Incident Handling

- There are essentially six basic steps that an incident handler will follow when dealing with a computer security incident.

- We will define the term "**incident**" here as any irregular or adverse event that occurs in a computer system and/or network.

- Examples of possible incident categories include:

  - Unauthorized use of another user's account and privileges (compromise of system integrity)
  - Denial of system resources
  - Unauthorized or illegal access to a system (penetration attempt or an intrusion)
  - Malicious use of system resources, or any kind of damage to a system.
  - Discovery of a virus that has infected a system(s) on your network
  - Discovery of an intruder logged into a system in your network

- We will define an "**event**" here as any observable occurrence in a computer system or network such as:

  - An unfamiliar process running and accumulating a lot of CPU time
  - A pattern of system crashes
  - An IDS reports penetration attempts or scans from a remote site
  - A very high number of packets flooding the network.

- Note that not every event is an incident. An event is something that we occurred because it was directly observed by someone and/or recorded in a log or audit file.

Some Important Considerations

- A computer security incident can occur at anytime of the day or night. Although most hacker/cracker incidents occur during the off hours when hackers do not expect system managers to be around and monitoring their key systems.

- However, worm and virus incidents can occur any time during the day. Thus, time and distance considerations in responding to the incident are very important.

- If the first person on the call list to be notified cannot respond within a reasonable time frame, then the second person must be called in addition to the first. \

- It will be the responsibility of the people on the call list to determine if they can respond within an acceptable time frame.

- The media is also an important consideration. If someone from the media obtains knowledge about a security incident, they will attempt to gather further knowledge from a site currently responding to the incident.

- Providing information to the wrong people could have some very undesirable side effects. In fact, publicizing the incident and damaging the company's reputation may very well have been the attackers intent in the first place.

General Procedures

- Always keep a detailed logbook. Logging of information is critical in situations that may eventually involve law enforcement authorities and the possibility of a criminal trial.

- The implications from each security incident are not always known at the beginning of, or even during the course of an incident.

- Therefore, a written log should be kept for all security incidents that are under investigation.

- It is imperative that the information be logged in a location that cannot be altered by anyone else.

- Manually written logs are preferable since on-line logs can be altered or deleted. Examples of the types of information that should be logged are:

- Dates and times of incident-related phone calls.
- Dates and times when incident-related events were discovered or occurred.
- Amount of time spent working on incident-related tasks.
- People you have contacted or have contacted you during the course of the incident.
- Names of systems, programs or networks that have been affected.

The Emergency Action Plan

- Without an emergency action plan that has been developed ahead of time and understood by every member of the response team, the situation will degenerate into chaos and valuable evidence and time will be lost.

- Stay calm and do not rush through the incident. One good way of staying calm and forcing yourself to move slowly and deliberately is to take notes and examine logs.

- Take detailed notes as you go through each compromised system on the network. Always keep in mind that those notes may be examined as evidence in a court of law.

- Key items to consider during the note-taking process are: **Who**, **What**, **When** and **Where**. As you collect more evidence you can consider: **How** and **Why**.

- Notify the organization’s security office or coordinator and your immediate manager to get assistance in the incident handling process.

- Enforce a “**need to know**” policy. The main reason for this was mentioned earlier. Another important consideration is that many incidents turn out to be a mistake made by an individual. Publicizing this will cause mistrust within the organization.

- Another important consideration for this policy is to minimize the chances of alerting the attacker to the fact that an investigation is underway.

- Use means of communication (telephone and faxes) other than email and other network based communication.

- Keep in mind that inference is a strong tool in incident handling. A flurry of email (even encrypted) indicates incidents and investigations.

- Contain the problem by disconnecting the compromised systems from the network and make backup copies of the affected drives as soon as possible.

- Make backups of system information as well as file-system information. Process tables, network connections, the /tmp directory and other volatile data sources should be dumped to files and then backed up with the rest of the file-system.

- Make multiple full backups using at least two different methods. Ensure file-system integrity with the first method and analytical portability with the second method.

- The ***ufsdump*** and ***tar*** commands are good examples of each. However, any executables employed in the incident handling process should be trusted software.

- Kill all active processes activated by the attacker and remove any files or programs that she may have left on the system.

- Change passwords for any accounts that were accessed by the attacker. At this stage, the attacker should be locked out of the system.

- Get back in business as soon as possible. Learn from the experience and ensure that all deficiencies that allowed this incident to take place are addressed and eliminated (until the next time).

Incident Handling Phases

- The steps involved in handling a security incident are categorized into six stages:

- Preparation
- Identification of the problem
- Containment of the problem
- Eradication of the problem
- Recovering from the incident
- Follow-up analysis.

Preparation

- Establish clear policies on computer usage and network access. Then make sure these are enforced.

- Any policy that is established and approved must be developed on the presumption of privacy.

- Establish a policy for dealing with incidents that involve remote computers and networks used by employees and those involving outside contractors.

- Establish a policy for Intranet and Internet monitoring.

- Select and put into place an incident handling team that is made up of qualified individuals.

- Develop an emergency communications plan. Make sure every member of the team has a copy of an incident notification call list.

- Develop interfaces with law enforcement agencies and Computer Incident Response Teams (CIRTs).

- Finally set up planning/training meetings on scenarios (war games) to familiarize team members with tools and techniques.

- Prepare and acquire an incident response toolkit:
- Small tape recorder
- Binary backup – Ghost or more expensive tools such as “Image MASSter”.
- Forensic Software (Coroners Toolkit or EnCase)
- Backup Media
- CD’s with binaries
- Windows Resource Kits
- Hub or switch
- A laptop with dual OS (Windows and Linux).
- Call list and phone book.
- Cell phone and pager.
- Variety of cables and cords.

- You should always have a set of key utilities that are guaranteed to be clean and without defect on a CD.

- Ensure that you have clean copies of at least ls, ps, find, netstat, ifconfig, df, du, tar, rm, mv, cp, chown, chgrp, chmod, gzip/gunzip family and dd. Additionally, top can be really valuable.

Identification

- The focus here is to identify and contain the incident.

- The bulk of the information alerting us to an incident will be information provided by a network sensor or IDS.

- However users within the organization can also provide useful information that can be correlated with sensor logs and alerts. Ensure users know who to report unusual events to and how to report them.

- Designate a highly qualified individual to be responsible for the incident who is available to help you respond to and investigate the incident.

- The first thing that must be done is to determine whether or not the event is actually a security incident.

- Unfortunately, most Unix Rootkits provide versions of system commands that work to hide any sign of system compromise.

- Key system monitoring programs are usually replaced because of the important role that they play in forensic investigation.

- This is why it is crucial that only the binaries from the response toolkit CD be used to investigate a suspected incident.

- Examine the **syslog** files, process table and file system to see if there are any odd and unexplainable messages, processes, or files. Monitor the system for any activity that includes:
- Two xinetd processes

- ssh running as EUID root but not as UID root
- Core files for RPC services (or any other inetd-started services) in /
- New setuid/setgid programs
- Files that are quickly growing in size
- df output that does not closely match du output
- perfmeter/top/BMC Patrol/SNMP monitors not matching vmstat/ps output
- Higher than normal inbound or outbound network traffic and unexpected bound network ports that appear in lsof or netstat output.

- Be careful to maintain a provable chain of custody by getting the company lawyer or legal department involved. At the very least the following must be done:
- Identify every piece of evidence with a witness.
- Sign, seal and date a copy of everything.
- Place everything in a tamper-proof locked place that only a very limited number of people have access to (and be able to prove only a limited number of people have access).
- Sign, seal and date a copy of everything.
- Be prepared to show how you were logging things before and after the compromise. Make sure you examine log files periodically and monitor system activity.

- It is essential that your ISP be notified of the incident as soon as it is validated. The ISP can block incoming and outgoing traffic and trace the source.

- They can go through the proper procedures for an electronic wiretap if needed. They can help identify the source(s). They can contact other ISPs that might be involved.

- Provide them with as much information as you can. Dates, times, IP addresses, MAC addresses, patterns, messages, etc.

- Ensure that Network/System Security Officer at your site has been notified. Then contact the local law enforcement office and see if there is a person assigned to a Computer Crime section.

- If law enforcement is involved from the beginning, there may be a better chance of keeping a provable chain of custody.

- The people contacted may be aware of other incidents similar to yours that will help in your efforts to contain and eradicate the problem.

- In addition they will be able to provide the proper guidance as to what's proper and what's not in an ongoing investigation.

Containment

- Deploy a small on-site team to survey the situation. The team should work to keep a low profile and when possible, avoid the disruption of normal routines.

- As always they should take copious notes so that nothing is left to memory in court.

- The first thing the on-site team should do is interview the person that discovered the intrusion and the incident handler.

- The on-site team will need to know how the intrusion was discovered, what has been done so far, how widespread the intrusion is and who has been contacted (or who else knows about the intrusion).

- The more information the incident handler can give the on-site team, the better the on-site team will be able to deal with the intrusion and determine where to begin.

- Time is of the essence so it is essential that the on-site team doesn’t duplicate the work that the incident handler has done.

- Once the on-site team has assessed the situation, they should be able to make an educated guess about the direction to proceed.

- It is especially important to keep a low "electronic" profile. Resist the natural urge to start tracking the perpetrators using ping, finger, traceroute or whois in order to gather information about the source of an attack.

- Do not scan the IP address with **nmap** or other such scanners because they will be monitoring for this kind of activity and will know that their compromise has been discovered.

- If multiple systems from your site are attacking other sites, deploy an egress filter to stop that traffic at the firewall.

- It is a very bad idea to immediately get on the system in question and blindly start typing commands, simply because any of the system binaries could be compromised.

- Instead use the CD with the useful monitoring utilities discussed earlier. Make sure that you use these binaries instead of the binaries on the compromised machine(s).

- Don't copy binaries from other machines unless you are absolutely *certain* they have not been trojaned or compromised.

- After the system has been disconnected from the network, take a snapshot of the current system activity.

- Perform this activity by mounting the toolkit CD that was created earlier and only using commands from there.

- First, run the ***ps*** command with options to get a full listing, including the parent process id of each process. Send the command's output to a file:

  ```
  ps –auxw > snapshot.txt
  ```

- Next, use the ***netstat*** command (or the equivalent on the system) with the options to report all open connections and not to do lookups of numbers to names:

  ```
  netstat –anp –ip > connections.txt
  ```

- Remember to backup the /tmp directory. This directory is usually cleared when the system boots up.

- At this point the system can be halted and you can proceed to the main interest, which is recovering control of the system with as little additional damage as possible.

- There are three archival commands that are very useful in this step: ***tar***, ***dump***, and ***dd***.

- Each is suited for different types of backups. Combined they form a versatile toolkit for performing backups.

- The three primary functions of tar are to create an archive, extract files from the archive, and generate a table of contents for a tar file. It is simple to use, and ideal for backing up only a particular directory tree or a list of files.

- To create tar file:

```
tar -cvf archive file
```

- Extract tar file

```
tar -xvf archive file
```

- List contents of tar archive

```
tar -tvf archive file
```

- Copy current directory to another

```
tar cpf - . | ( cd newdir; tar xvpf - )
```

- Where "**archive**" is a file or device, and "**file**" is the file or directory to archive.

- The ***dump*** utility provides the option to archive either an entire file-system, or only the files that have been changed since a previous dump.

- A full **dump** should be run after an upgrade or re-install of the operating system. This is because dates on files represent when the files were "mastered", not actually copied to your system.

- Dump accesses the raw device that typically is readable only by root, so non-privileged users cannot run it (without use of sudo, or set UID script

- A level 0 dump captures an entire file system. Incremental dumps (levels 1-9) record files modified since a dump of lower level.

- Dump uses the /etc/dumpdates file to record what level dump was done on which file system and when. Dump also keeps track of the amount of media used.

- **The simplest form of the dump command is *dump*, *dump level*, *u* (update dumpdates file) *f* (device name) and the file system to dump.**

- **The last parameter may be specified as mount point like */usr* or a disk device name: /dev/sda0.**

- **The following example is a full dump of the */usr* file system:**

# dump 0uf /dev/cdrom /usr

- The ***dd*** utility reads input files block by block. If you specify a disk device, you can capture file system metadata, blocks of "data" marked deleted that could be useful for evidence gathering following a break in.

- This data would be missed if using only ***tar*** or ***dump,*** which rely on the UNIX file system.

- The input file for ***dd*** can be a storage device or disk device name. This enables you to make disk-to-disk copies without having to unpack the archive.

- To image copy of a file system

dd if=/dev/sda0 of=/dev/cdrom

- CD to CD copy

dd if=/dev/cdrom of=/dev/cdrw

- Depending on the data already collected, the consensus might be to leave the machine as is for a short while to collect more data or possibly trace the attack.

- The team should be aware that they must take into consideration other systems on the same subnet and other trusted systems that regularly connect to the affected machine before making this decision.

- Check neighboring systems and trust Relationships to determine who mounts (or exports) files via NFS.

- Also check entries in their .rhosts, .shosts, or hosts.equiv. Typically an attackers will not compromise just one computer, they hop from host to host, and attempt to hide their tracks while creating as many potential back doors as possible.

- If the intruders compromised the root account or if the system does not use a shadowed password structure, then all users must be required to change their passwords. The root password should be changed in any case.

Eradication

- This is the most difficult issue in the incident handling process because it involves complete, safe and total removal of any backdoors and malicious code.

- The following are the basic steps in this phase.

- Determine the cause and symptoms of the incident using data collected in the previous phases.

- Improve the defenses by deploying firewalls and gateway filters and changing the system name and IP address.

- Perform system and network vulnerability analysis to detect any related vulnerabilities.

- Remove the cause of the incident.

- Locate the most recent clean backup and load a copy on the system.

Recovery

- Restore the system from backups, making certain that you are not restoring compromised code.

- Then, if possible apply all patches to the system before putting it back in service. Keep in mind that the intruders got into the system somehow and you want to close as many of the holes as you can so that they don't come directly back in.

- The next step is to validate the system by verifying that the operation was successful and the system is back to its normal condition.

- Use a network-monitoring tool to watch the traffic to the system once it is back up. The idea is to monitor for back door activity that may have escaped detection.

Follow-Up

- Start on a follow-up report as soon as possible. Obtain data from a detailed forensic analysis from the compromised system(s).

- Conduct a “lessons learned” meeting and generate a set of recommended changes to management.

- **Implement the approved changes.**