



## **Penetration Testing: Comprehensively Assessing Risk**

### **What is a penetration test?**

Penetration testing is a time-constrained and authorized attempt to breach the architecture of a system using attacker techniques. This form of testing relates the most accurate and comprehensive view of an organization's information security stance, as it evaluates an entire system, exploiting vulnerabilities to determine precisely how an unauthorized user can get control of valuable information assets.

The form of such a test depends greatly on the client's own situation. Tests can range from a brief overview of the security of an existing infrastructure, to an extensive simulated break-in, with the goal of obtaining specific information. Only a comprehensive penetration test can determine the real risk to network resources, thereby making it possible to immediately prioritize corrective measures and to set the overall direction for an organization's security strategy.

### **A penetration test can:**

- Show if installed security system is inadequate and can be bypassed and whether and how the system reacts to attack. This could help managers or IT persons in your company feel implicated.
- Reveal which information can be obtained from outside of the network.
- Put into test the security of an environment and qualify its resistance to a certain level of attack.
- Reveal whether it is possible to break into the system, using available or existing knowledge and which information becomes accessible, if the system is broken into
- In addition to a security audit: a penetration test can reveal security problems caused by some inconsistency between elements. Complex interactions are sometimes difficult to apprehend during an audit which focus on architecture, IP filtering, operating systems, web servers, and applications, one by one.

### **Why penetration testing: Why would you want it?**

There are several reasons why organizations choose to perform a penetration test; they range from technical to commercial but the most common are:

- Identify the threats facing your organization's information assets so that you can quantify your information risk and provide adequate information security expenditure.
- Reduce your organization's IT security costs and provide a better return on IT security investment (ROSI) by identifying and resolving vulnerabilities and weaknesses. These may be known vulnerabilities in the underlying technologies or weaknesses in the design or implementation.
- Provide your organization with assurance - a thorough and comprehensive assessment of organizational security covering policy, procedure, design and implementation.
- Gain and maintain certification to an industry regulation (BS7799, HIPAA etc).
- Adopt best practice by conforming to legal and industry regulations.



**What are the different types of tests available?**

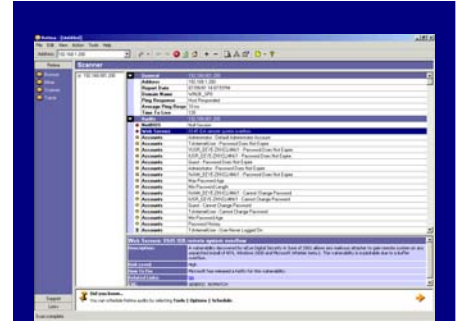
**External Penetration Testing** is the traditional approach to penetration testing. The testing is focused on the servers, infrastructure and the underlying software comprising the target. It may be performed with no prior knowledge of the site (black box) or with full disclosure of the topology and environment (white box). This type of testing typically involves a comprehensive analysis of publicly available information about the target, a network enumeration phase where target hosts are identified and analyzed, and the behavior of security devices such as screening routers and firewalls are analyzed. Vulnerabilities within the target hosts will be identified, verified and the implications assessed.

**Internal Security Assessment** follows a similar methodology to external testing, but provides a more complete view of the site security. Testing will typically be performed from a number of network access points, representing each logical and physical segment. For example, this may include tiers and DMZ's within the environment, the corporate network or partner company connections.

**Application Security Assessment** is designed to identify and assess threats to the organization through bespoke, proprietary applications or systems. These applications may provide interactive access to potentially sensitive materials, for example. It is vital that they be assessed to ensure that, firstly, the application doesn't expose the underlying servers and software to attack, and secondly that a malicious user cannot access, modify or destroy data or services within the system. Even in a well-deployed and secured infrastructure, a weak application can expose the organization's crown-jewels to unacceptable risk.

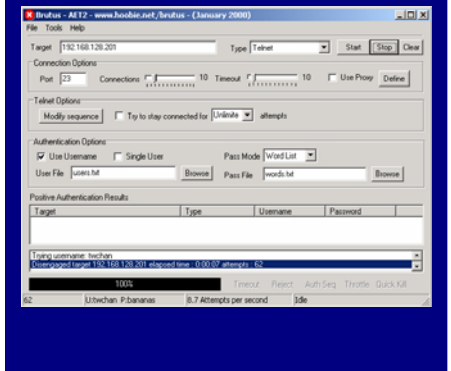
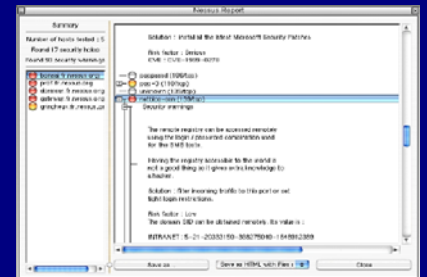
**Wireless/Remote Access Assessment (RAS) Security Assessment** addresses the security risks associated with an increasingly mobile workforce. Home-working, broadband always-on Internet access, 802.11 wireless networking and a plethora of emerging remote access technologies have greatly increased the exposure of companies by extending the traditional perimeter ever further. It is vital that the architecture, design and deployment of such solutions is secure and sound, to ensure the associated risks are managed effectively.

**Telephony Security Assessment** addresses security concerns relating to corporate voice technologies. This includes abuse of PBX's by outsiders to route calls at the targets expense, mailbox deployment and security, voice over IP (VoIP) integration, unauthorized modem use and associated risks.



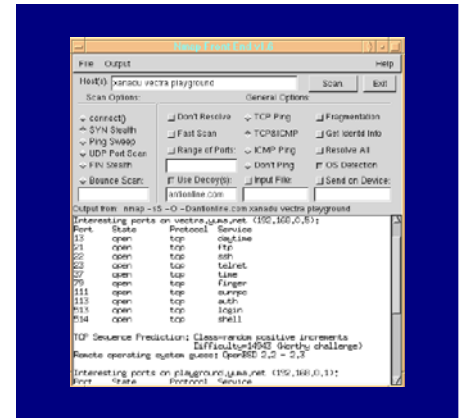
**The different types of approach: "Black-box" and "White-box":**

Penetration tests can be conducted in one of two ways: black-box (with no prior knowledge the infrastructure to be tested) or white-box (with complete knowledge of the infrastructure to be tested).





**Social Engineering** addresses a non-technical kind of intrusion; it relies heavily on human interaction and often involves tricking other people into breaking normal security procedures. Social engineering usually involves a scam; trying to gain the confidence of a trusted source by relying on the natural helpfulness of people as well as their weaknesses; appealing to their vanity, their authority and eaves dropping are natural techniques used. Other techniques involve searching refuse bins for valuable information, memorizing access codes by looking over someone's shoulder, or taking advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed.



## Deliverables: What do you get for the money?

A penetration test will involve the systematic analysis of all the security measures in place. A full project includes some or all of the following areas, with the exact requirements being agreed in a formal scoping document prior to commencing:

- **Network Security**
  - Network Surveying
  - Port Scanning
  - System Identification
  - Services Identification
  - Vulnerability Research & Verification
  - Application Testing & Code Review
  - Router Testing
  - Firewall Testing
  - Intrusion Detection System Testing
  - Trusted Systems Testing
  - Password Cracking
  - Denial of Service Testing
  - Containment Measures Testing
- **Information Security**
  - Document Grinding
  - Competitive Intelligence Scouting
  - Privacy Review
- **Social Engineering**
  - Request Testing
  - Guided Suggestion Testing
  - Trust Testing
- **Wireless Security**
  - Wireless Networks Testing
  - Cordless Communications Testing
  - Privacy Review
  - Infrared Systems Testing
- **Communications Security**
  - PBX Testing
  - Voicemail Testing
  - FAX review
  - Modem Testing
- **Physical Security**
  - Access Controls Testing
  - Perimeter Review
  - Monitoring Review
  - Alarm Response Testing
  - Location Review
  - Environment Review



Stealth – ISS Inc.'s assessments begin with a scoping exercise whereby the policies and procedures that are in place are examined against agreed standards. This is then followed by a technical review of the systems themselves.

Depending on the specification, this can include external, infrastructure or application devices, wireless/RAS or telephony, from vulnerability analysis through to full exploitation.

Our security assessments are performed with the industry's leading open source and commercial network vulnerability assessment tools, along with custom intrusion tools developed in-house; as directed from a full disclosure (White Box) or zero-knowledge (Black Box) perspective.

The final result consists of a report that details the findings for three different audiences; an Executive Summary, aimed at board members; a Management Overview, for management governing IT security and a Technical Detail section for those responsible for implementing the recommendations.

How We Offer it.

We offer a straightforward, yet comprehensive approach to our Testing Services:

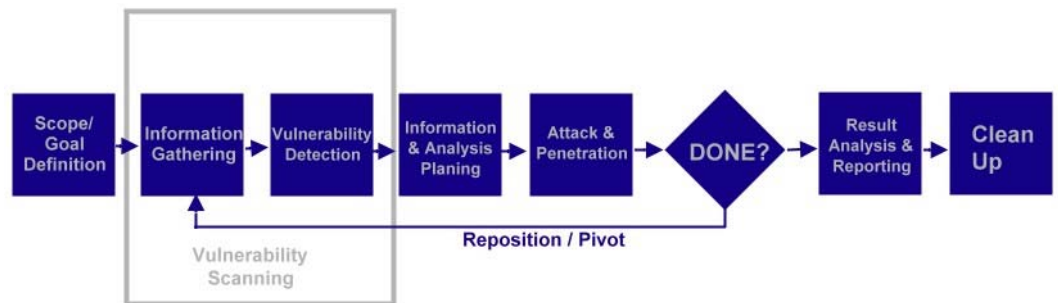
**Assess.** We'll start off with a free phone consultation to assess your needs. We'll help walk you through a brief fact-finding requirement stage that gives us information on goals, objectives, budget, timeline, configuration, special needs or requests, etc.

**Plan.** Once we have a solid understanding of your needs, network complexity, etc., we will develop a Project Plan Quote. We identify the strategy, timeline, and budget that is right for your security and penetration test needs.

**Scanning and Penetration.** This is our favorite part, and the one we do best - finding all those vulnerabilities you thought you never had and that could bring down your business, expose sensitive data, etc. We use many different attacks and approaches that will stress your solution to the max using state-of-the-art tools and proven test methods. At any point of time during the testing when we find a major vulnerability that either we (or you) consider serious or that could present a block for testing, we'll report that back to you immediately. This gives you an opportunity to make modifications and respond to a severe security risk as quickly as possible

**Deliver.** After we've completed our penetration test, analyzed it and found security holes, we'll present you with a final report that provides detailed information about the work done, including a summary of all testing performed, full test results with how to reproduce every defect, and conclusions and recommendations for remediation.

**OUR PENETRATION TESTING PROCEDURES**





## Why use Stealth – ISS Inc. for penetration tests?

### **Confidentiality**

We will preserve and protect the information we develop and gain during testing from disclosure to any other parties. A non-disclosure agreement will be signed with customers prior to testing. We do not use any external consultants or hackers for this service.

### **Qualifications**

Our security personnel has strong technical credentials, with the latest training in their field hold the highest levels of accreditations such as CISA, CISSP,CCSP and other.

### **Methodology**

Not only do we use the latest technology but also we use high-level methodology that follows standards such as OSSTMM, CHECK and OWASP. Also, we do perform all security audits and penetration test according to national and international security and IT standards such as ISO 17799, BS 7799 and others.

### **Security policy**

We will ask to review the customers security policy to help us understand prevailing security standards, practices, procedures—and potential weaknesses.

### **Technology**

We use latest commercial technology for penetration tests with daily updates as well as open-source software and the know how of our security staff. In order to ensure the quality and outcome of the test, we do perform manual checks on latest vulnerabilities also. The technology we use during testing is being used by institutions such as Department of State, Department of Defense, Bank of America, Citibank, Hewlett Packard, Rolls Royce, PriceWaterhouse Coopers, British Airways and many more.

### **Reporting results**

A written report will be provided, containing manager level overview, summary of the issues identified sorted by severity, technical details of each issue complete with outline-associated recommendations. Also included is a full listing of the actual tests results, and notes on the scope and limitations of tests. We will also provide the customers with copies of all logs, reports and other raw data collected during the testing process.

### **Projects**

Our security staff has done penetration testing for mid-size and large corporations as well as governmental institutions throughout Europe, international organization as well as NATO member states and institutions.

### **Customer cooperation**

Our penetration tests are always designed in collaboration with the client.

### **Flexibility**

We provide our services in-house and/or external and have adopted a flexible and personable strategy in a client-valued environment, to ensure our service suits both information security requirements and business needs.

### **Guaranteed Results**

We don't just test. We negotiate test priorities and goals with our clients and we guarantee to meet those goals. You get the testing and test results that we claim.