Global Information Assurance Certification Paper

TESTS OF PENETRATION IN A DATA NETWORK

1. INTRODUCTION

The digital world does not differ almost in anything from the real world, is defined as the reflection on which it is lived nowadays, it is as well as it is due to begin to visualize the concept of comp uter science security and of the areas associated to this, as far as the audit it is counted on the penetration tests, like a feedback process, that contributes in a high degree to the securing, management and maintenance of information system.

In the real world there is a great variety of human beings, with activities, interest, different tastes, customs and cultures, constituting the human biodiversity, which as all system tends to maintain a balance to coexist and to guarantee its survival in the future.

From the beginning of humanity a balance between good and evil has existed, estigmatizes in each one of the cultures and therefore with multiple conceptions, for example laws have been denominated to tipify and classify different behaviors that have evolved with the passage of time, which causes that day to day they exist new forms to act and therefore new forms to regulate. That the this challenge to be faced when confronting and interacting with the digital world, knowing beforehand that there has to be control for a diversity of users to guarantee a balance that allows the operation, through schemes that prevent , detect and react to behaviors that in some cases have not been contemplated in the present legislations.

Security Computer Science is then an assembly of rules, call security policies , which are implanted and supported by schemes that involves hardware, software and people, who additionally count on processes like the audit for their evaluation and update, which can and must be alter nated with tests of penetration for its benefits . The content of the present document wants to create a methodology oriented to penetration tests, that covers a high percentage with the most common weaknesses of a technological platform

2. DESCRIPTION

The penetration tests enter to form part of the securing processes, maintenance and evaluation of information system, their mission consists of proving the implanted policies of security in a technological platform, using a assembly of techniques that result in an analysis that demonstrates all the weaknesses that put in risk the confidentiality, integrity and availability of the information, giving a start point to proceed to the accomplishment of adjustments in the security policies and generating a feedback with other processes, the real knowledge of the present situation and determining the optimization and/or application of new technologies and processes that increase the reliability degree.

3. OBJECTIVE

The general objective of a penetration test is by m eans of its execution, to detect the weaknesses and to contribute with recommendations to the process of security of a

technological platform, and it also looks to enrich the processes of continuous improvement of the audit, management and maintenance of an information system.

4. JUSTIFICATION

The technology has facilitated and well -known improved the form to work of the companies, has offered speed in its operation through the use of information system, generating continuously a better reflected perfor mance in the satisfaction of the final client; unfortunately this goes along with a series of serious disadvantages when the technology does not operate correctly, Pretended losses of yield in the servers, continuous disconnection of the workstations, freq uent falls of the communication channels are just some examples that live the companies at the present time, where probably the most serious problem is the ignorance of the causes of these problems for lack of knowledge, tools or specialized services and e ven worse when the organization faces the use of Internet like means of commercialization of her goods and like a basic tool for his operation

To face this almost obligatory alternative is a challenge that is due to confront seriously, since the informat ion system are remarkably at risk and therefore they must be protected through a culture of continuous improvement, generating a policy of security totally opened to changes, but of obligatory character in its fulfillment. Finally the application of the mo st advisable technologies for the atmosphere of work of the company is determined and which reflect 100% the decisions taken in the established policy. The penetration tests must be made once are defined the operation and security policies , also the techn ological infrastructure has to be assured 100% and the results must give feedback the audit process, with which it is due to put in to generate the cycle of continuous improvement

5. RESOURCES

5.1 Human

You must count on a human group whose knowledge cover th e following areas: Operating systems, networking, applications and telephony, in addition it is important to have contact and/or access to the world underground (recognized groups of hackers).

5.2 Logical and physicist

- Computer or computers with different operating systems like: Windows 2000, Linux, Solarix, Beos, Os2.. Connectivity to the private or public network, through an analog or digital Modem, network adapter, Wireless, etc..

Tools as applications, devices and specialized, considered techniques in some cases like tools of hacking

- **Port Scanners:** Tools that detect the existence of equipment in a network, and the services that offer.

Commercial: Ws Ping Pro Pack
Free: Nmap, Hping, Jackal, Cheese

- **Analyzers of vulnerabilities**: Tools that make automat ed verifications of vulnerabilities.
  Commercial: Cybercop Scanner, Iss, Retina Gratuitous: Nessus, Saint, Sara

- **Sniffers or Traffic analyzers :** Tools that capture all the visible traffic in a network segment, being able to capture usuary and passwords of protocols that do not use coding schemes.
  Commercial: Nai Sniffer, I dominate, Advisor
  Free: Analyzer, Ethereal, Tcpdump

- **Password crackers**: Common tools that try to obtain the access passwords to a system by means of dictionaries, lists of passwords and brute force.
  Commercial: Lopht Crack.
  Free: John the Ripper, Crack

- **Trojan Horses**: Software catalogued like virus, whose objective is to have the control of computers and/or servers.
  Examples: Netbus, SubSeven, Back Orifice

- **Networks Management**: Software to detect configurations and originating information of agents SNMP and readings of MIBs.
  Commercial: Unicenter TNG, Tivoli, HP OpenView, What`s UP, Insigh Manager, Top Tools, Dell Open Manager, Trascend, Cisco Works, Net View, Nways Campus to manager, SM S

- **Social Engineering**: It includes/understands a assembly of tactics catalogued like the most powerful weapon for the access to IS, cradles in the common sense and the human error.

- **Interpersonalización (Supplanting):** Technical more transparency, effecti ve and destructive of hacking, to look for to supplant an authorized user to obtain access to any type of information, made through the use of troyanos, the crakeo of access keys and social engineering

6. METHODOLOGY

6.1 International policies and standards

Like introduction to the raised methodology, The existing policies and international standards are mentioned and where the penetration tests become vital, although they are only a single task within these, is very important to know the context in that they are developed, Up next will be a brief review of the standards which they have arisen through the time, as well as the ones used at the time

Trusted Computer System Evaluation Criteria (Tcsec. Orange Book)

Developed by the government of the United St ates in 1980 to provide a standard in the manufacture with governmental systems and as an evaluation criteria to determine the confidence degree that fulfills an information system, also known like Orange Book

Trusted Interpretation Network (TNI) Given the necessity to interchange information and with the evolution of computers networks, is born the necessity of an evaluation criteria, which in 1987 is developed by the government of the United States and based on the interpretation of the TCSEC for comput ers and network communications systems

International Technology Security Evaluation Criteria (ITSEC)
Developed by European countries, is born of the combination of the criteria of the orange book and the best European evaluation criteria, additionally it covers contemplated integrity and availability that not tapeworm in the TCSEC

Common Criteria (CC) Represents the efforts of the international community in aligning and developing a criteria of evaluation in security, like result of the European and North American standards. The Common Criteria combines the best elements of the ITSEC, the CTCPEC (of Canada) and Criteria North American Federal (FC), the intention of the common criteria is to identify and to evaluate characteristic in products and syste ms, which are ratified by standard ISO 15408

17799 ISO
This based on the 1995 standard British BS7799 and developed to provide a coherence with the controls jeopardize in the best ones you practice in security information and where the only source of in formation is the company C & A Systems Security LTD

6.2 Propose basic methodology

6.2.1 Description

As a global vision for the development of the penetration tests has a physical and logical integral perspective, commits and external of the objective, a nalogous it is described like the integration and comparison between the real world and the virtual world; consequently one resorts to the application of the scientific method like methodology to follow, from which the processes of obtaining of information , analysis of the information and formulation of hypothesis, the experimentation (development and use of tools) are derived and finally the documentation of the results and the conclusions; through the analysis of the results obtained in each one of the processes, one settles down the strategy and tactics to use. The propose strategy is supported in several known techniques as they are it social engineering, the common sense and the application of tools of hardware and software. 4 phases have been denominated that they search to contribute information to the process of securing of the information, with the results obtained and based on the cycle of prevention, detection and answer

6.2.2 Phase 1: Obtaining of information

Has defined the use of scenes, eac h one of these represents a type of user and information according to the type of connection is compiled. Both first scenes A and B count on restricted profiles (according to policies of standard security); both remaining they count on privileged access, s cene C on the platform and scene D establishes a physical and/or logical connection on the network and is independent in the administration and execution of processes and tasks on a computer

Scenarios :

Scenarios A: Well-known user - Common User
Scenarios B: Well-known user - User with advanced knowledge.
Scenarios C: Well-known user - User administrator of system.
Scenarios D: External user to the company

Types of Connection:

LAN: Locally connected user
INTRANET: User connected from the interna l network.
EXTRANET: User connected from an external network (partner)
INTERNET: User from an external connection.

6.2.3 Phase 2: Analyses of the information and formulation of hypothesis

Based in the collected information, the group of experts anal yze and classify the possible weaknesses detected by critical levels, this looks for to feed the phase on tools application according to the type of detected services and the formulation of hypothesis, which represents a diagnose of the present state of th e technological platform at issue. Afterwards these hypotheses are validated with the experimentation process

6.2.4 Phase 3: Experimentation (Development and use of tools)

In first instance resorts to the DNS search of the servers associated to the doma in , an example of a tool that contributes to this task is the command nslookup.exe of the operating system of Microsoft Windows NT/2000.

Once identified the public servers, three possibilities of global operation can be faced, depending on the physical location of the technological infrastructure

1. External : Internet Solutions Provider ISP + Applications Solutions Provider ASP.
2. Internal : ISP + Department of Computer Science and Technology.
3. Mixed: ISP + ASP + Department of Computer Science and Technolo gy

Once identified the model of global operation, it is come to identify the models of operation for the benefit of services, these models can nowadays be mixed according to the policy of operation of the company, these are known generally like:

Outsourcing: Service of renting and administration of the operation of IT
Hosting: Service of renting of services in the servers of ISP or ASP.
Housing: Service of renting of physical space in a ISP, mainly for teams of communications and servers of the company.
Insourcing: Service of administration of servers of the company by a third party
IT Department: Administration service for servers of the company is internally assumed.

The question arises then: How to identify and to classify the models of global operation and services?. The answer is the use of commands and applications of the operating system like: Ping, Tracert, Nbtstat, Net, Finger, FTP, telnet, Tftp, among others, that help to obtain information of the services in the public servers, the equipment of communications, the private network and the scheme of security that may be in use for his protection

It is important to stand out that through the use of commands and applications of the operating system it is managed to obtain important information that with knowledge of cause or not the company does not have to immediately begin to evaluate the degrees of administrative privileges on the computers for the users, who in most of the cases are of full control, allowing not only to have access to the c onfigurations but to the installation of non -authorized software.

When facing this type of situation is potentially exposed that a user with knowledge or simple curiosity begins to install and to prove the different types from tools mentioned in the data network previously. Once made the obtaining of information and with base in the analysis of the obtained results of the use of commandos and applications, it is possible to be determined a type of situation and global weakness of the platform

Situation A: They do not count on a security scheme.
Possible weakness: Total ignorance of the concept of Computer science Security.

Situation B: They count on an incomplete scheme of security with faults and/or, administered and possibly monitored.
Possible weakness: Policies of security are not defined , faults or omission of elements in the scheme of security like: Rules in the Firewall, filter of content, detection of intruders, decoys, VPN, PKI, etc.

Situation C: They count on an installed scheme of security, administered and possibly monitored.
Possible weakness: Vulnerability of the scheme by faults in the maintenance and/or human.

Each one of these situations has managed to identify elements of the technological platform and of the security scheme used fo r its protection, the following step is to use the tools to verify and evaluate the degrees of prevention, detection and reaction

of the system, using as base of evaluation the alarms and LOGs generated in the use of these. The results obtained through the use of this tool can throw the following situations

Use of nonsafe services on concentrators (Hubs): It represents a high risk for the information system since any connected user could listen to the data, users and keys of access of the following servic es: electronic mail, Web, applications client/server, Data bases search , among other services. Use of nonsafe services on commutators (Switches): Although it diminishes the listening risk, are left other possibilities open that there would be to evaluate like: the ports mirror (port mirror), Segmentation (VLANs) and Gestión (SNMP)

Identification of the services, weaknesses and schemes of passwords: It represents a high degree of risk when exposing publicly the technological platform and the information system, underestimating the use of security elements and/or implementations with faults. Access to the services directly on the production server: It represents a high risk for the information system since any connected user could jeopardize the computer and the services available. Services protected by firewall: Although it diminishes the risk of direct bonding, are left other possibilities open that there would be to evaluate as the content filter on the services, the systems of detection of intruders, de coys, PKI, VPN, among others.

Services protected by a security scheme: When one faces this type of situation, the commitment of the personnel with the policy of security of the company is due to evaluate, it looks for then the human error through techniq ues of social engineering and interpersonalizacion (Supplanting).

6.2.5 Phase 4: Documentation of the results and conclusions.

Document that compiles all the information obtained in the different phases, summarizes the analysis of the results and the d ocumentation of the tests, in addition it raises the recommendations that contribute to the cycle of continuous improvement, contributing to the adjustment in the policies of established security and consequently to the implanted security system, this with the purpose of controlling those services that were not considered initially or which they are totally new within the scheme and which they represent potentially alternative of danger against integrity, confidentiality and availability of the information.

Finally it is very important that 100% of the employees of the company, with base in the obtained or informed experiences, are committed and contributed in the fulfillment of the security policies, of this form this taking a great step in the social apprehension of the culture in computer science security

7. BIBLIOGRAPHY

Common Criteria or ISO 17799:
http://www.sans.org/infosecFAQ/standards/ISO17799.htm
Underground:

www.astalavista.com
Security Site (Spanish):
www.kriptopolis.com
Documents of Asociación Colombiana de Ingenieros de Sistemas:
http://www.acis.org.co/Paginas/publicaciones/archivos.html
Understanding Ethical Hacking:
http://www.itp-journals.com/search/m04133.htm

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor