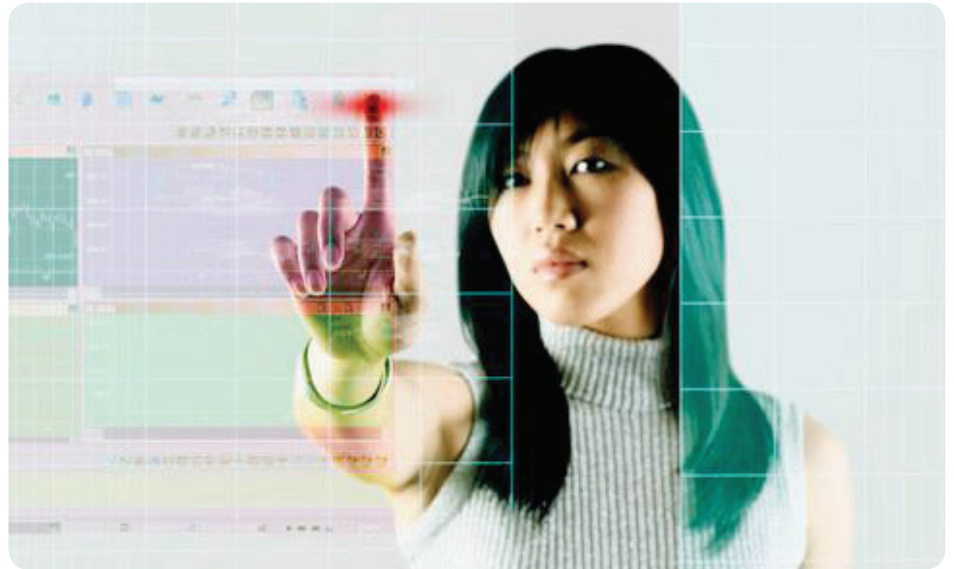




SecureWorks



## Penetration Testing

**Regular penetration testing is a recognized best practice for any information security program. Third party penetration testing is mandated by PCI DSS and satisfies requirements for GLBA, HIPAA, SOX, NERC CIP and FISMA compliance.**

### Service features

- Obtain a true understanding of your security and risk posture
- Leverage our deep knowledge base gained by delivering services to thousands of customers
- Understand the techniques used by attackers
- See your organization as it would be seen by a cybercriminal
- In-depth reporting, relevant to your organization and stakeholders
- Comply with industry regulations and information security best practices

### What is a penetration test?

A penetration test determines how well your organization's security controls protect your assets from a direct Internet attack. In this testing, we try to gain access to your network and information assets in the same way a hacker would. A penetration test is beneficial because it allows you to identify the extent to which your network could be compromised by an external malicious attacker, so that you can strengthen your defenses and prevent a successful attack from occurring. Only a real penetration test by an experienced professional can simulate what would happen if a determined hacker were to attack your organization.

Dell SecureWorks has deep expertise in attacks and exploits used against mission-critical assets, through monitoring and protecting the networks of thousands of customers. The Dell SecureWorks attack database contains more than 1 billion attacks that we have prevented. As a result, when we conduct a penetration test on your network, we know what attacks are out there and which are the most commonly used against organizations like yours. Our tests are finely tuned using this unique, global expertise, which translates into a more focused and relevant penetration test.

### Penetration testing methodology

Dell SecureWorks uses a multi-phase process to find and exploit vulnerabilities in your network. We use scanning tools to automate repetitive and time consuming tasks, and use manual techniques for tasks which require deeper insight and situational context. The key is a judicious mix to maximize efficiency. Network testing may include firewalls, routers or other network infrastructure devices, intrusion detection and prevention systems, Web servers, email systems, and virtual private networking (VPN) systems. We use a combination of commercial and publically available tools, as well as custom scripts and applications.

### Discovery

It is important to obtain as much information as possible about the target organization within a reasonable period of time. This step uses largely non-invasive reconnaissance to identify the footprint of the target organization or network range. During this step we will use publically available databases, search engines and other open source intelligence gathering tools and techniques. Results from these activities vary across

organizations, but the goal is to be able to identify as much as possible about your external network and to see your Internet presence as a true attacker would.

### Enumeration and vulnerability mapping

Following the discovery phase, Dell SecureWorks will perform more interactive and invasive reconnaissance of the target hosts. The tester will use a variety of tools to manually interact with the hosts, and obtain more detailed information on the target environment. They use this to map the profile of your environment to publicly known or, in some cases, emerging vulnerabilities. Dell SecureWorks has a dedicated Counter Threat Unit<sup>SM</sup> research team, which is constantly combing the “blackhat” community for new and emerging vulnerabilities and attack techniques.

### Exploitation and penetration

The goals of exploitation are to gain user-level and privileged access to your systems. The penetration tester will employ a variety of real-world tactics used by cybercriminals to attempt to gain access to your organization’s sensitive information. Testing can include attacks such as buffer overflows, SQL injection, cookie tampering, router exploits, operating system specific exploits, and attacks specific to custom coded applications. The key to this phase is manual testing. No automated tool can replicate the processes of an experienced penetration tester skilled in the art.

### Documentation and reporting

During the project, Dell SecureWorks will thoroughly document all activities so that we can provide relevant information and evidence to support our conclusions. This may include screenshots, code snippets, logs and other data collected during testing. We will provide a preliminary draft report to your technical point of contact for review and clarification, followed by a final report at the conclusion of testing. The report will include:

- **Executive summary** – A jargon-free, true executive-level summary of the project.
- **Penetration testing results** – This section describes the degree to which Dell SecureWorks was able to penetrate the environment and the vulnerabilities that were exploited.
- **Findings and recommendations** – The report describes the environment, findings, and recommendations based on risk to your organization.
- **Summary of methods** – This section contains details specific to the engagement methodology.

## Why Dell SecureWorks?

### We know the real threats

Dell SecureWorks provides Managed Security Services to thousands of customer around the world. We observe more than 13 billion events every day and continuously monitor security events and attacks across these networks. Our Counter Threat Unit research group is frequently first to market with the identification of new threats, exploits and attack techniques. Information sharing between our Security Operations Center analysts, Counter Threat Unit researchers and Security and Risk consultants enables each group to perform even more effectively. This level of visibility across the security landscape allows us to identify real, not just theoretical, risks to your business.

### We only hire seasoned security professionals

Recruited from diverse backgrounds including military, government, law enforcement, research and development, and private industry, Dell SecureWorks’ consultants are premier professionals committed to helping you achieve your security and business objectives. Our consultants are among the most technically proficient in the industry. We also place strong emphasis on our consultants’ ability to communicate effectively with all audiences, from engineer to auditor to board of directors.

### We will reduce your overall risk exposure

Our expert security professionals who understand the real risks can help your organization prioritize any remediation efforts that need to be made to secure your infrastructure. This guidance can save you time and effort as you determine the most effective means to mitigate or accept the identified risks. Dell SecureWorks is available for up to one year to provide additional support for findings and recommendations, or any remediation efforts.

