

Računalna forenzika u službi IT-a

Na treningu se, kroz tri dana, obrađuje sljedeće:

Općenito o računalnoj forenzici – polaznik će se upoznati s osnovnim konceptima računalne forenzike i alatima koji se koriste za tu namjenu. Bit će definirani digitalni dokazi i načini ispravnog prikupljanja digitalnih dokaza u svrhu upotrebe u sudskim i vansudskim procesima.

Sustavi za pohranu podataka – nakon definiranja tipova konektora kojima se mediji za pohranu podataka mogu priključiti na računalo, bit će definirani tipovi medija (HDD, SSD, optički mediji) i specifičnosti vezane uz svakog od njih.

File sustavi – obradit će se poznatiji file sustavi kao što su FAT32, NTFS, EXT3 i specifičnosti svakoga od njih. Spomenut će se načini spašavanja obrisanih podataka, te će polaznik u praktičnom dijelu predavanja vratiti obrisane fileove korištenjem standardne undelete metode i korištenjem data carving metode.

Forenzika memorije – s pojavom sve naprednijih i pametnijih malicioznih programa, sve je teže identificirati vektore kojima su ti programi došli na zaraženo računalo. Obično jedini trag koji ostavljaju za sobom čeka u memoriji kako bi bio otkriven. Polaznik će analizom unaprijed pripremljenog memorijskog image-a odgovoriti na pitanja poput, kada, kako i kojim putem je računalo zaraženo.

Steganografija – jedan od najčešćih načina skrivanja informacija od neželjenih pogleda je neki vid steganografije – skrivanja podataka unutar drugih podataka. U ovom modulu polaznici će se upoznati s osnovama steganografije i u vježbi će imati priliku sakriti podatke unutar drugih podataka.

Forenzika mrežnih logova – Svaka interna forenzička analiza kao dio posla koji treba odraditi koristi i analizu mrežnih logova, tj. mrežnog prometa. Neki od poznatijih besplatnih alata su Wireshark, MS Message Analyzer i NetworkMiner. Svaki od njih ima različitu primjenu u računalnoj forenzici što će biti pokazano u demo dijelu predavanja.

EFS – Microsoft Encrypted File System (EFS) je sastavni dio NTFS file sustava i distupan je u MS operacijskim sustavima od Windowsa 2000. U pitanju je file level enkripcija koja koristi PKI arhitekturu kako bi bila što je moguće robusnija i otporna na napade. No, u pitanju je tehnologija koja radi transparentno i ne zahtijeva nikakvu interakciju s korisnikom, pa je samim tim i napad na nju „relativno“ jednostavan. U forenzičkoj analizi često se susrećemo s kriptiranim fileovima, pa tako i EFS-om, pa će se polaznik u ovom modulu upoznati s PKI arhitekturom i načinima kako razbiti EFS enkripciju.

Forenzički izazovi – Za kraj predavanja posvetit ćemo se forenzičkoj istrazi preko dva cjelovita zadatka u kojima treba upotrijebiti upravo stečeno znanje i korištenjem steganografije, EFS dekripcije, mrežne forenzike i alata koje smo obrađivali prethodnih dana pronaći tražene informacije.

Potrebno predznanje:

Ethical hacking bootcamp (**Pogled na sigurnost računarskih sistema s „tamne strane“**)

1. Općenito o forenzici
 - Što su sve digitalni dokazi
 - Kako prikupiti digitalne dokaze na ispravan način
 - Kako sačuvati digitalne dokaze
 - Alati (FTK, EnCase, besplatni alati ..)
 - VJEŽBA: Izrada image-a diska
2. Sustavi za pohranu podataka
 - Tipovi konektora
 - HDD
 - SSD
 - Optički mediji
3. File sustavi
 - FAT
 - NTFS
 - EXT3
 - VJEŽBA: File recovery (undelete)
 - VJEŽBA: File recovery (data carving)
4. Forenzika memorije
 - Čemu služi i ima li smisla u istražnom procesu?
 - Kako napraviti dump memorije
 - VJEŽBA: izrada image-a memorije
 - VJEŽBA: analiza napada kroz dump memorije
 - DEMO: probijanje BITLocker enkripcije pomoću memory dump-a
5. Steganografija
 - Općenito o steganografiji
 - Primjena steganografije
 - Važnost steganalize u forenzičkoj istrazi
 - DEMO: detekcija i ekstrahiranje steganografskog materijala
6. Forenzika mrežnih logova
 - Snifanje prometa
 - Alati (Wireshark, MS Message analyzer, Network miner)
 - DEMO: Analiza mrežnog prometa poznatijim alatima
7. EFS
 - PKI osnove
 - Što je EFS?
 - Kako radi EFS
 - Napadi na EFS
 - DEMO: dekriptiranje fileova kriptiranih EFS enkripcijom
8. Forenzički izazovi
 - Steganografija i mrežna forenzika
 - EFS dekriptiranje i traženje skrivenih informacija na windows OS image-u