Mrežna forenzika

Šeruga, Dona

Undergraduate thesis / Završni rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:131:435178

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2017./ 2018.

Dona Šeruga

MREŽNA FORENZIKA

Završni rad

Mentor: dr.sc. Vjera Lopina

Zagreb, 2018.

Sadržaj

1. Uvod 4
2. Forenzika 5
2.1. Digitalna forenzika 6
2.2. Mrežna forenzika 7
2.1.1. Metode upada u mrežu 8
2.1.2. Metodologija OSCAR 9
3. Dokazi 10
3.1. Digitalni i mrežni dokazi 11
3.1.1. Aktivno i pasivno prikupljanje dokaza 13
3.1.2. Fizičko presretanje 13
3.1.3. Programi za praćenje prometa 14
3.1.4. Aktivno prikupljanje dokaza 15
4. Mrežna forenzika u praksi 17
4.1. Slučaj – krađa bolničkog laptopa 17
4.2. Obrazovanje 18
4.2.1. Hrvatska 18
4.2.2. Kanada i SAD 19
4.3. Certifikacija 20
4.3.1. Mrežni branitelj 20
4.3.2. Etički haker 21
4.3.3. Sigurnosni analitičar 22
4.3.4. Ispitivač probojnosti 22
5. CERT 23
5.1. Uloga i misija 23
5.2. Izvještaji nacionalnog CERT-a 24
6. Zaključak 27
Popis literature 28
Popis internetskih izvora 28
Prilozi 30

Sažetak

Mreža je tok podataka, ako je njezina sigurnost ugrožena, ugroženi su i podaci. U ovom radu ću se baviti temom mrežne forenzike, granom digitalne forenzike koja se fokusira na kriminal na Internetu, Ethernetu, mrežnim protokolima te bežičnom prometu. Budući da je računalni kriminal sve rasprostranjeniji u svijetu, tako i u Hrvatskoj, kibernetička sigurnost se javlja i u obrazovanju. Iznijet ću statističke podatke Computer Emergency Response Team-a, kao uvid u trenutnu situaciju i blisku budućnost razvitka sigurnosti računalnih mreža.

Ključne riječi: *računalna mreža, mrežna forenzika, digitalna forenzika, mrežni protokoli, bežični promet, kibernetička sigurnost*

Network forensics

Abstract

Network is a data flow, if its security is compromised, data is compromised. In this paper I will deal with the topic of network forensics, a branch of digital forensics focused on crime on the Internet, Ethernet, network protocols and wireless traffic. Since cybercrime is increasingly widespread in the world, as well as in Croatia, cybersecurity also appears in education. I will outline the Computer Emergency Response Team's statistics, as an insight into the current situation and the close future of the development of computer network security.

Key words: *computer network, network forensics, digital forensics, network protocols, wireless traffic, cybersecurity*

1. Uvod

Svakim danom svjedočimo brzom razvoju računalnih tehnologija i mreža, a time i porastu kibernetičkog kriminala. Mrežna forenzika se počinje razvijati upravo iz tog razloga. Metodom dedukcije, u prvom djelu rada će biti objašnjen pojam forenzike općenito, pa digitalna i mrežna forenzika. U početku idućeg poglavlja će biti objašnjeno što je to forenzika, njezin razvoj i koja sve područja obuhvaća. Nakon toga, bit će definirana digitalna forenzika i njezine grane. Jedna od grana digitalne forenzike je mrežna forenzika, koja je ujedno i tema ovog rada. Nakon definiranja samog pojma mrežne forenzike, bit će objašnjeni ciljevi i metode napada na mrežu, a zatim i metodologija koju forenzičari koriste tijekom istrage. Sljedeće poglavlje će govoriti o dokazima, njihovoj važnosti, te načinima i problemima prikupljanja istih. U ovom radu, iznijet ću i primjer slučaja u kojem su mrežni forenzičari sudjelovali, da bi se stekao dojam o tome kako to sve izgleda u praksi. Također, mrežna i digitalna forenzika postaju dijelom obrazovnih sustava u Sjedinjenim Američkim Državama, Kanadi, ali i u Hrvatskoj. Osim toga, sve su raširenija i tečajevi s certifikacijom vještina koje su bitne u mrežnoj forenzici. Posljednje će poglavlje biti vezano za Nacionalni CERT, tijelo zaduženo za informacijsku sigurnost građana Republike Hrvatske. Na kraju rada bit će izneseni grafikoni CERT-ovih izvještaja koji će prikazati najčešće incidente i prijetnje na hrvatskoj domeni.

2. Forenzika

Forenzika ili forenzična znanost (eng. *forensic science*) izvedena je iz latinske riječi *forensis*, što znači javna diskusija, odnosno debata s javnog mjesta, foruma, i latinske riječi *scientia*, što znači znanost, znanje, stručnost.[1][2] U modernijem kontekstu forenzična znanost predstavlja primjenu znanstvenih metoda i procesa u rješavanju kriminalističkih slučajeva. Forenzika se razvijala od 16. stoljeća kada je bila dio medicine, kroz 18. stoljeće kada je otkriven prvi dokaz moderne patologije pa sve do 1909. kada je otvorena prva škola forenzične znanosti. Od 1909. godine do danas, nevjerojatne znanstvene inovacije i sam napredak forenzike, omogućili su da postane jedna od razvijenijih znanosti koja se sastoji od niza disciplina i velikog broja forenzičara, specijaliziranih za mnoga područja. Forenzika ima karakteristike fizike, kemije i biologije, s naglaskom na prepoznavanje, identifikaciju i evaluaciju fizičkih dokaza. Iz tog je razloga forenzika ostala bitan dio pravosudnog sustava. Forenzična znanost može dokazati postojanje zločina, počinitelja i povezanost sa zločinom kroz ispitivanje fizičkih dokaza, primjenu testova, tumačenje podataka, jasno i sažeto izvješće i svjedočenje forenzičara. Forenzičari koriste mikroskope i druge složene instrumente, matematičke i znanstvene principe te literature za analizu dokaza. Mogu raditi unutar laboratorija ili mrtvačnice, ali i na mjestu zločina. Forenzičari se mogu podijeliti u tri grupe: forenzični patolozi, koji se bave medicinskim i kliničkim ispitivanjem te autopsijom, forenzični znanstvenici koji se bave toksikologijom, oružjem i dokazima te povezani znanstvenici kao što su botaničari, antropolozi, stomatolozi i drugi. Forenzika se dijeli na velik broj poddisciplina kao što su analiza dokaza, kriminalistika, forenzična toksikologija, psihologija, patologija, lingvistika, DNK analiza, botanika, stomatologija, forenzični inženjering, digitalna forenzika i druge.[3]

[1] Forensic (adj.). Online Etymology Dictionary. Preuzeto sa:.https://www.etymonline.com/word/forensic (02.05.2018.)
[2] Science (n.). Online Etymology Dictionary. Preuzeto sa: https://www.etymonline.com/word/science (02.05.2018.)
[3] What is Forensics? Crime Scene Investigator Education. Preuzeto sa: https://www.crimesceneinvestigatoredu.org/what-is-forensic-science/ (02.05.2018.)

2.1. Digitalna forenzika

Razvojem tehnologije, razvija se i relativno mlada grana forenzike. Nove računalne tehnologije i Internet dostupni su svima. Iz tog su razloga računala, laptopi, tvrdi diskovi i slični predmeti, sve češći dokazi na sudu. Digitalna forenzika se bavi prikupljanjem i analiziranjem takvih dokaza. Česti sinonim za digitalnu forenziku je računalna forenzika, ali se ona odnosi na kolekciju tehnika i alata koji se koriste za prikupljanje dokaza isključivo na računalu.[4] Digitalna forenzika se odnosi na korištenje znanstveno izvedenih i dokazanih metoda za očuvanje, prikupljanje, potvrđivanje, identifikaciju, analizu, tumačenje, dokumentaciju i predstavljanje digitalnih dokaza izvedenih iz digitalnih izvora, zbog olakšavanja rekonstrukcije događaja za koje se utvrdi da su povezani sa zločinom ili zbog predviđanja neovlaštenih radnji za koje se pokazalo da ometaju planirane operacije.[5] Digitalna forenzika se dijeli na tri discipline s obzirom na vrstu uređaja ili medija, a to su računalna forenzika (eng. *computer forensics*), mobilna forenzika (eng. *mobile device forensics*) i mrežna forenzika (eng. *network forensics*). Osim njih, postoji i forenzika baza podataka (eng. *database forensics*). Računalna forenzika, kao što je ranije navedeno, prikuplja dokaze s računala ili povezanih računalnih sustava. Mobilna forenzika se bavi prikupljanjem i očuvanjem dokaza iz mobilnih uređaja, odnosno mobilnih telefona, USB-ova, PDA-ova, GPS uređaja, digitalnih kamera i tableta.[6] Forenzika baza podataka se bavi bazama podataka i njihovim metapodacima. Problemi s kojima se forenzičar za baze podataka suočava su pad baze, izbrisani podaci i informacije iz baze, nestabilnost baze i sumnjivo ponašanje korisnika baze.[7]

[4] Reith, M., Carr, C., Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal Of Digital Evidence, 1(3). Preuzeto sa: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.13.9683 (05.05.2018.)
[5] Digital Forensics Research Workshop. "A Road Map for Digital Forensics Research" 2001. http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf
[6] ISACA (2015). Overview of Digital Forensics. Rolling Meadows,Illinois. Preuzeto sa: http://www.infosecurityeurope.com/__novadocuments/83665?v=635652368156170000 (05.05.2018.)
[7] What is Database Forensics? InfoSec Institute. Preuzeto sa: http://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/application-forensics/overview-types-of-database-forensics/#gref (05.05.2018.)

2.2. Mrežna forenzika

Definirajući forenziku i digitalnu forenziku, dedukcijom dolazimo do mrežne forenzike kao grane digitalne forenzike. Mrežna forenzika (eng. *network forensics*) je upotreba znanstveno dokazanih tehnika za prikupljanje, spajanje, prepoznavanje, ispitivanje, povezivanje, analizu i dokumentaciju digitalnih dokaza iz višestrukih aktivnih obrada i prijenosa digitalnih izvora radi otkrivanja činjenica povezanih s planiranim namjerama ili neovlaštenim aktivnostima za prekid, kvar ili kompromitiranje komponenti sustava.[8] Mrežna forenzika je, u užem smislu, prikupljanje, bilježenje i analiziranje događaja na mreži, kako bi se otkrio izvor sigurnosnih napada. Snimanje mrežnog prometa je u teoriji jednostavno, ali je u praksi vrlo složeno zbog velike količine podataka koji prolaze kroz mrežu i kompleksne prirode samih protokola. Iz tog razloga nije moguće snimiti sve podatke koji prolaze kroz mrežu, ali posao mrežnog forenzičara je da od svih podataka koje uspije snimiti, napravi sigurnosne kopije za kasniju obradu i analizu.[9] Metode mrežne forenzike često variraju. Neke istrage prate sav promet na mreži, dok druge koriste posebna i ciljana promatranja prometa. Stručnjaci dijele mrežnu forenziku u dvije kategorije: „*catch-it-as-you-can"* i „*stop, look and listen*". „*Catch-it-as-you-can*" je sustav u kojem se svi paketi koji prolazi kroz određen promet bilježe i zapisuju u pohranu, dok se analiza obavlja naknadno u serijskom načinu rada. Ovaj pristup zahtjeva više prostora za pohranu. „*Stop, look and listen*" je sustav u kojem se svaki paket analizira posebno u memoriji i samo se određeni podaci spremaju za buduću analizu. Ovaj pristup zahtjeva manje prostora za pohranu, ali može zahtijevati brži procesor kako bi nastavio pratiti dolazni promet.[10] Mrežni forenzičari mogu tražiti uspostavljanje digitalnih vremenskih linija za mrežne događaje i prikupljanje drugih podataka o upotrebi mreže, uključujući IP adrese i razmjene šifriranih i nešifriranih poruka. U nekim slučajevima, zakoni o zaštiti privatnosti i druge vrste zakonskih ograničenja primjenjuju se na ovakve istrage.[11]

[8] Digital Forensic Research Workshop (2001). A Road Map for Digital Forensic Research. In *The Digital Forensic Research Conference*. Utica, New York. Preuzeto sa: http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf (05.05.2018.)
[9] EC-Council (2010). Computer Forensics: Investigating Network Intrusions and Cyber Crime. Preuzeto sa: https://news.asis.io/sites/default/files/Investigating_Intrusions_Network_CyberCrime.pdf (05.05.2018.)
[10] Network Forensics. TechTarget. Preuzeto sa: https://searchsecurity.techtarget.com/definition/network-forensics (27.06.2018.)
[11] Network Forensics. Techopedia. Preuzeto sa: https://www.techopedia.com/definition/16122/network-forensics (27.06.2018.)

2.1.1. Metode upada u mrežu

Mrežni forenzičari mogu otkriti kako je napadač upao u mrežu, kojim putem, tehnike koje je koristio i tragove koje je ostavio. Osobe koje žele upasti u mrežu ili sustav koriste metode poput nabrajanja, iskorištavanja ranjivosti, viruse i trojance, zaraza elektroničke pošte, napade na usmjernike i otkrivanje zaporki. Nabrajanje (eng. *enumeration*) je proces skupljanja informacija o mreži, koje bi pomogle pri napadu na mrežu. Provodi se putem interneta, a skupljaju se informacije poput topologije i arhitekture mreže, popisa aktivnih poslužitelja (eng. *live host)*, vrste mrežnog prometa i potencijalne ranjivosti u sustavu. Iskorištavanje ranjivosti podrazumijeva otkrivanje slabosti sustava, mreže ili elemenata mreže i njihovo iskorištavanje pri napadu, a provodi se pomoću različitih programa za pretraživanje ranjivosti ili slabosti. Virusi su zlonamjerni programi koji izmjenjuju ponašanje računala ili drugog uređaja na mreži, bez dopuštenja ili znanja korisnika. Trojanci su programi koji sadrže ili instaliraju zlonamjerne programe na ciljane sustave, a koriste se za upade u sustav i za krađu podataka. Zaraza elektroničke pošte (eng. *e-mail infection*) je korištenje elektroničke pošte u svrhu napada na mrežu. Najčešći se provodi slanjem neželjene pošte (eng. *spam*), koja može izazvati uskraćivanje usluge (eng. *denial-of-service*). Usmjernik (eng. *router*) je glavni ulaz na mrežu i sav promet prolazi kroz njega, što znači da napad može srušiti cijelu mrežu. Otkrivanje zaporki (eng. *password cracking*) je posljednje sredstvo napada sustava ili mreže.[12] Otkrivanje zaporki je tehnika krađe zaporki korisničkih računa. Postiže se oporavljanjem zaporki iz podataka na računalu ili podataka izvedenih s računala. Otkrivanje zaporke je moguće neprestanim nagađanjem zaporke, ali danas je to olakšano zbog računalnih programa koji probijaju zaporku nekom vrstom algoritma.[13]

[12] EC-Council (2010). Computer Forensics: Investigating Network Intrusions and Cyber Crime. Preuzeto sa: https://news.asis.io/sites/default/files/Investigating_Intrusions_Network_CyberCrime.pdf (05.05.2018.)
[13] Password Cracking. Techopedia. Preuzeto sa: https://www.techopedia.com/definition/4044/password-cracking (07.05.2018.)

2.1.2. Metodologija OSCAR

Upoznajući se s metodama napada, slijede metode istrage ili OSCAR. Metodološki okvir mrežne forenzike OSCAR je akronim za *Obtain information*, *Strategize*, *Collect evidence*, *Analyze* i *Report* odnosno prikupi informacije, formuliraj strategiju, prikupi dokaze, analiziraj i napravi izvješće. Prvi korak istrage je dobiti informacije o samom slučaju i o okolini. Informacije o slučaju podrazumijevaju opis događaja, datum, vrijeme i metodu otkrivanja slučaja, koje osobe imaju veze sa slučajem, koji su sustavi i podaci uključeni u slučaj, koje su radnje poduzete od otkrivanja slučaja, pravna pitanja, vremensko razdoblje za istragu i rješavanje istrage, ciljeve istrage i druge podatke ovisno o slučaju. Prikupljanje podataka o okolini ovisi o poznavanju same okoline. Informacije o okolini uključuju poslovni model, pravna pitanja, topologiju mreže, dostupne izvore mrežnih dokaza, organizacijsku strukturu, komunikacijske sustave te ostale izvore poput radnika, opreme, financiranja i vremena. Drugi korak istrage je formuliranje strategije. Za dobru strategiju treba razumjeti ciljeve i vremenski okvir istrage, zapisati izvore (osoblje, vrijeme i opremu), identificirati moguće izvore dokaza, za svaki izvor dokaza, procijeniti vrijednost i trošak dobivanja istog, planirati prikupljanje i analizu te odlučiti o metodama i vremenu komunikacije. Sljedeći korak je prikupljanje dokaza koje ću detaljnije objasniti u idućem poglavlju. Zatim se obavlja analiza te su tada bitne stavke korelacija, vremenska crta, zanimljivi događaji, potvrda, prikupljanje dodatnih dokaza i interpretacija. Korelacija podrazumijeva koje podatke je moguće sastaviti, iz kojih izvora i kako ih se može povezati. Potrebno je voditi vremensku crtu da bi znali tko je napravio što i kada te kako je to osnova bilo kakve teorije slučaja. Neki događaji će biti relevantniji od drugih pa ih je bitno razdvojiti da bi shvatili njihovu važnost. Potvrda je bitna jer u slučajevima postoji problem "lažnog pozitivnog", zato treba potvrditi događaje kroz izvore. Prikupljanje dodatnih dokaza je bitan dio analize jer će se kroz istragu uvijek pojaviti novi dokazi. Interpretacija kao zadnji korak analize podrazumijeva razvijanje i konstrukcija teorija o tome što se dogodilo, ali je ona samo hipoteza koja može, ali ne mora biti istinita. Posljednji korak metodologije je izvješće. Kada su svi koraci učinjeni, bitno je iznijeti svoje rezultate istrage drugim forenzičarima i kolegama. Izvješće mrežnog forenzičara mora biti razumljivo netehničkim laicima, detaljno i činjenično.[14] Kao što je navedeno ranije, bitan dio strategije je određivanje važnosti pojedinih dokaza i redoslijed njihova prikupljanja. U sljedećoj tablici

[14] Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace. Upper Saddle River, New Jersey: Prentice Hall. (08.05.2018.)

navedeni su prioriteti u prikupljanju dokaza s obzirom na njihovu vrijednost (eng. *value*), napor u prikupljanju (eng. *effort)* i promjenjivost ili nestabilnost dokaza (eng. *volatility*).

Source of Evidence	Value	Effort	Volatility	Priority
Firewall logs	High	Medium	Low	2
Web proxy cache	High	Low	Medium	1
ARP tables	Low	Low	High	3

Tablica 1: Određivanje prioriteta pri prikupljanja mrežnih dokaza (Izvor: Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace)

3. Dokazi

Dokaz je iskustveni ili misaoni podatak koji opravdava prihvaćanje neke prosudbe (mišljenja, teorije); postupak kojim se potkrjepljuje valjanost neke tvrdnje.[15] Prikupljanje dokaza je kompleksan posao mrežnog forenzičara. Svako prikupljanje dokaza zahtjeva tri koraka: dokumentaciju svih pristupljenih sustava i radnji tijekom prikupljanja dokaza, "hvatanje" dokaza, odnosno paketa na mreži, kopiranje zapisnika (eng. *logs*) na tvrdi disk i čuvanje dokaza te zapisivanje svih osoba koje su pristupile dokazu. Dokaze je najbolje što ranije i zakonito prikupiti, potrebno je napraviti kriptografski provjerljive kopije, presnimiti originalne dokaze pod ograničenim pristupom, analizirati samo kopije, koristiti ugledne i pouzdane alate te dokumentirati svaku radnju.[16] U pravnom sustavu, bilo u Sjedinjenim Američkim Državama ili Europi, spominju se različite vrste dokaza – pravi, najbolji, direktni, indirektni, prepričavanje ili *hearsay* dokazi i digitalni te mrežni dokazi. Pravi dokazi se odnose na fizičke ili opipljive predmete koji su relevantni za slučaj – oružje ubojstva, otisak prsta/cipele, potpisani ugovor, tvrdi disk, USB ili računalo. Najbolji dokazi su oni koji će najbolje poslužiti na sudu umjesto originala – fotografija mjesta zločina, kopija potpisanog ugovora, datoteka iz tvrdog diska ili snimka mrežnog prometa. Direktni dokazi su izjave svjedoka koji su se našli na mjestu zločina – "Vidjela sam ga s tim USB uređajem." ili "Gledao sam ga kako pokušava otkriti zaporku s tim alatom.". Indirektni dokazi ne podržavaju konkretan zaključak, ali mogu biti povezani s drugim dokazima koji vode do zaključka – potpis elektroničke pošte, datoteka sa zaporkama na računalu osumnjičenika ili serijski broj USB uređaja. *Hearsay* dokazi su izjave osoba koje nisu bile direktan svjedok čina

[15] Dokaz. Proleksis Enciklopedija. Preuzeto sa: http://proleksis.lzmk.hr/18159/ (13.05.2018.)
[16] Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace. Upper Saddle River, New Jersey: Prentice Hall. (13.05.2018.)

– “Rekao mi je da je to učinio.” ili “Vidjela sam snimku čina.”. Također, u dokaze se uključuju i poslovne evidencije poput ugovora, računa isplate i drugih.[17]

3.1. Digitalni i mrežni dokazi

Digitalni dokaz je svaka dokumentacija koja zadovoljava zahtjev dokaza u sudskom postupku, a postoji u digitalnom obliku. Primjeri digitalnih dokaza su elektronička pošta, IM sesije, bankovni računi, zapisnici pristupa i drugi. Potencijalni digitalni dokazi su i adresari, elektronička pošta, audio i video datoteke, slikovne datoteke, kalendari, baze podataka, tablice, šifrirane datoteke, skrivene datoteke, sigurnosne kopije, zapisne datoteke, datoteke za konfiguraciju, ispisne datoteke, kolačići, sistemske datoteke, povijest preglednika, privremene datoteke, dokumenti i mnogi drugi.[18]

Mrežni dokazi su digitalni dokazi koji su rezultat komunikacije preko mreže. Primjerice mrežni dokazi su također elektronička pošta i IM sesije, ali i aktivnost preglednika i elektroničke pošte na mreži, zapisnici paketa i drugi. Mrežni dokazi predstavljaju mnoge izazove forenzičarima. Prikupljanje (eng. *acquisition*) mrežnih dokaza je jedan od tih izazova. Samo lociranje pojedinih dokaza predstavlja problem. Mreža sadržava velik broj izvora dokaza – od bežičnih pristupnih točaka do mrežnih posrednika i središnjih poslužitelja. Iako je moguće saznati lokaciju dokaza, također problem predstavlja pristup dokazu zbog pravnih ili tehničkih razloga. Drugi izazov mrežnih dokaza je njihov sadržaj. Mrežni uređaji mogu, ali i ne moraju sadržavati sve detalje i metapodatke dokaza te često imaju ograničeni kapacitet pohrane. Mrežni uređaji ne koriste sekundarnu ili trajnu pohranu, a posljedica toga su nestabilni podaci, koji bi se izgubili pri resetiranju uređaja. Privatnost predstavlja još jedan problem, pogotovo kod prikupljanja podataka na Internetu gdje privatnost ni ne postoji. Zbrinjavanje tvrdog diska može biti problem pojedincu ili organizaciji, ali je moguće izraditi kopije izvornika tako da kritične operacije mogu nastaviti s daljnjom istragom. S druge strane, zbrinjavanje mrežnog uređaja predstavlja veći izazov. U ekstremnim slučajevima cijeli dio mreže se može srušiti na neodređeno vrijeme. Posljednji izazov mrežnih forenzičara je prihvatljivost – mrežni dokazi nisu još dio većine zakona, ali se predviđa da će postati standard zbog povećanja stope kibernetičkog kriminala.[19]

[17] Ibid.
[18] Protrka, N. (2011). Računalni podaci kao elektronički (digitalni) dokazi. Policija i sigurnost, 20 (1), 1-13. Preuzeto s https://hrcak.srce.hr/79204 (14.05.2018.)
[19] Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace. Upper Saddle River, New Jersey: Prentice Hall. (14.05.2018.)

Mrežni dokazi se mogu prikupiti iz mnogo izvora. Svaki izvor ima svoju vrijednost za mrežnog forenzičara. Izvori mogu biti žičani (eng. *on the wire*) i bežični (eng. *in the air*), preklopnici (eng. *switches*), usmjernici (eng. *routers*), DHCP poslužitelji (eng. *Dynamic Host Configuration Protocol server*), imenski poslužitelji (eng. *name servers*), poslužitelji za autentikaciju (eng. *authentication servers*), sustavi za detekciju/prevenciju mrežnih upada (eng. *network intrusion detection/prevention systems*), vatrozidi (eng. *firewalls*), mrežni posrednici (eng. *web proxies*), aplikacijski poslužitelji (eng. *application servers*) i centralni zapisnički poslužitelji (eng. *central log servers*). Žičani izvori omogućavaju povezivanje mreže, a to su bakrene upletene parice (eng. *twisted pair*) ili koaksijalni kabeli. Danas su sve češći i optički kabeli, koji se sastoje od optičkih vlakana unutar svjetlovoda. Vrijednost ovih izvora je u tome što forenzičari mogu spojiti prislušne uređaje da bi kopirali i sačuvali mrežni promet. Osim žičanih izvora, postoje i bežični koji se sastoje od radio frekvencijskih valova. Forenzičari kod ovih izvora mogu doći do prometa koji je najčešće šifriran. U tom slučaju mogu legitimno doći do ključa i dešifrirati kôd te saznati podatke poput MAC adrese uređaja, ali i do mrežnih paketa. Preklopnici su mostovi koji fizički spajaju brojne stanice ili mrežne dijelove da bi stvorili lokalnu mrežu. Oni sadrže CAM tablicu (eng. *Content Addressable Memory*), koja pohranjuje putanje između fizičkih priključaka i svake MAC adrese mrežne kartice. Otkrije li mrežni forenzičar MAC adresu uređaja, lako će pronaći napadača povezanog s tim uređajem. Usmjerivači povezuju podmreže ili mreže i olakšavaju prijenos paketa između različitih mrežnih segmenata, čak i kada imaju različite sheme adresiranja. Preklopnici sadrže CAM tablice, a usmjernici tablice usmjeravanja, koje pohranjuju putanje od priključaka do mreže. Tako omogućavaju mrežnom forenzičaru praćenje mrežnog prometa prema drugim mrežama. DHCP poslužitelji dodjeljuju IP adrese uređajima lokalne mreže, kako bi mogli komunicirati s drugim uređajima na lokalnoj mreži, kao i drugim povezanim sustavima. To omogućava praćenje IP adrese pomoću zapisa koji je evidentiran pri dodjeljivanju same adrese. Imenski poslužitelji povezuju IP adrese s ljudski-čitljivim imenima sustava i mreža. Poslužitelji za provjeru autentičnosti pružaju centralizirane usluge provjere autentičnosti korisnicima diljem organizacije tako da se korisničkim računima može upravljati na jednom mjestu. Pri svakoj prijavi evidentira se zapis i tako se mogu otkriti napadi na zaporke ili prijave u sumnjivo vrijeme ili s neuobičajenih lokacija. Sustavi za detekciju/prevenciju mrežnih upada su namijenjeni pružanju pravodobnih podataka koji se odnose na štetne događaje na mreži. Vatrozidi su specijalizirani usmjerivači koji obavljaju dublji pregled mrežnog prometa kako bi se odlučili koji promet bi trebao biti proslijeđen, a koji odbijen. Mrežni posrednici se koriste kako bi poboljšali svojstva uređaja lokalnim

međuspremanjem (eng. *cachingom)* mrežnih stranica ili za prijavu, pregled i filtriranje mrežnog prometa. Mrežni posrednik može dopustiti ili odbiti zahtjev za mrežnu stranicu (često na temelju objavljenih crnih listi poznatih neprikladnih ili zlonamjernih mrežnih mjesta ili na ključnim riječima u izlaznom prometu). Aplikacijski poslužitelji uključuju poslužitelje baza podataka, mreže, elektroničke pošte, poslužitelje čavrljanja (eng. *chat servers)*, govorne pošte i VoIP poslužitelje (eng. *Voice over Internet Protocol servers*). Centralni zapisnički poslužitelji pomažu prepoznati i riješiti sigurnosne incidente na mreži.[20] Svatko ostavlja otisak, pa tako i forenzičari, u kontekstu mrežne forenzike taj otisak može biti i fizički, ali se uglavnom odnosi na otisak na mreži. Otisak na mreži može utjecati na podatke, ali i sam proces prikupljanja dokaza te zato mrežni forenzičari moraju veoma oprezno obavljati svoj posao. [21]

3.1.1. Aktivno i pasivno prikupljanje dokaza

Mrežni forenzičari spominju "pasivno" u odnosu na "aktivno" prikupljanje dokaza. Pasivno prikupljanje dokaza je praksa prikupljanja dokaza iz mreže bez emitiranja podataka na drugom sloju (podatkovnom sloju OSI modela) i slojevima iznad. Prikupljanje mrežnog prometa je zapravo pasivno prikupljanje. Aktivno ili interaktivno prikupljanje dokaza je praksa prikupljanja dokaza interakcijom s uređajima na mreži. To može uključivati prijave na mrežne uređaje putem konzole ili mrežnog sučelja i skeniranje mrežnih priključaka za određivanje trenutnog stanja. [22]

3.1.2. Fizičko presretanje

Fizičkim presretanjem (eng. *physical interception*) moguće je doći do mrežnog prometa bez slanja ili mijenjanja podataka na mreži. Iako je teško prikupiti dokaze bez ostavljanja otisaka, proces snimanja ili prisluškivanja (eng. *capturing/sniffing*) prometa se ne može provesti bez utjecaja na okolinu. Postoji velik broj načina prijenosa podataka preko fizičkih medija i jednako mnogo načina presretanja tih podataka. Najbolji primjer je uređaj povezan s drugim uređajem preko bakrenog kabela. Napon na bakru se lako može pojačati i redistribuirati. Koncentratori (eng. *hubs*) i preklopnici (eng. *switches*) dizajnirani su kako bi proširili signale fizičkih medija s dodatnim uređajima. Forenzičari mogu i pasivno prikupiti mrežni promet presretanjem, jer se prenosi preko kabela, zrakom ili putem mrežne opreme. Fizičko

[20] Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace. Upper Saddle River, New Jersey: Prentice Hall. (14.05.2018.)
[21] Ibid.
[22] Ibid.

presretanje se odnosi na bakrene i optičke kabele, radio frekvenciju (bežični promet), koncentratore i preklopnike.

3.1.3. Programi za praćenje prometa

Nakon dobivanja fizičkog pristupa mrežnom prometu, potreban je program za snimanje istog. Najpoznatije programske biblioteke(eng. *libraries*) za snimanje, parsiranje i analizu paketa su libpcap/tcpdump (http://www.tcpdump.org/) i WinPcap (https://www.winpcap.org/). Najčešće korišteni alati temeljeni na tim bibliotekama su tcpdump i Wireshark. Opisat ću i metode filtriranja prometa tijekom i nakon snimanja, budući da se važnost filtriranja ističe zbog povećanja prometa na mreži. Libpcap je UNIX C biblioteka koja pruža API (eng. *Application programming interface*) za snimanje i filtriranje podataka na podatkovnom sloju mreže, koju je 1994. godine razvio Nacionalni laboratorij Lawrence Berkeley. Pet godina kasnije, objavljena je biblioteka WinPcap za operacijski sustav Windows. Obje biblioteke su besplatne i otvorenog koda. Mnogi alati temeljeni na libpcapu imaju posebne funkcije, poput mogućnosti spajanja snimljenih paketa, razdvajanje snimki po TCP tokovima ili redovno pretraživanje sadržaja paketa. Libpcap uključuje jezik filtriranja Berkeley Packet Filter (BPF). Koristeći BPF filtre, možete odrediti koji će se promet snimati i pregledavati, a koji ignorirati. Tcpdump je prvi alat za snimanje, filtriranje i analizu mrežnog prometa, razvijen iz libpcap biblioteke. Osnovna svrha tcpdumpa je snimanje mrežnog prometa, a zatim ispisivanje ili pohrana sadržaja za analizu. Wireshark je grafički, otvoreni alat za snimanje prometa. Ima jednostavno grafičko korisničko sučelje što ga čini odličnim alatom za početnike u mrežnoj forenzici. Neke od mogućnosti Wiresharka su filtriranje paketa, dešifriranje protokola i podrška za PDML jezik (eng. *Packet Details Markup Languag*e). Razvio ga je Gerald Combs 1998. godine i tada se nazivao Ethereal, a 2006. je preimenovan u Wireshark. Ovaj alat omogućava prikaz paketa u realnom vremenu, a zbog mogućnosti analize protokola potrebna mu je velika procesorska snaga. Tshark je alat koji sadrži terminal za analizu protokola u sklopu Wiresharka. Dumpcap je također specijalizirani alat Wiresharka, koji omogućava snimanje paketa, ali uz manje procesorske snage. Potrebno je imati dobar procesor za ove alate, jer ako se preoptereti, podaci i paketi mogu biti izgubljeni.[23]

[23] Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace. Upper Saddle River, New Jersey: Prentice Hall. (14.05.2018.)

3.1.4. Aktivno prikupljanje dokaza

Aktivno prikupljanje dokaza modificira okolinu. Mrežni forenzičari moraju biti svjesni da prikupljanje dokaza mijenja okolinu i uređaje i trebali bi raditi svoj posao na način uz što manje utjecaja na te promjene. Moguće je dobiti pristup uređajima koji su aktivni na mreži na sljedeće načine: konzolom, *Secure Shellom* (SSH), *Secure Copy* (SCP) i *SSH File Transfer* protokolima (SFTP), *Simple Network Management* protokolom (SNMP), *Trivial File Transfer* protokolom (TFTP) i mrežnim sučeljem. Konzola je sustav za unos i prikaz, najčešće tipkovnica i monitor povezani s računalom. Mnogi mrežni uređaji imaju serijski priključak koji služi za povezivanje terminala s konzolom. U današnjoj praksi, moguće je povezati laptope i stolna računala na serijsku konzolu mrežnih uređaja pomoću USB adaptera. *Secure Shell* (SSH) je protokol kojim je moguće prikupiti dokaze udaljenim pristupom. SSH šifrira podatke za autentikaciju i podatke u tranzitu, što znači da čak i ako se promet presreće (*intercept*), napadač ne može vratiti korisničko ime, zaporku ili sadržaj komunikacije. SSH implementira SCP protokol, koji služi za prijenos datoteka između umreženih sustava. SNMP ili *Simple Network Management Protocol* je jedan od najviše korištenih protokola za kontrolu i upravljanje mrežnih. Najčešće služi kao medij za komunikaciju i prikupljanje podataka o upravljanju mreže i sigurnosnih podataka. U mrežnoj forenzici SNMP se koristi na dva načina: kao upozorenja vezana za događaje i za konfiguracijske upite. TFTP ili *Trivial File Transfer Protocol* se koristi za prijenos datoteka među udaljenim sustavima, iako je manje siguran od drugih protokola. Mrežni forenzičari ga koriste za izvoz datoteka s usmjernika, preklopnika ili drugog uređaja koji ne podržava SCP ili SFTP. Mrežna sučelja se mogu pristupiti putem HyperText Transfer protokola ili HyperText Transfer Secure protokola. Popularna su jer prijenosna i korisnik ne treba instalirati poseban klijent da bi pristupio uređaju. Najveći nedostatak im je zapisivanje forenzičkih aktivnosti. Istraga se također može provoditi bez pristupa, u slučaju da forenzičar nema zaporku ili slično. Podatke o konfiguraciji ili stanju uređaja moguće je prikupiti vanjskom istragom pomoću skeniranja priključaka i ranjivosti. Skeniranja priključaka provodi se pomoću alata nmap (https://nmap.org/). Nmap omogućava učinkovito dohvaćanje informacija o otvorenim priključcima i verzijama programa na uređaju. Skeniranje ranjivosti je drugi način vanjske istrage. Pretraživači ranjivosti (eng. *vulnerability scanners*) ispituju velik broj poznatih ranjivosti na ciljanim sustavima. Oba načina su aktivni procesi, jer generiraju mrežni promet i mijenjaju stanje ciljanog uređaja, a pri skeniranju ranjivosti sustav može u potpunosti pasti, pa je potrebno biti vrlo oprezan.

Forenzičari će u svakom trenutku istrage ostaviti otisak i više njih, ovisno o tome koliko će virtualnih mjesta posjetiti tražeći valjane dokaze. Na sreću, postoje načini da se smanji utjecaj na okolinu. Ukratko, savjeti za provođenje istrage uz što manji broj otisaka su: ne isključiti ili resetirati uređaje, spojiti se putem konzole, a ne mreže, zapisivati vrijeme sustava na kojem se istražuje, prikupljati dokaze s obzirom na razinu promjenjivosti i zapisivati aktivnosti tijekom istrage.[24]

[24] Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace. Upper Saddle River, New Jersey: Prentice Hall. (14.05.2018.)

4. Mrežna forenzika u praksi

4.1. Slučaj – krađa bolničkog laptopa

Liječnica prijavljuje da joj je ukraden laptop iz ureda u bolnici. Iako laptop ima zaporku, tvrdi disk nije šifriran. Liječnica tvrdi da se na laptopu nalaze kopije laboratorijskih rezultata pacijenata, zaštićene zdravstvene informacije iz privitaka elektroničke pošte, imena, datumi rođenja i identifikacijski brojevi pacijenata, bilješke vezane uz posjetu i dijagnoze. Potrebno je obavijestiti pacijente čije su informacije ukradene, ali i medije što bi utjecalo na reputaciju bolnice i financijski gubitak. Forenzičari prvo moraju odrediti kada je laptop ukraden ili saznati kada ga je liječnica zadnji put koristila. Saznajući kad ga je zadnji put koristila, mogu početi s pregledavanjem snimki kamera u bolnici i zapisnika pristupa (eng. *access logs*). Zatim pregledavaju zapisnike pristupa mreže, da bi saznali je li laptop bio povezan s mrežom bolnice nakon krađe i s koje lokacije. Mrežni dokazi uključuju i zapisnike bežičnih pristupnih točaka (eng.*wireless access point logs*), zapisnike DHCP-a (eng. *Dynamic Host Control Protocol (DHCP) lease assignment logs),* događaje aktivnog direktorija (eng. *Active Directory events*), zapisnike mrežnog posrednika (eng.*web proxy logs*) i program za praćenje laptopa kao što je Lojack (https://www.absolutelojack.com/). Također, forenzičari trebaju otkriti koje su se informacije pacijenata nalazile na laptopu. Zapisnici elektroničke pošte mogu otkriti koji su privitci preuzeti, a poslužitelj elektroničke pošte bolnice sadrži kopije sve poslane i primljene elektroničke pošte, što je korisno u sastavljanje liste pacijenata čiji su podaci ugroženi. Otkrivajući točno vrijeme krađe putem zapisnika bežičnih pristupnih točaka, forenzičari prate laptop do garaže za posjetitelje. Kamere u garaži otkrivaju lice kradljivca, a video snimka je poslana policiji koja je saznala registracije auta i uspjela identificirati kradljivca. Laptop je pronađen među hrpom drugih uređaja. Analiza tvrdog diska je utvrdila da laptop nije bio uključen nakon krađe i zaključeno je da podaci o pacijentima nisu procurile. Kao odgovor na incident, bolnica je postavila šifre na sve tvrde diskove i uvela alate za fizičko zaključavanje laptopa.[25]

[25] Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace. Upper Saddle River, New Jersey: Prentice Hall. (17.05.2018.)

4.2. Obrazovanje

Pitanje koje je postavljeno na konferenciji o istraživanju digitalne forenzike 2001. je glasilo koja znanja i vještine su potrebne za digitalnu forenziku. Grupe sudionika su se složile da je bolje pitanje koja znanja ne trebaju. Područja na razini fakulteta povezana s digitalnom i mrežnom forenzikom su računalna znanost, inženjering, fizika, matematika, kriminalistika, psihologija, sociologija, lingvistika, logika, statistika i vjerojatnost, kriptologija i druga.[26]

4.2.1. Hrvatska

Tehničko veleučilište u Zagrebu je 2017. godine otvorilo specijalistički diplomski stručni studij – Informacijska sigurnost i digitalna forenzika. Studij svake godine prima 35 izvanrednih studenata, traje 4 semestra, a po završetku student stječe zvanje stručni specijalist inženjer informacijske sigurnosti i digitalne forenzike. Kompetencije koje student stječe završetkom studija su primjena informacijsko-komunikacijskih tehnologija u informacijskoj sigurnosti i digitalnoj forenzici, implementacija, upravljanje i organiziranje sustava informacijske zaštite, organiziranje i upravljanje analizama digitalne forenzike i primjena zakonskih osnova informacijske sigurnosti i digitalne forenzike. Neki od kolegija na ovom studiju su: zakonska osnova digitalne forenzike, matematički modeli sigurnosti, sigurnost mrežnih aplikacija, primijenjena kriptografija, sigurnost računalnih mreža, etičko hakiranje, forenzika mobilnih uređaja i tehnike sigurnog programiranja. [27] Split, uz Zagreb, jedini u Hrvatskoj ima diplomski studij forenzike. Za razliku od TVZ-a, Odjel za forenzične znanosti u Splitu, nudi niz kolegija iz kriminalistike, prava i računovodstva, kao što su istraživanje mjesta događaja, kazneno procesno pravo i gospodarski kriminalitet. Većina kolegija vezana su uz poddiscipline forenzike, pa imaju forenzičnu antropologiju, veterinarsku forenziku i računalnu forenziku kao obavezan kolegij prvog semestra.[28]

[26] Digital Forensics Research Workshop. "A Road Map for Digital Forensics Research" 2001. http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf (18.05.2018.)
[27] Digitalna forenzika // Diplomski. Tehničko veleučilište u Zagrebu. Preuzeto sa: https://www.tvz.hr/studiji/digitalna-forenzika/diplomski (18.05.2018.)
[28] Diplomski sveučilišni studij forenzike. Sveučilišni odjel za forenzične znanosti. Preuzeto sa: http://forenzika.unist.hr/Nastava/Diplomskisveu%C4%8Dili%C5%A1nistudijforenzike/tabid/497/Default.aspx (18.05.2018.)

4.2.2. Kanada i SAD

U Americi sveučilišta nude velik broj edukacija mrežne i digitalne forenzike na preddiplomskoj i diplomskoj razini, ali i certifikacije istih. Navest ću nekoliko programa koji se mogu pohađati i na mreži. Ryerson University u Torontu nudi preddiplomski certifikat u računalnoj sigurnosti i digitalnoj forenzici. Potrebno je proći osam kolegija unutar šest godina za certifikat. Neki od kolegija su sigurnost računalnih mreža, računalna kriptografija i digitalna steganografija, sustavi digitalne forenzike, arhitektura i dizajn sigurnosti.[29] Stevenson University u Marylandu nudi diplomu za magistra znanosti u digitalnoj forenzici. Kolegiji koji se provode u ovom programu su sigurnost elektroničkih sustava, mrežna i cloud forenzika, kibernetički terorizam i drugi. Boston University Metropolitan College u Bostonu nudi certifikat na diplomskoj razini. Iako se većina kolegija provodi na mreži, studenti moraju prisustvovati na četiri predavanja svaki semestar. Da bi dobili certifikat moraju proći četiri kolegija i imaju mogućnost upisati diplomski studij računalnih informacijskih sustava na istom fakultetu. Kolegiji uključuju komunikaciju poslovnih podataka, digitalnu forenziku i istrage i mrežnu forenziku.[30] Utica College u New Yorku ima diplomske i preddiplomske studije kibernetičke sigurnosti sa specijalizacijom u računalnoj forenzici, mrežnoj forenzici i kibernetičkom kriminalu. Po završetku preddiplomskog specijalističkog studija mrežne forenzike studenti mogu raditi u administraciji mrežne sigurnosti, digitalnoj forenzici, kao ispitivači probojnosti (eng. *penetration tester)* i savjetnici IT sigurnosti.[31] National University u San Diegu, također nudi specijalizaciju u digitalnoj forenzici na diplomskoj razini. Studenti na ovom studiju uče prikupiti i analizirati digitalne dokaze, otkrivati upade u sustave, otkrivati viruse i istraživati legalne probleme vezane za digitalnu forenziku. Kolegiji unutar kurikuluma uključuju principe i tehnologije digitalne forenzike, principe forenzike baza podataka i etičko hakiranje. Pri završetku studija studenti mogu raditi kao specijalisti digitalne forenzike i u korisničkoj podršci za odgovaranje na računalne incidente (eng. *Computer Incident Responders).*[32]

[29] Computer security and Digital Forensics. Ryerson University – The Chang School of Continuing Education. Preuzeto sa: https://ce-online.ryerson.ca/ce/default.aspx?id=3359 (18.05.2018.)
[30] 15 Universities with Online Computer Forensics Programs. Forensics Colleges. Preuzeto sa: https://www.forensicscolleges.com/blogs/15-universities-with-online-computer-forensics-programs (18.05.2018.)
[31] 17 Best Schools with Online Computer Forensics Programs. Cyber Degrees. Preuzeto sa: https://www.cyberdegrees.org/listings/best-online-computer-forensics-programs/ (18.05.2018.)
[32] National University's Nationally-Recognized Cyber Security Program Adds Focus in Computer Forensics. National University. Preuzeto sa: https://www.nu.edu/News/2014-CyberSecurityProgramAddsFocusinComputerForensi.html (18.05.2018.)

4.3. Certifikacija

Osim mnogih sveučilišnih programa, postoje i tečajevi vezani za mrežnu forenziku. Dobivanjem certifikata za etičkog hakera, analitičara sigurnosti (eng. *security analyst*) ili ispitivača probojnosti možete biti korak bliži prema karijeri u mrežnoj forenzici. Tečajevi za ove profesije postoje na mreži uz certifikate ili bez njih. U Hrvatskoj, Otvoreno učilište Algebra nudi tečaj etičkog hakiranja i polaganje za certifikat. U svijetu je, za navedene certifikate, najpoznatiji EC-Council. EC-Council ili International Council of E-Commerce Consultants je najveće svjetsko tijelo za certifikacije vezane za kibernetičku sigurnost. Najpoznatiji programi koje EC-Council nudi su certificirani etički haker (eng. *Certified Ethical Hacker*), istražitelj forenzike za računalne upade (eng. *Computer Hacking Forensics Investigator*), certificirani analitičar sigurnosti (eng. *Certified Security Analyst*) i licencirani ispitivač probojnosti (eng. *Licensed Penetration Tester*).[33] Osim certifikacije EC-Council ima i svoje akademske programe. Sveučilište se sastoji od preddiplomskog studija kibernetičke sigurnosti u trajanju od dvije godine, diplomskih studija digitalne forenzike, IT analize i drugih i specijalizacija na razini magistra znanosti u području digitalne forenzike, sigurnosne arhitekture i drugih.[34] Pobliže ću objasniti tri razine certifikacije, počevši s temeljnom razinom etičkog hakera, preko napredne razine analitičara sigurnosti do zadnje, stručne razine ispitivača probojnosti. Prije temeljne razine etičkog hakera, potrebno je položiti i program za certificiranog mrežni branitelj (eng. *Certified Network Defender)*, a nakon temeljne i napredne razine i praktični dio etičkog hakiranja i analize sigurnosti.[35]

4.3.1. Mrežni branitelj

Temeljni certifikat koji se treba položiti da bi se uopće moglo krenuti s etičkim hakiranjem je *Certified Network Defender* (CND). To je sveobuhvatni tečaj mrežne sigurnosti. Program priprema mrežne administratore na tehnologije za zaštitu, otkrivanje i odgovore upada na mrežu. Sadrži praktične vježbe u najpoznatijim alatima za mrežnu sigurnost. Polaznici na tečaju uče razne kontrole, protokole i uređaje mrežne sigurnosti. Polaganjem certifikata moći će otkriti različite prijetnje na mreži te ih otkloniti. Ovaj tečaj se preporučuje mrežnim

[33] About Us. EC-Council. Preuzeto sa: https://www.eccouncil.org/about/ (23.05.2018.)
[34] Academics. EC-Council University. Preuzeto sa: https://www.eccu.edu/academics/ (23.05.2018.)
[35] Certified Ethical Hacker Certification. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (23.05.2018.)

administratorima te administratorima i inženjerima mrežne sigurnosti, ali i tehničarima, analitičarima i operatorima.[36]

4.3.2. Etički haker

Nakon CND-a slijedi Certified Ethical Hacker (CEH). Ovlašteni etički haker je stručnjak koji razumije i zna kako tražiti slabosti i ranjivosti u ciljanim sustavima te koristi znanja i alate kao zlonamjerni haker, ali na zakonit legitiman način kako bi procijenio sigurnost samih sustava.[37] Ovaj program je najpoželjniji kod stručnjaka za informacijsku sigurnost. Tečaj se sastoji od preko 140 praktičnih vježbi, 2200 poznatih hakerskih alata i više od 1700 vizualno bogatih slajdova. Ova certifikacija se preporučuje sigurnosnim stručnjacima, revizorima, administratorima mrežnih stranica i svima kojima se bave mrežnom infrastrukturom. Tečaj sadrži sljedećih 20 modula, a neki od njih su: ostavljanje otisaka i izviđanje, skeniranje mreža, analiza ranjivosti, hakiranje sustava, prijetnje zlonamjernih programa, snimanje prometa, socijalni inženjering, hakiranje mrežnih poslužitelja i aplikacija, hakiranje bežične mreže i mobilnih platformi, kriptografija i drugi.[38] Prije kretanja na iduću razinu, potrebno je položiti praktični dio CEH-a. Ispit traje šest sati i potrebno je pokazati praktičnu primjenu etičkog hakiranja, odnosno vještine poput prepoznavanja prijetnji, skeniranja mreže, analiziranja ranjivosti i hakiranja. Ispit se sastoji od 20 situacija iz stvarnog života - oponaša pravu korporacijsku mrežu kroz virtualne mašine, mreže i aplikacije. [39]

[36] Certified Network Defender Certification. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-network-defender-cnd/ (24.05.2018.)
[37] Certified Ethical Hacker Certification. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (24.05.2018.)
[38] Certified Ethical Hacker Certification. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (24.05.2018.)
[39] Certified Ethical Hacker Practical. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh-practical/ (24.05.2018.)

4.3.3. Sigurnosni analitičar

Nakon temeljne razine slijedi napredna razina koja se sastoji od EC-Council Certified Security Analysta i njegovog praktičnog dijela. Ovaj certifikat se preporučuje etičkim hakerima, ispitivačima probojnosti, sigurnosnim inženjerima, administratorima mrežnih poslužitelja i vatrozida, ispitivačima sigurnosti, administratorima sustava i stručnjacima za procjenu rizika. Tečaj se fokusira na metodologiju ispitivanja probojnosti na mreži, u socijalnom inženjeringu, mrežnim aplikacijama, bazama podataka, bežičnom prometu i oblaku.[40] Praktičan dio se sastoji od 8 izazova u simuliranoj organizaciji i mreži s više domaćina. Polaznici moraju demonstrirati primjenu metodologije ispitivanja probojnosti za obavljanje sveobuhvatne sigurnosne revizije organizacije. [41]

4.3.4. Ispitivač probojnosti

Posljednja, stručna razina naziva se Licensed Penetration Tester (LPT). Ispit se u potpunosti polaže na mreži, traje ukupno 18 sati i sastoji se od 9 izazova – za certifikat je potrebno riješiti 5 zadataka. Od polaznika se očekuje da pokažu metodički pristup testiranju i potvrđivanju sigurnosti sustava. Tečaj se sastoji od 9 modula, od kojih su neki uvod u procjenu ranjivosti i ispitivanje probojnosti, metodologija prikupljanja informacija, prepoznavanje i iskorištavanje ranjivosti, priprema izvješća i praktičan dio. Nakon certifikata, polaznik će moći koristiti tehnike i koncepte poput iskorištavanje ranjivosti operacijskog sustava, ubacivanje SQL-a (eng. *SQL injection*), iskorištavanje ranjivosti pomoću udaljenih (eng. *RFI Remote File Inclusion*) ili lokalnih datoteka (eng. *LFI – Local File Inclusion*) i druge. Za ovaj tečaj preporučuje se znanje skriptnih jezika poput Perla, Pythona ili Rubyja, jer je potrebno pisanje skripti zbog rješavanja mehanizama zaštite na temelju potpisa i anomalija.[42]

[40] EC-Council Certified Security Analyst ECSA: Penetration Testing. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-security-analyst-ecsa/ (24.05.2018.)
[41] EC-Council Certified Security Analyst Practical. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-security-analyst-ecsa-practical/ (24.05.2018.)
[42]The LPT (Master) Training Program: Advanced Penetration Testing Course. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/licensed-penetration-tester-lpt-master/ (24.05.2018.)

5. CERT

5.1. Uloga i misija

CERT (eng. *Computer Emergency Response Team*) ili CSIRT (eng. *Computer Security Incident Response Team*) je organizacijski entitet koji reagira na računalno-sigurnosne incidente te preventivnim djelovanjem radi na poboljšanju računalne sigurnosti informacijskih sustava. Nacionalni CERT osnovan je u skladu sa Zakonom o informacijskoj sigurnosti Republike Hrvatske. Jedna od glavnih zadaća je usklađivanje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalim u Republici Hrvatskoj, ili u drugim zemljama i organizacijama, ako su povezani s Republikom Hrvatskom. Nacionalni CERT se bavi incidentom, ako se jedna od strana u incidentu nalazi u Hrvatskoj (odnosno, ako je u .hr domeni ili u hrvatskom IP adresnom prostoru). U okviru svog djelovanja provodi proaktivne i reaktivne mjere. Proaktivne mjere se provode prije incidenta ili drugih događaja koji mogu ugroziti sigurnost informacijskih sustava, a u cilju sprječavanja ili ublažavanja mogućih šteta. Informacije o proaktivnim mjerama su javne. Proaktivne mjere podrazumijevaju sigurnosne obavijesti, praćenje računalno-sigurnosnih tehnologija, diseminacija informacija iz područja računalne sigurnosti, unapređenje svijesti o značaju računalne sigurnosti i edukacija i obuka o računalnoj sigurnosti. Reaktivne mjere se provode nakon što se incident ili drugi događaj koji može ugroziti sigurnosti informacijskih sustava dogodio. Reaktivne mjere podrazumijevaju sigurnosna upozorenja, sigurnosne preporuke i koordinacija rješavanja značajnijih incidenata. Prema prioritetu, incidenti se rješavaju sljedećim redoslijedom:

1. Incidenti kao potencijalna ugroza za živote ljudi
2. Incidenti koji uključuju infrastrukturu Interneta u Republici Hrvatskoj
3. Incidenti značajnog opsega
4. Nove vrste ugrožavanja računalne sigurnosti
5. Ostali incidenti

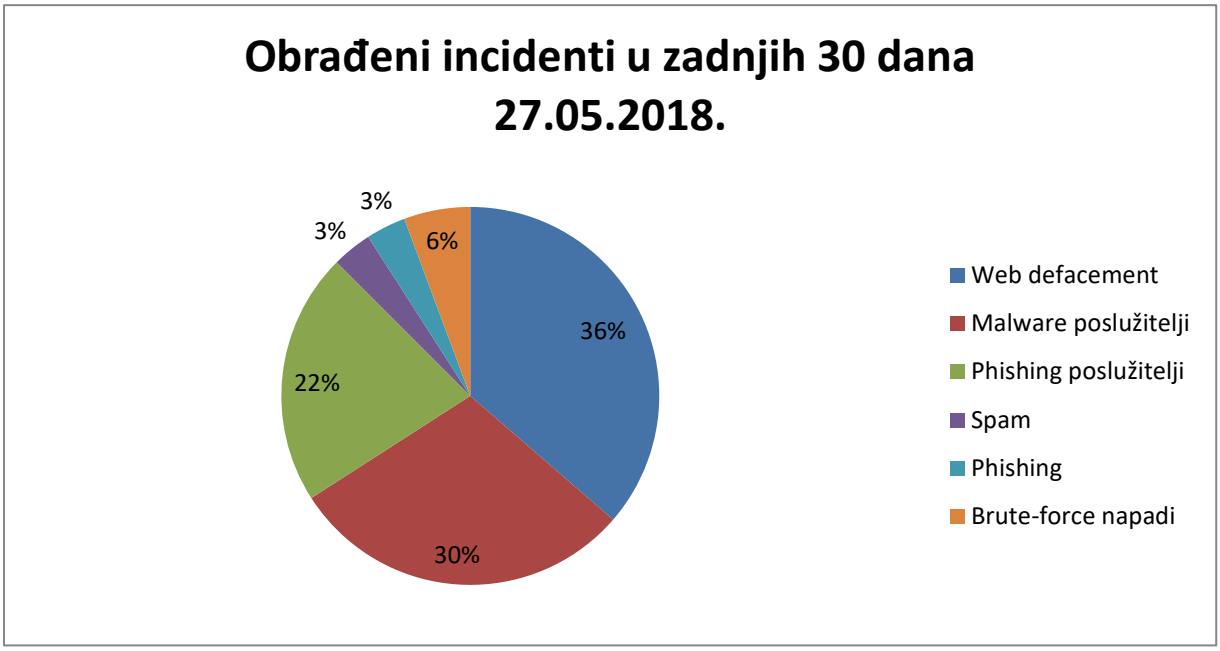
CERT surađuje sa Zavodom za sigurnost informacijskih sustava, Uredom vijeća za nacionalnu sigurnost, Ministarstvom unutarnjih poslova te Ministarstvom obrane i sa stranim CERT-ovima. U djelokrug rada Nacionalnog CERT-a nije uključeno: operativno rješavanje problema i briga o sigurnosti pojedinih sustava, kažnjavanje problematičnih korisnika, arbitraža u sporovima i pokretanje kaznenih prijava.[43]

[43] O nacionalnom CERT-u. CERT.hr. Preuzeto sa: https://www.cert.hr/onama/ (26.05.2018.)

5.2. Izvještaji nacionalnog CERT-a

Nacionalni sustav ranog upozoravanja (SRU@HR) CERT-a obrađuje napade i incidente poput web defacementa, zlonamjernih i phishing poslužitelja, spama i phishing incidenata te brute force napada. *Web defacement* je napad na mrežnu stranicu kojim se mijenja izgled sjedišta ili stranice. Ovaj napad najčešće izvode crackeri sustava koji provaljuju u mrežne poslužitelje i zamjenjuju mrežnu stranicu sa svojom.[44] Ciljane stranice web defacementa su uglavnom stranice religioznog sadržaja, stranice povezane s vladom i politikom i stranice korporacija.[45] Hrvatski hakeri su 2016. godine napali stranicu tvrtke Acunetix koja proizvodi softver za sigurnost mrežnih stranica.[46] *Phishing* je kibernetički napad kojim se napadač predstavlja kao legitimna ustanova, najčešće putem elektroničke pošte, telefona ili SMS poruke, kako bi ukrao osobne podatke pojedinca. Ti podaci uključuju identifikacijske informacije, bankovne podatke i podatke kreditnih kartica, zaporke i ostalo, a mogu napadaču poslužiti za pristup korisničkim računima, krađu identiteta ili novaca.[47] Jedan od poznatijih phishing napada u Hrvatskoj, zabilježen je 2017. godine kada se pošiljatelj elektroničke pošte predstavljao kao FINA. Naslov poruke je glasio Elektronička obavijest o pokretanju ovršnog postupka, a u tekst poruke umetnut je phishing URL koji korisniku nudi preuzimanje zlonamjerne datoteke.[48] *Spam* je neželjena elektronička poruka poslana zbog namjere oglašavanja raznog propagandnog sadržaja, ili u svrhu phishing napada, ili kao sredstvo distribucije poveznica do zlonamjernog softvera.[49] *Brute force* napad ili napad uzastopnim pokušavanjem je jednostavna, ali uspješna tehnika rješavanja problema koja se sastoji od sustavnog pronalaženja svih mogućih kandidata za rješenje i isprobavanja svakog od njih. Brute force napad je jednostavan za implementaciju i često se koristi za probijanje zaporki ili raznih enkripcija, a osim što je jednostavan, uvijek pronalazi rješenje, ako ono postoji.[50] Sljedeći grafikon prikazuje obrađene incidente Nacionalnog sustava ranog upozoravanja CERT-a.

[44] Website Defacement Definition. Cybercrime.org.za. Preuzeto sa: http://cybercrime.org.za/website-defacement (26.05.2018.)
[45] Website defacement. Wikipedia. Preuzeto sa: https://en.wikipedia.org/wiki/Website_defacement (26.05.2018.)
[46] Hakiran je Acunetix. CERT.hr. Preuzeto sa: https://www.cert.hr/28625/ (26.05.2018.)
[47] What is Phishing? Phishing.org. Preuzeto sa: http://www.phishing.org/what-is-phishing (26.05.2018.)
[48] Zlonamjerna kampanja putem elektroničke pošte. Mreža za IT profesionalce. Preuzeto sa: http://mreza.bug.hr/zlonamjerna-kampanja-putem-elektronicke-poste/ (26.05.2018.)
[49] Spam. CERT.hr. Preuzeto sa: https://www.cert.hr/19795-2/spam/ (26.05.2018.)
[50] Brute force napadi. Edicija dokumenata iz područja informacijskih znanosti. Preuzeto sa: https://www.cis.hr/www.edicija/Bruteforcenapadi.html (26.05.2018.)



Graf 1: Obrađeni incidenti u zadnjih 30 dana - 27.05.2018. (Izvor: https://www.cert.hr/sru/)

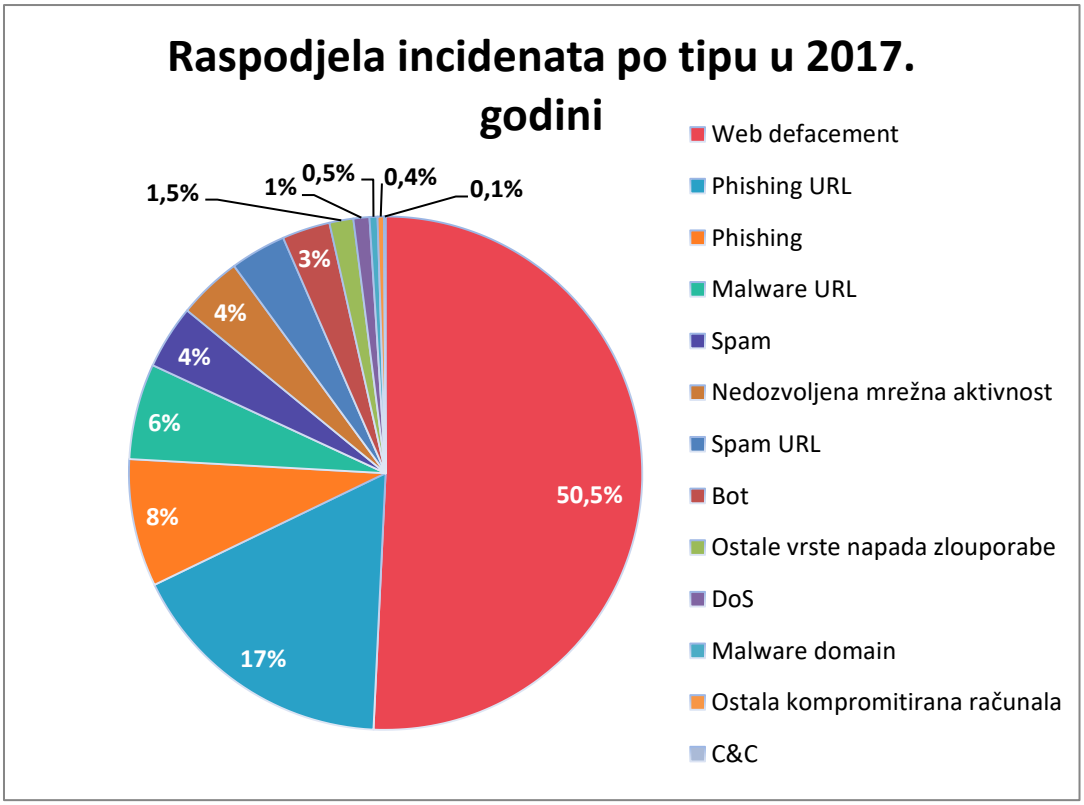
Nacionalni CERT je objavio godišnji izvještaj za 2017. godinu u kojem navodi usluge koje nudi, međunarodnu i nacionalnu suradnju, projekte, statistike i značajnije incidente, otkrivene ranjivosti i događaje. Iznijet ću nekoliko zanimljivosti iz samog izvještaja. U travnju 2017. provedena je vojna vježba "Paukova mreža" u kojoj je sudjelovalo osamdesetak pripadnika Oružanih snaga Republike Hrvatske s predstavnicima Fakulteta organizacije i informatike u Varaždinu, Zavoda za sigurnost informacijskih sustava i Nacionalnog CERT-a. "Paukova mreža" je prva nacionalna vježba iz područja obrane od kibernetičkih napada na stacionarne i razmjestive informacijsko-komunikacijske sustave. Vježbom su testirane sposobnosti sudionika za otkrivanje zlonamjernih aktivnosti na sustavima, provedba digitalne forenzike, ispitivanje funkcionalnosti zlonamjernog koda, uklanjanje prijetnji i provedbu postupaka oporavka sustava. [51]

Sredinom svibnja 2017. godine zabilježen je novi oblik prijetnje na Internetu u obliku zlonamjernog ransomware programa – „WannaCry". Ovim ransomwareom bila su zahvaćena sva računala s operacijskim sustavom Windows na kojima nije bila instalirana zakrpa objavljena u ožujku. Kako se radilo o globalnom incidentu ovakvog intenziteta, suradnja i razmjena informacija između tijela odgovornih za područje informacijske sigurnosti bila je od ključne važnosti za njegovo uspješno rješavanje. Nacionalni CERT na ovu je prijetnju

[51] Hrvatska akademska i istraživačka mreža – CARNET (2017). Godišnji izvještaj Nacionalnog CERT-a za 2017. godinu. Zagreb.

reagirao brzo i odgovorno te je poduzeo brojne aktivnosti kako bi se spriječilo širenje incidenta ili kako bi se smanjila šteta u slučaju infekcije. Aktivnosti uključuju informiranje putem TV emisija, e-mail poruka i svoje službene web stranice te odgovaranje na pitanja novinara, objava upozorenja i smjernica za zaštitu putem proaktivnih i reaktivnih mjera te načina postupanja u slučaju infekcije, slanje obavijesti svim članicama CARNET mreže, telekom operaterima te javnim i privatnim tvrtkama s kojima surađuje, suradnja sa sistemskim inženjerima i mrežnim odjelom unutar CARNET-a s ciljem sprečavanja širenja ransomwarea te analiza mreže s ciljem otkrivanja potencijalnih kompromitiranih računala.[52]

Nacionalni CERT je tijekom 2017. godine zaprimio i obradio ukupno 732 prijave koje se mogu klasificirati kao računalni incidenti u nadležnosti CERT-a. Vodeći tipovi incidenata su web defacement, phishing URL i phishing. Najznačajnija promjena u odnosu na 2016. godinu je rast broja phishing incidenata, što je rezultat nekoliko učestalih phishing kampanja koje su ciljale korisnike u Hrvatskoj te su bile dobro pripremljene, uglavnom na jezično ispravnom hrvatskom jeziku. Sljedeći grafikon prikazuje omjere incidenata po tipu u 2017. godini, koji su zabilježeni u sustavu za obradu incidenata.[53]



Graf 2: Raspodjela incidenata po tipu u 2017. godini. (Izvor: https://www.cert.hr/)

[52] Hrvatska akademska i istraživačka mreža – CARNET (2017). Godišnji izvještaj Nacionalnog CERT-a za 2017. godinu. Zagreb.
[53] Ibid.

6. Zaključak

Ulaskom u digitalno doba, razvija se kibernetički kriminal koji se širi računalnim mrežama i Internetom velikom brzinom. Broj napada na mrežu u cijelom svijetu raste, pa se iz tog razloga razvija nova grana forenzike – mrežna forenzika. Ova relativno mlada djelatnost bavi se prikupljanjem, bilježenjem i analiziranjem događaja na mreži, zbog otkrivanja izvora sigurnosnih napada. Mrežni forenzičar se u pravilu mora svakodnevno prilagođavati napadačima, koji nalaze nove načine i metode upada na mrežu. Napadači ostavljaju tragove i dokaze koji olakšavaju mrežnom forenzičaru cjelokupnu istragu, iako moraju biti oprezni s prikupljanjem tih dokaza jer su veoma promjenjivi. Prikupljanje dokaza može biti aktivno ili pasivno. Aktivno prikupljanje dokaza podrazumijeva rad s uređajem na mreži, a pasivno je ustvari prikupljanje mrežnog prometa. Prikupljanje se može obavljati fizičkim presretanjem i programima za praćenje i snimanje prometa. S obzirom na to da je mrežna forenzika dio velikog broja nacionalnih sigurnosnih službi, otvaraju se sveučilišni programi u cijelom svijetu, a najviše u Kanadi i Sjedinjenim Američkim Državama. Fakulteti u Americi nude preddiplomske i diplomske studije vezane za digitalnu i mrežnu forenziku, ali i kolegija i specijalizacije vezane za informacijsku sigurnost. Uz visokoškolsko obrazovanje, postoje i tečajevi s certifikacijom za neke od vještina koje su potrebne na putu do mrežnog forenzičara. Vještine za koje je moguće položiti certifikat su penetration testing, analiza sigurnosti i etičko hakiranje, a tečajevi se mogu polagati online putem, ali i u učionicama. Iako su mrežni forenzičari vezani za državne sigurnosne službe, bitnu ulogu od početka kibernetičkih napada ima Computer Emergency Response Team. CERT je organizacija koja se bavi računalno-sigurnosnim incidentima te preventivnim djelovanjem zbog poboljšanja računalne sigurnosti informacijskih sustava. Nacionalni CERT Republike Hrvatske se bavi računalno-sigurnosnim incidentima na hrvatskoj domeni. U njihovom se izvještaju za 2017. godinu vidi iz priloženog grafikona da su najveći udio računalnih incidenata u obliku web defacementa ili promjena izgleda mrežne stranice, a zatim incidenti u obliku phishinga ili predstavljanja kao legitimne ustanove u svrhu krađe podataka. Izvještaji Nacionalnog CERT-a pokazuju da u Hrvatskoj još uvijek nema potrebe za mrežnim forenzičarima, iako su tečajevi etičkog hakiranja sve popularniji, a 2017. godine otvoren je i prvi specijalistički diplomski studij Digitalne forenzike u sklopu Tehničkog veleučilišta u Zagrebu. Brzo širenje Interneta ukazuje na to da Internet više nije mjesto zabave, upoznavanja i relaksacije, već da polako postaje mjesto kriminala – od krađe identiteta, preko povreda privatnosti, do prodaje droge i Darkneta, te je upravo u tome potreba za mrežnom forenzikom.

Popis literature

1. Davidoff, S., Ham, J. (2012). Network Forensics: Tracking Hackers through Cyberspace. Upper Saddle River, New Jersey: Prentice Hall.
2. Hrvatska akademska i istraživačka mreža – CARNET (2017). Godišnji izvještaj Nacionalnog CERT-a za 2017. godinu. Zagreb.
3. Protrka, N. (2011). Računalni podaci kao elektronički (digitalni) dokazi. Policija i sigurnost, 20 (1), 1-13. Preuzeto sa: https://hrcak.srce.hr/79204
4. Reith, M., Carr, C., Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal Of Digital Evidence, 1(3). Preuzeto sa: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.13.9683

Popis internetskih izvora

1. 15 Universities with Online Computer Forensics Programs. Forensics Colleges. Preuzeto sa: https://www.forensicscolleges.com/blogs/15-universities-with-online-computer-forensics-programs
2. 17 Best Schools with Online Computer Forensics Programs. Cyber Degrees. Preuzeto sa: https://www.cyberdegrees.org/listings/best-online-computer-forensics-programs/
3. About Us. EC-Council. Preuzeto sa: https://www.eccouncil.org/about/
4. Academics. EC-Council University. Preuzeto sa: https://www.eccu.edu/academics/
5. Brute force napadi. Edicija dokumenata iz područja informacijskih znanosti. Preuzeto sa: https://www.cis.hr/www.edicija/Bruteforcenapadi.html
6. Certified Ethical Hacker Certification. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
7. Certified Ethical Hacker Practical. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh-practical/
8. Certified Network Defender Certification. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-network-defender-cnd/
9. Computer security and Digital Forensics. Ryerson University – The Chang School of Continuing Education. Preuzeto sa: https://ce-online.ryerson.ca/ce/default.aspx?id=3359
10. Digital Forensics Research Workshop. "A Road Map for Digital Forensics Research" 2001. http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf
11. Digitalna forenzika Diplomski. Tehničko veleučilište u Zagrebu. Preuzeto sa: https://www.tvz.hr/studiji/digitalna-forenzika/diplomski
12. Diplomski sveučilišni studij forenzike. Sveučilišni odjel za forenzične znanosti. Preuzeto sa: http://forenzika.unist.hr/Nastava/Diplomskisveu%C4%8Dili%C5%A1nistudijforenzike/tabid/497/Default.aspx
13. Dokaz. Proleksis Enciklopedija. Preuzeto sa: http://proleksis.lzmk.hr/18159/
14. EC-Council (2010). Computer Forensics: Investigating Network Intrusions and Cyber Crime. Preuzeto sa: https://news.asis.io/sites/default/files/Investigating_Intrusions_Network_CyberCrime.pdf

15. EC-Council Certified Security Analyst ECSA: Penetration Testing. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-security-analyst-ecsa/
16. EC-Council Certified Security Analyst Practical. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/certified-security-analyst-ecsa-practical/
17. Forensic (adj.). Online Etymology Dictionary. Preuzeto sa: https://www.etymonline.com/word/forensic
18. Hakiran je Acunetix. CERT.hr. Preuzeto sa: https://www.cert.hr/28625/
19. ISACA (2015). Overview of Digital Forensics. Rolling Meadows,Illinois. Preuzeto sa: http://www.infosecurityeurope.com/__novadocuments/83665?v=635652368156170000
20. National University's Nationally-Recognized Cyber Security Program Adds Focus in Computer Forensics. National University. Preuzeto sa: https://www.nu.edu/News/2014-CyberSecurityProgramAddsFocusinComputerForensi.html
21. Network Forensics. Techopedia. Preuzeto sa: https://www.techopedia.com/definition/16122/network-forensics
22. Network Forensics. TechTarget. Preuzeto sa: https://searchsecurity.techtarget.com/definition/network-forensics
23. O nacionalnom CERT-u. CERT.hr. Preuzeto sa: https://www.cert.hr/onama/
24. Password Cracking. Techopedia. Preuzeto sa: https://www.techopedia.com/definition/4044/password-cracking
25. Science (n.). Online Etymology Dictionary. Preuzeto sa: https://www.etymonline.com/word/science
26. Spam. CERT.hr. Preuzeto sa: https://www.cert.hr/19795-2/spam/
27. The LPT (Master) Training Program: Advanced Penetration Testing Course. EC-Council. Preuzeto sa: https://www.eccouncil.org/programs/licensed-penetration-tester-lpt-master/
28. Website Defacement Definition. Cybercrime.org.za. Preuzeto sa: http://cybercrime.org.za/website-defacement
29. Website defacement. Wikipedia. Preuzeto sa: https://en.wikipedia.org/wiki/Website_defacement
30. What is Database Forensics? InfoSec Institute. Preuzeto sa: http://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/application-forensics/overview-types-of-database-forensics/#gref
31. What is Forensics? Crime Scene Investigator Education. Preuzeto sa: https://www.crimesceneinvestigatoredu.org/what-is-forensic-science/
32. What is Phishing? Phishing.org. Preuzeto sa: http://www.phishing.org/what-is-phishing
33. Zlonamjerna kampanja putem elektroničke pošte. Mreža za IT profesionalce. Preuzeto sa: http://mreza.bug.hr/zlonamjerna-kampanja-putem-elektronicke-poste/

Prilozi

1. Tablica 1: Određivanje prioriteta pri prikupljanja mrežnih dokaza. Izvor: Davidoff, S., Ham, J. (2012). Network forensics: Tracking Hackers through Cyberspace

2. Graf 1: Obrađeni incidenti u zadnjih 30 dana - 27.05.2018. Izvor: https://www.cert.hr/sru/

3. Graf 2: Raspodjela incidenata po tipu u 2017. godini. Izvor: https://www.cert.hr/