1D0-470

CIW

CIW Security Professional

Visit: http://www.pass4sureofficial.com/exams.asp?examcode=1D0-470

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your 1D0-470 exam in first attempt, but also you can get a high score to acquire CIW certification.

If you use pass4sureofficial 1D0-470 Certification questions and answers, you will experience actual 1D0-470 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 1D0-470 exam. Every point from pass4sure 1D0-470 PDF, 1D0-470 review will help you take CIW 1D0-470 exam much easier and become CIW certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial CIW 1D0-470 course:

** Up-to-Date CIW 1D0-470 questions taken from the real exam.*
** 100% correct CIW 1D0-470 answers you simply can't find in other 1D0-470 courses.*
** All of our tests are easy to download. Your file will be saved as a 1D0-470 PDF.*
** CIW 1D0-470 brain dump free content featuring the real 1D0-470 test questions.*

CIW 1D0-470 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 1D0-470 exam training are an absolute favorite in the industry. You will pass CIW 1D0-470 certification test and career opportunities will be open for you.

Question: 1
Why is password lockout an effective deterrent to cracking attempts?

A. Passwords cannot be changed through brute-force methods
B. A limited number of login attempts before lockout reduces the number of guesses the potential cracker can made
C. Passwords protected in this manner are impossible to find because they are locked out of the Main flow of information on the WAN
D. Password lockout provides no real improvement over traditional locking methods.

Answer: B

Explanation:
Password lockout is where the user account is locked out and disabled after a specified number of consecutive incorrect password attempts. The duration of the lockout can be a time period, or until an administrator goes in and manually re-enables the account. Usually a time period is used to reduce administration. In either case this reduces the guesses. For example, suppose we set a lockout so that a lockout occurs after 3 failures, and then automatically remove the lockout after 20 minutes. This provides a maximum of 9 failures per hour, or 216 passwords per day. Without lockout, on a fast system, a hacker could probably run thousands of guesses per hour, so password lockout introduces a substantial speed bump to the cracking process.

Incorrect Answers:
A: Password lockout does not affect password changing, unless the account requires the original password to make the change. At this point the hacker already has the password, because entry to the account has already occurred.
C: Whether passwords are in the clear, or encrypted, lockout does not protect the actual password as it flows through the system. Password lockout acts as a governor on attempts to use brute force to guess the actual password. No one is looking for the actual passwords as they flow through the WAN, this is eavesdropping such as sniffing or snooping, and password lockout is not a solution for that type of problem.
D: Password locking is highly effective.

Question: 2
Which of the following choices best defines the Windows NT security account manager?

A. It is the portion of the GINA DLL that controls security
B. It is the database containing the identity of the users and their credentials
C. It is the name of the machine responsible for the management of all the security of the LAN
D. It is the interface that is responsible for logging on and user IDs

Answer: B

Explanation:
The Windows NT security account manager, a.k.a “the SAM” is a set of files that make up the database where user and password information is stored.

Incorrect Answers:
A: The GINA DLL is called to process the logon request. It is only the logon interface that interacts with the user. Eventually the information gathered has to be compared to the SAM, so GINA DLL may USE the SAM, but it does not fit as a definition of the SAM.
C: The machine(s) in Windows NT responsible for security on the LAN is either the Windows NT machine itself (if using local security) or a PDC/BDC domain controller if using Domain accounts. The name of any such machine does not fall in the definition of the SAM.
D: Since the GINA DLL is part of that interface, see the explanation in A above.

Question: 3
Under the level C2 security classification, what does “discretionary access control” mean?

A. Discretionary access control means that the owner of a resource must be able to use that resource
B. Discretionary access control is the ability of the system administrator to limit the time any user spends on a computer
C. Discretionary access control is a policy that limits the use of any resource to a group or a security profile
D. Discretionary access control is a rule set by the security auditor to prevent others from Downloading unauthorized scripts or programs.

Answer: A

Explanation:
This is a definition, and basically it says that the owner of the resource should be able to use the resource. The point is simple, what good is a security system if no one can do their work. Some people will joke that the most secure system is a system that is powered off. And in some senses, this is correct, if the computer is powered off, no code is executed, so no damage can occur. But there would be no discretionary access since the owners of the resources would not be able to use those resources.

Incorrect Answers:
B,C,D: are wrong because they do not fall into the definition, as explained above.

Question: 4
Michel wants to write a computer virus that will cripple UNIX systems. What is going to be the main obstacle preventing him from success?

A. UNIX computers are extremely difficult to access illicitly over the internet, and therefore computer viruses are not an issue with UNIX systems
B. Due to the file permission structure and the number of variations in the UNIX hardware architectures, a virus would have to gain root privileges as well as identify the hardware and UNIX flavor in use.
C. Due to availability of effective free anti-virus tools, computer viruses are caught early and often. Michel’s virus would have to evade detection for it to succeed.
D. Due to the extensive use of ANSI “C” in the programming of UNIX, the virus would have to mimic some of the source code used in the infected iteration of the UNIX operating system

Answer: B

Explanation:
Unix has a strong permission structure that in order to breach the system, root privilege will be required. Root is a superuser account, and is kept locked up by a secure system because of the power that the root user has. Hardware variations will make the use of machine and assembly language difficult. Most viruses depend on modifying machine instructions, and the instruction set can vary widely. Since Unix is written in C language, the operating system is very portable. But to write an effective virus, the use of machine language is NOT portable, so the virus will not really work on all platforms.

Incorrect Answers:
A: Unix systems are easy to access, and many accounts get cracked due to easy passwords or no passwords at all. However, from the accounts that do get accessed, not much damage can be done. The root account has to be breached in order to do some serious damage.

C: Because of the ingenious variations of virus coding, there still is not an effective detection tool to find new virus attacking the system. Usually a virus is found after the fact, and detection tools are put into place to scan for the virus signature of the new virus. Until the virus is detected, and a detection signature is built and distributed, an effective virus can do a lot of damage.

D: Most Unix source code is freely distributed, so finding out the coding will not be difficult. Since the virus does not operate at the C compiler level, but at a lower machine language level, the virus needs to mimic the machine language generated by that source code, which varies based on platform.

Question: 5
Which of the following best describes the problem with share permissions and share points in Windows NT?

A. Share points must be the same value as the directory that serves the share point
B. Share points contains permissions; and any file under the share point must possess the same permissions
C. Share permissions are exclusive to root directories and files; they do not involve share points, which define user permissions
D. Share points are set when connection is established, therefore the static nature of file permissions can conflict with share points if they are not set with read and write permissions for everyone.

Answer: B

Explanation:
If we give assign permission to the share point, this permission is applied to all folders and files within that share point.

Note: A share point is a share in Windows NT and Windows 2000. The share point allows the resource to be shared across the network When using a file system, such as NTFS, the files and directories also have permissions. The effective permissions of a file or directory access through a share point is the most limiting of both. For example, for a file NTFS says read and write, but the share point permissions says read-only. The effective permission is read-only – the most restrictive. The only way to prevent this type of conflict is set the share point permission to full control, and let the NTFS permissions take precedence.

Incorrect Answers:
A: Share point naming is not dependent on the directory (folder) that the share point is based. You can even have multiple sharepoints on the same directory.
C: Share permissions are not exclusive to root directories, they also restrict subdirectories. Also, devices, such as printers, may be assigned permissions which can conflict with the share permissions for that device.
D: Both share permissions and file permissions are applied. Microsoft recommends using Full permission for everyone and restrict with file permission. This is just a recommendation and doesn't have to be followed.

Question: 6
What do the discretionary ACL (access control list) and the system ACL in Windows NT have in common?

A. Both share properties for storing secure object identifiers
B. Both can grant or deny permissions to parts of the system
C. Both are installed by default on the system in different sections of the client/server model
D. Both are responsible for creation of the master access control list

Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time $99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads
http://www.pass4sureofficial.com/allexams.asp

View list of All Study Guides (SG) downloads
http://www.pass4sureofficial.com/study-guides.asp

View list of All Audio Exams (AE) downloads
http://www.pass4sureofficial.com/audio-exams.asp

Download All Exams Samples
http://www.pass4sureofficial.com/samples.asp

To purchase $99 Lifetime Full Access Membership click here
http://www.pass4sureofficial.com/purchase.asp

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	SNIA