COMSEC Consulting

Penetration Testing Service

By Comsec Information Security Consulting

February, 2007

Comsec Information Security

Background Information

The number of hacking and intrusion incidents is increasing year by year as technology rolls out. Equally, there is no hiding place – your information can be found through a variety of means: DNS, Name Server Lookup, Newsgroups, Website trawling, e-mail properties and so on.

Whether the motivation is financial gain, espionage, political gain, intellectual challenge, or simply trouble making, you may be exposed to a variety of intruder threats. However, nowadays a business cannot afford not to provide the opportunity of the Internet, whether by e-commerce or just a plain Website. This business conflict poses a big challenge for many managers. That is why many organizations today have come to the conclusion that testing their systems is the only way to be absolutely sure. Conducting a Penetration Test is a very good possibility. The Penetration Tests include manipulating different layers of systems' input, hoping to achieve unauthorized access to database information, deletion of log/database information, replacing contents of a Website, Denial of Service, compromising sensitive data integrity and confidentiality, etc.

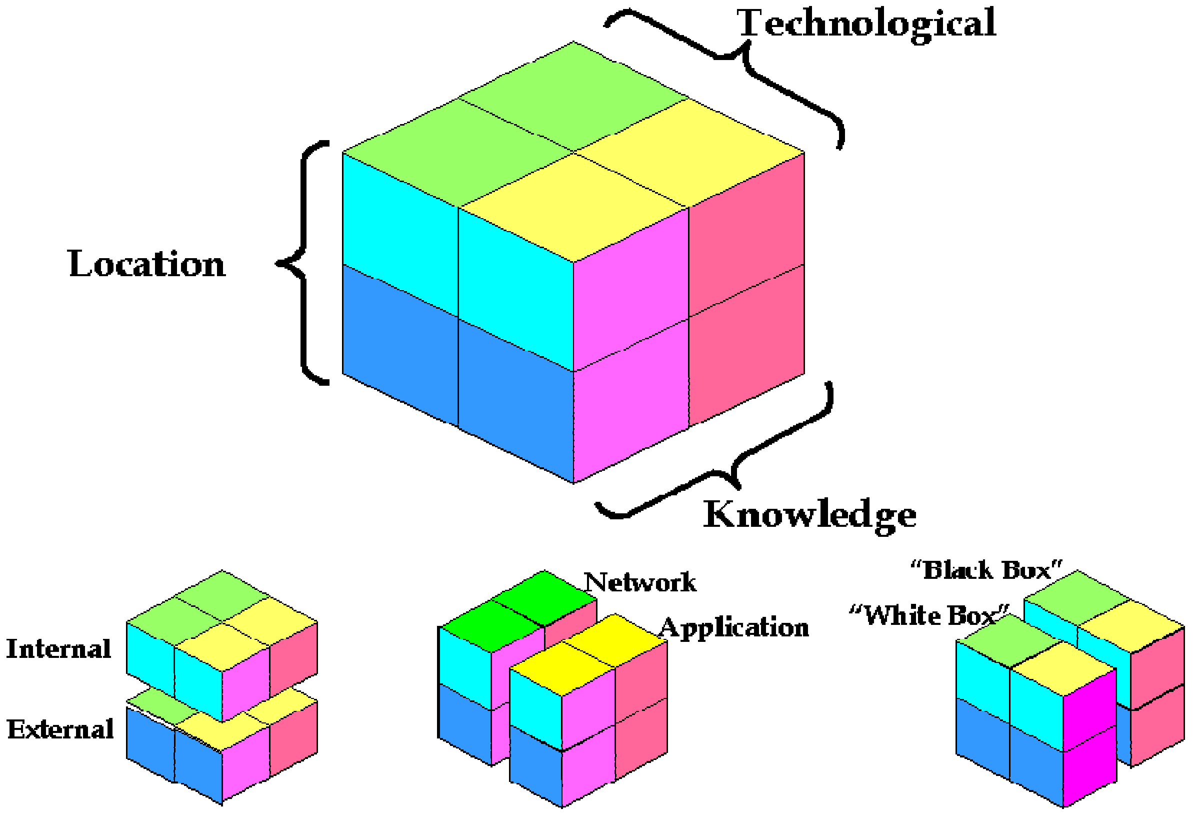
The objective of Penetration Testing is of course to investigate the system from the attacker's perspective. The primary aim is to identify exposures and risks to businesses before seeking a solution.

Methodology

The best way to prove the strength of your defense is attempting to penetrate it. To do so, Comsec has developed a proprietary Penetration Testing methodology, based on its extensive know-how and using open source, commercial & proprietary tools.

The Penetration Test is basically a simulation of attempts to penetrate or circumvent existing security mechanisms of the system, followed by a direct attack on specific servers. This is done to assure that breaches in the specific level of security are identified and subsequently, that the steps necessary to mitigate these breaches are implemented. Comsec distinguishes between several modes of Penetration Tests, similar in their general way of operation and the tests executed, yet differ in the logical source of location (inside or outside the examined network), the level of tests and the existance of initial information prior to the test performance. ***Comsec Consulting Intrusion Testing*** (CCIT^{TM}) is a propriety model, developed to define and differentiate the types of Intrusion / Penetration Tests Comsec performs.

The CCIT^{TM} model is defined by three dimensions, as presented in the chart below:



1.1. *Location*

Defines the logic source point of the Penetration Testing:

An **external Penetration Test** simulates unauthorized access, performed by an external factor possessing the initial information of a single IP address of a network / element, which is connected to external communication devices (router, firewall, Web server, etc.). The method enables us to assess the possible damages that an external intruder can inflict.

An **internal Penetration Test** simulates unauthorized access performed by either a legitimate network user or an unauthorized user who gained physical access to one of the communication devices (routers, hubs, etc.). The internal Penetration Test is performed with a direct connection to the attacked server. The security logic behind this act is that a server, which is protected from direct penetration, is most definitely protected from an external attack by a firewall.

1.2. *Technology*

Defines the layer of the system and the environment to be tested:

Infrastructure Testing includes the competency of the system's servers, operating systems, networking equipment and security mechanisms (Firewalls, Intrusion Detection Systems, Anti-Virus, etc.).

Application Security Testing is performed whenever an application is involved. This form of testing enables to focus on the application level, in addition to the infrastructure level. The testing procedure consists of examining the application itself for potential software malfunctions that may jeopardize the security of the system by directly attacking it. The application test aims at examining the following potential risks:

- Hidden Field Manipulation
- Denial of Service
- Impersonation
- SSL Private Key Theft
- Cookies Poisoning
- Parameter Tampering
- Cross-site Scripting (XSS)
- Forceful Browsing
- Buffer Overflow

1.3. *Knowledge*

Defines the level of information the Penetration Team has, prior to the project launch:

This is devided into **Black Box** testing and **White Box** testing. Black Box tests are conducted without prior knowledge of the system, and approach the system in the same manner that a user or a hacker would.

White Box testing is conducted under the assumption that some or all of the information regarding the system is revealed. Using this information, Comsec searches for security vulnerabilities and faults in the system. This is the most comprehensive form of security auditing and provides a high success rate for uncovering vulnerabilities.

Black Box tests are essential to any security software product, software system or computer network. It quickly uncovers vulnerabilities and weaknesses related to the specification of the system. Where a high level of security is required, Black Box testing should be combined with White Box testing. White Box testing is better for uncovering weaknesses such as back doors, undocumented features and long-term race conditions.

The Process

Under the scope of the service, Comsec security experts analyze the security level of a network or system by attempting to penetrate it. The starting point is usually IP address (provided by the customer) of a device or servers in the network, which is connected to the external communication. During the test the Comsec Team simulate an uncertified access attempt, aiming to explore the following risks:

- External **unauthorized penetration** to the internal organizations' networks.
- **Information leakage** and damage caused by hostile Applets.
- Viruses and Trojan Horses – **infection through e-mail** or web services.
- **Denial of service attacks** on the Internet and Hosting environments.
- **Hacking** into the systems or into the customers' data stored in infrastructures and facilities.
- **Availability and integrity** exposure of the customers' data and the business information.

The Penetration Testing process includes the following elements:

- Gathering information regarding the components of the analyzed network
- Applying penetration tools in order to locate breaches, risks and exposures
- Using computerized penetration tools to find the recently published breaches
- Using sniffers to intercept communication over the network
- Testing possibilities for network distortion (Denial of Service, vandals, etc.)
- Exploiting the detected breaches in order to extract data from the network
- Testing the information security level of the different systems that are connected to the network including database servers, mail servers, web servers, etc.

While performing Penetration Tests Comsec uses various tools such as:

- ✓ Network scanners
- ✓ Sniffers
- ✓ Application scanners
- ✓ Vulnerability scanners
- ✓ Password crackers
- ✓ War Dialers
- ✓ Proprietary intrusion tools

Comsec Information Security

The Deliverable

Following the testing process, Comsec's experts analyze the vulnerabilities detected and produce a detailed report as a stand-alone document. Within this report various breaches and attack scenarios are described and the probabilities of exploitation of the breaches, their level of severity and possible inflicted damage on the company. Initial recommendations for a corrective action plan are provided and initial counter actions for each vulnerability is included to help raise the security level at the first stage. The methodology embedded in this document will state the entity as the key issue and its risks as the attributes. This report provides a bird's eye view of the security level implemented in the tested system and helps prioritize the necessary counter actions and security plan.

Comsec has a unique approach to vulnerability scanning, which is provided with a tailored programme that not only identifies potential vulnerabilities but also provides analysis from experienced security consultants. This experience assists to identify real risks to business and recommend remedial action.

Service Benefits

- ✓ Penetration Tests reduce significant risks of information leaks thus enhancing information integrity.
- ✓ The organization's management will receive a clear understanding of the exposure level and the business impact caused by information security breaches
- ✓ Penetration Tests prioritize the detected risks by setting their level of severity
- ✓ The final stage of the service, which is the analysis and deliverable, provides guidance on to how to mitigate the detected vulnerabilities
- ✓ Detecting vulnerabilities during the development stages of a system's lifecycle by conducting a Penetration Test dramatically increases the efficiency of the development process.
- ✓ Comsec, with its comprehensive proven methodology, dedicated security experts, expertise in security best practices and years of Penetration Testing experience is your total solution provider for Penetration Testing.