Netzwerkangriffe von innen

Von Paul Sebastian Ziegler
*ebooks | Download PDF | *ePub | DOC | audiobook*

Produktinformation -Verkaufsrang: #1663941 in BcherVerffentlicht am: 2008-07-30Abmessungen: 9.17 x .75b x 7.24l, Einband: Gebundene Ausgabe272 Seiten | File size: 16.Mb

Von Paul Sebastian Ziegler : Netzwerkangriffe von innen before purchasing it in order to gage whether or not it would be worth my time, and all praised Netzwerkangriffe von innen:

KundenrezensionenHilfreichste Kundenrezensionen1 von 1 Kunden fanden die folgende Rezension hilfreich. Mehr berblick ber die Gefahren im eigenen NetzwerkVon gweep"Netzwerkangriffe von innen" beginnt im ersten Teil mit "einfachen" Beispielen/Skripts in Phyton, die Problematik im Netzwerk zu beschrieben, wie man diverse Dienste zu seinem Vorteil als Blackhat Hacker nutzt. Dabei werden verschiedene Themen wie ARP, DHCP, Switches, ICMP, Mac-Flooding, Portstealing, usw. aufgegriffen und erklrt. Hier merkt man schon, wenn man kein Spezialist fr Security ist, das man einfach manche Probleme gar nicht erst erkennt oder wahrnimmt.Des Weiteren werden diverse Tools beschrieben die man zu seinem eigenen Vorteil nutzen kann, als auch Script-Kiddies oder Blackhat-Hacker fr sich.Im letzten Teil geht es um die Absicherung des Netzwerks. Dabei gibt der Autor keine genauen Vorgaben, da er hier offensichtlich auf die Vielfalt der Angriffsmglichkeiten aufmerksam machen mchte und es kein Allheilrezept

gibt.Dieses Buch ist kein Handbuch bei dem es darum geht: "Wenn... dann... " sondern vielmehr die Gefahren aufzeigt und damit klar macht, wie wichtig eigentlich auch die Interne Sicherheit ist. Da ein Buch mit "Wenn das passiert, dann tue das ..." nur fr eine bestimmte Zeit gelten kann, bis Hacker ihre Taktiken ndern oder andere Technologien nutzen. Dieses Buch ist ein "zeitloses Buch" das auch in ein paar Jahren noch Gltigkeit haben wird, weil es die Problematik aufzeigt, und welche Wege man einschlagen kann.Fr meinen Geschmack ein Klasse Buch das sich nicht auf Punkte fixiert sondern eben "zeitlos" ist. Die Technik um den Angriffen aus dem Weg zu gehen oder sich davor zu schtzen, liefern die Hersteller. Die Anstze um die richtige Richtung zu finden, dieses Buch.Dieses Buch ist sicher fr mehrere Schichten gedacht, der Administrator der sich die ntigen Anstze holen kann, der IT'ler der sich generell mit der Problematik im Netzwerk befassen mchte als auch der IT-Manager um einen berblick ber die Gefahren im eigenen Netzwerk zu bekommen.1 von 1 Kunden fanden die folgende Rezension hilfreich. Tiefer technischer Einstieg in die Sicherheit von NetzwerkenVon CustomerDas Buch "Netzwerkangriffe von innen" von Paul Sebastian Ziegler wendet sich vornehmlich an IT-Praktiker und Administratoren. Es beschreibt detailreich Sicherheitsrisiken im Intranet und konzentriert sich dabei vor allem auf die Netzwerkebene.Der Autor gliedert sein Buch in vier Abschnitte. Der erste Abschnitt erklrt wichtige Netzwerkprotokolle und Angriffe auf Netzwerkdienste (z.B. ARP, DHCP, ICMP) und Netzwerkhardware. Im zweiten Abschnitt geht es um Verschlsselung (TSL und SSH) und deren Angriffspunkte. Die Angriffserkennung und Gegenmanahmen werden im dritten Abschnitt angesprochen. Im letzten Abschnitt beschreibt der Autor Motivation und Mglichkeiten der Angreifer, diese berlegungen nutzt er um auf Gefhrdungspotentiale und weitere Gegenmanahmen zu schlieen.Wer praktisch mit Sicherheits-Themen umgeht wei das vielfach kleine Ursachen groe Wirkungen haben. Deswegen fhrt der Autor die Angriffsszenarien mit Beispielen (in Python) vor und scheut sich nicht auch auf Protokoll Ebene einzelne Dienste (z.B: ARP, DHCP, ICMP) detailliert zu erklren und ihre Schwchen herauszuarbeiten. Angriffstypen wie Port Stealing und Angriffe auf verschlsselte Verbindungen werden erklrt und es werden mgliche Gegenmanahmen durch den verantwortlichen Administrator aufgezeigt. Wer in das Thema Sniffing und "Man in the Middle" Angriffe tief einsteigen mchte findet mit "Netzwerkangriffe von innen" einen technisch anspruchsvolle Einfhrung. Weitergehende Sicherheitsfragen werden nur kurz angesprochen. Wer umfassend in das Thema Sicherheit einsteigen mchte sollte zustzlich Bcher zu den Themen Social Engineering und Sicherheit auf Anwendungsebene, beispielsweise zu Cross-Site Scripting und sicherer Software Entwicklung lesen.Das Buch erklrt die technischen Angriffspunkt im Netz und im Bereich Verschlsselung sehr gut, leider geht es nur am Rande auf die oben genannten anderen Aspekte der IT-Sicherheit ein. Deswegen Punktabzug, ein Buch das sich mit Intranet Sicherheit befasst sollte breiter angelegt sein.1 von 2 Kunden fanden die folgende Rezension hilfreich. Leider sehr enttuschendVon Christopher KunzTrotz der auf dem Klappentext aufgefhrten Meriten des Autors (Speaker auf der Blackhat und so) kann dieses Buch mich nicht berzeugen. Mehr noch, es enttuscht mich auf ganzer Linie. Meine persnliche Melatte fr Nischenliteratur von O'Reilly ist noch immer (trotz einiger Ausreier in der Vergangenheit) recht hoch und ich erwarte bei einem Buch zu einem so eng umrissenen Thema wie "Sicherheitsrisiken diesseits der Firewall" ein Buch, das in die Tiefe geht - nicht in die Breite.Leider kann das vorliegende Werk diese Hoffnung in keinem Punkt erfllen. Geht Ziegler anfangs noch durchaus planvoll zu Werk, schleicht sich allmhlich ein etwas zwiespltiger Eindruck ein. Kapitel wie das recht gelungene ber Portstealing lassen diesen Eindruck aber zunchst vergessen.In den fr mich interessanteren Teilen weiter hinten im Buch folgt dann die Ernchterung: Teilweise nur dreiseitige Kapitel, die nichts auer Allgemeinpltzen von sich geben (da man das Pseudonym eines Angreifers womglich aus Daten lesen kann, die er auf angegriffenen Systemen hinterlt, ist wahrlich nicht der Erwhnung wert) und bisweilen sachlich falsch sind, vergllen die Lektre.Insbesondere der Teil zu SSL, Zertifikaten, PKI und Co. enthlt leider Fehler und falsche Begrifflichkeiten. Der Unterschied zwischen ffentl. Schlssel und Zertifikat scheint nicht verstanden worden zu sein. Klar, jeder macht mal Fehler, aber das ist ja doch eine recht fundamentale Sache...Die letzten 50 bis 70 Seiten des Buches erwecken auf mich den Eindruck, als habe der Autor dringend fertig werden mssen - zu knapp sind einige Themen ausgefhrt, aus denen man definitiv htte mehr machen knnen.Sprachlich konnte das Werk mich leider auch nicht berzeugen - es wirkt, obgleich es eine dt. Originalausgabe ist, wie aus dem Englischen bersetzt.Insgesamt kann ich nur sagen: Guter Ansatz, guter erster Teil, aber danach wird es leider ziemlich unschn. Wenn der Autor und der Verlag sich fr die zweite Auflage gengend Zeit nhmen und das Buch grundstzlich berarbeiten wrden, knnte ein wirklich empfehlenswertes Werk daraus werden.

KurzbeschreibungLeider ist das Wissen um die Gefahren, die im eigenen Netzwerk lauern, bei Weitem nicht so weit verbreitet wie das Wissen um die Gefahren des Internets. Viele Betreiber lokaler Netzwerke schenken der Sicherheit nur wenig Beachtung. Mitunter wird einem einzelnen Administrator aufgetragen, sich um alle Probleme von buchstblich tausenden von Computern zu kmmern. Dieses Buch wird Ihnen die gngigsten im Intranet anzutreffenden Angriffe zeigen und erklren. Es richtet sich speziell an Systemadministratoren, denen zwar die technischen Zusammenhnge klar sind, die aber bisher wenig Kontakt mit Sicherheitsfragen hatten. Unsichere Protokolle Der erste Teil von Netzwerkangriffe von innen beschftigt sich mit unsicheren Protokollen in Netzwerken. Der Leser wird mit

modernen Hacking-Techniken wie Sniffing und Man-in-the-Middle-Angriffen vertraut gemacht, die Angreifer nutzen knnen, um aufgrund unsicherer Protokolle wertvolle Informationen aus netzinterner Kommunikation zu gewinnen. Wie ein Angreifer agiert, wird mit dem Sniffing-Tool Wireshark (frher Ethereal) im Detail gezeigt. Schwachstellen in ARP, DNS, DHCP und ICMP werden dabei ausfhrlich dargestellt und mit Beispielen erlutert, ebenso wie die fortgeschrittenen Angriffstechniken Portstealing und MAC-Flooding. Sichere Protokolle Das Verschlsseln von Daten schafft in vielen Fllen effektive Abhilfe, um den Angreifer zurckzudrngen. Aber ihre Strke sollte auch nicht berschtzt werden. In diesem Abschnitt wird sich der Leser ausfhrlich mit Techniken auseinandersetzen, die das Aufbrechen von Verschlsselungen ermglichen. Dabei wird stets die Unachtsamkeit des Administrators, Programmierers oder Nutzers ausgenutzt. Die Funktionsweise von Transport Layer Security (TLS) und Secure Shell (SSH) stehen dabei im Vordergrund. Absichern des Netzwerkes Wie der Systemadministrator das Netzwerk systematisch und effektiv gegen Angreifer von innen absichern kann, wird im nchsten Teil von Netzwerkangriffe von innen ausfhrlich und praxisnah dargestellt. Dabei wird stets die Denk- und Handlungsweise eines Angreifers genau analysiert. Beliebte Hacker-Tools werden dabei auch dargestellt. Mit einer Philosophie der digitalen Sicherheit schliet dieses herausragende IT-Sicherheitsbuch.ber den Autor und weitere MitwirkendePaul Sebastian Ziegler befasst sich seit seinem 16. Lebensjahr intensiv mit Systemadministration und Whitehat-Hacking. Er vertritt die Ansicht, dass Sicherheit nur aus Wissen resultieren kann, und ist daher sowohl publizistisch als auch vortragend ttig. Nhere Informationen und Kontaktmglichkeiten lassen sich auf seiner Homepage observed.de finden.