

## PENETRATION TESTING

How secure are you?

### Security System Effectiveness

Sound security consists of a system that integrates plans and policies, training, assessments, technology, and review to protect personnel and assets. Oftentimes reviews—such as exercises, tests, and audits—are conducted by company personnel, who may be blind to security deficiencies, and overlook a critical piece of the system. Many times, a security system can benefit from an outside review.

### A Mature Security System can Benefit from Penetration Testing

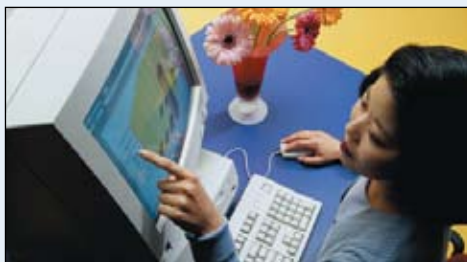
ENSCO has been conducting a variety of penetration testing methods since the mid-1990s; including open source collection, site surveillance, social engineering, electronic penetration, and physical penetration. Our process identifies vulnerabilities that can be exploited by an adversary, such as a corporate spy, a criminal, or a terrorist. In addition, we recommend workable countermeasures based on the knowledge we've acquired conducting assessments for more than 10 years on more than 100 targeted facilities and operations.

**The following activities are part of the ENSCO penetration testing process. They often occur in conjunction with one another.**

#### Open Source Collection

A plethora of information about an organization is often available on the Internet or from other publicly available sources.

Time and time again, we have discovered open source information (Internet data, overhead imagery, etc.) that reveals information an organization should protect. Our analysts use this freely available information, much as a criminal or terrorist would, to identify potential targets. Open source collection continues throughout the course of the assessment. In fact, subsequent collection activities often reveal additional avenues for open source collection.



#### Electronic Penetration

Often in conjunction with open source collection and site surveillance, our analysts conduct electronic penetrations. We do this by remotely accessing information or by “hacking” into computer systems to gain information and identify ways to deny, disrupt, or destroy operations.



#### Site Surveillance

Armed with open source information, ENSCO analysts conduct covert surveillance of the site to verify open source information, identify additional collection needs, and to develop attack scenarios.



#### Physical Penetration

A facility can actually be entered to ascertain information or identify

vulnerabilities. Physical penetration can occur in a variety of ways. For example, our analysts could climb a perimeter fence, enter through an unlocked door, or pose as a legitimate visitor.



#### Social Engineering

Social engineering is another technique for obtaining information. This approach uses various techniques including seemingly innocent lines of questioning to gain information. The information obtained is used for attack planning and identifying additional avenues for open source collection.

(continued on reverse side)



Innovation Starts Here

**CORPORATE HEADQUARTERS**  
3110 Fairview Park Drive, Suite 300  
Falls Church, VA 22042-4501  
703-321-9000 • 800-ENSCO-VA  
info@ensco.com • www.ensco.com

## The Nature of Penetration Testing

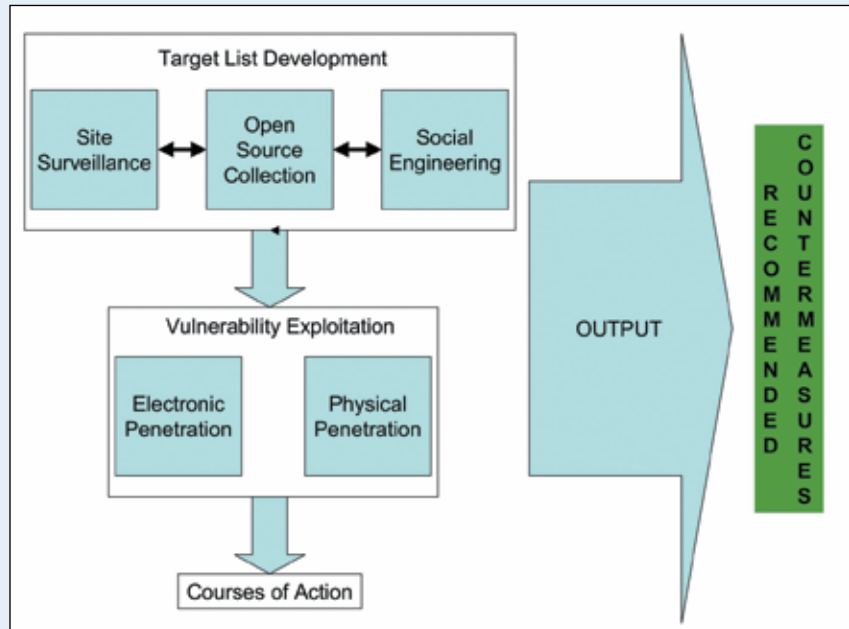
There are various legal and safety issues surrounding social engineering, electronic penetration, and physical penetration. Because ENSCO has been conducting such testing since the mid-1990s, we understand the issues and can work with your organization to minimize concerns.

Our security service experience pre-dates September 11, 2001 by many years. We've been evaluating security programs and providing solutions to make the world a safer place for more than 20 years.

With almost 800 employees, ENSCO is small enough to provide the personalized attention and responsiveness, yet large enough to have the trained and experienced staff and financial resources necessary to get the job done. You are never more than a phone call away from executive management, staff, or the president of ENSCO.

## Penetration Testing Products

At any point in the evaluation process, from identifying exploitable information obtained during a search of the Internet to validating computer-related or physical vulnerabilities, our team can generate a useable report. Our approach can tailor the output to the customer's requirements and budget and provide workable solutions to identified problems.



**For more information,  
please contact:**

Jim Byers  
Deputy Director,  
Security Services Group  
703.321.4607  
byers.james@ensco.com

Thomas Plutt  
Deputy APA Division Manager,  
Security Systems Group  
703.767.9736  
plutt.thomas@ensco.com

05.0160

EXPERIENCED, PROVEN, FLEXIBLE