NetRecon Report

Network Vulnerabilities Detail Report
Grouped by Network Resource Name

Report Generated by:	Symantec NetRecon 3.5
Licensed to:	computec.ch
Serial Number:	6871651987
Machine Scanned from:	WS2 (192.168.0.12, 192.168.190.1, 192.168.244.1)
Scan Date:	26.04.2003
Scan Duration:	3 minutes, 3 seconds
Scan Objective:	Heavy scan
Resources Scanned:	192.168.0.13
Resources Reported On:	All scanned network resources.

Network Resource:	**192.168.0.13**
Resource Type:	IP host
Aliases:	
# of Unique Vulnerabilities	3
Highest Risk Level Found	16

Vulnerability Name:	**network resource detected via ICMP protocol**
Risk:	15
Vulnerability Description:	NetRecon has discovered that this network resource responds using the ICMP protocol. ICMP, as part of the IP layer, handles error messaging and other control conditions. This message is a catch-all message because NetRecon has intercepted an ICMP datagram, regardless of its type. If you receive this message, you may also receive messages for the other ICMP vulnerabilities that NetRecon discovers, such as Responds to ICMP Echo (ping) Requests. In discovering this vulnerability, NetRecon sent a UDP service request and a number of ICMP datagrams to this system and received one or more ICMP responses. The following are known threats to the legitimate use of the ICMP protocol: - An ICMP reply tells an attacker that a remote system exists and is running. - An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships. - An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.) - An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.) - An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)
Vulnerability Solution:	Symantec recommends filtering all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)
Additional Information:	
Links:	

Network Resource:	**192.168.0.13**	**(cont.)**

Vulnerability Name:	**network resource detected via ICMP protocol**	(cont.)

Details:

Vulnerability Name:	**network resource identified**
Risk:	16
Vulnerability Description:	NetRecon has obtained information that helps to identify a particular network resource. This information could include full or partial identification of the operating system, server types (SMB server, for example), whether a machine is an IP host, etc. Once an attacker has identified a specific target, he or she can find and exploit weakness in that resource.
Vulnerability Solution:	Using the data table in NetRecon, determine how the information was obtained. Either eliminate the service responsible or configure it to not give any clues that can help identify the network resource.
Additional Information:	
Links:	

Details:

Type = IP host

Vulnerability Name:	**responds to ICMP echo request (ping)**
Risk:	15
Vulnerability Description:	NetRecon has discovered that this system responds to an ICMP echo request (commonly referred to as ping). ICMP is part of the IP layer. It is used to handle IP status and control messages. The following are known threats to the legitimate use of this service: - An ICMP reply tells an attacker that a remote system exists and is running. - An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships. - An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.) - An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends

Network Resource:	**192.168.0.13**	**(cont.)**

Vulnerability Name:	**responds to ICMP echo request (ping)** (cont.)
	an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.) - An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)
Vulnerability Solution:	Symantec recommends filtering all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.) However, disabling ICMP on the firewall is only a partial solution. The complete solution should include patching or upgrading the OS kernel so that it can handle oversized ping requests (if possible with your OS). Many operating system vendors have created patches that prevent the Ping o' Death vulnerability. Consult your OS vendor to see if your system can handle oversized packets.
Additional Information:	For additional information about ICMP's ping vulnerabiility, read CERT(R) Advisory CA-96.26 at the following URL: http://www.cert.org/advisories/CA-1996-26.html (1) See Common Vulnerabilities and Exposures CVE-1999-0128 (2)
Links:	1. http://www.cert.org/advisories/CA-1996-26.html 2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0128

Details: