The Basic Elements Of Cracking

By: C0ldPhaTe

Introduction

First off understanding how crackers work is vital for any system administrator, while you continue to read this, you will soon realize a true cracker is going to understand and have a reason why before they begin to take the time to breach your system security. The cracker will know exactly what he is trying to get and exactly what he needs to gain access.

Once the cracker knows why they need to gain access to your system this will determine how long they will take trying to gain unauthorized access, this will also prevent them from wasting there time on attacking sites that have no value. So before a cracker will even start attacking they will have a game plan of exactly how there going to do things.

Now the system administrators that are protecting the system the cracker is trying to breach should read as many text files or books on cracking as possible, because by reading information about cracking it will help them create a stronger and harder to penetrate operating system.

Now anyone who knows anything about cracking knows it's a form of Black Art of "cracking" this might just lead you into heavy problems with the law or even end up in your having to serve jail time and making friends with a guy named Bubba. So if your going to breach a system make sure to go to any means necessary to protect yourself because all it takes it was little slip up or just being plain to lazy to cover your tracks.

About Penetrating The Security

There is more then one way to penetrate a systems security, and a good cracker would know as many of them as possible. Hosts with remotely good security should be able to block more then half of the stuff listed within the document. But the real trick to gaining access is being persistent, but you will need to realize any signs of long term attacks is going to show up in the systems log files. This in return will alert the systems administrators that someone is trying to breach their systems security. So a good cracker will spread there're attacks across a certain period of time and across a number of different remote sites. But doing this it will minimize your chances of being caught and bring up a less chance of being detected.

System "Backdoors"

System backdoors can be found in a variety of different ways. The better the understanding of IP network protocols, odd switches on the user and system commands of the target operating system greatly increases the crackers chance of gaining access. Good crackers are always reading more often then so. You will find a lot of good crackers often reading the average security book to see what it recommends to secure a site.

Password Attacking

One of the few oldest ways of gaining access to the password file is using tools such as Crack tools like crack can be used to obtain plain text passwords. Example if your target is running Sun's Network Information Services (NIS) a good crack will know to go and get tools to crack the target system with. In this particular cause the cracker would try and get a hold of a tool known as YPX and try guessing the NIS domain. If your lucky enough to get the domain right and you shell get the password file to the whole domain.

This brings me to another form of password files. There are two types of password files one is Unshadowed and the other one is Shadowed. Unshadowed password files will display the password and login in plain text but shadowed password files on the other hand will not. In order to crack an unshadowed password file you will have to get some tools from the net. An older trick which is not used much because it shows up as someone trying to breach there system security is known as Brute Forcing. Brute Forcing is when the program you're running repeatedly tries userid password combinations. However sites and servers now a days simply disconnect you from their site after three failed attempts. However you will come across some sites that do not disconnect you. If you do indeed gain access to the site it's a good idea to find the sites or servers log files and clean them up. If you indeed have the opportunity to do this do than do it. This will make the system administrator job a lot harder finding how the security was breached and who exactly breached it.

Gaining Privileges

There are many ways to break into a system. Breaking into a system requires deep knowledge of the fundamentals and ways that networks and systems work; this helps the cracker gain access to the system using ordinary tools. So now that the crack is in what should you do next? Unless your just going to surf around the system and read users email or use the normal users facilities you will need to get some system privileges. To make all the time your taking to breach the system you will want to get admin privileges.

There are numerous reasons why you might want administrative privileges; these reasons will more or less depend on the remote host. A good cracker will always know why there choosing the target they chose. There are not a lot of reasons why a cracker would want to enter the system a couple of them are as follows

- To install Services that run on low privileged ports or hosts
- Installing fake users to allow them to get back into the server later
- To place one or more Ethernet interfaces into promiscuous mode
- Ability to hide there presents on the system
- To make adjustments to the system itself
- To be able to edit server logs to cover there break in

There are numerous ways of getting system privileges, all the ways depending on the system that the cracker is using and they normally fall into one or more categories. Hierarchy of system privileges occurs in most systems. Privileges with the lower user at the bottom and the system administrator at the very top, but in between these two there can be a majority of users with different user privilege levels. So in return this makes all the users within a system worth investigating.

Once a cracker has the necessary system privileges they can now advance forward to take control of the computer or do whatever there set purpose was for cracking the system in the first place. Most crackers will not destroy any data on a cracked computer because all this does is give crackers bad names. Bu “ethical” crackers on the other hand target things such as porn sites and they will do there best to destroy the site and computer. The reasons for this are obvious, because a lot of sites on the web now a day has nothing but kiddy porn located within the web page itself.

Network Filing Services

The one most common found service offered on any Local Area Network (LAN) is the network filling service. This service allows access to files stored remotely on a server as though the files would be located locally. In order for these services to work the map a network connection containing things known as “File Handles” to the actual physical filing system within the server. In order for a user to get a file that is needed within a server their computer makes a connection to the program providing the network filling services. This is done by the Local Area Network, the server then calls the operating systems routine to provide access to the local files, which is then sent back to the client trying to get the file through another connection.

Network filing systems are capable of doing disk access on the server, so that means that more then half the time they are written to run in a privileged mode. Many subversions of the network filing system protocol can be used to lead you to access to files or maybe programs located on the server.

Most network filing systems contain vulnerabilities and by using a packet sniffer you can possibly determine file handles of date being read from the server then with you luck you can reuse these file handles to spoof access. Commonly you will find some network filing systems suffer from something known as buffer overflows in command handling, just like other services and these can also be exploited to run remote code against the specific target. Implementations of the same network filing system are known to be alike. With a good understanding of how remote host calls the server this can be used to provide file access which in return can be used to manipulate the filing system on the server, if the servers remote service supports undocumented or low level routines.

Remote Procedure Calls (RPC)

Computer systems designed for networking, such as Unix provide a mechanism to allow users on remote hosts to be able to execute commands on a server. These are known as Remote Procedure Calls (RPC) these calls can be abused if the systems administrators do not take the correct security precautions. Services such as network filing services and remote printing services these are commonly found services that are offered a Remote Procedure Calls. A good cracker will often ascertain which services are also running this can be figured out by using the “rpcinfo” command.

You will find a lot of software vendor’s use Remote Procedure Calls (RPC) to code remote routines on the server. Software vendors do this because the server overhead is lower than using a TCP/IP service; this in return will make the response time quicker. A good cracker will always investigate any unusual services they find running on a remote host and learn about what they can do with what the find and how they can possibly use it to control access. Targets running PC/NFS a service which allows client Personal Computers to use the network filing system. This means that a cracker can exploit the differences between Personal PC and Unix file systems.

Commands For Remote Access

Apart From Remote Procedure Calls (RPS) there is another group of programs to facilitate remote access called the “r” commands, they are called this because the all start with “r” to designate remote access versions of common system commands. These commands are designated to allow users working on one host to access another host this will give you a valid userid. The use of the “r” commands in a Local Area Network (LAN) seriously compromises security.

COMMAND	DESCRIPTION
rlogin	Remote login to hosts
rcp	Remote copy files from hosts to hosts
rsh	Remote shell passes commands to hosts for execution
rdist	Remote distribution files
rwho	Remote "Who"
rusers	Find info about logged on users
rwall	Write messages to all remote hosts

How Crackers Cover There Tracks

Once a cracker gets into a remote system they will need to hide themselves from the pesky system administrators. This is yet another reason why a cracker needs to know why they are cracking the target there attacking. If you are cracking a common system such as Solaris or Linux. There are tools known as root kits. Root kits contain every tool a cracker could possibly ever need, a root kit will also contain software that can be compiled on the target system and that will also be needed to cover the crackers tracks.

Conclusion

When cracking a system you have to remember one thing, not to get caught. Also before just randomly attacking a system remember to have a reason to attack what you're attacking. If the law catches you there is going to be some heavy fines and even possibly some jail time. Remember to always cover your tracks I cant stress that enough. There are thousands of young hackers/crackers getting busted everyday for hacking or cracking .gov systems because they lack the knowledge of the target system or because they just plain forget to cover there tracks. If you would like to contact me you can do so at the following places.

MIRC - irc.dal.net #cctc, #ncl, #hackalot, #hack-i, #antilamer, #MINDtech
E.Mail - **gbrooks@mcintoshstudent.com**
AOL IM: Myst1kal One

Other Documents I Have Written

Microsoft IIS Unicode Exploit Explained - November 13, 2002
The Basic Elements Of Cracking - November 17, 2002