

INFORMATION
TECHNOLOGY
FORENSICS

CONSULTING &
INVESTIGATIONS

▶ INFORMATION
SECURITY

PENETRATION TESTING

24 hours a day, 365 days a year, cyber criminals are stalking the Internet looking for vulnerable systems. Whether you have a small network of a few computers or a complex global network of thousands, your perimeter defenses are continuously being examined for weaknesses, and if found cyber criminals will exploit them.

OnlineSecurity's Penetration Testing Service provides organizations with an assessment of their perimeter security under real world testing conditions allowing them to patch holes before they are exploited.

Service Description

- ▶ OnlineSecurity's penetration testing protocols are based on the Open Source Security Testing Methodology (OSSTM) and rely on two types of attack.
 - Passive attacks do not directly influence or trespass upon the target but are often a form of surveillance and data collection.
 - Intrusive attacks do trespass upon the target and can potentially be detected, monitored, and logged.
- ▶ OnlineSecurity uses these general attack methodologies to evaluate the following four areas of the target environment and recommend security presence that should be securing the environment.
 - Visibility: what can be seen, logged, or monitored passively or intrusively within the target environment.
 - Access: entry points (including physical, cyber, or wireless) into the target environment.
 - Trust: access to specialized pathway into the secure target environment including but not limited to virtual private networks, backdoors, remote PC access programs, etc.
 - Alarm: assessment of client's response to activities that violate or attempt to violate the secure environment and gain visibility, access, or trust.

Delivery Mechanism

- ▶ OnlineSecurity will meet with the client to determine the scope and goals of the penetration test and prepare a proposal and/or work plan accordingly.
- ▶ As penetration testing is a measure of external security, the majority of the work will occur away from the client location. OnlineSecurity will be in constant communication with the client prior to and during the penetration test to assure that the testing has not affected the network performance in any way.

Deliverables

- ▶ OnlineSecurity will provide to the client a detailed penetration testing report encompassing systems tested, penetration methodologies utilized, vulnerabilities discovered and their implications for the organization, and recommendations to secure the organization.

Pricing

- ▶ Quotes for penetration testing are based on the specific considerations of the engagement, i.e. location, number of systems, scope of the assessment, etc. and will be priced by time and material required.
- ▶ Expenses are billed on a 'no- load' pass through basis, and Travel time is billed at 1/2 rate.



Los Angeles

5870 W. Jefferson Blvd., Suite A
Los Angeles, CA 90016
voice: 310.815.8855
fax: 310.815.8808

New York

Boston

Seattle