Cyber Security Interview Questions

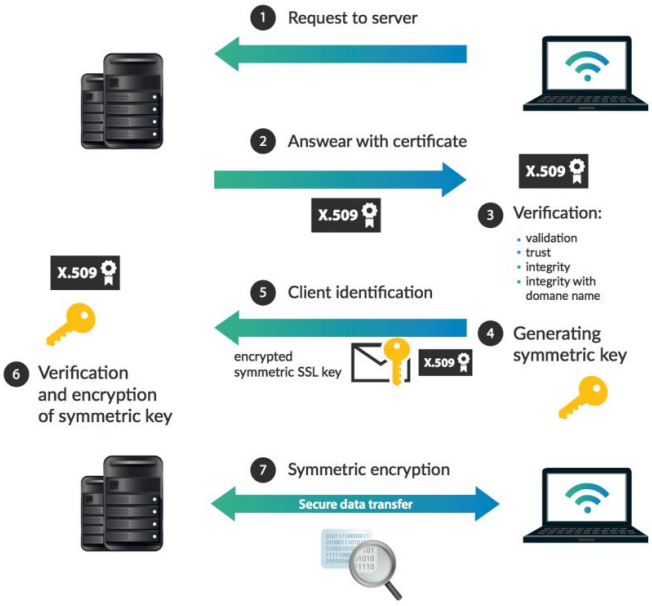
Here will taking some advanced Pentesting Level Interview Questions some are focusing on Cryptography and Web App Attack area.

1. ***How SSL and TLS are working?***

Answer:

Establishing an SSL/TSL connection works in this fashion:

- On the client side, the end user enters a URL address into their Web browser. This then initiates the SSL/TLS connection by transmitting a particular message to the server on which the website resides
- This server then returns a Public Key (or even a certificate) back to the end user's Web browser
- The browser then closely inspects this Public Key, and if all looks good, a Symmetric Key is transmitted back to the server. If there are anomalies detected from within the Public Key, the communications are instantly cut off
- Once the server gets the Symmetric Key, it then sends the encrypted webpage that is being requested back to the end user's Web browser
- The browser then decrypts the content into a form that can be easily understood by the end user It is important to note that this entire process can also be referred to as the SSL/TSL Handshake.



More Info: [Top 10 Best Reliable SSL Certificate Providers in 2020 (znetlive.com)]

2. Explain the different phases of a network Intrusion Attacks

Answer:

The phases are as follows:

- Reconnaissance: This is where the pentester learns more about the target they are about to hit. This can either be done on an active or passive basis. In this step, you learn more about the following:
    - The IP address range that the target is in
    - Finding out its domain name
    - DNS records
    - Scanning: This is the step where the pentester learns about the vulnerabilities of the particular target. Weaknesses are found in

the network infrastructure and the associated software applications. For example, this include the following:

- Ascertaining the services that are currently being run
- Any open ports
- The detection of any firewalls
- Weaknesses of the operating system in question

- Gaining the needed access: This is the part where the pentester starts to actually initiate the launch of the cyber-attack, based on the weaknesses and the vulnerabilities that they have discovered in the last step
- Maintaining the access: The pentester has entered the target itself and tries to keep that access point open so that they can extract as much private information and data as possible
- Covering their tracks: In this last step, the pentester ensures that any "footprints" left behind in the course of their attack are covered up so that they can't be detected. For instance, this involves the following:
  - The deletion of any log-related files
  - Closing off any backdoors
  - Hiding all controls that may have been used

3. Where we do exchange the Deffie-Hellman key for pentesting services?

Answer: This was actually one of the first Public Key protocols to be put into place, and it is a methodology that can be utilized to securely exchange Public Keys over an open network line of communications. A pentest can be done

here in order to determine and ascertain any kind of weak/TLS services that are associated with this exchange process.

4. ***After a pentest is conducted, what are some of the top network controls you would advise your client to implement?***

Answer: The following types of controls should be implemented:

- Only use those applications and software tools that are deemed "whitelisted"
- Always implement a regular firmware upgrade and software patching schedule, and make sure that your IT staff sticks with the prescribed timetable
- With regards to the last point, it is absolutely imperative that the operating systems(s) you utilize are thoroughly patched and upgraded
- Establish a protocol for giving out administrative privileges only on an as-needed basis, and only to those individuals that absolutely require them

5. ***How does traceout/tracert exactly work?***

Answer: This is used to determine exactly the route of where the data packets are exactly going. For example, this method can be used to ascertain if data packets are being maliciously redirected, they take too long to reach their destination, as well as the number of hops it takes for the data packets to go from the point of origination to the point of destination.

6. ***What is Omniquad Border Secure?***

Answer: This is a type of specific service that can help to perform network-based audits or even automated pentesting of an entire network infrastructure. It can give the pentesting team detailed information and data as to how the cyber-attacker can gain access to your network-based digital assets. It can also be used to help mitigate any form of threat that is launched by a malicious third party.

7. ***What number of vulnerabilities can the abovementioned service actually detect?***

Answer: All types of network infrastructures can be pentested, and up to a thousand total vulnerabilities can be detected with this particular service.

8. ***Describe the theoretical constructs of a threat model that can be used in a pentesting exercise.***

Answer: The constructs behind a threat model include the following:

- Gathering the required documentation
- Correctly identifying and categorizing the digital assets that are found within the IT infrastructure of a corporation or business
- Correctly identifying and categorizing any type of kind of cyber-threat that can be targeted towards the digital assets
- Properly correlating the digital assets with the cyber-threat that they are prone to (this is can also be considered as a mapping exercise where a digital asset is associated with its specific cyber-threat).

It is also important to note that there are three types of threat models that a pentesting team can use, and they are as follows:

- Digital Asset-Centric
- Cyber-Attacker-Centric
- Software Application-Centric.

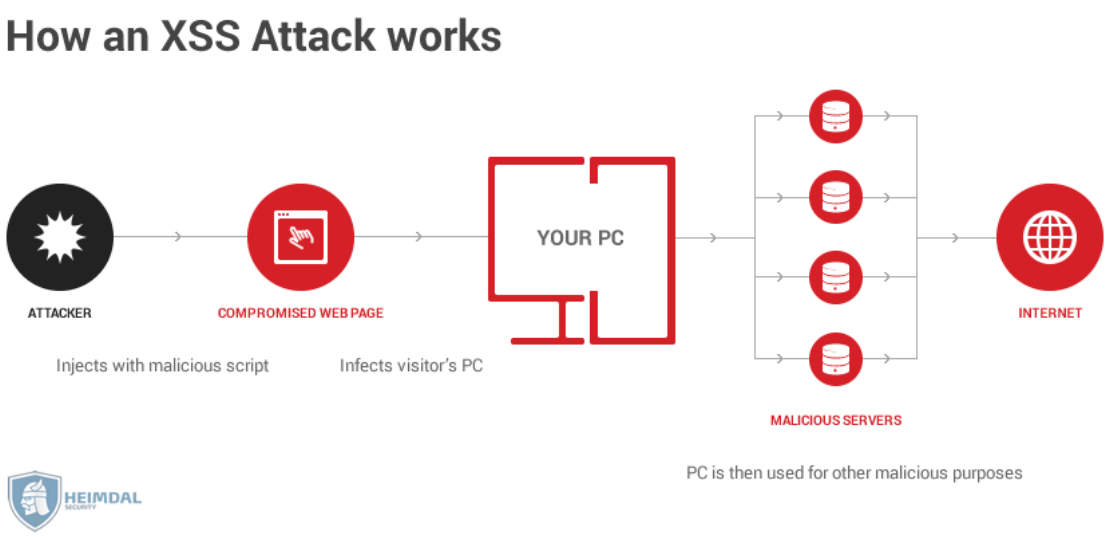
9. What are the three types of cross-site scripting (XSS)?

Answer: The three types are as follows:

- Persistent/Stored XSS: This is where the malicious input is stored onto the target server, such as a database, and is reflected at the page where the end user entered in their information (such as a “Contact Us” form)
- Reflected XSS: Any form of malicious user input is instantaneously returned by the Web-based application as an “Error Message.” As a result, this data is deemed to be unsafe by the Web browser, and it is not stored in any fashion
- DOM-based XSS: This will actually for any type or kind of client scripting language (such as Java) to access and maliciously modify the end user input. It can also covertly alter the content, structure and even the particular style of a webpage.

  The types of objects that can be manipulated include the following:

  - Document.URL
  - Document.location
  - Document.referrer



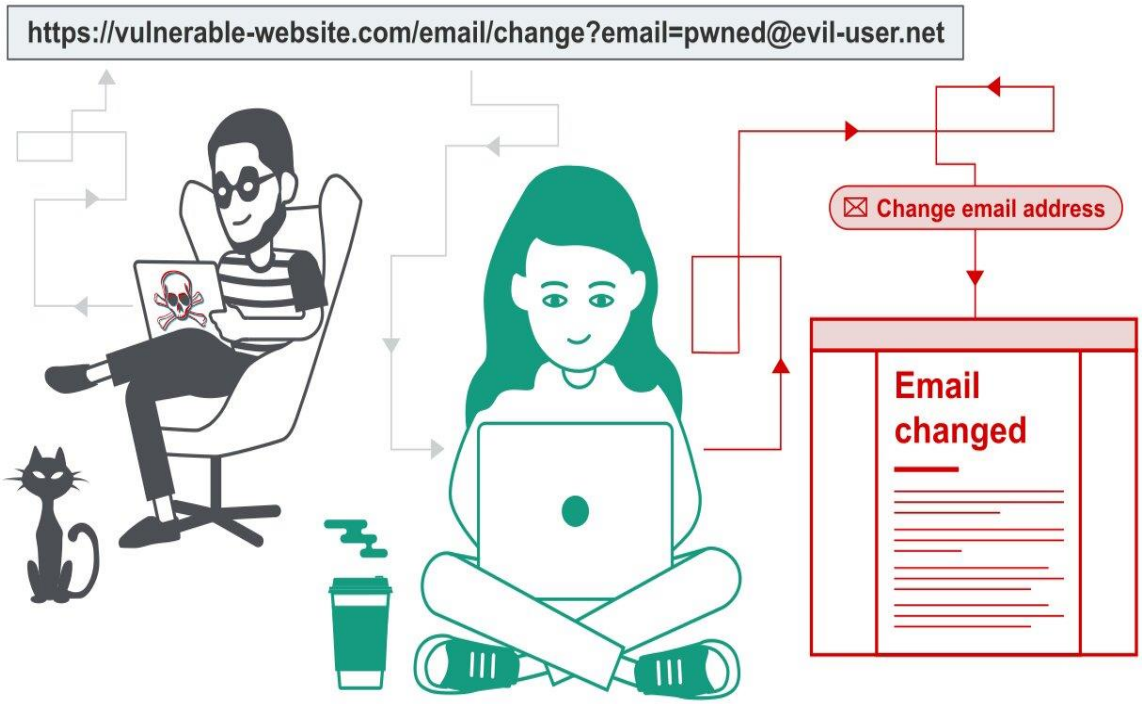
More Info: [What Is Session Hijacking. Session Hijacking Types and Prevention (heimdalsecurity.com)]

10. What exactly is CSRF and how can it be prevented when executing a pentest exercise?

Answer: This stands for cross-site request forgery, and it takes advantage of the trust levels that are established in an authenticated user session. For example, in these scenarios, Web-based applications typically do not conduct any form of verification tests that a specific request actually came from an authenticated user; rather, the only form of verification is sent by the particular Web browser that the end user is utilizing.

There are two ways to avoid this scenario:

- Double-check the specific CSRF token that is being used
- Confirm that the specific requests are coming from within the same origin



More Info: portswigger.net

Stay tune to out next set of Interview Questions

Follow us:

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

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