Database Final Exam

Gurveer Sandhu

Q1: What is normalization?

A2: Normalization is a database design technique that reduces data redundancy and eliminates undesirable characteristics like Insertion, Update and Deletion Anomalies. The purpose of Normalization in SQL is to eliminate repetitive data and ensure data is stored logically.

Q2: What is 1NF? Explain with examples.

A2: A database is in first normal form if it satisfies the following conditions:

- Contains only atomic values
- There are no repeating groups
- An atomic value is a value that cannot be divided.

Q3: What is 3NF? Explain with examples.

A3: A relation is in third normal form if it is in 2NF and no non key attribute is transitively dependent on the primary key.

Q4: What is BCNF? Explain with examples.

A4: Boyce–Codd normal form (or BCNF or 3.5NF) is a normal form used in database normalization. It is a slightly stronger version of the third normal form. If a relational schema is in BCNF then all redundancy based on functional dependency has been removed, although other types of redundancy may still exist.

Q5: What is Operating system? Give examples?

A5: An operating system is system software that manages computer hardware, software resources, and provides common services for computer programs. Without an operating system, every application would need to include its own UI, as well as the comprehensive code needed to handle all low-level functionality of the underlying computer, such as disk storage, network interfaces and so on.

Examples:

- MacOs
- Windows
- Linux
- Unix

Q6: What is Linux operating system? Why it is considered as better alternative than windows?

A6: Linux is the best-known and most-used open source operating system Unix-like operating systems based on the Linux kernel,[10] an operating system kernel first released on September 17, 1991, by Linus Torvalds.

Q7: What is trojen horse?

A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system.

Q8: What is MD5 hash and exlpain its significance using a practcal example?

A: MD5 is a widely used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files

Q9: What is dark web?

A: The dark web is the World Wide Web content that exists on darknets: overlay networks that use the Internet but require specific software, configurations, or authorization to access. The dark web is a part of the internet that isn't indexed by search engines.

Q10: How can be we access dark web?

Getting to the dark web is actually a lot easier than you might think. All you have to do is download a dark web browser, like the Tor browser. Once you install a dark web browser on your device, it functions just like a regular browser: type in a URL, and off you go.

However, finding the material you're looking for on the dark web is more difficult than using a search engine like Google. The dark web doesn't have an index or ranking system to help you find what you need.

Q11: What is black and white hat hackers?

A: White Hat Hacker: White hat hackers choose to use their powers for good rather than evil. Also known as "ethical hackers," white hat hackers can sometimes be paid employees or contractors working for companies as security specialists that attempt to find security holes via hacking.

White hat hackers employ the same methods of hacking as black hats, with one exception- they do it with permission from the owner of the system first, which makes the process completely legal.

Black Hat Hackers: Like all hackers, black hat hackers usually have extensive knowledge about breaking into computer networks and bypassing security protocols. They are also responsible for writing malware, which is a method used to gain access to these systems.

Their primary motivation is usually for personal or financial gain, but they can also be involved in cyber espionage, protest or perhaps are just addicted to the thrill of cybercrime. Black hat hackers can range from amateurs getting their feet wet by spreading malware, to experienced hackers that aim to steal data, specifically financial information, personal information and login credentials. Not only do black hat hackers seek to steal data, they also seek to modify or destroy data as well.

Q12: Which operating systems are used for hacking and penetration testing?

A12: Kali Linux. Kali Linux is the most widely known Linux distro for ethical hacking and penetration testing.

Q13: Why windows are more prone to viruses?

A13: Windows is without any doubt the most famous and widely used operating system, it only makes sense that the majority of hackers will focus on creating viruses for it and not for Linux or MAC. The logic of this is pretty straight forward, if you want to infect as many people as possible with a virus, you'll have to forward it to the operating system that most people use, and that is Windows. Because there are so many hackers that are looking for ways to bypass the security of Windows, the chances of it happening increase a lot.

And other than that, there is also the problem that you get full Administrative privileges by default. That is great for installing multiple applications from the internet and such, but it can be an open door for a virus too.

Q15: What is open source software?

A15: Open source software is software with source code that anyone can inspect, modify, and enhance. "Source code" is the part of software that most computer users don't ever see; it's the code computer programmers can manipulate to change how a piece of software—a "program" or "application"—works. Programmers who have access to a computer program's source code can improve that program by adding features to it or fixing parts that don't always work correctly.