



Vulnerability Assessment – Nullifying threats and managing risks

Company Name assesses the vulnerabilities in your organization and strategizes a road map to eliminate the threats to key resources.

INTRODUCTION

Every business is prone to risks; be it the risk of data loss, a system crash or a fraud. Risk analysis, for the detection and eventual elimination of a risk, has been around for many years and is known to most companies. However, risk analysis only focuses on locating the risk object, its direct consequence, and its elimination. This process completely neglects the indirect consequences of a risk and also fails to uncover hidden risks in the system.

Vulnerability assessment fills that gap. Vulnerability assessment is a process that defines, identifies, and classifies the security holes in a computer, network, or communications infrastructure. In addition, vulnerability assessment can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.

Why Vulnerability Assessment

Vulnerability assessment is used to gain comprehensive visibility into the security flaws present in your network. It helps an organization analyze how a vulnerability occurs; identify ways to counter the problem and, finally, the protective measures to take so that those flaws never occur again.

Identification	<ul style="list-style-type: none">• Understand and identify potential points of security violation• Categorize and rank the key assets and resources• Set risk thresholds for the key assets, resources and processes
Evaluation	<ul style="list-style-type: none">• Quantify the impact of potential security violation points• Assess key assets and resources hierarchy• Define a baseline of best practices to evaluate against
Protection	<ul style="list-style-type: none">• Protect your brand from potential attacks• Protect the integrity of all key assets and resources• Protect intellectual property• Reduce risk of public disclosure and loss of sensitive data
Prevention	<ul style="list-style-type: none">• Prevent financial loss through fraud• Mitigate or eliminate the most serious vulnerabilities for the most valuable resources• Prevent your online business from crashing due to hacks and malware attacks

Action

- Use it as a catalyst to involve people throughout the organization in security issues
- Establish permanent forums / councils to take care of future issues
- Identify key players, and establishes a set of cross-functional groups that can convert those recommendations into action

Where Vulnerability Assessment is headed

With more and more organizations taking their business online, the dynamics of vulnerability assessment are slowly changing. Also, with a steadily increasing dependence on mobile devices, the organization has never been more vulnerable. The possibility of malware creeping into mission critical enterprise applications and devices is imminent. Vulnerability assessment will thus take much more precedence in the future.

Multiple access points

The average enterprise of today has gone mobile. A majority of the workforce works on notebooks, and this workforce stays connected via Wi-Fi networks. There is a distinct possibility of a hack on this network, which could lead to a lot of official data out in the open. Vulnerability assessment will have to move to cover the Wi-Fi networks also, and prevent the possibility of any attack on the enterprise network.

Cloud level risk assessment

Cloud computing has taken the world by storm. With its apparent benefits; the user need not have any knowledge of the technology, nor have any expertise in it, and need not exercise any control over the infrastructure, cloud computing is set to take over the world of enterprise technology.

Yet, with no knowledge of where your organizations' data has been stored, unclear data recovery norms and data segregation clauses, cloud computing could become a major reason for vulnerability assessment.

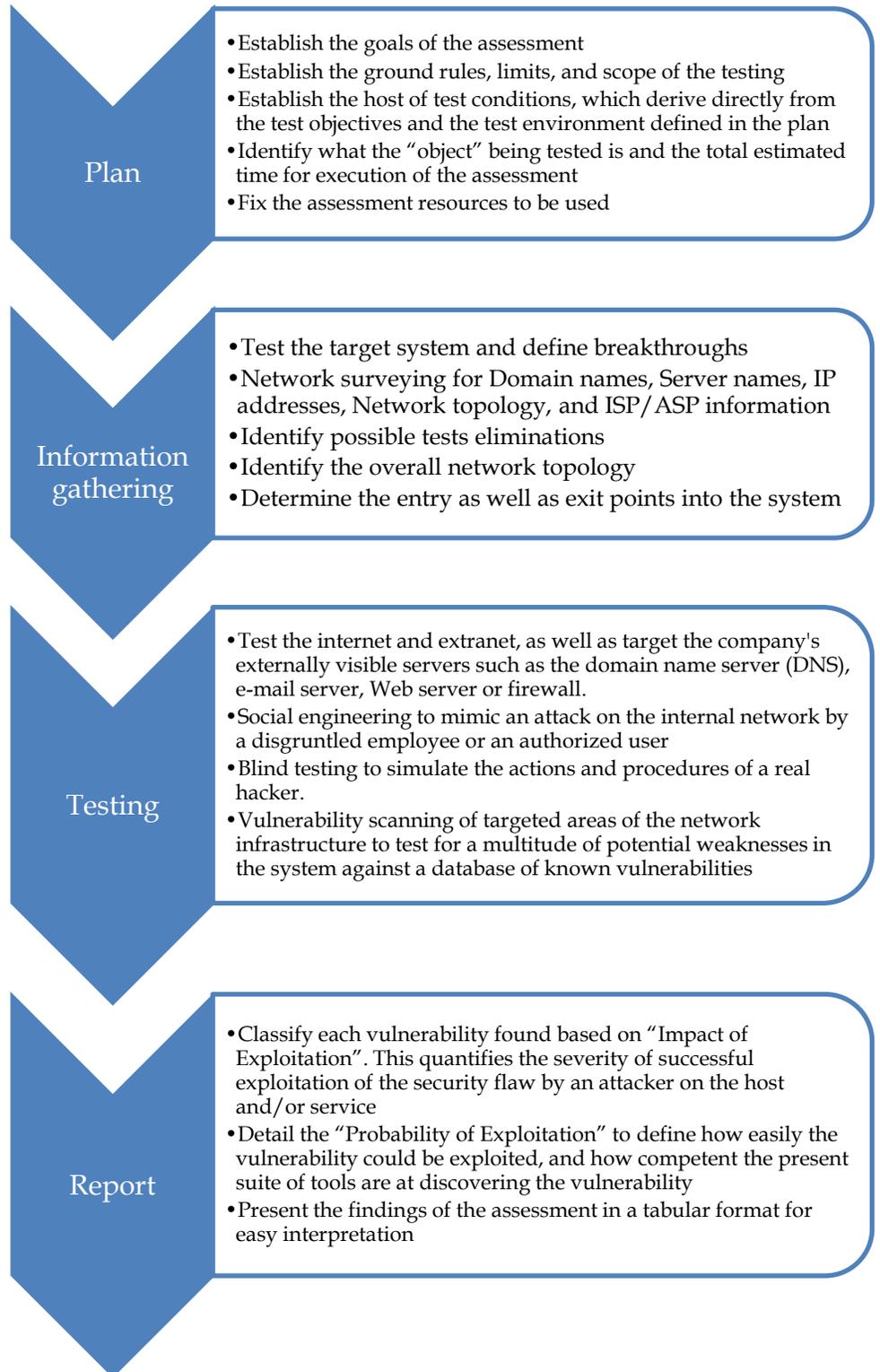
“Vulnerability Assessment will eventually give you a complete picture of all the network-attached devices and how that network operates as a living entity”

Challenges in Vulnerability Assessment

- *Strengthening of current network security processes and procedures to protect against virulent worm/virus attacks from both external and internal threats*
- *Deploying new security solutions that go beyond core-level technology to span your entire network*
- *Responsiveness to changing customer and partner requirements, through organizational and operational procedures*
- *Performing routine vulnerability assessments of the network*
- *Identifying and categorizing key assets and resources*
- *Understanding the most likely and potential breach points*

How do we do it?

Our Vulnerability Assessment services are specifically designed to meet the needs of each of our clients, and as such, our services will help reassure you of the safety of your vital enterprise applications



“Company Name utilizes a dual classification system for evaluating each of the discovered vulnerability; its impact on your organization and the probability of it happening”

Our Vulnerability Assessment Services

We offer a comprehensive range of Vulnerability Assessment services that identify vulnerabilities, assess the risk they pose to your organization, prioritize these risks and eliminate them by a coordinated application of resources.

Application Testing

- Evaluate controls over e-commerce servers, on-line financial applications, distributed applications, and Internet front ends to legacy systems
- Evaluate applications' usage of encryption to check how users are authenticated, integrity of the Internet user's session with the host application, etc.
- Analyze all application-based code to ensure that it does not contain any sensitive information

Network testing

- Identify security gaps or flaws in design, implementation or operation of wireless network
- Find available servers on the network by gaining access to the wireless network, even though it is protected by WEP2.
- Determine the services on those servers available for connection (and exploitation) and find well-known vulnerabilities which can be used to gain unauthorized access

Social Engineering

- Pose as a representative of the IT department; attempt to make users divulge their user account & password information
- Pose as an employee and gain physical access to restricted areas that may house sensitive information; intercept mail / courier packages or even trash to search for sensitive information on printed material

Add-on Services

Network Hardening

- Identify critical network elements & services. Also check for currency of patches
- Prepare network hardening plan based on the above - disabling unnecessary services, ports & accounts
- Execute network hardening plan and check post-implementation to ensure the network is secure as per plan
- Provide best-practices and recommend activities for improving your company's security posture

OS Hardening

- Check OS version and updates to ensure OS level vulnerabilities are identified
- Identify and remove all non essential tools, utilities and other systems administration options, any of which could be used to ease a hacker's path to your systems
- Ensure that all appropriate security features are activated and configured correctly
- Recommend additional activities and OS usage to help secure daily operations

CLIENT EXPERIENCE

Our client, a digital agency specializing in strategy, creative and technology fields, was expanding its business online. The need to keep business resources running 24/7 while eliminating downtime was paramount.

However, they realized that their online business was prone to such risks as-

- Hacking
- Password attacks
- Proxy server attacks
- Remote file system attacks
- Denial of service testing

In order to mitigate these risks, they chose Company Name Vulnerability Assessment services. Upon analysis, Company Name recommended the following services to them –

- Network surveying
- Port scanning
- Application testing
- Router and firewall testing
- Denial of service testing

The chosen services helped them -

- Discover the key target systems
- Identify security bugs in server and client applications of the system
- Identify penetration points of router and firewall, and their subsequent fortification
- Discover vulnerabilities at different levels such as OS, Services & Applications.

Benefits of the Company Name Approach

Company Name aims at ensuring a well managed infrastructure as well as to providing competitive advantage by delivering more value to the end user. We also ensure that your enterprise applications are secure, impervious to the latest attacks, and that the possible breach points are under constant 24/7 monitoring.

Improved reliability	<ul style="list-style-type: none"> • Clients can focus more effectively on running their business better, while we worry about keeping the applications that run his business safe • Our expertise and scale in providing comprehensive solutions provides our clients with increased reliability • Our experience helps us understand applications better, aids in quicker and better assessments, and leads to findings which keeps an organization immune from attacks • Our specialists will not only help fix the vulnerabilities, but will also provide their expertise
Improved asset utilization	<ul style="list-style-type: none"> • Our ability to quickly respond to client requirements, and our expertise in offering a wide range of services enables clients to better utilize their valuable assets and resources • We help increase asset uptimes, eliminate the possibility of an attack, and make optimum utilization of assets for maximum performance possible • Build an IT asset protection roadmap • Increase awareness of possible security measures that need to be implemented
Better ROI	<ul style="list-style-type: none"> • Increase in asset utilization, which helps increase productivity, thus leading to an improvement in ROI • Eliminate downtimes, and gain revenue while covering the same operational costs • Training on security solutions to better impel attacks in the future and protect the organization’s mission critical processes
Round the clock monitoring	<ul style="list-style-type: none"> • Identify & track your mission critical enterprise assets and resources, and we do this round the clock. • Key components and devices are monitored, to build a complete pro-active system of immediate problem detection, real-time alerts, and multimedia notifications.

ABOUT COMPANY NAME

Company Name is a global IT services company offering technology consulting, software product development, testing, remote infrastructure management and knowledge process outsourcing services. The company was setup in 1997 with a vision to deliver value to clients worldwide using an effective Global Delivery Model. Company Name core competency is in building ‘Extended Teams’ in India that are dedicated to clients, based on their specific requirements, that consistently deliver quality services, and in due course become a seamless extension of the client. This delivers a competitive advantage beyond traditional cost-efficiencies.

To know more, please visit us at www.Company Name.com