Top 30 Penetration Tester (Pen Tester) Interview Questions and Answers for 2018

Introduction

It seems like hardly one Cyber threat comes out, many variants of it soon follow affecting both individuals and business/corporations alike. One of the key areas in which the Cyber attacker is able to launch their threats is by looking for vulnerabilities and weaknesses in the lines of defenses that are set up.

Many organizations simply think that by deploying the latest Security technologies that they will be immune from any form of a Cyber-attack. However, this is far from the truth. What they fail to understand is that apart from implementing these tools, their entire IT Infrastructure needs to be thoroughly tested from the inside out.

How can this be done? Probably one of the best ways to do this is through what is known as Penetration (Pen) Testing. With this kind of analysis, a team of experienced IT professionals actually behave like a real Cyber attacker, but within legal and ethical bounds.

Their primary goal is to launch just about any kind of attack that is imaginable, in an effort to discover any unknown Security gas and weaknesses. Their findings are then summarized into a comprehensive report, supported with solutions as to how these vulnerabilities can be fixed.

Because of the dynamic nature of the Cyber threat landscape, as one can imagine, the job growth demand in Pen Testing is quite high, and is expected to be so into the coming future. Becoming a Penetration Tester requires a mixture of both quantitative and qualitative skills.

For example, he or she has to decipher the complex reports that are outputted by the Pen Testing tools, as well as having the patience to work very long hours, and at odd times.

It takes years of experience to be a fully qualified Pen Tester, and this particular individual must be able to keep with the latest trends and happenings in this field. In any job interview situation, you could be potentially asked just about question imaginable as it relates to Pen Testing. For instance, they could range the gamut from what Pen Testing means to what tool you should use in a particular situation to even what kind of Cyber attack you would launch and why.

In this article, we review the top 30 questions you could face in a potential interview.

Level 2 Questions

In this grouping of questions, basic Penetration Testing questions are asked, focused upon the following:

- A definition of Pen Testing;
- The purpose and goals of Pen Testing;
- The difference between Vulnerability Testing and Pen Testing;
- The types of Pen Testing Methodologies;
- The teams that are required to conduct a Pen Testing exercise;
- The certs that are required in order to demonstrate deep skills and knowledge in Pen Testing;
- How a Pen Tester should explain the results of a Pen Test to a C-Level Executive.

1) ***What is a specific definition of Pen Testing***?

A precise definition of it as follows:

Penetration testing (or pen testing) is a security exercise where a cyber-security 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. This is like a bank hiring someone to dress as a burglar and try to break into their building and gain access to the vault. If the 'burglar' succeeds and gets into the bank or the vault, the bank will gain valuable information on how they need to tighten their security measures. (SOURCE: 1).

2) What is the primary purpose of Pen Testing?

The main purpose of a Pen Test is to literally 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 Pen Tester not to attempt to strike a hard blow right at the very beginning; but rather, escalate the intensity of the Cyber attack over a period of time.

3) What are the goals of conducting a Pen Testing exercise?

The goals are as follows:

- To test the compliance of 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 Pen Testing. 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 Pen Test, a full scale or even a series of Cyber attacks are launched with explicit permission from the client (or whomever 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 Pen Testing 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 (though this trend is changing – they are spending much more time researching their targets and intended victims). 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". Thus, in this kind of scenario, the Pen Tester will not have any knowledge whatsoever about the target(s) they are going to hit. As a result, this kind of Pen Test can take a very long time to conduct, and the use of automated tools is heavily relied upon. This kind of exercise is known as a "Trial and Error" approach.

White Box Testing:

This kind of Pen Test is also known as a "Clear Box Testing". In these instances, the Pen Tester 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. While the advantage of this is that this kind of Pen Testing can be more precise, but the tools required to execute it can be more complex.

Gray Box Testing:

This kind of Pen Testing is a combination of both of Black Box and Gray Box Testing. This simply means that the Pen Tester 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 are required to carry out a Pen Test?

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 Pen Testers acts like the actual Cyber-attack. Meaning, this team is the one that launches the actual threat, in order to break downs, the lines of defense of the business or corporation, and attempting to further exploit any weaknesses that are discovered.

The Blue Team:

These are the Pen Testers that act like the actual IT staff in an organization. Their main objective is to thwart off 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 also 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, and because of that, the Pen Testers of the Purple team cannot be biased in any regard, and have to maintain a neutral point of view.

9) ***What kinds of certifications are the most in demand for Penetration Testing?***

There is no doubt that in the Cyber security field, there an endless number of certs one can pursue. But if a Pen Tester 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 the Offensive Security);
- The Exploit Researcher & Advanced Penetration Tester (aka GXPN - this is administered by the GIAC).

10) ***The results of a Pen Testing exercise have to be made available not only to the IT Staff, but also to the C-Level Execs. The latter may not possess a strong, technical knowledge like their IT staff does. So, how would you explain the results to them?***

The C-Suite can understand results when it is explained to them in terms of financial impact. Thus, in this regard, a Pen Testing Report should also include a Risk Analysis which demonstrates the benefit versus the cost of any of the vulnerabilities that are discovered and are not fixed. It should also have financial calculations demonstrating the impacts of a Security breach.

Level 3 Questions

In this set of questions, intermediate level questions about Penetration Testing questions are asked (either of the candidate or the actual Pen Tester themselves), with an emphasis upon the following:

- Cross Site Scripting;
- Data Packet Sniffing;
- Various abbreviations that are used in Pen Testing;
- The common Network Security vulnerabilities;
- Pen Testing Techniques;
- The various Network Ports;
- SQL Injection Attacks;
- Asymmetric/Symmetric Cryptography;
- SSL/TLS.

1) ***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 actual, trusted websites. These kinds of attacks typically occur when the Cyber attacker uses a vulnerable Web based application from which to insert the malicious lines of

code. This can occur on the client side, or the browser side of the Web based application. As a result, when an unsuspecting victim accesses this particular application, their computer can then be used to access sensitive information and data, wherever any type of user input is required. 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 nor encoded, nor is it encrypted.

2) ***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 occur. 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 Cyber 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 that of Wireshark.

3) Please provide the exact names of the following abbreviations that are commonly used in a Pen Testing: 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”.

4) What are some of the most common Network Security vulnerabilities that a Pen Tester comes across?

Of course, there are countless numbers of issues that can impact the Network Infrastructure of an organization, but some of the following are the most prevalent:

- The usage of extremely weak passwords in the Network Security tools themselves, which include the Routers, Firewalls, Network Intrusion Devices, etc. Very often, business entities are in a rush to deploy these kinds of technologies, therefore they forget many times to create a robust and secure password, thus the default one set up by the vendor is very often used.
- Implementing Security patches on the wrong servers and related network components. There are also times even when a Security patch is installed on the right machine, it is often 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 those of 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 Pen Testing techniques?

The Pen Testing 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 Pen Testing 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);
- SMTP (Port #25).

In these particular instances, "Nmap" is the most commonly used tool.

7) Describe in detail what SQL Injection is all about?

` This is a method in which malicious SQL code inserted into the database, or the backend 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 Cyber 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 the Web based applications, the Cyber attacker can also target the SQL database just by itself as well.

8) What is the primary difference between Asymmetric and Symmetric Cryptography? What is an example of the former?

In the case of Symmetric Cryptography, only one type of key is used, which 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 its main disadvantage is that it requires considerably

more processing power resources. An example of an Asymmetric Cryptography system is that of the Public Key Infrastructure, also known as the PKI.

9) What are the permutations that are required for a robust SSL connection to take place?

The following characteristics are required:

- The Session Identifier;
- A Peer Certificate;
- An established Compression Method;
- Any associated Cipher specs.

10) What is SSL and TSL?

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. SSL's 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 the SSL. It is important to note that with TSL, it can come with three types of Encryption:

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

Level 4 Questions

In this grouping of questions, advanced level questions about Penetration Testing questions are asked (either of the candidate or the actual Pen Tester themselves), with a focus on the following:

- The SSL/TSL Handshake;
- The phases of a Network Intrusion Attack;
- Diffie-Hellman Public Key Exchanges;
- The establishment of Network Controls;
- Traceout/Tracert;
- Omiquad Bordersecure;
- The various Pen Testing models;
- The types of Cross Site Scripting (XSS);
- Cross Site Request Forgery.

1) How exactly does SSL/TSL work?

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 upon;

- 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 then transmitted back to the server. If there are anomalies detected from within the Public Key, the communications are then instantly cut off;
- Once the server gets the Symmetric Key, it then sends the encrypted web page that is being requested back to the end user's Web browser;
- The Web browser then decrypts the content into a decipherable 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".

2) Describe the different phases of a Network Intrusion Attack?

The phases are as follows:

- Reconnaissance:

  This is where the Pen Tester 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, etc.

- Scanning:

  This is the step where the Pen Tester learns about the vulnerabilities of the particular target. Weaknesses are found in the Network Infrastructure, and any weaknesses that are found in 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, etc.

- Gaining the needed access:

  This is the part where the Pen Tester starts to actually initiate the launch of the Cyber-attack, based upon the weaknesses and the vulnerabilities that they have discovered in the last step.

- Maintaining the access:

  This is the phase where the Pen Tester has actually gained entry into 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 the tracks:

  In this last step, the Pen Tester ensures that any "footprints" left behind in the course of their Cyber attack are all covered up, so that they cannot 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, etc.

3) ***What is a specific Pen Testing exercise that can be done with a Diffie-Hellman exchange***?

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 Pen Test 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 Pen Test is conducted, what are some of the top Network Controls you would advise your client to implement?

The following types of controls should be implemented:

- Only use those applications and software tools that are deemed as "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?

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 an Omiquad Bordersecure?

This is a type of specific service that can help to perform network-based audits or even automated Pen Testing of an entire Network Infrastructure or just parts of it. It can give the Pen

Testing 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 is the total number of vulnerabilities that the above-mentioned service actually detects?

All types and kinds of Network Infrastructures can be Pen Tested, and to 1,000 total vulnerabilities can be detected with this particular service.

8) Describe the theoretical constructs of a Threat Model that can be used in a Pen Testing exercise?

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 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 Pen Testing Team can use, and they are as follows:

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

The above is an example of a Digital Asset-Centric Threat Model.

9) What are the three types of Cross Site Scripting (XSS)?

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 Web page. Further, the types of objects that can be manipulated include the following:

*document.url;

*document.location;

*document.referrer.

10) What exactly is CSRF and how can it be prevented when executing a Pen Test exercise?

This stands for "Cross Site Request Forgery", and it takes total advantage 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 requested actually came from an authenticated user; rather, the only form of verification is sent only 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.

Conclusions

Overall, this article has examined some of the interviews that you could be asked if you are applying for a Pen Testing job. Likewise, these questions can also be asked of a Pen Tester if they are currently employed in this field. It is important to keep in that although answering these questions will demonstrate to the interviewer your in-depth knowledge of Pen Testing, it takes other qualitative skills as well in order to become a successful Pen Tester.

For instance, you must have the ability to work well with others in a team-oriented fashion, and have the ability to work *l*ong hours. Pen Testing also requires you to have a great deal of patience on your part, as it these kinds of exercises do not happen in just one day.

A successful Pen Test can take weeks or even months to accomplish. Finally, you must also have the ability to take all of the techno jargon that is associated with the results you have obtained and bring it down to a level that your client can understand and implement. You will also be gauged on these qualitative factors as well in your interview.

If you want to review more in-depth Pen Testing questions, click on the link here. Skillset is a practice exam engine featuring thousands of certification exam questions for security and IT pros. Users benefit from detailed question explanations and exam readiness scores, letting them know exactly when they are ready to sit their exams.

Sources

1) https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/
2) https://www.swascan.com/swascan-penetration-testing/
3) https://allabouttesting.org/interview-questions-answers-penetration-testing/4/
4) https://en.wikipedia.org/wiki/SQL_injection
5) https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-https
6) https://www.wisdomjobs.com/e-university/penetration-testing-interview-questions.html
7) https://www.aditiconsulting.com/11-important-interview-questions-for-network-penetration-testers/
8) https://digiaware.com/2017/09/cyber-security-vapt-interview-questions-with-answers-part-1/
9) http://www.kirklandwa.gov/Assets/Finance+Admin/Finance+Admin+PDFs/Purchasing/Q$!26A+Network+Security+Assessment.pdf
10) https://sneakerhax.com/pentester-interview-questions/
11) https://www.pcicomplianceguide.org/the-top-5-questions-to-ask-a-prospective-penetration-tester/