

Computer Forensics

Sikkerhedsforum.dk 2002

© 2002 KPMG

cj@computerforensics.dk

2 helt forskellige ting...!

”Computer Forensics” og ”Incident Response”

Computer forensics

1. "Search and seizure" – beslaglæggelse af elektronisk bevismateriale
2. Detaljeret gennemgang af data

Meget detaljeret tilgang, hovedformål = retsforfølgelse

Incident Investigation

Hovedformål at genoprette BUSINESS FUNCTIONS

- **Undermål at finde ud af hvad der er sket (hvor og hvordan angriber kom ind i systemet).**

Forensics

Tankegang:

**Alt hvad man gør skal senere kunne forklares i retten
= bevar beviser**

**Temp filer/swap filer, ændre access tider ved at kikke
på filer, overskrive slettede filer**

Step 1 – sikre bevismateriale

Do ***NOT*** touch the keyboard or the computer yet unless you absolutely have to.

We repeat. Do ***NOT*** touch the keyboard or the computer yet.

Did you hear us? **STAY AWAY FROM THE COMPUTER!** Anything you do will destroy evidence, so simply don't touch it for now, or do as little as possible and don't start looking for damage yet.

Step 1 – sikre bevismateriale

1. Ødelæg ikke bevismateriale
2. Dokumenter alt hvad du gør
3. Eksekver ikke programmer direkte på host
4. Backup - sluk ikke før data i midlertidig hukommelse er gemt
5. Opbevar backup, logfiler, dokumentation osv sikkert

Step 2 - analyse

Systematisk eftersøgning + analyse af data

- dokumenterer og fremlægge

Sikkerhedspolitikker/procedurer

Hvad skal en bruger gøre – og hvad med administratoren?

**Tilbage til starten: 1.spørgsmål
”Computer Forensics” eller ”Incident Response”**

Hvor lang tid tager det?

”bekræfter, at webstedet blev lagt ned af hackere igen først på ugen.

- Jeg mener, at vi var i drift igen i løbet af en halv time, siger han.

Direkte adspurgt om, hvad han synes om sikkerheden på webstedet, når det bliver hacket igen og igen, svarer kommunikationschefen:

- Vi opdager det, vi retter det. Det går hurtigt, og sådan er det.”

Hvor lang tid tager det?

ACTION

EXPERTISE REQUIRED

TIME CONSUMED

Go back to work

None

Almost none

Minimal effort

Installing system software

1/2 - 1 day

Minimum Recommended

Jr. system administrator

1-2 days+

Serious effort

Sr. SA

2+ days - weeks

Fanaticism

Expert SA

days - months+

**Honeynet: gennemsnit 48 timer
(fra 10 – 104)**

Spild af tid?

”De fleste ved ikke hvordan data der kommer tilbage skal fortolkes” – mangel på tid/mangel på viden...

Tilkalde specialister?

Windows Tools (step 1)

(Step 1)

Mål: Nok information til at finde ud af om noget er sket - på en måde der kan bringes for retten om nødvendigt.

Ikke så meget fokus på hvad der er sket

Windows Tools – live demo

Microsoft: netstat

Windows Tools – live demo

Foundstone: fport

Windows Tools – live demo

Sysinternals: listdlls
handle
pslist

Tool kits – live demo

procdmp.pl: H. Carvey, keydet89@yahoo.com
<http://patriot.net/~carvdawg/>

350 KB -> HTML-fil:

Microsoft:	netstat
Foundstone:	fport
Sysinternals:	listdlls
	handle
	pslist

Tool kits – live demo

FRED.bat: "First Responder's Evidence Disk"

Air Force Office of Special Investigations

800 KB → txt-fil:

Foundstone: fport

Microsoft: Netstat, arp, net, nbtstat, route, cmd.exe

Sysinternals: listdlls

handle

pslist

psinfo

psloggedon

?:

MD5sum.exe

Tool kits – live demo

ircr.exe: "Incident Response Collection Report"

<http://www.incident-response.org/IRCR.htm>

(3 MB .exe fil -> HTML-fil):

memory dumper

Eventlog, securitylog, systemlog, applicationlog

Dir, hidden files

Registry checks (startup, info)

Microsoft: net, arp

md5sum

Andre tools

Ntsecurity.nu

PromiscDetect checks if your network adapter(s) is running in promiscuous mode, which may be a sign that you have a sniffer running on your computer.

Ntsecurity.nu

ListModules lists the modules (EXE's and DLL's) that are loaded into a process.

(som listdlls fra sysinternals, men færre detaljer)

**ListModules 1.1 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- <http://ntsecurity.nu/toolbox/listmodules/>**

Loadad modules in process number 488:

- C:\WINNT\System32\cmd.exe**
- C:\WINNT\System32\ntdll.dll**
- C:\WINNT\system32\KERNEL32.dll**
- C:\WINNT\system32\USER32.dll**
- C:\WINNT\system32\GDI32.dll**
- C:\WINNT\system32\ADVAPI32.dll**
- C:\WINNT\system32\RPCRT4.DLL**
- C:\WINNT\system32\MSVCRT.dll**
- C:\WINNT\System32\IMM32.DLL**

ListDLLs V2.23 - DLL lister for Win9x/NT
Copyright (C) 1997-2000 Mark Russinovich
<http://www.sysinternals.com>

CMD.EXE pid: 488

Command line: "C:\WINNT\System32\cmd.exe"

Base	Size	Version	Path
0x4ad00000	0x48000	5.00.2195.4803	C:\WINNT\System32\cmd.exe
0x77f80000	0x7b000	5.00.2195.5400	C:\WINNT\System32\ntdll.dll
0x77e80000	0xb6000	5.00.2195.5400	C:\WINNT\system32\KERNEL32.dll
0x77e10000	0x5f000	5.00.2195.5931	C:\WINNT\system32\USER32.dll
0x77f40000	0x39000	5.00.2195.5907	C:\WINNT\system32\GDI32.dll
0x77db0000	0x5d000	5.00.2195.5385	C:\WINNT\system32\ADVAPI32.dll
0x77d30000	0x71000	5.00.2195.5419	C:\WINNT\system32\RPCRT4.DLL
0x78000000	0x46000	6.01.9359.0000	C:\WINNT\system32\MSVCRT.dll
0x75e60000	0x1a000	5.00.2195.4314	C:\WINNT\System32\IMM32.DLL

Sysinternals

Autoruns shows what programs are configured to run during system bootup or login. These programs include ones in the startup folder, Run, RunOnce, and other Registry keys.

<http://unxutils.sourceforge.net/>

Pclip.exe, from the UnxUtils.zip archive, sends the contents of the clipboard to STDOUT

<http://unxutils.sourceforge.net/>

**”grep” og andre tools – specielt hvis vant til dem
(ikke ”strings” ...)**

WIN-dd + NetCat/CryptCat

```
c:\>cc -L -p 7070 > c:\securedata\netstat.log
```

```
E:\>netstat -an | cc 192.168.0.1 7070
```

Sender output fra "netstat -an" kommando fra CD-ROM drevet på "victim" system til forensics workstation:

Forensic Acquisition Utilities

<http://users.erols.com/gmgarner/forensics/>

Imaging a 40 GB hard drive using conventional methods (e.g. the standard versions of dd, md5sum and netcat on Linux) may take 6 hours or more, particularly if the output of dd is piped to gzip before being piped to netcat, as is a common practice.

Six hours is a long time when responding to an incident and a significant cost factor in terms of lost productivity and labor at current hourly rates for incident response personnel.

Forensic Acquisition Utilities

<http://users.erols.com/gmgarner/forensics/>

1. **dd.exe:** A modified version of the popular GNU dd utility program
2. **md5lib.dll:** A modified version of Ulrich Drepper's MD5 checksum implementation in Windows DLL format.
3. **md5sum.exe:** A modified version of Ulrich Drepper's MD5sum utility.
4. **Volume_dump.exe:** An original utility to dump volume information
5. **wipe.exe:** An original utility to sterilize media prior to forensic duplication.
6. **zlibU.dll:** A modified version of Jean-loup Gailly and Mark Adler's zlib library based on zlib-1.1.4.
7. **nc.exe:** A modified version of the netcat utility by Hobbit.
8. **getopt.dll:** An implementation of the POSIX getopt function in a Windows DLL format.

Biatchux

(F.I.R.E, the Forensic and Incident Response Environment)

biatchux distribution of dd incorporates md5 checksums into the imaging process.

forensic analysis, incident response, data recovery, virus scanning and vulnerability assessment.

Also capable of providing necessary tools for live forensics/analysis, just mount the cdrom on your choice of OS win32, sparc solaris and x86 linux trusted static binaries are available in /statbins.

Ntsecurity.nu

macMatch lets you search for files by their last write, last access or creation time without changing any of these times.

Carvdawg (Keydet89)

MAC.pl collects MAC times and owner from files in a directory from NT/2K systems for opening in Excel.