1D0-570

CIW

CIW v5 Security Professional

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 1D0-570 exam in first attempt and also get high scores to acquire CIW certification.

If you use OfficialCerts 1D0-570 Certification questions and answers, you will experience actual 1D0-570 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our CIW exam prep covers over 95% of the questions and answers that may be appeared in your 1D0-570 exam. Every point from pass4sure 1D0-570 PDF, 1D0-570 review will help you take CIW 1D0-570 exam much easier and become CIW certified.

Here's what you can expect from the OfficialCerts CIW 1D0-570 course:

** Up-to-Date CIW 1D0-570 questions as experienced in the real exam.*
** 100% correct CIW 1D0-570 answers you simply can't find in other 1D0-570 courses.*
** All of our tests are easy to download. Your file will be saved as a 1D0-570 PDF.*
** CIW 1D0-570 brain dump free content featuring the real 1D0-570 test questions.*

CIW 1D0-570 certification exam is of core importance both in your Professional life and CIW certification path. With CIW certification you can get a good job easily in the market and get on your path for success. Professionals who passed CIW 1D0-570 exam training are an absolute favorite in the industry. You will pass CIW 1D0-570 certification test and career opportunities will be open for you.

http://janetdailey.com/?certs=exams.asp?examcode=1D0-570

QUESTION: 1
The chief operations officer (COO) has questioned the need for end-user training. Which of the following is the most effective response?

A. Indicate that you will not be responsible for the next virus outbreak.
B. Remind the CEO about the last virus attack and the expense incurred.
C. Explain that the cost of end-user training is a fraction of the cost of the last security breach caused by end users.
D. Provide statistics that definitively show how end-user training reduces the likelihood of security breaches on the corporate network.

Answer: C

QUESTION: 2
Consider the following sequence: user1@zeppelin:/public$ su - root@zeppelin:~# chmod 1777 /public root@zeppelin:~# exit Which of the following most accurately describes the result of this command?

A. Only the root user can create and delete files in the /public directory.
B. All users can create, delete and read files in the /public directory, but only root has execute permissions.
C. All users can create and read files in the /public directory, but only root can delete another user's file.
D. Any user can create files in the / directory, but no user can delete a file in this directory unless root permissions are obtained.

Answer: C

QUESTION: 3
What is the first step of a gap analysis?

A. Scan the firewall.
B. Review antivirus settings.
C. Review the security policy.
D. Review intrusion-detection software settings.

Answer: C

QUESTION: 4
Consider the following firewall rules:
Incoming traffic:
TCP Port 25
TCP Port 139: Denied
UDP Port 137: Denied
UDP Port 138: Denied
ICMP echo request: Denied
ICMP echo reply: Denied
Outgoing traffic:
TCP Ports 1024 through 65,535 to port 80: Denied
TCP Port 80: Denied
ICMP echo request: Denied
ICMP echo reply: Denied
TCP Port 139: Denied
UDP Port 137: Denied
UDP Port 138: Denied

All company production servers reside behind the corporate firewall. However, you discover that the Web server performance is very low. After sniffing the traffic to the Web server, you learn that the Web server is experiencing a distributed denial-of-service attack in which millions of ping packets are being directed at the server. Which of the following is the most plausible explanation for this situation?

A. There is a flaw in the firewall rule set.
B. The firewall is not configured to block ICMP packets generated by the ping command.
C. The attack is originating from a wireless access point (WAP) connected to the corporate network.
D. The attack is originating from a Web server that has not been properly updated, and which has been infected with a Trojan horse.

Answer: C

QUESTION: 5
A Linux system running Apache Server has received millions of SYN packets that it can no longer respond to, because the client's operator is maliciously withholding the necessary reply packet. What is the most common solution for this problem?

A. Implement SSL.

B. Implement SYN cookie support.
C. Upgrade the TCP/IP stack with new software.
D. Upgrade the operating system to support IPsec.

Answer: B

QUESTION: 6
Two routers in your company network require a firmware upgrade. Which of the following upgrade strategies will reduce downtime?

A. Conducting the upgrade while the routers are still running
B. Upgrading the routers using the latest upgrade software
C. Conducting the upgrade after rebooting the router
D. Upgrading the routers after business hours

Answer: D

QUESTION: 7
You and your team have created a security policy document that is 120 pages long. Which of the following techniques will help ensure that upper-level managers read the essential policy elements?

A. Including a sign-off sheet
B. Including an executive summary
C. Using bold type to emphasize essential elements
D. Using italic type to emphasize essential elements

Answer: B

QUESTION: 8
Which of the following is a main function of a company's information security policy?

A. It obligates the IT department to basic services.
B. It defines basic responsibilities for all stakeholders.
C. It defines the responsibilities of employees and managers.
D. It defines basic responsibilities for executive management.

Answer: B

QUESTION: 9
After consulting with the IT department, you have determined that a particular security solution is quite effective for protecting a particular resource, but not necessary due to the expense. Which of the following was conducted to enable this conclusion?

A. Risk analysis
B. Cost-to-benefit analysis
C. Physical security analysis
D. Resource priority analysis

Answer: B

QUESTION: 10
You want to learn more about a security breach that was recently discovered in a Windows server. Which organization should you consult?

A. ISO
B. SANS
C. CERT
D. IETF

Answer: C

QUESTION: 11
Your supervisor asks you to recommend a firewall. The firewall must provide the following services: The ability to filter specific traffic types (e.g., HTTP, SIP, POP3) User authenticationWeb page caching for later use Which type of firewall would you recommend?

A. Proxy
B. Stateful
C. Packet filter
D. Circuit-based

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams we offer;
http://www.officialcerts.com/allexams.asp

To contact our Support;
http://www.officialcerts.com/support.asp

View FAQs
http://www.officialcerts.com/faq.asp

Download All Exams Samples
http://www.officialcerts.com/samples.asp

To purchase Full Version and updated exam;
http://www.officialcerts.com/allexams.asp

Shop now using PayPal

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google