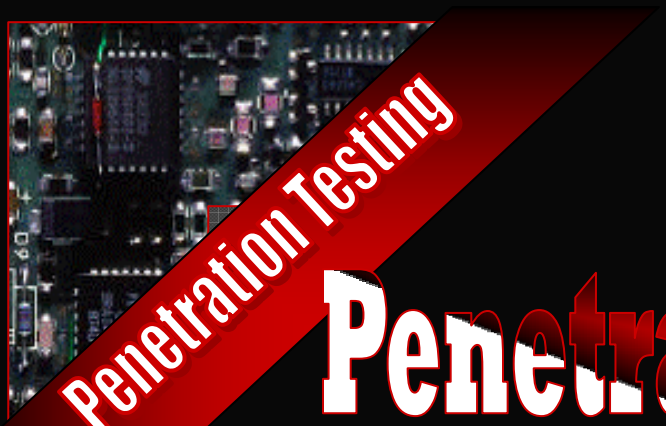

Penetration Testing

Penetration Testing

Snapshot in time attack against your company's network

Our highly skilled team of network penetration engineers act like a team of hackers. We perform what is known as a *snapshot in time* attack against your network. This means if we find weaknesses or vulnerabilities against your current network configuration it is only valid until your next configuration change.

It is recommended that companies have penetration testing performed every quarter. Even if configuration changes are not taking place, new vulnerabilities may have been discovered since the last test period.

Our penetration test engineers specialize in performing open source data collection against a network before running tools against a network. Most penetration test teams fail to perform a thorough information gathering phase prior to penetration testing which may impede the overall effectiveness of the teams ability to cover all areas of a company's network.

Our penetration test engineers work under strict "ethical hacking" guidelines which help protect customer information when a vulnerability is discovered and protects client data from being exposed to the internet. When a serious vulnerability is discovered during testing the penetration test team will contact the system administrators and help them tighten down the problem as soon as possible.

All penetration testing is performed on a case by case basis. Ideally, we like to perform this testing on a test network with non-critical data. Discussions with the customer will help our team best decide or recommend how the testing should be accomplished. We can perform testing late at night so your daily activities are uninterrupted or we can perform testing without the networking staff being told which will add the element of a real world attack to the situation.

For more information, please call the Futures Inc team today to discuss your company's options. We look forward to hearing from you.

FUTURES inc.