INTERNATIONAL SECURITY INSTITUTE

MEĐUNARODNI INSTITUT ZA BEZBEDNOST

NAZIV KURSA: Digitalna forenzička istraga „DFI“

- Digitalna forenzika i digitalni dokaz (osnovni pojmovi u digitalnoj forenzici, pojam digitalnog dokaza, rad sa digitalnim dokazima, prikaz vrsta forenzičke istrage zvanična i korporacijska)
- Proces digitalne forenzičke istrage (četiri faze forenzičke istrage: sakupljanje podataka, ispitivanje prikupljenih podataka, analiza prikupljenih podataka, izveštavanje - veštačenje)
- Akvizicija podataka (dva pristupa prikupljanju podataka, live odnosno forenzika računara u radu bez isključivanja i klasična forenzika isključenog računara)
- Privremeni i drugi forenzički relevanti fajlovi (prikaz relevantih fajlova za forenzičku istragu na sistemima Windows, Linux, MacOS)
- Forenzička analiza prikupljenih podataka (tri faze istrage, analiza softvera, analiza hardvera, analiza kibernetičkog prostora - internet)
- Forenzički alati (prikaz forenzičkih alata, hardverski i softverske alati, kao i alati sa komandnom linijom i oni koji imaju grafičku koristički interfejs GUI)
- Izveštavanje (prikaz rezultata forenzičke istrage kroz veštačenje kompjuterskog kriminala na sudu ili kroz izveštavanje menadzmentu firme u slučaju korporacijske privatne istrage, edukacija pravosudnih organa)
- Windows forenzika (fajl struktura NTFS i FAT, registry, privremeni fajlovi, šifrovani i kompresovani fajlovi, zanimljive lokacije gde se nalaze podaci bitni za forenzičku istragu u windows okruzenju)
- Linux/Unix forenzika (fajl struktura EXT2, EXT3, RaiserFS, privremeni fajlovi, šifrovani i kompresovani fajlovi, zanimljive lokacije gde se nalaze podaci bitni za forenzičku istragu u unix okruzenjima)
- Forenzika slike (upoznavanje sa tehnikama manipulacije slikom i tehnikama automatske detekcije, copy-move napad, patcmatch algoritam, SIFT algoritam)

- Forenzika mobilnih telefona, PDA i tableta (forenzička analiza smart uredjaja sa android ili iOS operativnim sistemom Oxygene forensic i UFED, izvlačenje različitih podataka kao što su SMM i MMS poruke, kontakti, emailovi, GPS lokacije, slike i video fajlovi, log fajlovi o korišćenju kamere i sl..)
- Cloud forenzika (pojam Cloud-a ondonsno oblaka, vrste oblaka, forenzika podataka u oblaku, specifičnosti prikupljanja podataka iz oblaka, problemi prilikom prikupljanja pravni-tehnički, pet efikasnih tehnika za prikupljanje podataka iz cloud okruženja)
- Email forenzika (forenzika elektronske poste, tehnike i alati za prikupljanje i analizu podataka vezanih za korišćenje email-a, pronalazenje odredjenih mailova po različitim kriterijumima, prikaz različitih alata)
- Router forenzika (specifična oblast forenzike gde se ne koristi računar kao dokaz već deo aktivne mreže opreme odnosno router, pregled tabela rutiranja, arhitektura, Internetwork Operating System(IOS), tipovi napada na rutere)
- Forenzička analiza log fajlova (analiza relevantnih log fajlova za forenzičku istragu, lokacije relevantnih fajlova, vrste log faljova, alati za analizu)
- Monitoring mreže (posebna vrsta aktivne forenzičke istrage koja se vrši u toku napada jer se prati mrežni saobracaj, filtriranje TCP i UDP protokola, alati za ovu namenu WinDump, Ethereal, NetIntersect, SNORT)
- Antiforenzika (Antiforenzika odnosno proces suprotan od forenzike, skrivanje dokaza da je izvršeno odredjeno krivično delo kompjuterskog kriminala, metode i alati BackTrack, EvidenceEliminator, korišćenje virtualnih mašina kao antiforenzičkih alata)

TRAJANJE KURSA: dva radna dana (14 nastavnih časova)

PREDAVAČ: mr Igor Franc – magistar bezbednosti informacionih sistema

KOME SE KURS-SEMINAR PREPORUČUJE: stručnjacima u oblasti bezbednosti IKT, istraživačima u oblasti kompjuterskog kriminala, veštacima u oblasti IKT, sistem administratorima za bezbednost, ostalim licima sa osnovnim IT znanjima.