ZAJIŠTĚNÍ DAT PRO FORENZNÍ ANALÝZU

Národní úřad
pro kybernetickou
a informační bezpečnost

Používejte externí úložiště pro spouštění nástrojů k akvizici dat i pro ukládání získaných souborů. Omezí se tak vykonané zápisy na interní úložiště a tím předejdete přepsání informace v nealokovaných blocích. Použijte vhodný souborový systém uložiště (FAT32 neumožňuje vytvářet soubory větší než 4 GB).

Společně se získanými soubory předávejte i následující informace:
- Seznam dokumentovaných uživatelů systému a jejich oprávnění
- Čas zajištění a hash všech souborů
- Nástroje použité k akvizici
- Identifikátory externího úložiště (výrobce, jméno svazku a jeho mapování v systému)

Pokud je počítač vypnutý, postupujte dle pokynů v sekci vypnutý počítač.

LINUX

PAMĚŤ RAM

LIME (https://github.com/504ensicsLabs/LiME)

Obraz paměti je možné vytvořit pomocí modulu jádra LiME. Ve chvíli, kde je tento modul nahrán do jádra, uloží obraz paměti do zvoleného souboru nebo přenese obraz po síti připojením ke specifikovanému TCP portu.

Stažení, kompilace a zavedení do jádra
- `git clone https://github.com/504ensicsLabs/LiME.git`
- `cd LiME`
- `make`

Zápis obrazu paměti RAM do souboru
- sudo insmod lime-*.ko "path=/out/memory.img format=lime"
- sudo rmmod lime (odebrání modulu z jádra)

Přenos po síti
- `sudo insmod lime-*.ko "path=tcp:4444 format=lime"`
- Na jiném stroji je možné tento obraz uložit do souboru
  - `nc <IP> 4444 > memory.img`
    `<IP>` je IP adresa stroje, ze kterého je zajišťován obraz
    Netcat posílá data nešifrovaným kanálem
- `sudo rmmod lime` (odebrání modulu z jádra)

DISK

Pro vytvoření obrazu disku stroje je nejprve potřeba zjistit, které zařízení v `/dev` odpovídá kterému disku.
To je možné provést pomocí příkazů `df -Th` nebo `fdisk -l`. Typicky se jedná o první disk, například `/dev/sda`.

DD

Nejpoužívanější nástroj pro vytvoření obrazu disku je program dd.
Tento program je součástí GNU Coreutils a měl by tedy být dostupný v základní instalaci většiny distribucí.
- `sudo dd if=/dev/sda of=/out/disk.img status=progress conv=sync,noerror`

Volba `status=progress` slouží k zobrazení aktuálního postupu. Tato volba je dostupná v dd od verze 8.24.
Další možností jak zobrazit postup dd je pomocí příkazu kill.
- `sudo kill -USR1 $(pgrep ^dd)`

Vytvoření hashe získaných dat
- `sha512sum /out/disk.img > /out/disk.sha512`

Při použití šifrování předejte také klíče pro obnovení.

VIRTUÁLNÍ PROSTŘEDÍ

VMWARE

PAMĚŤ RAM

Obsah souboru VMEM běžícího virtuálního stroje je obraz jeho paměti RAM. Stačí zkopírovat tento soubor.

INTERNÍ ÚLOŽIŠTĚ

VMware typicky používá formát VMDK pro uchování interního úložiště. Pro analýzu ve většině případů stačí poskytnout VMDK soubor. Pokud je disk rozdělen, je nutné dodat všechny soubory, ze kterých se úložiště skládá.

CHYTRÉ TELEFONY A JINÁ MOBILNÍ ZAŘÍZENÍ

Chytré telefony a jiná mobilní zařízení mají na rozdíl od běžných počítačů velmi různorodý hardware i operační systémy a navíc není možné jednoduše vytvořit obraz úložiště dat bez přímého připojení k jinému zařízení. Z těchto důvodů je uvedena pouze sada "best-practice" doporučení, jak podezřelé zařízení bezpečně zajistit pro transport a následnou forenzní analýzu.

- Sepsat jaké předcházející akce vedly k tomuto incidentu.
- Uvést zařízení do režimu "letadlo" a zkontrolovat, že je Wi-Fi vypnutá.
- Zkontrolovat, zda je baterie zařízení dobita alespoň na 50%.
  (V opačné případě dobijte zařízení jedině připojením do zásuvky, nikoli přes USB připojené k PC, či jinému zařízení!)
- Přelepte neprůsvitnou páskou všechny kamery a mikrofony.
- Pokud je k dispozici, vložte zařízení navíc do stíněného nepropustného pouzdra.

Takto zajištěné zařízení předejte k analýze.

VYPNUTÝ POČÍTAČ

Vypnutý **počítač nezapínejte.** Pokud je to možné, vyjměte a předejte celé interní úložiště.
V opačném případě připojte disk pouze pro čtení a vytvořte obraz disku pomocí nástrojů FTK Imager nebo dd. Při použití šifrování předejte také klíče pro obnovení.