Pen Testing – Information sheet

What kind of penetration testing services do we provide?

- **Application Security Testing**

Applications are the core of your business, without them we will be unable to access your data. Making sure that your applications are secured properly will prevent malicious users from accessing, deleting, or modifying data that they should not be allowed. Methods of doing this are analyzing source code, brute force testing (Trying various methods to break/bypass the software), or if it is very common commercial software, running scans against it for known weaknesses. Even the most secure network will not protect you from a weak application.

- **External Testing**

This is a typical method of testing; it simulates an attacker trying to break into your systems from the outside, directly on the Internet. Gathering information about your company, and performing standard scans against Internet facing equipment, is in summary of what this type of testing involves.

- **Internal Testing**

Very similar to external testing, with the exception that the scans take place from within your network. This will give you an idea as to how vulnerable your systems are from attacks originating within your organization. These kinds of attacks could be launched from a disgruntled employee, a compromised internal system or user account.

- **Social Engineering Testing**

Social engineering is quite popular with attackers of all sorts including typical computer hackers. Social engineering is the act of tricking persons into revealing, or doing things that they may normally not do. An attacker may use social engineering to directly get the information that they want, or to gather additional information to assist with an attack at a later date. While this is not a technical test as the others are; this is more of a test of staff, and security policies.

• **Wireless Testing** Wireless technology such as 802.11 as becomes increasingly cheaper and easier to implement. Because of this security is easily forgotten about with these devices. Tier3 owns surveys in the past that have revealed that 60% of wireless networks are wide-open. A wide-open wireless network can allow anyone with just a laptop and wireless card to access your network. Securing your wireless network devices will make sure that only authorized persons are using your resources, and accessing your information.

Why we are good at it? - Our approach to penetration testing

At **Tier3 Cyber Security Services Pakistan,** we are not your average pen testers carrying laptops with pre-loaded software ready to print standard reports for your company. We understand Security is a very personal and private thing for our clients and we provide them with consultation and services which give them confidence in their security posture.

We perform our testing primarily from the attacker's point of view.

Meaning we don't just run a couple of scanning applications and give you the canned report from these tools. We combine that information with observations, and other information that we can find about your hardware, software, and organization just like a real attacker would.

Using all of this information we try various methods of accessing information. These methods have revealed several undocumented bugs in software, and security issues that our customers (and our selves or sometimes even the software vendor) were not aware existing. This is often referred to in the penetration testing business as "black box testing". "Black box testing" gets its name because no knowledge about the systems in place is given the team performing the testing.

The opposite of this is "White box testing", where diagrams and documentation of how internal systems work, operate, and are supposed to function are provided to the testing team so that they have complete knowledge of the network and systems.

While "black box testing" might give us a good idea as to what an attacker might be able to compromise and gain access to, it is not a 100% accurate picture. We don't forget about the possibility of internal staff performing an attack. This is what "White box testing" is designed to reveal.

Each form of testing reveals things that the other might not. We always recommend that our customers have us perform both forms of testing to give them a truly accurate representation of their attack risks.

Tier3 follows standardized approach of penetration testing execution standard (PTES) and all above mentioned tests include following main sections.

- **Pre-engagement Interactions**
- **Intelligence Gathering**
- **Threat Modeling**
- **Vulnerability Analysis**
- **Exploitation**
- **Post Exploitation**
- **Reporting**

Reports – Vulnerabilities and Recommendations

This all depends upon what kind of testing you have us perform, but you can expect to have a detailed report listing what we uncovered, bugs, exploits, ports open, and vulnerabilities found, etc. for each application, server and networking device we were authorized to test.

After a careful assessment of technical information on what we have found, we provide an action list of what should be done to correct these issues. This action list is clear and straight forward, and will give you what you need to start correcting your security weaknesses immediately.

We can also adjust our report to include or exclude any information that you may want like extra load balancing tests. Some companies only want an action list, while others might want an executive summary, or just technical information of what was found.

Our reports are in accordance with penetration testing execution standard (PTES).

Money Matters - Pricing / Packages

In realm of cyber security it is always hard to have a solution that suits all and many, and it is highly difficult to put a set price tag for Pen testing services as these packages are always bespoke and tailored exclusively to meet our client's requirements. It is one of the main reasons most providers are reluctant to publish their fees for penetration testing.

Please find below a tentative pricing for different Pen Testing Approaches.

S.No	Type	Description	Starting Prices
1.	External Network	Security vulnerabilities on the network layer and host configuration vulnerabilities, limit of 64 IP addresses and 2 subnets.	2,00,000 Rs
2.	Internal Network	Security vulnerabilities on the network layer and host configuration vulnerabilities, limit of 64 IP addresses and 2 subnets.	3,00,000 Rs
3.	Web Application	Single web application, in conjunction with an external or internal network penetration test. All extensions of application like databases, servers and other connected system and apis etc will be tested too.	1,50,000 Rs
4.	Social Engineering	Remote social engineering test, including Five separate electronic attack vectors including spear phishing email, Social network attack and Vishing Phone calls directed at human targets within your organization	3,00,000 Rs
5.	Wireless	One wireless access point and associated client devices.	2,00,000 Rs

Final Pitch – Conclusion

At Tier3 we don't just believe in making a difference. We believe in making the difference.

In an evolving digital world, protecting information and the infrastructure and applications that support it is becoming increasingly challenging. Hackers are becoming more sophisticated while technologies such as mobile devices, cloud virtualization and collaborative tools create vulnerabilities and can leave businesses exposed.

Our people are experts in a wide range of industries and we bring in specialists from across our firm to ensure our clients receive the best service.

Our clients choose us for Cyber Security services in Pakistan because we challenge convention to find the solutions that really work – in practice, not just on paper.

Then we roll up our sleeves and get the job done.

Our qualified consultants are experienced in helping businesses of all sizes to identify their risks and implement a robust security protocols. We have consultants from both ISO and more technical backgrounds including CLAS and CISSP, to ensure your business gets the expert support it needs.

If there are any more question and queries please feel free to contact us on **info@tier3.pk**.

Cyber Security Tools & Partners