integrirana sigurnost

Analiza logova u računalnoj forenzici

Damir Delija
Dr.Sc.E.E

Plan predavanja

- Analiza logova - što je to
- Korištenje logova i analize logova u računalnoj forenzici.
  - razni načini izvođenja analiza, prikupljanja podataka iz raznih vrsta logova
  - razni alati i potrebne vještine
  - postoje i neortodoksni postupci, osnovani na čisto forenzičkim pristupima ili preventivnoj računalnoj forenzici

Što je analiza logova

- Analiza logova je ključni dio kontrole svakog računalnog sustava
- Ekvivalent „early warning radarskog“ sustava
- Pouzdan trag svega što se događalo, što se događa i što se može desiti u nekom sustavu

- Negdje se još može čuti i „gatanje iz logova“

Korištenje logova i analize logova u računalnoj forenzici

- U slučaju vještog napadača jedini tragovi koji se mogu naći su logovi na offline log collecting sustavu
  - Uz napomenu da u taj remote logging sustav napadač nije mogao ili nije znao provaliti… ☺
- Dakle posljednja linija obrane gledano sa stanovišta klasične reaktivne forenzike
- Osim toga bogat, prebogat, izvor podataka o radu sustava i korisnika

Događaji u sustavu

- U logovima se bilježe važni događaji za sustav
- Događaj (event) situacija koja se može opazitii
  - Modifikaicija unutar zadanog okruženja u nekom vremenskom periodu.
  - Događaj može biti određeno stanje ili promjena stanja sustava.
  - Može biti opisan ili zabilježen u log (zapis)
- Pojedinačni zapis naziva se log (log entry).
- Pojedinačni zapis sadrži opis jednog ili više događaja.

Podjele logova

- Podatke koje dobivamo iz logova može se grubo podijeliti u dvije grupe
  - Vremenske serije
    - Osnovni podaci iz logova
    - Svaki zapis ima “time stamp” koji ga vremenski pozicionira u nizu drugih zapisa
  - Statičke podatke
    - Konfiguracije,
    - Debug outpute i sl
  - Napomena: ima i drugih podjela

Razumijevanje logova

- Važan dio analize logova je
  - Prikaz logova i podatka iz logova u razumljivom obliku
  - Racionalizacija i pretprocesiranje logova
  - Adminstracija logova - uvjek zaboravljena ili bar zanemarena
- Vizualizacija logova je umjetnost za sebe

Vizualizacija logova

- Izuzetno važan ali zanemaren pristup logovima i radu sa podacima iz sustava
- Uz malo vještine može se puno postići
  - Improvizacije – obični tablični kalkulator može napraviti čuda
- Osim što jako olakšava rad sa podacima, omogućuje i jednostavan prikaz “netehničkom” osoblju, obično onima koji donose odluke …

- Raffael Marty: “Applied Security Visualization”, 2008, Addison Veslley ISBN-13: 978-0-321-51010-5

Računalna forenzika

- Vrlo kratko:
  - Osiguravanje i izuzimanje svega što je „digitalni dokaz“
  - Pronalaženje dokaza i analiza znanstvenom metodom
- Formalno:
  - Računalna forenzika ili digitalna forenzika definira se kao prikupljanje, zaštita i analiza dokaza u digitalnom obliku
  - Prezentacija digitalnih dokaza kao materijalnih dokaza u kasnijim eventualnim sudskim postupcima..

Elementi računalne forenzike

- Računalnu forenziku dijelimo na
  - Forenziku računala
  - Forenziku mreža (umreženih sustva)
  - Forenziku logova sustava (system log forensic)
- Postoji i podjela na :
  - Proaktivnu forenziku
  - Reaktivnu forenziku (klasična)

Računalna forenzika i forenzičko značenje logova

- To je forenzika logova sustava - system log forensic
- Analiza zabilježenih ključnih događaja u sistemskim logovima (centraliziranim ili lokalnim)
- Osnovna svrha gradnje vremenskog slijeda („timelinea“) događanja

Sustavi za prikupljanje i analizu logova

- Komercijalni ili free teško reći što je bolje
  - Svima isti cilj prikupiti i čuvati logove
  - Analizirati logove
  - Prikaz rezultata analiza – izvještaji
- Obično uvjetovani zahtjevima regulatora
- Odabir alata je kompleksan postupak, postoje kuharice za odabir

Forenzički alati i analiza logova

- Analiza logova dio funkcionalnosti alata
- Podržani formati logova rasprostranjenih operacijskih sustava
- Primjer: Guidance Software Encase
  - http://www.guidancesoftware.com/
  - Modul za pronalaženje i analizu windows i unix logova unutar automatske pripreme slučaja
- Mogu poslužiti i obični alati za analizu logova
  - bitno je da ne mijenjaju sadržaj logova

Zaključak

Bez logova nema forenzike sustava

- Analiza logova se isplati I u drugim situacijama, tj kad se radi sa logovima treba se postupati inženjerski pouzdano
- Artefakti na file sistemu nam omogućuju da vidimo zadnje stanje i vlasništva,
- Logovi nam kažu prošlost, tko je i kada je nešto promijenio.
- Da bi logovi bili forenzički korisni moraju biti potpuni i precizni.
- Navedeni primjeri pokazuju da logovi i njihovo korištenje ima velike potencijalne, ali samo ako ih se obradi, analizira i prikaže na pravi način i pravim alatima.

Korisni linkovi i reference

- Security Log Management, Syngress, Jacob Babbin January 2006, ISBN-13: 978-1-59-749042-9;
- Short Topics in System Administration Building a Logging Infrastructure, Abe Singer and Tina Bird, USENIX Association, 2004, ISBN 1-931971-25-0;
- Crimeware http://en.wikipedia.org/wiki/Crimeware;
- http://www.sans.org/reading_room/whitepapers/logging/;
- "EnCase® Enterprise", https://www.guidancesoftware.com/;
- Common Event Expression white paper, http://cee.mitre.org, 2007;
- Marty, Rafael, „Applied security visualization“ Addsison Wealey 2008, ISBN 0-321-51010-0;
- David N. Blank-Edelman , "Perl for System Administration", ISBN 1-56592-609-9, First edition;

Pitanja

- Kako vi kod sebe koristite logove ?
- Da li bi u slučaju incidenta mogli nešto izvući iz podataka ?

- Pitanja za mene na:

  damir.delija@insig2.hr