Global Information Assurance Certification Paper

Understanding Computer Break-Ins

Computer security consulting groups across the country are conducting security studies that identify intrusion detection and reporting as a high priority amongst organizations. Encrypted passwords, firewalls, and occasional security updates for software are necessary basic precautions. However, assuming that after having taken these precautions all is safe is a grave mistake. What good is locking the servers behind closed doors if a hacker has the key?

It takes but one oversight to allow a hacker to invade a company and steal vital competitive information, or even cripple its infrastructure. There is also an asymmetry between the value of the information which may be lost to the hacker – which may be intrinsically small – and the privacy, civil liability, customer liaison and regulatory damage which may be caused to an organization – which may be very great.

An organizations greatest weapon against internal and external attacks should be the ability to monitor its networks for unauthorized behavior, which can provide protection, and timely and effective countermeasures in the event of a breach, as well as deterrent against abuse. However, without the proper resources and mandates in place to implement and carry out such a task, the security of an organization information infrastructure and competitive advantage are at risk.

Everyday, all over the world, computer networks and hosts are being broken into. The level of sophistication of these attacks varies widely; while it is generally believed that most break-ins succeed due to weak passwords, there are still a large number of intrusions that use more advanced techniques to break in. Less is known about the latter types of break-ins, because by their very nature they are much harder to detect.[1]

Computer break-ins occur in many ways because systems connected the Internet almost always have certain vulnerabilities. To protect their internal networks, companies install firewalls, powerful defensive software that blocks unauthorized intruders. Nevertheless, determined hackers can usually uncover ways of circumventing a firewall.[2]

Desktop systems make up the bulk of any large corporation's IT assets, yet they are often the least well protected. Due to the nature of their design and use, they are also the most vulnerable to compromise and attack. The most notable threat is of course the virus. Because of weak security and careless application design, desktop workstations are particular vulnerable to malicious code that can be transmitted by e-mail and the file exchanges. Some virus attacks are merely an annoyance, but as the recent Melissa virus proved, enough annoying behavior can paralyze or even cripple a company's infrastructure. The CIH virus is an example of a particularly vicious type of attack. It will destroy the data on the hard drive and then attempt to corrupt the system BIOS. The result is a system where the data as well as the operational capacity has been completely destroyed. The time period during reconstruction is particularly susceptible for hacker

attack.
For years, "hackers" have broken into computer systems, and now an entire industry is dedicated to computer network security. Both hackers and computer security professionals have developed software tools for either breaking into systems or identifying potential security problems within computer networks.

An intrusion can be defined as:

Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusions can be categorized into two main classes:

1. Misuse intrusions are well-defined attacks on known weak points of a system. They can be detected by watching for certain actions being performed on certain objects.
2. Anomaly intrusions are based on observations of deviations from normal system usage patterns. They are detected by building up a profile of the system being monitored, and detecting significant deviations from this profile.[3]

When conducting examinations of systems that have been successfully attacked, certain patterns emerge. Data recovered from both the attacked systems and the computers of the intruders reveal similarities in how the intruders target and attack their victims. It has become clear that many of the components of the attacks are automated and facilitated through the use of sophisticated software toolkits.

The tools and techniques can be broken down into five distinct categories. Each category defines tools and techniques that have been developed to exploit a specific type of system vulnerability. These categories are scanners, remote exploits, local exploits, monitoring tools or sniffers, and stealth and backdoor tools.

With a collection of tools and "exploit scripts" in hand, the intruder can then move on to attack a computer network. Many intrusions are conducted against random targets where the main goal is to breach network security. These attacks, while common, are motivated by intellectual challenge rather monetary gain. However, there is mounting evidence of a more focused type of attack on the networks of specific organizations for the purpose of fraud and espionage.[4]

The need for a scalable, flexible, upgradeable intrusion detection system, which can address a variety of threats in an integrated, cost-effective manner, is thus paramount to an organization. The tools being used by most organizations today are capable of security scanning and log analysis, but are only used for network availability management. These monitoring products as they are currently being used are not configured to provide comprehensive intrusion monitoring, as they do not protect against nor detect security incidents. Consequently, such an organization has no means of responding in a timely manner to prevent damage to computer systems and therefore is in danger of being compromised.

Firewalls are powerful defensive tools that can block unauthorized intruders or simply be used as a method for connecting external connections to some area – for instance a DMZ or to an intranet. However, in many cases, determined hackers can usually uncover ways of circumventing a firewall – unless all corollary sources of intrusion – non-IP, telephony, and internal media – have been secured.

There are seven stages of system penetration:[5]

Reconnaissance – gather information about the target system or network. This
Probe and attack – probe the system for weaknesses and deploy the tools.
Toehold – exploit security weakness and gain entry into the system.
Advancement – advance from an unprivileged account to a privileged account.
Stealth – hide tracks; install a backdoor.
Listening post – establish a listening post.
Takeover – expand control from a single host to other hosts on the network.

New sources of damage, such as the highly publicized threats of computer viruses and computer hackers, continue to emerge. Such threats to information security are expected become more widespread, more ambitious and increasingly sophisticated. At the same time, because of increasing dependence on IT systems and services, your organization may be becoming more vulnerable to security threats. The growth of the networking presents new opportunities for unauthorized access to computer systems. The sooner you take action to safeguard your information systems, the cheaper and more effective it will be for your organization in the long run.[6]

A good understanding of the security risks to your organizations infrastructure, both threats and vulnerabilities, to organization assets and of the level of security inside the organization, which should be based on the value of importance of the assets. Also, effective marketing of security to all managers and employees is critical to securing your companies assets as well as the distribution of comprehensive guidance on information security policy and standards to all employees and contractors.

There is always a trade-off to be made between making a computer secure and the function it can provide. In the extreme case, the most secure computer is one that is turned off. Knowing why something is a problem is the real key to learning and to making an informed, intelligent choice as to what security really means for your organization.

---

[1] Farmer, Dan, Improving Your Site by Breaking Into It, Sun Microsystems, zen@sun.com
[2] Meinel, Carolyn, How Hackers Break In and How They are Caught, Scientific American, October, 1998
[3] Intrusion Classification, http:///www.cs.purdue.edu/coast/intrusion-detection/classification.html
[4] Boulanger, A., Catapults and Grappling Hooks: The Tools and Techniques of Information Warfare, http://www.research.ibm.com/journal/sj/371/boulanger.html, 1998
[5] Boulanger, A., Catapults, IBM, 1998
[6] Information Security Management, Part 1. Code of Practice for Information Security Management Systems, 1995