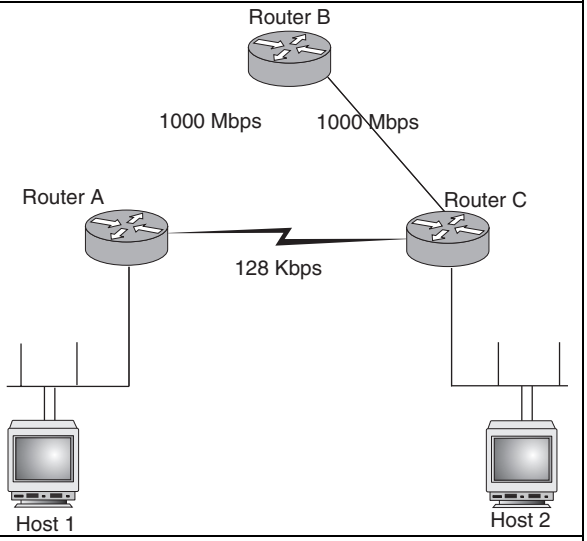
Inside Network Perimeter Security

0735712328

Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, and Ronald W. Ritchey

Warning and Disclaimer: Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied. The information is provided on an as-is basis. The authors and New Riders Publishing shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

Misprint	Correction
Global ACK and SYN should not have the Mono font applied to them anywhere in the book.	
Global Ipchains	IPchains
Global Placeholder text should appear as *italic* without < and > tags around it.	
Page 28 Assemble your Cisco router access list following the percept of "allow what you need" rather then "deny what you don't."	Whenever possible, assemble your access lists following the percept of "allow what you need" rather than "deny what you don't."
Page 64 This tcpdump trace shows the three-way handshake between a contacting client named Host and the SANS GIAC web server, Maverick.	This Tcpdump trace shows the three-way handshake between a contacting client named Host and the SANS GIAC web server, Maverick.
Page 74 `PING`	`Ping`
Page 104 Firewall rules look simple when we are looking at a Checkpoint FW1 GUI, but underneath might be many complex decisions and assumptions.	Firewall rules look simple when we are looking at a Check Point FireWall-1 GUI, but underneath might be many complex decisions and assumptions.
Page 109 Even with good rules that are properly organized though, our policy can be subverted or made unenforceable through those two Mac truck-sized holes living at TCP 80 and 25.	Even with good rules that are properly organized though, our policy can be subverted or made unenforceable through those two Mack truck-sized holes living at TCP 80 and 25.
Page 109 Many of these tools aren't just using port 80; they are actually encoding their traffic in HTTP with `get`, `put`, `posts`, and markup language tags.	Many of these tools aren't just using port 80; they are actually encoding their traffic in HTTP with `get`, `put`, `POST`, and markup language tags.
Page 139 `Source ip/port - Translated IP/port – contacted IP/port`	`Source IP/port - Translated IP/port – contacted IP/port`
Page 157 (A *sniffer* is a hardware device that captures detailed packet information.)	(A *sniffer* is a device that captures detailed packet information.)
Page 205 (This is most noticable in the last packet listed, seq=0x3.)	(This is most noticable in the last packet listed, `seq=ox3`.)
Page 221 **28.** Run the `Ipsecmon` command from the run line.	**28.** Run the `ipsecmon` command from the run line.
Page 290 "Separating Resources," calls for the use of `Chroot` to create a "jail" around an application on	"Separating Resources," calls for the use of Chroot to create a "jail" around an application on a UNIX system.

a UNIX system.	
Page 325 If BIND is set up to operate in a chroot jail, located in `/usr/local/vind-chroot`, the named process will be started from `/usr/local/bind-chroot/usr/local/sbin/named`.	If BIND is set up to operate in a chroot jail, located in `/usr/local/vind-chroot`, the `named` process will be started from `/usr/local/bind-chroot/usr/local/sbin/named`.
Page 326 An effective method of reliability separating one application from another involves dedicating a server to each application.	A more effective method of reliability separating one application from another involves dedicating a server to each application.
Page 339 When deciding where to place DNS servers and whether to split DNS servers into multiple security zones, consider two primary users of DNS services:	When deciding where to place DNS servers and whether to split DNS servers into multiple security zones, consider two primary types of users of DNS services:
Page 345 AirSnort accomplishes this by implementing a vulnerability in the key scheduling algorithm of RC4, discover by Scott Fluhrer, Itsik Mantin, and Adi Shamir.	AirSnort accomplishes this by exploiting a vulnerability in the key scheduling algorithm of RC4, discover by Scott Fluhrer, Itsik Mantin, and Adi Shamir.
Page 416 In addition, Router A has a 300Mbps connection to Router C.	In addition, Router A has a 128Kbps connection to Router C.
Page 417 Figure 15.1	
Page 535 `18:28:10.964249 <external_if>.53153 > 64.58.77.195.80: S…`	`18:28:10.964249 <external_if>.53153 > 64.58.77.195.80: S…`
Page 543 In fact, you might want to include copies of `netstat`, `ifconfig`, `ipconfig`, `lsof`, `Fprot`, `ls`, and other common utilities that attackers might replace on penetrated servers to hide their activities.	In fact, you might want to include copies of netstat, ifconfig, ipconfig, lsof, Fprot, ls, and other common utilities that attackers might replace on penetrated servers to hide their activities.
Page 572 ♣ UDP: # nmap –sU 192.168.1.0 – 192.168.1.255 ♣ SYN: # nmap –sS 192.168.1.0 – 192.168.1.255	♣ `UDP: # nmap –sU 192.168.1.0 – 192.168.1.255` ♣ `SYN: # nmap –sS 192.168.1.0 – 192.168.1.255`
Page 638 ♣ Any use of FTP outbound requires a \ passive (PASV) FTP client and server support for the same.	♣ Any use of FTP outbound requires a passive (PASV) FTP client and server support for the same.

This errata sheet is intended to provide updated technical information.
Spelling and grammar misprints are updated during the reprint process,
but are not listed on this errata sheet.