Hardware

Danas postoji toliko različitog sklopovlja da ga je nemoguće cijelog pokriti u ovom članku. Stoga će se pružiti generalni pregled tipova sklopovlja koji se može očekivati u forenzičkim istragama.

I/O uređaji

Input/output se odnosi na prijenos podataka između procesora i vanjskih uređaja. Npr. prilikom pisanja na tipkovnici, ona šalje unos računalu koje dobivene podatke prikazuje na ekranu. Jedan od prvih koraka prilikom analize bi trebao biti popis svih korištenih I/O uređaja. Na temelju tog popisa se može vidjeti koji alati su pogodni za analizu informacija. Isto tako može dati do znanja koja područja su podložna upadima i koja je potrebno nadzirati.

Poslužitelji

Poslužitelj (eng. *server*) je računalo koje ima kapacitet pružanja usluga drugim računalima preko mreže. Poslužitelji mogu imati više procesora, veliku količinu memorije i puno tvrdih diskova (eng. *hard drive*).
Mogu imati različite uloge čijim se identificiranjem lakše mogu odrediti potrebni alati. Česte uloge poslužitelja su aplikacije, podaci, *web hosting*, print, e-mail i FTP.
Trebala bi se odrediti i fizička lokacija poslužitelja. Da li mu se pristupa samo iz unutarnje mreže, samo iz vanjske ili oboje? Na ovaj način se lakše mogu odrediti ranjivosti kao i potrebne mjere zaštite.

Radne stanice

- **Radna stanica** (eng. *workstation*) je desktop računalo s naprednim procesorskim mogućnostima, memorijom i sposobnošću za obavljanje posebnih funkcija kao što su razvoj softwarea ili igara. Istražitelj treba tražiti popis svih radnih stanica u zgradi kao i korisnika koji radnim stanicama pristupaju od kuće.
- **Desktop** je osobno računalo osmišljeno da trajno bude na istoj lokaciji jer su mu komponente prevelike za jednostavni prijenos.
- **Osobno računalo** (eng. *Personal Computer* - PC) je namijenjeno generičnom korištenju pojedinaca. Osobna računala su izvorno bila poznata kao “mikroračunala” jer su bila puno manja od velikih sustava koji su bili najčešći izbor za firme.

Personal Digital Assistants

PDA uređaji mogu funkcionirati kao mobiteli, fax uređaji, web preglednici i organizatori. Osmišljeni su da rade zajedno s osobnim računalom ili laptopom. Komunikacija se odvija putem serijskog USB porta na PDA uređaju, IR (eng. *infrared*) tehnologijom, bežičnom tehnologijom ili telefonskim modemom. Treba obratiti pažnju na to da su PDA uređaji maleni i lako se gube ili kradu čime se osjetljive informacije izlažu riziku. Također, podaci se presresti prilikom bežičnog prijenosa s ili na računalo

ukoliko nisu zaštićeni.
Istražitelj treba znati da li se PDA uređaji koriste u mreži jer ih pojedinci sa zloćudnim namjerama mogu koristiti za krađu osjetljivih podataka.

Ostali uređaji

- ***Floppy* uređaj**
  Floppy diskovi mogu biti veličine 3.5 inča, 5.25 inča i najstariji 8 inča.
- **CD/DVD-ROM/RW uređaj**
  Optički diskovi s kapacitetom od 700 MB do 4 GB.
- **Zip uređaj**
  Mali, prijenosni floppy disk uređaj velikog kapaciteta, razvijen od strane Iomega Corporation i korišten uglavnom za pohranjivanje rezervne kopije diska, ali i za datoteke. Zip diskovi imaju kapacitet 100 MB, 250 MB i 750 MB.
- **Jaz uređaj**
  Zamjenjivi tvrdi disk. Svaka Jaz patrona je u biti tvrdi disk s nekoliko ploča pohranjen u čvrstom, plastičnom pakiranju.

Iako se u nekim dijelovima svijeta neki od ovih uređaja ne koriste, istražitelj ne smije zaboraviti da nije posvuda isto. Stoga uvijek treba biti spreman s rezervama svih vrsta diskova te odgovarajućim vanjskim uređajima za čitanje tih diskova.

Neautorizirani hardver

Česti su slučajevi kad zaposlenici instaliraju vlastite uređaje na poslovnim računalima. Neautorizirane instalacije predstavljaju sigurnosni rizik za organizaciju. Nakon što se provjeri popis svih dopuštenih uređaja u organizaciji, potrebno je potražiti one nedopuštene.

Modemi

Modemi (eng. ***mod****ulator-****dem****odulator*) se koriste za slanje digitalnih podataka preko telefonske linije. Modem pošiljatelj konvertira podatke u signal koji je kompatibilan s telefonskom linijom, a odredišni modem ga konvertira natrag u digitalni signal.

War dialing je napad u kojem se koristi automatizirana aplikacija za biranje telefonskih brojeva u danom rasponu kako bi se otkrilo da li neki od tih brojeva koriste modemi.

Kablovski i DSL modemi nisu skloni takvim napadima, ali izloženi su opasnosti zbog činjenice da su uvijek spojeni na Inrernet. Uz to, kablovski modemi pružaju pristup Internetu putem dijeljenog kabla što znači da sve podatke koji putuju od ili prema nekom računalu u mreži mogu presresti drugi korisnici istog kabla.

Key Loggers

Key logger može biti u obliku programskog rješenja ili fizičkog uređaja. On skuplja i pohranjuje sve pritisnute tipke na tipkovnici što uključuje e-mail poruke, IM poruke, web adrese, osobne podatke, lozinke, brojeve kreditnih kartica…
Organizacije koriste ove uređaje iz više razloga:

- radi potencijalnih istraga računalnih zločina,
- za nadgledanje ili detekciju neautoriziranih pristupa,
- da bi se spriječilo neprihvatljivo korištenje organizacijskih resursa …

Razlog zbog kojeg su key loggeri na popisu neautoriziranih uređaja je taj da se sve može koristiti u zle svrhe. Neautorizirani korisnici ih mogu koristiti da bi ukrali tuđe korisničke podatke.

I/O uređaji

Postoji još mnogo vrsta uređaja koji su dovoljno mali da ih se ne primjeti, a dovoljno brzi da ih je teško otkriti u trenutku dok se upad događa. Njihovo korištenje treba biti regulirano unutar organizacije.