Penetration Testing

Protect
Service

OVERVIEW

Networks are under constant attack by individuals motivated by financial gain, political gain, intellectual challenge, or just mischief.

The most accurate testing methodology is penetration testing, sometimes referred to as "ethical hacking". Using commercial, open source, and proprietary tools, skilled vulnerability researchers will use the same techniques that a hacker would use to assess your network's security. By taking on the role of an outside hacker or a disgruntled employee, testers will: (1) demonstrate how the network was compromised, (2) prove that an actual compromise took place, and (3) provide real information on how to mediate against future attacks of this type.

DigitalDefence testers use both vulnerability scans and penetration testing to provide the most accurate view of network security, resilience of the network, and the survivability of your data when faced with an attack.

BENEFITS OF REGULAR PENETRATION TESTING

- Identifies vulnerabilities and allows you to focus on those that are the most critical to your specific network—provides proof of real threats to your data's security—compelling evidence for management action!

- Prevents financial loss—a security breach for even a small company can incur significant costs, including recovery costs, lost revenue, reduced employee productivity, and intangible costs, such as a damaged reputation

- Supports vulnerability management—provides detailed information on the presence of actual and potential vulnerabilities, allowing you to plan expenditures and allocate resources for patching or mediation

- Proves due diligence; satisfies regulators, shareholders and investors, and clients that you are providing the highest degree of security to their data

- Ensures regulatory compliance under frameworks such as ISO 27001, PCI DSS, HIPAA / HITECH; required for many insurance policies

Improve corporate risk reduction with strategic security and privacy services.

Is the Penetration Testing Service right for your company?

- Have you validated the secure operation of your network's firewalls and other security devices?

- How effective are your network and operational controls against a determined attacker?

- Can you prove the security of your network and its data to an independent auditor?

- Are you required to assess network security to remain PCI compliant?

SERVICE DESCRIPTION

The scope and breadth of DigitalDefence network and system security tests are specifically tailored to client networks. Using a proprietary methodology, the service will include some or all of the following:

- Interviews with key stakeholders, including a review of relevant policies, procedures, and other documentation
- On-site physical security inspection of the network, key facilities (data centres, wiring closets,)
- Review of administrative, physical, technical, and logical controls
- A vulnerability scan of the target network to map out the test space, identify basic vulnerabilities, focus additional testing
- An external penetration test (attempting to break into the client network from the public Internet or across a remote connection such as wireless, VPN, or phone. This testing may be done with no knowledge of the underlying infrastructure or configuration ("black box" testing)
- Internal network and host assessment, based on full knowledge of all network components, configurations ("white box" testing). This is the most effective technique for finding vulnerabilities and maximizing the return on your investment
- Advanced testing of network components, including: wireless networks, voice over IP, virtualized environments, "cloud computing" configurations, SCADA, etc

To support our testing against increasingly complex networks, Digital Defence will also customize its own attack tools and exploits. We also conduct extensive vulnerability research in our own Trial and Evaluation laboratory to ensure that testing is accurate, and that there is minimal disruption to your network during testing.

Once the network or application has been compromised, and Digital Defence has demonstrated that an exploitable vulnerabilities exists, we provide a comprehensive report that details (1) the vulnerabilities identified, including proof of exploitation, and (2) the step-by-step process to mediate the weakness that is most appropriate for your organization.

When to Test Your Network's Security

Although many organizations test their networks on a semi-annual or annual basis as part of their regular security program, additional testing may be required when:

- A confirmed or suspected security breach has occurred
- Satisfying regulatory requirements (PCI DSS)
- Implementing new technologies (wireless, VoIP)
- Introducing new critical applications, especially those with connectivity to third parties or untrusted networks such as the Internet
- Actual evidence of an exploitable vulnerability is required
- Terminating employment of individuals with privileged access levels

About Digital Defence

Digital Defence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss.

Digital Defence Inc.
Toll-Free 800-385-1632 | Tel 519-771-8808
info@digitaldefence.ca | www.digitaldefence.ca