Forenzika

Tehnički i socijalni aspekti

Aco Dmitrović

Što je forenzika?

- Računalna forenzika, *computer forensics*
- Istraga koja nastoji otkriti što se dogodilo na računalnom sustavu

- Prikupljanje tragova
- Istraga i analiza
- Izvještaj o rezultatima
- Sudski proces?

Definicije

- Sigurnosni događaj
- Sigurnosni incident

Hakeri, crackeri

- hackeri, crackeri, scriptie kidz, kriminalci
- Trend profesionalizacije i kriminalizacije
- Sve manje hobista, mladenačkog dokazivanja
- Prodaja izvornog koda exploita, virusa
- Prodaja botneta, mreže zombija
- Prodaja informacija prikupljenih na mreži, s provaljenih računala

Forenzika kakvu ne želite

- Policija kuca na vrata s nalogom
- Traži dokaze da je počinjena kriminalna radnja
- Ako ih nađe, pečati računala i odlazi po sudski nalog za zapljenu opreme
- Istraga i sudski proces mogu biti dugotrajni

Dokazi

- Zaplijenjena oprema je sudski dokazni materijal

- Osim računala, plijene
  - medije (CD-ove, vanjske diskove, diskete, USB memorije…)
  - Dokumente, papire iz pisača itd.

Povod

- Na dojavu, ili u sklopu (međunarodne) istrage

- Najčešći povod:
  - Dječja pornografija
  - Kršenje autorskih prava
  - Provale izvršene s računala tvrtke

Interna istraga

- Naručuje je organizacija koja ima probleme
- Da se ustanovi što se dogodilo i spriječi ponavljanje
- Mogu je obaviti “domaći” ljudi
- Ali se najčešće naručuje od vanjske tvrtke
  - Objektivnost, nema sukoba interesa

Pravilo br. 1

- Sačuvati integritet dokaza, ne kompromitirati “mjesto zločina”

- Što manje intervencija i izmjena, da se ne poremete dokazi
- Na pr.
  - priključivanje USB diska na Windowsima izaziva izmjenu u Registry-ju
  - *ls* na Unixu mijenja *access time*

Dilema

- Konfliktni ciljevi:
- Što prije vratiti računala u produkciju
- Ustanoviti što se dogodilo
  - Poduzeti mjere da se smanji rizik od ponavljanja incidenta

Gasiti ili ne?

- Shutdown – počisti se memorija, *swap*, nestanu programi koji su se izvršavali
- Prekid napajanja: ostaje *swap*, privremene datoteke, gube se procesi

Produkcija

- Naručitelj može zahtijevati da računalo ostane u produkciji
- Kopiranje bit-po-bit
  - memorije
  - cijelog sadržaja diska
  - pokretnih medija (diskete, CD, USB flash…)

Nulto stanje

- Preslike se digitalno potpišu, napravi se *hash (na pr. MD5)*
- Sastavi se zapisnik, koji potpiše nekoliko svjedoka
- *Hash* se prepiše s ekrana, svjedoci potpisom potvrde da je vrijednost u zapisniku identična onoj na ekranu

Istraga

- Istraga se obavi na miru u labu
- Forenzičkim alatima pretražuju se preslike
- Svaki zahvat i nalaz zapisuje se
  - Najbolje odmah
- Na kraju se piše zapisnik o istrazi
- Treba biti oprezan i precizan, točno navesti sve radnje i nalaze
- Izbjegavati nagađanja, držati se činjenica

Sud?

- Moguće je da će se rezultati istrage koristiti u internom, stegovnom postupku
- Ili kao dokazni materijal u sudskom procesu
- Forenzičar ima status vještaka
- Može očekivati napade branitelja, kojem je dovoljno posijati sumnju u dokaze
  - *Reasonable doubt*

Forenzički alati

- Da bi se dokazi održali na sudu, koriste se certificirani forenzički alati
- Komercijalni
- *freeware* – na pr. *Heelix,*

Timski rad

- Istraga se često obavlja u paru
- Kolega može potvrditi navode
- Snimanje!
  - video zapis
  - fotografiranje ekrana
- Jedan se koncentrira na računalo
- Drugi na ljude, materijale koji se mogu naći u okolini
- Dokazi mogu biti i na Internetu

Oprez

- Na licu mjesta ne govoriti ništa ako u to niste sigurni
- Spriječiti glasine
- Igra “pokvarenih telefona”
- Lokalni ljudi mogu izgledati kooperativni, ali možda prikrivaju dokaze, navode na krivi put

Krivi tragovi

- *Crackeri* poznaju forenzičke metode
- Ostavljaju pogrešne tragove
- Gubi se vrijeme, promaknu pravi dokazi

Analiza

- Opis sustava
- *Timeline*
  - Tragovi u logovima mogu ukazati na vrijeme provale
  - Vrijeme kreiranja, izmjena datoteka
  - ctime, mtime, atime
- Analiza medija ovisno o OS-u
  - Windows, Linux…

Analiza…

- Povrat podataka (*Data recovery*)
  - obrisane datoteke
  - swap
- Privremeni podaci (*Volatile data*)
  - memorija
  - procesi
  - mrežne konekcije
- Traženje ključnih riječi (*String/keyword search*)

Počinitelj

- Vanjski napadač
- Lokalni igrač
  - zlonamjeran
  - nemaran, glup
- Vanjski uz pomoć iznutra

Izvještaj

- Informacije prikupljene analizom
  - Dokazi koji potvrđuju pretpostavku
  - Dokazi koji opovrgavaju pretpostavku
  - Vjerojatnost?
- Nalazi i zaključci
  - Koji bi se mogli održati na sudu

Zaključak

- Forenzičku istragu uvijek treba provesti profesionalno
- Nije bitno hoće li dokazi biti korišteni u procesu, sudskom ili disciplinskom
- Forenzičar treba biti upoznat sa zakonima i sudskom praksom
  - razlike USA - EU