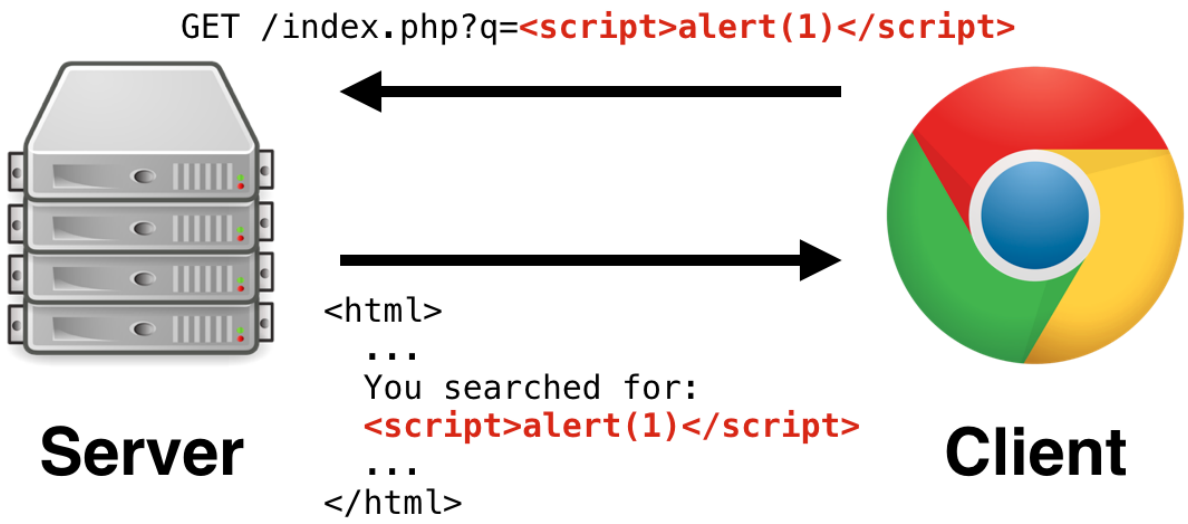
Cyber Security Interview Questions

Here the questions are for Intermediate Level for Penetration Testing concepts.
More focus on Web App Testing part

1. ***What is XSS? Give a Short Brief on it?***

Answer: This is a type of cyber-attack where malicious pieces of code, or even scripts, can be covertly injected into trusted websites. These kinds of attacks typically occur when the attacker uses a vulnerable Web-based application to insert the malicious lines of code. This can occur on the client side or the browser side of the application. As a result, when an unsuspecting victim runs this particular application, their computer is infected and can be used to access sensitive information and data. A perfect example of this is the contact form, which is used on many websites. The output that is created when the end user submits their information is often not encoded, nor is it encrypted.

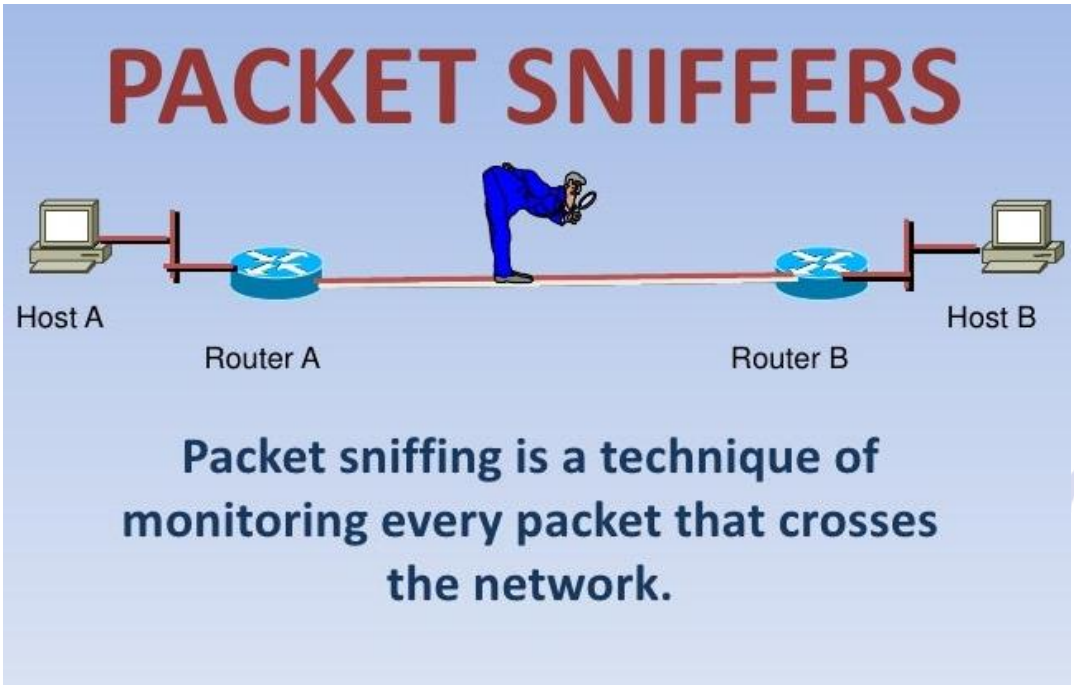


More Info: [46 Prevent Cross Site Scripting Javascript - Javascript Nerd Answer (lovebleeding9ffedd.blogspot.com)]

2. ***Did you know about Packet Sniffing? Where we use and why it used widely in Industry level?***

Answer: It is a specific process in which network traffic that can captured all the traffic from inbound and outbound part. It is use for deep analysis of the data packets to check the activities in the network going on.

Very famous and an open-source tool we have available be name called "Wireshark" that we using for packet capture and protocol analyzer part.



More Info: [Packet sniffers (slideshare.net)]

3. ***Elaborate the Full form which we use commonly in Pentesting?***

2FA, 2S2D, 2VPCD, 3DES, 3DESE, 3DESEP

Answer:

2FA means "Two-Factor Authentication"
2SD2D means "Double-Sided, Double Density"
2VPCP means "Two-Version Priority Ceiling Protocol"
3DES means "Triple Data Encryption Standard"
3DESE means "Triple Data Encryption Standard Encryption"
3DESEP means "Triple Data Encryption Standard Encryption Protocol"

4. ***What are some of the most common network security vulnerabilities that a Pentester comes across?***

Answer: Of course, there are countless numbers of issues that can impact the network infrastructure of an organization, and you probably have your own stories about what you've encountered. The following vulnerabilities are some of the most prevalent:

• The usage of extremely weak passwords in the network security tools themselves, which include the routers, firewalls, network intrusion devices and so on. Very often, business entities are in a rush to deploy these kinds of technologies, and they forget to create a robust and secure password. This leads to them using the insecure default one set up by the vendor

• Implementing security patches on the wrong servers and related network components. There are also times when a security patch is installed on the right machine but not configured properly, thus leaving it wide open to a cyber-attack

• The misconfiguration of network devices, as described previously

• The use of infected portable media devices (primarily USB drives) and inserting them into a server and other related network components

• The lack of a coherent network security policy; even if one was implemented, compliance is still a huge issue

5. ***What are the different pentesting techniques?***

Answer: Pentesting techniques fall into these following categories:

• Web Application Testing

• Wireless Network/Wireless Device Testing

• Network Infrastructure Services

• Social Engineering Testing

• Client-Side Application Testing

6. ***What network ports are commonly examined in a pentesting exercise, and what tool can be used for this?***

Answer: They are as follows:

• HTTPS (Port #443)

• FTP (Port #'s 20 & 21)

• NTP (Port #123)

• SSH (Port #22)

- HTTP (Port #80)
- Telnet (Port #23)
- SMTP (Port #25)

7. ***Describe in detail what SQL injection?***

Answer: This is a method in which malicious SQL code is inserted into the database or the back end of the Web-based application. These are typically deployed into an entry-level field so that the malicious code can be executed. This kind of attack is used primarily for heavy data-driven applications in which multiple security vulnerabilities can be found and exploited. It should be noted that although SQL injection attacks are primarily used to hit Web-based applications, the attacker can also target the SQL database just by itself as well.

8. ***What is the primary difference between asymmetric and symmetric cryptography?***

Answer: Only one type of key is used in symmetric cryptography, and this key is known as the Private Key. Although the main advantage of this is that this type of system is relatively easy to deploy, the primary disadvantage of it is that if the Private Key falls outside the reach of the sending and receiving parties, the cyber-attacker can easily capture the ciphertext and decrypt it very easily. With asymmetric cryptography, two keys are used: the Public Key and the Private Key. The advantage of this system is that it offers far greater levels of security as opposed to just using a Private Key, but it requires considerably more processing power resources. An example of an asymmetric cryptography system is Public Key Infrastructure, also known as PKI.

9. ***What are the permutations required for a robust SSL connection to take place?***

Answer: The following characteristics are required:

- The session identifier
- A peer certificates
- An established compression method
- Any associated cipher specs

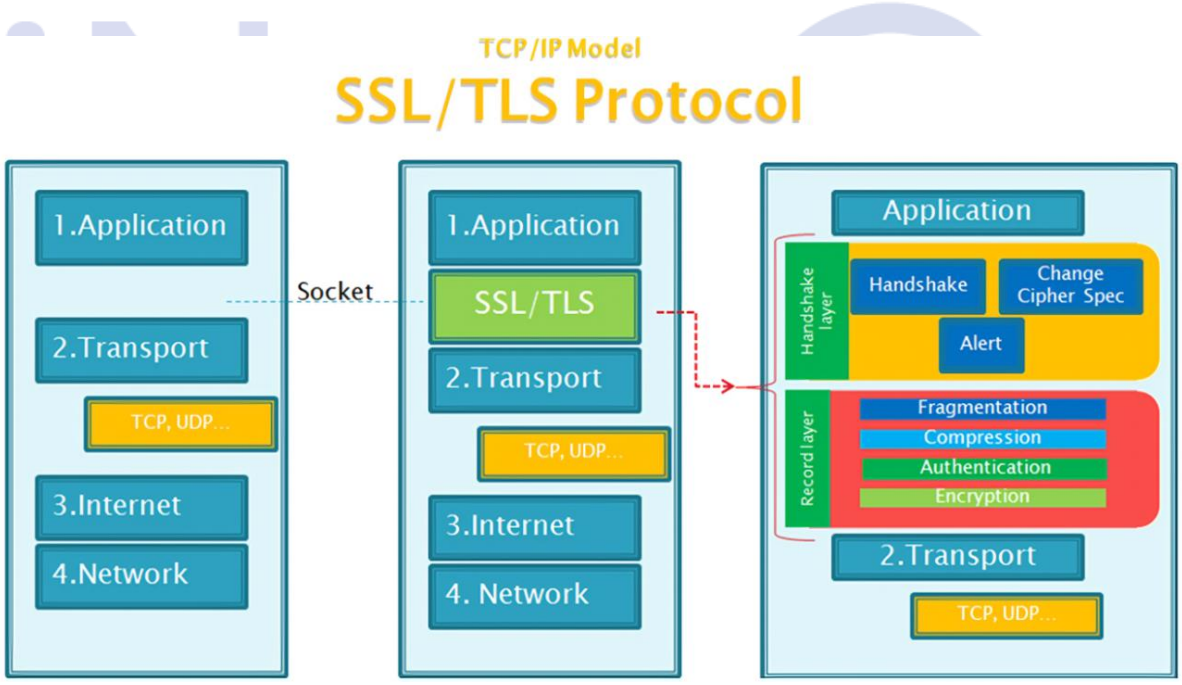
10. What is SSL and TSL?

Answer:

SSL stands for “Secure Sockets Layer.” This is the de facto standard to keep all Internet connections safe and secure. You will know that a particular website can be safely accessed when it has “HTTPS” in its URL address. SSLs are used most in e-commerce-based applications, in which credit card and other personal information and data is transmitted to the online merchant.

TSL stands for “Transport Layer Security” and is actually a much more updated and advanced version of SSL. It is important to note that with TSL, it can come with three types of encryptions:

- Elliptical Curve Cryptography (ECC)
- Rivest–Shamir–Adleman (RSA)
- Digital Signature Algorithm (DSA)



More Info: SSL/TLS原理详解_服务器应用_Linux公社-Linux系统门户网站 (linuxidc.com)

Stay tune to out next set of Interview Questions

Follow us:
https://www.linkedin.com/company/ineuron-ai/mycompany/
https://www.linkedin.com/in/mukeshkumarrao/