Network Security Audit

Vulnerability Assessment (VA)

Introduction

Vulnerability Assessment is the systematic examination of an information system (IS) or product to determine the adequacy of security measures. It helps to identify security deficiencies, provide data from which one can predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Features

Discover and manage all network devices and applications
Identify and remediate network security vulnerabilities
Measure and manage overall security exposure and risk
Ensure compliance with internal policies and external regulations

Why is it required?

To Identify the present vulnerability that exist in your network , like missing patches, Buffer overflow, Default user names & Password , Un used users, file/folder Sharing found on the network etc.

Who require it?

Every Company which has computer network requires this service and has critical data which flows on the network.

How this can be implemented?

Study the scope of IT architecture & components required for assessment.
Determine the boundary of analysis.
Specify people in charge of system resources and assigned tasks.
Impact analysis for Active scans, which includes assessment of Service (s) or Server (s) scans in online production.
Formulating the processes and action-plan for recuperating server's operation.
Estimate the scan process, based on the complexity of the target network (s) and hosts.
Define the scan Policy for each target. Scan Policy to define the level of scan
Information gathering, Finger printing, Port scanning, Password analysis, Attack stimulation.
Scan the targeted network (s) and host (s), based on the defined scan policy 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.
Comparing the configurations with the industry standards and rating them.
Submission of Assessment Reports with suggestions and recommendations to fix the vulnerabilities.

Service Provider Methodology

Identification of Target: Evaluating the risk of getting information about the target.
Port Scanning: Finding open ports on the target host.
System Fingerprinting: Finding what OS and services present on the target
Identification Of Vulnerabilities: Finding vulnerable services and OS
Result Collation and Report Writing: Projecting report in easy understanding way

Typical Time for implementation?

Vulnerability Assessment is done on the IP's Bases, For e.g. Service Provider take 5 IP's address to complete the above task in one single day

If the Network is heterogeneous and has multiple locations & IP address, base on this the man-days can be revised

Inter lock/weave with other standards/specifications

Service Provider use SANS TOP 20 Vulnerability & industries best practices for Vulnerability Assessment

Benefits of this Service

Enhanced ability to make effective security improvements to existing systems and applications.

Enhanced ability to comply with regulatory requirements.

More efficient allocation of available resources.

Higher return on security investments.

Can Compare Network current posture with SANS TOP 20 Vulnerabilities)

Typical ROI

Vulnerability Assessment Services help organizations identify, understand, and address security or compliance issues that affect their internal information assets.

Our in-depth and comprehensive testing also provides organizations with an accurate snapshot of their security posture along with an excellent baseline to measure change and ongoing security efforts.

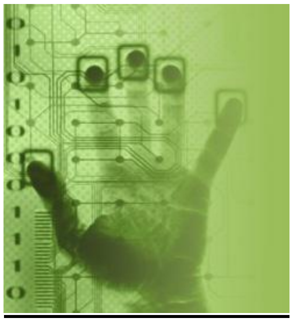
Reducing unnecessary procurement of network which cost to companies

Reducing network management cost

Utilizing full benefits of existing LAN

Reducing downtime by 90%

Ethical Hacking (Penetration Testing - PT)



Introduction

A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious hacker. The process involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities.

Features

Enables you to see if your • networks and web applications can be penetrated from the outside

Gives you a comprehensive list of • all security vulnerabilities on your perimeter network

Allows an organization to • schedule, contract, and execute third-party network assessments more quickly and cost-effectively while still gaining the benefit that comes from using the same commercial scanning tool

Provides an executive summary • which details trends, architectural, and systemic issues

Provides a rapid and efficient • inventory of the devices, services, and vulnerabilities of internet-connected networks

Why is it required?

From a business perspective, penetration testing helps safeguard your organisation against failure, through:

Preventing financial loss through fraud (hackers, extortionists and disgruntled employees) or through lost revenue due to unreliable business systems and processes.

Proving due diligence and compliance to your industry regulators, customers and shareholders. Non-compliance can result in your organisation losing business, receiving heavy fines, gathering bad PR or ultimately failing. At a personal level it can also mean the loss of your job, prosecution and sometimes even imprisonment.

Who require it?

Every Company which has computer network requires this service and has critical data which flows on the network.

How this can be implemented?

Service Provider consultant requires the IP address of the identified components & the same need to be audited from public domain.

Service Provider Methodology

- **Identification of Target:** Evaluating the risk of getting information about the target.
- **Port Scanning:** Finding open ports on the target host.
- **System Fingerprinting:** Finding what OS and services present on the target.
- **Identification Of Vulnerabilities:** With Vulnerability assessment being conducted via commercial tools and freeware, security loopholes and possible threats can be analysed
- **Exploitation:** Potential threats via pre existing vulnerabilities present within the system are exploited via running appropriate exploits, scripts etc to gain unauthorised access to systems and simultaneously escalate the attacker's privilege.
- **Result Collation and Report Writing:** Projecting report in easy understanding way, and is mapped with SAN TOP 10 Vulnerabilities.

Typical Time for implementation?

Ethical Hacking (Penetration Testing) is done on the IP's Bases, For e.g. Service Provider take 1 IP's address to complete the above task in 1.5 days
Base on the Total IP's Address the man-days can be revised

Inter lock/weave with other standards/specifications

Service Provider use industries best practices for Ethical Hacking (Penetration Testing)

Benefits of this Service

From a business perspective, penetration testing helps safeguard your organization against failure, through:

Preventing financial loss through fraud (hackers, extortionists and disgruntled employees) or through lost revenue due to unreliable business systems and processes.

Proving due diligence and compliance to your industry regulators, customers and shareholders. Non-compliance can result in your organization losing business, receiving heavy fines, gathering bad PR or ultimately failing. At a personal level it can also mean the loss of your job, prosecution and sometimes-even imprisonment.

Protecting your brand by avoiding loss of consumer confidence and business reputation.

Identifying vulnerabilities and quantifying their impact and likelihood so that they can be managed proactively; budget can be allocated and corrective measures implemented.

Typical ROI

Ethical Hacking help organizations identify, understand, and address security or compliance issues that affect their External information assets before attackers exploit them. Our in-depth and detail oriented testing also provides organizations with an accurate snapshot of their security posture along with an excellent baseline to measure change and ongoing security efforts.

Web Application Security Audit

Introduction

Web application Penetration testing can be effective, in testing activities on the security findings discovered. To meet time-to-market pressure, web applications typically move through a development life cycle that focuses on application functionality, not security. Source code security audits encompass a process where an engineer reviews the application code, scrutinizing the key security areas and functionality line-by-line. Compared to pen testing, code audits are both more time consuming and much more costly.

Features

Application Vulnerability Assessment:
Unauthorized Users: (Black Box)Evaluates the risks that are presented by Internet users who are not legitimate customers of your web application.
Authorized Users: (Grey Box) Identifies the risks presented by legitimate users who attempt to exceed their privileges or perform malicious activities.

Why is it required?

The requirement for web application security is to discovery and enumeration of the any weaknesses associated with the Client's web application which exposed to the public domain / internal network from the perspective of potential attackers with minimal or no knowledge of Client Web Application or control framework.

Who require it?

Any company who deals with online transition or dose software development

How this can be implemented?

The SERVICE PROVIDER Web-Application Penetration Test cycle walks through a series of tasks specially designed for the identification of vulnerabilities of assets exposed to the public domain. Each step is a result of carefully and meticulous researched study, which follows a proven methodology. Every stage of the methodology generates an output that may serve as a piece of information for individual reporting or as input for a subsequent task.

Few of the vulnerabilities are listed down
Xss: Evaluate the risk of code injection by malicious web users into the web pages viewed by other users.
Input data validation testing: Evaluate the risk for data input from end user.
Cookie Poisoning: Evaluate the risk of modification of the contents of a cookie in order to bypass security mechanisms.
SQL Injection: Identifies the risk to execute SQL statements via an Internet browser.
Password Brute force: Evaluate the risk of a common approach to repeatedly try guesses for the password
Running found Exploits: Evaluate the risk of common exploit found freely on web.

Service Provider Methodology

Port Scanning:
Port scanning is the process of probing system ports on the transport and network level of the target systems. Port scanning is used to enumerate live or accessible Internet services.

Here, the scan is run in various modes such as connect, SYN, FIN, Xmas, Null, UDP, and FTP Bounce to identify the operating system, version and lists of services running on a target host.

System Fingerprinting:
System fingerprinting is the process of probing target systems to confirm host operating systems and version levels. This process also gathers other explicit and implicit information about target systems.

Application Testing:
This phase involves in gathering the application information and configuration using various web attack methods (accessing all the entry points in the application). The SERVICE PROVIDER team will also use various techniques and tools to attempt the penetration of the application.

Re-Engineering:
Decompose or deconstruct the binary codes, if accessible/downloadable / necessary

Authentication:
Find possible brute force password guessing access points in the applications. Find a valid login credentials with password grinding, if possible. Bypass authentication system with spoofed tokens. Bypass authentication system with replay authentication information

Session Management:
Determine the session management information - number of concurrent sessions, IP-based authentication, role-based authentication, identity-based authentication, cookie usage, session ID in URL encoding string, session ID in hidden HTML field variables, etc.

Input Manipulation:
Find the limitations of the defined variables and protocol payload - data length, data type, construct format etc. Service Provider also test buffer overflows, Cross-site scripting of the application

Output Manipulation:
Retrieve valuable information from the client application cache, serialized objects and temporary files and objects

Information Leakage:
Find useful information in hidden field variables of the HTML forms and comments in the HTML documents.

Running vulnerability assessment tools against target hosts
Discovery and enumeration of the vulnerabilities of target hosts
Matching of discovered vulnerabilities to application's services
Collection and categorization of all vulnerabilities according to applications and operating systems

Typical Time for implementation?
Web Application Security Audit is done on the size of an application, For e.g. If an application is of 25 dyanmic pages and 100 static pages Service Provider does audit in 5 man-days.

Base on the application size the man-days can be revised

Inter lock/weave with other standards/specifications

Service Provider Follows OWASP & Industries best practices as standards

Benefits of this Service

To measure the security resilience of clients Web application, Service Provider evaluate the application vulnerability categories. Service Provider create application security profiles, and then use these profiles to determine the security strength of an application.

We find holes in applications • before the hackers do

We perform security quality • assurance before applications are released

We understand your risk and the • potential impact to your business and products

We do manual testing for • accuracy and effectiveness

We offer active knowledge • transfer of testing techniques, issues, and remediation to our customers

Typical ROI

Web application penetration testing services help organizations identify, understand, and address vulnerabilities, design flaws, and compliance issues affecting their organization's Web-based applications. By doing so, it could ultimately save an organization thousands and possibly millions of dollars in losses to reputation, customer confidence, market share, productivity, legal recourse, and more.

Wireless Security Audit

Introduction

Going wireless with network is a great choice. Wireless networks offer increased mobility and productivity to your organization. Unfortunately they can also provide an easy way for attackers to bypass your network's perimeter security. Wireless access points employing weak encryption or incorrect configurations allow attackers an untraceable gateway into your organizations network. Service Provider's wireless network assessments provide your organization an effective way to expose vulnerabilities in your wireless network.

Features

Service Provider's wireless security assessments help to mitigate the risks involved with your wireless network. The wireless security assessments offered by us, are conducted by certified information security consultants and, are designed to identify vulnerabilities and any misconfigurations in your wireless access points. We can give to demonstrable assurance, to make your wireless network a secure and optimally functional asset to your organization.

Why is it required?

Malicious intruders are constantly probing networks for access points for misconfigurations, vulnerabilities, and weak security controls to compromise network defenses. The growth in the use of remote access to networks through wireless technologies has opened the floodgates to would-be intruders and has increased risk to organizations. Service Provider has extensive experience helping clients identify access points and rogue devices, analyze their security configurations, test for vulnerabilities, and implement security policies that minimize this risk.

Who require it?

Any Organization who use wireless access point

How this can be implemented?

Locate unauthorized access points connected to your network
Analyze strength of wireless encryption
Determine and maps wireless network range
Assess configuration of wireless access points if accessible

Service Provider Methodology

Security Policies and Procedures Review: Reviewing the existing Wireless security policies, this provides a benchmark for determining whether or not a company is complying with their own policies and makes corresponding recommendations for policy modifications. Need be it, develop a new policy (Additional Man days required)

System architecture Review: Assess the network for any design flaws or misconfigurations. Read through related documentation to gain an understanding of the system's architecture and configurations of access points.

Interview with end-users: Interact with the users to determine the level of security awareness.

Review Wireless devices configuration: Verify the wireless device configurations and make appropriate recommendations to comply with industry best practices.

Verify physical installations of wireless devices: In person, verify the installation of access points by noting their physical accessibility, antenna type and orientation, and radio wave propagation into portions of the facility that don't have physical security controls. And make the necessary recommendations
Identify unauthorized access points. Scan the network for unauthorized access points as part of the assessment. Our approach to detect such points is to walk through the set up and verify the configurations of the access points

Penetration tests: Access corporate resources from a Hacker's point of view. Provide proof for the findings.
Analyze security gaps. Analyze the current security posture of the organization to identify the gaps. This includes issues with policy, network architecture, operational support, and other items that weaken security.

Reports & Recommendations: Report on the findings and recommendation for fixing the discovered issues. The detailed procedures will assist the clients to make the suggested changes. Based on the assessment findings, a structured Technical Risk Assessment will be carried out by mapping with the Threats and Vulnerability database. The outcome of this will be the Risk Assessment report.

Typical Time for implementation?
For single access point Service Provider requires 5 man-days.
Base on number of access point man-days can be revised

Inter lock/weave with other standards/specifications
Service Provider Follows Industries best practices for wireless audit

Benefits of this Service
Service Provider has pioneered cutting edge techniques for evaluating wireless networks. Understanding how enterprise vulnerabilities are exploited and how to measure subsequent risks allows our experts to create the right solutions to secure your critical assets. Working with your staff, Service Provider wireless network security consultants identify and inventory all wireless network access points, identify and exploit weaknesses in the wireless network, and assess the overall exposure of the company to wireless network attacks. They then recommend the best methods to secure the environment based on internal business requirements and best practices for wireless security.

Typical ROI
How intruders discover, DoS and • compromise wireless networks
Diluting the risks each individual faces • when using wireless networks
Security countermeasures and • best practices to reduce risk