Defcon-5

Penetration Testing

9430 Rapidan Dr.
Fredericksburg, VA 22407
(540) 455-7609

What kind of penetration testing do you need?

- Application Security Testing
  - Applications are the core of your business, without them you 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 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 become increasingly cheaper and easier to implement. Because of this security is easily forgotten about with these devices. Defcon-5 as done 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.

Defcon-5
9430 Rapidan Dr.
Fredericksburg, VA 22407
(540) 455-7609

Our approach to penetration testing

We perform our testing primarily from the attackers 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 ourselves, 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 you a good idea as to what an attacker might be able to compromise and gain access to, it is not a 100% accurate picture. 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 recommend that our customers have us perform both forms of testing to give them a truly accurate representation of their attack risks.

What kind of report can you give us?

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, ports open, and vulnerabilities found, etc. for each server and networking device we are authorized to test. After each server/device's technical information on what we 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 want. Some companies only want an action list, while others might want an executive summary, or just technical information of what was found.

Some companies may charge you to present their report to you, we do not believe in this. We believe that if you have any questions regarding our reports that we should provide you any answers that we physically can.