Mrežna forenzika

Mrežna forenzika uključuje analizu mrežne opreme kao što su usmjeritelji, preklopnici (eng. *switch*), koncentratori (eng. *hub*), NIC (eng. *Network Interface Card*), samo računalo te razni mediji poput parica, optičkih kablova i sl. Konkretni podaci se mogu naći na sljedećim uređajima:

- Računalo domaćin (eng. *host*)
  Riječ je o "standardnom" prikupljanju podataka. Obuhvaća slike (eng. *image*) uređaja za pohranjivanje, sadržaj radne memorije i bilo kakve statičke podatke unutar dohvata računala koji se mogu slati preko mreže. Tu se ne broje samo pojedina računala već i svi poslužitelji na mreži (e-mail, datotečni, s bazama podataka, poslužitelji pisača)

- Usmjeritelj (eng. *router*)
  Usmjeriteljski zapisi mogu sadržavati greške do kojih je došlo tijekom usmjeravanja, detalje o komponentama usmjeritelja (npr. sučelja) te sumnjive aktivnosti (ovisno o postavkama zapisa). Osim toga, usmjeritelji čuvaju tablice IP i MAC adresa prema kojima usmjeravaju promet.

- Vatrozid (eng. *firewall*)
  Vatrozid pohranjuje detaljne zapise aktivnosti sustava kao što su prepoznati napadi, odbačeni paketi, aplikacije kojima je dopušten ulaz ili izlaz te popisuje sve sumnjive aktivnosti.

- Preklopnik (eng. *switch*)
  Preklopnici ne stvaraju zapise, ali su korisni za postavljanje prisluškivača ili tzv. zrcala kako bi se kopirali nadolazeći podaci u stvarnom vremenu. No u CAM memoriji (eng. *Content Addressable Memory*) se mogu pronaći podaci o MAC adresama povezanih s određenim portovima, kao i podaci o virtualnim lokalnim mrežama (VLAN – eng. *Virtual Local Area Network*).

- IDS (eng. *Intrusion Detection System*)
  Zapisnici IDS-a sadrže sve što se smatra imalo sumnjivim. Jedna od funkcija IDS-a je zapisivanje događaja za kasniju analizu kako bi se spriječilo ponavljanje incidenta. IDS-ovi su osmišljeni da budu pasivni i mogu se smatrati protuprovalnim alarmom kod računala. Zapisuju se podaci kao što su:
    - skenovi portova,
    - nadolazeći promet iz sumnjivih portova (npr. portovi koji ne bi trebali biti otvoreni, a jesu) ili protokola (npr. protokol koji koristi krivi port),
    - poznate prijetnje poput crva ili virusa koji pokušavaju prodrijeti u mrežu,
    - anonimni pokušaji korištenja FTP ili drugih servisa u mreži,
    - IP adrese izvora napada,
    - iskorištenost veze (eng. *bandwidth usage*).

- IPS (eng. *Intrusion Prevention System*)
  IPS-u je svrha blokirati ili isključiti svaku uočenu prijetnju u mreži. Zapisuje mnoge događaje kao i IDS, ali glavna mu je funkcija analizirati podatke na mreži u stvarnom vremenu. Ako se IDS može usporediti sa protuprovalnim alarmom, IPS bi pozvao policiju i blokirao vrata.

- Mrežni pisač (eng. *network printer*)
  Moderni pisači često pohranjuju zapise o ispisivanim dokumentima zajedno s metapodacima tih dokumenata.

- Mrežni uređaji za kopiranje (eng. *network copier*)
  Kao i pisači, pohranjuju zapise o kopiranim i ispisanim dokumentima.

- WAP (eng. *Wireless access point*)
  WAP zapisuje sve što i normalni “žičani” usmjeritelj uz podatke specifične za bežični promet kao što su SSID identifikatori mreža.