Attacks

Weaknesses of security commonly exploited

Author: Jorge A. Mieres
E-Mail: jamieres#gmail.com
Personal Blog: http://mipistus.blogspot.com
www.evilfingers.com (January 2009)

White paper

Content

Introduction

Throughout time, the advancement of technology and communication has led to the emergence of new attack vectors and new forms of crime that have turned to the Internet and computer technologies in areas most hostile to any kind of organization, and person that has equipment connected to the World Wide Web.

Unlike what happened years ago, where people with extensive skills in the computer world enjoyed researching these issues with the aim of incorporating more knowledge, at present has been completely distorted giving rise to new characters who use computer resources and knowledge on its operations as tools to commit crime and get some economic benefit.

Every day new vulnerabilities are discovered and, usually, only those responsible for IT including in its just measure the importance of safety and how they can address the serious problem that exists behind vulnerabilities that allow an attacker to violate security environment and commit crimes using the data stolen.

Under this stage where the main actors are organizations of any size and business, information systems, money and crime, it becomes really necessary and essential to devise strategies that provide safety defensive barriers to mitigate attacks effectively both external and inmates.

But to achieve effectively mitigate the impact caused by the attacks, is crucial to know how to attack and what are the weaknesses of a system commonly used in those efforts should focus on security to prevent them.

Accordingly, this paper aims to provide a quick overview on the weaknesses commonly exploited by attackers to shift plans for security in computer systems, along with possible countermeasures under which you may rely to prevent effectively the different types of attacks receives a daily basis.

What does this mean?

An attack is to seize any computer failure or weakness (vulnerability) in the software, hardware, and even in people who are part of an IT environment, to obtain a benefit, usually economic in nature, causing a negative impact on system security, which then directly affects the assets of the organization.

To minimize the negative impact caused by attacks, there are procedures and best practices that facilitate the fight against criminal activities and reduce significantly the scope of the attacks.

One of the most important steps in security, is education. Understand what the most common weaknesses that can be exploited and what are the associated risks, will know how to attack a computer system to help identify weaknesses and risks and then intelligently deploy effective security strategies.

Anatomy of a computer attack

Know the different stages that make up a computer attack offers the advantage of learning to think like attackers and never underestimate their mentality. From the perspective of occupational safety, they should take those skills to understand and analyze how the attackers carried out an attack.

The following image shows the five stages through which often happens when a computer attack to be executed:

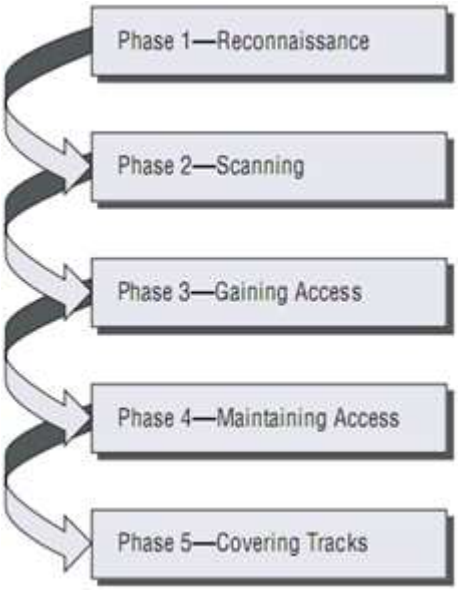

Figure 1. Common phases of a computer attack

Phase 1: Reconnaissance. This stage involves the acquisition of information (Information Gathering) with respect to a potential victim who can be a person or organization.

Usually during this phase are used to different Internet resources like Google, among others, to collect data from the target. Some of the techniques used in this first step is *Social Engineering*, *Dumpster Diving* on the *Sniffing*.

Phase 2: Scanning. In this second stage uses the information obtained in Phase 1 to probe the target and try to get information about the victim such as IP addresses, host names, data authentication, among others.

Among the tools that an attacker can use during the exploration is the *Network Mappers*, *Port Mappers*, *Network Scanners*, *Port Scanners* and *Vulnerability Scanners*.

Phase 3: Gaining Access. In this instance the attack begins to materialize through the exploitation of the vulnerabilities and shortcomings of the system (*Flaw Exploitation*) discovered during the reconnaissance and exploration.

Some of the techniques that an attacker can use *Buffer Overflow* attacks are of *Denial of Service* (*DoS*), *Distributed Denial of Service* (*DDoS*), *Password* and *Session Hijacking Filtering*.

Phase 4: Maintaining Access. Once the attacker has gained access to the system, look for tools that enable them to deploy again in the future to access from anywhere you have Internet access. To do this, utilities often resort to *Backdoors*, *Rootkits* and *Trojans*.

Phase 5: Covering Tracks. Once the attacker was able to obtain and maintain access to the system, try to erase all traces that he was leaving for the intrusion to avoid detection by the security professional or network administrators. Therefore, seek to remove the log files and alarm Intrusion Detection System (IDS).

> *"If you're using the enemy to defeat the enemy, you will be powerful in any place to go."* [2]

[2] Sun Tzu, El arte de la guerra.

Aspects of an attack that compromises safety

The security consists of three fundamental elements that form part of the objectives which the attackers try to compromise. These elements are confidentiality, integrity and availability of resources.

In this perspective, the attacker tries to exploit the vulnerabilities of a system or network to find a weakness in one or more of the three elements of security.

For that, conceptually speaking, is more clear how committed each of these elements at any stage of the attack, let us take as an example the following scenarios as the element concerned.

Confidentiality. An attacker could steal sensitive information like passwords or other data that travel in clear text over networks reliable, violating confidentiality by allowing another person who isn't the recipient has access to data. An example is this element that engages the poisoning of the ARP table (ARP Poisoning).

Integrity. While the information is transmitted through the communication protocol, an attacker could intercept the message and make changes to certain bits of the ciphertext with the intention of altering the data in the cryptogram. This type of attack is called Bit-Flipping and are considered attacks on the integrity of information.

The attack is carried out directly against the cipher, but with a message or a series of coded messages. In the end, this can become a *Denial of Service* attack against all messages on a channel that uses encryption.

Availability. In this case, an attacker could use the resources of the organization such as the bandwidth of the DSL connection to flood the system message and force the victim fall from it, thereby denying resources and services to legitimate users of the system. This is known as *Denial of Service* and directed against the integrity of the information.

Weaknesses of security commonly exploited

Fortunately, there is now a very wide range of security tools effective enough to obtain an adequate level of security against unauthorized intrusion, making the work of the attackers into a difficult road to travel.

Social Engineering

However, beyond any of the forms of security that might arise from an organization, there are strategies of attack that are based on deception and are clearly aimed at exploiting the weaknesses of the human factor: Social Engineering. The attackers know how to use these methods and have incorporated as a fundamental element to implement any kind of attack.

While this technique is used in any field, as far as computers are concerned, is to obtain sensitive information and/or confidential information of a user close to a system or organization to exploit certain features that are typical of human beings.

Undoubtedly, people are one of the most important problems of security for any organization because, unlike the technological components, the only element within a secure environment with the ability to decide to "break" the rules set out in policies for information security.

Whether through ignorance, negligence or coercion, may allow an attacker to gain unauthorized access, who, thus, may circumvent the complex patterns and security technologies that have been implemented in the organization. For example, in this sense, trust and information disclosure are two of the weaknesses exploited to obtain data related to a system.

As countermeasure, the only way to deal with the methods of social engineering is education. Absolutely everyone who is part of the organization, from the secretary, the administrators of the network and the largest dome, must be trained regarding the weaknesses and the methods of deception most commonly used by attackers to succeed in identifying and notifying any anomaly that occurs on the computer or at a particular environment.

This doesn't mean that every employee should take courses in computer security, but the training should be part of the Policy and Information Security should be implemented through dynamic awareness plans.

It's also very common misconception that the staff creates its position within the institution or organization is small and therefore couldn't be attacked, but in contrast, are actually the favorite target for attackers; therefore, education is a very effective countermeasure, but it's vital that people take real awareness that they are the perfect target for social engineering.

> *"You may have implemented the best technology, firewalls, intrusion detection systems or complex systems of biometric authentication... but*

all that is needed is a phone call to an employee unprepared and without access to the system. They have everything in your hands" [3]

Factor Insiders

When speaking about people who are dedicated to attacking computer systems, it's assumed that it was someone unknown who carried out the attack and manages everything from a remote location carried out late at night. Although in some cases it may be true, several studies have shown that most security breaches are committed by the Insiders factor, ie by the same employees from within the institution or organization.

One of the most effective ways that an attacker has to break the patterns of security, from inside the organization. For example, the attacker could get a job in the organization you want to attack and get a sufficient level of confidence in the organization and then use the access points. Similarly, any member can become a disgruntled employee and decide to steal information and/or damage as a form of revenge.

When such acts are committed with intent to obtain financial benefits through corporate information, is denoted Insiders Trading.

In either case, many of the tools and safety measures to be implemented in the environment will not be effective. Under this perspective, it's necessary to resort to internal and defense strategies for the control of specific attacks caused by the personnel of the organization. These strategies will work as defensive countermeasures.

One of the best solutions is to conduct audits that include continuous monitoring programs through *Keyloggers* that can be hardware or software mechanisms that prevent the installation of software by staff, setting the principle of strict minimal privileges, disabling USB ports and prohibiting the use of removable storage devices to prevent the leakage of information and input from other threats such as malware, if the computers are part of a domain is necessary to establish strict policies in Active Directory, among others.

"... if you think that technology can solve all security problems, then do not understand the problem and don't understand the technology" [4]

Malicious Software

Malicious Soft**ware**, or *Malware*, is also a major security threats to any institution or organization and it may seem a trivial issue, usually cause significant economic losses.

This threat refers to programs that cause any damage or anomaly in the system. Within this category are programs trojans, worms, viruses, spyware, backdoors, rootkits, keyloggers, among others.

[3] Kevin Mitnick, The Art of Intrusión.
[4] Bruce Schneier, Secrets & Lies.

Currently, almost 80% of attacks carried out by malicious code are carried out through programs troyanos. [5] This type of malware enters a system so completely surreptitiously activating a hazardous cargo, called payload, which displays the instructions malicious.

The damaging charge that incorporate the trojans can be anything from instructions designed to destroy a sector of the disk, usually the MBR (Master Boot Records), delete files, record keystrokes that are written through the keyboard, monitor network traffic, among many other activities.

Attackers often use trojans in combination with other types of malicious code. For example, when you have gained access via the trojan, the system implemented in other malware like rootkits that can hide the traces that the attacker is on your left (Covering Tracks), and backdoors to re-enter the system as often as deemed necessary, however, to remotely and without, in most cases, network administrators realize their business.

While any person with basic computer skills can create and combine a trojan payload with its benign programs through automated and applications designed for this, the trojans have a special requirement that must be met for achieving success: the need of intervention human factor, in other words, they must be executed by the user.

That is why these threats are spread through different technologies such as USB devices, instant messaging, P2P networks, e-mail, etc., through any method of deception (Social Engineering) programs appear to be harmless under protective cover as screen, virtual cards, flash games, different types of files, pretending to be security tools, among many others.

With regard to internal attacks, as discussed in Factor Insiders often common malware execution by employees, install software or keyloggers ARP Poisoning attacks, with the intention to capture private information such as authentication data.

Countermeasures to prevent attacks through this kind of threat, lie primarily in implementing programs that operate under antivirus detection mechanisms such as advanced heuristics, which can monitor, control and manage in a centralized way each of the nodes involved in the network, along with education plans aimed at creating awareness among staff about security risks represents the malware.

> *"But we, going to another topic and sings the stratagem of the wooden horse Epeo produced with the help of Athena, the ambush that once led the divine Odysseus to the Acropolis, filling it with the men who destroyed Ilion."* [6]

[6] La Odisea de Homero. Canto VIII, 490.

Password

Another factor commonly exploited by attackers are the passwords. While there are now sophisticated authentication systems, passwords are still and will continue to be one of the most widely used measures of protection in any system.

Therefore, constitute one of the most wanted white attackers computer up because the main component used for simple authentication process (username/password) where each user has an identifier (username) and password associated with that identifier, together, let the system identify themselves.

In such process, known as single factor, the security of authentication scheme inevitably lies in the strength of the password and keep it in complete secrecy, to be potentially vulnerable to social engineering techniques, where the owners will not have a proper level of training to prevent such attacks.

If the environment is solely based on protection through simple authentication systems, the possibility of being attacked cracking or unauthorized intrusion is power. Coupled to this there are automated tools designed to "crack" passwords through various techniques such as brute force attacks, dictionary or by a hybrid very short term, the problem is multiplied even more.

Based on the above explanation, it can be assumed that the solution to this problem is to create much longer passwords (which does not mean they are robust). However, this strategy is ineffective, simply because the staff isn't prepared to remember long strings of characters and end up writing in places or sites accessible by any other person, even to people who don't belong to any particular area restricted access.

While a password that is longer than ten characters, and that people can remember, it's much more effective than a four-character, yet there are other problems that are often exploited by attackers. Below is some of them:

- Using the same password on multiple accounts and other services.
- Access to resources they need authentication from public places where the attackers may have introduced programs or physical devices such as keyloggers that capture the information.
- Use of insecure communication protocols which transmit information in clear text such as email, web browsing, chat, etc..
- Techniques such as *Surveillance* (video), or *Shoulder Surfing* (looking behind the shoulder), among others, which evade security checks.

As a countermeasure designed to strengthen this aspect of security, it's possible to implement stronger authentication mechanisms such as "dual factor strong authentication" which not only needs to have something that is known (the password) but it's also necessary to have something that is like an electronic key or a USB card that stores digital certificates so that through them or not to validate user access to the resources of the organization.

> *"There is no point if we use strong passwords are forgotten or shared, as this compromises the security of the whole authentication mechanism."*

Misconfigurationes

The default settings in both operating systems, applications and devices implemented in the computer environment, form another of the weaknesses that are often overlooked by mistakenly thinking that this isn't trivial factors are present in the list of the attackers.

However, the default settings make the attack a simple task for anyone who runs it as it's very common for a computer vulnerabilities are exploited through codes which exploit the scenario that assumes that code is that the target is set with default parameters.

Many applications are designed for automated exploit these vulnerabilities, taking into account the default settings, even, there are websites that store databases with information related to user names and their associated passwords, access codes, configurations, among others, the default operating systems, applications and physical devices. Simply type in a search engine key words "default passwords" to see the myriad of resources available that offer this type of information.

Therefore, one of the most effective countermeasures to mitigate and prevent safety problems in this aspect and that is often ignored, is simply change the default values. In this regard it's important not to sacrifice the availability of resources to gain security. You must find a balance between usability and security.

Practice to strengthen the IT environment in a safe setting technology to counter the attack vectors is called hardening. In this regard, the responsibility for everything that is within their power to change the default rests with those responsible for the administration of the teams.

It's important that during the hardening process is also tested other aspects such as options that are configured by default when you install operating systems and other resources, such as path names, folder names, components, services, settings and other adjustments required or unnecessary to provide an adequate level of protection.

> *"Nothing makes attacking a target within a network as easy as when the objectives are the default values set by the device manufacturer."*[7]

OSINT (Open Source Intelligence)

The attackers, especially those outside attackers, learn constantly attack techniques that allow you to penetrate the security schemes that are more complex. Consequently, the question that immediately comes up is how do they succeed?, and although the answer might seem somewhat complicated, it's more simple you might imagine. The answer is research.

One of the first aspects of a computer attack, consists of gathering information through various techniques such as *Reconnaissance*, *Discovery*, *Footprinting* or *Google Hacking* and

[7] Ten ways hackers breach security. Global Knowledge.

precisely, Open Source Intelligence refers to obtaining information from public sources and open.

The information gathered by the attacker, it's simply the result of a detailed research on the target, get focused on all public information available about the organization from public resources. In this aspect, an attacker will spend more than 70% of their time in reconnaissance activities and obtain information that the attacker learns the more on target, the easier it's to successfully carry out the attack.

What is really worrying lack of awareness in this regard because there is no doubt that information is the most important asset for any organization. In most cases, companies offer a vast amount of data that make the task of collecting a matter as simple as reading this article.

Generally, intelligence on the attackers make their goals for several months before beginning the first goal against the logical interactions across different tools and techniques such as scanning, banner grabbing (capture holders) and scanning utilities. Still, these polls are just looking for subtle verify the data obtained.

The heads of the organizations are surprised to see the wealth of information that can be found on the Internet, not only the activities of the organization, but also information on the activities of employees and their families.

Through the following list reflects some specific examples of the type and sensitivity of the information that an attacker could get to OSINT:

- The names of senior managers/executives and any employee can be obtained from press releases.
- Business address, telephone numbers and fax numbers from various public records, or directly from the website.
- What or which companies provide the Internet service (ISP) through simple techniques such as DNS lookup and traceroute.
- The home address of the staff, their phone numbers, curriculum vitae, details of family members, into which functions, criminal records and more looking for their names in different places.
- Operating systems that are used in the organization, the main software, programming languages, special platforms, manufacturers of the devices for networking, file structure, file names, the web server platform, and more.
- Physical weakness, accesspoint, signals active endpoint, satellite images, among others.
- Confidential documents accidentally or intentionally sent to personal accounts of people who don't at present have no connection with the organization, beyond the passage through it.
- Vulnerabilities in the products used, problems with staff, publications, statements, policies of the institution.
- Comments on blogs, reviews, case law and competitive intelligence services.

As you can see, there is no limit to the information that an attacker can obtain from public sources open where, in addition, data obtained may lead to the discovery of more information.

With regard to preventive measures that can be implemented, there is a starting point defined by the information already available on the Internet and those that are published in a future public sources.

In the first case, once the information is there on the Internet is always available without being modified or deleted, therefore, continue to erode the security of the institution. However, there is always the ability to clear any information resource that is under its direct control, contacting people who have the information and request the change.

With regard to the information being published, before doing so must be executed effective countermeasures that provide protection of certain information. This is achieved through strict security policies to control or limit information that goes in the future to the world outside the organization, being discreet ads in details of projects and products, press releases, and so on.

> "Most organizations are bleeding data freely give companies too much information that can be used against them through various kinds of logical and physical attacks."[8]

[8] Ten ways hackers breach security. Global Knowledge.

Conclusion

It's extremely necessary to act proactively against possible attacks that the organization can suffer. This is accomplished by looking for problems with the same dedication with which the attackers seek to exploit vulnerabilities.

One must keep in mind that once the attacker had gained access to the system, the first thing you do is to implement tools to hide their tracks (rootkits) and enter the computer each time you need no matter where log (backdoors) making gain greater control over the target. In addition, an unauthorized intrusion can not be detected almost indefinitely if it's carried out by an attacker with many patients.

There are multiple access points and paths that the attacker can use to obtain information and access to an environment that is considered safe. Therefore, don't skip any of the issues related to the IT environment that seem to minimum, and follow the best practices recommended by security professionals is good advice to keep in mind.

Always remember that the enemy is ignorance and ignorance always favors the attacker.

Bibiography

- Report on Latin America malware, ESET Latinoamérica Laboratory, 2008. http://www.eset-la.com/threat-center/1732-informe-malware-america-latina
- Ten ways hackers breach security. Global Knowledge. 2008 http://images.globalknowledge.com
- Bruce Schneier, Secrets & Lies. Digital Security in a Networked World. John Wiley & Sons, 2000.
- Kevin Mitnick, The Art of Intrusión. John Wiley & Sons, 2005.
- The “Odyssey” of Homer.
- Official Certified Ethical Hacker, Sybex. 2007.
- Sun Tzu, The Art of War. Samuel Griffith version. Publisher Benedikt Taschen. 2006.