

DATA SECURITY MANAGEMENT

COMPROMISE RECOVERY AND INCIDENT HANDLING

Sumit Dhar

INSIDE

Before We Start; Incident Handling Steps; Preparation; Detection and Identification;
Containment and Analysis; Eradication and Recovery

Fool me once, shame on you. Fool me twice, shame on me!

— Lieutenant Scott, Star Trek (Friday's Child)

INTRODUCTION

Most systems administrators are too busy to pay any special attention to security. Often, they will pull out the required installation CD, plunk it into the CD-ROM drive, and proceed with a default installation. As a result, many such installations are susceptible to crackers and sooner or later get compromised.

Crackers might use the compromised box for a variety of purposes, including:

- Storing porn
- Setting up an illegal *warez* server
- Launching attacks against other sites
- Running programs such as IRC, Crack, Trinoo/TFN, etc.
- Compromising other servers on your network

If your server is hacked and used for the purposes outlined above, you might face legal repercussions. Hence, it is important that such compromises are discovered quickly and corrective action taken immediately. This article is aimed at Linux/UNIX systems administrators and information security administrators who would like to learn a little bit more

PAYOFF IDEA

Most systems administrators are too busy to pay any special attention to security. Often, they will pull out the required installation CD, plunk it into the CD-ROM drive, and proceed with a default installation. As a result, many such installations are susceptible to crackers and sooner or later get compromised. It is important that such compromises are discovered quickly and corrective action taken immediately. This article explains the steps to be taken for compromise recovery and ways to handle such incidents.

about the steps that should be taken for compromise recovery and ways to handle such incidents.

BEFORE WE START

Before we talk about the various steps involved in *compromise recovery* and *incident handling*, it is important to keep the following key points in mind:

- *Policies and procedures.* Ensure that you have policies and procedures in place for handling such incidents, long before the compromise occurs. This enables the people involved with incident handling and compromise recovery to have a clear-cut idea about the work expected of them, the sequence of steps to be taken, the response procedure, the people they should contact, etc.
- *Do not panic.* Discovering a compromised system on the network can cause any systems administrator to lose his cool. But it is important not to act in haste. Every decision must be taken after careful consideration. Launching counter-attacks against the *perceived attacker(s)* is certainly not recommended.
- *Inform the concerned parties.* Sooner or later you will need to inform the concerned parties. An important point to remember while informing the concerned parties is to use the “need-to-know” principle.
- *Use secure communication mechanism.* Often, the intruders monitor network traffic for interesting tidbits. Using the network to communicate about the compromise might alert the intruders and provide them with information about the steps you are taking. During such a crisis, it might be a good idea to use the phone or the fax.

INCIDENT HANDLING STEPS

Step 1: Preparation

This step must be carried out before the intrusion takes place. It includes selecting the various tools/packages required to respond to an intrusion, understanding how to use these tools, and having knowledge of what crackers do after compromising the system.

After compromising a system, crackers do several things to hide their intrusion. They replace quite a few common binaries with Trojans. The programs that might be Trojaned include telnet, login, ps, du, df, ls, netstat, find, su, inetd, shared libraries, static system libraries, lsof, who, finger, md5sum, top, w, etc. As a result, the output returned by any program on the compromised system cannot be trusted. They will not show any activity related to the crackers and might lead you to believe that no such compromise has taken place.

Thus, you will need to prepare an “Incident Handling CD-ROM” that will contain all the necessary programs and whose integrity you can trust. This step should ideally be performed before the compromise takes place. The following are some of the programs you should have on the Incident Handling CD: ps, du, df, dd, ls, netstat, find, shared libraries, static system libraries, lsof, passwd, who, finger, md5sum, top, gcc, tar, gzip, cp, mv, chown, chgrp, cat, less, vim, and w. If

you think you might also need some other programs, feel free to add them to this CD.

Most of these programs use *dynamically linked libraries*. But because the crackers may have also modified these libraries, it is a good idea to compile the above-mentioned programs as *static binaries*. If the source code of the program is available, then compiling it with the `-static` flag of `gcc` will ensure that it is a stand-alone executable.

Sometimes, the source code of the program might not be available and you are forced to use the dynamically linked binaries. In that case, the following approach will be useful:

The shared libraries are stored in `/lib` or `/usr/lib`. Copy these from the file system of a trusted machine on to the Incident Handling CD. Then export the `LD_LIBRARY_PATH` variable to the relevant directories on the CD. This way, when you run a dynamically linked binary, it looks for the shared libraries on the CD first and does not use the unreliable ones of the compromised system.

```
[root@dragonfang root] mount /dev/cdrom /mnt
[root@dragonfang root] export LD_LIBRARY_PATH=/mnt/lib:
/mnt/usr/lib
```

To ensure the binaries on the Incident Handling CD are used, you can either give the complete path (`/mnt/bin/ls`) or export the environmental `PATH` variable to the directory containing those executables:

```
[root@dragonfang root] export PATH=/mnt/bin/
[root@dragonfang root] ls
```

Along with the Incident Handling CD, you might also need to:

- Have an archive of various original installation CDs of the OS you use and various applications.
- Maintain a local archive of various vendor-released security patches.
- Maintain a database of people to contact, their phone numbers, home addresses, etc.

Step 2: Detection and Identification

The incidents of false positives are too high to be taken lightly. Before you go around announcing that the system has been compromised, take some time to make doubly sure. This identification can usually be done on the basis of:

- Strange processes running on the machine under consideration
- Strange files in locations where users do not have write permissions
- `nmap` showing strange open ports on the target machine
- Empty log files or log files with very little information
- New accounts in the `/etc/passwd` file
- Strange files with SUID/SGID bits set

- Files with a varying MD5sum when compared to the originals

If you observe these phenomena, you can be reasonably sure that the system has been compromised. But the absence of these phenomena does not guarantee the security of the system. Many crackers replace the system binaries with their own programs that specifically hide traces of their malicious acts.

A Trojaned version of “ls,” for example, will not show files owned by the cracker; a Trojaned “ps” will not show processes being run by the cracker; a Trojaned ‘login’ will always allow him to log in with a particular username and password, even if such a username/password pair does not exist in the /etc/passwd file. Thus, it is difficult to trust the output of the programs on the compromised machine. That is the reason why we prepared an Incident Handling CD in Step 1. Use the programs from the CD while checking the system.

During the Detection and Identification phase, assign a person with a good understanding of the operating system *and* incident handling to investigate the system. Once you have ascertained that the machine has been compromised, you need to inform the concerned parties. These could be the upper management, your company’s lawyers, your ISP, or even the local law enforcement agency. As cautioned earlier, use a “need-to-know” principle while informing the concerned parties. Of the parties mentioned, your upper management should be the first to know. After informing the concerned parties, move quickly into the next step: Containment and Analysis.

Step 3: Containment and Analysis

Once you have correctly identified the incident as a compromise, the first thing that you should do with the compromised computer is to disconnect it from the network and seal the room where it is placed. Often, “insiders” are involved with such activities and it is important that no unauthorized person has any kind of access to that computer. However, do not reboot the machine, as that will stop quite a few processes that the intruder might have started. If you do not disconnect, the intruders will remain in a position to do considerable damage (remove log files, delete system critical files, etc.)

Analysis involves understanding what vulnerability was used to compromise the system, what information was accessed or modified, and what actions were taken by the cracker after the intrusion.

Start the Analysis part by taking a snapshot of the system. The snapshot includes information about the processes running, the open network connections, users currently logged in, files being written to, and a list of files on the system and their contents. Use the programs from the Incident Handling CD for this.

```
[root@dragonfang root] mount /dev/cdrom /mnt
[root@dragonfang root] /mnt/bin/ps auwx > /home/dhar/
processlist
[root@dragonfang root] /mnt/bin/w > /home/dhar/userlist
```

```
[root@dragonfang root] /mnt/bin/netstat -anlp > /home/dhar/netconn
[root@dragonfang root] /mnt/bin/lsof > /home/dhar/openfiles
[root@dragonfang root] /mnt/bin/ls -latR / > /home/dhar/filelist
```

Next, you can take a systemwide backup of the compromised machine. The programs that can be used to take a backup are `dd`, `tar`, and `dump`. Use `tar` when you want to just save the contents of the files, `dd` when you want to save a disk image along with the file system metadata, and `dump` for a quick intelligent backup. The `dump` program allows you to back up only the files that have changed since the last backup. You can run one of the following commands:

```
[root@dragonfang root] tar -czvf backup.tgz /
[root@dragonfang root] dd if=/dev/hda1 of=/dev/hda2
[root@dragonfang root] dump 0uf /dev/hda2 /dev/hda1
```

Going into the depth of these commands is beyond the scope of this article. Readers are requested to check out the main pages of these commands for additional information.

Once you have taken a backup of your system, you should try and find out the various actions performed by the cracker on the compromised machine. To consolidate their hold on your network or to hide their traces, crackers usually do the following:

Install Sniffers. Sniffers are programs that log and monitor network traffic. An intruder will mostly use a sniffer to capture the usernames and passwords of other machines on your network. To check whether or not a sniffer is running on your system, check to see if your network interface is in a promiscuous mode. If a network interface is in a promiscuous mode, then it is accepting packets meant for other machines. This is a strong indication that a sniffer has been installed on your system. Certain tools that can help detect a promiscuous mode include:

- *ifstatus*: available at http://sunsite.csi.forth.gr/sunsite/net_tools/ifstatus/
- *ifconfig*: available as default on all Linux distros
- *cpm*: available at <ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/cpm>

Install Trojan Programs. According to legend, the Greeks won the Trojan War by hiding in a huge hollow wooden horse to get into the city of Troy. That is exactly what a Trojan horse program is. It is a malicious security-breaking program that hides in something benign. Intruders usually use Trojan horse programs to hide their presence or create backdoors to make future access easier.

A list of common binaries that are replaced by crackers was previously given. One way to discover if a binary has been Trojaned is to match its MD5 checksum against

the MD5 checksum of a known good binary. The MD5 program generates a unique, 128-bit cryptographic message digest value derived from the contents of the file. If as much as a single bit is modified in the file, the MD5 checksum changes. Forgery of a file in such a way that the MD5 checksum remains same is presently considered impossible.

You can also get help from software such as Tripwire. Tripwire is a tool that checks to see what has changed on your system. It monitors the key attributes of a file that should not change (e.g., binary signature, size, date, etc.) You can download Tripwire from <http://www.tripwire.org/downloads/index.php>.

Malicious crackers often replace even the MD5 program with one of their own. As cautioned earlier, you cannot trust the programs on the compromised machine; use the md5sum program from the Incident Handling CD.

Install Backdoors. Backdoors are a system administrator's worst nightmare. They are programs that are designed to hide inside a target host and allow the intruder to access the system without normal authorization or vulnerability exploitation. Backdoors are installed after gaining root access and can be of various types:

- *Hidden SUID/SGID Shells.* On a Linux system, all a malicious attacker has to do is something like this (as root):

```
[root@dragonfang root] cp /bin/bash /usr/doc/newt-0.50.8/vitasta
[root@dragonfang root] chmod 4755 /usr/doc/newt-0.50.8/vistasta
```

Now whenever an ordinary user executes `/usr/doc/newt-0.50.8/vitasta`, he will get a shell with UID of the root. This is a clumsy method and can be detected. If you, as the root, want to locate SUID files, you can do so via the `find` command:

```
[root@dragonfang root] find / -perm 4755 -print
```

This will print a list of files with SUID bit set. Remember that quite a few programs (such as `passwd`, `ping`, etc.) need to have the SUID bit set to work properly. You should be looking for strange, non-system files with the SUID bit set.

- *Changing configuration files.* An intruder can easily add the following lines in `/etc/inetd.conf` and `/etc/services` file:

Entry to the `/etc/inetd.conf` file:

```
backdoor stream tcp nowait root /bin/sh sh -i
```

Entry to the `/etc/services` file:

```
backdoor 34567/tcp
```

After this, the intruder just needs to restart the inet daemon and on telnetting to the target machine on port 34567, he will be presented with the rootshell without being asked for a password or a username. Again, this method is not very sophisticated, as running nmap against this machine from a trusted server will show this suspicious port. In this connection, I would like the readers to check out a program called SAdoor (<http://cmn.list-projects.darklab.org/>), which will not be visible via a normal nmap scan and but gets activated on receiving TCP packets on certain ports in a particular order with particular flags.

- *Rootkits.* A rootkit is a set of programs that provides the crackers with a backdoor into the system, collects information, and masks the fact that the system has been compromised. Rootkits are available for almost all operating systems. A good collection of rootkits is available for study at <http://packetstormsecurity.org/UNIX/penetration/rootkits/>. Out of the ones listed on the page, the ones worth checking out are Knark (<http://packetstormsecurity.org/UNIX/penetration/rootkits/knark-2.4.3.tgz>) and LRK (<http://packetstormsecurity.org/UNIX/penetration/rootkits/lrk5.src.tar.gz>).

Programs such as Knark and LRK are very advanced and discovering them is a very challenging task. Unless the intruder did a poor job of hiding his traces, a rootkit can be almost impossible to detect. Ideally, I would suggest reinstalling the entire OS once you discover a rootkit has been installed on your system.

There are certain automated tools that can help administrators detect rootkits. Chkrootkit is a shell script that checks system binaries for rootkit modifications. It can detect more than 40 rootkits and runs on Linux, BSD, and Solaris. You can obtain it at <http://www.chkrootkit.org/>.

You should also check neighboring machines and see if they were also compromised. It is possible that the cracker might have sniffed the passwords of users and gained root on neighboring machines too.

Step 4: Eradication and Recovery

As a part of the Eradication step, you will need to find out how the system got compromised in the first place. What vulnerability was exploited to gain root access to the system? For this, you will need to search the log files of the compromised machine. Because many crackers delete the log files, you might need to refer to the log files of your router, your firewall, and your intrusion detection system.

You will also need to prevent further intruder access. This can be accomplished by changing the system passwords on the compromised machine and using TCP Wrappers (ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/tcp_wrappers/tcp_wrappers_7.6.tar.gz) or Firewalls (<http://www.netfilter.org/>) to deny access to the machines you suspect belonging to the attacker.

Once you have carried out the steps cited under Eradication, you can begin the Recovery Process. Start by doing a clean reinstall of the operating system. The crackers may have installed backdoors, rootkits, Trojan programs, or hacked Loadable Kernel Modules. It is not easy, even for an expert, to detect all of these. As a result, just patching the vulnerability might not be sufficient.

Take care to apply the latest security patches. You should also try to harden the system to make it immune to such attacks. Disable unnecessary services. Remove SUID bit from programs that do not need it. Use ssh and sftp instead of telnet and ftp.

Quite a few good documents on hardening various operating systems are available on the Net. Consult such documents and try and secure your machine. You can also use automated programs for the hardening process. Bastille-Linux (<http://www.bastille-linux.org>) is one such program for Linux and HP-UX, while Jass (<http://www.sun.com/software/security/jass/>) does the same for Solaris.

Keep in touch. It pays to know the latest vulnerabilities and patch them accordingly. CERT is a good site to visit (<http://www.cert.org>). Periodically review your security. You can do this by either hiring a reputable outside organization or using someone knowledgeable within the organization. Automated vulnerability assessment tools such as Nessus (<http://www.nessus.org>) are also very good at detecting weaknesses in your network's security.

Perform regular checks of your system logs. This is one of the most important, but overlooked, aspects of security. You can use logwatch (<http://www.log-watch.org/>) or swatch (<http://www.oit.ucsb.edu/~eta/swatch/>) to automate this task for you.

On important network segments, install an intrusion detection system. Snort (<http://www.snort.org>), along with a fronted ACID (<http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html>), are excellent tools for detecting various attacks launched against your system.

Install file integrity checking software such as Tripwire or ViperDB (<http://www.resentment.org/projects/viperdb/>). They will alert you when certain key attributes of a file on the system change. Use COPS (<ftp://coast.cs.purdue.edu/pub/tools/unix/cops>) or Tiger (<http://ftp.cdut.edu.cn/pub2/linux/security/tools/tiger/>) for checking the system's security configuration. Run Crack once a month to get a list of bad user passwords.

When you are confident that you have recovered from the attack, you can reconnect the compromised machine to the network.

CONCLUSIONS

In an ideal scenario, your servers might never get compromised. The world, however, is far from ideal. The best thing you can do is to be prepared. Finally, the most important thing you should do is learn from the intrusion. This should help to reduce the possibility of such an intrusion happening again.

Sumit Dhar works with Reliance Infocomm as an information security analyst. In addition to Infosec, his interests include reading, movies, music, and the open source movement. He can be contacted at sumit.dhar@reliance-info.com.