tracesecurity
Compliance, simplified.

White Paper

Mitigating IT Security Risks with Penetration Tests

The First Step in Total Network Protection

Executive Overview

Penetration testing is much more than a necessary process to satisfy compliance obligations: it is a critical first step in the information and network security lifecycle and an important component of a full IT Security Compliance program. The purpose of a penetration test is to emulate real-world scenarios a hacker may use to determine (1) the feasibility of an attack, (2) where vulnerabilities may exist, and (3) the impact a successful exploit would create to the organization. Penetration testing can offer an invaluable means to establish a baseline assessment of an organization's security posture as it appears from both inside and outside the network boundaries.

In this paper we will explore the following:

1. What is a penetration test?
2. Where does a penetration test fall short?
3. Reasons to perform a penetration test.
4. Who should the organization choose to perform a penetration test?

The Role of Penetration Testing in a Comprehensive Security Program

Penetration tests alone can not provide adequate protection for network security, yet they are an integral component of a comprehensive security program. Best Practices suggest deploying the fol-lowing key measures to ensure the optimal level of protection:

1. Security Risk Assessments
2. Strong Information Security Policies
3. Training on Policies/Procedures
4. Penetration Testing
5. Vulnerability Assessments
6. Physical Protection of the Perimeter (Intrusion Detection, Firewalls, etc)

What is a Penetration Test?

Penetration testing (also referred to as "Pen Testing") is the practice of testing a computer system, network or web application to determine if it is vulnerable to unauthorized access or other malicious activity. From the entire network down to single web application layers, penetration tests are designed to analyze and substantiate many facets of a computer system. They can even test the controls and processes that are deployed around the networks and applications.

The testing process employs methods used by real-world attackers which help determine the actual security weaknesses that may be exploited by an attacker in order to compromise the system and access protected information. The overall objective of penetration testing is to provide the organization a clear view of how vulnerable their systems are to a potential attack.

The three main types of penetration tests are performed on networked computer systems for the purpose of identifying vulnerabilities within an organizations virtual infrastructure:

External Penetration Test

External testing refers to attacks on the organization's network perimeter. This is the boundary between the internal side of a network (where the organization's information assets are con-trolled) and the public side of a network which is usually managed by an internet service provider. An external penetration is an iterative process that leverages minimal access to gain greater access. The test mimics the actions of an actual attacker exploiting weaknesses in the network security, but without the usual dangers that come with an actual attack. This test examines external IT systems (for example, firewalls, web servers, online banking servers, e-mail servers, and any other externally available services) for any weakness that could be used by an external attacker to disrupt the confidentiality, integrity or the availability of the network. The process allows the organization to prioritize a plan of action and address each weakness individually.

Internal Penetration Test

Internal penetration testing examines the internal IT systems behind the network perimeter (for example, core processors, Active Directory servers, email servers, etc.) for any weaknesses that could be exploited by an attacker. It is typically performed from within an organization's technology environment, but may also be carried out remotely. This type of test usually mimics an attack originating from inside the company, perhaps from a disgruntled employee, an unauthorized visitor, or an external hacker who managed to get to the internal network via wireless access or by a successful external penetration test.

Web Application Tests

The increased use of web applications, along with the various application layer vulnerabilities, naturally makes them attractive to hackers as an entry-point for an attack. Hackers can leverage a relatively simple vulnerability to gain access to confidential information or Non-public Personal Information (NPPI), such as credit card data, social security numbers and health records.

It is critical for an organization to ensure that its web applications are not susceptible to these types of attacks. While firewalls and intrusion detection systems are an important layer of any Information Security Program, they can't readily defend against attack on web applications. Even nonpublic-facing web applications are at risk to the most common vulnerabilities, like cross-site scripting and SQL injections.

Web App tests, as they are commonly known, generally focus on assessing the code integrity of web facing applications. Although the best practice is to test the web application while still in development – or at least before the application is deployed in a live environment - that is not always an option for organizations that integrate 3rd-party apps into their electronic infrastructure. That is why it is imperative that special attention be given to testing these web-based applications periodically. Assessing web applications will not only help protect the confidential data of customers/members, but also allow the organization to demonstrate compliance to mandated legislation and regulations set forth by the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley.

Non-Traditional "Penetration Tests"

In addition to testing their networked environments, organizations should also test other sensitive areas that may be vulnerable to a breach. Most notably is testing the effectiveness of different facets of the organization's security policy and awareness programs. Although not traditionally considered a penetration test, Social Engineering testing is an invaluable part of a comprehensive security program. In fact, these tests often reveal how criminals can exploit specific vulnerabilities to literally penetrate the security of an organization in order to access confidential information.

Failure of employees to properly follow the security policies and procedures of the organization has proven to be a major vulnerability to the overall Information Security program. Social Engineering testing allows an organization to assess its Information Security policies and the employees' adherence to the policies. Thorough testing typically involves attempts to manipulate an organization's employees into allowing unauthorized access to confidential information. These tests can identify failure points and highlight areas where employees need to be further trained in order to prevent an actual breech.

Depending on whether the testing is performed on-site or remotely, different facets of the security program may be evaluated.

Onsite Social Engineering Tests

Common methods employed for onsite social engineering tests typically include having a tester pose as a "Trusted Authority", such as a delivery person or a service vendor, in order to gain entry and attempt to gain confidential information. Another common tactic is for a tester to go "dumpster diving" in an attempt to find confidential information that has been improperly discarded. These on-site tests reveal if any issues exist in the following areas:

- Proper disposal of sensitive data
- Privacy Policy awareness and implementation
- Institution Policy Awareness
- Violation reporting
- Access privileges
- Sensitive area security
- Device/System Compromise
- Technical Preventative and Detective Controls

Remote Social Engineering Tests

Testing remotely usually involves manipulating the organization's human resources by telephone or email in an attempt to get employees to divulge user names, passwords, customer NPPI or other confidential information. Common methods used in remote social engineering tests include:

- **Pretext Calling:** impersonating someone else to gain confidential information, such as biographical or account-related information
- **Phishing:** using bogus, yet authentic-looking e-mails to request information from users or direct them to a fake website that requests information
- **Email Hoaxes:** mail messages that include misinformation intended to trick the recipient into becoming involved in a larger scale \ scam

The goal of remote social engineering tests is to evaluate:

- The awareness and effectiveness of the organization's Privacy Policy
- The Institution's overall adherence to organizational policies
- The reporting of violations and suspicious activities
- Access Privileges of employees
- Privacy Filtering
- Effectiveness of technical preventative and detective controls

Where Does Penetration Testing Fall Short?

Security is a moving target that is most effectively managed with a continued lifecycle approach. There are new viruses and worms developed daily, new vulnerabilities, natural disasters, changes in the organizations and new technologies being implemented. All of these can affect the security posture in the organization at any given point-in-time. That is why it is important to recognize that while penetration testing is a critical first step in the information and network security lifecycle, it is only a baseline evaluation of security posture at a specific point in time.

Penetration tests can reveal a lot of information about an environment in a relatively short time frame, but they can also be limited in scope. It is important to understand the comprehensiveness of the tests being performed. For example, consider the household security analogy; if you test two points of entry and find fault with one of them, the tester can clearly show that the house can be broken into. However, the results of this simple test are inadequate to suggest that simply fixing the faulty entry point will make the house secure. In fact, a fault may exist at a 3rd point of entry that was not even tested, thus not remediated, which will continue to be a source of vulnerability.

Reasons to Perform a Penetration Test

Penetration testing is one of the oldest, most trusted methods used for assessing security risks because the process is designed to simulate a real-world attack using the tools and techniques em-ployed by actual hackers. Therefore, the primary reason organizations will conduct a penetration test is to find and fix vulnerabilities before a criminal does. Its early roots are in the 1970s when the Department of Defense began penetration testing to demonstrate the security weaknesses in its computer systems. The government believed that the best way to assess security was to try to break it.

The research firm, IDC, echoes this sentiment: **"The only way an organization can know its true risks is to take a "hacker's eye" approach to evaluating the effectiveness of its internal and external defenses".**

Most organizations within heavily regulated industries understand that periodically testing their security posture (through a combination of vulnerability assessments, security audits and penetration tests) is considered to be a best practice. However, many organizations that fall under the guidelines set forth by GLBA, FFIEC and HIPAA may not be fully aware they are required to have an independent third-party conduct the periodic tests.

According to the FFIEC IT Examination Handbook, "Independence provides credibility to test the results. To be considered independent, testing personnel should not be responsible for the design, installation, maintenance, and operation of the tested system, or the policies and procedures that guide its operation. The reports generated from the tests should be prepared by individuals who also are independent of the design, installation, maintenance, and operation of the tested system."

FFIEC Guidelines suggest that the frequency of testing should be determined based on the results of the organization's risk assessment, although "high risk systems should be subject to an independent test at least once a year." The guidelines also point out that institutions should take into consideration certain factors that may require increasing the frequency of testing, such as significant changes to a network configuration, results of other testing, and even changes in potential attacker profiles and techniques.

PCI-DSS regulations even require high-volume merchants and service providers to have a security assessment annually. As part of the annual assessment, merchants are required to have a penetration test on all systems connected to the cardholder data. In addition to being a requirement for some organizations, there are various business and technical benefits that organizations reap from penetration testing.

Business Benefits of Penetration Testing

- Avoid network downtime due to breach
- Provides a way to evaluation the effectiveness of security controls and countermeasures
- Helps identify the effectiveness of security awareness training
- Discover methods hackers could use to compromise customer/member data
- Helps organizations understand their security posture
- Provides information to support regulatory compliance
- Provides a strong basis for helping to determine appropriate security budgets
- Allows IT staff to identify real and potential vulnerabilities without being overburden by numerous false positives
- Assists IT in prioritizing remediation for discovered vulnerabilities
- Helps verify the findings of the IT staff and track known vulnerabilities
- Enhances the effectiveness of an overall security lifecycle
- Demonstrate the feasibility of an attack and the impact of an attack without incurring the risk
- An effective way to test new technology and reconfigured systems before implementing them in a live environment

Penetration Tests vs. Vulnerability Assessments

Due to a few superficial similarities between vulnerability assessments and penetration tests, there seems to be confusion surrounding the appropriate uses of the two unique tests. Therefore, it may be helpful to classify vulnerability assessments as a passive approach and penetration testing as an active approach when evaluating network security.

A vulnerability assessment may be considered passive because its goal is simply to identify all the potential vulnerabilities that exist on the network without compromising the system. Conversely, penetration testing may be viewed as active because the process mimics the actions of a real-world attack to breach security and gain as much access as possible.

The chart below details the primary differences between each test:

	Vulnerability Assessments The Passive Approach	Penetration Testing The Active Approach
Scope of Test	Scans network for all potential vulnerabilities. Does not simulate attacks that will allow for testing of other security technologies (IDS, IPS, Firewall, etc.). Does not address connections between network, endpoint and application components.	Identifies actual vulnerabilities and determines if they can be exploited. Employs real-world attack methods to determine the adequacy of other security technologies, policies and procedures. Exploits trust relationships between networks, endpoints, applications and end users to determine effective paths of attack.
How Test Results Are Used	Vulnerabilities are categorized based on standardized information, but not specific to the target network. Provides false positives and identifies vulnerabilities that cannot be exploited.	Tests vulnerabilities on a specific network and its resources, enabling prioritization of remediation efforts. Identifies only those vulnerabilities that pose actual threats to network resources, then exploits those vulnerabilities.
Remediation Assistance	Produces a lengthy list of vulnerabilities, with limited types of remediation options (usually widespread patching or code revision).	Potential risks of specific vulnerabilities are assessed which allows end-users to prioritize remediation strategies and test the effectiveness of proposed solutions.
Assessment of Security Risk	Does not effectively gauge security risk because the test only identifies missing patches or improper configurations within the network.	Evaluates risk based on tangible threats to the network. Mimics the actions of real-world hackers and malware attacks to provide a snapshot of the network's security posture.

Who Should the Organization Choose to Perform Penetration Tests?

The internal IT departments at many organizations are certainly capable of performing a certain degree of penetration tests, yet most departments lack the knowledge and experience to conduct a comprehensive and accurate battery of tests. Not only is the testing process a very labor-intensive activity, it also requires great expertise to minimize the risk to targeted systems. As discussed in the previous section, many organizations are required to partner with an independent third party to conduct periodic penetration tests (as well as other security audits and assessments) that adhere to a specific set of standards and guidelines.

Penetration tests are typically performed by a security service provider with the required best practice expertise and field proven experience. As a result, most IT organizations find that with the help of an experienced security partner that they can much more effectively and economically address the risk factors that are found during penetration testing. The chart below lists a number of important questions each organization must consider when selecting a Penetration Test Service Provider.

Questions To Ask Potential Penetration Test Providers:

- Does the provider use a documented methodology to perform the tests?
- Are there qualified professionals available for remediation assistance?
- Does the service provider have adequate liability insurance?
- Can a company representative be present to oversee the penetration test?
- Does the service provider have relevant references?
- Will the service provider have relevant references?
- Will the service provider show example deliverables?
- Does the service provider offer a software solution to manage the process?
- Does the provider offer both onsite and remote options?
- Is there an easy way to convert results into a readable report?
- What are the provider’s security credentials?
- Will the service provider utilize manual hack methods to discover vulnerabilities or rely on automated scanning techniques?
- Will the provider notify you immediately if high-risk vulnerabilities are found during the test, rather than waiting to inform you until the final report?

When selecting a third-party provider for penetration tests, organizations should perform careful due diligence on each potential provider. An important consideration in the process is to avoid conflicts of interest. To maintain compliance with FFIEC regulations, organizations should eliminate the partner who provided, installed or manages the system(s) to be tested. Conflicts may arise if the network partner that administers an organization’s IT infrastructure also tests its security posture. Simply stated, it is not a good practice for a vendor to check his own work. An independent set of eyes will provide an unbiased evaluation of the vulnerabilities and flaws within the system.

Conclusion

Penetration testing is not the end all answer for security testing. It does not replace other security measures such as comprehensive vulnerability assessment, a full security assessment, Policy Assessment or a comprehensive risk assessment. However, a penetration test is a valuable part of comprehensive security program and can provide clear and concise direction on how to secure an IT infrastructure from real-world attacks and the potential risk of vulnerabilities.

Security compliance best practices state that each organization should regularly test their information security program to ensure confidentiality, integrity, and availability of data. Partnering with a qualified and experienced third party provider who is independent of any responsibilities concerning the design, installation or maintenance of the organization’s network is the suggested method to maintain compliance and accurate test results.

IT Systems change, new threats emerge, and business processes are updated. Testing should be repeated at frequent intervals and should be part of an overall IT security compliance program that includes comprehensive security assessments on the internal and external network, security policy reviews and end user security awareness.

To Learn More

TraceSecurity offers various types of penetration testing, as well as full IT Security Compliance, Risk and Audit solutions. For more information about TraceSecurity products and services, contact us at **877-275-3009**, or visit **www.tracesecurity.com.**

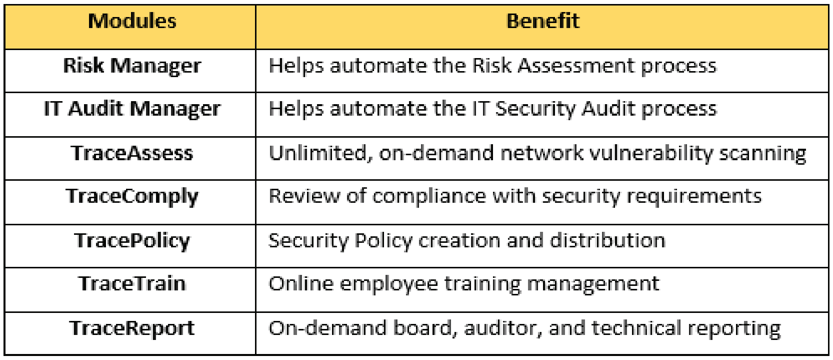
References used in this resource:

1. Information Supplement: Payment Card Industry Data Security Standard (PCI DSS) Requirement 6.6
2. Health Insurance Portability and Accountability Act of 1996 Security Rule; Section §164.308(a)(1)(i))
3. FFIEC IT Examination Handbook; Information Security Booklet
4. NIST Special Publication 800-42: GUIDELINE ON NETWORK SECURITY TESTING

The Advantage of a Comprehensive Software Solution

Managing all the aspects of an information security program can be a daunting task. That's why TraceSecurity has developed **Compliance Manager™**, a suite of cloud-based software tools to help organizations streamline each process. Compliance Manager™ allows users to develop standard procedures based on best practice standards that adhere to the appropriate compliance regulations.

One of the most beneficial advantages of Compliance Manager™ is the ability to have access to all the necessary tools to identify, evaluate and remediate security issues within one comprehensive portal.



Modules	Benefit
Risk Manager	Helps automate the Risk Assessment process
IT Audit Manager	Helps automate the IT Security Audit process
TraceAssess	Unlimited, on-demand network vulnerability scanning
TraceComply	Review of compliance with security requirements
TracePolicy	Security Policy creation and distribution
TraceTrain	Online employee training management
TraceReport	On-demand board, auditor, and technical reporting

About TraceSecurity's Penetration Tests

Internal Penetration Testing

TraceSecurity's Internal Penetration Test follows documented Best Practices security testing methodology. This test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability, or integrity of the network, thereby allowing the organization to address each weakness. TraceSecurity can perform this testing, both onsite or remotely, and includes:

- Internal Network Scanning
- System Fingerprinting
- Exploit Research
- Limited Application Layer Testing
- Firewall and ACL Testing
- Password Aging and Strength Testing
- Database Security Controls Testing
- Hardened Server/Device Configuration Tests
- Port Scanning
- Services Probing
- Manual Vulnerability Testing & Verification
- Manual Configuration Weakness Testing & Verification
- Administrator Privileges Strength Testing
- Network Equipment Security Controls Testing
- Internal Network Scan for Know Trojan/Hacker Ports
- Third-Party/Vendor Security Configuration Testing

TraceSecurity's Internal Penetration Test also includes on-demand access to the TraceAssess and TraceReport modules of our flagship solution TraceCompliance Manager. The TraceAssess module provides on-demand vulnerability scanning of your network. The TraceReport module allows reports to be generated as needed for both executive/board level and technical staff.

External Penetration Testing

TraceSecurity's External Penetration Test follows documented Best Practices security testing methodology.
The TraceSecurity test includes:

- External Network Scanning
- System Fingerprinting
- Exploit Research
- Firewall and ACL Testing
- Password Strength Testing
- Remediation Retest
- Port Scanning
- Services Probing
- Manual Vulnerability Testing and Verification
- Intrusion Detection/Prevention System Testing
- External Network Scan for Know Trojan/Hacker Ports

TraceSecurity's External Penetration Test also includes on-demand access to the TraceAssess and TraceReport modules of our flagship solution TraceCompliance Manager. The TraceAssess module provides on demand vulnerability scanning of your network. The TraceReport module allows reports to be generated as needed for both executive/board level and technical staff.

Web Application Tests

TraceSecurity's Application Test is an analysis and report on defined online Applications, identifying weaknesses in: general architecture, session management, transport security, access control and authorization, logging, data validation, system attacks, parameter manipulation, privacy concerns and cryptographic algorithms. TraceSecurity Application Test is based on the Open Web Application Security Project (OWASP) methodology. This in depth analysis will provide up-to-date security auditing for vulnerabilities such as:

- Input Validation Attacks
- Cross Site Scripting Attacks
- CGI Vulnerabilities
- Cookie Theft
- Web/Application Server Insecurity
- Security of Plug-Ins & Developer Code
- Privacy Exposures
- Software Infrastructure/Design Weaknesses
- Script Injection Attacks
- Password Cracking
- User Privilege Elevation
- Database Vulnerabilities
- 3rd Party Software Vulnerabilities

Social Engineering Tests

TraceSecurity is a foremost authority on combating Social Engineering. With over 1,000 Social Engineering attempts for a variety of organizations around the world, TraceSecurity's expertise has been recognized by major news organizations, including recurring appearances within special consumer safety segments NBC's Today Show and several featured articles for print and online media outlets like the Associated Press, MSNBC, FOXNEWS.com and Wall Street Technology.

During the Social Engineering testing, TraceSecurity experts attempt to manipulate an organization's employees into allowing unauthorized access to confidential information. This allows the organization to test their Information Security Policy and their employees' adherence to that policy. TraceSecurity has designed techniques that can be performed both onsite and remotely.

During an onsite engagement, the TraceSecurity experts will use various techniques to gain physical access to obtain records, files, and/or equipment that may contain confidential information. The remote Social Engineering engagement involves the manipulation of the organizations by telephone or email in an attempt to get employees to divulge user names, passwords, customer NPPI or other confidential information.

The onsite engagement techniques typically include both **"Dumpster Diving"** and **"Trusted Authority"** dis-guises, such as fire inspectors, air condition repairman, pest control employee, etc. The onsite engagement tests for the following vulnerabilities:

- Proper Disposal of Sensitive Data
- Institution Policy Adherence
- Access Privileges
- Device/System Compromise
- Privacy Policy Awareness & Implementation
- Violation Reporting
- Sensitive Area Security
- Technical Preventive and Detective Controls

The remote Social Engineering engagement involves the manipulation of the organizations by telephone or email in an attempt to get employees to divulge user names, passwords, customer NPPI or other confidential information. The remote engagement techniques typically include:

- **Pretext calling:** impersonating someone else to gain confidential information, such as biographical or account-related information
- **Phishing:** using bogus, yet authentic-looking e-mails to request information from users or direct them to a fake Web site that requests information
- **Email Hoaxes:** email messages that include misinformation intended to trick the recipient into becoming involved in a larger scale scam

The remote engagement tests for the following vulnerabilities:

- Privacy Policy Awareness & Implementation
- Violation Reporting
- Privacy Filtering
- Institution Policy Adherence
- Access Privileges
- Technical Preventive and Detective Control

About TraceSecurity

TraceSecurity is a leading provider of cybersecurity and compliance solutions that helps organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. With a combination of software and services, TraceSecurity can help organizations manage their information security program and supplement it with third-party validation.