



# 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 Bootcamp Style (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, tpack, 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.

# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive