GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

© SANS Institute 2005, Author retains full rights.

Be Prepared for a Penetration Test

GSEC certification

Practical Assignment

Option 1
Version 1.4c

Jan, 5th 2005

Claire Brec
Sans Security Essentials
Washington
July, 26-30 2004

© SANS Institute 2005 Author retains full rights.

Table of Contents

List of Figures

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Abstract

Following the first penetration test which took place in our organization, we had some issues with the integrity of one of our systems. This brought up some questions:

Were we completely prepared to run this test?
Did we do everything to make sure everything was under control?

Although lots of effort had been made on securing the network/systems, we found some vulnerabilities. One of the attacks potentially corrupted a database which could only be restored from a backup that was several weeks old.
So, I have taken the opportunity of the GIAC paper to work on this subject as an exercise to understand what a penetration test is and better prepare for the next one we will be running.

Document Conventions

When you read this practical assignment, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

`Command`	Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell.
`filename`	Filenames, paths, and directory names are represented in this style.
`computer output`	The results of a command and other computer output are in this style
URL	Web URL's are shown in this style.
Quotation	A citation or quotation from a book or web site is in this style.

© SANS Institute 2005 Author retains full rights.

What is a penetration test?

In 1999, a US government website was defaced; in 2000, many widely-known Internet companies (Yahoo, Amazon, eBay) were taken offline for several hours by Denial of Services (DoS) attacks.

Web-site defacements are more and more often seen in external security incidents. This has reached such a point that an unidentified group announced a "defacement contest" to be held on July 6th 2003. The goal of the contest was to deface as many sites as possible during a 6-hour period.[1] Ninety cases of web defacement have been recorded for the year 2003 in the US: http://www.us-cert.gov/federal/statistics/; 226 cases were recorded for the month of November 2004 in the World : http://www.cert-in.org.in/defacementdetails.htm

Hundreds of web-sites are defaced each month in the world and this has contributed to companies putting information security as strategic to the IT role, with the mission to prevent such incidents.

One of the “tools” used by IT organizations to help keep up-to-date with their security role is the penetration test.

A penetration test is an exercise to “simulate” external intrusions to a network or a system. During a penetration test a security analyst will first gathers information related to the company. This information could later be useful to compromise the target systems. Next the testers analyze this information to figure out what are the vulnerabilities and which tools could exploit them. Finally, they conduct the real attacks and publish a report with the vulnerabilities found and recommendations to secure them. In other words, during this exercise, the tester team is acting as hackers to the company environment with the intent to point out weaknesses and propose recommendations to solve them, not with the intent of doing any harm to the company.

This “test” can be performed with partial information from an organization (partial-knowledge test) or none at all (zero-knowledge test)[2]. Although it could be done by internal people who have IT security expertise, having an external company do the job is more efficient. For most of the time, the IT security experts are also systems administrators and have few possibilities to escape from their admin tasks long enough to perform this exercise on the company-wide scale. Finally, an external company can be more objective.

The option of “announcing” the test amongst the IT community of the company is a debate which has no real easy answer. Advising the IT teams can expose to

[1] SANS Internet Storm Center - http://isc.sans.org//diary.php?date=2003-07-03
[2] SecureNet Solutions - http://www.securenetsol.com/na_pt_test_approach.html

© SANS Institute 2005

Author retains full rights.

some false security feelings (if for example known vulnerable equipments are shutdown before the test. Not telling them could block the penetration testing if administrators think there is something going wrong and start applying some of the incident response procedures that have been put in place in the company
In a company which does not have procedures for on-call support outside normal office hours, an un-announced test could lead to difficulties finding to find someone to help with remote equipment which crashed or did not react well to the testing. If IT people are not aware that they should be at least on-call during the testing period, a result could be that you cannot reset the equipment or restart a service in time.

A penetration test is useful to a company for validating the level of security that has been implemented. There is absolutely no interest at all in planning for a penetration test if no specific security actions/policies are already in place in the company. The amount of weaknesses and vulnerabilities would be so huge, that it would just confirm that nothing was done in terms of security, which obviously IT management would already know. Before even thinking of running through the process of activating a penetration test request within your company, start working on implementing some security policies, and baseline standards.

Reasons for conducting a penetration test can be found at different levels:
- increase upper management awareness about security issues in the organization
- test procedures in place for response to intrusion detection

Companies that are candidates for penetration testing exercises are those with equipment in a Service Area (network zone opened to the world), and even more those which are doing eCommerce.

Like technologies, weaknesses of Information Systems evolve, and performing a penetration test is not a definitive one-shot project, it is a recurring exercise that should be planned on a regular basis.

A penetration test should be composed of 4 phases:
- *Preparation* : probably the most studious part of the project (at least the first time)
- *Test:* when you cross your fingers hoping no catastrophe is going to happen ;-)

© SANS Institute 2005, Author retains full rights.

- *Report Analysis* : when you get all the headaches
- *Action Plan & Follow-up* : actions to correct problems

As this is not a one shot process, the more you document, the easier it is the next time.

Figure 1 : A never ended process

© SANS Institute 2005, Author retains full ri

Preparation

Select who will do the penetration test (internal people / vendors)

As already stated in the abstract, an internal team, skilled in the IT security could do the testing, but indeed, these IT security people are most of the time already in possession of tons of information about the organization and the equipments and could never start from "scratch" as a hacker would. So the only kind of penetration test internal IS staff can ever pretend performing is a "partial-knowledge test", never a "zero-knowledge test". However, internal IS staff could well perform security testing on which they are NOT the sysadmins.

An external company with a number of references on already performed penetration tests could be a good solution. Their expertise in this kind of project would really be helpful to even start working out the scoping of the project, at minimum on the first run.

It is not a good idea to keep the same company to run every penetration tests in an organization. Switching between 2 vendors seems a rather good compromise. For example if the organization has chosen to run two penetration tests a year, it would be better to go with Company A for the first test and Company B for the second.

Define scope and objectives

This area is a really important part of the project and should not be considered as the easiest one. This is the time when you specify the borders of the test, how far you want to go. What you want to see, which areas you want to cover?

Spend a lot of time with the engineers from the selected company to create a coherent and realistic project description. Again, remember that this exercise is not a unique one and, depending on the size and infrastructure of your organization, do not try to cover all domains at once.

Do you want your test to only validate your information security regarding to unauthorized access? Or do you also want to see the organization's ability to detect intrusion attempts and see how the incident response team can handle the issue? This would help figuring out if you want to inform IT community of the test or not.

Not advising the IT community is better for real external hacking conditions, but then doing so, you expose yourself to difficulties and delays in case you have to get hold of people for repairing damaged systems, or for recovery

© SANS Institute 2005 Author retains full rights.

actions. If you want to include incident response procedures validation, then you should not advertise this exercise to the IT teams.
Also you may want to determine what logging tools are going to be used to log the tests. A keystroke capture utility might really be good to use. This should allow you to later dig in the logs of what has been performed and could be really useful, especially if there is a conflict in potential system or data damage.

Define what you want to see in the report

1) An executive summary :

A description of the work done, in comprehensive language for managers who need to understand why and how the money was spent, and what are the outcome for the company.

2) A detailed record of the test itself :

The records there should provide enough information to recreate the penetration test steps. It might be necessary to review these records in case of disagreement on how some damages could have occurred on systems. This also could be very useful in case of data corruption on databases.
Together with the logs of the company equipment this should be complete enough to understand and explain why such databases might have been corrupted, or why that equipment might have reacted unexpectedly.

3) A detailed report that includes :

- Definition and scope of the penetration test
- Goals of the penetration test
- Methodology used
- Work plan (chronology/timeline of the test)
- General recommendations
- Detailed list of vulnerabilities and recommendations to solve them
- Conclusions

Ensure legal written approvals are ready

© SANS Institute 2005 Author retains full rights.

Doing a penetration test to an organization is close to play with legal laws and therefore, specific caution must be taken in granting the people who are involved in this project. Ensure the CIO provides a written authorization to do so, as a "keep out of jail" card. As you can see in appendix A, the penalties could be very high depending on the countries; it can range from simple fine to years of imprisonment.
The Internet has no geographical boundaries; it is not easy to determine which jurisdiction is to be taken into account. Examples of international laws are listed in Appendix A.

Build Timetable for the test

Keep in mind that a penetration test, even if the chosen option is not to go up to the real "breaking" of system or changing of data, can always go a little bit further than expected. Therefore it is highly recommended to run this over a low business activity timeframe for the organization.

Most of the time, weekends are good time for these exercises. The counter point of this choice of course is that you could have several systems powered off over the week-end at some sites, but you could always ask for these ones to be left powered on this specific week-end if necessary.

Allow some time after the penetration test for other groups to verify the integrity of their data, especially on the production applications side. For example, you could consider having some system administrators of the e-business team run database queries on critical tables to ensure that contents of databases are still accurate. If there is a doubt, then you could start the process of restoring the database from last backup.

Plan the post-penetration testing internal actions such as changing passwords which might have been discovered during the test.

Question is open as should you advise your customers on the Internet of potential closing of the website during the weekend. This indeed would depend on the service level agreement the company has in place.

Ensure IT people are ready to restore systems or recover data

One pre-requisite you might consider when organizing a penetration test is performing a verification of the integrity of the backups for all the critical environments (systems or databases).

Organize some minimum on-call support and make sure relevant IT specialists will be contactable during that test, in case there are some actions needing for example to restore a service on a network equipment, restart /rebuild a server, or restore a database .

© SANS Institute 2005 Author retains full rights.

Keep the backups, which ran the day before the test, inside the walls instead of sending them to the usual offsite secure storage area. If there is a need to restore, you save the time of having the backup media being brought back to the site.

© SANS Institute 2005, Author retains full rights.

Actual Test

Step 1. Gather information

The objective there is to get the maximum information on the target network. This step can be cut in 2 phases, the indirect and the direct investigations.

Indirect investigations:

Try to learn as much as possible on the company without directly trying to contact it. This can be done with investigations on the Internet tools, and does not really need that much of technical skills.

- whois databases : (ie http://www.internic.net/whois.html).
  This can give many information, such as which company is hosting the site, give some mail addresses, postal address, name of administrator … The information available through this mean are legally obtained.

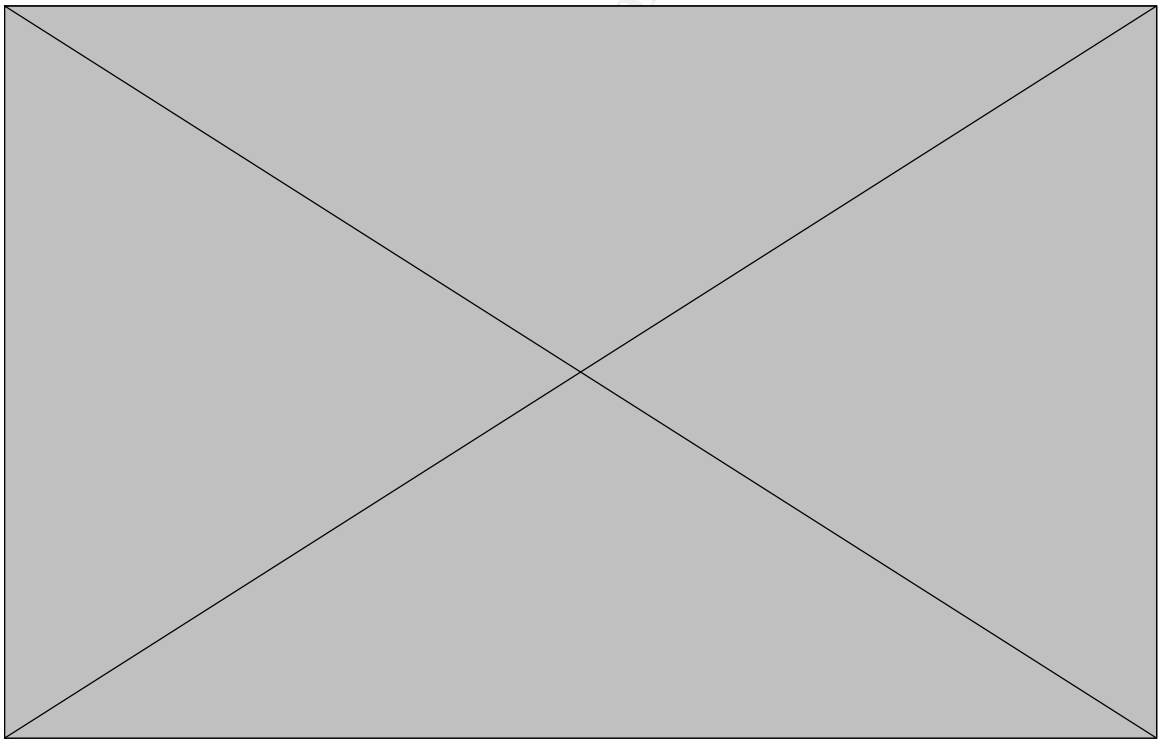

Figure 2 : Whois

- newsgroups (ie http://groups.google.com) and web search tools.

© SANS Institute 2005

Author retains full rights.

Searching these areas on domain names is a source of technical information on systems and software used in the organization, and may be on personal information that can be used for social engineering. Mail accounts retrieved from the whois previous searches can be looked for in theses newsgroups.

Direct investigations:

Try to scan directly the targeted organization and retrieve whatever useful using any kind of tools. This will help trying to figure out the topology of the network of the company.

- Remote social engineering, with phone, fax, mail to get confidential information such as passwords, phone numbers, IP addresses …
- DNS queries :
  - To retrieve the DNS ns for the domain : host -v -t ns *domain*

Figure 3 : Authoritative DNS

  - To retrieve mail servers of the domain : host -v -t mx *domain*

Figure 4 : Mail servers

- Ping queries to search for machines which are up. Although more and more companies are now filtering pings and sometimes a timeout response does not mean the machine is not up.
- Traceroute queries to find a router to access the organization
- Scan ports on IP addresses gathered; with fingerprinting determine active computers and OS they are running. Nmap is the most well known free tool capable of doing these scans.

The last two investigations require a much higher level of technical understanding of TCP/IP and the scan itself can, in some cases, not only slow down the networks with all its broadcasting, but also crash active systems.

Step 2. Analyze information

With all the information retrieved in the previous step, identify which vulnerabilities can be exploited, and what tools are available to do so.
This step is also often called the vulnerability scanning.

All machines that have been discovered in the previous steps are examined and searched for open ports, operating system and applications running on them.
Together with accurate information available on the Internet vulnerability databases, relevant exploits are listed.

This phase requires a very good expertise on the existing vulnerabilities

© SANS Institute 2005 Author retains full rights.

databases of equipments and systems, and an up-to-date knowledge of the tools available to exploit them.

Output of this step phase would be a document listing all the target hosts with their IP address, Operating System, known running application, banner information, known vulnerabilities.

- Nmap : can return information on open port and potentially on the OS running on the machine : nmap -O *hostname or ipaddress*

```
Starting nmap 3.75 ( http://www.insecure.org/nmap ) at 2004-12-28 15:53 Romance
Standard Time
Interesting ports on xxxxxxxxxx.xxxxx.com (xxx.xxx.xx.xx):
(The 1651 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
5631/tcp open  pcanywheredata
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Pro or Advanced
Server, or Windows XP
Nmap run completed -- 1 IP address (1 host up) scanned in 1.172 seconds
```

```
S
In
(
P
2
389/tcp open ldap
1352/tcp open lotusnotes
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20
Uptime 71.918 days (since Sun Oct 17 19:05:01 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 2.274 seconds
```

Als… Ap… more info on the version of application which is running.
Depending on the OS found for a machine, there are some more specific tools which can also provide more information for vulnerabilities searches.
For example a tool like netcat can retrieve the home page of a website:

nc -v *hostname* 80

```
xxx.xxx.xxx.com [xxx.xx.xx.xx] 80 (http) open
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 28 Dec 2004 16:25:20 GMT
Server: Apache/1.3.24 (Win32) mod_ssl/2.8.8 OpenSSL/0.9.6c
Last-Modified: Mon, 20 Oct 2003 15:09:02 GMT
ETag: "0-16d-3f93fa8e"
Accept-Ranges: bytes
Content-Length: 365
Connection: close
Content-Type: text/html

<HTML>
 <HEAD>
  <TITLE>You are here</TITLE>
 </HEAD>
 <BODY BGCOLOR="#FFFFFF">
<a href="https://xxxxx.xxxxx.xxxxx.com:443/cgi/xxx/DEV/xxxx/xxx;start=xxx.xxxxLogin.run">click me</a>
<br>
Click the above link to go to the secured site.
<br>
This is only for testing purposes.
<br>
 </BODY>
</HTML>
```

Figure 7 : Netcat output - website homepage

© SANS Institute 2005, Author retains full rights.

Step 3. Perform attacks

There are several kinds of attacks that can be generated from the vulnerabilities of an organization. Penetration testers will rely on them to perform deliberate attacks on the company. To do that, there are lots of tools available and the book "Hack I.T. Security Through Penetration Testing" [3] provides some very detailed explanation on how to use scanners, discovery tools, OS-related tools, web-related tools. But in any case, the tools that are to be used during a penetration test have to be the latest one, and the most up-to-date. Without going too much in detail, here are some examples of what can be used today:

1. *Network attacks :*
    a. **IP Spoofing** : fake another's IP address
    b. **TCP Session Hijacking**: insert your machine in an existing connection between 2 other machines.
    c. **ARP Redirect** or ARP Spoofing : redirect network traffic from a machine to another (need physical access to organization network)
    d. **DNS Spoofing**: confuse the DNS server by returning wrong information to DNS queries.
    e. **Sniffing:** view network traffic, looking for clear text showing unencrypted names and passwords.
    f. **War Dialing:** use brute force dialing programs to scan the range of company phone numbers to identify potential active modems. Then try to access them and connect to systems through them.
2. *Attacks on applications :*
    a. **Configuration weaknesses:** most common error there is to keep the default install parameters active (example: default account name and password). Second one is bad parameters of access authorizations.
    b. **Bugs** : bad programming of applications can generate most important vulnerabilities
    c. **Buffer overflow**: again due to bad coding, when a variable, send as an argument to a specific function is copied to a buffer before first validating its size.
    d. **Scripts** : there are some ways to exploit Perl or PHP scripts
    e. **CGI** (Common Gateway Interface): Most of the time, CGI programs are left running with the same privileges as the web server

[3] " Hack I.T. Security Through Penetration Testing" by Klevinsky, Laliberte , Gupta , published by Pearson Education Inc. Aug 2004.

© SANS Institute 2005 Author retains full rights.

software does. This opens an exploit to deface websites.

f. **Default Services :**
   i. **Imap and Pop:** these are mail protocols used to access e-mail remotely, therefore opened to the internet.
   ii. **Sendmail, FTP, IIS, SNMP:** all these services are installed by default on servers (depending on the os) and do have lots of vulnerabilities associated to them.

g. **Password cracking:** there are some password cracking programs that can find a password from a dictionary in seconds or minutes. Weak passwords are probably the biggest internal weakness of a company. People have so many passwords to remember that they stick them under their keyboard, on their screen, never change them when possible.

3. *Denial of Service :*

Whether this test is part of the penetration test is something which has been determined in the preparation.

When the two first kinds of attacks are more “reading attacks”, the denial of service attack will result in the unavailability of a service, an application, or a machine. To perform this kind of attack, there is a need for several powerful machines to run simultaneously the attack on a target.

Denial of Service attack can be described as an attempt from hackers to keep an application or a service too busy for the company users to be able to have access to it : “flooding” a network to prevent legitimate traffic or break connection between two machines to close access to a service can be examples of Denial of Service attacks.

Tools which can lead to Denial of Service attacks:

a. **Fragment attacks**: split large packets in segments to send to a target which then tries to re-consolidate the fragments which in fact is too big for the application.

b. **Flooding:** port or SYN flooding to keep CPU 100% busy managing all the connection attempts.

c. **Destruction or Alteration of Configuration Information**: for example, if an intruder can change the routing information in your routers, your network may be disabled. If an intruder is able to modify the registry on a Windows NT machine, certain functions may be unavailable.

© SANS Institute 2005, Author retains full rights.

c. **Physical Destruction or Alteration of Network Components**. This can be done simply with physical access to unauthorized computers, routers, network cabinets, power station.

© SANS Institute 2005, Author retains full rights.

Step 4. Publish report

This is the document that the company is most waiting for, and its content must have been discussed during the project preparation time.

The report should contain the list of all the vulnerabilities found, and for each of them, the risks for the company and the recommendations to cure. This part of the report will help the company to assign priorities and develop countermeasures. These recommendations should cover both short-term corrections and long-term proposal, and should also show policies, design or organization necessary reviews.

It will also contain the description of the methodology used during the test and the action taken.

As an appendix to the documentation, the company could get the logs and outputs of the vendor related to all the actions performed on the company network and equipment. This is where software like key-loggers can be really important to be part of the tool-kit (tools like ***KGB Key logger - http://www.refog.com/*** or Advanced Key Logger - http://www.mykeylogger.com/keylogger/keylogger-features.php).

© SANS Institute 2005, Author retains full rights.

Post Penetration Test

From the vendor report, build a summary presentation to the management:

- Prepare clear explanation on the issues and the risks and how these issues are going to be handled in the organization, in terms of procedures and resources, and how this will be improved as a regular process.

- Propose time frame for correction of these issues, fixing the revealed vulnerabilities following the recommendations provided by the pen-testers.

Also ensure that more long-term actions are conducted on how the company will keep current as every day, new exploits and new tools are being brought to the wild. This can be done with real security architecture global to the company (would include: policies, baseline standards and awareness trainings).

Build another more technical-oriented presentation for IS technicians to bring awareness of dangers and also involve them in the improvement of the security processes.

Make sure the policies and Baseline standards are updated to reflect the result of the test, and also ensure the security awareness training materials is updated too.

© SANS Institute 2005 Author retains full rights.

Conclusion

Single security snapshots are useful for single-use purposes, however systems, networks and staff change on a regular basis and new exploits are constantly discovered. It is strongly recommended that Penetration Testing exercises are repeated at regular intervals. It only takes one undiscovered hole for hackers to compromise the data.