Information Security Officer Job Interview Questions And Answers

Interview Questions Answers

https://interviewquestionsanswers.org/

About Interview Questions Answers

Interview Questions Answers . ORG is an interview preparation guide of thousands of Job Interview Questions And Answers, Job Interviews are always stressful even for job seekers who have gone on countless interviews. The best way to reduce the stress is to be prepared for your job interview. Take the time to review the standard interview questions you will most likely be asked. These interview questions and answers on Information Security Officer will help you strengthen your technical skills, prepare for the interviews and quickly revise the concepts.

If you find any **question or answer** is incorrect or incomplete then you can **submit your question or answer** directly with out any registration or login at our website. You just need to visit Information Security Officer Interview Questions And Answers to add your answer click on the *Submit Your Answer* links on the website; with each question to post your answer, if you want to ask any question then you will have a link *Submit Your Question*; that's will add your question in Information Security Officer category. To ensure quality, each submission is checked by our team, before it becomes live. This Information Security Officer Interview preparation PDF was generated at **Wednesday 29th November, 2023**

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

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

If you need any further assistance or have queries regarding this document or its material or any of other inquiry, please do not hesitate to contact us.

Best Of Luck.

Interview Questions Answers.ORG Team
https://InterviewQuestionsAnswers.ORG/
Support@InterviewQuestionsAnswers.ORG

Information Security Officer Interview Questions And Answers Guide.

Question - 1:

Explain how does HTTP handle state?

Ans:

It doesn't, of course. Not natively. Good answers are things like "cookies", but the best answer is that cookies are a hack to make up for the fact that HTTP doesn't do it itself.

View All Answers

Question - 2:

Do you know what is salting, and why is it used?

Ans:

You purposely want to give the question without context. If they know what salting is just by name, they've either studied well or have actually been exposed to this stuff for a while.

View All Answers

Question - 3:

Tell me what are your first three steps when securing a Windows server?

Ans:

Their list isn't key here (unless it's bad); the key is to not get panic.

View All Answers

Question - 4:

Tell me what kind of attack is a standard Diffie-Hellman exchange vulnerable to?

Ans:

Man-in-the-middle, as neither side is authenticated.

View All Answers

Question - 5:

Do you know what exactly is Cross Site Scripting?

Ans:

You'd be amazed at how many security people don't know even the basics of this immensely important topic. We're looking for them to say anything regarding an attacker getting a victim to run script content (usually JavaScript) within their browser.

View All Answers

Question - 6:

Tell me what are your first three steps when securing a Linux server?

Ans:

Their list isn't key here (unless it's bad); the key is to not get panic.

View All Answers

Question - 7:

Explain what's the difference between stored and reflected XSS?

Ans:

Stored is on a static page or pulled from a database and displayed to the user directly. Reflected comes from the user in the form of a request (usually constructed by an attacker), and then gets run in the victim's browser when the results are returned from the site.

View All Answers

Question - 8:

Tell me do you prefer filtered ports or closed ports on your firewall?

Ans:

Look for a discussion of security by obscurity and the pros and cons of being visible vs. not. There can be many signs of maturity or immaturity in this answer.

View All Answers

Question - 9:

Explain how would you login to Active Directory from a Linux or Mac box?

Ans:

While it may sound odd, it is possible to access Active Directory from a non-Windows system. Active Directory uses an implementation of the SMB protocol, which can be accessed from a Linux or Mac system by using the Samba program. Depending on the version, this can allow for share access, printing, and even Active Directory membership.

View All Answers

Question - 10:

Do you know how to change your DNS settings in Linux/Windows?

Ans:

Here you're looking for a quick comeback for any position that will involve system administration (see system security). If they don't know how to change their DNS server in the two most popular operating systems in the world, then you're likely working with someone very junior or otherwise highly abstracted from the real world.

View All Answers

Question - 11:

Explain what do you have on your home network?

Ans:

Nothing shows you how to break and fix things more than a test environment, and for most people that means their home network. Whether its a Windows laptop with a wireless generic router and a phone all the way up to 14 Linux Workstations, an Active Directory Domain Controller, a dedicated Firewall appliance and a net-attached toaster - as long as you are learning and fiddling with it, that's what matters.

View All Answers

Question - 12:

Explain how does one defend against CSRF?

Ans:

Nonces required by the server for each page or each request is an accepted, albeit not foolproof, method. Again, we're looking for recognition and basic understanding here-not a full, expert level dissertation on the subject. Adjust expectations according to the position you're hiring for.

View All Answers

Question - 13:

Do you know what is the difference between a Black Hat and a White Hat?

Ans:

This particular question can lead into a major philosophical debate about freedom of information, and if something is implemented in a deliberately broken way it isn't actually breaking into it, etc etc. The one I've heard the most is the classic Jedi example - same tools, different ideologies. Personally, with the people I know that have worked on both sides of the line it comes down to this - the difference between a Black Hat and a White Hat is who is signing the check..

View All Answers

Question - 14:

Explain what's the difference between Diffie-Hellman and RSA?

Ans:

Diffie-Hellman is a key-exchange protocol, and RSA is an encryption/signing protocol. If they get that far, make sure they can elaborate on the actual difference, which is that one requires you to have key material beforehand (RSA), while the other does not (DH). Blank stares are undesirable.

View All Answers

Question - 15:

Tell me why would you want to use SSH from a Windows pc?

Ans:

SSH (TCP port 22) is a secure connection used on many different systems and dedicated appliances. Routers, Switches, SFTP servers and unsecure programs being tunnelled through this port all can be used to help harden a connection against eavesdropping. Despite the fact that most times when you hear about somebody 'SSHing' into a box it involves Linux, the SSH protocol itself is actually implemented on a wide variety of systems - though not by default on most Windows systems. Programs like PuTTY, Filezilla and others have Windows ports available, which allow Windows users the same ease-of-use connectivity to these devices as do Linux users.

View All Answers

Question - 16:

Explain what kind of network do you have at home?

Ans:

Good answers here are anything that shows you he's a computer/technology/security enthusiast and not just someone looking for a paycheck. So if he's got multiple systems running multiple operating systems you're probably in good shape. What you don't want to hear is, "I get enough computers when I'm at work..." I've yet to meet a serious security guy who doesn't have a considerable home network-or at least access to one, even if it's not at home.

View All Answers

Question - 17:

Tell us what are the three ways to authenticate a person?

Ans:

Something they know (password), something they have (token), and something they are (biometrics). Two-factor authentication often times uses a password and token setup, although in some cases this can be a PIN and thumbprint.

View All Answers

Question - 18:

Tell me how would you find out what a POST code means?

Ans:

POST is one of the best tools available when a system will not boot. Normally through the use of either display LEDs in more modern systems, or traditionally through audio tones, these specific codes can tell you what the system doesn't like about its current setup. Because of how rare these events can be, unless you are on a tech bench day in and day out, reference materials such as the Motherboard manual and your search engine of choice can be tremendous assets. Just remember to make sure that everything is seated correctly, you have at least the minimum required components to boot, and most importantly that you have all of your connections on the correct pins.

View All Answers

Question - 19:

Explain how would you judge if a remote server is running IIS or Apache?

Ans:

Error messages oftentimes giveaway what the server is running, and many times if the website administrator has not set up custom error pages for every site, it can give it away as simply as just entering a known bad address. Other times, just using telnet can be enough to see how it responds. Never underestimate the amount of information that can be gained by not getting the right answer but by asking the right questions.

View All Answers

Question - 20:

Tell me what are your daily news checks?

Ans:

It seems like we can't go more than a few days anymore without hearing about a major breach, which on the surface would make it seem that more people and places are being hacked than ever before (which to be honest is true). However, it also shows that detection and reporting of attacks is improving per requirements of both government entities and insurance companies. As a result, the public and security professionals are both better informed as to what they can do to help protect themselves and watch out for falsified charges on their accounts. Keeping up to date on these matters is vital for anyone interested in Information Security.

View All Answers

Question - 21:

Tell us where do you get your security news from?

Ans:

Here I'm looking to see how in tune they are with the security community. Answers I'm looking for include things like Team Cymru, Reddit, Twitter, etc. The exact sources don't really matter. What does matter is that he doesn't respond with, "I go to the CNET website.", or, "I wait until someone tells me about events.". It's these types of answers that will tell you he's likely not on top of things.

View All Answers

Question - 22:

Tell me what are Linux's strengths and weaknesses vs. Windows?

Ans:

Look for biases. Does he absolutely hate Windows and refuse to work with it? This is a sign of an immature hobbyist who will cause you problems in the future. Is he a Windows fanboy who hates Linux with a passion? If so just thank him for his time and show him out. Linux is everywhere in the security world.

View All Answers

Question - 23:

Explain what is SSL and why is it not enough when it comes to encryption?

Ans:

SSL is identity verification, not hard data encryption. It is designed to be able to prove that the person you are talking to on the other end is who they say they are. SSL and its big brother TLS are both used almost everyone online, but the problem is because of this it is a huge target and is mainly attacked via its implementation

(The Heartbleed bug for example) and its known methodology. As a result, SSL can be stripped in certain circumstances, so additional protections for data-in-transit and data-at-rest are very good ideas.

View All Answers

Question - 24:

Suppose what is the difference between a vulnerability and an exploit?

Ans:

A lot of people would say that they are the same thing, and in a sense they would be right. However, one is a potential problem while the other is an active problem. Think of it like this: You have a shed with a broken lock where it won't latch properly. In some areas such as major cities, that would be a major problem that needs to be resolved immediately, while in others like rural areas its more of a nuisance that can be fixed when you get around to it. In both scenarios it would be a vulnerability, while the major cities shed would be an example of an exploit - there are people in the area, actively exploiting a known problem.

View All Answers

Question - 25:

Explain what do you think of social networking sites such as Facebook and LinkedIn?

Ans:

This is a doozy, and there are an enormous number of opinions for this question. Many think they are the worst thing that ever happened to the world, while others praise their existence. In the realm of security, they can be the source of extreme data leaks if handled in their default configurations. It is possible to lock down permissions on social networking sites, but in some cases this isn't enough due to the fact that the backend is not sufficiently secured. This also doesn't help if somebody else's profile that you have on your list gets compromised. Keeping important data away from these kinds of sites is a top priority, and only connecting with those you trust is also extremely helpful.

View All Answers

Question - 26:

Tell me what's the difference between a threat, vulnerability, and a risk?

Ans:

As weak as the CISSP is as a security certification it does teach some good concepts. Knowing basics like risk, vulnerability, threat, exposure, etc. (and being able to differentiate them) is important for a security professional. Ask as many of these as you'd like, but keep in mind that there are a few differing schools on this. Just look for solid answers that are self-consistent.

View All Answers

Question - 27:

What is certified Firewall Analyst?

Ans:

It declares that the individual has proficiency in skills and abilities to design, monitor and configure routers, firewalls and perimeter defense systems

View All Answers

Question - 28:

Tell me what is a pentest?

Ans:

"Pentest" is short for "penetration test", and involves having a trusted security expert attack a system for the purpose of discovering, and repairing, security vulnerabilities before malicious attackers can exploit them. This is a critical procedure for securing a system, as the alternative method for discovering vulnerabilities is to wait for unknown agents to exploit them. By this time it is, of course, too late to do anything about them.
In order to keep a system secure, it is advisable to conduct a pentest on a regular basis, especially when new technology is added to the stack, or vulnerabilities are exposed in your current stack.

View All Answers

Question - 29:

Tell us what project that you have built are you most proud of?

Ans:

For some people, this would be the first computer they ever built, or the first time they modified a game console, or the first program they wrote, the list can go on and on. In my case, that would be a project for work that I was working on for years. It started out as an Excel spreadsheet that the Engineering department were using to keep track of their AutoCAD drawings, and ended up evolving through a couple hundred static HTML pages, an Access Database and frontend, and finally to a full on web application running in MySQL and PHP. This simple little thing ended up becoming an entire website with dedicated Engineering, Sales and Quality web apps used by the company globally, which just goes to show you you never know where something might lead.

View All Answers

Question - 30:

Tell me what is Cross-Site Request Forgery?

Ans:

Not knowing this is more forgivable than not knowing what XSS is, but only for junior positions. Desired answer: when an attacker gets a victim's browser to make requests, ideally with their credentials included, without their knowing. A solid example of this is when an IMG tag points to a URL associated with an action, e.g. http://foo.com/logout/. A victim just loading that page could potentially get logged out from foo.com, and their browser would have made the action, not them (since browsers load all IMG tags automatically).

View All Answers

Question - 31:

Tell me are open-source projects more or less secure than proprietary ones?

Ans:

The answer to this question is often very telling about a given candidate. It shows 1) whether or not they know what they're talking about in terms of development, and 2) it really illustrates the maturity of the individual (a common theme among my questions). My main goal here is to get them to show me pros and cons for each. If I just get the "many eyes" regurgitation then I'll know he's read Slashdot and not much else. And if I just get the "people in China can put anything in the kernel" routine then I'll know he's not so good at looking at the complete picture.
The ideal answer involves the size of the project, how many developers are working on it (and what their backgrounds are), and most importantly - quality control. In short, there's no way to tell the quality of a project simply by knowing that it's either open-source or proprietary. There are many examples of horribly insecure applications that came from both camps.

View All Answers

Question - 32:

Do you know what is the difference between an HIDS and a NIDS?

Ans:

Both acronyms are Intrusion Detection Systems, however the first is a Host Intrusion Detection System whereas the second is a Network Intrusion Detection System. An HIDS runs as a background utility in the same as an anti-virus program for instance, while a Network Intrusion Detection System sniffs packets as they go across the network looking for things that aren't quite ordinary. Both systems have two basic variants: signature based and anomaly based. Signature based is very much like an anti-virus system, looking for known values of known 'bad things', while anomaly looks more for network traffic that doesn't fit the usual pattern of the network. This requires a bit more time to get a good baseline, but in the long term can be better on the uptake for custom attacks.

View All Answers

Question - 33:

Do you know what's the difference between Symmetric and Asymmetric encryption?

Ans:

To boil down an extremely complicated topic into a few short words, Symmetric encryption uses the same key to encrypt and decrypt, while Asymmetric uses different keys for encryption and decryption. Symmetric is usually much faster, but is difficult to implement most times due to the fact that you would have to transfer the key over an unencrypted channel. Therefore many times an Asymmetric connection will be established first, then send creates the Symmetric connection. This leads us into the next topic...

View All Answers

Question - 34:

Explain what's the goal of information security within an organization?

Ans:

This is a big one. What I look for is one of two approaches; the first is the uber-lockdown approach, i.e. "To control access to information as much as possible, sir!" While admirable, this again shows a bit of immaturity. Not really in a bad way, just not quite what I'm looking for. A much better answer in my view is something along the lines of, "To help the organization succeed."
This type of response shows that the individual understands that business is there to make money, and that we are there to help them do that. It is this sort of perspective that I think represents the highest level of security understanding--a realization that security is there for the company and not the other way around.

View All Answers

Question - 35:

Explain how exactly does traceroute/tracert work at the protocol level?

Ans:

This is a fairly technical question but it's an important concept to understand. It's not natively a "security" question really, but it shows you whether or not they like to understand how things work, which is crucial for an Infosec professional. If they get it right you can lighten up and offer extra credit for the difference between Linux and Windows versions.
The key point people usually miss is that each packet that's sent out doesn't go to a different place. Many people think that it first sends a packet to the first hop, gets a time. Then it sends a packet to the second hop, gets a time, and keeps going until it gets done. That's incorrect. It actually keeps sending packets to the final destination; the only change is the TTL that's used. The extra credit is the fact that Windows uses ICMP by default while Linux uses UDP.

View All Answers

Question - 36:

List out various WEP cracking tools?

Ans:

Various tools used for WEP cracking are
* Aircrack
* WEPCrack
* Kismet
* WebDecrypt

View All Answers

Question - 37:

Tell me what does it mean for a machine to have an "air gap"? Why are air gapped machines important?

Ans:

An air gapped machine is simply one that cannot connect to any outside agents. From the highest level being the internet, to the lowest being an intranet or even bluetooth.

Air gapped machines are isolated from other computers, and are important for storing sensitive data or carrying out critical tasks that should be immune from outside interference. For example, a nuclear power plant should be operated from computers that are behind a full air gap. For the most part, real world air gapped computers are usually connected to some form of intranet in order to make data transfer and process execution easier. However, every connection increases the risk that outside actors will be able to penetrate the system.

View All Answers

Question - 38:

Tell us on a Windows network, why is it easier to break into a local account than an AD account?

Ans:

Windows local accounts have a great deal of baggage tied to them, running back a long long way to keep compatibility for user accounts. If you are a user of passwords longer than 13 characters, you may have seen the message referring to this fact. However, Active Directory accounts have a great deal of security tied onto them, not the least of which is that the system actually doing the authenticating is not the one you are usually sitting at when you are a regular user. Breaking into a Windows system if you have physical access is actually not that difficult at all, as there are quite a few dedicated utilities for just such a purpose, however that is beyond the scope of what we'll be getting into here.

View All Answers

Question - 39:

Do you know what's the difference between encoding, encryption, and hashing?

Ans:

Encoding is designed to protect the integrity of data as it crosses networks and systems, i.e. to keep its original message upon arriving, and it isn't primarily a security function. It is easily reversible because the system for encoding is almost necessarily and by definition in wide use. Encryption is designed purely for confidentiality and is reversible only if you have the appropriate key/keys. With hashing the operation is one-way (non-reversible), and the output is of a fixed length that is usually much smaller than the input.

View All Answers

Question - 40:

Suppose you manage to capture email packets from a sender that are encrypted through Pretty Good Privacy (PGP). What are the most viable options to circumvent this?

Ans:

First, one should be considering whether to even attempt circumventing the encryption directly. Decryption is nearly impossible here unless you already happen to have the private key. Without this, your computer will be spending multiple lifetimes trying to decrypt a 2048-bit key. It's likely far easier to simply compromise an end node (i.e. the sender or receiver). This could involve phishing, exploiting the sending host to try and uncover the private key, or compromising the receiver to be able to view the emails as plain text.

View All Answers

Question - 41:

Tell me you see a user logging in as root to perform basic functions. Is this a problem?

Ans:

A Linux admin account (root) has many powers that are not permitted for standard users. That being said, it is not always necessary to log all the way off and log back in as root in order to do these tasks. For example, if you have ever used the 'run as admin' command in Windows, then you will know the basic concept behind 'sudo' or 'superuser (root) do' for whatever it is you want it to do. It's a very simple and elegant method for reducing the amount of time you need to be logged in as a privileged user. The more time a user spends with enhanced permissions, the more likely it is that something is going to go wrong - whether accidentally or intentionally.

View All Answers

Question - 42:

Tell me how would you implement a secure login field on a high traffic website where performance is a consideration?

Ans:

We're looking for a basic understanding of the issue of wanting to serve the front page in HTTP, while needing to present the login form via HTTPs, and how they'd recommend doing that. A key piece of the answer should center around avoidance of the MiTM threat posed by pure HTTP. Blank stares here mean that they've never seen or heard of this problem, which means they're not likely to be anything near pro level.

View All Answers

Question - 43:

Suppose you had to both encrypt and compress data during transmission, which would you do first, and why?

Ans:

If they don't know the answer immediately it's ok. The key is how they react. Do they panic, or do they enjoy the challenge and think through it? I was asked this question during an interview at Cisco. I told the interviewer that I didn't know the answer but that I needed just a few seconds to figure it out. I thought out loud and within 10 seconds gave him my answer: "Compress then encrypt. If you encrypt first you'll have nothing but random data to work with, which will destroy any potential benefit from compression.

View All Answers

Question - 44:

Explain me what is WEP cracking? What are the types of WEP cracking?

Ans:

WEP cracking is the method of exploiting security vulnerabilities in wireless networks and gaining unauthorized access.

There are basically two types of cracks
* Active cracking: Until the WEP security has been cracked this type of cracking has no effect on the network traffic.
* Passive cracking: It is easy to detect compared to passive cracking. This type of attack has increased load effect on the network traffic.

View All Answers

Question - 45:

Explain me techniques used to prevent web server attacks?

Ans:

* Patch Management
* Secure installation and configuration of the O.S
* Safe installation and configuration of the web server software
* Scanning system vulnerability
* Anti-virus and firewalls
* Remote administration disabling
* Removing of unused and default account
* Changing of default ports and settings to customs port and settings

View All Answers

Question - 46:

Tell me what are personal traits you should consider protecting data?

Ans:

* Install anti-virus on your system
* Ensure that your operating system receives an automatic update
* By downloading latest security updates and cover vulnerabilities
* Share the password only to the staff to do their job
* Encrypt any personal data held electronically that would cause damage if it were stolen or lost
* On a regular interval take back-ups of the information on your computer and store them in a separate place
* Before disposing off old computers, remove or save all personal information to a secure drive
* Install anti-spyware tool

View All Answers

Question - 47:

Explain me what are web server vulnerabilities?

Ans:

The common weakness or vulnerabilities that the web server can take an advantage of are
* Default settings
* Misconfiguration
* Bugs in operating system and web servers

View All Answers

Question - 48:

Explain what is the difference between Encoding, Encryption and Hashing?

Ans:

At a very high level, all these 3 terms might appear to be similar and people often confuse between them. But each of the technique is distinct and has different use case. The purpose of encoding is to transform data so that it can be properly (and safely) consumed by a different type of system, e.g. binary data being sent over email, or viewing special characters on a web page. The goal is not to keep information secret, but rather to ensure that it's able to be properly consumed. It does not require a key as the only thing required to decode it is the algorithm that was used to encode it. Examples: ASCII, Unicode, URL Encoding, Base64. The purpose of encryption is to transform data in order to keep it secret from others. It uses a key, which is kept secret, in conjunction with the plaintext and the algorithm, in order to perform the encryption operation. Examples: AES, Blowfish, RSA. The purpose of hashing is to take arbitrary input and produce a fixed-length string that has the following attributes:
The same input will always produce the same output.
Multiple disparate inputs should not produce the same output.
It should not be possible to go from the output to the input.
Any modification of a given input should result in drastic change to the hash.
Examples- MD5, SHA1, SHA2 etc. Hashing is often used in computer forensics to verify integrity of the digital evidence.

View All Answers

Question - 49:

Suppose you find out that there is an active problem on your network. You can fix it, but it is out of your jurisdiction. What do you do?

Ans:

This question is a biggie. The true answer is that you contact the person in charge of that department via email - make sure to keep that for your records - along with CCing your manager as well. There may be a very important reason why a system is configured in a particular way, and locking it out could mean big trouble. Bringing up your concerns to the responsible party is the best way to let them know that you saw a potential problem, are letting them know about it, and covering yourself at the same time by having a timestamp on it.

View All Answers

Question - 50:

Tell me in public-key cryptography you have a public and a private key, and you often perform both encryption and signing functions. Which key is used for which function?

Ans:

You encrypt with the other person's public key, and you sign with your own private. If they confuse the two, don't put them in charge of your PKI project.

View All Answers

Question - 51:

Suppose you find PHP queries overtly in the URL, such as /index.php=?page=userID. What would you then be looking to test?

Ans:

This is an ideal situation for injection and querying. If we know that the server is using a database such as SQL with a PHP controller, it becomes quite easy. We would be looking to test how the server reacts to multiple different types of requests, and what it throws back, looking for anomalies and errors.
One example could be code injection. If the server is not using authentication and evaluating each user, one could simply try /index.php?arg=1;system('id') and see if the host returns unintended data.

View All Answers

Question - 52:

Tell me what is an easy way to configure a network to allow only a single computer to login on a particular jack?

Ans:

Sticky ports are one of the network admin's best friends and worst headaches. They allow you to set up your network so that each port on a switch only permits one (or a number that you specify) computer to connect on that port by locking it to a particular MAC address. If any other computer plugs into that port, the port shuts down and you receive a call that they can't connect anymore. If you were the one that originally ran all the network connections then this isn't a big issue, and likewise if it is a predictable pattern then it also isn't an issue. However if you're working in a hand-me-down network where chaos is the norm then you might end up spending a while toning out exactly what they are connecting to.

View All Answers

Question - 53:

Suppose if you were a site administrator looking for incoming CSRF attacks, what would you look for?

Ans:

This is a fun one, as it requires them to set some ground rules. Desired answers are things like, "Did we already implement nonces?", or, "That depends on whether we already have controls in place..." Undesired answers are things like checking referrer headers, or wild panic.

View All Answers

Question - 54:

Explain cryptographically speaking, what is the main method of building a shared secret over a public medium?

Ans:

Diffie-Hellman. And if they get that right you can follow-up with the next one.

View All Answers

Question - 55:

Tell me what are the advantages offered by bug bounty programs over normal testing practices?

Ans:

You should hear coverage of many testers vs. one, incentivization, focus on rare bugs, etc.

View All Answers

Question - 56:

Tell me for security analyst what are the useful certification?

Ans:

Useful certification for security analyst are
* Security Essentials (GSEC): It declares that candidate is expert in handling basic security issues- it is the basic certification in security
* Certified Security Leadership: It declares the certification of management abilities and the skills that is required to lead the security team
* Certified Forensic Analyst: It certifies the ability of an individual to conduct formal incident investigation and manage advanced incident handling scenarios including external and internal data breach intrusions
* Certified Firewall Analyst: It declares that the individual has proficiency in skills and abilities to design, monitor and configure routers, firewalls and perimeter defense systems

View All Answers

Question - 57:

List out the steps to successful data loss prevention controls and Explain?

Ans:

* Create an information risk profile
* Create an impact severity and response chart
* Based on severity and channel determine incident response
* Create an incident workflow diagram
* Assign roles and responsibilities to the technical administrator, incident analyst, auditor and forensic investigator
* Develop the technical framework
* Expand the coverage of DLP controls
* Append the DLP controls into the rest of the organization
* Monitor the results of risk reduction

View All Answers

Question - 58:

Tell me what is the difference between proxy, firewall, IDS and IPS?

Ans:

A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Firewall is basically meant for network traffic control/filtering mainly at layer-3. It allows/denies packets and connections based on certain pre-defined rules. IDS- Intrusion Detection System is an application which tries to detect intrusion attempts based on attack signature database it has. IPS- Intrusion Prevention System detects the intrusion (like IDS) and goes one step ahead to prevent it as well. It simply drops the packet it thinks suspicious (based on rules)
Examples:
* proxy - Squid
* Firewall- IPTables, CISCO Pix, ZoneAlarm
* IDS- SNORT
* IPS- IBM Proventia

View All Answers

Question - 59:

Do you know how can an institute or a company can safeguard himself from SQL injection?

Ans:

An organization can rely on following methods to guard themselves against SQL injection
* Sanitize user input: User input should be never trusted it must be sanitized before it is used
* Stored procedures: These can encapsulate the SQL statements and treat all input as parameters
* Regular expressions: Detecting and dumping harmful code before executing SQL statements
* Database connection user access rights: Only necessary and limited access right should be given to accounts used to connect to the database
* Error messages: Error message should not be specific telling where exactly the error occurred it should be more generalized.

View All Answers

Question - 60:

Tell me what is phishing? How it can be prevented?

Ans:

Phishing is a technique that deceit people to obtain data from users. The social engineer tries to impersonate genuine website webpage like yahoo or face-book and will ask the user to enter their password and account ID.
It can be prevented by:
* Having a guard against spam
* Communicating personal information through secure websites only
* Download files or attachments in emails from unknown senders
* Never e-mail financial information
* Beware of links in e-mails that ask for personal information
* Ignore entering personal information in a pop-up screen

View All Answers

Question - 61:

Explain what is data leakage? What are the factors that can cause data leakage?

Ans:

The separation or departing of IP from its intended place of storage is known as data leakage. The factors that are responsible for data leakage can be
* Copy of the IP to a less secure system or their personal computer
* Human error
* Technology mishaps
* System misconfiguration
* A system breach from a hacker
* A home-grown application developed to interface to the public
* Inadequate security control for shared documents or drives
* Corrupt hard-drive
* Back up are stored in an insecure place

View All Answers

Question - 62:

Explain how do you keep yourself updated with latest trends in Information Security?

Ans:

I refer to various security news sites , blogs etc. Also I am subscribed to various online security magazines like Pentest magazine, HackInsight etc and I surf through the archives of various security conferences held worldwide.

View All Answers

Question - 63:

Suppose you find yourself in an airport in the depths of of a foreign superpower. You're out of mobile broadband and don't trust the WI-FI. What do you do? Further, what are the potential threats from open WI-FIs?

Ans:

Ideally you want all of your data to pass through an encrypted connection. This would usually entail tunneling via SSH into whatever outside service you need, over a virtual private network (VPN). Otherwise, you're vulnerable to all manner of attacks, from man-in-the-middle, to captive portals exploitation, and so on.

View All Answers

Question - 64:

Suppose you are remoted in to a headless system in a remote area. You have no physical access to the hardware and you need to perform an OS installation. What do you do?

Ans:

There are a couple of different ways to do this, but the most like scenario you will run into is this: What you would want to do is setup a network-based installer capable of network-booting via PXE (if you've ever seen this during your system boot and wondering what it was for, tada). Environments that have very large numbers of systems more often than not have the capability of pushing out images via the network. This reduces the amount of hands-on time that is required on each system, and keeps the installs more consistent.

View All Answers

Question - 65:

Do you know what are salted hashes?

Ans:

Salt at its most fundamental level is random data. When a properly protected password system receives a new password, it will create a hashed value for that password, create a new random salt value, and then store that combined value in its database. This helps defend against dictionary attacks and known hash attacks. For example, if a user uses the same password on two different systems, if they used the same hashing algorithm, they could end up with the same hash value. However, if even one of the systems uses salt with its hashes, the values will be different.

View All Answers

Question - 66:

Explain how would traceroute help you find out where a breakdown in communication is?

Ans:

Tracert or traceroute, depending on the operating system, allows you to see exactly what routers you touch as you move along the chain of connections to your final destination. However, if you end up with a problem where you can't connect or can't ping your final destination, a tracert can help in that regard as you can tell exactly where the chain of connections stop. With this information, you can contact the correct people - whether it be your own firewall, your ISP, your destination's ISP or somewhere in the middle.

View All Answers

Question - 67:

Tell me what are the common defenses against XSS?

Ans:

Input Validation/Output Sanitization, with focus on the latter.

View All Answers

Question - 68:

Explain the last program or script that you wrote. What problem did it solve?

Ans:

All we want to see here is if the color drains from the guy's face. If he panics then we not only know he's not a programmer (not necessarily bad), but that he's afraid of programming (bad). I know it's controversial, but I think that any high-level security guy needs some programming skills. They don't need to be a God at it, but they need to understand the concepts and at least be able to muddle through some scripting when required.

View All Answers

Question - 69:

Explain who's more dangerous to an organization, insiders or outsiders?

Ans:

Ideally you'll hear inquiry into what's meant by "dangerous". Does that mean more likely to attack you, or more dangerous when they do?

View All Answers

Question - 70:

Tell me who do you look up to within the field of Information Security? Why?

Ans:

A standard question type. All we're looking for here is to see if they pay attention to the industry leaders, and to possibly glean some more insight into how they approach security. If they name a bunch of hackers/criminals that'll tell you one thing, and if they name a few of the pioneers that'll say another. If they don't know anyone in Security, we'll consider closely what position you're hiring them for. Hopefully it isn't a junior position.

View All Answers

Question - 71:

What is certified Forensic Analyst?

Ans:

It certifies the ability of an individual to conduct formal incident investigation and manage advanced incident handling scenarios including external and internal data

breach intrusions

View All Answers

Question - 72:

Tell me how would you lock down a mobile device?

Ans:

Another opinion question, and as usual a lot of different potential answers. The baseline for these though would be three key elements: An anti-malware application, a remote wipe utility, and full-disk encryption. Almost all modern mobile devices regardless of manufacturer have anti-malware and remote wipe available for them, and very few systems now do not come with full-disk encryption available as an option directly within the OS.

View All Answers

Question - 73:

Tell me what makes a script fully undetectable (FUD) to antivirus software? How would you go about writing a FUD script?

Ans:

A script is FUD to an antivirus when it can infect a target machine and operate without being noticed on that machine by that AV. This usually entails a script that is simple, small, and precise
To know how to write a FUD script, one must understand what the targeted antivirus is actually looking for. If the script contains events such as Hook_Keyboard(), File_Delete(), or File_Copy(), it's very likely it wil be picked up by antivirus scanners, so these events are not used. Further, FUD scripts will often mask function names with common names used in the industry, rather than naming them things like fToPwn1337(). A talented attacker might even break up his or her files into smaller chunks, and then hex edit each individual file, thereby making it even more unlikely to be detected.
As antivirus software becomes more and more sophisticated, attackers become more sophisticated in response. Antivirus software such as McAfee is much harder to fool now than it was 10 years ago. However, there are talented hackers everywhere who are more than capable of writing fully undetectable scripts, and who will continue to do so. Virus protection is very much a cat and mouse game.

View All Answers

Question - 74:

Tell me what is the difference between Information Protection and Information Assurance?

Ans:

Information Protection is just what it sounds like- protecting information through the use of Encryption, Security software and other methods designed to keep it safe. Information Assurance on the other hand deals more with keeping the data reliable - RAID configurations, backups, non-repudiation techniques, etc.

View All Answers

Question - 75:

Explain me how do you protect your home Wireless Access Point?

Ans:

This is another opinion question - there are a lot of different ways to protect a Wireless Access Point: using WPA2, not broadcasting the SSID, and using MAC address filtering are the most popular among them. There are many other options, but in a typical home environment, those three are the biggest.
By now you've seen more than a fair amount of troubles. You've got a toolkit of regularly used programs, a standard suite of protection utilities, you're comfortable with cleanups and you've spent quite a bit of time discovering that there are a lot of ways to make things go boom. You've also seen that it doesn't take much to have data disappear forever, and that you need help to protect and manage it. By this stage you are more than likely a member of a team rather than a lone figure trying to work out everything, and as a result you are now on the specialization track. You may or may not however have a pointed hat and a predisposition to rum.

View All Answers

Question - 76:

Tell us you need to reset a password-protected BIOS configuration. What do you do?

Ans:

While BIOS itself has been superseded by UEFI, most systems still follow the same configuration for how they keep the settings in storage. Since BIOS itself is a pre-boot system, it has its own storage mechanism for its settings and preferences. In the classic scenario, simply popping out the CMOS (complementary metal-oxide-semiconductor) battery will be enough to have the memory storing these settings lose its power supply, and as a result it will lose its settings. Other times, you need to use a jumper or a physical switch on the motherboard. Still other times you need to actually remove the memory itself from the device and reprogram it in order to wipe it out. The simplest way by far however is this: if the BIOS has come from the factory with a default password enabled, try 'password'.

View All Answers

Question - 77:

Tell me what personal achievement are you most proud of?

Ans:

For me at least, this one is easy- getting my CISSP. I studied for months, did every possible thing I could to improve my recall and asked for anybody and everybody to help ask questions and modify them in ways to make me try to think around corners. Everybody has at least one thing that they are proud of, and while this and the next question may be the same answer, all that matters is showing that you are willing to move forward and willing to be self-motivated.

View All Answers

Question - 78:

Tell me what are the various ways to handle account brute forcing?

Ans:

Look for discussion of account lockouts, IP restrictions, fail2ban, etc.

View All Answers

Question - 79:

Tell me why is DNS monitoring important?

Ans:

If they're familiar with infosec shops of any size, they'll know that DNS requests are a treasure when it comes to malware indicators.

View All Answers

Question - 80:

Tell us can you describe rainbow tables?

Ans:

Look for a thorough answer regarding overall password attacks and how rainbow tables make them faster.

View All Answers

Question - 81:

What is certified Security Leadership?

Ans:

It declares the certification of management abilities and the skills that is required to lead the security team

View All Answers

Question - 82:

Tell me what is the role of information security analyst?

Ans:

From small to large companies role of information security analyst includes:
* Implementing security measures to protect computer systems, data and networks
* Keep himself up-to-date with on the latest intelligence which includes hackers techniques as well
* Preventing data loss and service interruptions
* Testing of data processing system and performing risk assessments
* Installing various security software like firewalls, data encryption and other security measures
* Recommending security enhancements and purchases
* Planning, testing and implementing network disaster plans
* Staff training on information and network security procedures

View All Answers

Question - 83:

Do you know what is residual risk?

Ans:

I'm going to let Ed Norton answer this one: "A new car built by my company leaves somewhere traveling at 60 mph. The rear differential locks up. The car crashes and burns with everyone trapped inside. Now, should we initiate a recall? Take the number of vehicles in the field, A, multiply by the probable rate of failure, B, multiply by the average out-of-court settlement, C. A times B times C equals X. If X is less than the cost of a recall, we don't do one." Residual Risk is what is left over after you perform everything that is cost-effective to increase security, but to go further than that is a waste of resources. Residual risk is what the company is willing to live with as a gamble in the hopes that it won't happen.

View All Answers

Question - 84:

Tell me is there any difference between Information Security and IT Security? If yes, please explain the difference?

Ans:

Yes. Information Security and IT Security are both different terms often used interchangeably. IT Security focuses on purely technical controls (like implementing antivirus, firewall, hardening systems etc) while Information Security is more wider term which implies securing "information" as an asset be it in any form. (ex shredding of paper documents to prevent dumpster driving etc). So IT security can be considered as a subset of Information Security.

View All Answers

Question - 85:

Do you know what is social engineering?

Ans:

"Social engineering" refers to the use of humans as an attack vector to compromise a system. It involves fooling or otherwise manipulating human personnel into revealing information or performing actions on the attacker's behalf. Social engineering is known to be a very effective attack strategy, since even the strongest security system can be compromised by a single poor decision. In some cases, highly secure systems that cannot be penetrated by computer or cryptographic means, can be compromised by simply calling a member of the target organization on the phone and impersonating a colleague or IT professional.

View All Answers

Question - 86:

Do you know what is the CIA triangle?

Ans:

Confidentiality, Integrity, Availability. As close to a 'code' for Information Security as it is possible to get, it is the boiled down essence of InfoSec. Confidentiality- keeping data secure. Integrity- keeping data intact. Availability- keeping data accessible.

View All Answers

Question - 87:

Tell me what is data protection in transit vs data protection at rest?

Ans:

When data is protected while it is just sitting there in its database or on its hard drive- it can be considered at rest. On the other hand, while it is going from server to client it is in-transit. Many servers do one or the other- protected SQL databases, VPN connections, etc, however there are not many that do both primarily because of the extra drain on resources. It is still a good practice to do both however, even if it does take a bit longer.

View All Answers

Question - 88:

Do you know what is XSS?

Ans:

Cross-site scripting, the nightmare of Javascript. Because Javascript can run pages locally on the client system as opposed to running everything on the server side, this can cause headaches for a programmer if variables can be changed directly on the client's webpage. There are a number of ways to protect against this, the easiest of which is input validation.

View All Answers

Question - 89:

Explain what is the primary reason most companies haven't fixed their vulnerabilities?

Ans:

This is a bit of a pet question for me, and I look for people to realize that companies don't actually care as much about security as they claim to-otherwise we'd have a very good remediation percentage. Instead we have a ton of unfixed things and more tests being performed.
Look for people who get this, and are ok with the challenge.

View All Answers

Question - 90:

Do you know what's the difference between HTTP and HTML?

Ans:

Obviously the answer is that one is the networking/application protocol and the other is the markup language, but again, the main thing you're looking for is for him not to panic.

View All Answers

Question - 91:

Tell me what port does ping work over?

Ans:

A trick question, to be sure, but an important one. If he starts throwing out port numbers you may want to immediately move to the next candidate. Hint: ICMP is a layer 3 protocol (it doesn't work over a port) A good variation of this question is to ask whether ping uses TCP or UDP. An answer of either is a fail, as those are layer 4 protocols.

View All Answers

Question - 92:

Tell me what's the difference between symmetric and public-key cryptography?

Ans:

Standard stuff here: single key vs. two keys, etc, etc.

View All Answers

Question - 93:

Explain me what's more secure, SSL or HTTPS?

Ans:

Trick question: these are not mutually exclusive. Look for a smile like they caught you in the cookie jar. If they're confused, then this should be for an extremely junior position.

View All Answers

Question - 94:

What is security Essentials (GSEC)?

Ans:

It declares that candidate is expert in handling basic security issues- it is the basic certification in security

View All Answers

Question - 95:

Do you know what is the 80/20 rule of networking?

Ans:

80/20 is a thumb rule used for describing IP networks, in which 80% of all traffic should remain local while 20% is routed towards a remote network.

View All Answers

Security Most Popular & Related Interview Guides

1 : **Safety Officer Interview Questions and Answers.**

2 : Security Guard Interview Questions and Answers.

3 : Sheriff Interview Questions and Answers.

4 : Protocols Officer Interview Questions and Answers.

5 : Military Analyst Interview Questions and Answers.

6 : Central Intelligence Agency Interview Questions and Answers.

7 : Bank Guard Interview Questions and Answers.

8 : Aviation Security Interview Questions and Answers.

9 : Airport Security Officer Interview Questions and Answers.

10 : Secret Service Agent Interview Questions and Answers.

Follow us on FaceBook
www.facebook.com/InterviewQuestionsAnswers.Org

Follow us on Twitter
https://twitter.com/InterviewQA

For any inquiry please do not hesitate to contact us.

Interview Questions Answers.ORG Team
https://InterviewQuestionsAnswers.ORG/
support@InterviewQuestionsAnswers.ORG