Level 1 Questions

This group of questions will cover the basics of penetration testing, focused on the following areas:

- A definition of pentesting
- The purpose and goals of pentesting
- The difference between vulnerability testing and pentesting
- The types of pentesting methodologies
- The teams that are required to conduct a pentesting exercise
- The certs that are required in order to demonstrate deep skills and knowledge in pentesting
- How a pentester should explain the results of a pentest to a C-level executive

1.What is a specific definition of pentesting?

Let's ask the people in the know. Cloudflare.com says the following: "Penetration testing (or pentesting) is a security exercise where a cybersecurity expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of."

2.What is the primary purpose of pentesting?

The main purpose of a pentest is to conduct a "deep dive" into the IT Infrastructure of a business or a corporation with the primary intention of gaining access to any (and if possible, all) of the electronic based assets that exist. It is important to note that the goal of the pentester is not to attempt to strike a hard blow right at the very beginning; rather, they escalate the intensity of the cyber-attack over a period of time.

3.What are the goals of conducting a pentesting exercise?

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 in
- 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.

4.There is very often confusion between vulnerability testing and pentesting. What is the primary difference between the two?

With vulnerability testing, one is simply scanning for any weaknesses that may reside in any component of the IT Infrastructure. In a pentest, a full-scale cyber-attack or series of cyber-

attacks is launched with explicit permission from the client (or whoever is requesting it) in order to specifically find any types or kinds of gaps that have not yet been discovered by the IT security staff.

5.What are the three types of pentesting methodologies?

The three types are as follows:

- Black-Box Testing
- White-Box Testing
- Gray-Box Testing

6.Describe these tests in much more detail.

Black-Box Testing

In some instances, the cyber-attacker may know nothing about their intended target. So in an effort to try to break through the lines of defense, the cyber-attacker will carry an all-out attack, also known as a brute-force Attack. In a black-box scenario, the pentester will not have any knowledge whatsoever about the target(s) they are going to hit. As a result, this kind of pentest can take a very long time to conduct, and automated tools are heavily relied upon. This kind of exercise is also known as a trial-and-error approach.

White-Box Testing

This kind of pentest is also known as clear-box testing. In these instances, the pentester has advanced knowledge to some degree about the Web application that they are about to hit and its underlying source code. This kind of attack takes a shorter amount of time to launch when compared to the black-box test.

Gray-Box Testing

This kind of pentesting is a combination of both of black-box and white-box testing. This simply means that the pentester has some advanced knowledge on the targets they plan to attack. This kind of exercise requires both the use of automated and manual tools. When compared to the other two tests, this one offers the highest chances of discovering unknown security holes and weaknesses.

7.What are the teams that can carry out a pentest?

The teams are as follows:

- The Red Team
- The Blue Team
- The Purple Team

8.Can you describe these teams in more detail?

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 certifications in the most demand for penetration testing?

There is no doubt that in the cybersecurity field, there an endless number of certs one can pursue. But if a pentester is to be recognized as the top in their field, the following certs are a must-have:

- The Certified Ethical Hacker (aka CEH – this is administered by the EC Council)
- The Offensive Security Certified Professional (aka OSCP – this is administered by Offensive Security)

10.The results of a pentesting exercise have to be made available not only to the IT staff, but also to the C-level executives. The latter may not possess a strong technical knowledge like their IT staff does. How would you explain the results to them?

The C-suite can understand results when they are explained to them in terms of financial impact. Thus, a pentesting report should also include a risk analysis which demonstrates the benefit versus the cost of any of the vulnerabilities that are discovered and not fixed. It should also have financial calculations demonstrating the impacts of a security breach.

Level 2 Questions

In this section, we'll look at some intermediate-level questions about penetration testing concepts. These will focus on the following:

- Cross-site scripting
- Data packet sniffing
- Various abbreviations that are used in pentesting
- Common network security vulnerabilities
- Pentesting techniques
- The various network ports
- SQL injection attacks
- Asymmetric/symmetric cryptography
- SSL/TLS

11.Explain what cross-site scripting (XSS) is all about.

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.

12.What exactly is data packet sniffing, and what are some of the most widely used tools?

Data packet sniffing is a specific process in which network traffic can be captured ether across the entire IT Infrastructure, or just certain parts of it. Once this has been accomplished, then a deep analysis of the data packets in question can then be made.

For example, if a business or a corporation is hit by a cyber-attack, examining the network traffic and the data packets that were associated with it at the time of the security breach occurred becomes extremely crucial, especially from the standpoint of forensics. Even if no attack is imminent, it is still very crucial for the IT staff to conduct a check on their network traffic in order to determine if there is any sort of anomaly that is present. There are many data packet sniffing tools that are available today, but probably the most widely-used one is Wireshark.

13.Please provide the exact names of the following abbreviations that are commonly used in pentesting: 2FA, 2S2D, 2VPCP, 3DES, 3DESE, 3DESEP.

The acronyms stand for the following:

- 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”

14.What are some of the most common network security vulnerabilities that a pentester comes across?

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

15.What are the different pentesting techniques?

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

1.6What network ports are commonly examined in a pentesting exercise, and what tool can be used for this?

They are as follows:

- HTTPS (Port #443)
- FTP (Port #’s 20 & 21)
- NTP (Port #123)
- SSH (Port #22)
- HTTP (Port #80)
- Telnet (Port #23)