Vulnerability & Penetration Test
### Threats Continue to Rise....

| Code Red infected 359,000 servers in less than 14 hours – at the peak, it infected more than 2,000 new hosts/minute – estimated cost? $2.6B | Second largest malicious codes come from India –  
www.business-standard.com |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Computer Economics)</td>
<td>1 vulnerability exists in every 1500 lines of code (IBM’s Watson Research Lab) ; Windows XP has 45M lines of code; W2K has 35M lines of code; MS code lines double every 866 days....</td>
</tr>
<tr>
<td>India's Railway Email System hacked by Pakistan Cyber Army</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.thehackernews.com">www.thehackernews.com</a></td>
<td></td>
</tr>
<tr>
<td>Within 24 hours of NIMDA hitting, 50% of the infected hosts went offline</td>
<td>According to Symantec Critical Infrastructure Protection Survey 2010, over half of India’s critical infrastructure providers were victims of cyber attacks– Symantec</td>
</tr>
<tr>
<td>(CNet)</td>
<td></td>
</tr>
</tbody>
</table>
| India was the third most-infected country for Stuxnet with 10 per cent infections – | Over 35,697 active bot computers in India. Average of 435 bots per day in 2010 –  
www.business-standard.com |
Compliance to various security standards and regulations such as ISO 27001, IT ACT 2000, SOX, HIPAA, PCI, etc.

To improve information security awareness

To mitigate risk immediately

To assist in decision making processes

To assess risk

To reinforce the information security process

To Validate that current security mechanisms are working

Highest Security Risk
What is VA/PT

Vulnerability assessment is the process of identifying and quantifying vulnerabilities in a system. A vulnerability assessment is what most companies generally do, as the systems they are testing are live production systems and can’t afford to be disrupted by active exploits which might crash the system.

A form of Stress testing, which exposes weaknesses or flaws in a computer system Art of finding an Open

Door

A Valued Assurance Assessment tool

PT can be used to find Flaws in Specifications, Architecture, Implementation, Software, Hardware any many more....
BLACK BOX TESTING

Tester need to acquire the Knowledge and Penetrate:

- Acquire knowledge using tools or Social Engineering techniques
- Publicly available information may be given to the penetration tester

Benefits:

- Black box testing is intended to closely replicate the attack made by an outsider without any information of the system. This kind of testing will give an insight of the robustness of the security when under attack by script kiddies.

- It is also known as “Zero-Knowledge” testing
WHITE BOX TESTING

It is known as “Complete Knowledge” testing:

- Testers are given full information about the target system they are supposed to attack.
- Information include:
  - Technology overviews
  - Data flow & Network diagrams
  - Code snippets
  - & More

Benefits:

- Black box testing is intended to closely replicate the attack made by an outsider without any information of the system. This kind of testing will give an insight of the robustness of the security when under attack by script kiddies.
- It is also known as “Zero-Knowledge” testing.
The tester simulates an inside Employee. The tester is given an account on the internal network and standard access to the network.

This test assesses internal threats from employees within the Company.

The relative merits of all these approaches are debatable. In most cases, it is preferable to assume a worst-case scenario and provide the testers with as much information as they require, assuming that any determined attacker would already have acquired this.
Methodology for VA-PT

- Scope / Goal Definition
- Information Gathering
- Information Analysis & Planning
- Attack & Penetration / Privilege Escalation
- Vulnerability Detection
- Result Analysis & Reporting
- Clean Up
The goal of the external network Penetration Testing is to demonstrate the existence of known security vulnerabilities that could be exploited by an attacker as they appear outside the perimeter of the network, usually from the internet. External testing involves analysis of publicly available information, a network enumeration phase and the behaviour of the security devices is analyzed. It is the traditional approach to Penetration Testing and it involves assessing the servers, technology infrastructure and the underlying software comprising the target. It is performed with no prior knowledge of the target environment. All web servers, mail servers, firewalls, routers, IDPS, etc should undergo the Penetration Testing activity to evaluate the security posture.
Infopercept VAPT Methodology

Internal Penetration Testing:

The goal of the external network Penetration Testing is to demonstrate the existence of known security vulnerabilities that could be exploited by an attacker as they appear outside the perimeter of the network, usually from the internet. External testing involves analysis of publicly available information, a network enumeration phase and the behaviour of the security devices is analyzed. It is the traditional approach to Penetration Testing and it involves assessing the servers, technology infrastructure and the underlying software comprising the target. It is performed with no prior knowledge of the target environment. All web servers, mail servers, firewalls, routers, IDPS, etc should undergo the Penetration Testing activity to evaluate the security posture.
Standards we follow for External Penetration Testing

- Open Web Application Security Project (OWASP) Testing Guide
- Payment Card Industry (PCI) Penetration Testing Guidance
- The Penetration Testing Execution Standard (PTES)
Methodology for VA-PT

Planning & Execution

Planning:
1. Intelligence Gathering
2. Review Rules of Engagement

Execution:
1. Reconnaissance
2. Threat Modelling
3. Vulnerability Analysis
4. Exploitation
5. Post Exploitation
6. Reporting
VAPT Tests and Tools

Frameworks
- Kali Linux
- R3 Security Onion

Reconnaissance
- Smartwhois
- MxToolbox
- CentralOps
- Dnsstuff
- Nslookup
- DIG
- netcraft

Discovery
- Angry IP scanner
- Colasoft ping tool
- nmap
- Maltego
- NetResident
- LanSurveyor
- OpManager

Port Scanning
- Nmap
- Megaping
- Hping3
- Netscan tools pro
- Advanced port scannerService
- Fingerprinting
- Xprobe
- nmap
- zenmap

Enumeration
- Superscan
- Netbios enumerator
- Snmpcheck
- onesixtyone
- Jxplorer
- Hyena
- DumpSec
- WinFingerprint
- Ps Tools
- NsAuditor
- Enum4Linux
- nlookup
- Netscan
VAPT Tests and Tools

**Scanning**
- Nessus, GFI
- Languard
- Retina
- SAINT
- Nexpose

**Password Cracking**
- Ncrack
- Cain & Abel
- LC5
- Ophcrack
- pwdump7
- fgdump
- John The Ripper
- Rainbow Crack

**Sniffing**
- Wireshark
- Ettercap
- Capsa Network
- Analyzer

**MiTM Attacks**
- Cain & Abel
- Ettercap

**Exploitation**
- Metasploit
- Core Impact
1. Scope/Goal Definition

- Which attacker profile the tester will use
  - Hacker with no knowledge about the target
  - Hacker with knowledge about the target
  - Internet user with access

- Which System or network the test will be conducted

- Duration of Test
2. Information Gathering

- Information about the Target

  ➢ Who is: ARIN; RIPE; APNIC

  ➢ Google: General Information; Financial, Phone Book, Google Hacking Databases; Web Searching

  ➢ DNS Retrieval, SOA Record, MX Records, NS Records, A Records etc.

  ➢ Tools / Websites: Cheops-ng, Sam Spade, www.dnstuff.com

  ➢ Social Engineering

  ➢ Dumpster Diving

  ➢ Web Site Copy
3. Vulnerability Detection

- Manual Detection

  Manually probe the target host from common misconfiguration or flaws because a vulnerability scanner can fail to identify certain vulnerabilities.

  - Ex: Database configuration etc.
  - Open TCP Ports
  - Closed TCP Ports
  - Open UDP Ports
  - Closed UDP Ports
  - Service Probing
4. Information Analysis & Planning

- Collating the information gathered in previous stages.
- Preparation of High level attack planning.

- Overall Approach
- Target identification.
5. Penetration & Privilege Escalation

- **Attack & Penetration**
  - Known / available exploit selection – Tester acquires publicly available s/w for exploiting.
  - Exploit customization – Customize exploits s/w program to work as desired.
  - Exploit development – Develop own exploit if no exploit program Available
  - Exploit testing – Exploit must be tested before formal Test to avoid damage.
  - Attack – Use of exploit to gain unauthorized access to target.
5. Penetration & Privilege Escalation

- Privilege Escalation

  What can be done with acquired access / privileges.
  
  - Alter
  - Damage
  - What not
7. Cleanup

- Cleaning of all that has been done during the testing
  - Any System alterations
  - Exploits
Vulnerability Database

- National Vulnerability Database - nvd.nist.gov
- Common Vulnerabilities and Exposures - cve.mitre.org/cve/
- Security Focus Bugtraq - www.securityfocus.com/vulnerabilities/
- Open Source Vulnerability Database
- www.osvdb.org/search.php
- US-CERT Vulnerability Notes
- Database - www.kb.cert.org/vuls/

Tools and Technologies

- Nmap
- Professional Version of Nessus
- Acunetix
- Back Track
- In House Scripts
- Back Track Tool Kit
- Manual Intelligence
CHALLENGES AND WHY
Infopercept

- Quality & Experience of Pen Testers
- Quality & Effectiveness of Tools
- Usage of Globally Accepted Methodology such as OSSTMM, OWASP etc.
- Ensuring all the findings are reported to the Management.
- Follow stringent program to Fix Vulnerabilities.
- Conduct Periodic Testing.
By accessing/proceeding further with usage of this platform/tool/site/application, you agree with the Company’s/Infopercept Consulting Pvt. Ltd.’s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions, kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.