PENETRATION TESTING METHODOLOGY

for fun and profit

[Draft v1.2]
Efrain « ET » Torres – et@cyberspace.org LoWNOISE 2001-02-19

INTRODUCTION

Penetration testing is a growing field, but is easy to see a great many misconceptions in the way most people describe and implement it. Firstly some believe "penetration testing" doesn't follow an exact methodology, claiming it depends directly on the tester's experience, so, by this logic, exclusively "depends" on the difficulty of the defined target. However without a defined methodology it is easy to make mistakes, loose time, money and the client's confidence in receiving an excellent product.

Almost as bad as no methodology is using a methodology that is far too general, the most common case in point being the 3 step methodology: information gathering, penetration, documentation. The worst aspect of this methodology is it's pervasiveness. Far too many company's have the idea that a penetration test constitutes nothing more than running a security scanner and getting a nice report at the end. The main fault with this method is its results depend only on how many problems where discovered. Thats a massive oversight if you are familiar with the way security scanners work and know about the false-positives and false-negatives they produce.

I have seen far too many sloppy and expensive penetration tests done by big companies; that base the results on automated tools without a deeper analysis. Or penetration tests done without even considering the use of "Trashing" or Social Engineering skills on the target to gather additional information.

"There is much more to penetration testing than running a few tools and producing a report. For as many vulnerabilities that are checked by those testing tools, there are as many additional techniques that are available to an ethical hacker for finding vulnerabilities. While ethical hackers are usually bound by time, legal permission and experience, they have an obligation to provide as realistic of an assessment as possible. "
(Broadening the Scope of Penetration Testing Techniques by Ron Gula rgula@securitywizards.com)

This document is a proposal, is just a draft. I hope to continually add on to this document, so I encourage you to add your contributions in order to make it a more complete overview on effective penetration testing. I am certain it will HELP to prevent bad penetration tests, sometime which is all to common nowadays.

There is no Copyright, no disclaimer, if you use it just give me some credit. Excuse my English and the title of this document, I know it sucks. *Gracias* to Daniel « Mr_FrEaK| » Padilla for his comments. ☺

Test Types

There are two penetration tests types.

External Penetration Test

An external penetration test emulate an attack by a external entity attempting to breach internal networks from the outside.

Internal Penetration Test

An internal penetration test emulate an internal attack by a malicious user / employee assessing the amount of damage that could be caused to the organization. The initial internal point should be defined by the client.

Each one can be subdivided into additional categories like external penetration test with and/or without initial information about the target. That depends solely on the client's expectations and the target's characteristics.

Initial Information

The first and most important part in any penetration test, external or internal, is information gathering. But before this step, a target must first be defined. It's crucial to clearly define a target; it can be a host, a network, data , etc.

Some clients prefer not to give any kind of initial information about the target's characteristics or the environment around it, forcing you to acquire it. The environment can be the network's topology, firewalls, proxies or phone numbers to access RAS. After you have selected a target define what kind of info you need to begin the tests. This is not about quantity but about quality. Like I said earlier that depend entirely on the client's expectations and the target's characteristics.

Penetration Test Team / Tiger Team

The group which is going to perform the penetration is called Penetration Test Team or "Tiger Team". The number of members depends on the size of the network, the target, the environment's difficulty and the target's

characteristics. Sometimes the tiger team will consist only on 1 person, but again that “depends.”.

When a organization looks for a penetration test and pays for it, the organization is TRUSTING the Tiger Team. It is trusting the Tiger Team will not disclose any confidential information it may have garnered while conducting the test. Occasionally, the client should require the members of Tiger Team to sign a confidentiality agreement.

Some Tiger Team members may not be trustworthy or may lack the necessary expertise. So it is always a good idea to list Team members and establish rules of engagement.

Rules of engagement:

(Taken from “Rules of engagement: Testing the security of your enterprise“ By Winn Schwartau)

Now, criminals will do a lot of things that even we, as 'friendly hackers' will not, and can not legally do. The so-called 'Out of Bounds Behavior' must be defined and adhered to. Nonetheless, all possible methods must be considered ahead of time. I like to put these issues on the table even if only to have them consciously removed. Assuming that the customer understands all possibilities is a freshman mistake. The bad guys will not preclude using them just because they are illegal and it is prudent to understand how far real criminals might be willing to go.

Attack Methodology	***Permitted?***
Electronic Mapping – External	*Yes*
Electronic Mapping – Internal	*Yes*
Social Engineering By Telephone	*Yes*
Social Engineering By Mail	*No*
Adopt Employee Identity – Remote	*Yes*
Adopt Employee Identity - On Site	*No*
Break into Employee Workstations?	*Yes*
Read Corporate E-mail	*No*
Pretend to Be Technical Supplier	*Yes*
Dumpster Diving - On Site Outside	*No*
Dumpster Diving - On Site inside	*Yes*
Dumpster Diving - Off Site	*Yes*
Target Sensitive Corporate Resources	*No*
Personnel Extortion, Blackmail and Coercion	*No*
Investigate Personnel Backgrounds of Staff	*No*
Penetration of Business Partners	*No*

Some of these actions may seem really crazy at first, but think how far the 'bad guys' could go if they chose to. How can we impose our personal bias

limits on attack methodologies knowing full well that they do not reflect the real world?

The above list is just an example. Another item that should be added to the list is "Denial of Service / Distributed Denial of Service permitted?"

Tools

Make a list of GENERIC tools that will be used in the penetration test. There is always the possibility of using many other nonlisted tools, that depend directly on the test's findings. These tools may include mundane programs such as PING, NSLOOKUP and even web browsers, but don't list them, is very unprofessional to receive a list containing "*traceroute*". Here is an example of that list:

- Portscanners
- Wardialers
- ARP Redirectors
- Sniffers
- Password Crackers
- Cgi Scanners
- Anti-IDS Tools
- Commercial Security Scanners
- Non-commercial Security Scanners
- Tools developed by the tiger team
- Zero-day exploits

Just describe the tools used (Name, version), when you annex the results to the documentation. (Ex. ISS Security Scanner Version x.x).

NOTE: A an effective Tiger Team knows that sometimes non-commercial tools are better than commercial ones. Be extremely careful when planning penetration tests based on just one security scanner (a very big mistake, they lie), older security scanners like SATAN, or older program versions in general.

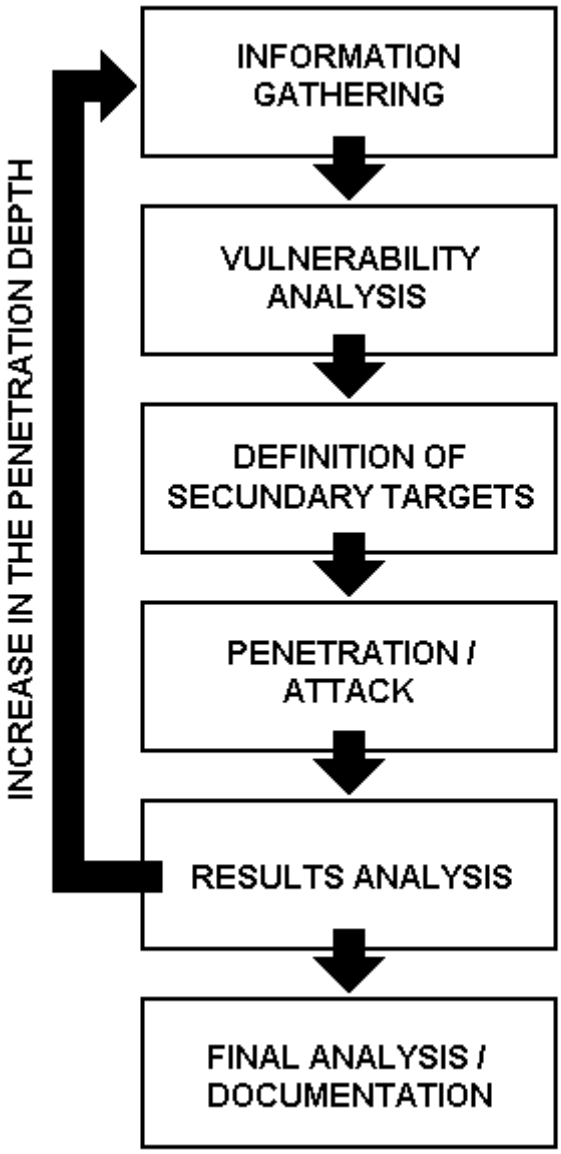
Test Platform

Describe the equipment, Operating System(s) , and the requirements that the client should provide. The platform should be dynamic; depending on the data obtained during the tests the platform should be adapted to fulfill the objectives, and conquer the target. Example: Be prepared to flip between Oss like WinNT / Linux.

For INTERNAL tests, the test platform should be a joint decision between Tiger Team and the client. The reason being is an INTERNAL test should reproduce a internal user/ employee's typical equipment while keeping in mind that a internal user/employee can easily change his platform, install programs, use a laptop, etc.

Methodology

The following 6 steps outline a complete process, some portions of the process can be grouped and/or be adapted according to the necessities.



NOTE: An INCREASE IN THE PENETRATION DEPTH is considered during the tests like an approach towards the final target. An example of this approach

can be understood as obtaining new information that opens new options to obtain access to the target and/or access to intermediate hosts that could serve as a bridge to reach the final target.

Step 1: Information Gathering / " Discovery "

Gathering information to identify Servers, routers, firewalls, telephone numbers, EVERYTHING. This information will help build a picture, or 'footprint' of what the target network's electronic perimeter looks like. If the test is done with initial information then the information gathering step is BASED (not REPLACE) on that information.

Step 2: Vulnerability Analysis

Determine security problems in the different elements found during the information Gathering process.

Step 3: Definition of secondary targets to attack

Based on the information generated by the vulnerability analysis, determine the specific objectives that offer a greater possibility of obtaining the final goal and/or an approach towards the final target. If everything is going ok the secondary target is the final target.

Step 4: Penetration / Attack

Attack the targets selected in the previous step using the discovered vulnerabilities.

Step 5: Results Analysis

Analysis of the attack results. When the result is a INCREASE IN THE PENETRATION DEPTH to reach the goal , repeat the cycle returning to Step 1. If the goal has been reached or the time to finish the tests is over follow to step 6.

Step 6: Final analysis and Documentation

Generation of a consolidated report that details the results obtained during the tests, with the corresponding analysis of this information to be correctly interpreted by the client and to understand the security implications on the analyzed infrastructure.

References

- "An approach to systematic network auditing" Security papers by Mixter mixter@newyorkoffice.com http://members.tripod.com/mixtersecurity/
- "ANATOMY OF A FRIENDLY HACK Testing The Security of Your Enterprise" by Winn Schwartau
- JSC AIS Security Home Page http://www.jsc.nasa.gov/security/JAS_homepage.html
- "Broadening the Scope of Penetration Testing Techniques" by Ron Gula rgula@securitywizards.com
- "Audits from hell – find out how to avoid those audit nightmares" by Carole Fennelly carole.fennelly@sunworld.com http://www.sunworld.com/swol-02-1999/swol-02-security.html