

INTRUDERS

A significant security problem for networked systems is hostile, or at least unwanted, trespass being unauthorized login or use of a system, by local or remote users; or by software such as a virus, worm, or Trojan horse.

One of the two most publicized threats to security is the intruder (or hacker or cracker), which Anderson identified three classes of:

- Masquerader: An individual who is not authorized to use the computer (outsider)
- Misfeasor: A legitimate user who accesses unauthorized data, programs, or resources (insider)
- Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection (either)

Intruder attacks range from the benign (simply exploring net to see what is there); to the serious (who attempt to read privileged data, perform unauthorized modifications, or disrupt system).

The intruder threat has been well publicized, particularly because of the famous “Wily Hacker” incident of 1986–1987, documented by Cliff Stoll. Intruder attacks range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there. At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system.

One of the results of the growing awareness of the intruder problem has been the establishment of a number of computer emergency response teams (CERTs). These cooperative ventures collect information about system vulnerabilities and disseminate it to systems managers.

The techniques and behavior patterns of intruders are constantly shifting, to exploit newly discovered weaknesses and to evade detection and countermeasures. Even so, intruders typically follow one of a number of recognizable behavior patterns, and these patterns typically differ from those of ordinary users.

Examples of Intrusion

GRAN04] lists the following examples of intrusion:

- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password
- Using an unattended, logged-in workstation without permission

Hackers

Traditionally, those who hack into computers do so for the thrill of it or for status. The hacking community is a strong meritocracy in which status is determined by level of competence. Thus, attackers often look for targets of opportunity, and then share the information with others. Benign intruders might be tolerable, although they do consume resources and may slow performance for legitimate users. However, there is no way in advance to know whether an intruder will be benign or malign. Consequently, even for systems with no particularly sensitive resources, there is a motivation to control this problem.

Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are designed to counter this type of hacker threat. In addition to using such systems, organizations can consider restricting remote logons to specific IP addresses and/or use virtual private network technology.

One of the results of the growing awareness of the intruder problem has been the establishment of a number of computer emergency response teams (CERTs). These cooperative

ventures collect information about system vulnerabilities and disseminate it to systems managers. Unfortunately, hackers can also gain access to CERT reports. Thus, it is important for system administrators to quickly insert all software patches to discovered vulnerabilities.

Hacker Behavior Example

The techniques and behavior patterns of intruders are constantly shifting, to exploit newly discovered weaknesses and to evade detection and countermeasures. Even so, intruders typically follow one of a number of recognizable behavior patterns, and these patterns typically differ from those of ordinary users. Table 20.1a, based on [RADC04] summarizes an example of the behavior of hackers. This example is a break-in at a large financial institution.

The intruder took advantage of the fact that the corporate network was running unprotected services, some of which were not even needed. In this case, the key to the break-in was the pcAnywhere application. The manufacturer, Symantec, advertises this program as a remote control solution that enables secure connection to remote devices. But the attacker had an easy time gaining access to pcAnywhere; the administrator used the same three-letter username and password for the program. In this case, there was no intrusion detection system on the 700-node corporate network. The intruder was only discovered when a vice president walked into her office and saw the cursor moving files around on her Windows workstation.

1. select target using IP lookup tools
2. map network for accessible services
3. identify potentially vulnerable services
4. brute force (guess) passwords
5. install remote administration tool
6. wait for admin to log on and capture password
7. use password to access remainder of network

Criminal Enterprise

Organized groups of hackers have become a widespread and common threat to Internet-based systems. These groups can be in the employ of a corporation or government, but often are

loosely affiliated gangs of hackers. Typically, these gangs are young, often Eastern European or Russian hackers who do business on the Web. They meet in underground forums with names like DarkMarket.org and theftservices.com to trade tips and data and coordinate attacks. A common target is a credit card file at an e-commerce server. Attackers attempt to gain root access. The card numbers are used by organized crime gangs to purchase expensive items, and are then posted to carder sites, where others can access and use the account numbers; this obscures usage patterns and complicates investigation.

Whereas traditional hackers look for targets of opportunity, criminal hackers usually have specific targets, or at least classes of targets in mind. Once a site is penetrated, the attacker acts quickly, scooping up as much valuable information as possible and exiting.

IDSs and IPSs can also be used for these types of attackers, but may be less effective because of the quick in-and-out nature of the attack. For e-commerce sites, database encryption should be used for sensitive customer information, especially credit cards. For hosted e-commerce sites (provided by an outsider service), the e-commerce organization should make use of a dedicated server (not used to support multiple customers) and closely monitor the provider's security services.

- organized groups of hackers now a threat
 - corporation / government / loosely affiliated gangs
 - typically young
 - often Eastern European or Russian hackers
 - often target credit cards on e-commerce server
- criminal hackers usually have specific targets
- once penetrated act quickly and get out
- IDS / IPS help but less effective
- sensitive data needs strong protection

Criminal Enterprise Behavior

1. act quickly and precisely to make their activities harder to detect
2. exploit perimeter via vulnerable ports
3. use trojan horses (hidden software) to leave back doors for re-entry
4. use sniffers to capture passwords
5. do not stick around until noticed
6. make few or no mistakes.

Insider Attacks

Insider attacks are among the most difficult to detect and prevent. Employees already have access and knowledge about the structure and content of corporate databases. Insider attacks can be motivated by revenge or simply a feeling of entitlement. An example of the former is the case of Kenneth Patterson, fired from his position as data communications manager for American Eagle Outfitters. Patterson disabled the company's ability to process credit card purchases during five days of the holiday season of 2002.

As for a sense of entitlement, there have always been many employees who felt entitled to take extra office supplies for home use, but this now extends to corporate data. An example is that of a vice president of sales for a stock analysis firm who quit to go to a competitor. Before she left, she copied the customer database to take with her. The offender reported feeling no animus toward her former employer; she simply wanted the data because it would be useful to her.

Although IDS and IPS facilities can be useful in countering insider attacks, other more direct approaches are of higher priority. Examples include: enforcing least privilege, monitor logs, protect sensitive resources with strong authentication, on termination delete employee's computer and network access and make a mirror image of employee's hard drive before reissuing it.

- among most difficult to detect and prevent
- employees have access & systems knowledge
- may be motivated by revenge / entitlement
 - when employment terminated

- taking customer data when move to competitor
- IDS / IPS may help but also need:
 - least privilege, monitor logs, strong authentication, termination process to block access & mirror data

Insider Behavior Example

1. create network accounts for themselves and their friends
2. access accounts and applications they wouldn't normally use for their daily jobs
3. e-mail former and prospective employers
4. conduct furtive instant-messaging chats
5. visit web sites that cater to disgruntled employees, such as f'dcompany.com
6. perform large downloads and file copying
7. access the network during off hours

Intrusion Techniques

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. Most initial attacks use system or software vulnerabilities that allow a user to execute code that opens a back door into the system. Alternatively, the intruder attempts to acquire information that should have been protected. In some cases, this information is in the form of a user password. With knowledge of some other user's password, an intruder can log in to a system and exercise all the privileges accorded to the legitimate user.

Knowing the standard attack methods is a key element in limiting your vulnerability. The basic aim is to gain access and/or increase privileges on some system. The basic attack methodology list is taken from McClure et al "Hacking Exposed".

- aim to gain access and/or increase privileges on a system
- often use system / software vulnerabilities
- key goal often is to acquire passwords

- so then exercise access rights of owner
- basic attack methodology
 - target acquisition and information gathering
 - initial access
 - privilege escalation
 - covering tracks

Password Guessing

Password guessing is a common attack. If an attacker has obtained a poorly protected password file, then can mount attack off-line, so target is unaware of its progress. Some O/S take less care than others with their password files. If have to actually attempt to login to check guesses, then system should detect an abnormal number of failed logins, and hence trigger appropriate countermeasures by admins/security. Likelihood of success depends very much on how well the passwords are chosen. Unfortunately, users often don't choose well.

- one of the most common attacks
- attacker knows a login (from email/web page etc)
- then attempts to guess password for it
 - defaults, short passwords, common word searches
 - user info (variations on names, birthday, phone, common words/interests)
 - exhaustively searching all possible passwords
- check by login or against stolen password file
- success depends on password chosen by user
- surveys show many users choose poorly

Password Capture

There is also a range of ways of "capturing" a login/password pair, from the low-tech looking over the shoulder, to the use of Trojan Horse programs (eg. game program or nifty utility with a covert function as well as the overt behaviour), to sophisticated network monitoring tools, or extracting recorded info after a successful login - say from web history or cache, or last number dialed memory on phones etc. Need to educate users to be aware of whose around, to check they really are interacting with the computer system (trusted path), to beware of unknown source s/w, to use secure network connections (HTTPS, SSH, SSL), to flush browser/phone histories after use etc.

- another attack involves **password capture**
 - watching over shoulder as password is entered
 - using a trojan horse program to collect
 - monitoring an insecure network login
 - eg. telnet, FTP, web, email
 - extracting recorded info after successful login (web history/cache, last number dialed etc)
- using valid login/password can impersonate user
- users need to be educated to use suitable precautions/countermeasures