Security Audit (VA & PT) Services
**Vulnerability Assessment** tools uncover all possible network weaknesses, leaving customers guessing as to which vulnerabilities pose real, imminent threats.

**Penetration Testing** safely exploits vulnerabilities to eliminate "false positives" and reveal tangible threats. Penetration test results enable IT staff to delineate critical security issues that require immediate attention from those that pose lesser risks.

**Scope**

The scope of this document is to establish a Vulnerability Assessment Methodology which helps paint an accurate picture of the risks, weaknesses, information leaks and vulnerabilities. The VAPT Methodology described in this document incorporates the best security testing practices of the industry conforming to Information Security compliance standards and Locuz commitment to ensure the highest possible confidentiality.

The methodology needed to perform this test allows for a systematic checking for known vulnerabilities and pursuit of potential security risks.
Vulnerability Assessment

Study & Scope of the IT infrastructure & Components

Determine boundary Of assessment

Perform impact analysis for active scans

Plan for downtime & contingency

Define the scan policy for each target

Scan the targeted network & hosts

Classification of vulnerabilities discovered

Explanation of findings & risks for each vulnerability

Recommended action items including immediate fixes

Executive summary highlighting key findings

Locuz opinion regarding clients overall security posture
Methodology

Preparation

In this phase, a formal contract is signed which also contains a Non-Disclosure Agreement. The contract also outlines infrastructure perimeter, evaluation activities, time schedules and resources available to a tester.

- A template is provided to the client to receive the details of the IT Infrastructure which assist Locuz to analyze the critical areas to perform the audit
- Study & Scope of the IT architecture & components for assessment
- Determine the boundary of assessment
- Identify asset owners & schedule tasks, if any
- Perform Impact analysis for active scans, which includes analysis of Service(s) or Server(s) scans in online production environment
- Estimate the scan process, based on the complexity of the target network(s) and host(s)
- ICMP access to perform the audit.

Scanning

After gathering the preliminary information we will identify systems that are alive and reachable via the Network/Internet, and what services they offer. We define the Scan policy for each target. Scan policy to define the level of – Scan, Information gathering, policy checking, port scanning, Password analysis, attack stimulation etc. We perform followings activities based on the architecture and complexity of the network.

- Active Scans
- Passive Scans

The live systems will probed for available services. The process of scanning can involve many tools and varying techniques depending on what the goal is and the configuration of the target host or network.

Below is a list of some common tools to perform scanning:

- Nmap
- Nessus
- GFI LanGuard
- Retina
Enumeration

If acquisition and non-intrusive probing have not turned up any results, then a tester will next turn to identifying valid user accounts or poorly protected resource shares.

- Enumeration involves active connections to systems and directed queries
- The type of information enumerated by tester:
  - Network resources and shares
  - Users and groups
  - Applications and banners

Vulnerability Analysis

Vulnerability Analysis is the act of determining which security holes and vulnerabilities may be applicable to the target network or host. The vulnerability analysis phase is started after some interesting hosts are identified via scanning tools and is preceded by the enumeration phase.

Following are the points taken care during this phase:
- Identification & Filtration of False Positives
- Identification & Filtration of False Negatives
- Banners exposing internal information
- Exposed Web Applications variables, etc
- Default configuration mistakes

Documentation

Step 1: Collect the scan results and analyze for security loopholes, configuration errors, default installation settings, overlooked setups, password quality, firmware/software revisions, patch fixes, security policy violations etc.

Step 2: Classify the vulnerabilities discovered within the environment spanning – Technical, Organizational and Process issues; into categories of High, Medium, and Low risk.

Step 3: Perform impact analysis of the vulnerabilities discovered and threats arising thereof, per se the client’s IT architecture.

Submission of Reports

Step 1: Detailed explanations of the implications of findings, impacts, and risks for each of the identified vulnerabilities.

Step 2: Recommended Action Items including immediate fixes, policy recommendations and product recommendations for improving the overall network security.

Step 3: An executive summary highlighting key findings and recommendations from a security perspective.
Penetration Testing

1. Identify Key Vulnerabilities
2. List of acceptable testing techniques
3. Define IP Addresses of machines from which PT will be conducted
4. Launch the exploits
5. Information gathering
6. Escalate attacks to other targets
7. Remove all testing traces & return to previous configuration
8. Detailed explanations on implications of findings impacts and risks
9. Cleaning Up

Submission of Reports

Recommended action items & summary of key findings

Locuz statement on overall security posture
**Methodology**

**Planning**

**Step 1:** Identify key vulnerabilities to be exploited

**Step 2:** Prepare a list of acceptable testing techniques (Ex: Password cracking, Denial of service, etc.) and research exploits to be launched

**Step 3:** Ascertain the times when the testing is to be conducted (Ex: During business hours, after business hours, etc.)

**Step 4:** Prepare identification of an estimated period for testing

**Step 5:** Determine IP addresses of the machines from which penetration testing will be conducted so that the client can differentiate the legitimate penetration testing attacks from actual malicious attacks

**Step 6:** Identify asset owners & schedule tasks, if any

**Step 7:** Plan for Downtime & Contingency, if applicable
Exploitation

Our approach is to review the list of vulnerabilities collected in the VA stage and sort them by likelihood of success and potential harm to the target network to see which may be helpful in our exploitation efforts. We examine the list of known vulnerabilities and potential security holes on the various target hosts and determine which are most likely to be fruitful. Next we pursue exploiting those vulnerabilities to gain access on the target system. Primary targets are open ports and potentially vulnerable applications.

The below mentioned tools are used to perform Penetration Testing.

1. Nmap
2. Nessus
3. GFI LanGuard
4. Retina
5. Metasploit

Cleaning Up

Remove all testing traces of compromised systems based on the detailed and exact list of all actions performed during the penetration test; returning the system and any compromised systems to the exact configurations that they had prior to the penetration test.

Reporting

**Step 1:** Detailed explanations of the implications of findings, impacts and risks for each of the identified vulnerabilities.

**Step 2:** Recommended Action Items including immediate fixes, policy Recommendations and product recommendations for improving the overall network security.

**Step 3:** An executive summary highlighting key findings and recommendations from a security perspective.
<table>
<thead>
<tr>
<th>Testing Scope</th>
<th>Vulnerability Assessment</th>
<th>Penetration Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testing Scope</td>
<td>Scans for all potential network vulnerabilities.</td>
<td>Identifies vulnerabilities and determines if they can actually be exploited.</td>
</tr>
<tr>
<td>Vulnerability Relevance</td>
<td>Categorizes vulnerabilities based on standardized, theoretical information - not customized to the tested network.</td>
<td>Tests vulnerabilities on specific network resources, enabling prioritization of remediation efforts.</td>
</tr>
<tr>
<td>Usefulness of Test Results</td>
<td>Provides false positives, identifying vulnerabilities that cannot be exploited.</td>
<td>Exploits vulnerabilities, identifying only those that pose actual threats to network resources.</td>
</tr>
<tr>
<td>Network Connection Testing</td>
<td>Does not address connections between network components.</td>
<td>Exploits trust relationships between network components to demonstrate actual attack paths.</td>
</tr>
<tr>
<td>Remediation Assistance</td>
<td>Delivers long lists of vulnerabilities, limiting remediation options to widespread patching.</td>
<td>Assesses the potential risks of specific vulnerabilities, allowing users to patch only what is necessary and to test the effectiveness of patches and other mitigation strategies, such as intrusion prevention.</td>
</tr>
<tr>
<td>Testing of Other Security Investments</td>
<td>Does not simulate attacks to test IDS, IPS or other security technologies.</td>
<td>Launches real-world attacks to determine if other security investments are functioning properly.</td>
</tr>
<tr>
<td>Security Risk Assessment</td>
<td>Only identifies missing patches, making it impossible to truly assess security risks.</td>
<td>Safely mimics the actions of a hackers and worms, providing risk evaluations based on tangible network threats.</td>
</tr>
</tbody>
</table>
About Locuz

Locuz is an IT Infrastructure Solutions and Services company focused on helping enterprises transform their businesses thru innovative and optimal use of technology. Our strong team of specialists, help address the challenge of deploying & managing complex IT Infrastructure in the face of rapid technological change.

Apart from providing a wide range of advisory, implementation & managed IT services, Locuz has built innovative platforms in the area of Hybrid Cloud Orchestration, High Performance Computing & Software Asset Analytics. These products have been successfully deployed in leading enterprises and we are helping customers extract greater RoI from their IT Infrastructure assets & investments.

Security Audit (VA & PT) Services

Locuz Enterprise Solutions
401, Krishe’ Sapphire, Main Road, Madhapur, Hyderabad-500018, Telangana, India