GCIA – GIAC Certified Intrusion Analyst Practice Test

GIAC GCIA

Version Demo

Total Demo Questions: 20

Total Premium Questions: 507

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	145
Topic 2, Volume B	146
Topic 3, Volume C	150
Topic 4, Volume D	66
Total	507

QUESTION NO: 1 - (SIMULATION)

SIMULATION

Fill in the blank with the appropriate term.

___________ is the practice of monitoring and potentially restricting the flow of information outbound from one network to another

ANSWER: Egress filtering

QUESTION NO: 2

Which of the following is the process of categorizing attack alerts produced from IDS?

A. Blocking

B. Site policy implementation

C. Intrusion classify

D. Alarm filtering

ANSWER: D

QUESTION NO: 3

Which of the following statements are true about routers?

Each correct answer represents a complete solution. Choose all that apply.

A. Routers do not limit physical broadcast traffic.

B. Routers organize addresses into classes, which are used to determine how to move packets from one network to another.

C. Routers act as protocol translators and bind dissimilar networks.

D. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.

ANSWER: B C D

QUESTION NO: 4

Which of the following parts of hard disk in Mac OS X File system stores information related to the files?

A. Resource fork

B. Data fork

C. System fork

D. Log fork

ANSWER: A

QUESTION NO: 5

Adam, a malicious hacker purposely sends fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65,536 bytes.

On the basis of above information, which of the following types of attack is Adam attempting to perform?

A. Fraggle attack

B. SYN Flood attack

C. Land attack

D. Ping of death attack

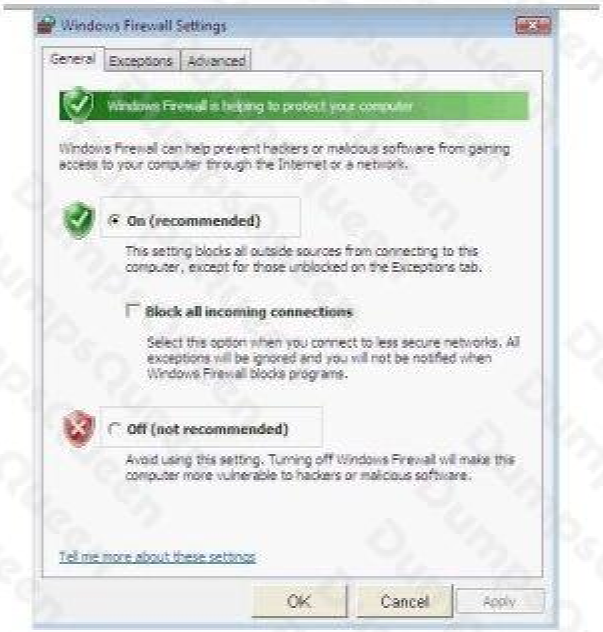
ANSWER: D

QUESTION NO: 6 - (HOTSPOT)

HOTSPOT

Steve works as a Network Administrator for Blue Tech Inc. All client computers in the company run the Windows Vista operating system. He often travels long distances on official duty. While traveling, he connects to the office server through his laptop by using remote desktop connection. He wants to run an application that is available on the server of the company. When he connects to the server, he gets a message that the connection is blocked by the firewall. He returns to his office to resolve the issue. He opens the Windows Firewall Settings dialog box. What actions should he perform in the dialog box given below to accomplish the task?

Hot Area:



Windows Firewall Settings

General | Exceptions | Advanced

Windows Firewall is helping to protect your computer

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.

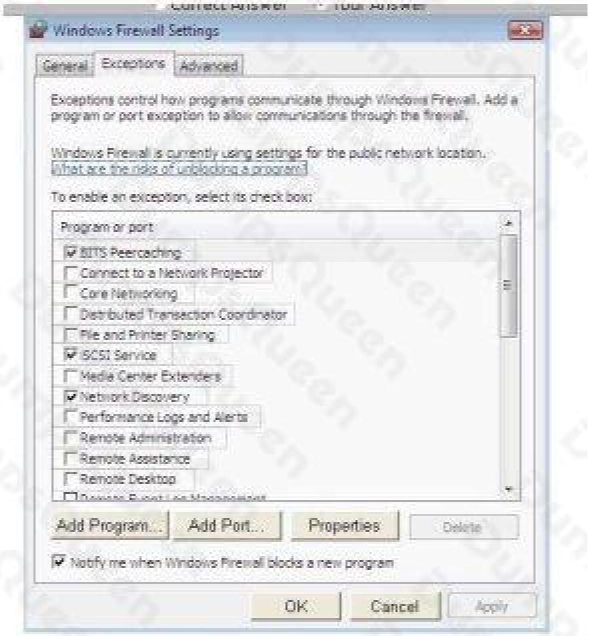
□ Block all incoming connections

Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.

○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

Tell me more about these settings



Correct Answer   Your Answer

Windows Firewall Settings

General | Exceptions | Advanced

Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

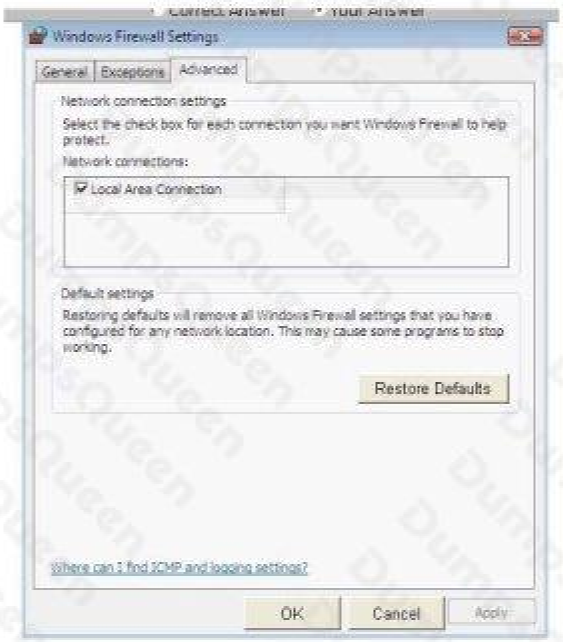
Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port

- ☑ BITS Peercaching
- □ Connect to a Network Projector
- □ Core Networking
- □ Distributed Transaction Coordinator
- □ File and Printer Sharing
- ☑ iSCSI Service
- □ Media Center Extenders
- ☑ Network Discovery
- □ Performance Logs and Alerts
- □ Remote Administration
- □ Remote Assistance
- □ Remote Desktop
- □ Remote Event Log Management

☑ Notify me when Windows Firewall blocks a new program



Correct Answer   Your Answer

Windows Firewall Settings

General | Exceptions | Advanced

Network connection settings

Select the check box for each connection you want Windows Firewall to help protect.

Network connections:

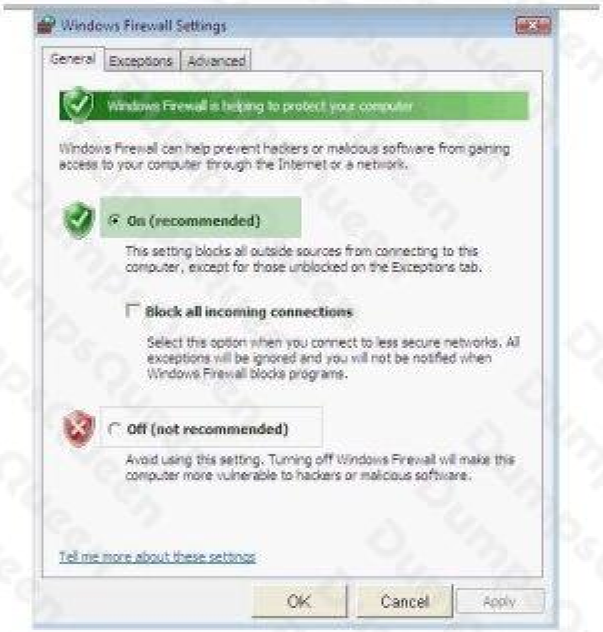
☑ Local Area Connection

Default settings

Restoring defaults will remove all Windows Firewall settings that you have configured for any network location. This may cause some programs to stop working.

Where can I find ICMP and logging settings?

ANSWER:



Windows Firewall Settings

General | Exceptions | Advanced

Windows Firewall is helping to protect your computer

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.

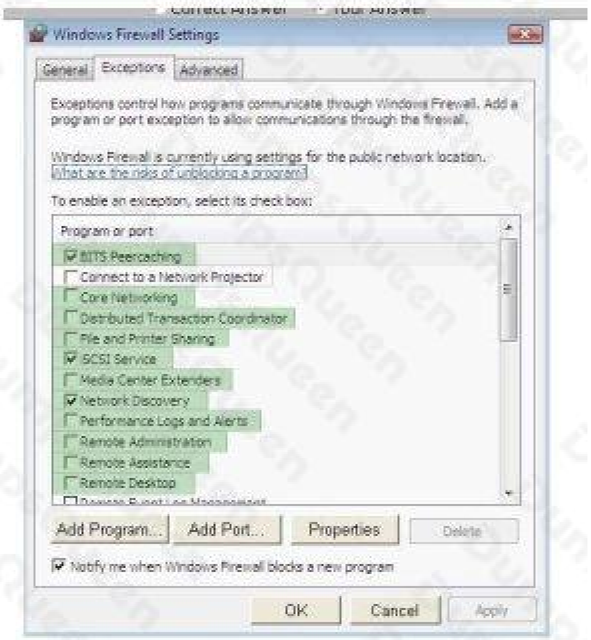
□ Block all incoming connections

Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.

○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

Tell me more about these settings



Windows Firewall Settings

General | Exceptions | Advanced

Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

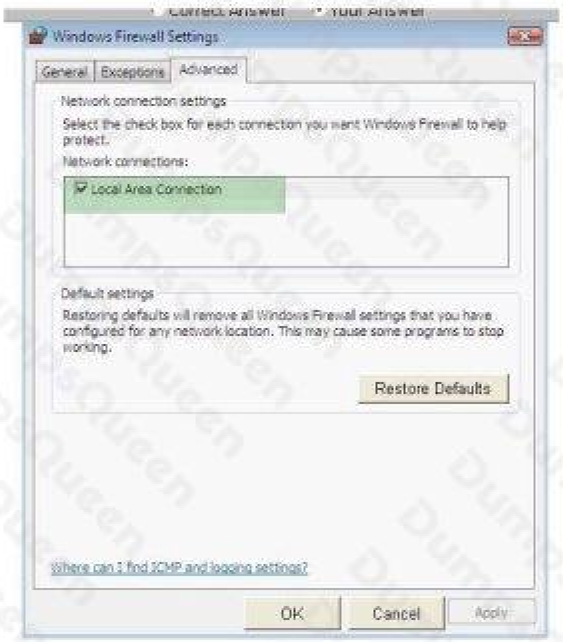
Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port

- ☑ BITS Peercaching
- □ Connect to a Network Projector
- □ Core Networking
- □ Distributed Transaction Coordinator
- □ File and Printer Sharing
- ☑ SCSI Service
- □ Media Center Extenders
- ☑ Network Discovery
- □ Performance Logs and Alerts
- □ Remote Administration
- □ Remote Assistance
- □ Remote Desktop
- □ Remote Event Log Management

☑ Notify me when Windows Firewall blocks a new program



Windows Firewall Settings

General | Exceptions | Advanced

Network connection settings

Select the check box for each connection you want Windows Firewall to help protect.

Network connections:

☑ Local Area Connection

Default settings

Restoring defaults will remove all Windows Firewall settings that you have configured for any network location. This may cause some programs to stop working.

Where can I find ICMP and logging settings?

Explanation:

QUESTION NO: 7

Which of the following work as traffic monitoring tools in the Linux operating system? Each correct answer represents a complete solution. Choose all that apply.

A. MRTG

B. John the Ripper

C. IPTraf

D. Ntop

ANSWER: A C D

QUESTION NO: 8

Mark works as a Network administrator for SecureEnet Inc. His system runs on Mac OS X. He wants to boot his system from the Network Interface Controller (NIC). Which of the following snag keys will Mark use to perform the required function?

A. D

B. N

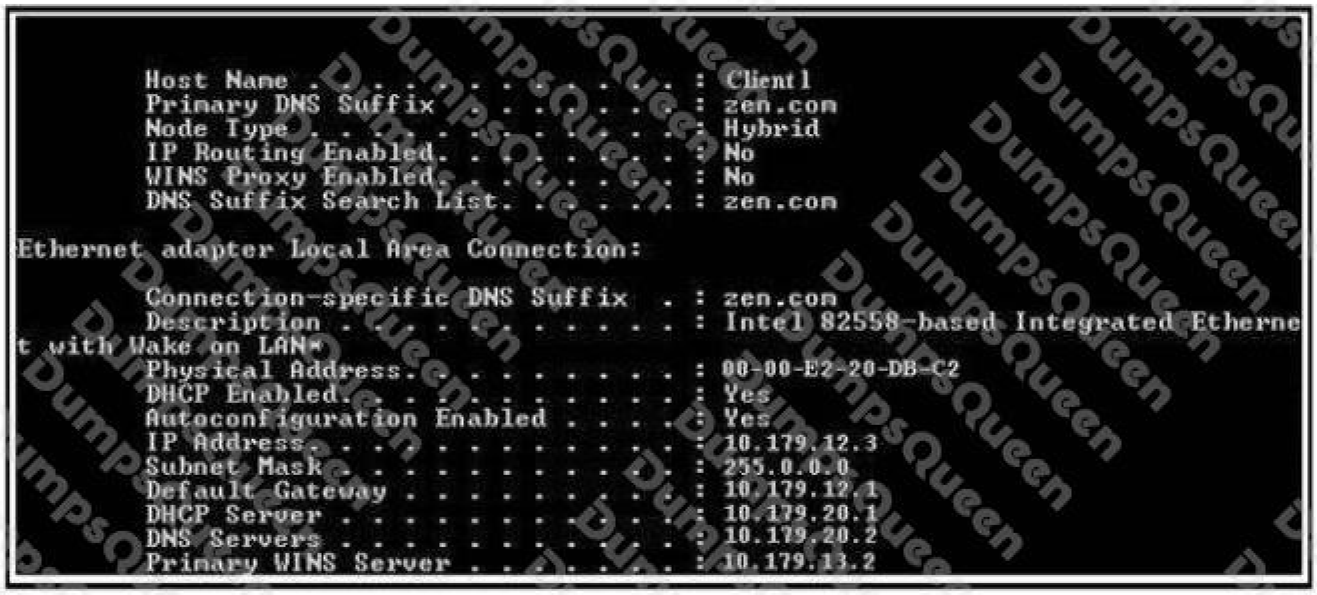
C. Z

D. C

ANSWER: B

QUESTION NO: 9

Which of the following utilities produces the output displayed in the image below?



```
        Host Name . . . . . . . . . . . . : Client1
        Primary DNS Suffix  . . . . . . . : zen.com
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : zen.com

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : zen.com
        Description . . . . . . . . . . . : Intel 82558-based Integrated Etherne
t with Wake on LAN*
        Physical Address. . . . . . . . . : 00-00-E2-20-DB-C2
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.179.12.3
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . : 10.179.12.1
        DHCP Server . . . . . . . . . . . : 10.179.20.1
        DNS Servers . . . . . . . . . . . : 10.179.20.2
        Primary WINS Server . . . . . . . : 10.179.13.2
```

A. IPCONFIG

B. TRACERT

C. PING

D. PATHPING

ANSWER: A

QUESTION NO: 10

Which of the following commands is a Packet sniffer?

A. tcpdump

B. strace

C. nmap

D. tail

ANSWER: A

QUESTION NO: 11

Which of the following wireless security features provides the best wireless security mechanism?

A. WPA

B. WPA with Pre Shared Key

C. WPA with 802.1X authentication

D. WEP

ANSWER: C

QUESTION NO: 12

Adam works as a Computer Hacking Forensic Investigator in a law firm. He has been assigned with his first project. Adam collected all required evidences and clues. He is now required to write an investigative report to present before court for further prosecution of the case. He needs guidelines to write an investigative report for expressing an opinion. Which of the following are the guidelines to write an investigative report in an efficient way?

Each correct answer represents a complete solution. Choose all that apply.

A. All ideas present in the investigative report should flow logically from facts to conclusions.

B. Opinion of a lay witness should be included in the investigative report.

C. The investigative report should be understandable by any reader.

D. There should not be any assumptions made about any facts while writing the investigative report.

ANSWER: A C D

QUESTION NO: 13

Which of the following tools are used to determine the hop counts of an IP packet? Each correct answer represents a complete solution. Choose two.

A. TRACERT

B. Ping

C. IPCONFIG

D. Netstat

ANSWER: A B

QUESTION NO: 14

What are the benefits of creating a new view using role-based CLI?

A. Scalability

B. Operational efficiency

C. Security

D. Availability

ANSWER: B C D

QUESTION NO: 15

Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation?

Each correct answer represents a complete solution. Choose all that apply.

A. Names of the victims

B. Date and time of incident

C. Nature of harassment

D. Location of each incident

ANSWER: A B D

QUESTION NO: 16

Which of the following tools performs comprehensive tests against web servers for multiple items, including over 6100 potentially dangerous files/CGIs?

A. Dsniff

B. Snort

C. Nikto

D. Sniffer

ANSWER: C

QUESTION NO: 17

Which of the following can be applied as countermeasures against DDoS attacks? Each correct answer represents a complete solution. Choose all that apply.

A. Limiting the amount of network bandwidth

B. Blocking IP address

C. Using LM hashes for passwords

D. Using Intrusion detection systems

E. Using the network-ingress filtering

ANSWER: A B D E

QUESTION NO: 18

Which of the following is an example of a firewall?

A. ZoneAlarm

B. PatriotBox

C. Specter

D. KFSensor

ANSWER: A

QUESTION NO: 19

You work as a Network Administrator for NetTech Inc. The company has a Windows Server 2008 domain-based network. The network contains four Windows Server 2008 member servers and 120 Windows Vista client computers. You are implementing a caching-only DNS server on one of the member servers. Your assistant wants to know about the caching-only DNS server. Which of the following statements about the caching-only DNS server are correct? Each correct answer represents a complete solution. Choose three.

A. It hosts zones and authoritative for a particular domain.

B. It reduces the amount of DNS traffic on a Wide Area Network (WAN)

C. It is useful at a site where DNS functionality is needed locally but there is not a requirement for a separate domain for that location.

D. It performs queries, caches the answers, and returns the results.

ANSWER: B C D

QUESTION NO: 20

You work as a Security Professional for PassGuide Inc. The company has a Linux-based network. You want to analyze the network traffic with Snort. You run the following command:

```
snort -v -i eth 0
```

Which of the following information will you get using the above command?

Each correct answer represents a complete solution. Choose all that apply.

A. Protocol statistics

B. Date stamp on the packets

C. Number of packets received and dropped

D. Application layer data

ANSWER: A B C