



Roentgenstrasse 49 **Street**
 CH-8005 Zuerich **Zip Code**
 Switzerland **Country**

+41(0)44 272 1876 **Voice**
 +41(0)76 200 7778 **Cell**

www.CyTRAP.eu **URL**
info@CyTRAP.eu **E-Mail**

Just the facts

Title	CyTRAP Labs– sense and nonsense regarding intrusion detection testing
Short description	<p>Penetration testing (also known as 'ethical hacking') evaluates the security of an organization's information system by simulating an attack. But how valuable are such tests? This paper outlines some of the shortcomings of classical penetration testing.</p> <p>In this brief we present the ComAnalytica Process Method that allows one to get a better picture about user behavior and communication patterns than 'classical' penetration tests. The method enables one to discover unauthorized processes and software, such as Kazaa or Skype, running on the network. In turn, security measures can be put in place to stop such activities.</p> <p>Most importantly, the ComAnalytica Process Method is an important part of the firm's internal control system. It provides vital information needed for achieving better governance regarding the organization's information assets and assuring legal compliance.</p>
CyTRAP ID Verify brief for updates	PenTesting-MakingSense-2007-05-23 Checking for the latest version of this document now

CyTRAP Labs

Table of content

1	Just the facts
2	Table of content
3	Sense and nonsense when it comes to penetration tests
3	Why penetration tests will never be able to show all possible weak spots
5	Logical penetration tests
5	ComProcess Analytica Method
6	ComProcess Analytica Method and risk management
7	Administrative

Sense and nonsense when it comes to penetration tests


As risk management experts it is our job to assess information security, privacy as well as data protection efforts a firm may have put into place. Moreover, following regulatory standards and assuring legal compliance is needed and suggestions regarding improvements are also provided.

Interesting is that nearly all firms hire outside experts to conduct comprehensive intrusion detection testing. The results obtained in those tests are usually submitted to management in form of a written report. Unfortunately, more than once it happened that such results were of limited help when it comes to improving the security of a network, also in terms of confidentiality, integrity and availability of data and information. Moreover, costs of such tests are often substantial.

These and other pertinent issues are discussed here and effective methods needed to achieve a greater bang for the buck are outlined. In particular, the tests' importance regarding internal control systems and risk management is also addressed.

Why penetration tests will never be able to show all possible weak spots

Enterprises may believe that penetration testing is the best, if not only, way to reveal weak defences or to detect risk exposure regarding possible threats against their systems and information assets. But in practice, things are more difficult:

- Regardless how long a penetration test might take and how many IP-addresses it may contain, penetration tests represent a cross-sectional sample, i.e. it is one picture of how things look today or at this moment. Unfortunately, this makes it impossible to test all IP-addresses, since it is highly unlikely that all equipment (e.g., printers, cameras, notebooks) are connected to the network in any one point of time. Unfortunately, all it takes is just one and really JUST ONE piece of equipment infected by malware (such as zombies, Trojans, worms or viruses) to make sure that the enterprise's security posture is far worse than one would believe.
- Malware cannot be discovered using penetration tests, because these programs are not behind a port that might be covered during a penetration test. Zombies work in the active/active mode. This means that they might receive instructions from a master, such as Port 80 and then execute these instructions. The latter could be to send out spam mail via Port 25. Worse is the situation whereby spyware may collect information in a passive mode which will then be transferred to the master using Port 80 or any other port open to the internet.
- Penetration tests are a technical tool to assess a situation. Therefore, employee behavior is not part of such an analysis. Unfortunately, end-users can circumvent with the simplest tool carefully drafted policy and security measures that were implemented to protect the organization's information assets.  mation.

CyTRAP Labs

- The logic of a real attack is not getting tested using a penetration test.

Which path would a potential attacker really take to penetrate the system?

Beginning with where he or she penetrates physical defences as an outsider or insider, all the way to successfully gaining unauthorized access to confidential information. Such a type of penetration test could be described as a logical penetration test.

At this stage it is most important to understand that a logical-type of penetration test is very likely successful in revealing the weak spots.

Looking at the above, one must ask why penetration tests may take weeks if not months, before they are completed. Because they represent a sample only, it should be possible to analyze and summarise collected information relatively quickly.

Worse is that such tests fail to provide a comprehensive picture of the situation and sometimes, they may lull management into a false sense of security, by providing an incomplete picture of the current situation.

Field work reveals that penetration tests can be conducted in relatively short blocs of time. To make findings useful and provide one with a comprehensive picture it is, however, necessary that a vulnerability scan as well as a logical penetration test are both part of the work. Behavioural patterns and trends exhibited by end-users (e.g., which software is used and how) and software (e.g., which ports for what) must be investigated as well.

Depending on the size of the firm, sometimes all it takes is about three days on premises in addition to time required for doing the analysis and write-up of the findings. In turn, very specific information regarding different security measures used by the enterprise can be provided. Such information can then be handed over to enterprise in a:

- Security Recommendation Overview Document.

What happens during the penetration test goes beyond the scope of this brief. Nonetheless, the following sections will delve a bit deeper into the matter of logical penetration tests. As well, how communication patterns can be systematically analyzed to reveal valuable information regarding risks and threats will be discussed.

CyTRAP Labs

Logical penetration tests

During a logical penetration test the expert, conducting the test, takes on the position of either:

- an internal attacker – is given the same user rights and software as an employee, and/or the
- external attacker – brings specialized software and / or hardware hackers use to penetrate the system.

Such logical penetration tests do result in data that can be highly revealing for the organization. Sometimes, a clever end-user can use a few simple means and achieve much that a complex attack scenario would not necessarily consider possible. For instance, experience indicates that cases of industrial espionage or fraud may occur simply, by users modifying data or taking data off premises without proper authorization.

ComProcess Analytica Method

On a more technical level as the logical penetration test, we provide the ComProcess Analytica Method (Protocol-Tracking-Analysis) test. This method collects information in the network on what is actually communicating. This allows the discovery of unauthorized software or improper use of authorized software and its removal/reconfiguration in the system and/or network.

This type of analysis shows management where the weak spots are and, therefore, enables the effective improvement of internal controls and risk management regarding these types of threats.

To illustrate, it is feasible that through a ComProcess Analytica analysis one discovers that numerous protocols or applications running in the network are neither authorized nor planned to be used on the system. This can mean that the actual number of unauthorized and unplanned applications running, is far higher than the number of applications that are authorized and do run on the network. Naturally, this indicates that a more effective internal control and authentication mechanism must be used to manage this risk better. Only then, the firm will be able to achieve legal compliance and, as importantly, manage such risks at levels that management deems acceptable.

With the help of the ComProcess Analytica Method the use of Kazaa-type services, as well as the use of Skype, unauthorized servers and zombies running on the network can be identified and shut down if needed. In some cases, the use of such programs may be a possible violation of the copyright legislation that could result in costly litigation for the enterprise. In other cases, such activities reveal industrial espionage and worse, research and development efforts, patents or other property rights and assets of the firm may be damaged by the activity. In some cases, the content may be illegal such as a corporate network being misused for distributing child pornography.



The ComProcess Analytica Method can be used and implemented easily from a technical perspective. All that is needed is to collect the stream of data flowing between, for instance, an Internet firewall and the internal network. Once these data have been collected, an expert can then begin to make sense out of them and extract the information that is needed to catch non-authorized applications. As well, experience regarding cybercrime does help in making sense out of these vast amounts of data. Putting oneself in the position of the attacker facilitates the analysis and evaluation of the information collected (e.g., what does this flow of data mean and what does the attacker want to accomplish with this activity?).

ComProcess Analytica Method and risk management

The method described above, particularly the ComProcess Analytic Method enables the firm to discover the weak spots in its networks. Non-authorized processes running on a network are a cost problem for sure (e.g., paying for bandwidth) but, more importantly, confidentiality, integrity and availability of data may be threatened. To illustrate, most countries require that instant message activities must be saved and archived. In cases where these have neither been authorized nor a centralized chat server was installed, these types of data streams cannot be saved. In turn, the firm is non-compliant. Discovering this weakness today is surely far less expensive than having to report this failure during an e-discovery process in a lawsuit.

The ComProcess Analytica Method shows the flow of data regarding non-authorized processes and communication activities. In turn, this enables the firm to stop such such type of activity and thereby reduce risk exposure significantly

It takes a step-by-step process that provides management with data needed identifying the weak spots as well as unauthorized activities. Thereafter, the necessary steps can be taken to stop such activities and minimize their future occurrence to acceptable levels of risk for management. As well, how these changes have succeeded in minimizing such unauthorized activities, discovery of botnets or zombies in the future requires auditing of such security defences using the ComProcess Analytica Method on a regular basis or at least as part of the annual audit. Only than, the board of directors can be certain that its internal control system as well as risk management regarding information assets meets regulatory requirements and demonstrates that weaknesses or unauthorized activities where eliminated.

CyTRAP Labs

Administrative

Author Urs E. Gattiker, Ph.D. & Andreas Wagner

Revisions 2007-05-18

Access Level 1

Contact Details Web: <http://info.CyTRAP.eu>

E-mail: [Intell at CyTRAP.eu](mailto:Intell@CyTRAP.eu)

Tel:+41(0)76-200-7778 or + 44(0)70-9237-6036

Fax:+44(0)70-9237-6036, dial 3 send fax

Copyright The preceding was not a legal opinion, and is not our organization's. Original portions Copyright 2007 CyTRAP Labs – Urs E. Gattiker and Andreas Wagner, all rights reserved.

Our work may be copied in whole or part, with **proper attribution**, as long as the copying is not for commercial gain.

Technorati tags

Apple	security
CASEScontact.org	outsourcing
best practices	offshore programming
case studies	India
cost-benefit analysis	due diligence
disaster recovery plans	checklist
information security	Sarbanes-Oxley
regulatory compliance	Sarbanes-Oxley
risk management	

Did you like this brief?

If yes, why not [bookmark it at Del.icio.us](#)