Exam Code: 1D0-470
CIW Security Professional

Demo Version

To Access Full Version, Please go to
www.itexamworld.com

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 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

Answer: A

Explanation: Both ACLs are used to restrict or grant access to a resource.
Incorrect Answers:
B: Only the system ACL can restrict parts of the system.
C: Only the system ACL is installed by default. DACL is added later by the administrator when locking down resources.
D: The ACLs work together, but do not create the master access control list.

QUESTION 7
Winlogon loads the GINA DLL. What does the GINA DLL then do?

A. It provides the interface for processing logon requests
B. It creates the link to the user database for the update of the local security authority
C. It creates the link to the master access list on the server
D. It checks the user database for correct date/time stamps of last modification

Answer: A

Explanation: GINA DLL is the interface part of Winlogon that prompts
for the userid and password and checks the values against the SAM database.
Incorrect Answers:
B: The local security authority (LSA) is not updated as the result of the logon request. C:
Any connection to the master access list is not done yet in this stage.
D: The date/time stamps of last modification does not need to be checked. Validation of
the userid and password is what will happen in GINA DLL.

QUESTION 8
You must apply permissions to a file named/home/myname/myfile.txt, and you need to
fulfill the following requirements:
You want full access to the file.
People in your group should be able to read the file.
People in your group should not be able to write the file.
People outside of your group should be denied access to the file.
What are the most secure permissions you would apply to the file?

A. Chage 700/home/myname/myfile.txt
B. Chage 744/home/myname/myfile.txt
C. Chmod
640/home/myname/myfile.txt
D. Chmod 064/home/myname/myfile.txt

Answer: C

Explanation: To change access permissions for a file or directory, the
chmod command is used.
The 6 in the 640 gives the owner, read and write permissions (execute is not required as this is a text file). The 4 in the 640 gives read only access to people in my group. And the 0 in the 640 prevents any access by anyone else.
Note:
Access permissions are expressed as three digits: user (=you), group, other.
Each digit codes permission as follows
1 = execute only
2 = write only
3 = write and execute (1 + 2)
4 = read only
5 = read and execute (4 + 1)
6 = read and write (4 + 2)
7 = read and write and execute (4 + 2 + 1)
Incorrect Answers:
A & B: The change age command is used for password aging for logon commands, and
right off the bat are not
even the commands to be used to set permissions.
D: A value of 064 locks me out as owner (I can't access my file), The groups have read

and write access, and everyone else will have read-only access. All in conflict with the requirements of the question.

QUESTION 9
Which level(s) of security as defined by the National Computer Security Center (NCSC) is attained by many "out of the box" implementations of commercially available operating systems?

A. Level B2
B. Level D
C. Level D through B2
D. Level B through B2

Answer: C

Explanation: Most products are rated at between D (minimal security) to B2. Windows NT has obtained a C2 rating, which is in-between.
Below is a summary of the various Security Levels, for a complete reference see: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html - HDR1
D: MINIMAL PROTECTION - This division contains only one class. It is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.
C: DISCRETIONARY PROTECTION
Classes in this division provide for discretionary (need-to-know) protection and, through the inclusion of audit capabilities, for accountability of subjects and the actions they initiate.
C1: DISCRETIONARY SECURITY PROTECTION
The Trusted Computing Base (TCB) of a class (C1) system nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data. The class (C1) environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.
C2: CONTROLLED ACCESS PROTECTION
Systems in this class enforce a more finely grained discretionary access control than (C1) systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.
B: MANDATORY PROTECTION
The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.
B1: LABELED SECURITY PROTECTION
Class (B1) systems require all the features required for class (C2). In addition, an informal statement of the security policy model, data labelling, and mandatory access control over named subjects and objects must be present. The capability must exist for

om

accurately labelling exported information. Any flaws identified by testing must be removed.
B2: STRUCTURED PROTECTION
In class (B2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) systems be extended to all subjects and objects in the ADP system. In addition, covert channels are addressed. The TCB must be carefully structured into protection-critical and non-protection-critical elements. The TCB interface is well defined and the TCB design and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for system administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration.
B3: SECURITY DOMAINS
The class (B3) TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant system engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security- relevant events, and system recovery procedures are required. The system is highly resistant to penetration.
A: VERIFIED PROTECTIONThis division is characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development and implementation.
A1: VERIFIED DESIGN
Systems in class (A1) are functionally equivalent to those in class (B3) in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature, starting with a formal model of the security policy and a formal top-level specification (FTLS) of the design.
Incorrect Answers:
A: The B2 is a high rating, and many systems don't achieve being classified as B2.
B: The D rating, which is minimal security, does not represent most systems, since many out of the box operating systems at least have some security or better.
D: The B to B2 rating is pretty high, and many systems don't achieve a system that tight.

QUESTION 10
What are the security issues that arise in the use of the NFS (Network File System)?

A. Synchronization of user and group IDs is poor, so it is easy to spoof trusted hosts and user names.
B. The lack of logging in one place or on one machine, and the multiple logs this then

requires, can create bottlenecks
C. The possibility arises for Cleartext passwords to be sniffed on the network if it does not use Secure RPC.
D. NFS uses a weak authentication scheme and transfers information in encrypted form

Answer: A

Explanation: Since the authentication is weak, it is easy to break into the session and spoof node addresses.
Incorrect Answers:
B: Logging bottlenecks are a performance issue, not a security issue.
C: The passwords are not cleartext, although the authentication algorithm is weak.
D: NFS was not designed with security in mind. NFS suffers from a poor authentication algorithm.NFS requests can be easily spoofed. However, data is not encrypted.

QUESTION 11
What is the major security issue with standard NIS (Network Information System)?
A. It is impossible to enforce a centralized login schemeB. NIS provides no authentication requirement in its native stateC. There is no way to encrypt data being transferred
D. NIS is a legacy service and, as such, is only used in order, less secure operating systems and networks

Answer: B

Explanation: The NIS service is inherently insecure. If you use NIS it is a constant target for unauthorized access to network.NIS is a method of distributing information throughout networks and was developed in the 1980s by Sun Microsystems.
Incorrect Answers:
A: NIS was designed to allow centralised administration of many machines. C: Encryption can very well be used in NIS.
D: NIS, Network Information Service, is a service designed to propagate information across the network. It is not a legacy service. It is a hot academic and research subject.

QUESTION 12
In a Linux system, how do you stop the POP3, IMAPD, and FTP services?

A. By changing the permissions on the configuration file that controls the service (/sbin/inetd), then recompiling /etc/inetd.config
B. By commenting out the service using the # symbol in the text file /etc/inetd.conf, then restarting the inetd daemon
C. By recompiling the system kernel, making sure you have disabled that service
D. By commenting out the service using the $ symbol in the text file /etc/inetd.conf, then restarting the inetd daemon.

Answer: B

Explanation: Use the # symbol to comment out the service, then restart inetd.
Incorrect Answers:
A: If this made any sense, you would also lock out the WWW service and disable the Web Server, which is not want you want to do here. Inetd.conf does not get compiled.
C: The services for inetd are loaded based on the control cards in the text file. It is not specified in the kernel, so recompiling it will not accomplish stopping the services.
D: The comment symbol is a #, not a $.

QUESTION 13
Which of the following choices lists the ports that Microsoft internal networking uses that should be blocked from outside access?

A. UDP 137 and 138, and TCP 139
B. Ports 11, 112, and 79
C. UDP 1028, 31337 and 6000
D. Port 80, 134 and 31337

Answer: A

Explanation: UDP & TCP 137 are used for NETBIOS name service. UDP 138 is used for the NETBIOS Datagram Service, and TCP 139 is used for the NETBIOS Session Service. Internal networking for Microsoft Windows systems uses NETBIOS for its redirector. Hacking into the Windows systems would be blocked if NETBIOS could not pass through the firewall. To logon to Windows, or access file or printer shares, access will have to be done via SMB (Service Message Blocks) which ride on NETBIOS.
Incorrect Answers:
B: 11 is systat, 112 is not used, and 79 is finger. Although you might want to block out these ports, including port 79 (finger) which can expose server information to a hacker, these are not part of Microsoft internal networking.
C: These ports are outside of the well known ports, and blocking them does not close any holes. These ports are not part of Microsoft internal networking.
D: Port 80 is HTTP, so to block it disables web browsing. Port 134 is not assigned to a service, and port 31337 is not a well known port. These ports are not part of Microsoft internal networking.

QUESTION 14
What is the best way to keep employees on a LAN from unauthorized activity or other mischief?

A. Reduce each user's permissions to the minimum needed to perform the tasks required by his or her job
B. Limit the number of logins available to all users to one at a time

C. Limit the number of files that any one user can have open at any given time
D. Implement a zero-tolerance policy in regard to employees who load games or other unauthorized software on the company's computers

Answer: A

Explanation: Obviously you don't give the employees free roam of the LAN. Accidents can happen (type a file name or file path wrong) or some employees may become curious. By giving them only the permissions that they need to do their job, can drastically limit where those users can go and cause damage.
Incorrect Answers:
B: The objective in the question is how to prevent an employee from unauthorized activity. Having multiple logons does cause some security concerns, but not that of the user. As long as the permissions are locked up tight, it won't matter how many logons the user has, if one can't get unauthorized access, then none should,
C: To limit the number of open files does not prevent this activity, and may prevent the user from actually doing work. Some programs will open multiple files, most programs open more than one file.
D: This is a good step and policy to implement. It still does not prevent unauthorized activity of corporate assets.

QUESTION 15
What is a spoofing attack?

A. A hacker pretends to be the superuser and spoofs a user into allowing him into the system
B. A hacker calls a user and pretends to be a system administrator in order to get the user's password
C. A computer (or network) pretends to be a trusted host (or network)
D. A hacker gains entrance to the building where the network resides and accesses the system by pretending to be an employee

Answer: C

Explanation: Spoofing is usually when you change your identity to portray yourself as someone else. One example is to change the source IP address in an IP packet to make it appear that the packet was sent by someone else.
Incorrect Answers:
A: The program that acts as another program is not called spoofing. This technique is called man in the middle.
B: This is called social engineering.
D: This is called social engineering.

QUESTION 16
Abjee is going to log on to his network. His network does not employ traffic padding mechanisms. Why will it be easy for someone to steal his password?

A. Because his password could be more than two weeks oldB. Because of he predictability of the length of the login and password promptsC. Because the Cleartext user name and password are not encrypted
D. Because there is no provision for log analysis without traffic padding, thus no accountability when passwords are lost

Answer: B

Explanation: By monitoring the size of the packets, it could be determined the password length. This makes brute force attacks easier to conduct, since you can eliminate passwords that are shorter or longer than the detected amount. Another issue on padding is timing. Suppose the successful password took longer to process, but the failed password gave a quick response. Using this timing, a hacker could determine whether a password would work just based on the response time of the login. If bad logons were padded out so they look the same elapsed time as a successful login, then this guessing and analysis could not be done.
Incorrect Answers:
A: Traffic padding would not protect a password based on the age of the password.
C: Passwords that are encrypted will still be the same length, because encryption is not compression. So it does not matter whether the password is in the clear or encrypted, the key here is to prevent guessing of the password length to make password guessing more difficult.
D: Log analysis is not related to traffic padding. The passwords would not even be logged, as that causes potential exposure of gaining access to the passwords, should the log file be compromised.

QUESTION 17
In a typical corporate environment, which of the following resources demands the highest level of security on the network?

A. Purchasing
B. Engineering
C. Sales
D. Accounting

Answer: D

Explanation: Accounting information is highly confidential and crucial for a business.
Incorrect Answers:
A: Purchasing is usually an internal application, and would not have outside users accessing the system. However, outside vendors may be given access to the system, but the vendors are identified up front, so they can be controlled, if necessary.
B: Engineering applications would be an internal application, with few outside users. If there are outside users, these can be easily identified and controlled,
C: Sales require high security as well. However, accounting demands the highest level of security.

om

Note: Sales will require the high security because using electronic sales, such as an e-commerce site, communicates with customers that will be accessing the sales application from outside the safe and confined corporate network. Many transactions may require the exchange of confidential information, including the customer's credit card information. For these types of transactions, SET (Secure Electronic Transactions) using SSL (Secure Sockets Layer) is commonly used to provide a secure transaction. Most of the potential customers are unknown until they want to make a purchase, leaving little notice and little control over the customers who want to make a purchase.

QUESTION 18
Luke is documenting all of his network attributes. He wants to know the type of network-level information that is represented by the locations of access panels, wiring closets and server rooms. Which of the following is the correct term for this activity?

A. Network mapping
B. IP service routing
C. Router and switch designing
D. War dialing

Answer: A

Explanation: Network mapping is the process of documenting and diagramming the network infrastructure. This includes locations of access panels, wiring closets and server rooms.
Incorrect Answers:
B: IP service routing concerns the routing of IP packets and not the documentation of the location of access panels, wiring closets and server rooms.
C: Router and switch designing concerns the planning of the deployment of routers and switches.
D: War dialing is a process used by hackers to find and locate modem banks. The dialer will dial phone numbers until it hit a modem carrier signal. This computer cracking technique uses a software program to automatically call thousands of telephone numbers to look for any that have a modem attached.

QUESTION 19
Which service, command or tool allows a remote user to interface with a system as if he were sitting at the terminal?

A. Host
B. Finger
C. SetRequest
D. Telnet

Answer: D

Explanation: Telnet, which operates on port 23, is a client that provides a terminal window on the target system.
Incorrect Answers:

om

A: Host is a Unix based command used to resolve a host name to an IP addresss, or IP address to the host name, and can also provide information on mail servers.
B: Finger is a command used to find out information about a node.
C: SetRequest is a function of SNMP, which is used for network monitoring and control.

QUESTION 20
Which command, tool or service on a UNIX network converts names to IP addresses and IP addresses to names, and can also specify which servers are mail servers?

A. Port scanner
B. Traceroute
C. Host
D. Nslookup

Answer: C

Explanation: The Host command can provide these functions.
Incorrect Answers:
A: A port scanner is used to check well known ports to find out which services are running at a particular target node.
B: Traceroute is used to trace the network hops and nodes between the host issuing the command and the target IP address. This is a diagnostic tool based on ICMP.
D: NSLookup is used to lookup names in a DNS server. It will provide information, including IP addresses and mail servers, but only if the name is registered in DNS. NSLookup can point to a specified name server.
