Kenne deinen Feind - Fortgeschrittene Sicherheitstechniken

Von Cyrus Peikari, Anton Chuvakin
*DOC | *audiobook | ebooks | Download PDF | ePub*

Produktinformation -Verkaufsrang: #813321 in BcherVerffentlicht am: 2004-07-01Einband: Taschenbuch602 Seiten | File size: 34.Mb

Von Cyrus Peikari, Anton Chuvakin : Kenne deinen Feind - Fortgeschrittene Sicherheitstechniken before purchasing it in order to gage whether or not it would be worth my time, and all praised Kenne deinen Feind - Fortgeschrittene Sicherheitstechniken:

KundenrezensionenHilfreichste Kundenrezensionen20 von 21 Kunden fanden die folgende Rezension hilfreich. Endlich ein "Hacker"-Buch fr FortgeschritteneVon AndiGrundstzlich gibt es in diesem Buch bei allen Kapiteln immer eine Windows und eine Linux Sicht. Es deckt sehr unterschiedliche Themen ab wie beispielsweise:- Reverse Engeniering (Disassembler, Cracken von Software)- berlufe (Puffer, Heap, Stack)- TCPIP-Analyse, -Attacken, Fingerprinting- Windowsangriffe, Linuxangriffe (und Verteidigung, Logfileauswertung usw.)- WLAN- Webservices- SQL InjectionDes Weiteren werden Intrusion Detection Systeme behandelt, Honeypots usw.Fr den Bereich Reverse Engeniering werden Assembler-Kenntnisse bentigt um sinnvoll mit dem Buch arbeiten zu knnen. Der Bereich "berlufe" setzt neben Assembler auch noch C voraus.Der ganze Bereich Netzwerkanalyse, Fingerprinting usw wird

ausfhrlich erleutert. Hier ist es sicherlich von Vorteil, wenn man prinzipielle TCPIP Kenntnisse hat, aber es gibt auch eine Einfhrung in die Thematik.Vom ersten Bereich profitieren Assembler und C Programmierer. Der zweite Bereich deckt viele Mglichkeiten von Netzwerkangriffen ab und ist vor allem fr Systemverwalter interessant.Auch wenn jemand den Status "Script Kiddy" verlassen will, ist das Buch ein geeignetes Werkzeug.Alles in allem ist es das bisher beste Buch im Themengebiet "Hacking". Viele Bcher wie die Hacker-Bibel oder Hacking intern halten nicht das was sie versprechen.

.deMan nehme 5 mittelalterliche Samurai wie auf dem Cover von Kenne deinen Feind und stelle sie vor den eigenen Webserver, um ihn vor Angriffen aus dem Netz zu schtzen -- Cyrus Peikari und Anton Chuvakin machen vor, wie das in der fortgeschrittenen Sicherheitsrealitt mithilfe von Selbstverteidigungstechniken fr Anwender und Systemadministratoren von Linux, Windows und Windows CE aussieht. Mit ihrem Buch wenden sich die Autoren an fortgeschrittene Anwender, die Erfahrung in Sicherheitsfragen etwa auf dem Niveau von Praktical Unix und Internet Security von O'Reilly besitzen und sich bei Netzwerkfragen und Programmiersprachen wohl und heimisch fhlen, nun aber ohne weitere Einfhrungen tiefer in die Sicherheitsmaterie, vor allem aus der Perspektive der Angreifer, einsteigen wollen. Das Buch ist in vier Teile gegliedert, die sich nach und nach durcharbeiten oder auch gezielt lesen lassen: Los geht es mit dem Software-Cracking: Der Fokus liegt hier auf dem Reverse Engineering/Reverse Code Engineering (RCE) fr Windows, Linux und auch Embedded-Plattformen sowie Windows Mobile Plattformen. Teil 2 behandelt dann die Grundlagen von Netzwerk-Angriffen, wie die Sicherheitsaspekte von TCP/IP inklusive IPv6 und Fragmentierungsangriffe. Ebenso dabei ist das Social Engineering, die Netzwerkaufklrung, das Betriebssystem-Fingerprinting bis hin zu den Techniken zum Verwischen der Spuren. Teil 3 heit Plattform-Angriffe und beleuchtet die Unterschiede und Grundlagen von Angriffen auf UNIX, Windows bis hin zu den Schwachstellen von drahtlosen Systemen einschlielich WLANs und Embedded-Malware. Zuletzt dann ein Hauptkapitel zur fortgeschrittenen Verteidigung: Protokollanalyse einschlielich der Logg-Aggregation und -Analyse. Fr viele neu drfte dann die Anwendung des Beayesschen Theorems auf die Implemtierung von Netzwerk-IDS-Systemen sein. Schritt fr Schritt wird auerdem der Aufbau eines Honey-Pot-Systems beschrieben, die Grundlagen des Incident Responce vorgestellt und forensische Tools fr UNIX und Windows erklrt. Der Anhang enthlt dann noch eine Liste ntzlicher SoftICE-Befehle und -Breakpunkte. Yepp, Kenne deinen Feind geht ans Eingemachte und fngt da erst an, wo sich der durchschnittliche Systemadministrator mit Sicherheit schon sicher fhlt. Anspruchsvolle, aber auch uerst ntzliche Lektre fr alle, die so weit gehen wollen, wie die feindlichen Angreifer vor der Tr. Nicht vorenthalten sollte man das Zitat am Anfang des Buches: "... Jeder Samurai sollte sich zweifellos dem Studium der Wehrwissenschaft widmen. Aber aus diesem Studium wird Schlechtes hervorgehen, wenn man es dazu verwendet, sein eigenes Ich aufzuwerten und seine Kameraden durch eine Menge hochtrabender, aber falscher Argumente herabzusetzen, die die Jungen nur in die Irre fhren und ihren Geist verderben. Denn diese Sorte Mensch hlt oft wortreiche Reden, die korrekt und dem Thema angemessen erscheinen, aber eigentlich geht es ihm nur um den Effekt und seinen eigenen Vorteil, was letzten Endes zur Auflsung seines Charakters und zum Verlust des wahren Samurai-Geistes fhrt. Dieser Fehler rhrt von einer oberflchlichen Beschftigung mit dem Thema her, deshalb sollten sich jene, die ein solches Studium beginnen, niemals damit zufrieden geben, nur den halben Weg zu gehen, sondern so lange durchhalten, bis sie alle Geheimnisse verstehen, und nur dann sollen sie zu ihrer ursprnglichen Einfachheit zurckkehren und ein ruhiges Leben fhren ..." (Daidoji Yuzan, Der Kodex des Samurai) --Wolfgang TreKurzbeschreibungSowohl Systemadministratoren als auch Benutzer sind zunehmend besorgt ber die Sicherheit ihrer Systeme und dies zu Recht. Die Angriffe werden mit jedem neuen Internet-Wurm und jedem aufgesprten Sicherheitsloch subtiler und gerissener. Was ist das Schlimmste, das Angreifer Ihnen antun knnen? Genau das lernen Sie in Kenne deinen Feind. Basierend auf dem Prinzip, dass eine gute Verteidigung die Methoden der Angreifer bis ins Detail kennt, deckt dieses Buch raffinierte Angriffsmethoden auf und beschreibt innovative Abwehrtechniken. Zu den behandelten Themen gehren: * Reverse Code Engineering (RCE) * Pufferberlauf-Angriffe * Social Engineering und Reconnaissance * Betriebssystem-Fingerprinting * Ausgeklgelte Angriffe gegen Unix- und Windows-Systeme * SQL-Injection * WLAN-Sicherheit * Intrusion-Detection-Systeme (IDS) * Honeypots * Incident Response * Computer-Forensik und Antiforensik Kenne deinen Feind legt einen besonderen Schwerpunkt auf das Reverse Engineering von Binr-Software. Reverse Engineering ist ein wichtiges Verfahren fr Administratoren, die sich mglicher Malware auf ihren Maschinen bewusst sein mssen: Trojaner, unschuldig wirkende Spyware usw. Dies ist das erste Buch, das das Reverse Engineering nicht nur fr Windows, sondern auch fr Linux und Windows CE behandelt. Kenne deinen Feind ist ein umfassendes Buch ber die Kunst der Selbstverteidigung in Computer-Netzwerken. Wenn Sie an vorderster Front stehen und Ihr Netzwerk oder Ihre Website gegen Angreifer verteidigen, dann kann Ihnen dieses Buch leidvolle Erfahrungen ersparen.ber den Autor und weitere MitwirkendeCyrus Peikari ist der Grnder der in Dallas ansssigen Airscanner Corporation, einem Forschungs- und Entwicklungsteam fr Funknetz-Sicherheitssoftware. Dr. Peikari schloss seine ersten vier Studienjahre im Jahr 1991 mit Auszeichnungen in Elektrotechnik an der Southern Methodist University ab. Er arbeitete auch als

Programmierer fr Telekommunikations-Software fr Alcatel, bevor er seinen Doktorgrad der Medizin von der Southwestern verliehen bekam. Dr. Peikari hat seitdem etliche preisgekrnte Sicherheitssoftware-Programme entwickelt. Er war Mitautor bei fnf Fachbchern ber IT-Sicherheit, bei dreien davon war er Hauptautor. Sein Buch Maximum Wireless Security, erschienen bei SAMS, ist seit seinem Erscheinen das meistverkaufte Buch seiner Art bei .com. Dr. Peikari spricht hufig auf Fachkonferenzen ber Informationssicherheit, einschlielich Defcon, NetSec und CSI. Er half verschiedenen Universitten dabei, neue Diplomstudienprogramme fr IT-Sicherheit ins Leben zu rufen, und er ist Site Host for Security der InformIt-Site von Pearson Education.Anton Chuvakin, Ph.D., GCIA, GCIH, ist Senior Security Analyst bei netForensics, einer Verwaltungsgesellschaft fr Sicherheitsinformationen. Bevor er bei netForensics anfing, arbeitete er fr Ubizen, einem europischen Anbieter fr Managed Security Services. Durch seinen Ph.D. in Physik fllt es ihm leicht, mit wissenschaftlichem Verstand an die Lsung schwieriger Sicherheitsprobleme heranzugehen. Anton Chuvakins Fachgebiete umfassen Intrusion Detection, das Hrten von Unix-Systemen, Computer-Forensik und Honeypots. Er hat zahlreiche Artikel und Buchrezensionen ber Computer- und Netzwerksicherheit verfasst, die unter anderem von SecurityFocus, Linux Journal, ;login, ISSA Password, der Online-Ausgabe des SC Magazine und LinuxSecurity.com verffentlicht wurden. In seiner Freizeit kmmert er sich um sein Sicherheitsportal http://www.info-secure.org und schreibt Rezensionen ber Bcher zum Thema Sicherheit. Er gehrt momentan unter anderem folgenden Fachorganisationen an: ISSA, InfraGard, USENIX, HTCIA, Honeynet Research Alliance usw. Er hat an SANS Top 20 Vulnerabilities (2002, 2003) mitgewirkt und ist aktives Mitglied des SANS GCIA Certification Advisory Board.