

VULNERABILITY SCANNING

- Conduct an initial meeting to understand the company's current configuration and security needs.
- Create a scanning profile for all devices on the network. This could be a basic scan or a deeper, more robust scan using a valid ID and password, or a full scan, to include brute force, denial of service, etc. The scan would include Operating System, application(s), policies, and security configuration vulnerabilities.
- Assess and prioritize the results of the scan vulnerabilities by the importance of the devices / data to the company.
- Deliver management and technical level reports, and provide assistance/guidance on the creation of enforceable policies.

PENETRATION TESTING

External Penetration Tests are usually carried out without any knowledge of the internal workings of the network. The penetration tester will carry out information gathering, scanning and probing, vulnerability assessment and exploitation by targeting devices such as web servers, routers, firewalls, email servers, DNS servers, and VPNs, without prior knowledge.

Internal Network Penetration Tests are usually carried out as if the tester were an insider, (employee). The penetration tester has detailed knowledge of the network and the environment such as web servers, routers, firewalls, email servers, DNS servers, and VPN.

Security Vulnerability assessment is vital. We will provide an Executive Summary, with a non-technical explanation of the impact and likelihood of more serious issues. Additionally, we will show you how to reduce the potential risk to your systems, with recommendations for system upgrades, configuration changes, and day-to-day policy changes.

RISK ANALYSIS

Even if your systems are patched, your applications upgraded to the latest level, your firewall configured correctly, and you are using strong encryption on data and email transmissions, you can still be at great risk if your day-to-day processing and procedures are not secure. A risk analysis can be performed and would consist of:

- Review of day-to-day processing with staff, including how data is received, processed, stored, and secured, strictly from a security perspective.
- Review how data is imputed (web site, data transmission via other sources); is it protected while being processed? Is it secured at day's end?
- Review how passwords and access to data are being handled (password sharing, weak passwords, shared files, etc.)
- Is your staff "security aware?" Do they have a strong security policy to follow? Is security education provided to the staff?
- How is the data stored? Are there strong backup procedures and safe storage of the files? Are permissions set correctly, and driven by critical nature of the data?



Services provided in partnership with McLean Security, LLC

