ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Penetration Testing

Daisy Suman[1], Sarabjit Kaur[2], Geetika Mannan[3]

M.Tech Computer Science& Engineering, CT Institute of Technology & Research, Jalandhar, India [1,3]

HOD, Computer Science& Engineering, CT Institute of Technology & Research, Jalandhar[2]

Abstract: Penetration tests are an excellent method for determining the strengths and weaknesses of a network consisting of computers and network devices. However, the process of performing a penetration test is composite, and without care can have disastrous effects on the systems being tested. The goal of this is not to cause damage, but more to identify attack surfaces, vulnerabilities, and other security weaknesses from the perspective of an attacker. Such testing can range across all aspects of a system; the areas of computer, operational, personnel, and physical security can all encompass potential weaknesses that a malicious attacker can use, and thus a penetration tester may examine. Depending on the organization's prime concern, risk assessment, and policies, some of these areas may be out of scope or not deemed as important, so a decreased scope penetration test may be conducted.

Keywords: penetration testing; network security; vulnerability; testing; pen testing tools.

I. INTRODUCTION

Penetration testing is the process of attempting to gain access to resources without the knowledge of their credentials other normal means of access. If the priority is on computer resources, then example of successful penetration would be obtaining confidential documents, databases and protected information.

Figure1. Collecting data in an unauthorized manner

Penetration testing is a form of stress testing which exposes weaknesses. The main thing that separates a penetration tester from attacker is permission. The penetration tester will have authorization from the owner of the computing resources that are being testing and will be responsible to provide a report. The goal of penetration testing is to increase the security of the computing resources being tested. In many cases, a pen tester will be given user level retrieve and in those cases, the goal would be to upgrade the status of the account or user other means to gain access to additional information that a user of that level should not have retrieve to. Penetration testing is a comprehensive method to test the complete, integrated, operational, and trusted computing base that consists of hardware, software and people. The process involves an active analysis of the system for any potential vulnerabilities including poor or improper system configuration, hardware and software flaws, and operational weaknesses in the process or technical countermeasures. Penetration testing, also known as pen testing , is one way to assess the security of a computer system or network, also that of online computing resources

II. PENETRATION TESTING

This process is carried out by simulating an unauthorized break both by malicious outsiders as well as by insiders. . It helps to find vulnerabilities that an attacker could exploit. A penetration test usually involves the use of attacking methods conducted by trusted individuals that are similarly used by hostile intruders or hackers. Pen tests can be automated with software applications or they can be performed manually.

Either way, the process includes collecting information about the target before the test , identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings. Most penetration tests involve looking for combinations of vulnerabilities on one or more systems that can be used to gain more access than could be achieved through a single vulnerability.

III. WHY CONDUCT PEN TESTING?

Penetration testing is often done for two reasons. This is either to expand upper Management recognition of security issues or to test interruption awareness and response capabilities. It also helps in accommodating the higher management in decision-making processes. The managing organization might not want to tackle all the unprotected data that are found in a vulnerability assessment but might want to specify its system weaknesses that are found through a pen test.

It can address all the shortcomings that are found in a vulnerability assessment can be expensive and most organizations might not be able grant the budget to do this .Penetration tests can have serious outcomes for the network on which they are run.

If it is being poorly conducted it can cause obstruction and machine fails. It can result in the exactly the thing it is purposeful to prevent. It is therefore necessary to have approval from the management of an organization before conducting a penetration test on its systems or network

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

IV. TYPES OF PEN TESTING

Testing is about variation-- finding the things in the software and its environment that can be modified, modifying them, and seeing how the software responds. The purpose is to ensure that the software performs reliably and securely under reasonable and even unreasonable production scenarios. So the most basic planning a tester can do is to understand what can be modified and what ways that modification needs to be staged for testing.

The various types of tests are:

Network services test: This is one of the most common types of penetration tests, and involves finding target machines on the network, searching for available network services, and then using them irreverently. Some of these network service penetration tests take place remotely across the Internet, targeting the organization networks.

Client-side test: This type of penetration test is intentional to find vulnerabilities in and to utilize client-side software, such as web browsers, media players etc.

Web application test: This type of penetration tests check for security vulnerabilities in the web-based applications and programs used and installed on the target environment.

Remote dial-up war dial: This type of penetration tests check for modems in a target environment, and normally involve password guessing or brute forcing to access to systems connected to discovered modems.

Wireless security test: This type of penetration tests includes discovering a target's physical environment to find uncertified wireless access points or certified wireless access points with security weaknesses.

Social engineering test: This type of penetration test involves attempting to make a user to disclose sensitive information such as a password or any other delicate data. These tests are often conducted over the users or employees, estimating actions, methodology, and user understanding.

4.1. PENETRATION TESTING STRATEGIES

Targeted testing

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes mentioned as a "lights-turned-on" approach because everyone can see the test being performed**.**

External testing:-This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The main goal is to find out if an outside attacker can get in and how far they can get in once they've acquired access.

Internal testing:-This test imitate an inside attack behind the firewall by a certified user with standard access privileges. This kind of test is useful for evaluating how much damage a disappointed employee could cause.

Blind testing: A blind test strategy replicate the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test in advance. Particularly, they may only be given the name of the company. Because this kind of test can require a ample amount of time for exploration, it can be expensive.

Double blind testing:-Double blind testing takes the blind test and carries it a step further. In this type of pen testing, only specific number of people within the organization might be aware a test is being carried out. Double-blind tests can be helpful for testing an organization's security monitoring and incident identification as well as its response procedures.

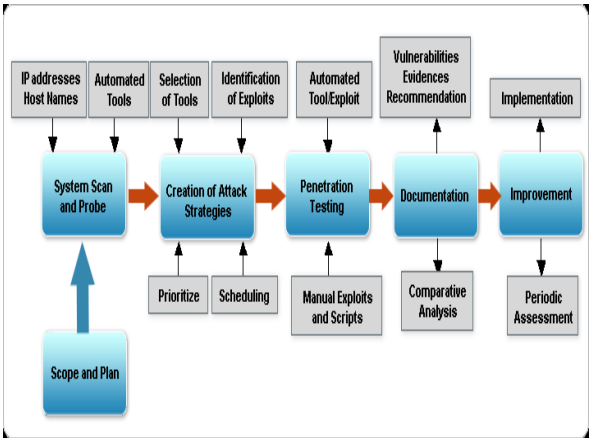

Figure 2 Penetration Testing Techniques

V. METHODOLOGY OF PEN TESTING

Once the threats and vulnerabilities have been estimated, design the testing to address the risks identified throughout the environment. The penetration test should be proper for the complexity and size of an organization. . The purpose of penetration testing is to determine whether unauthorized access to key systems and files can be achieved. If entry is achieved, the vulnerability should be corrected and the penetration test re-performed until the test is clean and no longer allows unauthorized access or other malicious activity.

Planning

In the planning phase, rules are recognized, management support is concluded, and the testing goals are set. The planning phase sets the preliminaries for a successful penetration test. No authentic testing occurs in the planning phase.

Discovery

The discovery phase starts the authentic testing. Network scanning (port scanning) is used to discover probable targets. In addition to port scanning, other techniques are commonly used to collect information on the targeted network.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

The second part of the discovery phase is vulnerability analysis. In this phase, services, applications, and operating systems of examined hosts are compared against vulnerability databases. Generally human testers use their own database or public databases to identify vulnerabilities manually.

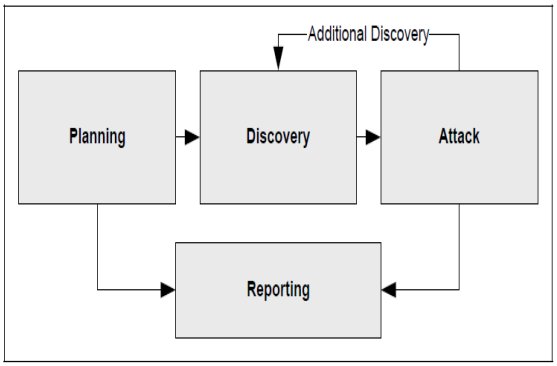

FIGURE 3 Four Stages Of Pen Testing

Attack

Executing an attack is at the heart of any penetration test. Figure 3 represents the individual steps of the attack phase—the process of verifying previously identified potential vulnerabilities by attempting to exploit them. If an attack is succeeded, the vulnerability is verified and safeguards are identified to mitigate the associated security exposure. In the event an attack on a specific vulnerability proves impossible, the tester should attempt to exploit another discovered vulnerability. If testers are able to exploit a vulnerability, they can install more tools on the target system or network to facilitate the testing process. These tools are used to gain access to additional systems or resources on the network, and obtain access to information about the network or organization.

Testing and analysis on multiple systems should be conducted during a penetration test to determine the level of access an adversary could gain. This process is represented in the feedback loop between the attack and discovery phase of a penetration testing While vulnerability scanners only check that a vulnerability may exist, the attack phase of a penetration test use the vulnerability, confirming its presence. Most vulnerabilities used by penetration testing and malicious attackers fall into the following categories:-

- **Misconfigurations**:- Misconfigured security settings, specially insecure default settings, are easily useable.

- **Kernel Defects**:- Kernel code is the core of an OS, and enforces the overall security model for the system—so any security flaw in the kernel puts the entire system in danger.

- **Buffer Overflows**:- A buffer overflow occurs when programs do not adequately check input for appropriate length. When this occurs, arbitrary code can be introduced into the system and executed with the privileges often at the administrative level of the running program

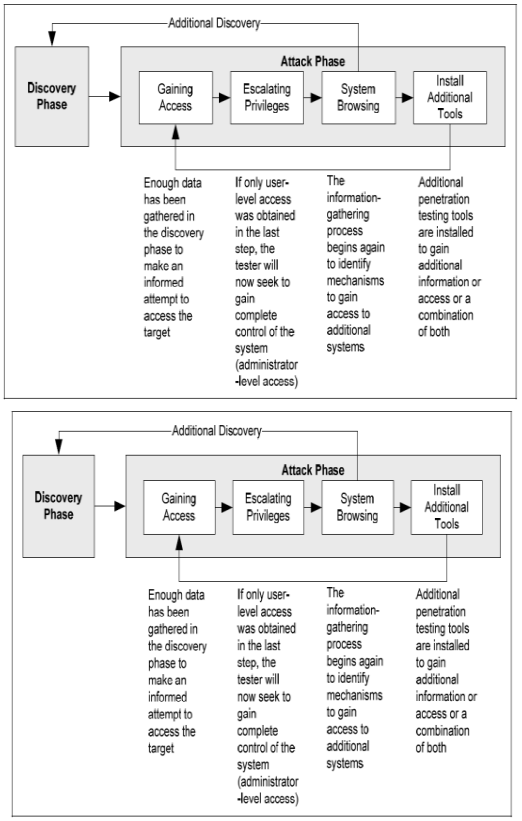

Figure 4 Attack Phase Steps with Loopback to Discovery Phase

Reporting

The reporting phase occurs concurrently with the other three phases of the penetration test. In the planning phase, rules of participation, test plans and written permission are evolved. In the discovery and attack phase, written logs are usually kept and regular reports are made to system administrators. Generally, at the end of the test an overall testing report is developed to describe the recognized vulnerabilities, provide a risk rating, and to give information on the reduction of the discovered weaknesses.

Penetration testing is important for deciding how vulnerable an organization's network is and the level of damage that can occur if the network is compromised. Because of the high cost and possible impact, annual pen testing may be adequate. The results of penetration testing should be taken very seriously and discovered vulnerabilities should be reduced

VI. PENETRATION TESTING VS VULNERABILITY ASSESSMENT

A vulnerability assessment usually involves a mapping of the network and systems attached to it, an identification of the services and versions of services running and the creation of a catalogue of the vulnerable systems. Vulnerability assessment normally forms the first part of a penetration test. The auxiliary step in a penetration test is

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

the utilization of any detected vulnerabilities, to confirm their presence, and to diagnose the damage that might result due to the vulnerability being utilized and the resulting influence on the organization.

In comparison to a penetration test a vulnerability assessment is not so unwanted and does not always require the same technical capabilities. Adversly it may be impractical to conduct such a thorough assessment that would guarantee that the most damaging vulnerabilities (i.e., high risk) have been identified.

The difference between a penetration test and a vulnerability assessment is becoming a significant issue in the penetration testing profession. There are number of penetration testers that are only capable of performing vulnerability assessments and yet present themselves as penetration testers

VII. PENETRATION TESTING TOOLS

Metasploit:- It is huge. Developed by Rapid7 and used by every pen tester and ethical hacker in the world. The Metasploit Project is a security project which delivers information about security vulnerabilities and helps penetration testing and Intrusion detection. The open source project – known as the Metasploit Framework, is used by security professionals to implement exploit code against a remote target machine – for penetration testing of course.

Nessus:- It is another giant – a security tool that focuses on vulnerability scanning. There is a free and paid version – free for personal use. Essentially Nessus scans for various types of vulnerabilities: ones that check for holes that hackers could exploit to gain control or access a computer system or network. Furthermore, Nessus scans for possible misconfiguration.

John The Ripper has the coolest name on Security Pen testing Tools. This very popular security tool, often abbreviated just to "John" is a free password cracking software tool. Intially created for the UNIX operating system, it currently works on every utmost operating system. Undoubtely , this tool is one of the most popular password testing and breaking programs used by information security professionals. The pen testing tool combines various password crackers into one concise package which is then able to identify password hash types through its own customizable cracker algorithm.

Acunetix :- It has a free and paid version. This hacking tool has many uses but in kernal it tests and reports on SQL injection. This security tool generates detailed reports that identify security issues and vulnerabilities.

Network Fingerprinting:- Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on Internet servers. Fingerprinting can be accomplished "passively" by sniffing network packets passing between hosts, or it can be accomplished "actively" by transmitting specially created packets to the target machine and analyzing the response**.** Passive fingerprinting is nonintrusive. It entirely observes the traffic on the network to determine the type and version of an operating system or application, but it does not actively examine the target by sending data, thus ignoring detection

VIII. NETWORK FINGERPRINTING ONLINE TOOLS

Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on Internet servers. Fingerprinting can be accomplished "passively" by sniffing network packets passing between hosts, or it can be accomplished "actively" by transmitting specially created packets to the target machine and analyzing the response**.**

To perform effective fingerprinting / reconnaissance against a target network using online tools. we must do an external penetration test (black-box) to a client company and the only initial information that we receive is the company name. The initial phase of the test must be to do information gathering and footprinting the client's external network.

Let's take an example do an external penetration test against **flipkart, Inc.** Since we do not have any information about the company's network, our first intention is to find all possible entry points, meaning all external IP addresses and their associated DNS names.

1. Finding sub domain

We start by manually searching public sources for domain names belonging to the target company (Flipkart). Of course, flipkart.com is the company's main domain and a simple Whois Lookup on this name gives us the response below:-

Starting query... [2014-04-22 11:51:14] Stay on this page for results!
Searching for subdomains - method 1 of 3 ...
Found 0 subdomains (total 0 unique)
Searching for subdomains - method 2 of 3 ...
Found 13 subdomains (total 13 unique)
Searching for subdomains - method 3 of 3 ...
Found 3 subdomains (total 14 unique)
Total 14 unique subdomains found:
digital.flipkart.com
download.flipkart.com
www.flipkart.com
api.flipkart.com
new.flipkart.com
m.flipkart.com
cms.flipkart.com
webreader.flipkart.com
test.flipkart.com
email.flipkart.com
img.flipkart.com
blog.flipkart.com
next.flipkart.com
www1.flipkart.com
Query finished [2014-04-22 11:51:25]

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

1. Whois Lookup

This tool authorize you to perform whois lookups online. 'Whois' is the name of the procedure that is used to examine the servers operated by Regional Internet Registries, which hold information about every method (IP address or domain name) registered on the Internet.
The information that you can gather about a resource is:

- Name of the company's holder
- Address of the company's holder
- The IP range that a IP belongs to
- phone number
- email
- Administrator's name
- Name servers

Parameters

- IP address or domain name: This recognizes the internet resource that you want to find information about.

Starting query... [2014-04-22 12:41:38] Stay on this page for results!
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered with many different competing registrars.

Go to http://www.internic.net
for detailed information.
Domain Name: FLIPKART.COM
Registrar: GODADDY.COM, LLC
Whois Server: whois.godaddy.com
Referral URL: http://registrar.godaddy.com
Name Server: PDNS1.ULTRADNS.NET
Name Server: PDNS2.ULTRADNS.NET
Name Server: PDNS3.ULTRADNS.ORG
Name Server: PDNS4.ULTRADNS.ORG
Name Server: PDNS5.ULTRADNS.INFO
Name Server: PDNS6.ULTRADNS.CO.UK
Status: clientDeleteProhibited
Status: clientRenewProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Updated Date: 16-apr-2013
Creation Date: 03-jun-2007
Expiration Date: 03-jun-2022

>>> Last update of whois database: Tue, 22 Apr 2014 12:38:50 UTC <<<

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Domain Name: FLIPKART.COM
Registrar URL: http://www.godaddy.com
Registrant Name: Flipkart Internet
Registrant Organization: Flipkart Internet Private Limited
Name Server: PDNS3.ULTRADNS.ORG
Name Server: PDNS2.ULTRADNS.NET
Name Server: PDNS6.ULTRADNS.CO.UK
Name Server: PDNS4.ULTRADNS.ORG
Name Server: PDNS1.ULTRADNS.NET
Name Server: PDNS5.ULTRADNS.INFO
DNSSEC: unsigned
For complete domain details go to:
http://who.godaddy.com/whoischeck.aspx?domain=FLIPKART.COM
Query finished [2014-04-22 12:41:39]

2. DNS Zone Transfer

DNS Zone Transfer' authentic you to detect if your target's name servers are vulnerable to DNS zone transfers. DNS servers should not authorize zone transfers to any IP address from the Internet. Since zone files contain entire information about domain names, subdomains and IP addresses put together on the target name server, collecting this particulars that are useful for increasing your attack surface and for best understanding the inner structure of the target

Parameters

Domain to query: This is the main domain name for which you want to attempt zone transfer.
Starting query... [2014-04-22 12:15:56] Stay on this page for results!

Searching for name servers of domain new.flipkart.com ...
Found name server: com is an alias for flipkart.com
Found name server: pdns2.ultradns.net
Found name server: pdns5.ultradns.info
Found name server: pdns6.ultradns.co.uk
Found name server: pdns4.ultradns.org
Found name server: pdns1.ultradns.net
Found name server: pdns3.ultradns.org

Attempting zone transfer against name server: com is an alias for flipkart.com...
Attempting zone transfer against name server: pdns2.ultradns.net...
Trying "new.flipkart.com"
; Transfer failed.
Trying "new.flipkart.com"
Using domain server:
Name: pdns2.ultradns.net
Address: 204.74.109.1#53
Aliases:

Host new.flipkart.com not found: 5(REFUSED)
; Transfer failed.
Attempting zone transfer against name server: pdns5.ultradns.info...
Trying "new.flipkart.com"
; Transfer failed.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Trying "new.flipkart.com"
Using domain server:
Name: pdns5.ultradns.info
Address: 204.74.114.1#53
Aliases:

Host new.flipkart.com not found: 5(REFUSED);
Attempting zone transfer against name server: pdns6.ultradns.co.uk...
Trying "new.flipkart.com"
; Transfer failed.
Trying "new.flipkart.com"
Using domain server:
Name: pdns6.ultradns.co.uk
Address: 204.74.115.1#53
Aliases:

Host new.flipkart.com not found: 5(REFUSED)
; Transfer failed.
Attempting zone transfer against name server: pdns4.ultradns.org...
Trying "new.flipkart.com"
; Transfer failed.
Trying "new.flipkart.com"
Using domain server:
Name: pdns4.ultradns.org
Address: 199.7.69.1#53
Aliases:

Host new.flipkart.com not found: 5(REFUSED)
; Transfer failed.
Attempting zone transfer against name server: pdns1.ultradns.net...
Trying "new.flipkart.com"
; Transfer failed.
Trying "new.flipkart.com"
Using domain server:
Name: pdns1.ultradns.net
Address: 204.74.108.1#53
Aliases:

Host new.flipkart.com not found: 5(REFUSED)
; Transfer failed.
Attempting zone transfer against name server: pdns3.ultradns.org...
Trying "new.flipkart.com"
; Transfer failed.
Trying "new.flipkart.com"
Using domain server:
Name: pdns3.ultradns.org
Address: 199.7.68.1#53
Aliases:

Host new.flipkart.com not found: 5(REFUSED)
; Transfer failed.
Query finished [2014-04-22 12:15:5]

3. FINDING Virtual Hosts

A single web server can be assembled to run multiple websites at onetime, under various domain names. These are the virtual hosts (or vhosts) and they are frequently found in shared hosting environments.
Example:
www.company1.com -> 109.11.231.5
test.company2.com -> 109.11.231.5
sales.company3.com -> 109.11.231.5

As a pen tester, finding all the vhosts that run on a web server (based on its IP address) is important because each website may contain vulnerabilities that infect the same server. Moreover, if one website is settled, there is a high chance that the attacker gains uncertified access to the other websites also that are running on the same server. Hence, testing all the vhosts is compulsary for a entire coverage of the pen test.

Parameters
IP address or hostname: This recognizes the server on which you search for virtual hosts. If a hostname is given, DNS purpose will be tried first in order to find its IP address.

Add DNS enumeration: When this option is enabled, the tool will try to do DNS enumeration after all previous methods have been completed. DNS enumeration will be done for each domain name formerly discovered in order to find subdomains that point to the same IP address.

Starting query... [2014-04-22 12:39:14] Stay on this page for results!

Searching for virtual hosts on ip: 180.179.145.106
Found 2 virtual hosts. Validating DNS resolution ...
1 virtual hosts resolve to the given IP address

www.flipkart.com 180.179.145.106
Query finished [2014-04-22 12:39:19]

4. Url Fuzzer

The 'URL Fuzzer' can be used to find hidden files and directories on a web server by fuzzing.
This is a detection activity which authentic you to discover resources that were not meant to be publicly accessible. Moreever, 'security by anoymity' is not always the better practice and it is our job as pentesters to disclose the hidden locations which may contain sensitive information.

Parameters

Base URL: This is the URL on the target server that will be fuzzed. All the peteion will be done by using this value as main url
Search for directories: If selected, the tool will find all directories located at the main url
Search for files: If selected, the tool will search for files located at the main url. You can identify the file extension that you want to search, including double extensions (ex. .php.old, .jsp.bak, .tgz, etc)
Starting query... [2014-04-22 12:59:59] Stay on this page for results!

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Searching for hidden files with extension: .txt ...
00% done...
10% done...
20% done...
30% done...
40% done...
50% done...
60% done...
70% done...
80% done...
90% done...
100% done...

Total 1 directories found
Directories HTTP Code
/sitemap/ 403
Query finished [2014-04-22 13:01:46]

IX. ADVANTAGES OF PEN TESTING

Discovering the most likely attack vectors that you will face

Each network or system is designed somewhat distinctly from others, even others of the identical kind. This applies especially to mature long running networks in which new devices, servers, website connections, databases and software get attached over time. Because of this, the most likely attack vectors can vary from case to case based on both design and system type. By performing a rigorous pen test, you'll rapidly identify what the easiest route of attack into your company systems is and be able to reassemble based on what you learn. Hackers and other intruders almost always take the easiest possible route when attempting to intrude and penetration tests will feel out your entire network/system to make sure that no easy routes are left open..

Discovering numerous smaller errors that could lead to high level risks

The most problems that get discovered through pen tests are numerous small things that by themselves don't pose an enormous immediate risk to your secured systems. However, by leaving these little defects open, you're giving potential hackers a chance to take benefit of them in such a way that several small security weaknesses can be combined and utilized together to open a much larger crack that leads to a total neglect of what you want to keep safe.

X. DISADVANTAGES OF PENETRATION TESTING

Penetration testing does generate some dispute and not all parties are consistent about its cost vs. benefit. There are a pair of things to consider previously you make the leap and financial outlay of having a test conducted.

Inperfect impression of security leading to unwarranted confidence

By performing a pen test and coming through with a clean bill of strongness, you might find yourself tempted to think that your network or system is protected and that you can rest easy. This is threating for two reasons. First, the test mainly does not address all important security issues and while it can give good signal of how an external attacker might penetrate and damage your network. However, unless truly comprehensive, a pen test will detect possibly entry weaknesses but may miss numerous internal sample of malicious code that's been well hidden deep within your machines.

Risk of System Damage

Penetration tests actually run the risk of doing damage to not only your security infrastructure but also your internal systems and databases themselves. This is a small risk but it can't be ignored completely since a inclusive test does need to see how it can best utilize vulnerabilities in your network. The risk of managing damage is something to weigh against important security benefit. Something else that should also be kept in mind and relates to this basic damage risk is the danger of having the people you hire to perform the test being negligent or irresponsible in how they tackle it.

XI. CONCLUSION

Penetration testing is an important component of an organization's overall security strategy and can definitely add value if there are major security weaknesses in its system controls, and a high risk of uncertified access due to the nature and operations of the business. Through controlled attempts to intrude into computer's network system, a collaboration of penetration testing techniques and strategies can be developed to fit an organization's needs in terms of nature of business and size . This will in turn enhance the assurance provided from auditors in assessing a company's internal controls and security system at the same time. Entire, ethical hacking and penetration testing should be considered as an efficient and effective means to mitigate and close security gaps and efficiencies before malicious hackers can otherwise utilize them.

REFRENCES

[1] Hale , Poynter And Sample, Holistic Security,2000
[2] Wilson,Zachary Hacking: The Basics 4 April 2001
[3] Bosworth ,Seymour; Michel E.Kabay, Editor;Computer Security Handbook, 4th Edition
[4] The Cert Guide To System And Network Security Practices, 1st Edition, Addison- Welsey Publishing Co., June 2001
[5] Web Penetration Testing with Kali Linux
[6] www.hacklabs.com
[7] www.sans.org
[8] www.securityxploded.com
[9] www.pentest-tools.com