

Penetration Testing versus Security Assessment

Both penetration testing and security assessments have their place in a security audit. The following is a short description of how AsTech views each service and which objectives are best met by each service.

General Objectives

Penetration Test Objectives:

- Capture a particular flag from outside of the target network (customer data, emails, root access) in a near real-word hacking scenario
- If flag is captured, game is over and no additional vulnerabilities will be identified
- Provide a report for third parties

Security Assessment Objectives:

- Comprehensive analysis of security environment including:
 - o Asset analysis
 - o Policy (including regulatory compliance)
 - o Technical Standards
 - o Procedures
 - o Component configurations
 - o Architecture
 - o Access controls/methods
 - o Physical security
 - o Monitoring
- Characterization of security environment against industry best practice and know vulnerabilities

Penetration Testing Does Not:

- Provide a comprehensive view of the security of a network
- Look at what assets need to be protected
- Evaluate policy or roles and responsibilities
- Usually include analysis of the many layers of security
- Test security from within the network

Information Gathering

An initial data gathering effort will be conducted by AsTech Consulting to try and determine starting IP addresses and phone numbers related to the target network environment. This data gathering will be conducted using public resources and methods that do not require more than superficial testing. The items identified in the information gathering will be checked by the target entity to determine ownership and authorization to proceed.

Some IP's and phone numbers may be of interest in testing but may not be discovered in the initial data gathering. In the interest of time and completeness of test, the target entity may want to provide additional approved starting points (IP's and phone numbers) that are to be included in the testing. AsTech will undertake an information gathering session to identify the publicly available information relative to a target, then before testing starts, we will review the starting points of the test and have the target entity include additional starting points as well as define items that are not of value in the test. This process provides a succinct way of bounding the testing while identifying what can be found in the public domain. Hours of time can be shaved off of the test through this process.

Testing

The initial testing will seek to identify vulnerabilities associated with the network architecture on the target network. Specific attention will be paid to Internet gateways, firewall systems, gateways and routers, and network servers.

AsTech Consulting will use a variety of automated tools to probe the specified networks for security vulnerabilities, known software bugs, configuration problems, and unnecessary services. Working from the data obtained during these initial tests, we will then employ additional custom tools, as well as interactive probing and analysis techniques to uncover potential security weaknesses. In addition, all documentation, experience and insight gained from the penetration testing will be carried over into subsequent phases of work.

AsTech Consulting will run scanning checks for accessible services (TCP, UDP and ICMP-based) and ports, exploitable trust relationships (such as NFS or X Windows), known software flaws and configuration errors. Our testing is based on a combination of CERT-reported vulnerabilities, previous consulting experience, and knowledge of vulnerabilities and exploitation methods gleaned from Internet newsgroups, mailing lists and "hacker" bulletin boards.

How we proceed will depend on what we find in initial scans. Our testing can be expected to check for susceptibility to most or all of the following security holes, as well as others appropriate to the specific configurations:

- Protocol-based attacks, such as packet spoofing, packet fragmentation, session hijacking, and packet eavesdropping;
- Attacks on active routing systems, network switches, remote access and WAN networking devices;
- Exploitable host-based vulnerabilities, such as password guessing and cracking, buffer overruns, suid programs, and reliance on transitive trust;
- Susceptibility of routers and hosts to SNMP and other management and informational protocol commands;
- Exploitable weaknesses in application-level software and databases

Penetration testing involves a scan of network devices and may disturb some services or cause some degradation of network performance. Testing includes interactive system probing. Attacks that are likely to cause services to be disabled for prolonged periods of time will not be tested. During testing it is normal to notice increased traffic, and there is the potential for decreased network performance while testing is under way.

The testing will not involve any activities designed to cause damage or loss of data, but the target network should be aware that some degradation of network performance or temporary denial of service may result from certain testing actions. The testing activity should be expected to generate alarms and event logs. Even though the possibility of service interruption or outage is low, the client is strongly advised to perform full backups prior to testing.

Security Assessment Detail

The security assessment provides a comprehensive view of the environment from beginning to end, inside and outside. An assessment will review architecture, data storage and transport, use of encryption, roles and responsibilities, physical security, application code review, router, server, firewall and workstation configurations, remote access methods access controls, monitoring, logging, security planning, change management, etc. In other words, a security risk assessment provides all that a penetration test would provide and more.

Information gathering

During the engagement for a security assessment, information will need to be provided on a number of aspects of the organization and infrastructure. Policy details and information on how policy is used within the organization will be gathered. Details on items that are considered corporate information assets will be gathered as well as information on how the assets are stored and managed. Information on how network components are configured will be gathered. Details on how new architecture elements are implemented and controlled will be gathered.

Testing/Analysis

Some testing is involved in the security assessment usually in the form of network scanning to validate items on the network and component configurations/vulnerabilities.

Analysis of the gathered information is made by looking at the risks associated with the environment, the assets at stake, the culture and organization, and the existing infrastructure to determine the appropriate level and layers of security controls to be applied.

How the analysis is conducted is critical to effective and efficient use of security controls. Without sensitivity to the business environment, existing infrastructure, regulatory environment, and corporate culture it is not likely that appropriate security controls will be identified.

Recommendations

The most valuable part of the security assessment is a prioritized recommendations report that defines the ease of implementation and the security benefits associated with the remediation.

Conclusion

If the choice between a penetration test and a security assessment needs to be made, a security assessment provides the comprehensive view and can really speak to the state of overall security because all of the layers involved in security are inspected. If a security assessment has already been completed along with remediation efforts, a penetration test can provide the extra layer of validation for the security of the overall environment.