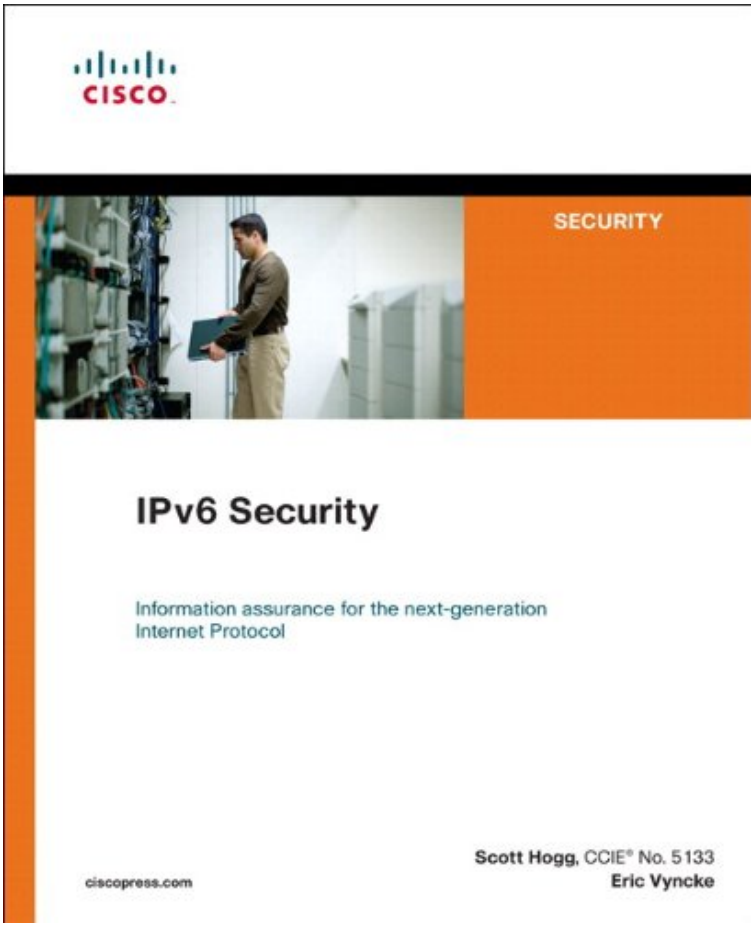
IPv6 Security (Networking Technology: Security)

Von Scott Hogg, Eric Vyncke
*ePub | *DOC | audiobook | ebooks | Download PDF*



Produktinformation -Verkaufsrang: #541949 in eBooksVerffentlicht am: 2008-12-11Erscheinungsdatum: 2008-12-11File Name: B001PBSDKC | File size: 19.Mb

Von Scott Hogg, Eric Vyncke : IPv6 Security (Networking Technology: Security) before purchasing it in order to gage whether or not it would be worth my time, and all praised IPv6 Security (Networking Technology: Security):

KundenrezensionenHilfreichste Kundenrezensionen4 von 4 Kunden fanden die folgende Rezension hilfreich. Eines der besten Bcher zu IPv6!Von Dietrich SchroffKapitel 1 gibt eine kurze Einfhrung in das Thema IPv6. Der schnste Satz ist "It is better to be safe than sorry". Gerade im Kontext von Security ist das ein passendes Leitmotiv.In Kapitel 2 werden die Schwachstellen des Protokolls durchgegangen. Es werden Abschnittsweise ICMPv6, Extension Headers und Ausphen von Netzwerken durchgegangen. Die Abschnitte sind sehr gut aufgebaut und wirklich illustrativen Bildern untersttzt (z.B. RH0-Angriffe sind sehr verstndlich dargestellt.).Mit Kapitel 3 ("Internet Security") macht der Autor klar, dass IPv6 bereits luft und selbst in vermeintlich IPv6-freien Umgebungen schon viele Devices per Default IPv6 enabled sind. Hier werden bereits erste IPv6-Wrmer und deren Verbreitungsmechanismen geschildert (Subnetz scannen mit 2^64 Adressen funktioniert jedenfalls nicht ;-). Folgende Punkte sind fr Provider und groe Fimrennetzwerk sehr interessant:* Ingress/Egress Filtering* Securing BGP Sessions* IPv6 over MPLS Security*

Prefix Delegation Threads* MultihomingKapitel 4 "Perimeter Security" setzt sich der typischen Sicherheitsdenkweise auseinander: Wir bauen ein Festung aus Firewalls...Hier gibt der Autor eine Zusammenstellung aller Netze, die auf jedenfall in einer IPv6-Firewall zu blockieren sind. Weitere Hilfestellung gibt es fr Tunnel-Mechanismen und natrlich das leidige Thema Firewall und/oder NAT. Natrlich gibt es hier (es ist ein Buch von Cisco) eine komplette Konfiguration einer Cisco-Firewall (Sehr ausfhrlich mit Netzbildern, Konfigurationen und Netzwerk-Traces).In Kapitel 5 geht es um die Sicherheit innerhalb eines Netzwerks. Hier werden Angriffstechniken bzgl. Stateless Address Autoconfiguration durchgespielt. Von RA ber ND bis DAD immer mit kleinen Netzwerkbildern und guter Beschreibung. Ebenfalls beschrieben ist SEND, aber da es derzeit noch kaum Implementierungen dazu gibt von eher akademischem Interesse.Kapitel 6 erscheint mir etwas durcheinander gewrfelt: Hardening IPv6 Network Devices. Hier werden sehr knapp RIPng, EIGRPv6, IS-IS, OSPF, HSRPv6 und GLBPv6 durchgemacht (auf 21 Seiten!). Hier sollte wohl gezeigt werden, was Cisco Router alles so drauf haben.In Kapitel 7 wird fr diverse Betriebssysteme beschrieben, welche Einstellungen bzgl. IPv6 getroffen sein sollten: Microsoft, Windows, Linux, BSD, Sun Solaris. Fr den Alltag als Referenz und Einstieg sehr hilfreich (z.B. wie wird die Neigbour-Tabelle jeweils abgefragt.).Kapitel 8 beschftigt sich mit dem meistzitiersten Punkt, warum IPv6 sicherer sein soll als IPv4: IPsec!Nun ja, IPsec ist inhrent dabei, es muss deshalb trotzdem nicht verwendet werden... Immerhin gibt es ber die Extension Header ein paar Optionen die mit IPv4 so nicht mglich waren. Auch hier wieder ein paar Cisco-spezifische Konfigurationen zum Ausprobieren.In Kapitel 9 wird Security for IPv6 Mobility dargestellt. Hier ist allerdings noch zu viel im Fluss, um sich wirklich auf dieses Kapitel verlassen zu knnen. Die Angriffsszenarien werden jedoch fr alle zuknftigen Lsungen weiter bestehen bleiben und sind daher auf jedenfall hilfreich.Kapitel 10 beschreibt die IPv4 nach IPv6 Transisition-Mechanismen und deren Sicherheitsprobleme. Dies wird fr einige Zeit ein wichtiges Kapitel bleiben...In den letzten beiden Kapiteln werden noch Monitoring in IPv6-Netzwerken dargestellt und Vergleiche zwischen IPv4 und IPv6 durchgefhrt.Abschlieend bleibt nur die Gratulation an die beiden Autoren fr ein sehr gelungenes Buch. Absolute Kaufempfehlung!

KurzbeschreibungIPv6 Security Protection measures for the next Internet Protocol As the worlds networks migrate to the IPv6 protocol, networking professionals need a clearer understanding of the security risks, threats, and challenges this transition presents. In IPv6 Security, two of the worlds leading Internet security practitioners review each potential security issue introduced by IPv6 networking and present todays best solutions. IPv6 Security offers guidance for avoiding security problems prior to widespread IPv6 deployment. The book covers every component of todays networks, identifying specific security deficiencies that occur within IPv6 environments and demonstrating how to combat them. The authors describe best practices for identifying and resolving weaknesses as you maintain a dual stack network. Then they describe the security mechanisms you need to implement as you migrate to an IPv6-only network. The authors survey the techniques hackers might use to try to breach your network, such as IPv6 network reconnaissance, address spoofing, traffic interception, denial of service, and tunnel injection. The authors also turn to Cisco products and protection mechanisms. You learn how to use Cisco IOS and ASA firewalls and ACLs to selectively filter IPv6 traffic. You also learn about securing hosts with Cisco Security Agent 6.0 and about securing a network with IOS routers and switches. Multiple examples are explained for Windows, Linux, FreeBSD, and Solaris hosts. The authors offer detailed examples that are consistent with todays best practices and easy to adapt to virtually any IPv6 environment. Scott Hogg, CCIE No. 5133, is Director of Advanced Technology Services at Global Technology Resources, Inc. (GTRI). He is responsible for setting the companys technical direction and helping it create service offerings for emerging technologies such as IPv6. He is the Chair of the Rocky Mountain IPv6 Task Force. Eric Vyncke, Cisco Distinguished System Engineer, consults on security issues throughout Europe. He has 20 years experience in security and teaches security seminars as a guest professor at universities throughout Belgium. He also participates in the Internet Engineering Task Force (IETF) and has helped several organizations deploy IPv6 securely. Understand why IPv6 is already a latent threat in your IPv4-only network Plan ahead to avoid IPv6 security problems before widespread deployment Identify known areas of weakness in IPv6 security and the current state of attack tools and hacker skills Understand each high-level approach to securing IPv6 and learn when to use each Protect service provider networks, perimeters, LANs, and host/server connections Harden IPv6 network devices against attack Utilize IPsec in IPv6 environments Secure mobile IPv6 networks Secure transition mechanisms in use during the migration from IPv4 to IPv6 Monitor IPv6 security Understand the security implications of the IPv6 protocol, including issues related to ICMPv6 and the IPv6 header structure Protect your network against large-scale threats by using perimeter filtering techniques and service providerfocused security practices Understand the vulnerabilities that exist on IPv6 access networks and learn solutions for mitigating each This security book is part of the Cisco Press Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks. Category: Networking: Security Covers: IPv6 SecurityKurzbeschreibungIPv6 Security Protection measures for the next Internet Protocol As

the worlds networks migrate to the IPv6 protocol, networking professionals need a clearer understanding of the security risks, threats, and challenges this transition presents. In IPv6 Security, two of the worlds leading Internet security practitioners review each potential security issue introduced by IPv6 networking and present todays best solutions. IPv6 Security offers guidance for avoiding security problems prior to widespread IPv6 deployment. The book covers every component of todays networks, identifying specific security deficiencies that occur within IPv6 environments and demonstrating how to combat them. The authors describe best practices for identifying and resolving weaknesses as you maintain a dual stack network. Then they describe the security mechanisms you need to implement as you migrate to an IPv6-only network. The authors survey the techniques hackers might use to try to breach your network, such as IPv6 network reconnaissance, address spoofing, traffic interception, denial of service, and tunnel injection. The authors also turn to Cisco products and protection mechanisms. You learn how to use Cisco IOS and ASA firewalls and ACLs to selectively filter IPv6 traffic. You also learn about securing hosts with Cisco Security Agent 6.0 and about securing a network with IOS routers and switches. Multiple examples are explained for Windows, Linux, FreeBSD, and Solaris hosts. The authors offer detailed examples that are consistent with todays best practices and easy to adapt to virtually any IPv6 environment. Scott Hogg, CCIE No. 5133, is Director of Advanced Technology Services at Global Technology Resources, Inc. (GTRI). He is responsible for setting the companys technical direction and helping it create service offerings for emerging technologies such as IPv6. He is the Chair of the Rocky Mountain IPv6 Task Force. Eric Vyncke, Cisco Distinguished System Engineer, consults on security issues throughout Europe. He has 20 years experience in security and teaches security seminars as a guest professor at universities throughout Belgium. He also participates in the Internet Engineering Task Force (IETF) and has helped several organizations deploy IPv6 securely. Understand why IPv6 is already a latent threat in your IPv4-only network Plan ahead to avoid IPv6 security problems before widespread deployment Identify known areas of weakness in IPv6 security and the current state of attack tools and hacker skills Understand each high-level approach to securing IPv6 and learn when to use each Protect service provider networks, perimeters, LANs, and host/server connections Harden IPv6 network devices against attack Utilize IPsec in IPv6 environments Secure mobile IPv6 networks Secure transition mechanisms in use during the migration from IPv4 to IPv6 Monitor IPv6 security Understand the security implications of the IPv6 protocol, including issues related to ICMPv6 and the IPv6 header structure Protect your network against large-scale threats by using perimeter filtering techniques and service providerfocused security practices Understand the vulnerabilities that exist on IPv6 access networks and learn solutions for mitigating each This security book is part of the Cisco Press Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks. Category: Networking: Security Covers: IPv6 SecurityBuchrckseite"IPv6 Security" Protection measures for the next Internet Protocol As the world's networks migrate to the IPv6 protocol, networking professionals need a clearer understanding of the security risks, threats, and challenges this transition presents. In IPv6 Security, two of the world's leading Internet security practitioners review each potential security issue introduced by IPv6 networking and present today's best solutions. "IPv6 Security" offers guidance for avoiding security problems prior to widespread IPv6 deployment. The book covers every component of today's networks, identifying specific security deficiencies that occur within IPv6 environments and demonstrating how to combat them. The authors describe best practices for identifying and resolving weaknesses as you maintain a dual stack network. Then they describe the security mechanisms you need to implement as you migrate to an IPv6-only network. The authors survey the techniques hackers might use to try to breach your network, such as IPv6 network reconnaissance, address spoofing, traffic interception, denial of service, and tunnel injection. The authors also turn to Cisco(R) products and protection mechanisms. You learn how to use Cisco IOS(R) and ASA firewalls and ACLs to selectively filter IPv6 traffic. You also learn about securing hosts with Cisco Security Agent 6.0 and about securing a network with IOS routers and switches. Multiple examples are explained for Windows, Linux, FreeBSD, and Solaris hosts. The authors offer detailed examples that are consistent with today's best practices and easy to adapt to virtually any IPv6 environment. Scott Hogg, CCIE(R) No. 5133, is Director of Advanced Technology Services at Global Technology Resources, Inc. (GTRI). He is responsible for setting the company's technical direction and helping it create service offerings for emerging technologies such as IPv6. He is the Chair of the Rocky Mountain IPv6 Task Force. Eric Vyncke, Cisco Distinguished System Engineer, consults on security issues throughout Europe. He has 20 years' experience in security and teaches security seminars as a guest professor at universities throughout Belgium. He also participates in the Internet Engineering Task Force (IETF) and has helped several organizations deploy IPv6 securely. Understand why IPv6 is already a latent threat in your IPv4-only networkPlan ahead to avoid IPv6 security problems before widespread deploymentIdentify known areas of weakness in IPv6 security and the current state of attack tools and hacker skillsUnderstand each high-level approach to securing IPv6 and learn when to use eachProtect service provider networks, perimeters, LANs, and host/server connectionsHarden IPv6 network devices against attackUtilize IPsec in IPv6 environments Secure mobile IPv6 networksSecure transition mechanisms in use during the migration from IPv4 to IPv6Monitor IPv6 securityUnderstand the security implications of the IPv6 protocol, including issues related to ICMPv6 and the IPv6 header structureProtect your network against large-scale threats by using perimeter

filtering techniques and service provider-focused security practicesUnderstand the vulnerabilities that exist on IPv6 access networks and learn solutions for mitigating each This security book is part of the Cisco Press(R) Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks. Category: Networking: SecurityCovers: IPv6 Security