



Today's businesses, schools and government institutions are increasingly sensitive to cybercrime attacks and customer identity theft by hackers. Most have databases of confidential information, and most conduct e-commerce with customers and other enterprises. Security breaches such as identity theft and fraud have far-reaching impacts—ranging from remediation costs and damages payable to victims, to the inestimable toll of negative publicity and lost business.

The High Price of Cybercrime

The **Federal Bureau of Investigation** conservatively estimates that cybercrime causes more than \$120 million in damages annually, but that only 9% of cybercrime is even reported. That puts the total cost of the problem at a staggering \$1.33 billion each year. And concern isn't confined to the FBI. A July 2007 report by the **Federal Trade Commission** confirms that email spam has become a significant global tool in the propagation of financial crimes.

Widespread Vulnerability

Hackers may come in all shapes and sizes, but they share one mission. They aggressively scan networks in search of vulnerabilities they can exploit to gain access to your most prized asset—your data.

A simple error like a misconfigured firewall can expose your internal network to millions of unauthorized users. A single hacker can embarrass your organization by defacing your website, crashing servers or selling corporate secrets.

It is no longer a question of whether you will face such threats—but how effectively you will be able to deflect them when they arise.

A Solution That Works For You

SECNAP® External Penetration Testing Services are a vital step in securing your assets, by helping you to identify and resolve network vulnerabilities before they become security breaches.

Thousands of automated tests are performed on each printer, router, firewall, and web and email server on your network to determine whether the devices are fortified against external penetration or require remediation. Some of the current tests are listed on the reverse side.

Additional tests are incorporated weekly as our unique Edge Attack Sensor Network, using more than 20,000 probes in 50 countries around the globe, discovers and documents new threats and develops appropriate tests to identify them.

Useful Reports, Actionable Recommendations

On completion of the extensive SECNAP test battery, we deliver a comprehensive report documenting vulnerabilities and their potential for abuse. Specific remedial actions are recommended, and prioritized so that your IT team can address the most significant vulnerabilities first. By leveraging these testing services on a regular basis, you can help ensure the most current protection for your corporate assets.

What You Gain from Penetration Testing

Conducted by experienced SECNAP Network Security auditors, our External Penetration Testing Services are designed to:

- ***Provide an objective, expert view of your security landscape***
- ***Identify and prioritize vulnerabilities and risks***
- ***Outsource testing so that your IT staff continue to focus on their primary work***

SECNAP offers three levels of expert testing, with a goal of recommending improvements to better protect your most prized asset—your data. Isn't it time you put us to work for you?

866-732-6276



Three Levels of Penetration Testing

SECNAP® auditors and engineers perform up to three levels of testing, depending on your network requirements and cost criteria. From virtually transparent testing at Level 1, to tests which may be intrusive to your network at Level 2, to Level 3 testing that will impact your network and require resources, these tests are designed to reduce your exposure and improve your security profile. They pinpoint where your network is vulnerable to external penetration, and offer actionable remediation solutions that will result in strengthened protection of your corporate assets.

Hackers may come in all shapes and sizes, but they share one mission. They aggressively scan networks in search of vulnerabilities they can exploit to gain access to your most prized asset—your data.

Level 1: Testing and Monitoring Phase

These tests are conducted during normal business hours, use little bandwidth, do not require client involvement, and pose no risk of adverse effects on your network.

Investigative/Non-Intrusive Tests

- Scan/identify all open ports and identify all available services
- Connect and determine all operating processes
- Check every port—no exceptions or assumptions

Network Timing Tests

- Provide IP addresses to client so ISP can be notified of upcoming tests
- Test throughput and latency from multiple IP locations

Full Network Map (IP address and services assessment)

- Complete full port scan of every external IP on client network
- Catalog all servers and services on client network

External Vulnerability Tests

- Run suite of more than 5,000 external tests

Banner Tests

- Compare SECNAP database of thousands of known external vulnerabilities
- Identify all suspected vulnerabilities and document remediation actions for each

Level 2: Attempt Exploits Phase

Because this phase attempts to exploit remaining vulnerabilities, these tests may be intrusive to your network. They are conducted only with your approval and under the specific guidance of your IT department.

- Repeat Level 1 tests
- Attempt to load files and programs
- Run suite of more than 2,000 exploit routines

Level 3: Windows and Intrusive Test Phase

This level of testing is intrusive and will impact your network. These tests are performed only with senior management approval and with the direct supervision and cooperation of your IT staff.

- Attempt “Kill Host” tests
- Attempt Denial of Service (DoS) attacks
- Run suite of more than 100 Microsoft Windows tests
- Attempt Microsoft permission exploitation tests

SECNAP External Penetration Testing Services ensure that your network is tested professionally and comprehensively. Upon completion of our thorough test report, you will have a complete picture of current vulnerabilities along with the steps you can take to resolve them.

*It is no longer a question of **whether** you will face security threats—but how effectively you will be able to **deflect** them when they arise.*

866-732-6276

