Penetration Testing: is a great way to discover where your business security fails

Md. Mushfiqur Rahman

Information Security, Penetration testing and Risk Practitioner

Information system auditing, vulnerability assessment and penetration testing is become essential to secure the information and systems which are using in the business. To beat a hacker, we need to havethink like a hacker. Penetration testers analyze network environments, identify potential vulnerabilities, and try to exploit those vulnerabilities (or coding errors) just like a hacker would. In simpler terms, penetration tester tries to break into your company's network to find security holes.

The Bank, telecom, corporate companies requires both an internal and external penetration test, to secure their Information systems. Penetration testing isn't limited any company can request a penetration test whenever they wish to measure their business security.

Vulnerability

Vulnerability assessment is the process of identifying weaknesses and quantifying security vulnerabilities in an environment. It is an in-depth evaluation of your information security posture, indicating weaknesses as well as providing the appropriate mitigation procedures required to either eliminate those weaknesses or reduce them to an acceptable level of risk.

Penetration Test

Penetration Tests are designed to achieve a specific, attacker-simulated goal and should be requested by customers who are already at their desired security posture. A typical goal could be to access the contents of the prized customer database on the internal network, or to modify a record in an HR system. There are different tools and techniques, the penetration tester attempts to exploit critical systems and gain access to sensitive data.Depending on the scope, a pen test can expand beyond the network to include social engineering attacks or physical security tests. Also, there are two primary types of pen tests: "white box", which uses vulnerability assessment and other pre-disclosed information, and "black box", which is performed with very little knowledge of the target systems and it is left to the tester to perform their own reconnaissance.

Benefits of penetration test – With the growing frequency and complexity of cyber-attacks, more and more companies are investing in a penetration test. A penetration test is a small cost compared to the disruption caused by a cyber-attack. Here are some benefits of undertaking penetration testing:

Protect company's profits and reputation – by avoiding financial disaster and negative publicity associated with a compromise of the systems.

Satisfy regulatory requirements – Penetration testing is the regulatory requirements as well in different countries and industries require penetration testing to comply with the regulation to secure the business and client's information.

Protection against compliance breaches – VAPT assure business is compliant with regulatory requirements and ensure avoidance of regulatory fines and potential law suits.

Vulnerability scanning and penetration testing are different

Some people mistakenly believe vulnerability scanning or antivirus scans are the same as a professional penetration test. Even some companies tout 'penetration testing services' when in fact, they only offer vulnerability scanning services. An external vulnerability scan is an automated, affordable, high-level test that identifies known weaknesses in network structures. Some are able to identify more than 50,000 unique external weaknesses.

Cost of a penetration test

With any business service, cost varies quite a bit based on a set of variables. The following are the most common variables with regard to penetration testing services:

Complexity: the size and complexity of your environment and network devices are probably the biggest factors of your penetration test quote. A more complex environment requires more labor to virtually walk through the network and exposed web applications looking for every possible vulnerability.

Experience: pen testers with more experience will be more expensive. Just remember, you get what you pay for. Beware of pen testers that offer prices that are too good to be true. I suggest looking for penetration testers with credentials behind their name like CISSP, CISA, CEH, CHFI, CLPTP. LPT, CCISO, ISO – ISMS 27001 LA, CCNA, CCNP, OCP, SCSA, RHCE, MCSA, MCSE, CASP etc…

Penetration tests are worth it, every time: If you think that price is unreasonable, think of this. A hacker only has to find one hole to get into your network and steal data. A pen tester works hard to find as many holes as possible that could allow you to be compromised. You are paying a professional to look through every nook and cranny of your business to find each possibility of compromise. There is no better way to test the actual effectiveness of your security systems than by the skills of an experienced penetration test team.

Become a Good Penetration Tester / Information System Auditor: It is important to consider different issues beyond raw technical knowledge that make a good tester. It's key to remember again that Penetration testing is not 'hacking' and although there is a place for the borderline-autistic who hacks on their neighbors' wireless. Again, I've added a bullet pointed list to describe some of what I consider key attributes of good and great testers.

Good knowledge of networking and network protocols –A penetration tester must have knowledge on networking it's protocols, routing, switching and Firewall, IDS, IPS systems.

Learn some basic scripting. Start with something simple like vbs or Bash. As a matter of fact, I'll be posting a "Using Bash Scripts to Automate Recon" video tonight. So if you don't have anywhere else to start, you can start there! Eventually you'll want to graduate from scripting and start learning to actually code/program or in short write basic software (hello world DOES NOT count).

Learn a little about databases, and how they work. Go download oracle, db2, MS SQL server, mysql, read some of the tutorials on how to create simple sample databases. I'm not saying you need to be a DB expert, but knowing the basic constructs help.

Always be willing to interact and share your knowledge with like-minded professionals and other smart people.

As part of the penetration test, the organization should assess the ability of its staff and systems to identify and respond to an ongoing attack. At the conclusion of the test, the testers should be thoroughly debriefed by the organization's information security staff and should work in cooperation with security staff to identify key weaknesses, based on risk, and develop a detailed mitigation and remediation plan finally submit the report and follow-up regarding the implementation and mitigation task which are recommended by the tester / auditor ◙