Cyber Security Interview Questions

Here will taking some advanced Pentesting Level Interview Questions some are focusing on Cryptography and Web App Attack area.

1. ***How you can reset a password-protected BIOS configuration. What do you do?***

Answer: While BIOS itself has been superseded by UEFI, most systems still follow the same configuration for how they keep the settings in storage.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”.

2. ***What is XSS?***

Answer: 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.

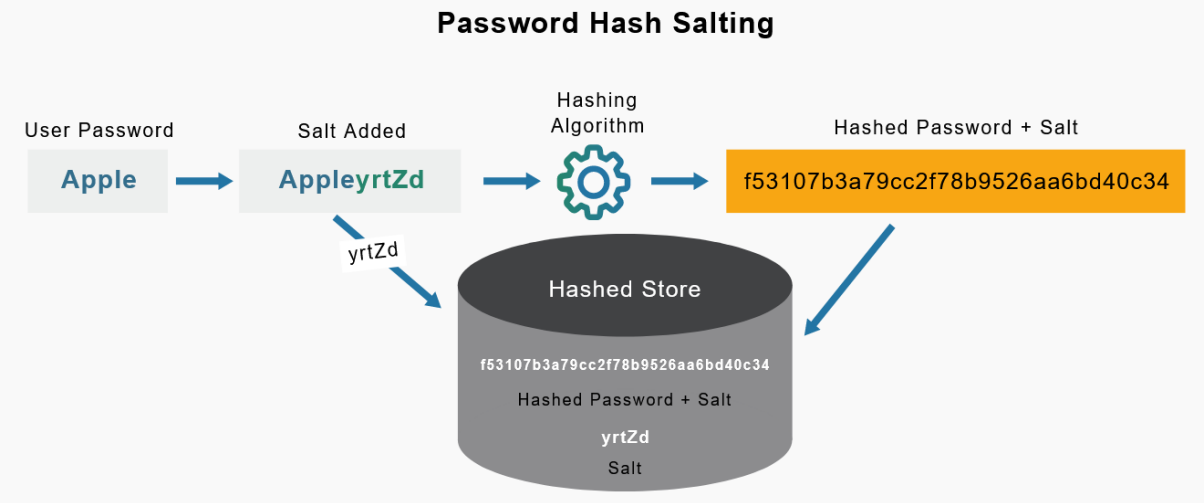
3. ***How would you login to Active Directory from a Linux or Mac box?***

Answer: 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.

4. ***What are salted hashes?***

Answer: 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. Get live, expert instruction from anywhere! Enroll in an upcoming live online boot camp and earn your certification, guaranteed.



More Info: https://websitesecuritystore.com/blog/what-is-password-salting/

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

Answer: 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.

6. ***What are the three ways to authenticate a person?***

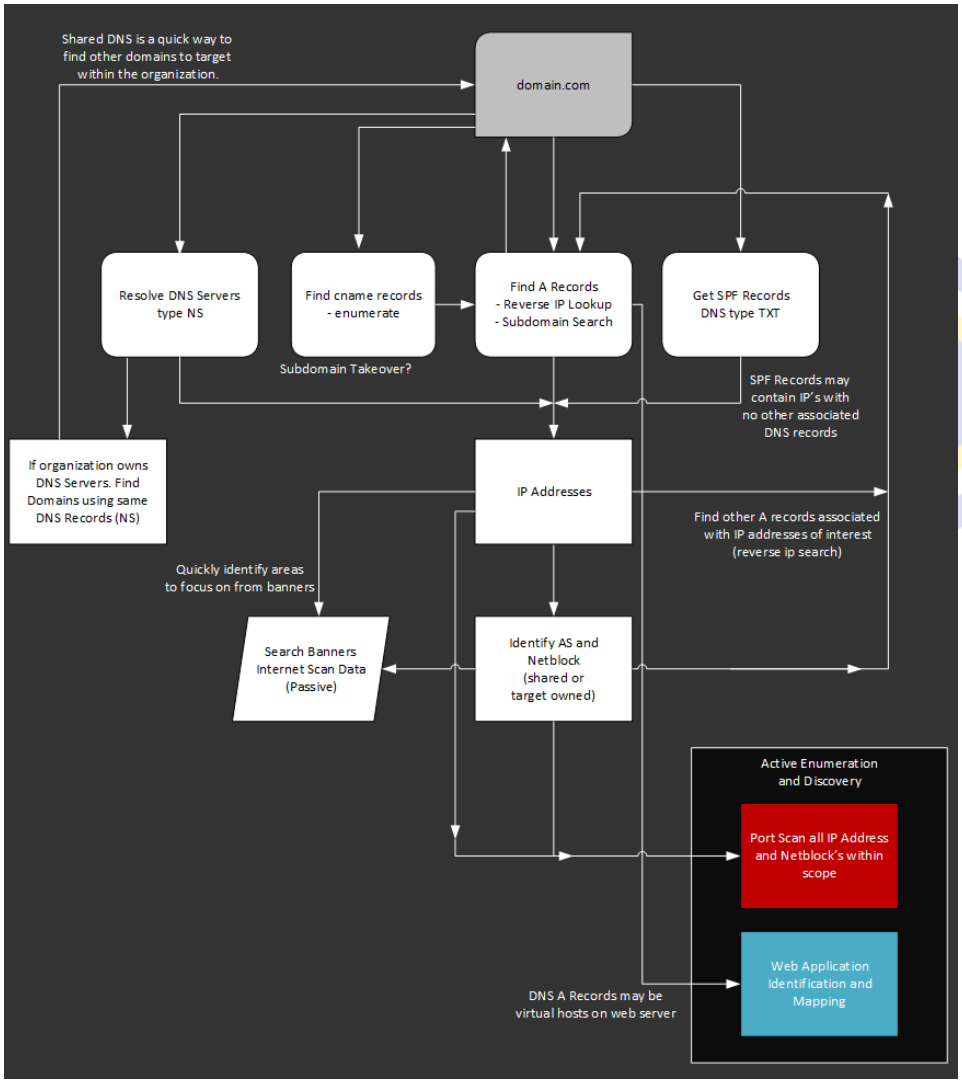
Answer: Something they know (password), something they have (token), and something they are (biometrics). Two-factor authentication often uses a password and token setup, although in some cases this can be a PIN and thumbprint.

More Info: https://gkaccess.com/support/information-technology-wiki/biometric-authentication/

Research on different Biometric Authentication procedure and what are the security vulnerabilities are available in Security Perspective?

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

Answer: 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.



More Info: https://dnsdumpster.com/footprinting-reconnaissance/

8. ***What is data protection in transit vs data protection at rest?***

Answer: 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.

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

Answer: 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.

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

Answer: 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.

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/