Cyber Security Interview Questions – Day1

So, as we Cyber Security in one of the IT domains, where the jobs are very high demand and if we think future perspective its very long journey, we have with good Salary also.

So, here I am providing some Interview Questions for Job Profiles:

- Penetration Tester
- Cyber Security Analyst
- Web Application Security Analyst
- VAPT Analyst
- Junior Pentester
- Ethical Hacker
- And fresher level job in Cyber Security

Mainly focus on Penetration Testing perspective:

1. What is Pentesting? Define Pentesting? What do you know about Pentesting? What does it mean to you about Pentesting?

Answer: Technical definition you can got from Wikipedia too.

Let's understand in simple way, let we have website name www.example.com, here we have to found some bug or threat present on the Web App that can be taken profit by the Hackers. So, pentesting is an exercise where we as Cyber Security expert attempts to find vulnerabilities into a system, computers,

hardware, software and web app. It's a kind of simulated attack we do to find loopholes and provide the defenses system to make it secure.

2. **What is the main goal about pentesting? Or the primary purpose?**

Answer: The main goal is to go deeper into software or hardware to find bugs or vulnerabilities, and try to gain the access. So, in that way we can found the different approach how hacker can compromise the systems or applications. Then we can able to patch the loopholes through developers. Also, as security expert, out target should be found the vulnerabilities at early stage of the application or system, so that we can earlier patch it before Hacker able to find it.

3. **What are the goals of conducting the Pentesting services? Or what we can achieving while performing the Pentesting services?**

Answer: The goals are as follows:

- To test adherence to the security policies that have been crafted and implemented by the organization
- To test for employee proactiveness and awareness of the security environment that they are present
- To fully ascertain how a business entity can face a massive security breach, and how quickly they react to it and restore normal business operations after being hit.
- To achieve the enterprise security so that organization can become secure before any big breach or cyber-attack

4. **Is the VAPT – Vulnerability Assessment and Penetration Testing are same or there is some difference present? Explain in your own word?**

Answer: Vulnerability Assessment: the main target is to found possible threats and vulnerability is present into a system or an application. Remember here we cannot perform any active attack or simulated activity to exploit or gain access.

Generally, we use manual information gathering approach and scanning tool, it can be open source or automate scanner tools present.

Example of tool: Nessus, Vega, Nikto, Aceuntix, etc

Penetration Testing: here the main fun is, we actually perform hacking activity to exploit the vulnerabilities we found in VA process. Also, we can able to proof that the vulnerability we found is exploitable or not. Its just like we are proving the real vulnerabilities, instead of just assuming that this vulnerability we have so we can replace the application or system. Else we can update it with new versions.

Example of tool: Metasploit, Routersploit, SQLMap, etc

5. **Describe the Three types of Pentesting Methodologies?**

Answer: Three types of Pentesting Testing are:

- White Box Testing
- Grey Box Testing
- Black Box Testing

6. **Can you describe them in more detail or with example?**

Answer:

White Box Testing: Here we perform testing, when we have initial information already given, like the target information and we don't have to perform any activity related to Information gathering process.

Grey Box Testing: Here we have some information and some information is not known, it's like 50-50 ratio we have information available, so we do perform active recon or information to reconfirm the target to perform pentesting on it.

Black Box Testing: Here we perform a Blind testing as we don't have any information about the target exactly and no information about application technologies or infrastructure of the organization.

More Info: https://www.packetlabs.net/posts/types-of-penetration-testing/

7. **Did you have different cyber security team we have who perform the above type of pentesting?**

Answer: Yes, off course we have many teams but dedicated we have

- **Red Team**
- **Blue Team**
- **Purple Team**

Check on Internet to learn more about these teams, what they do and comparison.

Ok, don't worry no waste time.

8. **I, explain the detail about these teams a short brief?**

Answer: The functionalities of these three teams can be described as follows:

The Red Team

This group of pentesters acts like the actual cyber-attack. That means this team is the one that launches the actual threat, in order to break down the lines of defense of the business or corporation and attempt to further exploit any weaknesses that are discovered.

The Blue Team

These are the pentesters that act like the actual IT staff in an organization. Their main objective is to thwart any cyber-attacks that are launched by the Red Team. They assume a mindset of being proactive as well as maintaining a strong sense of security consciousness.

The Purple Team

This is a combination of both the Red Team and the Blue Team. For example, they have the security arsenal that is used by the Blue Team and possess a working knowledge of what the Red Team is planning to attack. It is the primary job of the Purple Team to help out both these teams out. Because of that, the pentesters of the purple team cannot be biased in any regard and have to maintain a neutral point of view

9. **What kinds of certification is in demanding if you looking into this career path?**

Answer:

For Beginner level we have many certifications available, some our cheaper and some are costly. So, if you planning for any fresher level certificate in cyber security do check your Financial Stability also matter.

As per our preference:

EC-Council – CEHv12

E-learning – eJPT

Comptia – Security+ | N+

ISC2 – CC – certified in cyber security

Advanced level

Offensive Security – OSCP

EC-Council – CPENT

Comptia – Pentest+

10. **Talking about higher official management who are from Management or governance background, not you have submitted the report and they can't understand the technical report that we submit after the pentesting report is completed. So, as Cyber Security Engineer how you can explain this report to them?**

Answer: So, remember here, if you explaining the report in technical way, no one give any importance about your hard work, and they don't get serious about the vulnerabilities you have found.

So, here you have to explain them in simple but more on financial loss expectation need to explain. Like what happen if the application got compromise what kind of legal policies they can implement to stop and secure future cyber-attack. Do add some good Chart or table for showing the stats about the vulnerabilities and their level of severity. If the attack happens at that level how much loss they need to face in terms of financial perspective approach.

Stay Tune will come tomorrow with more Interview Questions in Cyber Security Different Job Profiles.