INFOSEC INSTITUTE

Top 50 information security interview questions

By Kurt Ellzey

January 2021

Let's face it, there's no shortage in potential questions at any given interview across a wide variety of topics in information security. On top of that, InfoSec means a lot of different things to a lot of different people. For example, information security covers everyone from the guy at Best Buy running a copy of Norton all the way up to the cryptomasters at the NSA. As a result, a single list of questions is not going to cover everything. That being said, there are tiers of possible questions that you can run into, and that is what this guide is about.

That's not to say that these questions cannot appear in different tiers — you may very well see some of the level 1 questions during a level 5 interview. Rather, this means that in order to reach level 5, you want to be comfortable with everything up to that point — not necessarily remember everything by rote, but at least be able to have a resource you can get the answers from quickly. So without further ado, let's begin.

Level 1 interview questions: The tech

Entry-level positions are almost always about the skills — what you know right now, and what you're willing to do to improve upon those skills. By the same token, a lot of these questions can help to understand more about what makes you, you — your personality and your existing preferences and opinions. At this stage you are still very much a technician or a security guy, but you've reached the point where you want to specialize, and for that you need to start learning more about what makes what you're trying to protect tick. At this stage, you care more about getting the thing to work than security, but you also know that you want to keep people in general from doing naughty things. Sadly, you probably do not know kung-fu.

1. What are your daily news checks?

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.

2. What do you have on your home network?

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.

3. What personal achievement are you most proud of?

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.

4. What project that you have built are you most proud of?

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 was 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.

5. How would traceroute help you find out where a breakdown in communication is?

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.

6. Why would you want to use SSH from a Windows PC?

SSH (TCP port 22) is a secure connection used on many different systems and dedicated appliances. Routers, switches, SFTP servers and unsecure programs being tunneled 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.

7. What's the difference between symmetric and asymmetric encryption?

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 create the symmetric connection. This leads us into the next topic …

8. What is SSL and why is it not enough when it comes to encryption?

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.

9. How would you find out what a POST code means?

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.

10. What is the difference between a black hat and a white hat?

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. The one I've heard the most is the classic Jedi example —

same tools, different ideologies. Personally, 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.

Level 2 interview questions: The breaker/fixer

Secondary positions usually require a bit more experience — a bit more legwork, a bit more time to think outside the box and discover things that make you go, “Huh. That’s funny.” You’ve had situations where you’ve had to break into different systems and wonder if you did the right thing and know that you could get into quite a bit of trouble if you did the same thing to say the accountant’s PC on the 4th floor. You’ve seen a few breakouts and know enough not to panic when you see a virus alert. Finally, when you are performing a cleanup on a box you know you want to gather information about how it got on there as well as save as much data as possible before either removing the offending infection or nuking the box. Not full blown digital forensics necessarily, but knowing the basics of the art will help you a great deal. Maxim #1: “Pillage, THEN burn.”

11. You need to reset a password-protected BIOS configuration. What do you do?

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”.

12. What is XSS?

Cross-site scripting is 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.

13. How would you login to Active Directory from a Linux or Mac box?

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.

14. What are salted hashes?

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.

15. What do you think of social networking sites such as Facebook and LinkedIn?

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 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.

16. What are the three ways to authenticate a person?

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

17. How would you judge if a remote server is running IIS or Apache?

Error messages oftentimes give away 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.

18. What is data protection in transit vs data protection at rest?

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. Even if it does take a bit longer.

19. You see a user logging in as root to perform basic functions. Is this a problem?

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.

20. How do you protect your home wireless access point?

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.

Level 3 interview questions: The savvy

By now you’ve seen more than a fair amount of troubles. You’ve got a toolkit of regularly used programs and a standard suite of protection utilities. You’re comfortable with cleanups, and you’ve spent quite a bit of time discovering 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.

21. What is an easy way to configure a network to allow only a single computer to login on a particular jack?

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.

22. 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?

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.

23. On a Windows network, why is it easier to break into a local account than an AD account?

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.

24. What is the CIA triangle?

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 is keeping data secure. Integrity is keeping data intact. Availability is keeping data accessible.

25. What is the difference between an HIDS and a NIDS?

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 the same as an antivirus program, for instance, while a NIDS 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 antivirus 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.

26. 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?

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. 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.

27. You are an employee for a tech department in a non-management position. A high-level executive demands that you break protocol and allow him to use his home laptop at work. What do you do?

You would be amazed how often this happens, even more so in the current BYOD environment. Still, the easiest way out of this one is to contact your manager again and have them give a yay or nay. This puts the authority and decision where it needs to be and gives you assistance if the department needs to push back. Stress can be a real killer in position where you have to say “no” to people that don’t like hearing it, so passing the buck can be a friend.

28. What is the difference between a vulnerability and an exploit?

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.

29. How would you compromise an “office workstation” at a hotel?

Considering how infected these typically are, I wouldn’t touch one with a ten-foot pole. That being said, a USB keylogger is easy to fit into the back of these systems without much notice. An autorun program would be able to run quickly and quietly leaving behind software to do the dirty work. In essence, it’s open season on exploits in this type of environment.

Level 4 interview questions: The keymaster

At this stage, if you have physical access to the box, you own it. You also have enough ethics to not break into every single thing you touch, and here is where personal ethics start to become a tremendous asset — provided you know where to draw the line. You’ve seen a lot of the dirty side of InfoSec, know that it can be used for good and bad just as much as anything else, and you very likely have done some things on both sides of the fence. By the same token, you know the truth of the saying, “It takes a thief to catch a thief,” and so you have gone through penetration testing events and may be a part of a regular team performing exercises against your network and its sites. Unfortunately, Gozer will not be stopping by for s’mores. Sorry about that.

31. What is worse in firewall detection, a false negative or a false positive? And why?

Far and away is a false negative. A false positive is annoying, but easily dealt with — calling a legitimate piece of traffic bad. A false negative is a piece of malicious traffic being let through without incident — definitely bad.

32. What's better, a red team or a blue team?

Another opinion question, more along the lines of where your interests lie. In penetration testing scenarios, a red team is trying to break in while a blue team is defending. Red teams typically are considered the "cooler" of the two, while the blue team is usually the more difficult. The usual rules apply like in any defense game: the blue team has to be good every time, while the red team only has to be good once. That's not entirely accurate given the complexities at work in most scenarios, but it's close enough to explain the idea.

33. What's the difference between a white box test and a black box test?

The difference is information given by the person commissioning the test. A white box test is one where the pentesting team is given as much information as possible regarding the environment, while a black box test is … well … a black box. They don't know what's inside.

34. What is the difference between information protection and information assurance?

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.

35. How would you lock down a mobile device?

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.

36. What is the difference between closed-source and open-source? Which is better?

Yet another opinion question. Closed-source is a typical commercially developed program. You receive an executable file which runs and does its job without the ability to look far under the hood. Open-source, however, provides the source code to be able to inspect everything it does, as well as be able to make changes yourself and recompile the code. Both have arguments for and against them, most have to do with audits and accountability. Closed-source advocates claim that open-source causes

issues because everybody can see exactly how it works and exploit weaknesses in the program. Open-source counter saying that because closed-source programs don't provide ways to fully check them out, its difficult to find and troubleshoot issues in the programs beyond a certain level.

37. What is your opinion on hacktivist groups such as Anonymous?

You might have guessed that this level is very much about forming opinions and drawing conclusions, and you'd be right. This one is an especially loaded question. Like any major group without a central leader, they seem to be mostly chaotic, at times seeming like a force for good, while at others causing havoc for innocents. Choose your words very carefully here, as it could be a deal breaker.

38. What is the three-way handshake? How can it be used to create a DOS attack?

The three-way handshake is a cornerstone of the TCP suite: SYN, SYN/ACK, ACK. SYN is the outgoing connection request from client to server. SYN/ACK is the acknowledgement of the server back to the client, saying that yes I hear you, let's open a connection. ACK is the final connection, and allows the two to speak. The problem is that this can be used as a very basic type of denial-of-service attack. The client opens up the SYN connection, the server responds with the SYN/ACK, but then the client sends another SYN. The server treats this as a new connection request and keeps the previous connection open. As this is repeated over and over many times very quickly, the server quickly becomes saturated with a huge number of connection requests, eventually overloading its ability to connect to legitimate users.

39. Why would you bring in an outside contractor to perform a penetration test?

Much like getting a fresh set of eyes on a problem, sometimes you have people that don't want to see or don't want to admit to an issue. Bringing in extra help as an audit can really help eliminate problems your team isn't able to resolve on their own. Granted they may cost a small fortune, but they are extremely good at what they do.

40. If you were going to break into a database-based website, how would you do it?

And here's other side of the coin: learning to break into your own systems so that you can pentest them yourself. While the exact methods are different for each type of database server and programming language, the easiest attack vector to test for first is an SQL injection technique. For example, if the input fields are not sterilized, just entering a specific set of symbols into a form field may be enough to get back data. Alternatively, depending again on how the site is written, using a specially crafted URL may be enough to get back data as well. Footprinting the server ahead of time can help in this task if it isn't one you built yourself.

Level 5 interview questions: The mastermind

By this stage, you are likely in charge of your own department and have a chosen team to work with you. You spend more of your time working on policy changes and directing where your people will be 12-36 months down the road than you do writing code, but you've more than made up for it in legal-jitsu. Protecting the organization at its highest levels is now your job, and the buck stops with you for better or worse. As a result, you need to be on your game all the time and have as much of an edge as possible over outsiders and disgruntled employees wanting to make a statement.

41. Why are internal threats oftentimes more successful than external threats?

When you see something day in and day out, even if it shocks you at first, you tend to get used to it. This means that if you see somebody that pokes around day after day, month after month, you might get used to the fact that he's just curious. You let your guard down, and don't react as quickly to possible threats. On the other hand, say you have an annoyed employee that is soon to be fired and wants to show his soon to be former employer that he can bring them down. So he sells his still active credentials and key card to a local group that specializes in white-collar crime. Still other infiltrators dress up as delivery people and wander around aimlessly in office buildings, getting information off of post-it notes and papers lying around. External threats do not have access to near this level of information about the company, and more often than not do not get in as far as somebody that spent 20 bucks on a knock-off UPS uniform.

42. What is residual risk?

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.

43. Why is deleted data not truly gone when you delete it?

When you press delete on a file, it doesn't actually go anywhere. A bit on the file is flipped telling the operating system that that file is no longer needed and it can be overwritten as is required. Until that happens, the file can still be restored no matter if it's in a Recycling Bin or not. There are ways around this, such as using file shredders and disk wipers, but both of these take quite a bit of time to finish their jobs to a reasonable degree.

44. What is the chain of custody?

When keeping track of data or equipment for use in legal proceedings, it needs to remain in a pristine state. Therefore, documenting exactly who has had access to what

for how long is vital when dealing with this situation. Any compromise in the data can lead to legal issues for the parties involved and can lead to a mistrial or contempt depending on the scenario.

45. How would you permanently remove the threat of data falling into the wrong hands?

If data is on physical media such as a diskette, CD or even paper, there are shredders, pulverizers and destroyers that can turn plastic and paper into confetti. For hard disks however, that becomes a bit more tricky. Most locations will turn to a two-fold method for ensuring a disk's destruction. First, they'll use a specially made disc-wiping program and take apart the hard drive, remove the platters and scratch them up beyond recognition. Then they'll degauss them with a high-powered magnet. This ensures that the data cannot be recovered through conventional means.

46. What is exfiltration?

Infiltration is the method by which you enter or smuggle elements into a location. Exfiltration is just the opposite: getting sensitive information or objects out of a location without being discovered. In an environment with high security, this can be extremely difficult but not impossible. Again we turn to our friends in the fake delivery uniforms wandering around the building, and see that, yes, there are ways to get in and out without a lot of issues.

47. I run an SMB. I have four people in my entire company and a web-based store. I don't have the time, patience or manpower to have a computer guy. Why should I care about exploits and computer jibberish?

This is a classic catch-22 situation: a company doesn't have enough money to secure their networks, but by the same token they can't afford a payout if they get compromised. At the same time, they really can't afford to have a dedicated computer technician, let alone a security consultant. If you are able to explain (in words that don't make it sound like you're just fearmongering), an SMB will acknowledge what they need to do to keep their store secure and keep receiving payments, since following the money will tend to help move things along.

48. I'm the CEO of a Fortune 500 company. I make more in an afternoon than you make in a year. I don't care about this stupid security stuff. It just costs time and money and slows everything down. Why should I care about this junk?

This one is significantly harder — they are used to having people lie, cheat and steal from them on a regular basis, and when somebody comes in saying that the company is going to lose all this money unless you pay for this, they're probably going to say no. Therefore, having done your homework and having the support of the local IT team instead of alienating them is vital. Performing site assessments, creating executive summaries and line-by-line breakdowns of what goes where can help them to better understand what is going to be done and keep the project going.

49. I'm the legal council for a large corporation. We have requirements to document assets and code changes. We have a very limited budget for this task. How would you resolve this?

This is actually one of the easier ones. You have an informed party, asking for assistance to something that is important. They have money for the project (albeit not much), but it is better than nothing. At the very bottom of the spectrum, this could be accomplished in nothing more than Excel with a lot of time and data entry, moving all the way up the chain to automated network scanners documenting everything they find to a database and programs that check-in and out programs with versioning and delta files. It all depends on how big the project is, and how big the company is.

50. I'm the new guy. I used to be a coder at my old job and my manager wants me to create some custom programs. I need domain administrator rights for this task. My boss said it's alright, and you either give me what I need or you're fired and I'll find somebody that will. How do you respond?

Unfortunately, you will run into the hardball guy at least once in your career. In this case though, like others we have run into, it's time to move it up the chain to the manager. They will be able to give the yay or nay depending on exactly what the project is and be able to take the brunt of an attack if it comes.

Interested in more interview questions? Check out the following articles:

Top 10 ethical hacking interview questions

Top 25 security+ interview questions

Top 10 CISSP interview questions