

A Vital Component of Any Security Strategy

Cybercrime is not only relentless—it is staggeringly expensive, and it is accelerating. Most recent reports suggest that cybercrime costs U.S. businesses \$1.3 Billion annually, while global estimates place the worldwide cost at \$3 Trillion. Information security has never been more vital, especially for organizations entrusted with the personally identifiable information (PII) of customers, employees, suppliers and other stakeholders.

Most organizations maintain 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 SECNAP External Penetration Testing Program provides a thorough, repetitive, and affordable means of assessing external Client defenses in order to identify vulnerabilities and make informed remediation decisions—and in doing so help to protect Client network and information assets from the rising tide of cybercrime.

Tools & Expertise

More than 45,000 automated tests are performed on each, router, firewall, web and email server and other network devices on your network to determine whether the devices are fortified against external penetration or require remediation.

Additional tests are incorporated into the test battery constantly, as the unique SECNAP Edge Attack Sensor Network deploys thousands of probes in more than 60 countries to discover and document new threats, and develop appropriate tests to identify them.

On completion of the extensive SECNAP test battery, a comprehensive report is compiled to document vulnerabilities and their potential for abuse. Specific remedial actions are recommended and prioritized so that your IT team can address the most significant vulnerabilities immediately.

Leveraging these testing services on a regular basis can help ensure that you maintain the most current and effective protection for your information and network assets.

Features & Benefits

As the central core of all business transactions, information is an integral asset to be tightly guarded and effectively protected. Monthly External Penetration Testing is recommended for several reasons: (1) organizations add new network devices frequently, (2) SECNAP updates its suite of tests routinely in order to include new and emerging threats, and (3) cybercriminals are constantly developing new attack vectors and threats. Conducted by experienced, certified SECNAP Network Security auditors, our External Penetration Testing services are designed to:

- *Provide an objective, expert view of your external security landscape*
- *Identify and prioritize vulnerabilities and risks to enable you to allocate IT resources*
- *Provide actionable recommendations to facilitate delegation of remediation activities*
- *Enable your IT staff to maintain normal operations and focus on mission-critical work.*

External Penetration Testing

External penetration testing consists of remote scans and tests generated from the SECNAP Secure Operations Center (SOC) to determine if known vulnerabilities can be detected in Internet-facing hosts. External penetration testing is an integral part of any security program.

SECNAP external penetration testing includes:

- *Automated scans* with tests for:
 - Open ports and inappropriate services
 - Operating system vulnerabilities
 - Known web server vulnerabilities
- Manual probes, which may include:
 - Verification of vulnerabilities detected
 - Use of “black hat” tools

This scanning incorporates tests that address more than 45,000 known vulnerabilities and weaknesses.

Tests will be configured to run in a non-destructive manner in order to prevent disruption of critical services.

They pinpoint where your network is vulnerable to external penetration, and offer actionable remediation solutions that will result in strengthened protection of your network assets.

Testing and Monitoring

These tests are designed to be non-obtrusive, use minimal bandwidth, do not require client involvement, and pose little to no risk of adverse effects on your network. The timing of network tests can be customized to accommodate client schedules.

This phase of testing includes the following activities:

- Scan/identify all open ports and identify all available services
- Connect and determine all operating processes
- Check every port—no exceptions or assumptions, and no random sampling
- Provide IP addresses to client so ISP can be notified of upcoming tests
- Complete full port scan of every external IP on client network

- Catalog all servers and services on network
- Run suite of more than 45,000 vulnerability tests
- Compare to SECNAP database of thousands of known external vulnerabilities
- Identify all suspected vulnerabilities and document remediation actions for each
- VoIP vulnerability testing
- Password testing
- Testing for malware and bots.

A Complete Picture of Your Network

SECNAP External Penetration Testing service ensures that your network is tested professionally and comprehensively, and provides a thorough test report that includes current vulnerabilities prioritized by severity and the actions you can take to resolve them.

*While external penetration testing is a vital element of any security program and a practical first step in the security process, we recommend a **complete IT security audit** in order to ensure that internal vulnerabilities are similarly discovered, prioritized and targeted for remediation.*

SECNAP also offers additional security audits, such as web application assessments, rogue access point detection, war dial and war drive, compliance audits and others.

Contact us for information about any of these services, or visit our website.

866-732-6276
www.secnap.com

