■ A physical access to the suspicious system should be given to the forensic investigator. Physical access is preferred to remote access, since the hacker could detect the investigations done on the system (by using a network sniffer for example).

■ A physical copy of the hard-disk might be necessary for forensic and evidence purposes. Finally, if needed, a physical access could be needed to disconnect the suspected machine from any network.

■ A good knowledge of the usual network activity of the machine/server is needed. You should have a file on a secure place describing the usual port activity, to compare efficiently to the current state.

■ A good knowledge of the usual services running on the machine can be very helpful. Don't hesitate to ask a Windows Expert for his assistance, when applicable. A good idea is also to have a map of all services/running process of the machine.

It can be a real advantage to work in a huge corporate environment, where all user machines are the same, installed from a master CD. Have a map of all processes/services/applications. On such environment where users are not allowed to install software, consider any additional process/service/application as suspicious.

The more you know the machine in its clean state, the more chances you have to detect any fraudulent activity running from it.

Please note that the **Sysinternals** Troubleshooting Utilities can be used to perform most of these tasks.

■ **Unusual Accounts**
Look for unusual accounts created, especially in the Administrators group:
C:\> *lusrmgr.msc*
or
C:\> *net localgroup administrators* or *net localgroup administrateurs*

■ **Unusual Files**
- Look for unusually big files on the storage support, bigger than 5MB. (can be an indication of a system compromised for illegal content storage)
- Look for unusual files added recently in system folders, especially C:\WINDOWS\system32.
- Look for files using the "hidden" attribute:
C:\> *dir /S /A:H*
  - Use "*windirstat*" if possible.
  -

■ **Unusual Registry Entries**
Look for unusual programs launched at boot time in the Windows registry, especially:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
Use "*HiJackThis*" if possible. (Also have a look in your Startup folder)

■ **Unusual Processes and Services**
Check all running processes for unusual/unknown entries, especially processes with username "SYSTEM" and "ADMINISTRATOR":
C:\> *taskmgr.exe*
(or *tlisk*, *tasklist* depending on Windows release)
Use "*psexplorer*" if possible.

■ **Check user's autostart folders**
C:\Documents and Settings\user\Start Menu\Programs\Startup
C:\WinNT\Profiles\user\Start Menu\Programs\Startup

■ **Look for unusual/unexpected network services installed and started**
C:\> *services.msc*
C:\> *net start*

■ **Unusual Network Activity**
- Check for file shares and verify each one is linked to a normal activity:
C:\> *net view \\127.0.0.1*
Use "*tcpview*" if possible.

- Look at the opened sessions on the machine:
C:\> *net session*

- Have a look at the sessions the machine has opened with other systems:
C:\> *net use*

- Check for any suspicious Netbios connexion:
C:\> *nbtstat –S*

- Look for any suspicious activity on the system's ports :
C:\> *netstat –na 5*
(5 makes it being refreshed each 5 seconds)
Use –o flag for Windows XP/2003 to see the owner of each process:
C:\> *netstat –nao 5*
Use *"fport"* if possible.

■ **Unusual Automated Tasks**
Look at the list of scheduled tasks for any unusual entry:
C:\> *at*
On Windows 2003/XP: C:\> *schtasks*

■ **Unusual Log Entries**
Watch your log files for unusual entries:
C:\> *eventvwr.msc*
If possible, use "*Event Log Viewer*" or such tool

Search for events affecting the firewall, the antivirus, the file protection, or any suspicious new service.

Look for a huge amount of failed login attempts or locked out accounts.

Watch your firewall (if any) log files for suspect activity.

■ **Rootkit check**
Run "*Rootkit Revealer*", "*Rootkit Hooker*", "*Ice Sword*", "*Rk Detector*", "*SysInspector*", "*Rootkit Buster*".

It's always better to run several of these tools than only one.

■ **Malware check**
Run at least one anti-virus product on the whole disk. If possible use several anti-virus. The anti-virus must absolutely be up-to-date.

Containment　　3

If the machine is considered critical for your company's business activity and can't be disconnected, backup all important data in case the hacker notices you're investigating and starts deleting files. Also make a copy of the system's memory for further analysis. (use tools such as Memoryze,win32dd etc.)

If the machine is not considered critical for your company and can be disconnected, shut the machine down the hard way, removing its power plug. If it is a laptop with a battery on, just push the "off" button for some seconds until the computer switches off.

Offline investigations should be started right away if the live analysis didn't give any result, but the system should still be considered compromised.

Make a physical copy (bit by bit) of the whole hard disk on an external storage support, using *EnCase, X-Ways,* or similar forensic tool (*dd, ddrescue* etc.).

Try to find evidences of every action of the hacker:

- ■ **Find all files used by the attacker**, including deleted files (use your forensic tools) and see what has been done with it or at least their functionality, in order to evaluate the threat.
- ■ **Check all files accessed recently**.
- ■ Inspect network shares to see if the malware has spread through it.
- ■ More generally, try to **find how the attacker got into the system**. All leads should be considered. If no computer proof of the intrusion is found, never forget it could come from a physical access or a complicity/stealing of information from an employee.
- ■ Apply fixes when applicable (operating system and applications), in case the attacker used a known vulnerability.

Remediation　　4

In case the system has been compromised:

- ■ Temporary remove all accesses to the accounts involved in the incident.
- ■ Remove all malicious files installed by the attacker.

Recovery　　5

No matter how far the hacker has gone into the system and the knowledge you might have about the compromission, as long as the system has been penetrated, the best practice is **to reinstall the system fully from original media and apply all fixes to the newly installed system.**

In case this solution can't be applied, you should:

- ■ **Change all the system's accounts passwords**, and make your users do so in a secure way: they should use passwords with upper/lower case, special characters, numbers, and at least be 8 characters long.

- ■ **Restore all files** that could have been changed (Example: *svchost.exe*) by the attacker.
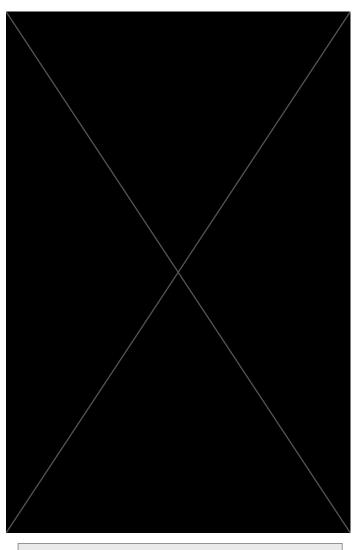
Aftermath　　6

Report

A crisis report should be written and made available to all of the actors of the crisis management cell.

The following themes should be described:

- ■ Initial detection
- ■ Actions and timelines of every important event
- ■ What went right
- ■ What went wrong
- ■ Incident cost

Capitalize

Actions to improve the Windows intrusion detection management processes should be defined to capitalize on this experience.

Incident handling steps

6 steps are defined to handle security Incidents

- ■ **Preparation: get ready to handle the incident**
- ■ **Identification: detect the incident**
- ■ **Containment: limit the impact of the incident**
- ■ **Remediation: remove the threat**
- ■ **Recovery: recover to a normal stage**
- ■ **Aftermath: draw up and improve the process**

IRM provides detailed information for each step.