# GETESTERS TERMS & CONDITION

## What is a Penetration Testing Agreement?

- Some businesses are responsible for highly sensitive data. This includes customers' contact information, trade secrets, credit card particulars, and more. Unfortunately, securing this data is not easy, and it can sometimes make your organization susceptible to hacking.

- This is where third-party penetration testing services come in handy. Penetration testing entails hiring another company to audit your business' systems and verify that there aren't any security loopholes that hackers can exploit.

- But before you entrust your company's most confidential information to a 'stranger', you should have a contract in place. A penetration testing agreement highlights all the necessary details that allow you and the persons working for you to perform penetration testing activities.

## When do I need a Penetration Testing Agreement?

- Do you run a company that offers penetration testing (Pentest) services? If so, having a pentest agreement each time you're dealing with a new client is essential. This contract enables you to define the terms and guidelines that your client(s) should adhere to.

- This agreement is equally important for the clients seeking penetration testing services. Given the sensitivity of the auditing process, a contract ensures that the pentesting company performs their job without violating any laws.

## What are the Key Clauses in the Penetration Testing Agreement?

- **Parties to the agreement** – The first section should highlight the personal details of all the parties involved. It should clearly state the name, address and contact information of the recipient company as well as that of the organization providing pentesting services.

- **Scope of work** – The second clause should explain the obligations of each party, that is, the company performing the security test and the client. On its part, the penetration tester agrees to:

- Conduct a thorough security test, employing a considerable amount of skill and care
- Produce a comprehensive test report in the end
- Provide appropriate measures or recommendations where systems are found to be vulnerable to security breaches
- The client is also responsible for:
- Obtaining necessary consent documents such as from the internet service provider
- Backing up vital data before the penetration test is conducted
- Providing suitable accommodation in instances where the security testing will occur on their premises
- **Timeframe** – Though it seems like a minor detail, it's important to establish a specific timeline for the penetration testing.
- For the best outcome, the client and pentester should split the project into milestones, then set a timeframe for each. This way, it's easy to create reasonable deadlines for each phase of the project. A typical timeframe for a penetration test is 4 to 6 weeks, divided as follows:
- Planning- this involves acquiring the necessary resources and reviewing the project guidelines
- Execution- actual testing of the organization's systems, takes place
- Analysis and quality assurance- this entails preparing a summary report

**Payment terms** – This clause explains how and when payments are made. With such a project, the fees are payable once the client receives a detailed report of his/her company's data security systems. In other cases, the client is required to make payment as soon as the testing is complete.

- Another point that should be clarified under this section has to do with the allocation of resources. To be specific, the two parties should agree on how testing materials/equipment will be obtained and paid for. On the same note, the contract should outline the action to be taken if the resources are not fully utilized.
- In the event of a termination, the payment clause also explains how remuneration will be handled.
- **Confidentiality** – Often, conducting a pentest results in the disclosure of sensitive information; from client data to production techniques and more.
- For this reason, the client may request the service provider to sign a non-disclosure agreement beforehand. This helps to guarantee the privacy of any information the penetration tester comes across- whether this happens intentionally or unintentionally.
- **Termination** – Ideally, both parties commit to a penetration testing agreement hoping that nothing goes wrong. But certain situations can cause either party to terminate the contract prematurely. This particular clause lists the circumstances that would lead to an early termination.
- For instance, if the client fails to pay a portion of the fees within a specified period, the penetration testing firm reserves the right to end the partnership. Similarly, the client can terminate the pact if the security testing is not done properly.
- This clause also explains the course of action to be taken upon terminating the contract. Ideally, the service provider should not attempt to access the client's servers or systems once the project is complete. Such unauthorized activity will be considered unlawful.

# Summary

- A penetration testing agreement is a legally binding contract made between a pentesting service provider and their client. The document lays out relevant details pertaining to their arrangement. These include names of the parties involved, terms of remuneration, termination procedure, and scope of services.
- Security is one of the biggest concerns for any organization. No one wants to see their data being leaked or their network being hacked. The best way to prevent that is to hire a penetration testing company that will have an expert check out your network, infrastructure, and even your website. It takes years for an organization to create a reputation in the market and all it takes is a single attack on your network or infrastructure to ruin that. Get in touch with a professional team of security analysts today.