



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Introduction to the Microsoft Windows XP firewall

SANS Security Essentials (GSEC) v1.2e

Questions

Matt Snitchler

© SANS Institute 2000 - 2005, Author retains full rights.

1. Which of Microsoft's Operating Systems is considered to be more stable?
 - a. DOS
 - b. Linux
 - c. **Windows XP**
 - d. Windows 95

Help

Windows XP will be built off of the Windows NT Kernel. This is thought to be a much more stable platform than the old DOS command.com platform. This is the platform Operating Systems like DOS and Windows 95 were built from.

2. What types of things would an attacker probably not be interested in that you might store on your computer?
 - a. **High scores in minesweeper**
 - b. Passwords
 - c. Credit Card Numbers
 - d. Personal email

Help

Attackers may have an interest in your personal information often stored on home computers. Do you store any passwords or credit card numbers on your computer? How about personal email or financial information, such as account numbers or electronic bank statements?

3. Which of the following would not be considered a type of firewall.
 - a. Packet filtering
 - b. Circuit-level gateway
 - c. **Server Level gateway**
 - d. Stateful inspection

Help

There are four basic types of firewalls. Packet filtering, Circuit-level gateway, Application-level gateway, and Stateful inspection firewall.

4. What type of environment might Microsoft's Internet connection firewall not be very well suited for?
 - a. Home user with a single computer
 - b. Home user with multiple computers
 - c. Small Business with a single computer
 - d. **Large Business with 100 computers**

Help

Internet Connection Firewall might be a tool used to protect a home computer or maybe a small home network. You also might find ICF protecting a small business network. Microsoft does also produce a full fledged firewall designed for

a dedicated server and a LAN.

5. What won't you find in the ICF log file?
 - a. Protocol
 - b. Src-ip
 - c. **Usr-name**
 - d. Tcp-win

Help

The log file will include things like date/timestamp, action, protocol, src-ip, dest-ip, src-port, dest-port, size, tcpflags, tcpsyn, tcpack, tcpwin, icmp type, icmp code, and/or info.

6. **True/False.** Microsoft's Internet Connection Firewall was designed to compete with personal firewall applications.

Help

Microsoft's Internet Connection Firewall was designed to work with personal firewall applications, not to compete with them.

7. **True/False.** Microsoft's Internet Connection Firewall is expensive to implement.

Help

ICF has no cost, it comes with the OS.

8. **True/False.** Windows XP was designed for expert computer users and beginners.

Help

Windows XP promises to be the OS that will appeal to Geeks and Power users as well as to beginners and users generally timid around computers.

9. **True/False.** Logs are generated in World Wide Web Consortium (W3C) Extended Log Format.

Help

Logs are generated in World Wide Web Consortium (W3C) Extended Log Format.

10. **True/False.** Microsoft's Internet Connection Firewall can be configured to block all Inbound and Outbound traffic.

Help

ICF doesn't block any outbound traffic.

© SANS Institute 2000 - 2005, Author retains full rights.