iNeuron

Cyber Security Interview Questions

Here will taking some questions for tech savvy guys, who are little interested with new stuff to do everyday while learning Cyber security and Administrator area.

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

   Answer: 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.

2. ***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?***

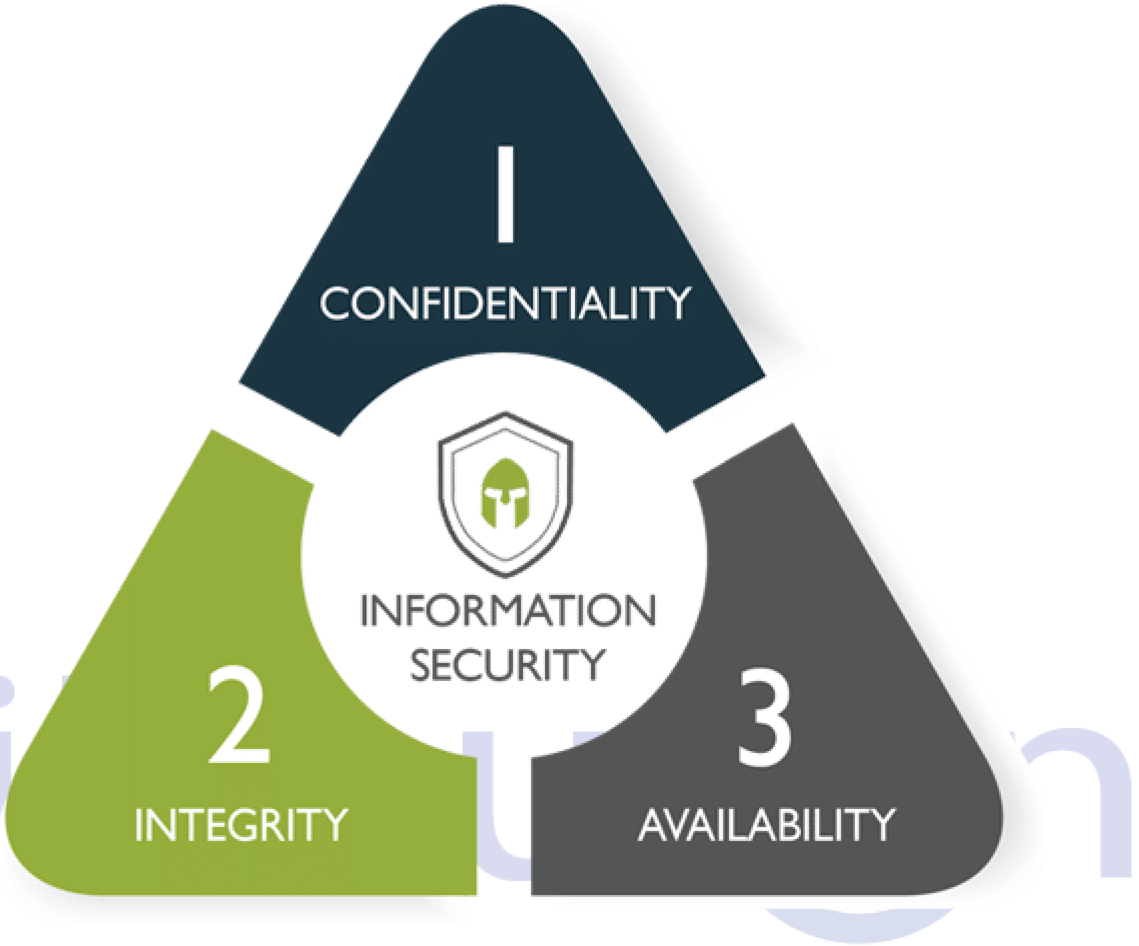
Answer: There are a couple of different ways to do this, but the most like scenario you will run into is this: What you would want to do is setup a network-based installer capable of network-booting via PXE (if you've ever seen this during your system boot and wondering what it was for, tada). Environments 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.

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

Answer: Windows local accounts have a great deal of baggage tied to them, running back a 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.

4. ***What is the CIA triangle?***

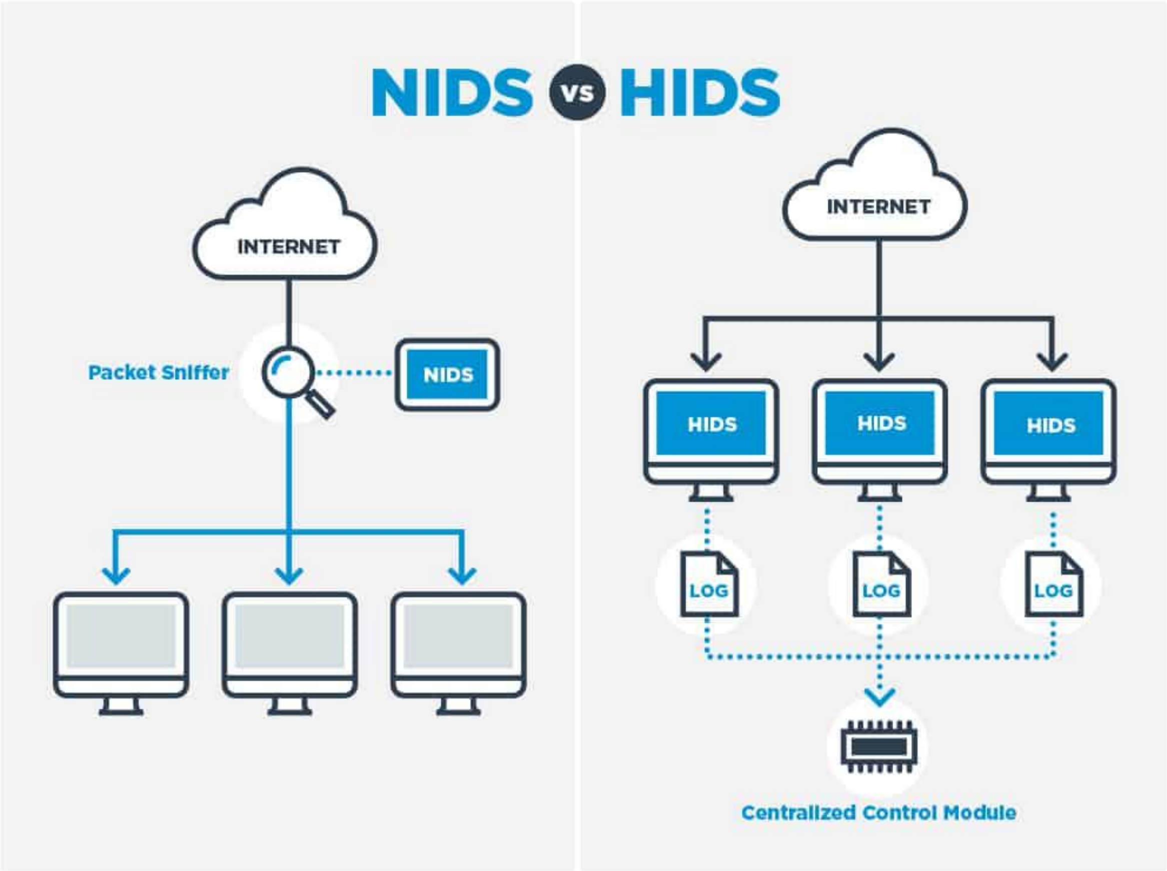
Answer: Confidentiality, integrity, availability. As close to a "code" for information security as it is possible to get, it is the boiled down essence of InfoSec. Confidentiality is keeping data secure. Integrity is keeping data intact. Availability is keeping data accessible.



More Info: https://comtact.co.uk/what-is-the-cia-triad/

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

Answer: 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.



More Info: https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

6. ***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?***

Answer: 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 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.

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

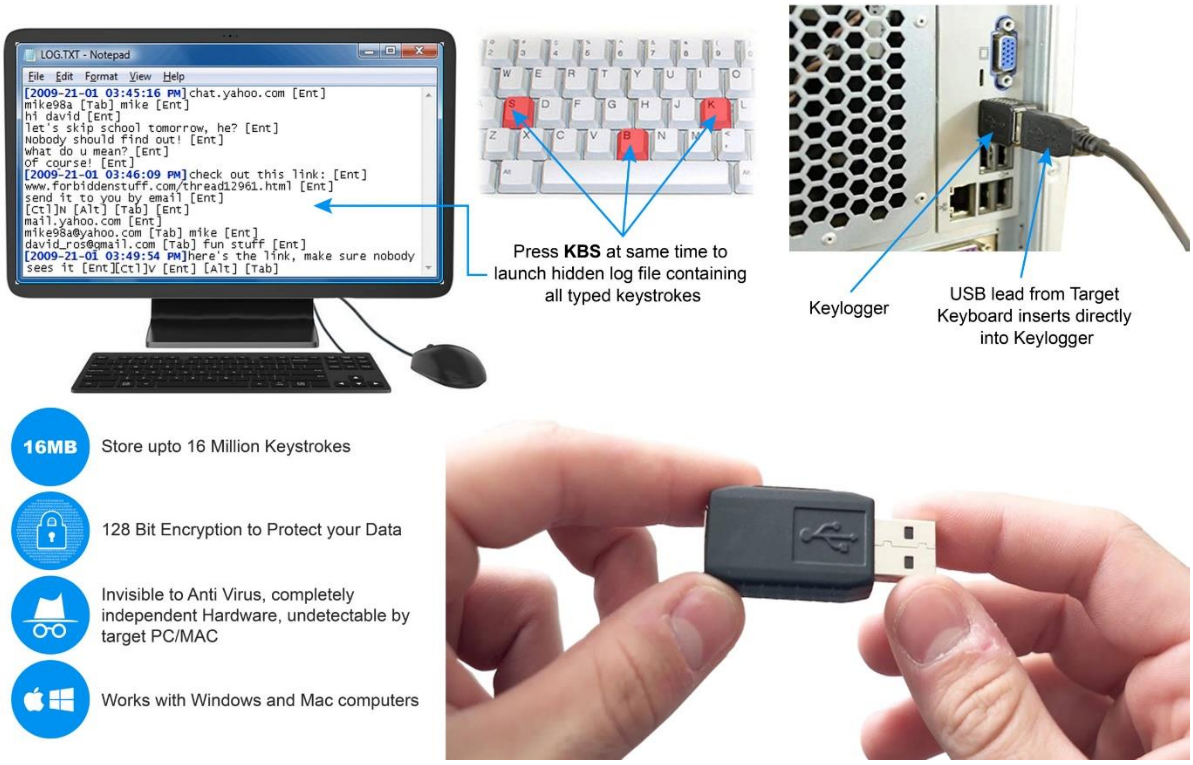
Answer: You would be amazed how often this happens, even more so in the current BYOD environment. Still, the easiest way out of this one is to contact your manager again and have them give a yay or nay. This puts the authority and decision where it needs to be and gives your assistance if the department 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.

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

Answer: 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.

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

Answer: 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.



```
[2009-21-01 03:45:16 PM]chat.yahoo.com [Ent]
mike98a [Tab] mike [Ent]
hi david [Ent]
let's skip school tomorrow, he? [Ent]
Nobody should find out! [Ent]
what do u mean? [Ent]
of course! [Ent]
[2009-21-01 03:46:09 PM]check out this link: [Ent]
www.forbiddenstuff.com/thread12961.html [Ent]
send it to you by email [Ent]
[Ctl]N [Alt] [Tab] [Ent]
mail.yahoo.com [Ent]
mike98a@yahoo.com [Tab] mike [Ent]
david_ros@gmail.com [Tab] fun stuff [Ent]
[2009-21-01 03:49:54 PM]here's the link, make sure nobody
 sees it [Ent][Ctl]V [Ent] [Alt] [Tab]
```

LOG.TXT - Notepad
File Edit Format View Help
Press KBS at same time to launch hidden log file containing all typed keystrokes
Keylogger
USB lead from Target Keyboard inserts directly into Keylogger
16MB
Store upto 16 Million Keystrokes
128 Bit Encryption to Protect your Data
Invisible to Anti Virus, completely independent Hardware, undetectable by target PC/MAC
Works with Windows and Mac computers

More Info: https://paraben-sticks.com/index.php/product/usb-keylogger-16mb/

iNeuron

Stay tune to out next set of Interview Questions

Credit: Internet and social media collected Questions

Follow us:

https://www.linkedin.com/company/ineuron-ai/

https://www.linkedin.com/in/mukeshkumarrao/

😍