Uzimanje slike sustava (image)

Nakon skupljanja promjenjivih podataka, može se uzeti slika hard drive-a.

Spajanje računala

Forenzičko računalo (računalo F) se pomoću crossover ili ethernet kabla spoji na istraživano računalo (računalo X) te se oba računala smjeste u istu podmrežu. Da bi mogli međusobno komunicirati, moraju biti na istom mrežnom segmentu. Dobra praksa je koristiti 10.0.0.1 za računalo X, a 10.0.0.2 za računalo F.
U komandim linijama oba računala upisati slijedeće naredbe:

```
$ ifdown eth0 (ili koji se već adapter koristi)
$ ifconfig eth0 10.0.0.n netmask 255.255.255.0 (n = 1 za računalo X, 2 za računalo F)
$ ifup eth0
```

Nakon postavljanja IP adresa, treba provjeriti da se računala mogu pingati. Također, računalo X mora biti isključeno iz svoje standardne mreže (npr. tvrtkina mreža) i biti umreženo jedino s forenzičkim računalom. U slučaju kad to nije moguće, potrebno je obavijestiti klijenta da će slika sustava biti iskrivljena i da zbog toga eventualne parnice neće biti moguće.

Mounting diskova

U savršenom svijetu, drive čija se slika uzima bi se zvao `/dev/hda1`, ali s obzirom da to nije slučaj, drive će se morati ručno potvrditi. Općenito se boot sektor nalazi u `/dev/hda`, a datotečni sustav (eng. *filesystem*) u `/dev/hda1`. Ako je drive SCSI, umjesto `hda` će biti `sda`.
Zadavanjem naredbe `mount`, ispisati će se svi mountani uređaji, uključujući i novostvorenu točku za mountanje. Ovi podaci se mogu pogledati i u dnevniku poruka u `/etc/mtab` te u `/proc/partitions`.

Prije uzimanja slike potrebno je proći pripremne korake:

- Na računalu X stvoriti mount točku prema računalu F.
- Na računalu F stvoriti mapu u koju će se pohraniti `dd` slika računala X. To će biti ranije mountani vanjski drive, a put bi trebao izgledati slično ovome: `/media/disk/IBM/customer_host`.
- Na računalu F pokrenuti NFS (eng. *Network File System*)
  UNDER CONSTRUCTION
- Nakon što je stvorena i provjerena mount točka, provjeriti vezu:
  - ući (`cd`) u direktorij,

    - provjeriti vezu, npr. stvaranjem datoteke: `$ touch foo`,
    - provjeriti da se datoteka može vidjeti s oba računala,
    - izbrisati datoteku: `$ rm -rf foo`.
- Provjeriti cjelovitost slike računanjem MD5 sažetka na računalu X: `$ md5sum /dev/hda > outfile`. Nakon toga poslati sažetak na računalo F putem mount točke.

Za raspravu nakon što saznam kako koristiti Sambu

On the forensic machine, start the Network File System (NFS) service: Service nfs start (this may vary from each system, .e.g /etc/init.d/nfs start) On the forensic system, export your share: vi /etc/exports Shift I (for insert mode) Add your mount point, in this example, /media/disk/IBM/customer_host ESC (exit current command selection), Shift : (exit edit mode), W (write), Q (quit),!(absolute write) www.syngress.com 58 Chapter 3 • Live Response: Data Collection On the forensic system, validate your share is being exported: showmount -e On the target system, mount the forensic share point: mount –t nfs 10.0.0.1:/media/disk/IBM/customer_host (target directory) /mnt/foo (local directory) Verify your NFS mount point on the TARGET system: mount An entry should now be seen at the bottom of the mount list which looks something like this: 10.0.0.1:/media/disk/IBM/customer_host on /mnt/foo type nfs (rw,addr=10.0.0.1) This may fail for several reasons, the most common of which are desktop fire- walls, improper eth0 configurations, bad media (i.e., a bad cable), or the NFS service needs to be restarted. If that is the case, attempt to unmount your NFS share, restart the NFS service, and try mounting it again. If for any reason this second mount fails, move on to the next method of acquisition.The role of a forensic investigator is to gather data, not troubleshoot OS problems. Make a note of the failure in the case logbook, and follow up later in a laboratory environment.

Uzimanje slike

- **Naredba**
  Na računalu X upisati naredbu:
  `$ dd if=/dev/hda1 (u savršenom slučaju) of=/mnt/foo`

  Ova naredba će započeti `disk dump` proces, uzimajući `/dev/hda1` i pohranjujući ga u jednu dd datoteku u direktoriju `/mnt/foo` na lokalnom sustavu što je zapravo NFS mount točka za računalo F.

- **Provjera napretka**
  Tijekom izvođenja naredbe, može se provjeriti napredak s naredbom `ls -la` na datoteci. Veličina bloka će kontinuirano rasti te će stati kad dosegne veličinu drivea čija se slika uzima. `If it does, KILL the dd image on the TARGET SYSTEM by pressing Ctrl-C.` (Kad dosegne tu veličinu, potrebno je prekinuti proces naredbom `Ctrl-C`?)

- **Provjera uspješnosti**
  Posljednji korak je računanje MD5 sažetka slike na računalu X te njegova usporedba s MD5 sažetkom slike na računalu F. Ukoliko se ne poklapaju, nešto je pošlo po krivu tijekom postupka uzimanja slike i potrebno je ponoviti postupak s nekim drugim alatom.

- **Uklanjanje mount točke**
  Ako se MD5 saželi poklapaju, uklanja se mount točka s računala X:
  `$ umount 10.0.0.1:/media/disk/IBM/customer_host`