Penetration Testing / Vulnerability Assesment

NEED OF PENETRATION TESTING / VULNERABILITY ASSESMENT

What exactly is Penetration Testing?

- Penetration Testing is a software attack launched on a Computer System that looks for security and vulnerabilities and weakness. And once you get access you can view the features and data. It can be a computer system or a network, web application for vulnerability for an attacker can exploit or could exploit. What a Penetration Tester does is he mimics a Hacker
- VA / PT actually evaluates the companies security measures and the IT's security.
- The process of actively evaluating company's information security measures and the results are delivered comprehensively in a report.
- Penetration test reports assess potential impacts to the organization and suggest countermeasures to reduce risk.

Need of Pen Testing

- To identify the threats facing an organization's information assets.
- To reduce an organization's IT Security cost.
- To provide a better Return on IT Security Investment (ROSI) by identifying and resolving vulnerabilities and weakness.
- To gain and maintain certification to an industry regulation such as HIPAA.
- For testing and validating the efficiency of security protections and control.
- To focus on high severity vulnerabilities and emphasizes application-level security issues to development teams and management.
- Evaluating the efficiency of network security devices such as firewalls, routers etc.
- For changing/updating existing infrastructure or software or hardware or network design.

What should be tested???

Public facing systems, websites, email gateways, and remote access platforms Mail, DNS, Firewalls, passwords, FTP, IIS, and web servers. Testing should be performed on all hardware and software components of Network Security system.

Defining the Scope

This involves:

- What will be tested?
- The extent of Testing

- From where it will be tested
- And who will test it

Reporting and delivering results involve:

- Listing the vulnerabilities
- Categorizing risks as Low, Medium or **High**
- Recommending repairs if vulnerabilities are found

Type of Test

A Non-Destructive Test

- Scans and identifies the remote system for potential vulnerabilities
- Investigates and verifies the findings
- Maps the vulnerabilities with proper exploits
- Does not attempt a Denial of Service (DoS) attack

A Destructive test

- Scans and identifies the remote system for potential vulnerabilities
- Investigates and verifies the findings
- Maps the vulnerabilities with proper exploits
- Attempt a Denial of Service (DoS) and Buffer Overflow attacks.

Type of Pen-Testing and Vulnerability Assessment

Black Box Pen-Testing

- No prior knowledge of infrastructure to be tested
- You will be given just a company name

Penetration test must be carried out after extensive information gathering and research. Time-consuming and expensive type of test.

White Box Pen-Testing

- You will be given Company Infrastructure
- Network Type
- Current Security Implementations
- IP Address / Firewall / IDS Details
- Company policies do’s and don’ts

Gray Box Pen-Testing

- Is a combination of White Box and Black Box Pen-Testing?
- The tester has limited knowledge of information

Announced Pen-Testing

- Announced pen testing is when a pen test is done with the knowledge of everyone in the organization and all employees.
- Security staff usually joins the penetration testing team to conduct these audits.
- It is an attempt to compromise systems on the client with the cooperation and knowledge.

Advantages of Announced Testing

- More efficient
- Team oriented

Disadvantages of Announced Testing

- Lack of Security
- Less reliable results

Unannounced Pen-Testing

- Is an attempt to access and retrieve pre-identified flag files or to compromise systems on the client network with the awareness of only the upper levels of management.
- This testing examines both the existing security infrastructure and the responsive of the staff

Manual Testing

- Manual testing is the best option an organization can choose to benefit from the experience of a security professional.
- The purpose of manual penetration testing is to identify specific application vulnerabilities within scoped domains.
- Manual testing requires planning, designing, scheduling, diligent documentation to capture the results of the testing process.

Strategies of Penetration Testing

- Network Security Assessment
- Internal Security Assessment
- Wireless/Remote Access Assessment
- External Penetration Testing
- Telephony Security Assessment

- Application Security Assessment
- Social Engineering

External Penetration Testing

- It is a traditional approach to penetration testing
- The testing is focused on Servers, infrastructure and the underlying software comprising the target
- It may be performed with no prior knowledge of the site (black box)
- Full disclosure of the topology and environment (crystal/white box)
- External penetration testing involves a comprehensive analysis of publicly available information about the target such as:

  Web Servers

  Mail Servers

  Firewall

  Routers

Application Security Assessment

- Even in a well-deployed and secure infrastructure, a weak application can expose the organization's crown jewels to unacceptable risk
- It is designed to identify and assess threats to the organization through bespoke, proprietary applications or systems
- The tests check on application so that a malicious user cannot access, modify or destroy data or services within the system

Types of Application Security Assessment

Source code review:

Analyze the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit the application

Authorization Testing

Test the systems responsible for the commencement and maintenance of user sessions. Identifies the permission status of logged-in system in case of unauthorized access

Functionality Testing

Involves the testing of systems that are responsible for the functionality of the application accessible to a user

Web Penetration Testing:

- Involves a web application such as J2EE, PHP, ASPNET

- Helps to identify web application vulnerabilities such as SQL injection problems, XSS, XSRF, weak authentication, and source code exposure

Network Security Assessment

- It scans the network environment for identifying vulnerabilities and helps to improve an enterprise's security policy
- It uncovers network security faults that can lead to data or equipment being cooperated or destroyed by Trojans, denial of service attacks and other intrusions
- It ensures that the security implementations actually provides the protection that the enterprise requires when any attack takes place on a network, generally by "exploiting" a vulnerability of a system
- It is performed by a team attempting to break into the network or servers

Wireless/Remote Access Assessment

Addresses the security risk associated with an increasingly mobile workforce

Wireless testing/wireless networks:

- 802.11a/54Mbps/5GHz
- 802.11b/11Mbps/2.4GHz
- 802.11g/54Mbps/2.4GHz

Wireless testing/Wireless Networks:

- Bluetooth
- GHz signals
- Wireless radio transmission
- Radio communication channels

Telephony Security Assessment

A telephony security assessment addresses security concerns relating to corporate voice technologies.

This includes abuse of PBXs by outsiders to route calls at the targets expense, mailbox deployment and security, voice over IP (VoIP) integration, unauthorized modem use, and associated risks.

Social Engineering

- Influence and persuasion to mislead people
- Referred to as people hacking
- Psychological tricks are used to gain access to sensitive information
- Human tendency to help can be exploited
- Social engineering addresses a non-technical kind of intrusion.
- It 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 weakness, appealing to their vanity, their authority and eavesdropping are a natural technique used.
- Popular means of Social Engineering is human-based
- Conditioned not to be exceedingly suspicious
- Correlate certain behavior and appearance
- Perform background research on a company

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 eavesdropping are natural techniques used.

Penetration Tester Responsibilities

- Perform formal penetration tests on web-based applications, networks, and computer system
- Conduct physical security assessment of servers, system and network devices
- Design and create new Penetration Testing Tools and Tests
- Probe for vulnerabilities in web applications, fat/thin client applications, and standard applications
- Pinpoint methods that attackers could use to exploit weaknesses and logic flaws
- Employ Social Engineering to uncover security holes (e.g. poor user security practices or password policies)
- Incorporate business considerations (e.g. loss of earnings due to downtime, cost of engagement etc.) into security strategies
- Research document and discuss security findings with Management and IT Teams
- Review and define requirements for Information Security Solutions
- Work on improvements for security services, including the continuous enhancement of existing methodology material and supporting assets
- Provide feedback and verification as an organization fixes security issues

Security Categories

Security Categories are to be used in the combination with vulnerability and threat information in assessing the risk to an organization by operating an Information System.

Low Impact: of loss of confidentiality, integrity, and availability of organizational assets, operations, or individuals may be limited.

- Other effects are degradation in Mission Capability to perform major functions
- Degradation in efficiency

- Little damage to the assets
- Little loss of income
- Damage to individuals

Moderate Impact: If the impact of potential loss of confidentiality, integrity, and availability could be adverse on organizational assets, operation, or individuals

- Degradation of mission capability to perform functions within stipulated time period is extensively affected
- Little damage to assets
- Significant loss of income
- Harmful to individuals and may lead to loss of life or serious injuries

High Impact: if the impact of potential loss of confidentiality, integrity, and availability could be severe or catastrophic on organizational assets, operations or individual

- Severe degradation or loss of mission capability and failure of the organization to perform even one or two of its primary functions
- Major damage to the assets of the organization
- Major loss of resources and income
- Severe harm to individuals and possible loss of life or serious injuries

ROI (Return Of Investment) on Penetration Testing and Vulnerability Assessment

http://www.symantec.com/connect/articles/demonstrating-roi-penetration-testing-part-one

by Marcia Wilson