Security Analysis

Contributed by RedOracle

RedOracle - Security Analysis

Information Protection is the key tenet in enabling organizations to develop and maintain a competitive edge. Protection of this information enables the organization to develop, grow, and increase revenue, through the belief that their critical knowledge and information systems are secure from prying eyes.

Organizations will often spend significant effort in ensuring the physical security of their environment and protection of their information. It is often the electronic environment is often left out of the protection loop.

As a result, organizations often leave themselves exposed to brand damage and potential liability through insufficient care and attention to their external systems.

{xtypo_quote}A RedOracle Network Intrusion Test will show our clients where they are vulnerable and provide a prioritised, risk based recommendations to improve the security of the systems under review.

RedOracle's approach to Network Intrusion Testing is based on the recognition that every client of ours is different.Our approach typically includes a combination of configuration assessments, automated network scans and manual penetration attempts.
This approach offers a far more detailed examination of our clients IT systems than a simple vulnerability scan.{/xtypo_quote}

A Network Intrusion Test uses a vulnerability scan merely as a starting point for detailed exploitation attempts. RedOracle believes that to provide real value to our clients, attempts should be made to exploit these vulnerabilities.

This provides our clients with a real indication of the problems that they could encounter in the event of an actual attack. Research has shown that around 70-80% of security incidents originate within the organization, and hence Internal testing is just as important as External testing.

A reasoned diagnosis of the organizational and techno-methodological statement of the IT Security System; comparision of the sector's best practises and intervention recommendations.

Security assessment of:

- Web Applications

- Web services

- Proprietary protocols and applications

- Client/server applications
- Network â€“ Internet/Extranet/Intranet audits

Key features of our services include:

Security Policy Compliance

We can identify issues and problems with the implementation of the security policy as it applies to the organization being tested.

Quality of Service:

RedOracle experts scrutinize the reports to add additional value where possible. This is a significant improvement in quality above that available from other service providers.

Risk Management:

Network Intrusion Testing is an important tool in the arsenal of protection against malicious hacking. Penetration Testing can provide an ongoing confidence in the integrity of the environment at least cost, and with maximum benefit.

Reduction in TCO:

Providing this level of service by internal personnel is costly to develop and maintain. Through scalability and a dedicated expert resource base, RedOracle provides an ongoing service with higher levels of quality and service than would be sustainable internally.

Useful Reports:
The Network Intrusion Testing report format is tailored to cater for all customer levels, from the executive level through to the technical team. The reports expand to include easy to understand details on the vulnerabilities found, including severity, risk, and suggested fixes.
Follow-throughRedOracle has industry leading security and network consultants that back up and support the Network Intrusion Testing service, including provision of expertise, resources, and solutions as required, to help resolve

vulnerabilities and issues identified in the testing.

{xtypo_rounded4}Vunerability Assessment vs Penetration Test

Vulnerability assessments are designed to only identify security issues within the client infrastructure.

Exploitation of discovered vulnerabilities is generally out of scope for these assessments.

Vulnerability assessments tend to provide wider coverage of a client's environment, without the considerable depth.Penetration tests are designed to effectively illustrate the insecurity of particular components.

They extend the discoveries made during a vulnerability assessment by exploiting discovered problems to gain privileged access and or take "trophies" such as password files or user data as proof of entry.

Penetration testing tends to be more time consuming and have a relatively higher cost per system than vulnerability assessments.{/xtypo_rounded4}