Digitalna forenzika

Pregled kursa

Cilj predmeta

- Razumijevanje forenzičkih tehnika i procedura.
- Fokus na korišćenju forenzičkih tehnika u službi računarske bezbjednosti za pomoć u rješavanju incidenata
- Primjena forenzičkih tehnika u drugim situacijama
- Najnoviji trendovi u digitalnoj forenzici

Značaj digitalne forenzike

- U posljednjoj deceniji broj krivičnih djela koja uključuju računare je porastao
- Pomaganje sprovođenja zakona u korišćenju računarski zasnovanih dokaza da se utvrdi ko, šta, gdje, kada i kako?
- Rezultat svega ovoga je digitalni dokaz relevantan pred sudom
- Razvoj velikog broj alata za sprovođenje forenzičkog procesa
- Forenzički alati mogu biti upotrijebljeni i za druge svrhe:
  - monitoring ili nadzor(vođenje dnevnika, identifikovanje i nepoštovanje pravila, revizija i drugo)
  - oporavak podataka (slučajno izmijenjeni, izbrisani, izgubljeni podaci)
  - prikupljanje podataka(napuštanje organizacije, dolazak novog zaposlenog zahtijeva kopiranje svih sadržaja sa radne jedinice zarad potencijalne upotrebe u budućnosti)

Neke popularne teme iz DF

- Forenzika memorijskih medijuma
- Forenzika fajlova
- Forenzika multimedijalnih sadržaja
- E-mail analiza
- Analiza mobilnih uređaja
- Društene mreže

Definicije

- Forensis (lat.)-ispred foruma
- Forensic (eng.) -sudski
- Forenzičke nauke možemo da definišemo kao primjenu nauke na zakon.
- Digitalna forenzika je poznata kao:
  - Kompjuterska forenzika (engl. Computer forensic)
  - Mrežna forenzika (engl. Network forensic)
- Generalno, smatra se kao primjena nauke u:
  - Identifikaciji,
  - Prikupljanju,
  - Ispitivanju,
  - i analizi podataka (sa zaštitom integriteta).

Čuvanje i prenos podataka

- Podaci mogu biti različiti digitalni informacioni sadržaji, struktuirani u specifičnom formatu.
- Poslovne organizacije dobijaju ogromne količine podataka iz različitih izvora.
  - podaci se mogu čuvati ili prenijeti standardnim računarskim sistemima,
  - umrežavanjem računarske opreme,
  - kompjuterskim periferijama (štampač, skener),
  - potrošačka elektronika (čitači kartica, biometrijski skener)

Tehnike za sprovođenje DF

- Zbog raznovrsnosti izvora podataka, digitalne forenzičke tehnike mogu da se koriste u razne svrhe:
  - istraga zločina i kršenje unutrašnje politike,
  - rekonstrukcija računarskog incidenta,
  - rješavanje problema operativnih sistema,
  - oporavljanje slučajno oštećenih sistema
- Praktično, svaka organizacija treba da umije da koristi tehnike digitalne forenzike.
- Bez ovakvih sposobnosti, organizacije će se susresti sa teškoćama tipa:
  - određivanje incidentnog događaja u sistemu,
  - određivanje incidentnog događaja na mreži,
  - kompromitovanje zaštićenih podataka

Proces sprovođenja DF

- Obuhvata sljedeće faze:
  - prikupljanje,
  - ispitivanje,
  - analiza,
  - Izvještavanje

Prikupljanje podataka

- Predstavlja:
  - identifikovanje,
  - obilježavanje,
  - snimanje,
  - prikupljanje podataka (iz mogućih izvora relevantnih podataka, sa nastojanjem očuvanja integirteta podataka)

Ispitivanje podataka

- Obuhvata:
  - forenzičku obradu prikupljenih podataka pomoću:
    - automatskih metoda
    - ručnih metoda
  - ocjenjivanje i vođenje podataka od posebnog interesa

Analiza podataka

- Predstavlja:
  - analizu rezultata ispitivanja upotrebom pravno dozvoljenih metoda i tehnika
  - pronalazak korisne informacije za podsticaj daljeg prikupljanja i saslušanja

Izvještavanje forenzičkog procesa

- Predstavlja:
  - izvještavanje o rezultatima analize,
  - opisivanje korišćenih akcija,
  - objašnjavanje kako su izabrani alati i procedure,
  - predlaganje budućih akcija(pregled dodatnih izvora, identifikacija slabosti, poboljšanje postojeće bezbjednosne politike),
  - davanje preporuka za unapređenje (politike, procedura, alata i drugih aspekata forenzičkog procesa)

Izvori podataka

- Slijede četiri glavne kategorije izvora podatka:
  - datoteke
  - operativni sistemi
  - mrežni saobraćaj
  - aplikacije
  - kombinovani izvori
- Zbog karakteristike navedenih izvora podataka, postoje specifičnosti za svaku od faza forenzičkog procesa (prikupljanje, ispitivanje i analiza podataka)
- Peta kategorija je istovremeno korišćenje više izvora podataka, radi boljeg razumijevanja događaja

Preporuke za organizacije

- Svaka organizacija treba da:
  - upodobi svoj sistem forenzičkoj istrazi (redovno obavlja monitoring, kontroliše sprovođenje procedura) u skladu sa zakonom
  - stvara i održava procedure i smjernice za obavljanje forenezičkih poslova sa važećim zakonima i propisima
  - osigura da njihova politika i procedure podržavaju razumno i adekvatno korišćenje forenzičkih alata
  - da edukuje stručnjake iz IT centra, da budu sposobni da učestvuju u forenzičkoj istrazi