**Wireless Network Penetration Testing and Security Auditing**

**What is Wireless Network Penetration Testing?**

Wireless Network Penetration Testing is a method of testing wireless networks to expose any security vulnerability. It is also known as external network-based wireless penetration testing and wireless auditing. Wireless penetration testing includes both the practice of finding vulnerabilities in a wireless network and exploiting them to gain access.

**What are the Wireless Penetration Testing Methodology and Techniques?**

The wireless penetration testing methodology and techniques apply the same as those used by professional auditors for traditional network penetration testing. Penetration testing (or pen-testing) is an attempt to circumvent network security in order to discover any exploitable vulnerabilities that would allow the attacker access into the network. The process typically begins with some form of reconnaissance, during which an attacker looks for information about possible targets, devices used on the network, and possible attack vectors.

Once reconnaissance has been performed, vulnerabilities are identified and exploited. This step often involves analysis of the target environment for possible attack vectors, such as insecure protocols or misconfigurations that might allow access to a system or open services (for example - dynamic routing protocol authentication issues).

Once an exploitable vulnerability has been discovered, the penetration tester would use social engineering techniques to take advantage of the vulnerability in order to gain access to the target environment.

**Importance of Security Auditing**

The importance of auditing wireless networks cannot be understated. Whether you are self-employed or work for a small company, penetration testing can help your business in patching vulnerabilities before criminals do. Criminals have the means to launch sophisticated attacks, so it is important that you protect yourself by performing penetration tests at regular intervals. Penetration testing is also an important step in making sure your business complies with regulations like PCI DSS, HIPAA, or FISMA.

**How do I determine if my wireless network is vulnerable to attack?**

One of the best ways to find out is by performing a penetration test on your own wireless network. Penetration testing tools exist that can be used to discover some of the vulnerabilities, but it is important to understand that no tool can protect you from your own bad security practices. As such, be careful about what attacks you attempt at home or in the office.

**What Penetration Testing Tools are Available?**

There exist a number of tools designed for performing Wi-Fi penetration testing and security auditing. However, most of these tools are designed for experienced security professionals and the scope and features vary widely.

- **Kali Linux**

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing purposes. It provides all of the tools built into BackTrack but adds a number of additional open-source packages as well as a slightly different focus. Kali is designed for advanced penetration testing purposes and is not intended to be simple or easy to use, but rather provides the best tools in one common operating system that you can run on an everyday computer (even a netbook) or inside of a virtual machine.

- **Aircrack-ng**

The project website for Aircrack-ng contains complete installation instructions for all operating systems it has been ported to.

- **Wireshark**

Wireshark is an open-source network protocol analyzer for Unix and Unix-like operating systems (BSD, Linux, OS X, Solaris). It is one of the most popular network analysis tools in the world, capturing packets from a live network and displaying those packets using a GUI.

- **Wifite**

Wifite is a new automated wireless attack tool. It is an easy-to-use wireless auditing tool that automates hand-picked wireless attacks to discover vulnerabilities in your network. Wifite uses aria2 to download the necessary packets from online repositories. Targets can be from a text file, stdin, or discovered automatically. It currently supports cracking cracks WEP/WPA handshakes and running a number of different de-authentication attacks against clients.

To know more Click here: Wireless Network Penetration Testing and Security Auditing