

## *A Vital First Line of Defense*

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.

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. SECNAP offers three levels of expert testing, with a goal of recommending improvements to better protect your most prized asset—your data.

---

### Tools & Expertise

More than 10,000 automated tests are performed on each printer, 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 more than 30,000 probes in 50 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. Only by conducting regular External Penetration Testing can an organization ensure that information and network assets remain safeguarded from unauthorized access and abuse.

Conducted by experienced, professionally 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*
- *Provide actionable recommendations*
- *Outsource testing so that your IT staff can continue to focus on mission-critical work.*

## External Penetration Testing

SECNAP auditors and engineers may perform up to three levels of testing, depending on your network requirements and budget. 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 network assets.

### Level 1: Testing and Monitoring Phase

These tests are conducted during normal business hours, use minimal 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 network

#### External Vulnerability Tests

- Run suite of more than 5,000 external tests

#### Banner Tests

- Compare to 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 delivery of our thorough test report, you will have a complete picture of current vulnerabilities as well as with the actions you can take to resolve them.

SECNAP also offers Internal Vulnerability Assessments, which we recommend deploying in tandem with External Penetration Testing. Together, these services provide a useful view of both internal and external vulnerabilities.

866-732-6276

[www.secnap.com](http://www.secnap.com)

