 37 |
| 3.1 Der Incident-Response-Prozess | 37 |
| 3.2 Organisatorische Vorbereitungen | 38 |
| 3.3 Zusammensetzung des Response-Teams | 39 |
| 3.4 Incident Detection: Systemanomalien entdecken | 41 |
| 3.4.1 Netzseitige Hinweise | 42 |
| 3.4.2 Serverseitige Hinweise | 42 |
| 3.4.3 Intrusion-Detection-Systeme | 43 |
| 3.4.4 Externe Hinweise | 44 |
| 3.5 Incident Detection: Ein Vorfall wird gemeldet | 45 |
| 3.6 Sicherheitsvorfall oder Betriebsstörung? | 48 |
| 3.7 Wahl der Response-Strategie | 52 |
| 3.8 Reporting und Manöverkritik | 53 |

| | | |
|----------|--|------------|
| 4 | Einführung in die Computer-Forensik | 55 |
| 4.1 | Ziele einer Ermittlung | 55 |
| 4.2 | Phasen der Ermittlung | 56 |
| 4.3 | Welche Erkenntnisse kann man gewinnen? | 57 |
| 4.4 | Wie geht man korrekt mit Beweismitteln um? | 64 |
| 4.4.1 | Juristische Bewertung der Beweissituation | 65 |
| 4.4.2 | Datenschutz | 67 |
| 4.4.3 | Welche Daten können erfasst werden? | 69 |
| 4.4.4 | Durchgeführte Aktionen dokumentieren | 70 |
| 4.4.5 | Beweise dokumentieren | 71 |
| 4.4.6 | Mögliche Fehler bei der Beweissammlung | 73 |
| 4.5 | Flüchtige Daten sichern: Sofort speichern | 75 |
| 4.6 | Speichermedien sichern: forensische Duplikation | 78 |
| 4.6.1 | Wann ist eine forensische Duplikation sinnvoll? .. | 78 |
| 4.6.2 | Geeignete Verfahren | 79 |
| 4.7 | Untersuchungsergebnisse zusammenführen | 80 |
| 4.8 | Häufige Fehler | 82 |
| 5 | Einführung in die Post-mortem-Analyse | 85 |
| 5.1 | Analyse des File Slack | 85 |
| 5.2 | MAC-Time-Analysen | 88 |
| 5.3 | NTFS-Streams | 90 |
| 5.4 | Auslagerungsdateien | 91 |
| 5.5 | Versteckte Dateien | 92 |
| 5.6 | Dateien oder Fragmente wiederherstellen | 96 |
| 5.7 | Unbekannte Binärdateien analysieren | 97 |
| 5.8 | Systemprotokolle | 106 |
| 6 | Forensik- und Incident-Response-Toolkits im Überblick | 111 |
| 6.1 | Sichere Untersuchungsumgebung | 111 |
| 6.2 | F.I.R.E. | 113 |
| 6.3 | Knoppix Security Tools Distribution | 117 |
| 6.4 | EnCase | 117 |
| 6.5 | dd | 119 |
| 6.6 | Forensic Acquisition Utilities | 122 |
| 6.7 | AccessData's Forensic Tool Kit | 123 |
| 6.8 | The Coroner's Toolkit und TCTUtils | 125 |
| 6.9 | The Sleuth Kit | 125 |
| 6.10 | Autopsy Forensic Browser | 132 |
| 6.11 | Eigene Toolkits für Unix und Windows erstellen | 136 |
| 6.11.1 | F.R.E.D. | 136 |
| 6.11.2 | Incident Response Collection Report (IRCR) | 137 |

| | | |
|-----------|--|------------|
| 7 | Forensische Analyse im Detail | 141 |
| 7.1 | Forensische Analyse unter Unix | 141 |
| 7.1.1 | Die flüchtigen Daten speichern | 141 |
| 7.1.2 | Forensische Duplikation | 147 |
| 7.1.3 | Manuelle P.m.-Analyse der Images | 151 |
| 7.1.4 | P.m.-Analyse der Images mit Autopsy | 158 |
| 7.1.5 | P.m.-Analyse der Images mit F.I.R.E. | 165 |
| 7.1.6 | Dateiwiederherstellung mit unrm und lazarus | 168 |
| 7.1.7 | Weitere hilfreiche Tools | 169 |
| 7.2 | Forensische Analyse unter Windows | 173 |
| 7.2.1 | Die flüchtigen Daten speichern | 173 |
| 7.2.2 | Forensische Duplikation | 175 |
| 7.2.3 | Manuelle P.m.-Analyse der Images | 179 |
| 7.2.4 | P.m.-Analyse der Images mit AccessData's FTK | 180 |
| 7.2.5 | P.m.-Analyse der Images mit EnCase | 183 |
| 7.2.6 | Weitere hilfreiche Tools | 186 |
| 7.3 | Forensische Analyse von PDAs | 200 |
| 7.4 | Forensische Analyse von Routern | 204 |
| 8 | Empfehlungen für den Schadensfall | 209 |
| 8.1 | Logbuch | 209 |
| 8.2 | Den Einbruch erkennen | 210 |
| 8.3 | Tätigkeiten nach festgestelltem Einbruch | 212 |
| 8.4 | Nächste Schritte | 215 |
| 9 | Backtracing | 217 |
| 9.1 | IP-Adressen überprüfen | 217 |
| 9.1.1 | Ursprüngliche Quelle | 217 |
| 9.1.2 | IP-Adressen, die nicht weiterhelfen | 218 |
| 9.1.3 | Private Adressen | 218 |
| 9.1.4 | Weitere IANA-Adressen | 219 |
| 9.1.5 | Augenscheinlich falsche Adressen | 219 |
| 9.2 | Spoof Detection | 220 |
| 9.2.1 | Traceroute Hopcount | 220 |
| 9.3 | Routen validieren | 223 |
| 9.4 | Nslookup | 227 |
| 9.5 | Whois | 229 |
| 9.6 | E-Mail-Header | 231 |
| 10 | Einbeziehung der Behörden | 235 |
| 10.1 | Organisatorische Vorarbeit | 235 |
| 10.2 | Strafrechtliches Vorgehen | 237 |
| 10.2.1 | Inanspruchnahme des Verursachers | 237 |
| 10.2.2 | Möglichkeiten der Anzeigeerstattung | 237 |
| 10.2.3 | Einflussmöglichkeiten auf das Strafverfahren | 240 |

| | | |
|------|---|------------|
| 10.3 | Zivilrechtliches Vorgehen | 240 |
| 10.4 | Darstellung in der Öffentlichkeit | 242 |
| 10.5 | Die Beweissituation bei der privaten Ermittlung | 243 |
| 10.6 | Fazit | 246 |
| | Anhang Tool-Überblick | 247 |
| | Index | 251 |