

1D0-470

TEST KING



LEADING THE WAY IN IT
TESTING AND CERTIFICATION TOOLS!

CIW SECURITY PROFESSIONAL

Version 2.2

Leading the way in IT testing and certification tools, www.testking.com

Important Note Please Read Carefully

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check for an update 3-4 days before you have scheduled the exam.

Here is the procedure to get the latest version:

1. Go to www.testking.com
2. Click on **Login** (upper right corner)
3. Enter e-mail and password
4. The latest versions of all purchased products are downloadable from here. Just click the links.
Note: If you have network connectivity problems it could be better to right-click on the link and choose **Save target as**. You would then be able to watch the download progress.

For most updates it is enough just to print the new questions at the end of the new version, not the whole document.

Feedback

Feedback on specific questions should be sent to feedback@testking.com. You should state

1. Exam number and version.
2. Question number.
3. Order number and login ID.

We will answer your mail promptly.

Copyright

Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if you find out that particular pdf file is being distributed by you, Testking will reserve the right to take legal action against you according to the International Copyright Law. So don't distribute this PDF file.

Q. 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 make
- 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.

Q. 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.

Q. 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.

Q. 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.

Q. 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.

Q. 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.

Q. 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.

Q. 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.

Q. 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 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 PROTECTION

This 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.

Q. 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.

Q. 11

What is the major security issue with standard NIS (Network Information System)?

- A. It is impossible to enforce a centralized login scheme
- B. NIS provides no authentication requirement in its native state
- C. There is no way to encrypt data being transferred
- D. NIS is a legacy service and, as such, is only used in older, 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 centralized 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.

Q. 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 what 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 \$.

Q. 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.

Q. 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.

Q. 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.

Q. 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 old
- B. Because of the predictability of the length of the login and password prompts
- C. 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.

Q. 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.
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.

Q. 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.

Q. 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:

- A:** Host is a Unix based command used to resolve a host name to an IP address, 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.

Q. 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.

Q. 21

Kerstin connected to an e-commerce site and brought a new mouse pad with her credit card for \$5.00 plus shipping and handling. She never received her mouse pad so she called her credit card company to cancel the transaction. She was not charged for the mouse pad, but she received multiple charges she knew nothing about. She tried to connect to the site again but could not find it. Which type of hacking attack occurred?

- A. Denial-of-service attack
- B. Hijacking attack
- C. Illicit server attack
- D. Spoofing attack

Answer: B

Explanation: This is a form of the man in the middle attack, where the hacker gathers the data and acts as one of the legitimate parties to the transaction.

Incorrect Answers:

- A:** A denial-of-service attack involves flooding a node so that the node cannot respond to other requests.
- C:** For this type of attack, Kerstin would have actually contacted the real e-commerce server, but code on that server would have been modified or replaced. Since Kerstin cannot locate the server anymore, this indicates that the transaction was with a rouge server.
- D:** Spoofing is most likely required in order to impersonate the e-commerce server, by spoofing the destination address. However, the e-commerce attack could also be done using other means to intercept the transaction, such as poisoning a DSN server. So, although spoofing can be used, it does not mean that spoofing was actually used.

Q. 22

Which service, tool or command allows a remote or local user to learn the directories or files that are accessible on the network?

- A. Traceroute
- B. Share scanner
- C. Port scanner
- D. Ping scanner

Answer: B

Explanation: Files and Directories in a Windows like environment (including Samba on Linux & Unix) can be located and detected using a share scanner. Files and directories are made available to a network by sharing those resources as a share.

Incorrect Answers:

- A:** Traceroute is used to locate and identify hops and map out a network, It is used as a diagnostic tool to determine where connectivity breaks down.
- C:** A port scanner is used to identify open and active ports on a node.
- D:** A ping scanner is used to expose the IP addresses on a network, to perform network mapping. Only the IP addresses are exposed, not the port numbers.

Q. 23

Which type of attack utilizes an unauthorized service or daemon running on your system to send out information to a hacker that can be used to further compromise the system?

- A. Virus attack
- B. Hijacking attack
- C. Man-in-the-middle attack
- D. Illicit server attack

Answer: D

Explanation: An illicit server attack is when you have an unauthorized service or daemon running on the system that can cause harm.

Incorrect Answers:

- A:** A virus attack is when a program or macro is executed and the virus is implanted into another executable. A virus can be used to implant the code for the illicit server attack, but the actual illicit server attack is when the service or daemon is running.
- B:** A hijacking attack is when someone gets in the middle of a transaction and takes over the transaction, spoofing himself as the original transaction partner.
- C:** A man-in-the-middle attack is also when someone gets in the middle of a transaction between two servers and intercepts the transaction flow. This differs slightly from the hijacking attack. In the hijacking attack the man-in-the-middle actually cuts in and impersonates one the partners, but in a man-in-the-middle attack, the intervening party only eavesdrops and listens to the stream.

Q. 24

Which type of attack uses a simple or complex program that self-replicates and/or deposits a payload on a remote or local computer?

- A. Dictionary attack
- B. Hijacking attack
- C. Illicit server attack
- D. Virus attack

Answer: D

Explanation: This is what a virus does.

Incorrect Answers:

- A:** A dictionary attack is the process of trying every character combination to guess a password (brute force) or using a dictionary type program to generate and try all character combinations.
- B:** A hijacking attack is when someone gets in the middle of a transaction and takes over the transaction, spoofing himself as the original transaction partner.
- C:** An illicit server attack utilizes an unauthorized service or daemon running on your system to send out information to a hacker that can be used to further compromise the system.

Q. 25

Which type of attack can use a worm or packet sniffer to crash systems, causing low resources and/or consuming bandwidth?

- A. Denial-of-service attack
- B. Illicit server attack
- C. Man-in-the-middle attack
- D. Virus attack

Answer: A

Explanation: A denial of service attack (DoS) is when a hacker causes access to a server, network, or other resource to be denied. One common method of DoS is to crash the network components so that network connectivity is lost. Another method is to flood the server or network with excessive traffic so that no one else can get in and access that sever or network. In order to do that, resources have to be depleted, or all of the bandwidth taken up. The bottom line is to consume most, if not all, of the resources so that other users, legitimate users, are locked out.

Incorrect Answers:

- B:** An illicit server attack utilizes an unauthorized service or daemon running on your system to send out information to a hacker that can be used to further compromise the system.
- C:** A man-in-the-middle attack is also when someone gets in the middle of a transaction between two servers and intercepts the transaction flow. This differs slightly from the hijacking attack. In the hijacking attack the man-in-the-middle actually cuts in and impersonates one the partners, but in a man-in-the-middle attack, the intervening party only eavesdrops and listens to the stream.
- D:** A virus is a type of attack that uses a simple or complex program that self-replicates and/or deposits a payload on a remote or local computer

Q. 26

Which service, command or tool discovers the IP addresses of all computers or routers between two computers on an internet/intranet network?

- A. Whois
- B. Port scanner
- C. Traceroute
- D. Nslookup

Answer: C

Explanation: The traceroute command is used to determine the hops between two computers, and identify their IP addresses. One of the computers is the computer where the traceroute command is executed. Traceroute uses the ICMP command, and limits the maximum hop count, until either the destination is reached or a timeout occurs.

Incorrect Answers:

- A:** The WHOIS command is used to discover primary and secondary name servers.
- B:** The port scanner is used to determine the active ports on a node..
- D:** The NSLOOKUP command is used to test out entries in a name server. If you can successfully imitate a secondary name server with NSLOOKUP you can initiate a Zone transfer with a Master. With a zone

transfer you can identify the IP address to Name mappings of all registered nodes. The reason why this is not the answer is that NSLOOKUP only discovers registered nodes, so if the node is not in DNS, or the mapping is wrong, or the node is obsolete but not deleted, you end up with a lot of missing and inaccurate information. Usually a router is not registered in DNS, so you would not get most of the routers. Compared to either the ping scanner or port scanner, those scanners perform live polling commands against the network and identify live and operational nodes. Even if you discovered the nodes, you can't generate a map to determine which of those nodes are in the path. TRACEROUTE will map the actual route, but NSLOOKUP will just tell you which nodes may be there, but it cannot give you the path, nor is the list accurate.

Q. 27

Which tool, service or command will enable you to learn the entire address range used by an organization or company?

- A. Traceroute
- B. Nslookup
- C. Port scanner
- D. Ping scanner

Answer: D

Explanation: A ping scanner is used to do network mapping. If you are able to ping a server, you can get its IP address. With the IP address, you can ping all addresses in that IP range to discover other devices on the network, mapping the responses that are received.

Incorrect Answers:

- A:** The TRACEROUTE command is used to identify hops between the source and target machines. It can be used to map out the location of routers within the network.
- B:** The NSLOOKUP command is used to test out entries in a name server. If you can successfully imitate a secondary name server with NSLOOKUP you can initiate a Zone transfer with a Master. With a zone transfer you can identify the IP address to Name mappings of all registered nodes. The reason why this is not the answer is that NSLOOKUP only discovers registered nodes, so if the node is not in DNS, or the mapping is wrong, or the node is obsolete but not deleted, you end up with a lot of missing and inaccurate information. Usually a router is not registered in DNS, so you would not get most of the routers. Compared to either the ping scanner or port scanner, those scanners perform live polling commands against the network and identify live and operational nodes.
- C:** A port scanner is similar to a ping scanner in that it discovers the IP addresses, but a port scanner also discovers active ports, and is mainly used for that purpose..

Q. 28

What is the final step in assessing the risk of network intrusion from an internal or external source?

- A. Using the existing management and control architecture
- B. Evaluating the existing perimeter and internal security
- C. Analyzing, categorizing and prioritizing resources
- D. Considering the business concerns

Answer: A

Explanation: All four proposed answers are part of the risk assessment. What I am going to do is list them in the proper order:

Analyzing, categorizing and prioritizing resources
Considering the business concerns
Evaluating the existing perimeter and internal security
Using the existing management and control architecture

Q. 29

A file is replaced by another file that provides the same service but also has a secret operation that is meant to subvert security. What is this type of attack called?

- A. A buffer overflow attack
- B. A Trojan attack
- C. A denial-of-service attack
- D. An illicit server attack

Answer: B

Explanation: This question can be confused with the illicit server attack. The question is asking about the process of the file replacement, not the execution of the service that the file provides. The file replacement process, where a file containing a service – but with a security back door, is called a Trojan horse, usually passed as the result of a virus.

Incorrect Answers:

- A:** A buffer overflow attack is where you send enough data to either deplete all the buffers or overflow the buffer itself. For example, you send a packet that is larger than the maximum size of the buffer, causing part of the system to be overlaid, and crashing the task or system. This occurs when there are bugs in the code that do not properly check for these conditions, and corrupt the system, leading to a failure.
- C:** Denial of service is when the attack prevents legitimate users from accessing the server. Usually the server is flooded with so many messages that no one else can gain access. Of course, if you crash the

server, and the server is down, that too is a denial of service because the server was made inaccessible to legitimate users.

D: An illicit server attack is when you have an unauthorized service or daemon running on the system that can cause harm.

Q. 30

Most hackers run two services first learn information about a computer or Windows server attached to the Internet or intranet. These services enable hackers to find weaknesses in order to infiltrate the computer or network. Which one of the following choices lists the two services?

- A. Ping and traceroute
- B. Nslookup and whois
- C. Whois and ping
- D. Nslookup and traceroute

Answer: B

Explanation: WHOIS is used to gain information about the primary and secondary name servers. NSLOOKUP is then used to query these name servers to find names and types of existent resources on the network. These tools are used by the hacker in the discovery phase.

Incorrect Answers:

- A:** The traceroute and the ping commands are essentially the same, both built on the ICMP command. Ping tells you if you can contact the target, and so does traceroute. However, traceroute ALSO gives you the path to the server, identifying hops and the routers along the way. Essentially the two commands are redundant.
- C:** Ping is useful to test connectivity and existence of resources. Nslookup is, however, a much more dangerous tool in the hands of a hacker.
- D:** WHOIS would identify the primary and secondary name servers, which you would need before you can use the NSLOOKUP command to query the name servers. At this stage, a ping would be sufficient to find IP addresses in use, and it is not required yet to determine path information.

Q. 31

What common target can be reconfigured to disable an interface and provide inaccurate IP addresses over the Internet?

- A. Routers
- B. E-mail servers
- C. DNS servers

D. Databases

Answer: A

Explanation: Routers are attacked, because they may have weak security. If the router uses SNMP, which passes the community name in cleartext, attacking the router is an easy target. One into the router, either via SNMP or using Telnet, interfaces can be disabled, or reconfigured with a new address.

Incorrect Answers:

- B:** E-mail servers do not have an interface that can be disabled, nor would it be easy to target the e-mail server to change the IP address.
- C:** DNS servers do not have an interface that can be disabled, no would it be easy to target the DNS server to change the IP address. It is possible to hack a secondary DNS server and fake a zone transfer into it, thus changing the addresses that the DNS server provides. But the server does not provide a means that a hacker can get into configuration and disable any interfaces.
- D:** Databases do not have interfaces (although database servers do), nor are there IP addresses in the databases that could be used to allow inaccurate distribution of data.

Q. 32

Lucy obtains the latest stable versions of server, services or applications. Which type of attack does this action help to prevent?

- A. Dictionary attack
- B. Buffer overflow attack
- C. Trojan attack
- D. Illicit server attack

Answer: B

Explanation: A buffer overflow attack is where you send enough data to either deplete all the buffers or overflow the buffer itself. For example, you send a packet that is larger than the maximum size of the buffer, causing part of the system to be overlaid, and crashing the task or system. This occurs when there are bugs in the code that do not properly check for these conditions, and corrupt the system, leading to a failure. These bugs are discovered as the system matures, and when the bugs are discovered, the vendor will distribute fixes to plug the holes.

Incorrect Answers:

- A:** A dictionary attack does not exploit bugs or holes in the system, so applying fixes should not help prevent the attack.
- C:** A trojan attack does not exploit bugs or holes in the system, so applying fixes should not help prevent the attack. Note that a Trojan may have been deposited by a virus and maybe the fixes will prevent or

irradiate the virus, but the Trojan horse has overlaid some code somewhere, and unless the fixes remove or replace the actual Trojan code, a Trojan attack is not prevented.

D: An illicit sever attack uses the same reasoning as why a Trojan attack would not be prevented.

Q. 33

What host-level information would you want to obtain so you can exploit defaults and patches?

- A. Servers
- B. Routers and switches
- C. Databases
- D. Firewall types

Answer: A

Explanation: Defaults and patches are applied to servers. In order to exploit default and lack of patches you must gain access to the servers. It is very important to hardening the Operating System by removing defaults and keeping updates, patches, hot fixes and service packs current.

Note: The way the exploitation works is this: Holes in security are discovered and published by the vendor, with a fix. Sometimes the vendor even gives an example of how to exploit the system so that the fix can be tested. Not everyone applies the fixes, consider the philosophy if it isn't broke, don't fix it. So a hacker identifies the server, checks the vendors site for vulnerabilities, and then makes the attack hoping that the fixes were not applied to the system, which leads to a breach.

Incorrect Answers:

- B:** Knowing the routers and switches does not usually provide a point of exposure. Although routers and switches are hardware devices, these devices do use code such as BIOS and firmware, and this code can be patched or upgraded. However, security exposures using hardware devices are very rare and usually don't provide a point of exploitation.
- C:** Knowing and processing databases do not provide an exposure point. Interfaces to the databases may be exploited to attack the databases, and databases may be left with default accounts, but you need to know the type of database and the version.
- D:** The outline line of defense is the firewall, however, defaults and patches on firewalls are not as useful for the hacker as they are on servers. If the operating system is not hardened the configuration of the firewall protection will not work.

Q. 34

Which of the following is a way to get around a firewall to intrude into a secure network from a remote location?

- A. IP services
- B. Active ports
- C. Identified network topology
- D. Modem banks

Answer: D

Explanation: Modem banks can provide a bypass to the firewall if the modem banks are connected INSIDE the network. The modem banks should be outside the network, for example installed in a DMZ.

Incorrect Answers:

- A:** The firewall should be filtering IP traffic, so IP services should not be able to bypass the firewall.
- B:** Active ports on the firewall should be handled by the firewall and protected. Active ports within the network are not an exposure since the firewall should prevent the passing of data to those ports.
- C:** Knowing the network topology may help, by understanding how the network is mapped. But knowing the network does not mean that you can bypass the devices in place to protect the network, unless there are other points into the network that are not protected.

Q. 35

You notice that your FTP service reveals unnecessary information about your server. Which of the following is the most efficient solution to this problem?

- A. Filter out the login banner using a packet filter
- B. Disable the service in question
- C. Place the service behind the firewall
- D. Disable the login banner for the service

Answer: D

Explanation: If the welcome message / login banner is a problem, then disable it.

Incorrect Answers:

- A:** The login banner is not a specific port or protocol that would allow a packet filter. If you applied the packet filter, then the FTP process won't work at all.
- B:** Disable the service, which is FTP, and it is unusable. You will stop the disclosure of the information, but you can't use FTP anymore.
- C:** Placing the service behind the firewall will not prevent disclosure of the information. The firewall will act like a packet filter, and can't distinguish the banner from the data to be transferred.

Q. 36

What is the most common security problem on a client/server network?

- A. Outdated software
- B. Old login accounts
- C. Non-secured ports
- D. Browser flaws

Answer: C

Explanation: These are ALL common security problems, making the choice of the most common difficult. Non-secured ports has to be the most common because ports are open and non-secured by default. It takes an action to determine which ports should be enabled and which locked up, and then to actually secure them. For most of the nodes that are installed, there is usually no effort to lock down the ports, especially for services not being used. Home users would be the most vulnerable because they will run a system right out of the box and not be aware of the ports being open and exposed. These systems are then connected to the Internet, without firewalls, and open the system for attack.

Incorrect Answers:

- A:** Outdated software could pose a threat if a known vulnerability was not corrected. Although this could be a common problem, it is not common security problem.
- B:** Old Login accounts don't pose a major threat unless the accounts can be identified and breached.
- D:** Browser flaws are rare, but security loopholes are occasionally found.

Q. 37

While assessing the risk of a network, which step are you conducting when you determine whether the network can differentiate itself from other networks?

- A. Considering the business concerns
- B. Analyzing, categorizing and prioritizing resources
- C. Evaluating the existing perimeter and internal security
- D. Using the existing management and control architecture

Answer: C

Explanation: When evaluating the existing perimeter, one task is to determine whether the network can differentiate itself from other networks.

Incorrect Answers:

- A:** Considering the business concerns is the process of looking at customer needs and gearing the solution to satisfy those needs.
- B:** Analyzing, categorizing and prioritizing resources – this is where you need to identify the most critical pieces of the network.
- D:** Using the existing management and control architecture, this is the process of using what is already in place.

Q. 38

Which type of attack occurs when a hacker obtains passwords and other information from legitimate transactions?

- A. Man-in-the-middle attack
- B. Denial-of-service attack
- C. Dictionary attack
- D. Illicit server attack

Answer: A

Explanation: A man-in-the-middle attack is when someone gets in the middle of a transaction between two servers and intercepts the transaction flow. This differs slightly from the hijacking attack. In the hijacking attack the man-in-the-middle actually cuts in and impersonates one of the partners, but in a man-in-the-middle attack, the intervening party only eavesdrops and listens to the stream.

Incorrect Answers:

- B:** Denial of service is when the attack prevents legitimate users from accessing the server. Usually the server is flooded with so many messages that no one else can gain access. Of course, if you crash the server, and the server is down, that too is a denial of service because the server was made inaccessible to legitimate users.
- C:** A dictionary attack is the process of trying every character combination to guess a password (brute force) or using a dictionary type program to generate and try all character combinations.
- D:** An illicit server attack is when you have an unauthorized service or daemon running on the system that can cause harm.

Q. 39

Which of the following layers of TCP/IP stacks is the most difficult to secure?

- A. Physical
- B. Network
- C. Transport

D. Application

Answer: D

Explanation: Securing the application layer is difficult since the application code on that layer is more diverse and written by many different entities. There is no security standard, and too many different developers are involved.

Incorrect Answers:

A, B, C: are lower layers within the OSI model. These layers are more standardized, and there are too not many variations. Outside of vendors, there are very few entities that will write their own interfaces on those levels. This makes it easier to standardize, and secure.

Q. 40

Kerstin wants to improve the security on her FTP server. She is worried about password-sniffing attacks. Which of the following is the best action for her to take?

- A. Disable anonymous logins
- B. Allow only anonymous logins
- C. Configure the firewall to block port 21
- D. Place the FTP server outside of the firewall

Answer: B

Explanation: FTP transfers login information in the clear. By setting the FTP server to allow only anonymous logins, no one can log into FTP using a valid user/password pairs. If the logins with passwords are prevented, then there is nothing to be exposed on the network by someone using a packet sniffer.

Incorrect Answers:

- A:** Disabling anonymous logins do not lock out the server. Anonymous logins are guest accounts and usually can't cause that much damage. However, allowing user/password pairs to login – of real passwords – is an exposure since the password are transferred in the clear and can be extracted from the packet flow on the network.
- C:** This will protect the user/password pairs, but also disables FTP. Making FTP unusable is most likely an undesired result.
- D:** Placing the FTP server on any side of the firewall does not protect the data. The passwords are still transmitted in cleartext and anyone can steal the user and password pairs for valid accounts.

Q. 41

What is the primary security problem with FTP?

- A. Anonymous logins do not require a password
- B. Damaging programs can be executed on the client
- C. Damaging programs can be executed on the server
- D. The login name and password are sent to the server in cleartext

Answer: D

Explanation: FTP transmits user name and password in the clear. Anyone on the LAN where that traffic passes through can monitor the line with a packet analyzer (or sniffer) and capture those login accounts.

Incorrect Answers:

- A:** Well, it is true that anonymous logins do not require a password. The anonymous account is not usually given permissions that allow it to do damage.
- B, C:** FTP does not execute programs at neither the client nor the server. All it does is download or upload the files.

Q. 42

Which type of port is used by a client when it establishes a TCP connection?

- A. Ephemeral
- B. Well-known
- C. Reserved
- D. Static

Answer: A

Explanation: When a connection is established the client side of the connection must use a source port number. Unless a client program explicitly requests a specific port number, the port number used is an ephemeral port number. Ephemeral ports are those ports above 1023 (1024-65535). These ports are dynamically assigned to the client, and released by the client. Once released, these ports may be used again by a different client.

Incorrect Answers:

- B:** A client could explicitly use a well-known TCP port. The default behavior, however, is to use a ephemeral port.
- C:** A reserved port is a port that is not yet assigned, and should not be used unless a formal assignment has been made by registering the port with the appropriate Internet registry service.

D: A static port is a port that is always open or closed. A dynamic port is a port that opens when it is assigned to a client or service, and then closes when the service or client releases the port. Dynamic ports are used in environments such as firewalls and proxy servers to hide ports and services, for example to limit the findings of a port scanner.

Q. 43

Which system provides relay services between two devices?

- A. Proxy server
- B. Gateway
- C. VPN
- D. Screening router

Answer: B

Explanation: By definition a gateway is a device that relays services between two systems. One example is a gateway that connects two (or more) network segments. This gateway is used when the two networks have different protocols and the gateway has to do a protocol conversion. The gateway then provides relay services between devices in the different segments.

Incorrect Answers:

- A:** A Proxy Server also connects two (or more) networks segments, and acts as a single control point to perform requests on behalf of the requesting client
- C:** A VPN (Virtual Private Network) provides secure remote point-to-point communication. It doesn't provide relay services.
- D:** A screen routing connects two (or more) network segments. It is a type of firewall, it only uses packet filters.

Q. 44

Which port does FTP use for a control connection?

- A. 21
- B. 25
- C. 53
- D. 162

Answer: A

Explanation: FTP uses Port 21 for the control connection.

Incorrect Answers:

- B:** Port 25 is used for SMTP.
- C:** Port 53 is used for DNS
- D:** Port 162 is used in SNMP (Trap).

Q. 45

Which port is used by DNS when conducting zone transfers?

- A. UDP port 53
- B. UDP port 23
- C. TCP port 53
- D. TCP port 23

Answer: C

Explanation: A zone transfer uses TCP port 53. All other DNS requests use UDP 53.

Incorrect Answers:

- A:** UDP port 53 is used for all other DNS calls and requests, but not the zone transfers.
- B:** Port 23 is not used for UDP, but port 23 is reserved for Telnet
- D:** TCP Port 23 is Telnet

Q. 46

What is the primary security risk in SNMP?

- A. Login names and passwords are not encrypted
- B. Damaging programs can be executed on the client
- C. Damaging programs can be executed on the server
- D. Passwords and Data is transferred in Cleartext

Answer: D

Explanation: All data is transferred in cleartext. Not that we are discussing SNMP V1.

Incorrect Answers:

- A:** SNMP does not have login security at all. However, in place of a password, SNMP uses community names. You need to know the community name to gain access to the SNMP device. The community name, as well as the rest of the data, is in the clear.

B, C: SNMP does provide for the execution of code on either the client or sever. There is a SNMP agent that runs on each device or node, but this is installed code which is not installed or modified unless actually doing maintenance on the node. It is not like sending a remote shell and executing programs.

Q. 47

Ulf wants to ensure that a hacker cannot access his DNS zone files. What is the best action for his to take?

- A. Filter TCP port 23
- B. Configure the firewall to block zone transfers and accept zone transfer requests only from specific hosts
- C. Configure all routers to block zone transfers and encrypt zone transfer messages
- D. Disable Nslookup

Answer: B

Explanation: Basing on the assumption that the hacker is outside the network, and is not someone who has physical access to the internal LAN, this is the best choice. It takes multiple actions to plug it. A DNS server outside the network (on the outside of the firewall) will refer DNS requests to the internal server. This does not require secondary servers on the outside, so zone transfers don't need to be transferred in either direction. By blocking TCP port 53 on the firewall, we prevent zone transfers. However, since all other DNS requests are UDP port 53, they pass. The next step of protection is to make sure that no one tries to poison the DNS database by transferring a bogus or corrupt zone intentionally. By only accepting zones transfers from known and authorized servers, no one can slip in a bad zone.

Incorrect Answers:

- A:** TCP port 23 is used for Telnet, and will have no effect on DNS operations.
- C:** If we blocked the zone transfers at all routers, then ALL the DNS servers, including all secondaries, would have to be on the same segment, which prevents load balancing and prevents protection from failure of the LAN segment. You can have encryption from router to router, using IPSec, but if you encrypt the zone at one router and pass the encrypted file to DNS directly, DNS can't use the file.
- D:** NSLOOKUP would have seen the obvious answer. NSLOOKUP is an exposure, since a hacker could transfer zone into the utility. However, NSLOOKUP does not use its own ports, it uses the normal DNS ports (UDP/TCP 53). So you can't filter traffic generated from NSLOOKUP vs. a regular DNS call, you can't tell the difference. Also, NLOOKUP is on the hacker's machine – which is outside your control. You can't get access to the command to disable it – because it is on someone else's network and machine.

Q. 48

What is a Windows NT equivalent to a UNIX daemon?

- A. A thread
- B. A process
- C. A protocol
- D. A service

Answer: D

Explanation: The equivalent is a service, that is something running in the background and servicing the network.

Incorrect Answers:

- A:** A thread is an execution path. A daemon will have threads too. When running multiple tasks through the same code, each logical path of execution that is running is called a thread. A daemon or service maybe running many threads at the same time.
- B:** User processes cannot be compared with UNIX daemons.
- C:** A protocol is a set of instructions on how a procedure will be conducted.

Q. 49

Which of the following is the correct order of events in the termination of a TCP/IP connection?

- A. Active close, passive close, FIN, ACK
- B. Passive close, Active close, FIN, ACK
- C. Active close, passive close, ACK, FIN
- D. Passive close, active close, ACK, FIN

Answer: A

Explanation: This is the correct order.

Incorrect Answers:

B, C, D: These are not the correct order.

Q. 50

Which protocol is normally used to communicate errors or other conditions at the IP layer, but has also been used to conduct denial-of-service attacks?

- A. TCP
- B. ICMP
- C. SNMP
- D. UDP

Answer: B

Explanation: ICMP is used for the PING command. It can be used in a smurf, teardrop, buffer overflow, and the ping of death attacks.

Incorrect Answers:

- A:** TCP does not run at the IP layer (Layer 3), TCP runs at the transport layer (Layer 4)
- B:** SNMP does not run at layer 3 IP Layer). SNMP runs at the application layer (Layer 7)
- D:** UDP does not run at the IP layer (Layer 3), UDP runs at the transport layer (Layer 4)

Q. 51

Which of the following will help control unauthorized access to an e-mail server?

- A. Disable CGI scripts
- B. Prohibit relaying
- C. Limit the number of e-mail messages a given account can receive in a day
- D. Scan all e-mail messages at the firewall or SMTP server

Answer: D

Explanation: The issue is to prevent a payload being sent as an attachment to an e-mail message. A dangerous payload could be a virus, Trojan horse, or other damaging code segment that when executed can take over or gain unauthorized access.

Also, with proper scanning techniques, e-mail messages for users not serviced by the local e-mail server can be discarded. This prevents undeliverable e-mail from entering the system. In order to get e-mail through this scan, it would have to be destined to a valid e-mail account.

Incorrect Answers:

- A:** Disabling CGI scripts would be desirable, but then you lose the services provided by those scripts, which would have to be rewritten in another language. Otherwise, if a WEB server is also on the e-mail server, then disabling would be reasonable.
- B:** To prohibit relaying would prevent the receipt and delivery of mail. Relaying is sometimes required, and beyond you control to configure it.

C: This is desirable, because if I send millions of e-mails to a single server, I can fill up the mail directories and disable the e-mail server. However, this does not gain unauthorized access, this fills up the queue and causes a denial of service.

Q. 52

What is the correct order of events in the establishment of a TCP/IP connection?

- A. Passive open, active open, ACK
- B. Passive open, ACK, active open
- C. Active open, active open, ACK
- D. Active open, passive open, ACK

Answer: D

Explanation: It is actually Active open, passive open, ACK, ACK

Incorrect Answers:

A, B, C: These are not in the proper order.

Q. 53

You are using a packet sniffer to capture transmissions between two remote systems. However, you find that you can only capture packets between your own system and another. What is the problem?

- A. You have configure your filter incorrectly
- B. You are sniffing packets in a switch network
- C. Tcpdump captures packets only between your host and another host
- D. Your system does not have its default gateway configured

Answer: B

Explanation: In a switching network the switch transfers frames from the source port to the destination port. Suppose you have a 32-port switch. If a one remote system is on Port 1 and the other remote system is on port 20, then frames are switched between port 1 and 20. Unless you are connected to either port 1 or 20, or a special monitor port on the switch, you can't see the traffic. Unlike a hub, where all ports see all the traffic, on a switch you only see frames being sent to the port you are connected to. All ports see the broadcast, since the switch is a single broadcast domain.

Incorrect Answers:

- A: If the filter was incorrect, then you would not capture traffic between you and the remote network. If you got data in the capture, then the original capture should have gotten some data.
- C: TCPDUMP is not restricted in this way. However, on Windows NT/2000 Server, network monitor DOES have this restriction.
- D: Well if you can get to one of the remote systems, then the default gateway has to be there. If it wasn't, or if it was wrong. You would not have reached one of the remote servers.

Q. 54

How might a hacker cause a denial-of-service attack on an FTP server?

- A. By executing a damaging program on the server
- B. By initiating an ICMP flood
- C. By initiating a broadcast storm
- D. By filling the server's hard drive to capacity

Answer: D

Explanation: When the space on the server is depleted, you can no longer upload files to the FTP server. If the FTP server is an upload server, a full disk becomes a problem because no more files can be written. A denial of service attack involves monopolizing all the resources so no legitimate user can use them. Here, the resource is disk space, and that is what has been monopolized. Depending on the location of the hard drive in relation to the Operating System and other tasks, filling the hard drive may even disable the FTP server and deny service on even downloads, and even possible crash of the entire server. This can happen when there is only one disk in the server, and the operating system comes to a halt due to lack of logging or paging space.

Incorrect Answers:

- A: Execution of a damaging program on the server is caused by a virus. A FTP server cannot directly invoke a virus because even though the file containing the virus can be deposited on the server by an upload FTP, the file cannot be executed. FTP does not invoke any user code in the normal execution of the FTP services.
- B: An ICMP flood would knock out the FTP server, and the increased traffic could also knock out the other servers on the subnet, and possibly connected subnets along the path. This question is trying to focus on a vulnerability specific to the FTP server itself.
- C: A broadcast storm would knock out the FTP server and every other server on the LAN. This question is trying to focus on a vulnerability specific to the FTP server itself.

Q. 55

Which type of port is used by HTTP for the control connection?

- A. Ephemeral
- B. Well-known
- C. Dynamic
- D. UDP

Answer: B

Explanation: The well-know ports are the ports numbered 0-1023. HTTP uses port 80 by default.

Incorrect Answers:

- A:** Ephemeral ports are those port above 1023 (1024-65535) used by the clients as source ports when connecting to a server. These ports are dynamically assigned to the client, and released by the client. Once released, these port may be used again by a different client.
- C:** A static port is a port that is always open or closed. A dynamic port is a port that opens when it is assigned to a client or service, and then closes when the service or client releases the port. Dynamic ports are used in environments such as firewalls and proxy servers to hide ports and services, for example to limit the findings of a port scanner.
- D:** HTTP uses the TCP protocol, not UDP. UDP/TCP are transport layer (layer 4) protocols, and not port numbers. However, the protocol is important when contacting a port.

Q. 56

Which security feature does NNTP possess that SMTP does not?

- A. Dynamic port assignment
- B. Separate control and data ports
- C. Usable in conjunction with SSL
- D. Strict bounds checking on arrays

Answer: C

Explanation: NNTP can use SSL. For SMTP MIME/E can be used and other security mechanisms.

Incorrect Answers:

- A:** From the server side, each application uses a single unique well known port (119 for NNTP and 25 for SMTP), and from the client side, both applications are capable of selecting a dynamic port.
- B:** Neither application has this feature.
- D:** Neither application has this feature.

Q. 57

Laura is a system administrator who wants to block all NNTP traffic between her network and the Internet. How should she configure her firewall?

- A. Disable anonymous logins in the NNTP configuration manager
- B. Configure all routers to block broadcast packets
- C. Configure the firewall to block port 119
- D. Configure the firewall to block port 25

Answer: C

Explanation: Network News Transmission Protocol (NNTP) uses port 119, and if you block that port, you are preventing NNTP traffic from crossing the firewall.

Incorrect Answers:

- A:** This would not block anyone with a valid userid, and the question says block all NNTP traffic.
- B:** Routers already prevent and block broadcast packets.
- D:** If the firewall is configured for port 25, you would only block out SMTP (mail).

Q. 58

Luke must advise his users about which client to employ when accessing remote systems. Which of the following is a connection-oriented protocol that can contain unencrypted password information from Telnet sessions?

- A. TCP
- B. TTP
- C. HTTP
- D. UDP

Answer: A

Explanation: TCP is a connection oriented protocol which operates on the transport layer (Layer 4). This is the transport used by the telnet client.

Incorrect Answers:

- B:** There is no TTP protocol.
- C:** HTTP is an application protocol that is based on TCP.
- D:** UDP is a connection-less protocol.

Q. 59

What is the term for the process of replacing source IP addresses with false IP addresses?

- A. Hijacking
- B. Spoofing
- C. Spamming
- D. Brute force

Answer: B

Explanation: Spoofing is the process of changing the source IP address to make it appear as if the packet originated from somewhere else.

Incorrect Answers:

- A:** A hijacking attack is when someone gets in the middle of a transaction and takes over the transaction, spoofing himself as the original transaction partner.
- C:** Spamming is the sending of unsolicited e-mails, sort of like junk mail.
- D:** Brute Force refers to processes that are exhaustive. For example, trying to crack a password by using every possible character pattern that can be generated.

Q. 60

Which ports are used by SNMP?

- A. UDP ports 161 and 162
- B. UDP ports 20 and 21
- C. TCP ports 161 and 162
- D. TCP ports 20 and 21

Answer: A

Explanation: UDP Ports 161 and 162. Port 161 is used for most calls, while port 162 is used for traps.

Incorrect Answers:

- B:** FTP uses TCP on ports 20 and 21.
- C:** SNMP uses UDP protocol, not TCP.
- D:** Ports 20 and 21 are used for FTP.

Q. 61

What is the most common type of network attack?

- A. Denial-of-service attacks, because they are easy to perpetrate
- B. Insider attacks, because most resources are spent defending against outside attacks
- C. Packet sniffing and other “benign” attacks, because there is no way to defend against them
- D. Brute-force password attacks, because most users do not employ good passwords

Answer: A

Explanation: The denial of service (DoS) attack has become the most common network type of attack. It is the actual network being attacked here. If it was a server being attacked, or a use, then ,maybe we would say virus. But attacking the network itself, DoS can be initiated in a way that is untraceable and does not require actually breaking into the system.

Incorrect Answers:

- B:** It would be difficult to attack the network from the inside without being discovered as the offender.
- C:** Packet sniffing by a user is becoming less common as networks move to switch technology. The switch isolates the traffic so that only relevant traffic, traffic that belongs to that user, is available. Although good packet sniffing tools are not normally made available to Windows users, a snoop utility is almost standard on many Unix platforms. Besides using switch technology, there are other methods to defend the eavesdropping of the network medium.
- D:** If a brute force attack was successful then it would not make a difference how complex the password was. But, brute force attacks take too long to come up with a solution, and there are methods that can be implemented, such as a lockout policy, to render the brute force attack useless. Complex password can be enforced by software enforced polices.

Q. 62

What is the different between digital signature mechanisms and simple encryption?

- A. Digital signatures are generally 128-bit encryption, whereas simple encryption is generally 56 bits
- B. Digital signatures are verified by third parties that vouch for the veracity of the sender and the contents
- C. Digital signatures carry timestamps, whereas standard encryption does not
- D. Standard encryption mechanisms have no provision for traffic padding to thwart password sniffers

Answer: B

Explanation: A digital signature is verified by a third party, which holds the public encryption keys and other information used to validate the signature. A common know third party is Verisign.

Incorrect Answers:

- A:** Digital signatures and regular encryption can use any bit length for the keys.
- C:** A digital signature is not required to carry a timestamp, so not all forms of digital signatures will have one.
- D:** This is not true.

Q. 63

What is problematic about a new NTFS partition?

- A. The “everyone” group has unrestricted access permissions on the new partition, thus restricting access to the new partition become problematic.
- B. NTFS cannot read user/group permissions tables on FAT systems, thus the group permissions file must be kept in the same file format as the new partition
- C. The “admin” group has exclusive access to the new partition, thus getting client machines to see the new partitions can be problematic
- D. NTFS allows only the root user to access it, thus it is difficult to divide the new partition

Answer: A

Explanation: When a new NTFS partition is created, the default access control gives the everyone group full access to all directories and files created on that volume, until some other permission scheme is explicitly defined.

Incorrect Answers:

- B:** A FAT partition does not have permissions tables.
- C:** This is not true. The default access permissions when creating a NTFS partition is the everyone group, giving every user, including guests, full control over the partition and any directory and file created on it.
- D:** This is not true. The default access permissions when creating a NTFS partition is the everyone group, giving every user, including guests, full control over the partition and any directory and file created on it.

Q. 64

Why is the rlogin command dangerous to network security?

- A. Remote logins are a security threat regardless of the protocol and should be avoided
- B. There is no way to prevent the user who successfully uses rlogin from becoming root
- C. The rlogin command has a long history of buffer overflows that has not been corrected

- D. If one system that has extensive rlogin privileges to other systems is compromised, then a hacker can spread throughout the entire network

Answer: A

Explanation: Remote logins can gain access to a server without a password, and is a major security risk. It is easily violated and transmits data in cleartext.

Incorrect Answers:

- B:** The remote user can be denied root access via security controls.
- C:** The rlogin is a very old and mature command, and has not experienced buffer overflows.
- D:** Any system open to rlogin can be attacked by anyone. Once it is open, you can't restrict who comes in via the command.

Q. 65

Which of the following choices lists the components that make up security descriptions for Windows NT objects?

- A. The user name, the password and the object-owner security identifier
- B. The UNAME the access profile of the object-owner SID, and confirmation by the system access control list
- C. The object-owner SID, the discretionary access control, the DACL, and the group SID
- D. The user name, the object identifiers, the set user identifier, and the time/date stamp

Answer: C

Explanation: The security identifier (SID) is a unique identifier used in Windows NT and Windows 2000 systems, including workstations and servers. The SID is used with other components to maintain a unique identifier of each and every object, not only within the system, but within the entire network. The SID is attached to the user object, and to the group object. One feature of the SID, when it is attached to an object, you can rename the object but it still has the same SID, so all security references do not change. The DACL is the mapping of permissions and access between objects.

Incorrect Answers:

- A:** The user name and passwords do not make up security descriptions. The user name is not significant, since security objects rely on the SID.
- B:** These do not make up the set of security descriptors.
- D:** These do not make up the set of security descriptors.

Q. 66

What is the major security problem with the SUID/SGID programs or utilities?

- A. The root account must be in order to utilize programs set this way
- B. These permission in a program in a program can temporarily grant root privileges to anyone
- C. SUID programs are not removed immediately from the swap/paging area, which results in a clear security risk
- D. The SGID is a clear violation of good security practice and is only used as a result of the SUID

Answer: B

Explanation: When a program changes its UID, it then gets a SUID (SetUID). If it was a GID, then it would be called a SGID. A SUID or GUID will grant a user more permissions than was initially entitled. This even includes setting the user as root.

Incorrect Answers:

- A: You don't have to be root to gain root.
- C: This is not true.
- D: The SGID has to be used in certain situations.

Q. 67

Carol wants to choose a strong password for her computer. Which of the following should she include in her password?

- A. A mixture of uppercase and lowercase letters, symbols and numbers
- B. An arcane phrase only she can remember
- C. An incorrect spelling of a word or a phrase
- D. A mixture of random words that form non-sense

Answer: A

Explanation: By mixing case, and combining it with non-characters will develop a complex password that cannot be easily cracked. If you used either lower case or upper case, then each position would require 27 different variations (26 letters and a blank). If you mix upper and lower case, then it is 53 (26 upper, 26 lower, and a space). Now add in numbers, and it is 63. Add in special characters and that number increases (exact number varies based on what special characters the system will allow in the password field). The increase in possible variations of one position of the password makes the solution space for the brute force attack exponentially large.

Incorrect Answers:

- B:** A phrase will contain valid words, which make the password crackable using a dictionary attack.
- C:** Even with an incorrect work spelling, dictionary attacks will vary the words in the dictionary to test words close to the correct spelling.
- D:** A phrase will contain valid words, which make the password crackable using a dictionary attack.

Q. 68

Why would Ulf refuse to run the command “chmod-Are 777/home/ulf”?

- A. The command will copy all his files to a public directory
- B. The command will allow everyone to read, write and execute all files in his directory
- C. The command will create problems when his profile file initialises his user settings
- D. The command is known to have security breaches associated with it, and should be avoided.

Answer: B

Explanation: Each position of the three digit number controls security for a different entity. The first digit is for owner, middle for group access, and the last for everyone else. A 7 in a position gives full access (including read and write), and a 777 gives full control to everyone. In this case, executing the command would open Ulf's home directory to everyone, who can access his directory and change or erase his files.

Incorrect Answers:

- A:** The chmod command affects permissions, it does not copy files.
- C:** This command will not create problems, since there will be no restrictions.
- D:** This is a very critical command in the Unix system, and must not have security breaches since it is used a lot.

Q. 69

Which command, service or tool allows you to imitate a secondary DNS server in order to obtain its records via a zone transfer?

- A. Traceroute
- B. Ping scanner
- C. Nslookup
- D. Host

Answer: C

Explanation: NSLOOKUP can be used to initiate a zone transfer.

Incorrect Answers:

- A:** Traceroute is used to identify the hops to a target host, and is used for mapping the structure of the network. It does not interface with DNS to acquire zone transfers.
- B:** A ping scanner is used to identify IP addresses in a network. It may locate a DNS server, but it can't obtain the zone files.
- D:** The host command is used to get host information, and can get the host by IP address or Host name, and convert host name to IP address and reverse.

Q. 70

Which type of attack uses a database or databases to guess a password in order to gain access to a computer system?

- A. Hijacking attack
- B. Virus attack
- C. Dictionary attack
- D. Man-in-the-middle attack

Answer: C

Explanation: A dictionary attack is the process of trying every character combination to guess a password (brute force) or using a dictionary type program to generate and try all character combinations.

Incorrect Answers:

- A:** A hijacking attack is when someone gets in the middle of a transaction and takes over the transaction, spoofing himself as the original transaction partner.
- B:** A virus attack is when a program or macro is executed and the virus is implanted into another executable. A virus can be used to implant the code for the illicit server attack, but the actual illicit server attack is when the service or daemon is running.
- D:** A man-in-the-middle attack is also when someone gets in the middle of a transaction between two servers and intercepts the transaction flow. This differs slightly from the hijacking attack. In the hijacking attack the man-in-the-middle actually cuts in and impersonates one the partners, but in a man-in-the-middle attack, the intervening party only eavesdrops and listens to the stream.

Q. 71

What is the name of the risk assessment stage in which you bypass login accounts and passwords?

- A. Penetration
- B. Control

- C. Activation
- D. Discovery

Answer: A

Explanation: In Penetration, all access controls (including login accounts and passwords) are bypassed.

Incorrect Answers:

- B:** Control is the stage where you show that you can control the resource, and show the methods that can be used to ensure prevention.
- C:** Activation is not a risk assessment stage.
- D:** Discovery is the task of testing the network security for effectiveness and locating weaknesses.

Q. 72

Which tool, command or service allows a remote or local user to find any open connection paths to the system on the Internet or an intranet?

- A. Traceroute
- B. Whois
- C. Nslookup
- D. Port scanner

Answer: D

Explanation: A port scanner is used to identify active ports which are open.

Incorrect Answers:

- A:** Traceroute is used to identify the hops to a target host, and is used for mapping the structure of the network.
- B:** Whois is used to get primary and secondary DNS server information.
- C:** NSLOOKUP is used to query a DNS server.

Q. 73

A hacker has just changed the information for a zone during a zone transfer. This attack caused false information to be passed on to network hosts as if it were legitimate. Which type of server is the target in such an attack?

- A. An e-mail server

- B. A DNS server
- C. A router
- D. A FTP server

Answer: B

Explanation: A zone transfer refers to DNS zones.

Incorrect Answers:

- A:** An e-mail server does not use a zone, nor does it get involved with a zone transfer.
- C:** A router server does not use a zone, nor does it get involved with a zone transfer.
- D:** A FTP server does not use a zone, nor does it get involved with a zone transfer.

Q. 74

Which of the following do hackers target because it usually communicates in Cleartext?

- A. Router
- B. DNS server
- C. FTP server
- D. E-mail server

Answer: C

Explanation: A FTP server does not use encryption techniques to protect passwords or the data stream. It is almost a sure bet that FTP will always be in cleartext.

Incorrect Answers:

- A:** Router communications (router to router, including routing information) can be secured. Routers will be targeted by hackers for reasons other reasons.
- B:** The DNS servers communicate in cleartext, but use a form of signature to prevent data changing during a hijacking attempt.
- D:** Most of the e-mail is transferred in the clear, but there are also e-mail servers which can protect the data via encryption and digital signatures.

Q. 75

Which directory holds the Microsoft NT operating system on an NT 4.0 server (using default installation)?

- A. \windows

- B. \winnt
- C. \winnt4.0
- D. \program files

Answer: B

Explanation: The \WINNT directory is the default directory.

Incorrect Answers:

- A:** WINDOWS is used for older systems, such as Windows 3.1, Windows 98 and Windows 95.
- C:** WINNT4.0 is not the directory used.
- D:** Program Files is the directory for application programs, not the Operating System.

Q. 76

Where are most of the binaries located on the hard drive of a UNIX server (using default installation)?

- A. /bin
- B. /sbin
- C. /usr
- D. /proc

Answer: C

Explanation: Most of the binaries will be located in the /usr directory. Many other binaries are in subdirectories of the /usr directory.

Incorrect Answers:

- A:** /bin holds system commands, and is really /usr/bin
- B:** /sbin holds administrative commands, and I really /usr/sbin
- D:** /proc is used for access to kernel variables,

Q. 77

Ulf is a systems administrator. He sees that an attacker from a remote location is sending invalid packets, trying to monopolize Ulf's connection so that a denial of service occurs. What characteristic of the activity makes Ulf think this is a denial-of-service attack?

- A. Bandwidth consumption
- B. Hijacking of internal user resources
- C. Polling

- D. Use of an illicit server

Answer: A

Explanation: Bandwidth consumption is a technique for denial of service, and Ulf would see his connection slowing down very fast.

Incorrect Answers:

- B:** Hijacking would not be used in a DoS attack.
- C:** Polling of Ulf's connection would not result in a DoS unless it was a lot of polling, generating a lot of traffic, and consuming bandwidth.
- D:** The illicit server attack is not a technique that would be used for DoS attack.

Q. 78

Which application is used to learn about an operating system's type and patch level?

- A. Traceroute
- B. Nmap
- C. Whois
- D. Ping

Answer: B

Explanation: Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers, and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL.

One of the features is OS Detection, which involves a feature called TCP/IP Stack Fingerprinting, which is used to determine the OS and the release levels.

Incorrect Answers:

- A:** Traceroute will not provide information about a system. It is based on an ICMP command and is used to find the route to a target system.
- C:** Whois is used to determine the primary and secondary name servers and does not expose the OS type or patch level.
- D:** Ping will not provide information about a system. It is based on an ICMP command and if there is an echo reply, lets you know if the IP address is active.

Q. 79

You have installed a proxy server that authenticates users. However, you find that one user has bypassed the proxy server by entering the default gateway IP address. How can you solve this problem?

- A. Configure the default gateway to deny access to all systems
- B. Confront the user
- C. Reconfigure the user's machine
- D. Configure the default gateway to reject all requests to all systems except for the proxy server

Answer: D

Explanation: By using the default gateway to get to the Internet (or anywhere else) the Proxy server can be bypassed. Usually this should not be the case since the proxy server should be connected directly to the outside network, and nothing else. When a network topology opens up additional paths to the outgoing router, that router port needs to be configured so that only the proxy server can access it.

Incorrect Answers:

- A:** If we deny all systems, then even the proxy server can't get out, and this is excessive control that prevents too much.
- B:** Confronting the user may plug the security hole that occurred (and it might not even be the user's fault), but action needs to be taken to prevent future breaches by other systems.
- C:** Same as confronting the user, it does not correct the problem so that it does not occur in the future – even with a different system.

Q. 80

What is the standard method for securing individual e-mail messages sent between a company and other users that do not use that e-mail server?

- A. Invoke encryption at the e-mail server
- B. Invoke encryption on each client
- C. Filter firewall port 42 on the company firewall
- D. Store all e-mail messages on a separate partition

Answer: B

Explanation: E-mail messages can be secured by encrypting them. A client application at receiver of the e-mail could then decrypt the e-mail messages. A possible solution would be to use PGP (Pretty Good Privacy) at both the server and the client.

Incorrect Answers:

- A:** Encryption would have to be enabled both the clients and at the server.
- C:** Instead of using the standard e-mail port, port 25, a secure port, port 42 for example, can be used to enhance security of e-mail. In this scenario, however, this is not applicable since some users don't use this e-mail server.
- D:** Locally securing the e-mail messages wouldn't help much when they are transferred.

Q. 81

Which one of the following choices lists the two greatest security problems associated with HTTP?

- A. Community names and encrypted passwords
- B. IP spoofing and ICMP spoofing
- C. Viewer applications and external programs used by the HTTP server
- D. No bound checking on arrays and anonymous access

Answer: D

Explanation: In general, HTTP is set up for anonymous access. Access can be secured, however that is not the normal operating environment for HTTP. HTTP by itself, does not protect the environment by bounds checking. That is left to the applications and languages to check and control.

Incorrect Answers:

- A:** HTTP does not use community names. Not all passwords are encrypted.
- B:** HTTP uses TCP, and spoofing is not the biggest problem.
Note: IP spoofing is used to gain access when the intruders create packets with spoofed source IP addresses. This exploits applications that use authentication based on IP addresses and leads to unauthorized user and possibly root access on the targeted system. Denial of Service (DOS) attacks often use IP Source Address Spoofing. DOS attacks can also be made by using UDP and ICMP flooding.
- C:** Viewer applications do not cause security issues since they don't change data. External programs that are used by the server do not present a security concern since it is under the control of the server administrator, and not delivered as part of a message payload.

Q. 82

Which tool utilizes a database of known security problems to test a network?

- A. Operating system add-on
- B. Network scanner

- C. Logging and log analysis tool
- D. SNMP

Answer: B

Explanation: A Network scanner collects information on the network. Most network scanners are configured to use a large database of common vulnerabilities, including CGI, FTP, registry exploits and more.

Incorrect Answers:

- A:** Third party solutions, operating system add-ons, security trouble-shooters that use databases of known security problem do exist.
- C:** Analyzing the log file could detect security problems. It is not the best way to detect these problems though.
- D:** SNMP (Simple Network Management Protocol) enables network administrators to manage network performance, find and solve network problems, and plan for network growth. SNMP is not usually configured to use a database of know security problems.

Q. 83

How are servers able to conduct a simple authentication check using DNS?

- A. Forward DNS lookup
- B. Reverse DNS lookup
- C. RARP
- D. Nslookup

Answer: B

Explanation: A simple authentication check can be performed by checking what name corresponds to the IP address of the computer. This is done a reverse DNS-lookup, a name to IP lookup. If there is a corresponding RR record with appropriate name the simple authentication succeeds.

Incorrect Answers:

- A:** For a simple authentication check we should use a name to IP lookup, a reverse DNS lookup, not a Forward DNS lookup.
- C:** RARP (Reverse Address Resolution Protocol) does not use DNS.
- D:** NSLOOKUP is a user command for a user to check DNS server functionality. The command is not directly used by the operating system of the server, although the procedure being executed will be similar.

Q. 84

Which port or ports are used for SMTP?

- A. 20 and 21
- B. 25
- C. 53
- D. 161 and 162

Answer: B

Explanation: SMTP uses port 25.

Incorrect Answers:

- A:** 20 and 21 are used for FTP.
- C:** 53 is used for DNS
- D:** 161 and 162 are used for SNMP

Q. 85

When using IIS, what has primary control over security?

- A. The operating system
- B. IIS
- C. The GINA
- D. The SSL Service

Answer: A

Explanation: IIS allows the Windows Operating system to control all aspects of security. For example, file security will be controlled by NTFS. You can modify IIS to further restrict file permissions, but not loosen them. NTFS has primary control, and the OS controls NTFS.

Incorrect Answers:

- B:** IIS does not have primary control. It has secondary control in that IIS can further restrict access, but the OS has the primary control.
- C:** The GINA.DLL is used for login authentication. It is not a control mechanism.
- D:** The SSL service is used for security between client and server, but does not secure the resources on the server.

Q. 86

Which of the following is the best way to secure CGI scripts?

- A. Configure the firewall to filter CGI at ports 80 and 443
- B. Disable anonymous HTTP logins when using CGI
- C. Ensure that the code checks all user input
- D. Active Java on the primary web server

Answer: B

Explanation: CGI are executable programs which run on the server. The CGI programs may need to access files and other resources. In order to insure protection, a user account should be used that has been authorized for access. When using the anonymous login, you are using a guest account, and assigning resources to a guest or anonymous account can create a large security exposure.

Incorrect Answers:

- A:** CGI is code that executes at the server. It is not inherent in the protocol, so it can't be filtered.
- C:** Producing a program that is perfect in that it checks all input and checks for all possible error condition is a perfect program. No one can write a perfect program and account for every possible condition. Plus, if you could, you can't be expected to enforce it, it is not always in your control.
- D:** Using JAVA may be used in place of CGI scripts, but JAVA does not add security to CGI.

Q. 87

Which type of gateway functions in all layers of the OSI/RM?

- A. A circuit-level gateway
- B. An application-level gateway
- C. A proxy gateway
- D. A universal gateway

Answer: B

Explanation: An application-level gateway operates at all levels of the OSI model. It is too high in the level to provide NAT, NAT has to be provided at a lower layer through a different service.

Note: An application-level gateway is often called an application-proxy gateway. Sometimes it is referred to as a proxy gateway.

Incorrect Answers:

- A: A circuit-level gateway operates at the session layer, and NAT is a primary advantage.
- C: A proxy gateway operates at the network layer.
- D: A universal gateway is not a term used to identify gateways.

Q. 88

Which device is similar to a packet filter, but also provides network address translation?

- A. A circuit-level gateway
- B. An application-level gateway
- C. A proxy server
- D. A choke router

Answer: A

Explanation: A circuit-level gateway operates at the session layer, and NAT is a primary advantage.

Incorrect Answers:

- B:** An application-level gateway operates at all levels of the OSI model. It is too high in the level to provide NAT, NAT has to be provided at a lower layer through a different service.
- C:** A proxy server can provide packet filtering, such as provided in Microsoft's Proxy Server and ISA server. However, the main functionality of the proxy server is to act in behalf of the clients it services. It is not similar to a packet filter when it is proxying, no to be confused in that it can also provide the packet filter feature.
- D:** A choke router is a router in which all traffic has to pass through it. Like a funnel. Usually a choke is used in a firewall, where all traffic entering and leaving a network has that one point of entry/exit. It does not provide network address translation (NAT).

Q. 89

Which of the following attacks specifically utilizes packet spoofing?

- A. Crack
- B. Smurf
- C. Flood
- D. Worm

Answer: B

Explanation: In a smurf attack an IP Ping using a broadcast address is sent to a segment. The source IP address of the IP PING command is spoofed to the target of the attack, When ALL the machines on the network respond to the ping, they respond to the target of the DoS attack, as all the replies go to the spoofed IP address.

Incorrect Answers:

A, C: These are not common terms used in making an attack.

D: A worm is not used in packet spoofing.

Q. 90

Tavo wants to check the status of failed Telnet-based login attempts on a Linux machine he administers. Which shell command can he use to see only that information?

- A. `cat/etc/passwd> newfile.txt`
- B. `grep login/var/log/messages`
- C. `more /var/log/secure`
- D. `more /etc/passwd`

Answer: B

Explanation: The grep command is used to search for information in a file.

Incorrect Answers:

A: The cat command is used to list information in a file, but does not filter it.

C: The more command will not filter information, and you don't scan the security log file for the messages.

D: The more command will not filter information, and you don't scan the password file for the messages.

Q. 91

Why is the rlogin command dangerous to network security?

- A. Remote logins are a security threat regardless of the protocol and should be avoided
- B. There is no way to prevent the user from becoming root if he successfully uses rlogin
- C. The rlogin command has a history of buffer overflows that has not been corrected
- D. The rlogin command relies on IP-based authentication, which is easily defeated

Answer: A

Explanation: Remote logins can gain access to a server without a password, and is a major security risk. It is easily violated and transmits data in cleartext.

Incorrect Answers:

- B:** The remote user can be denied root access via security controls.
- C:** The rlogin is a very old and mature command, and has not experienced buffer overflows.
- D:** rlogin is not based on IP authentication.

Q. 92

Which of the following is the most desirable goal that UNIX system crackers typically hope to achieve?

- A. To be able to write a message on the compromised computer's web page
- B. To be able to plant a virus that will wipe out the entire database
- C. To gain root privileges
- D. To alter the /var/log/messages file and thus escape detection

Answer: C

Explanation: Root is the super user account which allows full and unrestricted access.

Incorrect Answers:

- A:** Not all crackers are destructive. But in order to do anything to system files, you want to become a superuser.
- B:** Not all crackers are destructive. But in order to do anything to system files, you want to become a superuser.
- D:** After becoming root, this can be done, but the goal is to become the superuser.

Q. 93

What is the purpose of blocking services on any given server?

- A. To limit the number of targets a cracker can choose from
- B. To limit the number of processes that run at any given time, enhancing response time in case of a security breach
- C. To keep the operating system and its processes as simple as possible so administration is easier
- D. None; most services are needed and pose only minor security threats

Answer: A

Explanation: Unnecessary services running on a server should either be blocked or disabled. If the service is for the intranet and not required to be accessed from outside the organization, then those services should be blocked at the firewall. Leaving the service open in any of these cases leaves another target for the cracker to attack. The less services exposed, the less points of exposure.

Incorrect Answers:

- B:** Services that are not being used, but continue to run, usually do not consume much resources. Stopping those services will not gain that much of a performance gain.
- C:** Actually, keeping track of which services have to be disabled or blocked will slightly increase administration, since you are going against the norm and changing the system from the default installation. Operations of the system may be simpler with less tasks, but this is not the main purpose from a security perspective.
- D:** Not all services are required. For example, everyone does not need to be running a FTP server at their desk, and turning off the finger service will not prevent other programs from running.

Q. 94

What is the primary function of IPSec?

- A. It thwarts denial-of-service attacks
- B. It provides encryption
- C. It authenticates users
- D. It provides access control

Answer: B

Explanation: IPSec (IP Security) is the encryption of data, usually network data. It is used to encrypt tunnel traffic on Windows 2000 L2TP (Layer 2 tunnelling protocol) VPNs. It was originally used for router to router encryption of data streams when the medium between the two routers could be compromised.

Incorrect Answers:

- A:** IPSec cannot help reduce denial of service attacks.
- C:** Authentication of a user could happen since only the proper user will have the encryption keys, however it is not the purpose of IPSec to be an authentication protocol.
- D:** IPSec is not used for access control. Again, only someone with the encryption keys could read the stream, but it is no the purpose or intent that IPSec be used as an access control mechanism.

Q. 95

When setting up Microsoft Internet Information Server (IIS) in either Windows NT or Windows 2000, what should you change to help provide security?

- A. The default accounts must be renamed because they pose a security problem
- B. The domain controller must be queried for the default encryption for the user database
- C. The administrator must import default admin profiles for secure administration rights
- D. The default users must be trained in the errata and security features of internet information manager

Answer: A

Explanation: The default accounts should be renamed. This would decrease the risk of intrusion.

Incorrect Answers:

- B:** Encryption can be used to enhance security. One of the first steps to provide security would to rename the default account though.
- C:** The default security settings are probably not good enough.
- D:** The default user should not be required to learn of IIS security. That would be a costly investment.

Q. 96

Helga is going to log on to her network. Her network does not employ traffic padding mechanisms. Why will it be easy for someone to steal her password?

- A. Because her password could be more than two weeks old
- B. Because of the predictability of the login length and password prompts
- C. 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.

Q. 97

Why would a Windows NT/2000 administrator place the operating system, the program files and the data on different, discrete directories?

- A. To avoid confusion and duplication of upgrades between applications and the operating system
- B. To enhance security by modifying permissions for each resource as needed
- C. To restrict users from accidentally overwriting critical files (if they fill their home directories to capacity), which makes the operating system vulnerable to hacker attacks
- D. To keep the operating system partition from becoming overwhelmed with user program libraries and DLLs

Answer: B

Explanation: By keeping the classes of programs separate – we can control security easier. Security is usually applied to a directory, and then all the files in the directory inherit the security attributes of the parent folder. Separation of the different classes of program makes modification of the security easier to maintain.

Incorrect Answers:

- A: If there is any confusion or duplication issues, using different directories might not resolve those issues.
- C: If a user overfills their home directory, they do not just jump into a system directory and overwrite system files. If system files were shared, and no protected, they can be overwritten anyway. Having a separate home directory further separates the user into his own region of permissions.
- D: If there is only one partition on the system, then whether you have one directory, or separate directories, the disk is going to fill up.

Q. 98

Which layer of the OSI/RM do proxy servers usually address?

- A. Physical layer
- B. Network layer
- C. Transport layer
- D. Application layer

Answer: D

Explanation: Most proxy servers, for example proxy server firewalls, work at the application layer.

Incorrect Answers:

- A:** A proxy server does not work usually work at the physical layer.
- B:** A proxy server could work at the network layer, but it is usually run at the application layer.
- C:** A proxy server could work at the transport layer, but it is usually run at the application layer.

Q. 99

At which layer of the OSI/RM do packet filters function?

- A. Data link layer
- B. Physical layer
- C. Network layer
- D. Transport layer

Answer: C

Explanation: A packet filter operates at the IP (Network – Layer 3) level. Most packet filters are implemented in routers, and a router is a layer 3 device. Also, the terminology of data at the network layer is “packet”.

Incorrect Answers:

A, B, D: Packet Filters runs at the network layer, making the other answers incorrect.

Q. 100

Helga deleted extraneous services from a system to ensure that it is relatively secure from attack. Which term best describes this activity?

- A. Securing the system
- B. Operating system hardening
- C. Auditing
- D. System maintenance

Answer: B

Explanation: Hardening the OS requires removing possible holes, tools, and extraneous services that can be used to access and administer the OS.

Incorrect Answers:

- A:** Hardening the OS is just one part in securing a system.
- C:** Auditing is the process of tracking down specific events on the network. Auditing doesn't involve deleting of extraneous services.
- D:** Deleting extraneous services from the system is not included in the normal system maintenance.

Q. 101

Lucy is a system administrator who wants to block all NNTP traffic between her network and the Internet. How should she configure her firewall?

- A. Configure the firewall to block all incoming and outgoing packets except for those with the source and destination port of 119. Then, allow all traffic with destination ports above 1024 to transverse the firewall.
- B. Configure the firewall to block all incoming packets with the source port of 119, and outgoing packets with a source port lower than 1024. Then, block all packets with the destination port of 119 and with a source port lower than 1024.
- C. Configure the firewall to block incoming packets with the destination port of 119, and to block outgoing packets with the destination port of 119.
- D. Configure the firewall to block all incoming packets with the source port of 119.

Answer: C

Explanation: By blocking at the firewall all incoming packets at port 119, this prevents anyone on the Internet from access a NNTP server inside the corporate intranet. By blocking all outgoing packets with a destination port of 119, that prevents anyone from inside the corporate network from accessing a NNTP server out on the Internet.

Incorrect Answers:

- A:** This will block almost everything BUT NNTP.
- B:** When we block all outgoing packets with a port below 1024, we just disables ALL out servers, so if we have a Web Server TO THE INTERNET, it is now blocked. Blocking packets with a source address of less than 1024 now disables all incoming packets, and no one can access a server out on the Internet.
- D:** A source port of 119 is a message from NNTP. We need to even prevent the initiation of a NNTP connection, this is after the fact. And this does not affect incoming messages to connect to a NNTP server inside the company network.

Q. 102

Which port is used by HTTP to listen for secure connections?

- A. UDP 80
- B. TCP 443
- C. TCP 8080
- D. UDP 8080

Answer: B

Explanation: No discussion, 443 is the default designated port for secured HTTP, which is usually invoked by using HTTPS.

Incorrect Answers:

- A:** Port 80 is used for non-secure HTTP, but it is TCP port 80, not UDP port 80, which is not use right now.
- C, D:** Services listen using ports below 1024, which are well known ports. These ports are above that range. TCP 8080 is sometimes used for a proxy port to connect into the proxy server, but is not defined as any standard.

Q. 103

Raul is worried that his network might be attacked through modified ICMP messages. What can he do to prevent this?

- A. Disable anonymous logins
- B. Filter ICMP packets at the firewall
- C. Configure the firewall to block zone transfers
- D. Scan ICMP messages for viruses at the firewall

Answer: B

Explanation: The thing to do is to prevent the ICMP packets from passing the firewall. No one really needs to have users from outside the network from being able to ping their machines. In addition, ICMP is used for traceroute will allow someone to map out the network, so why even open the network to that type of exposure.

Incorrect Answers:

- A:** The login process, whether anonymous or not, does not use ICMP messages, so this will not have an effect.
- C:** ICMP messages are not used in zone transfers, so this will have no effect.

D: A ICMP message can be dangerous just based on the size of the message. Using a message too large can overflow buffers. It could be spoofed and you can't check that. An ICMP message would not be used to pass a virus in its payload, so scanning will have no effect.

Q. 104

Which layer of the OSI/RM stack controls the flow of information between hosts?

- A. Data link layer
- B. Physical layer
- C. Network layer
- D. Transport layer

Answer: A

Explanation: The data link layer provides flow control from host to host. This is a hop to hop connection.

Incorrect Answers:

- B:** The physical layer is the device driver level, and does not do flow control.
- C:** The network layer does routing to determine where a packet should be sent next.
- D:** The transport layer does end-to-end flow control.

Q. 105

What is the most important step in securing a web server?

- A. Logging all HTTP activity
- B. Enabling system-wide encryption
- C. Placing the operating system, web server program, and server files on the same partition
- D. Placing the operating system, web server program, and server files on separate partitions

Answer: D

Explanation: By separating the different data groups to different partitions, prevents changes to one group from affecting another group. For example, under IIS, which is a web server, also provides FTP access. If everything was on one partition, a hacker could fill up the partition (use up all freespace) and bring the system to a screeching halt as the operating system can't obtain anymore disk space.

Incorrect Answers:

- A:** Logging the activity is important, it will allow you to find out what was done – after the fact. But what is important is to be proactive and take actions that may prevent a problem in the future. Better for the

problem NOT to happen in the first place, then to run around and have to find out what happened and fix it.

- B:** The use of encryption protects the data stream, but does not protect you system from actual attacks. If the use of the server is for public access, then anyone should be able to obtain the public encryption key and attack the server.
- C:** Actually, you want to do the opposite, you want the items separated.

Q. 106

You have enabled Tripwire on your Linux system. Which location is best for storing the database file?

- A. On a CD-RW drive attached to the system
- B. In the default location
- C. On a write-protected floppy disk attached to the system
- D. On a CD-R drive attached to the system

Answer: D

Explanation: Tripwire is an intrusion detection security product. It scans the system and produces a database that snapshots the system. Then at a later time, the system administrator can run a check against the database to see if anything changed. By using a CD-R, which has been closed and not in a writer drive, the CD will be read-only and a hacker would not be able to modify the actual CD if the hacker should gain access to the CD drive.

Incorrect Answers:

- A:** A CD-RW drive can still write on the CD, and if a hacker gains access to the drive, the database might be modified to hide the tracks. Or, the database could be erased or corrupted so that no one can check the system to see where the hacker modified the system.
- C:** A Floppy will not be large enough to hold the database.

Q. 107

After installing a Linux server and activating SSH on it, you try to authenticate, but are rejected due to an “authenticated failure.” You have properly transferred host and public keys, and all of your servers use the same flavor of SSH (Open SSH). What is a likely cause for your failure to connect to this newly configured server?

- A. The version of SSH you are using is incompatible with your Linux system
- B. You must first conduct a Telnet session with the server
- C. You must first disable Telnet and rlogin for SSH to work properly
- D. Your name resolution is incorrectly configured

Answer: D

Explanation: SSH needs DNS to function properly. Apparently the name resolution is configured incorrectly.

An SSH (Secure Shell Protocol) session is very similar to a Telnet session. Where a SSH session differs from telnet is that your password is encrypted and not sent in the clear. OpenSSH is a FREE version of the SSH protocol suite.

Incorrect Answers:

A: SSH is an open standard. It does not depend on different versions of LINUX.

B: A SSH session is not a Telnet session. They are just similar.

C: The only reason for disabling Telnet is out of security. Telnet uses no encryption and sends the password in plain text.

Q. 108

What is another term for a network security manager who acts as a potential hacker (a person looking for security loopholes)?

- A. An agent
- B. An auditor
- C. An assessor
- D. An analyzer

Answer: B

Explanation: When a friendly party tries to act as a potential hacker he is called an auditor.

Incorrect Answers:

A: A friendly party that acts like a potential hacker is called an auditor, not an agent.

C: A friendly party that acts like a potential hacker is called an auditor, not an assessor.

D: A friendly party that acts like a potential hacker is called an auditor, not an analyzer.

Q. 109

Helga is a systems administrator. She sees that an attacker from a remote location is sending invalid packets, trying to monopolize Helga's network connection so that a denial of service occurs. What characteristic of the activity makes Helga think this is a denial-of-service attack?

- A. Bandwidth consumption
- B. Hijacking of internal user resources
- C. Use of an illicit server
- D. System slowdown

Answer: A

Explanation: Bandwidth consumption is a technique for denial of service, and Helga would see her connection slowing down very fast.

Incorrect Answers:

B: Hijacking would not be used in a DoS attack.

C: The illicit server attack is not a technique that would be used for DoS attack.

D: Since a denial of service (DoS) attack is normally used to consume network resources to the point of making a system inaccessible, you would not see a system slowdown. The system may be able to fight off the network traffic without committing system resources so everything may look fine.

Q. 110

What is the most secure policy for a firewall?

- A. To reject all traffic unless it is explicitly permitted
- B. To accept all traffic unless it is explicitly rejected
- C. To enable all internal interfaces
- D. To enable all external interfaces

Answer: A

Explanation: By rejecting all traffic unless it is explicitly permitted makes sure that there are no open holes. If we just let any traffic through, then someone (a hacker) can exploit that situation and compromise the network.

Incorrect Answers:

B: To explicitly reject traffic requires knowledge of ALL potentially damaging traffic that might be sent to the firewall. No one can really know ALL, and to know many could mean a lot of rules being put in place – but most likely never enough. There will always end up being one loophole that a hacker finds.

C, D: Enabling all interfaces might not be a good idea, especially if there are multiple interfaces and they are connected to segments that require protection, and there are no filters in place to sift out damaging traffic.

Q. 111

Which of the following do hackers target because it usually communicates in cleartext, and because it often carries sensitive information?

- A. Router
- B. DNS server
- C. FTP server
- D. E-mail server

Answer: C

Explanation: A FTP server is an attack point because it is usually open to the outside Internet, and does not use any encryption, such as SSL. Userids and passwords are in the clear, and by monitoring the network, user and passwords can be collected.

Incorrect Answers:

- A:** A router, if exposed, would not provide sensitive information. User and Password information on the router would usually be independent of other systems on the network, and would not provide an account to attack inside servers. The only traffic that the router generates is routing table updates, although possible useful, is not of great use to the hacker.
- B:** The DNS server also does all its traffic in the clear, including zone transfers. Although this traffic can be used to find out about the IP to Name mappings of a network, this is not very sensitive information.
- D:** An e-mail server could carry a lot of sensitive information, if someone was passing that as text in an e-mail. Such traffic, if very sensitive, should be encrypted, meaning all information is not in the clear. It is very unlikely, and only by chance, that a hacker can gain information from those memos to breach a network.

Q. 112

What can a hacker destroy or modify to make a server or network intrusion undetectable?

- A. User accounts
- B. Log files
- C. Operating systems
- D. Passwords

Answer: B

Explanation: Log files keep an audit trail of system activity. If a hacker wanted to cover his tracks, then destroying the log files will remove any footprints or traces of the hacker ever being there.

Incorrect Answers:

- A:** User accounts that are created or destroyed, or even changed, are usually audited and logged. So, examination of the log files will show that someone was doing this activity, and nothing is left undetected.
- B:** If the hacker destroys the operating system, someone will know because the system will be down. If the system is modified, then that modification will show up in a log file somewhere, and examination of the logs will show a trail of changes.
- D:** Modification of passwords will not hide the fact that someone got into the system. It might actually tip someone off that there was an intrusion when someone can no longer log onto their account because the password no longer works.

Q. 113

Which of the following targets is more vulnerable to hacking attacks because of its location in relation to the firewall?

- A. DNS server
- B. FTP server
- C. E-mail server
- D. Router

Answer: D

Explanation: The routers must often be physically placed outside the firewall. These routers are therefore vulnerable to hacker attacks.

Incorrect Answers:

- A:** The DNS server for the Intranet would be inside the firewall, and would communicate with outside DNS servers using forwarding. DNS servers placed outside the firewall would be open to an attack, and usually zone transfers should not be allowed to pass the firewall (as a good practice)
- B:** A FTP server is usually provided by a company so that outside clients can access it and download documents and other files. The FTP server should be placed inside the firewall, and would not be vulnerable for attacks due to its location to the firewall.
- C:** The E-Mail server services the corporation. It may communicate through the firewall to receive and deliver mail from the Internet. The e-mail server is usually kept inside firewall so that the firewall can run scanning software to check the e-mail for proper addressing, and viruses.

Q. 114

Helga's web server is placed behind her corporate firewall. Currently, her firewall allows only VPN connections from other remote clients and networks. She wants to open the internet-facing interface on her firewall so that it allows all users on the Internet to access her web server. Which of the following must Helga's rule contain?

- A. Instructions allowing all UDP connections with a destination port of 80 and a source port of 1024
- B. Instructions allowing all UDP connections with a source port of 80 on the external interface and a destination port of 1024
- C. Instructions allowing all TCP connections with a source port of 80 on the internal interface and a destination port of 80
- D. Instructions allowing all TCP connections with a source port higher than 1024 and a destination port of 80

Answer: D

Explanation: HTTP uses TCP port 80, so as a server, which will be a destination for the client, needs to be 80. All ports from 0-1023 are reserved for servers and are called well known ports. All ports above 1023 are used by clients as their source port. This will allow the web server to be used.

Incorrect Answers:

- A:** HTTP uses TCP, not UDP.
- B:** HTTP uses TCP, not UDP.
- C:** Since the ports used by the client are above 1023, both addresses will not be the same. One address should be a well known port (below 1024) for the server and for the client a port above 1023.

Q. 115

When assessing the risk to a machine or network, what step should you take first?

- A. Analyzing, categorizing and prioritizing resources
- B. Evaluating the existing perimeter and internal security
- C. Checking for a written security policy
- D. Analyzing the use of existing management and control architecture

Answer: C

Explanation:

The first step is to check for a written security policy.

The next step is Analyzing, categorizing and prioritizing resources

The next step is Consider Business Concerns

The next step is Evaluating the existing perimeter and internal security

The next step is Analyzing the use of existing management and control architecture

You first check for a written security policy to find out what is already in place and to assess the current situation.

Incorrect Answers:

A, B, D: are not the first, but above they are listed in the proper sequence.

Q. 116

Your company has suffered several denial-of-service attacks involving Microsoft Outlook e-mail clients. How can you protect your systems from such attacks in the future, yet still allows client users to accomplish their jobs?

- A. Install antivirus applications on the clients and the e-mail server
- B. Filter out all attachments from e-mail messages at the e-mail server
- C. Filter out all attachments from e-mail messages at the e-mail server, and install antivirus applications on the clients
- D. Install personal firewalls in the e-mail server and on each client

Answer: A

Explanation: DoS attacks coming from an e-mail applications that affects the client is usually virus code that causes damage to the client system so that it is disabled. Detection of these viruses before they can do damage is critical. Using antivirus applications on the clients and the e-mail server for this detection will help prevent future attacks. Also, if possible, scanning software can also be added to the firewall or proxy server.

Incorrect Answers:

B, C: Without the attachments, client users won't be able to still do their jobs. Those attachments can have documents or spreadsheets that those users need to process.

D: A firewall won't help, unless it can detect and act upon any threatening code in the e-mail message payloads.

Q. 117

Which type of device communicates with external servers on behalf of internal clients?

- A. A client-level gateway
- B. An application-level gateway

- C. A proxy server
- D. A packet filter

Answer: C

Explanation:

The key word here is behalf. The proxy server is a server used to protect networks, and is usually placed between a corporate network and the Internet. Requests sent to the proxy server are re-issued by the proxy server on behalf of the client, and externally the requests have the IP address of the proxy server.

Incorrect Answers:

- A:** A gateway is a device that does protocol conversion at layer 4 of the ISO model. It does protocol conversion, but does not act in behalf of any clients passing traffic through the gateway.
- B:** A gateway is a device that does protocol conversion at layer 4 of the ISO model. It does protocol conversion, but does not act in behalf of any clients passing traffic through the gateway.
- D:** A packet filter operates at Layer 3 of the ISO model, and inspects packet traffic and either allows or drops the packet after inspection. Even in the case of stateful inspection, packets are inspected and either allowed or denied. The packet filter, usually in a firewall, does not act on behalf of any client, it is just a censor of the datastream.

Q. 118

Which choice lists the components that form security descriptors for Windows NT/2000 objects?

- A. The user name (UNAME), the password (PWD), and the object-owner security identifier (SID)
- B. The UNAME, the access profile of the object-owner SID, and confirmation by the system access control list (SACL)
- C. The object-owner SID, the discretionary access control list (DACL), the SACL, and the group SID
- D. The user name, the object identifier (OID), the set user identifier (UID), and the time/date stamp

Answer: C

Explanation:

- All objects within the NT system have security descriptors, which hold the settings for security. This is what is contained in a descriptor:
 - Owner's SID
 - Group SID
 - *DACL*

Leading the way in IT testing and certification tools, www.testking.com

- *SACL*
- A DACL (Discretionary Access Control list) will possess a list of both users and groups and whatever permissions they have. (Allowed or Denied)
- The SACL (System Access Control List) will have contained a list of any events that are set to audit for that particular object.

Incorrect Answers:

A, B, D: Most of the fields, such as the USERNAME and password are not used as part of the security descriptor.

Q. 119

Which single service can you disable to stop approximately two-thirds of the exploration tools used against Windows NT/2000?

- A. The Schedule service.
- B. The POSIX subsystem with the C2Config tool.
- C. The Ansi.sys from the boot loader.
- D. The NetBIOS service.

Answer: D

Explanation: Disabling the NetBIOS service is a good server hardening precaution. Hackers can utilize the NetBIOS service to get account information on Windows 2000/NT systems.

Note: NetBIOS is the networking protocol used by Windows Machines to communicate with each other on the network.

Incorrect Answers:

- A:** All the schedule service provides is the ability to schedule other tasks to run at scheduled times. It would not prevent any tools or commands from running at all, it just prevents someone to schedule these tools and tasks from being scheduled on a time basis.
Note: The Schedule service was used to by hackers to gain access to Windows NT 4.0 Servers. This was due to a bug in Internet Explorer.
- B:** This is not the most vulnerable service on Windows NT/2000.
Note: The POSIX subsystem is the UNIX compatibility feature of Windows NT and Windows 2000. It is removed by using the C2Config tool provided in the Resource Kit. This feature is large, provides a lot more functionality that is rarely ever used, and can these resource can be released by using C2Configuration options. Many tools provided via the POSIX feature will be removed, including many of the exploration tools

- C:** ANSI.SYS: Defines functions that change display graphics, control cursor movement, and reassign keys. The ANSI.SYS device driver supports ANSI terminal emulation of escape sequences to control your system's screen and keyboard. An ANSI escape sequence is a sequence of ASCII characters, the first two of which are the escape character (1Bh) and the left-bracket character (5Bh). The character or characters following the escape and left-bracket characters specify an alphanumeric code that controls a keyboard or display function. ANSI escape sequences distinguish between uppercase and lowercase letters; for example, "A" and "a" have completely different meanings. ANSI.SYS is NOT an exploration tool, and only affects the local terminal/console.

Q. 120

Which is included in the formula that Windows NT/2000 uses to create the Security Identifier?

- A. A semi-random number generated by the CPU based on the number of processes in the queue
- B. A set of numbers based on the serial number of the computer CPU and the serial number of Windows NT
- C. The computer name and the current amount of CPU time used by the user mode
- D. The octal encryption of the user name and the password

Answer: C

Explanation:

- A SID is generated by a combination of:
 - Computer name
 - Current time
 - The amount of time that current user mode thread has been using the CPU or CPU time.

Incorrect Answers:

A, B, D: These are not the combinations used.

Q. 121

A computer on your network is responding very slowly to network requests, and then it stops responding at all. You use a packet sniffer and create a filter that views packets being sent to that host. You see that the host is receiving thousands of ICMP packets a minute. What type of attack is causing the system to slow down?

- A. A spoofing attack
- B. A root kit installed on the system

- C. A denial-of-service attack
- D. A man-in-the-middle attack

Answer: C

Explanation:

There is an excessive amount of ping commands hitting the server, most likely a smurf attack. When network traffic slows down the server, and the traffic is not normal traffic, it is most likely a denial of service attack. In this case, thousands of ICMP packets per minute is not normal.

Incorrect Answers:

- A:** A spoofing attack is when IP packets are changed to make the source of the packet look like it originated for a different user.
- B:** A root kit, usually used on Unix systems, provides a back door into the system.
- D:** A man-in-the-middle attack involves someone intercepting packets between two hosts and relays the information. In this attack the hacker does not take over the conversation (hijack), but does pose as one of the legitimate parties.

Q. 122

What is typically the most desirable asset for a hacker to obtain from a company or department?

- A. E-mail messages
- B. Router tables
- C. Database information
- D. DNS server records

Answer: C

Explanation:

To get access to files, for example database files, is very desirable for a hacker. Databases typically contain the most valuable company information and are therefore very desirable for a hacker.

Incorrect Answers:

- A:** E-Mail messages would be desirable if the objective was corporate espionage, but for most hackers this is not why they break into systems. This information could be an ultimate objective, but a hacker first needs information to allow further attack of the network and servers on it.
- B:** Router tables will expose some of the network structure, but DNS zones will expose actual assigned IP addresses. After exposing the DNS zones, then router tables would be the next step.

- C:** Breaching a database may provide confidential and valuable information, but this does not help the hacker break into the network. Hackers want to break into the network, and information in a regular database does not help the hacker advance into the network.
- D:** Though DNS server records are valuable to hackers. Files are a more valuable asset though.
Note: Hackers will attempt to get DNS information by attempting to initiate a zone transfer. The DNS database will expose the defined nodes in the network and their IP addresses. The first tools of attack used by a hacker are usually WHOIS and NSLOOKUP, which are used to find the zones and transfer them.

Q. 123

Which service, tool or command provides information about administrators, domain name servers, additional domains and physical locations?

- A. Whois
- B. Ping scanner
- C. Host
- D. Traceroute

Answer: A

Explanation:

The WHOIS command is used to find out information about the Primary and Secondary name servers and zones of the organization. Information about the zone administrators can be exposed using this command.

Incorrect Answers:

- B:** The ping scanner is used to determine which IP addresses are used in a network by pinging each possible IP address and seeing which nodes provide a response. It does not identify what kind of server responded, and does not have the ability by itself to get information about the domain structure. At best it can map the network.
- C:** The host command provides IP to Name and Name to IP address mapping. It provides a TCP/IP mapping of addresses, not any DNS information.
- D:** Traceroute (Tracert in Windows NT) uses ICMP to map a network path. It does not provide DNS information, although it might provide the fully qualified DNS name of the zone for the IP address – if reverse lookup is defined. For an IP to name mapping, you would need to know the host name in advance, and these functions are not provided as part of the ICMP commands themselves. Information of administrators and other domains would not be exposed using this command.

Q. 124

Your IDS application pages you at 3:00 a.m, and informed you that an attack occurred against your DNS server. You drive to the server site to investigate. You find no evidence of an attack, although the IDS application claims that a remote DNS server waged an attack on port 53 of your intranet DNS server. You check the logs and discover that a zone transfer has occurred. You check your zones and name resolution, and discover that all entries exist, and no unusual entries have been added to the database. What has most likely occurred?

- A. A DNS poisoning attack against your internal DNS server.
- B. A denial-of-service attack against your internal DNS server.
- C. A false positive generated by the IDS.
- D. A malfunction of the internal name server.

Answer: A

Explanation:

IDS is Intrusion Detection System. All entries exist and nothing added. BUT – has anything changed? A poisoning attack is where DNS records are modified to point somewhere else (a different IP address) other than where it should be pointed.

Incorrect Answers:

- B:** Most DoS attacks are to disable the server and prevent access. Causing a single zone transfer will not do this. If the DNS server showed hundreds or thousands of zone transfers in a short period, then maybe a DoS attack. The IDS would identify other activities if a DoS was being attempted.
- C:** A false positive could always be a possibility, but if the zone transfer is suspicious, it requires more examination to rule out modifications to the zone, since we only checked to see if the records are there, we didn't check to see if they were changed. Since a zone is usually transferred in a single shot, there is no tagging on individual records to determine when records were changed.
- D:** If the internal name server malfunctioned, there would be other indications in the log of a restart. Or, the DNS may fail and not even come up. A malfunction should not trip the IDS.

Q. 125

Which of the following is a potential security risk when using CGI scripts?

- A. CGI scripts can contain viruses that can be used against your system.
- B. Compromised CGI scripts are often used in packet spoofing because they do not check packets that generate.
- C. CGI scripts can create broadcast storms on the local network.
- D. Remote user input can be used to execute local commands.

Answer: D

Explanation:

CGI scripts are program executables capable of executing programs. A hacker could subvert the system and execute programs that might allow command execution.

Incorrect Answers:

- A:** Although this is a possibility, CGI scripts could be installed if only secure, for example only internal written CGI scripts, or making sure they are from reliable sources. In other words, you can be careful of what CGI scripts you install. The CGI script having viruses would not be a concern unless there was a method in place to upload new CGI modules. Since CGI scripts are used in HTTP, and HTTP usually does not provide upload facilities, having someone slip in a virus in a CGI module will be rare and difficult.
- B:** CGI scripts run at the HTTP level, which is an Application protocol. To spoof packets, where the IP addressees in the packet are altered, has to be done at lower layers in the protocol stack.
- C:** CGI scripts run at the HTTP level, which is an Application protocol. To cause a broadcast storm will require modification of the addresses in the packet and frame and has to be done at lower layers in the protocol stack.

Q. 126

Which choice best defines the Windows NT Security Account Manager?

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

Answer: B

Explanation: The Windows NT Security Account Manager main task is to manage the SAM database which contains identities and credentials for the users in the domain..

Incorrect Answers:

- A:** The GINA.DLL is used for login authentication.
- C:** The Windows NT Security Account Manager doesn't denote any particular machine in the LAN.
- D:** The Windows Security Account Manager is much more than the log on/lock interface.

Q. 127

Lucy wants to ensure that her Windows NT Server 4.0 and Windows 2000 systems do not incur any unauthorized changes. What can she do to help secure her registry from changes?

- A. Lock the registry so that it cannot be written to by any application.
- B. Enable auditing.
- C. Back up the registry.
- D. Configure the registry so that it does not change.

Answer: A

Explanation: By locking the registry so that applications are prohibited from making changes in it, we keep the registry secure.

Incorrect Answers:

- B:** You could set up auditing so that it logs information on who make changes to the registry, however this would not prevent anyone from changing the registry.
- C:** Backing up the registry is a good precaution, but it will not prevent the registry from being updated.
- D:** It is not possible to configure the registry so that it does not change.

Q. 128

Andreas wants to choose a strong password for his computer. Which of the following should he include for his password?

- A. A mixture of uppercase and lowercase letters, symbols and numbers.
- B. An arcane phrase only he can remember.
- C. An incorrect spelling of a word or a phrase.
- D. A mixture of random words that form non-sense.

Answer: A

Explanation: As a recommended best practice every password should be a mixture of uppercase and lowercase letters, symbols and numbers.

Incorrect Answers:

- B:** An arcane phrase is vulnerable for brute force attacks.
- C:** An incorrect spelled word or phrase is vulnerable for brute force attacks.
- D:** Random words are also vulnerable for brute force attacks.

Q. 129

What is the essential element in the implementation of any security plan?

- A. Testing to make sure any server-side scripts are secure
- B. Testing patch levels
- C. Proper firewall configuration
- D. Auditing

Answer: B

Explanation: It is important to apply and test the latest patch levels, hotfixes and service packs. Patch level testing is an essential element in a every security plan.

Incorrect Answers:

- A:** Securing server-side scripts is only a small part in a security plan. It isn't essential.
- C:** Proper firewall configuration is important, but it is not an essential element in a security plan. Not all scenarios contain firewalls.
- D:** Auditing will do no good if patch levels are not kept current.

Q. 130

A malicious user has connected to your system and learned the specifics of your operating system, including its current patch levels and the operating system name. What is the term for this type of scanning attack?

- A. SYN detection
- B. TCP priming
- C. Cache poisoning
- D. Stack fingerprinting

Answer: D

Explanation: Several new tools have been made available on the Internet that to a high degree of accuracy can tell the operating system of a host just by examining subtle details in the way the TCP/IP stack was implemented within that operating system. This method is called TCP/IP fingerprinting. With information in regards to the flavor and version of the operating system, a hacker could look for any number of possible vulnerabilities.

Incorrect Answers:

- A:** SYN detection is a preventive method against SYN floods. SYN floods use inherent characteristics in the TCP/IP protocol to flood a system with network packets. Eventually, the system will not be able to respond to network packets from anyone and the target system becomes unusable.
- B:** There is no hacker attack method called TCP priming.

C: Cache poisoning is planned corruption of DNS records by unauthorized users. Cache poisoning is not used to retrieve information on specifics of any installed operating system.

Note: Cache poisoning occurs when malicious or misleading data received from a remote name server is saved (cached) by a gullible name server. This bad data is then made available to programs running on workstations that request the cached data through the client interface (resolver). This can adversely affect the mapping between host names and IP addresses, among other things. Once this mapping has been changed, hosts looking for legitimate DNS responses from a corrupted server can be redirected to arbitrary sites.

Q. 131

Which type of attack causes a remote host to crash because it cannot respond to any new TCP connection requests?

- A. Crack attack
- B. Smurf attack
- C. SYN flood
- D. ICMP flood

Answer: C

Explanation: SYN floods use inherent characteristics in the TCP/IP protocol to flood a system with network packets. A SYN flood starts a TCP session by issuing a SYN request which is not completed and left unfinished. This is repeated continuously. Eventually, the system will not be able to respond to network packets from anyone and the target system becomes unusable.

Incorrect Answers:

A: The aim of a crack attack is to steal passwords, not to cause the remote host to crash.

B: Smurf attacks, attacks involving forged ICMP echo request packets sent to IP broadcast addresses, can result in large amounts of ICMP echo reply packets being sent from an intermediary site to a victim, which can cause network congestion or outages.

The ICMP echo requests does not use a TCP connection.

D: An ICMP flood is usually accomplished by broadcasting either a bunch of ICMP pings or UDP packets. The idea is, to send so much data to your system, that it slows you down so much that you're disconnected from IRC due to a ping timeout.

The ICMP ping does not use a TCP connection.

Q. 132

Tavo wants to improve the security on his FTP server. He is especially worried about password-sniffing attacks. Which of the following is the best action for Tavo to take?

- A. Disable anonymous logins.
- B. Allow only anonymous logins.
- C. Configure the firewall to block port 21.
- D. Place the FTP server outside of the firewall.

Answer: B

Explanation: We must protect against password-sniffing attacks, also known as man in the middle attacks. In this scenario we could do it in two ways:

- ensure that password authentication traffic is strongly encrypted.
This is however not an option in this scenario.
- only allow anonymous logins.
By only allowing anonymous access no passwords will be sent from the ftp user to the ftp server.

Incorrect Answers:

- A:** Enforcing passwords, and not using encryption, would allow a man in the middle to obtain the login id and password by sniffing.
- C:** Blocking port 21 would prevent FTP from working.
- D:** Placing the FTP server outside the firewall would make it more vulnerable and it would improve security.

Q. 133

Raul wants to know where to find encrypted passwords in a secured Linux server. Where is this information located on the hard drive?

- A. /etc/shadow
- B. /etc/passwd
- C. /secure/etc/shadow
- D. /etc/security/shadow

Answer: A

Explanation: User accounts, ids and passwords, on UNIX and Linux servers are by default stored in the /etc/passwd file. However, this file is world readable and somewhat of a security risk. On a secure server the shadow password format is used instead. This method stores account information in the /etc/passwd file in a compatible format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called "/etc/shadow", contains encrypted password as well as other information such as account

or password expiration values, etc. The /etc/shadow file is readable only by the root account and is therefore less of a security risk.

Incorrect Answers:

B: On a secure server the /etc/passwd file is not used to store passwords.

C: The /secure/etc/shadow file is not used to store passwords.

D: The /etc/security/shadow file is not used to store passwords.

Q. 134

In which risk assessment stage does the security auditor map the systems and resources on a network?

- A. Penetration
- B. Cancellation
- C. Activation
- D. Discovery

Answer: D

Explanation: Discovery is the task of testing the network security for effectiveness and locating weaknesses. During this stage you map out the network, the systems and resources, and attempt to discover every resource. This is the most time consuming test.

Note: The risk assessment stages usually include the following three stages: Discovery, Penetration, and Control.

Incorrect Answers:

A: In Penetration, all access controls (including login accounts and passwords) are bypassed. In this stage you inspect systems for possible weaknesses and try to break into these weaknesses.

B: There is no risk assessment stage called Cancellation.

C: Activation is not a risk assessment stage.

Q. 135

You installed SSH on an older Linux server. You want to allow users to authenticate securely. Which choice lists two actions that must occur first?

- A. Public keys must first be exchanged to enable data encryption, and then the system exchange host keys to enable authentication without passwords.

- B. The system must exchange host keys to enable data encryption, and individual users must exchange public keys to enable authentication without passwords.
- C. A key pair must be obtained from a CA to enable data encryption, then host keys must be exchanged to enable authentication.
- D. A key pair must be obtained from a CA to enable authentication, then host keys must be exchanged to enable data encryption.

Answer: A

Explanation: SSH uses a public key scheme. First public keys are exchanged to enable data encryption, then host keys are exchanged to enable authentication.

SSH uses two different kinds of key pairs: host keys and user keys. The user keys are public.

Note 1: An SSH (Secure Shell Protocol) session is very similar to a Telnet session. Where a SSH session differs from telnet is that your password is encrypted and not sent in the clear. OpenSSH is a FREE version of the SSH protocol suite.

Note host keys:

Part of the SSH installation process is the generation of a host key (pair). The host key generated at setup time can be used by that host indefinitely, barring root compromise. And Because the host key identifies the host, not individual users, each host needs only one host key. Note that host keys are used by **all** computers that run SSH regardless of whether they run only the SSH client (ssh), SSH daemon (sshd), or both.

SSH can negotiate keys and set up encrypted sessions completely transparent to users using host keys.

Incorrect Answers:

- A:** First host keys, not user keys, are used to enable data encryption.
- B:** The public keys are exchanged first, not the host keys.
- C:** A key pair doesn't have to be obtained from a CA, instead host keys can be used to initiate data encryption.
- D:** A key pair doesn't have to be obtained from a CA, instead host keys can be used to initiate data encryption.

Q. 136

You want to secure your SMTP transmissions from sniffing attacks. How can you accomplish this?

- A. Forbid relaying.
- B. Enforce masquerading.
- C. Use an SSL certificate.
- D. Use strict bounds checking on arrays.

Answer: C

Explanation: The best defense against sniffing, also known as man in the middle attacks, is to use strong encryption. SSL (Secure Sockets Layer) can be used to implement strong security for SMTP transmissions. SSL uses certificates to implement security.

Incorrect Answers:

- A:** To prohibit relaying would enable you to control the receipt and delivery of mail. Here however, we want to prevent anyone sniffing the SMTP traffic between the sender and receiver and relaying would not be of any use.
- B:** Masquerading is a technique is a Network Translation (NAT) scheme that is used to let many clients use the same IP address. It would not help against sniffing attacks however.
- D:** Strict bounds checking on arrays cannot be applied to SMTP traffic.