# Etičko hakiranje i njegova uloga u zaštiti podataka

**Čop, Tena**

SVEUČILIŠTE U ZAGREBU

FILOZOFSKI FAKULTET

ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

Ak. god. 2019./2020.

Tena Čop

# Etičko hakiranje i njegova uloga u zaštiti podataka

Završni rad

Mentor: Vjera Lopina

Zagreb, rujan 2020.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(potpis)

Sadržaj

# Uvod

U suvremenom dobu tehnologija se koristi u većini svijeta. Sve se može pronaći na internetu. Sve nam je pri ruci jer imamo tehnologiju koja to omogućava. Veliki problem o kojem ne razmišljamo je naša sigurnost na internetu. Ako je imamo na umu ne shvaćamo je kao jako blisku i stvarnu prijetnju. Samim time što smo na internetu i što smo mi udaljeni od onoga što smatramo izvorom opasnosti, mi se ograđujemo od mogućnosti da se nešto opasno može dogoditi našim podatcima koji su na internetu. Smatramo da se zloupotreba ne može nama dogoditi jer mi nismo ništa opasno radili na internetu. U tom načinu razmišljanja leži opasnost jer ako mi posjetimo neku internetsku stranicu koja nema najbolju zaštitu i nju napadnu ljudi sa lošim nakanama, naši podatci su im na dohvat ruke. Taj problem je mnoge tvrtke mučio dok nisu spoznali da se načini i oruđa tih zlokobnih ljudi mogu upotrijebiti kako bi se pomoglo i zaštitilo opće stanovništvo.

Jedno od najbrže rastućih područja sigurnosti mreže, a svakako i područje koje izaziva mnogo kontroverzija je etičko hakiranje. U današnjem kontekstu gdje je tehnologija spojila svijet također se vidi izvor tjeskobe za vlasnike računalnih sustava diljem svijeta. Glavni razlog ove nesigurnosti je hakiranje bolje rečeno hakiranje računalnih sustava. Stoga je potreba zaštite sustava od smetnji hakiranja koje stvaraju hakeri promicanje osoba koje će odgovoriti na nezakonite napade na naše računalne sustave. Takvi stručnjaci su u današnje vrijeme poznati kao sigurnosni stručnjaci ili etički hakeri. U potrazi za načinom popravka problema organizacije su shvatile da bi jedan od najboljih načina za otklanjanje i procjenu prijetnje uljeza za njihove interese bio da nezavisni stručnjaci za računalnu sigurnost pokušaju upasti u njihove računalne sustave. Ova je shema nije toliko različita od zapošljavanja neovisnih inspektora da ispitaju i provjere knjigovodstvene evidencije. U slučaju računalne sigurnosti etički hakeri koristili bi iste alate i tehnike kao i „crackeri“, ali ne bi oštetili ciljne sustave niti ukrali podatke. Umjesto toga, oni bi procijenili sigurnost ciljnih sustava i izvijestili vlasnike o ranjivostima koje su pronašli zajedno sa uputama kako ih otkloniti ili barem osigurati od daljnje infiltracije.

# Povijest hakiranja

U početku osobe koje su se smatrale hakerima su bili računalni entuzijasti i zaljubljenici koji nisu željeli ništa drugo nego optimizirati, prilagoditi i izmijeniti svoje strojeve i tehnologiju. Tek desetljećima kasnije kad su izrađeni prvi virusi i počinjena prva „cyber“ kriminalna dijela, tradicionalni hakeri su spojeni s onima koji imaju loše namjere i započelo je javno zaziranje hakiranja. Sam termin „hack“ nije proizašao iz svijeta računala. Prvi put je spomenut 1960-ih kada su studenti MIT-evog kluba željezničkih tehnoloških maketa htjeli poboljšati funkcionalnost određenih maketa. (Power, 2016) Ti rani hakeri su željeli samo poboljšati već postojeće programe i kodove. Oni su svijet računala gledali kao nešto što se treba istražiti, testirati i poboljšati. U 70-ima prošlog stoljeća taj pogled u svijetu računalne tehnologije se nastavio u istom tijeku, ali je i proizašlo i novija vrsta „hakiranja“. Ti su hakeri iskorištavali svoje otkriće da bi dobili besplatne pozive na daljinu. Takvi „hakeri“ su se zvali „phreakers“. Sub-kultura „phreakers“ nije ustupila mjesto samo utjecajnim hakerima poput John Drapera, već i digitalnim inovatorima. (Lichstein, 1963) Presudno desetljeće za hakere su bile 80-e jer su tada računala bila dostupnija široj javnosti, a ne samo institutima i korporacijama. To je dovelo do porasta broja hakera bili oni zainteresirani za poboljšanje sustava i programa ili onih koji imaju zlokobne kriminalne namjere. Nažalost u 80-ima se vidio porast broja hakera koji koriste svoje znanje o tehnologiji i radu s računalima radi izvođenja kriminalnih dijela za vlastitu korist. Dijela po kojima su takvi hakeri bili poznati vide se i u današnjem svijetu tehnologije, a to su: stvaranje virusa, krađa privatnih podataka drugih korisnika, piratstvo softvera i samo provaljivanje u sustave većih korporacija. Prva zakonodavna reakcija prema tim zloćudnim „hakerima“ se dogodila 1986. Reakcija se nije dogodila samo unutar zakona već i u medijima koji opisuju „hakere“ kao osobe koje su sposobne za velika i grozna dijela. Najpoznatiji prikaz hakera iz tog vremena je film „Ratne igre“ u kojem obični tinejdžer uspije hakirati računalni sustav američkog stožera i skoro započne treći svjetski rat. U 90-ima ozloglašenost hakiranja je u velikom porastu zbog zlonamjernih „crackera“ koji koriste vještine hakera i hakiranja da bi radili zlonamjerna i kriminalna dijela te visoki broj uhićenih „crackera“. U pokušaju suzbijanja računalnog kriminala, policija je pokrenula žestoke istrage, provela ranojutarnje racije i uhitila brojne hakere. Zbog takvih promjena nekada usko povezana zajednica koju su činili „hakeri“ se počela raspadati. Mnogi članovi te zajednice su informirali policiju o drugim članovima radi svog imuniteta.

Mnogi hakeri koji nisu koristili svoje vještine u kriminalne svrhe bili su u 2000-ima smatrani zloćudnima zbog „crackera“ i njihovih napada na velike tvrtke koje se bave tehnologijom i čije se usluge dobivaju preko digitalnih sustava kao što su Google, Amazon i druge. Ti napadi su dominirali u vijestima kad god bi se pronašao novi virus ili novi način na koji „crackeri“ ulaze u računalne programe i sustave velikih korporacija. Ono što je dovelo do još veće negativne slike pojma haker je to što je petnaestogodišnji dječak uspio uči u visoko čuvane vojne sustave i programe. U 2010-ima svijet hakera i crackera je postao

kompliciraniji jer je cijeli svijet bio u digitalnom dobu. To je bilo doba kada se naglo popeo broj korisnika internetskih usluga zbog sve veće dostupnosti i relativne jeftinosti računalne opreme te sve veće potrebe za digitalnim i računalnim vještinama. Vidio se procvat takozvanih „vukova samotnjaka“ te manjih hakerskih grupa koje poboljšavaju softvere radi poboljšanja samog doživljaja prema tehnologiji i njenoj mogućnosti ili one koji koriste „ransomwere“ kako bi zaradili koristeći kriminalna dijela ili pokušavaju sebi napraviti izazove pomoću tuđih veza i računala. Iako takvi hakeri i crackeri postoje, ovo desetljeće je obilježeno grupama koje sebe smatraju „hacktivistima“ kao što su Anonymous. Anonymous je grupa hakera koja samo ruko izlaže javnosti visoko klasificirane dokumente, izdvaja državne tajne i vode žestoke digitalne „križarske ratove“ u ime obrane javnosti od vlade koja po njima nanosi štetu „malom čovjeku“ te iskorištava ili zadržava informacije od šire javnosti. U istom tom desetljeću kao reakcija na hacktiviste i „cyber“ kriminalce, vladina tijela iz svih zemalja i velike korporacije pokušavaju poboljšati sigurnost svojih informatičkih objekata, a računalni divovi(Microsoft, Google,…) naporno rade na dotjerivanju svojih sustava. Unatoč svim tim naporima stručnjaka za „cyber“ sigurnost koji se i dalje zapošljavaju, sustavima koji se nadograđuju i tehnologija koja se inovira, hakeri svih vrsta dosljedno i pomalo očekivano ostaju korak ispred velikih korporacija i vlada. (Power, 2016)

## Hakiranje i crackiranje

Hakiranje je termin koji se interpretira sa nekoliko različitih značenja, ovisno o tome iz koje se perspektive razmatra. Iako su mnogi pogledi na riječ haker imali raznih konotacija. U nekim definicijama hacker je samo netko tko je vješt programer i to je bila prva definicija hakera, ali u mnogim i najčešćim definiranjima hakiranje je to je netko tko stječe neovlašten pristup računalima radi igranja igrica ili rađenja štete. Hakiranje samo po sebi se odnosi na aktivnosti kojima se želi ugroziti digitalni uređaj, poput računala, pametnih telefona, tableta, pa čak i cijelih mreža. (Malwarebytes, 2020.) I premda hakiranje možda nije uvijek u zlonamjerne svrhe, danas većina izvora koji spominju hakiranje i hakere karakteriziraju ih kao nezakonitu aktivnost kriminalaca. Njihovi razlozi mogu biti raznoliki i u razne svrhe, kao što su želja za financijskom dobiti, prosvjed nad nekom percipiranom nepravdom, prikupljanjem informacija od suparničkih tvrtki ili zemalja pa čak i samo radi zabave izazova koje hakeri mogu pronaći na world wide web-u. Najveća pogreška u shvaćanju hakera je to da su hakeri samouka djeca koja nemaju ništa bolje za raditi doma pa onda rade razne nestašluke i neugodnosti ljudima oko sebe ili čak i strancima na internetu. Najveća pogreška u modernom shvaćanju riječi haker je to što svi shvaćaju hakere kao kriminalce, ali to nije tako u sadašnjem dobu. Kriminalci koji kradu naše podatke i novac sa stranica se u novijem dobu zovu crackeri. U suštini hakiranje nije kriminalno djelo već pronalazak nenamjernih ili previđenih upotreba zakona i okolnosti određene situacije, a zatim njihova primjena na nove i inventivne načine za rješavanje problema. (Erickson, 2008) Velika razlika između hakera i crackera je to što se hakeri

pridržavaju hakerske etike, dok su crackeri bili više zainteresirani za brzi profit i zaradu. U hakerskom svijetu crackeri su smatrani manje sposobnima od elitnih hakera jer su samo koristili alate koje su hakeri napravili bez razumijevanja kako ti alati funkcioniraju. Cracker je isto sveobuhvatan termin za sve ljude koji rade ilegalne stvari sa računalima. Iako taj termin nije u uporabi od strane onih koji bi trebali upućivati ljude u njihovu opasnosti i razliku između njih i hakera. Cracker se koristi u većini slučajeva kada stručnjaci raspravljaju o kriminalnim aktivnostima na računalima i u samoj hakerskoj zajednici.

## Vrste Hakera

Jedna od najčešćih, ali i najlakše zapamtljivih podjela u svijetu „cyber“ kriminala je podjela na šešire. Ta podjela je proizašla iz razmatranja hakerskog svijeta kao na stari vestern gdje su antagonist i protagonist lako primjetljivi zbog šešira koje nose na glavi. Zato se smatra da haker s crnim šeširom ili cracker koristi svoje znanje o računalnim sustavima i softverima radi krađe nečeg vrijednog ili drugih zlonamjernih razloga. Motivi samog hakiranja mogu biti raznoliki, ali najčešći motiv za crne šešire su krađa, ugled u hakerskim krugovima, korporativna špijunaža i hakiranje od strane država. Aktivnosti crnih šešira su u potpunosti i neupitno ilegalne.

S druge strane, hakeri bijelih šešira nastoje poboljšati sigurnost sigurnosnih sustava organizacije pronalaskom ranjivih nedostataka kako bi spriječili krađu identiteta ili druge računalne zločine prije nego što crni šeširi primijete mogućnosti upada. Korporacije čak zapošljavaju vlastite hakere bijelo šeširaše kao dio svog pomoćnog osoblja. Osim toga tvrtke mogu prepustiti svoje hakiranje bijelo šeširskim uslugama kao što je Division Zero ili Garoa Hacker Clube, koji testiraju softverske proizvode za ranjivosti i greške u programu ili sustavu u zamjenu za nagradu. Zbog toga što su zaposleni i zbog toga što sve rade uz znanje vlasnika aktivnosti bijelih šešira su potpuno legalne.

U ovu klasifikaciju se ubraja i velika većina sivih šešira to jest oni hakeri koji hakiraju bilo koji sustav čak i ako nemaju dopuštenje za testiranje sigurnosti sustava, ali nikada neće ukrasti novac ili oštetiti sustav za razliku od crnih šešira, tj. crackera. U većini slučajeva ako pronađu kakve točke proboja u sustav ili stranicu to kažu administratoru tog sustava. Iako su i oni nezakoniti zbog testiranja sigurnost sustava za koji nemaju dopuštenje da testiraju. Hakiranje sivog šešira ponekad je legalno, a ponekad ne. (JavaTpoint, Types of Hackers, 2021)

Nakon tih najpoznatijih klasa podijele postoje još nekoliko vrsta hakera, kao što su: hakeri crvenog šešira (ovakvi hakeri hakiraju državne agencije, tajna informacijska središta i općenito sve što spada u kategoriju osjetljivih informacija), haker plavog šešira(haker izvan konzultantskih tvrtki za računalnu sigurnost koji je unajmljen za testiranje programskih pogrešaka na sustavu prije njegovog pokretanja), elitni hakeri(kad si prozvan elitnim hakerom to je više društveni status među hakerima koji opisuje najvještije hakere), „Script Kiddie“(onaj koji nije stručnjak, ali provaljuje u računalne sustave koristeći

unaprijed napravljene automatizirane alate koje su napisali drugi, obično s malo razumijevanja temeljnih koncepta hakiranja ili programa), početnik ili haker zelenog šešira(netko tko je tek započeo sa upoznavanjem sa hakiranjem i njegovim alatima i mogućnostima) te haktivist (onaj koji koristi tehnologiju za objavljivanje društvene, ideološke, vjerske ili političke poruke)

Drugi način na koji se mogu podijeliti hakeri je podjela prema tome što je napadnuto i sa kojom svrhom je napadnut sustav.

To se dijeli na nekoliko skupina od kojih su najšire podijeljene na: hakiranje web stranice(„Website Hacking“), mrežno hakiranje(„Network Hacking“), hakiranje e – pošte(„Email Hacking“), etičko hakiranje(„Ethical Hacking“), hakiranje lozinki(„Password Hacking“) i računalno hakiranje(„Computer Hacking“). (Tutorials Point, Ethical Hacking - Quick Guide, 2021)

## Alati u hakiranju

Hakeri koriste puno samo napravljenih programa i sustava, ali ima i nekoliko poznatih alata koji su već napravljeni unaprijed od strane ili sigurnosnih stručnjaka ili drugih hakera. Takvi alati mogu biti napravljeni u druge svrhe, ali zbog određenih mogućnosti i sposobnosti tih programa budu prilagođeni i korišteni u hakerske i sigurnosne svrhe. Neki alati sa kojima većina etičkih hakera upravlja su: NMAP ili „Network Mapper“(alat otvorenog koda koji se naširoko koristi za otkrivanje mreže i reviziju sigurnosti), Metasploit(pomoću kojeg se može provesti osnovne testove penetracije na malim mrežama), „Burp Suit“ (platforma koja se široko koristi za obavljanje sigurnosnih testiranja web aplikacija), „Angry IP Scanner“ (skener IP adresa i priključaka na više platformi), Cain & Abel (alat za oporavak lozinke za Microsoft operacijske sustave), Ettercap ili „Ethernet Capture“ (sadrži traženje živih veza, filtriranje sadržaja u hodu i mnoge druge mogućnosti), EtherPeek (alat koji pojednostavljuje analizu mreže u heterogenom mrežnom okruženju), SuperScan, QualysGuard, Acunetix (potpuno automatiziran program za etičko hakiranje koje oponaša hakera kako bi bio korak ispred zlonamjernih uljeza) i mnogi drugi.

Za razliku od etičkih hakera njihovi „suparnici“ u profesiji koriste programe i načine napada kao što su virusi(vrsta zlonamjernog softvera koji se pridružuje drugom programu, koji se može replicirati i širiti nakon što ga osoba prvi put pokrene na svom sustavu), botneti (botnet je mreža računala koja pokreću botove pod kontrolom „bot herder“-a. Botovi su softverske aplikacije koje pokreću automatizirane programe preko mreže, dok je „bot herder“ osoba koja kontrolira i održava botnet), otmice preglednika, napadi uskraćivanja usluge ili takozvani DDoS napadi(Ova vrsta napada uključuje slanje velike količine prometa iz više izvora na aplikaciju ili web stranicu sa namjerom rušenja same stranice ili programa), ransomware(vrsta zlonamjernog softvera koji sprječava korisnike u pristupu njihovom sustavu ili osobnim datotekama i zahtijeva otkupninu kako bi povratili pristup), rootkitovi(zlonamjerni softver koji inicijatorima tog programa pruža sredstva za daljinski

pristup i potpunu kontrolu nad zahvaćenim sustavima bez znanja korisnika), trojanski konj(vrsta zlonamjernog softvera koji koristi prijevaru i društveni inženjering kako bi natjerao korisnike koji ništa ne slute da pokrenu naizgled dobroćudne računalne programe koji skrivaju zlonamjerne svrhe) i crvi(podskup trojanskog konja koji se može širiti i samostalno kopirati s jednog računala na drugo bez ljudske aktivacije nakon proboja u sustav) koji su u širem pojmu poznati kao „maleware“. (Malwarebytes, 2020.)

## Etičko Hakiranje

Etičko hakiranje ima više definicija i stručnjaci se ne mogu složiti oko jedne sveobuhvatne definicije. Prema nekim stručnjacima etičko hakiranje je nenasilno korištenje tehnologije u nastojanjima, političkim ili drugim, za poboljšanje društva koji su često pravno i moralno dubiozni. (Maurushat, 2019) Za druge stručnjake to je uporaba tehnika hakiranja kako bi se tim sustavima zaštitile važne informacije pohranjene na serverima tvrtki koje zapošljavaju takve stručnjake. (Sapp, 2020) Još jedno objašnjenje za etičko hakiranje je ovlašteni pokušaj neovlaštenog pristupa računalnom sustavu, aplikaciji ili podacima. (Synopsys, 2021) Pomoću etičkog hakiranja pronalaze se sigurnosni propusti i popravljaju se prije nego što bi ih zlonamjerni napadač iskoristio.

Najvažnija stvar koju bi etički haker trebao primijeniti i nikada ne zaboraviti je da uvijek treba imati dopuštenje za bilo koju vrstu napada ili upada u sustav poslodavca. Etički kodeks koji etički haker mora implementirati u svaki zadatak kaže da se nijedna mreža ili sustav ne smije testirati niti ciljati ako ga ne posjedujete ili ako za to nemate dozvolu. (Sapp, 2020) U protivnom etički haker može biti proglašeni krivim za više zločina koji su se u međuvremenu dogodili. Prvo, to može naštetiti karijeri i povjerenju u etičke haker, a drugo, ako se radi o nečem ozbiljnom kao što je krađa osobnih podataka korisnika ili krađa novca, to može ugroziti slobodu sigurnosnog stručnjaka koji je radio na tom projektu.

Najbolje je dobiti ugovor od poslodavca u trenutku kada se testira ili napada traženi program ili sustav. Ugovor je pisano ovlaštenje koje daje dozvolu etičkim hakerima da ispitaju dijelove sustava, ali svaki etički haker treba imati na umu da treba ispitati samo dijelove sustava navedene u tom ugovoru. U tom pogledu ako poslodavac želi dopustiti hakiranje dodatnih dijelova sustava ili ukloniti ovlaštenje za prije navedene sustave, najprije treba promijeniti ugovor, a etički haker ima obvezu prestanka rada na sustavu do dobitka novog ugovora. Etički haker treba shvatiti da jedino što etičkog hakera razlikuje od crackera je ugovor. Često se događa da tijekom ispitivanja sigurnosti sustava od klijenta hakeri naiđu na intimne podatke, poslovne i osobne. Zbog toga ugovor inače ima dio koji opisuje tko smije čuti što etički haker pronađe u sustavu.

Etičko hakiranje ovlaštena je praksa zaobilaženja sigurnosti sustava radi identifikacije potencijalnih kršenja podataka i prijetnji na mreži. (Sapp, 2020)Tvrtka koja je vlasnik sustava ili mreže dopušta etičkim hakerima da izvode takve aktivnosti kako bi testirali

obranu sustava. Za razliku od zlonamjernog hakiranja, ovaj proces je planiran, odobren i legalan.

Etički hakeri imaju za cilj istražiti sustav ili mrežu radi pronalaska slabih točaka koje zlonamjerni hakeri mogu iskoristiti ili uništiti. Oni prikupljaju i analiziraju informacije kako bi pronašli načine za jačanje sigurnosti sustava. Time mogu poboljšati sigurnosni otisak kako bi mogao bolje izdržati napade ili ih preusmjeriti . Etičke hakere organizacije unajmljuju da ispitaju ranjivosti svojih sustava i mreža i razviju rješenja za sprječavanje kršenja podataka.

Svaki etički haker se treba pridržavati moralnih pravila i pravila same etičko hakerske zajednice. Svaki etički haker mora zatražiti odobrenje od organizacije koja je vlasnik sustava. Hakeri bi trebali dobiti potpuno odobrenje prije nego što izvrše bilo kakvu sigurnosnu procjenu u sustavu ili na mreži. Potrebno je odrediti opseg procjene i obavijestiti organizaciju o svom planu. Nikad se ne smije zaboraviti prijavit sve povrede sigurnosti i ranjivosti pronađene u sustavu ili mreži. Sa obzirom da je svrha etičkih hakera osigurati sustav ili mrežu, trebali bi pristati i poštivati ugovor o ne otkrivanju podataka. I nikako se ne smije zaboraviti izbrisati sve tragove hakiranja nakon provjere da li sustav ima ranjivosti što onda sprječava ulazak zlonamjernih hakera u sustav kroz već identificirane rupe.

Etički hakeri slični su ispitivačima penetracije, ali uloga etičkog hakera je šira i uključuje veći raspon dužnosti. Poput ispitivača penetracije, etički hakeri provaljuju u sustave legalno i etički. Međutim, etički hakeri također su odgovorni za popravljanje ranjivosti koje identificiraju. Odgovornosti etičkih hakera uključuju: pronalaženje otvorenih rupa i provođenje korektivnih mjera za sprječavanje potencijalnih napada, izbjegavanje sustava za sprječavanje upada, sustava za otkrivanje upada i „firewall“-a i drugih dubokih kutova mrežu za pronalaženje zaporki ili drugih osjetljivih podataka koji bi se mogli koristiti za napad na organizaciju, identificiranje i popravljanje pogreška u mreži, napuknutu bežičnu enkripciju, otete web poslužitelje i otetu web aplikaciju, osigurati da su instalacije zakrpa aktualne i pomoći u rješavanju problema u vezi za prijevaru zaposlenika na mreži i krađu digitalnih podataka.

# Proces Etičkog hakiranja

Sam proces nije univerzalan ako se uzme u obzir definicija samog hakiranja jer svaki etički haker ima svoj proces koji njemu/njoj najviše paše i najbolje funkcionira. Ali većina izvora se slaže oko šest potrebnih koraka u procesu hakiranja radi uspješno provedenog sigurnosnog testiranja. Ti procesi su: izviđanje, skeniranje, dobivanje pristupa, održavanje pristupa, „brisanje staza“ i izvještavanje poslodavca. Ti procesi nisu u velikoj mjeri drugačiji od običnog hakiranja oni imaju jednu fundamentalnu razliku. Ta razlika odvaja crne i bijele šešire u hakerskom društvu.

## Izviđanje

Izviđanje je faza u kojoj napadač prikuplja podatke o meti aktivnim ili pasivnim sredstvima. Alati koji se široko koriste u ovom procesu su NMAP, Hping, Maltego i Google Dorks. Prikupljanje informacija i upoznavanje ciljnih sustava prvi je proces u etičkom hakiranju. Izviđanje je skup procesa i tehnika (Footprinting, Scanning & Enumeration) koji se koriste za tajno otkrivanje i prikupljanje informacija o ciljnom sustavu. (Tutorials Point, Ethical Hacking - Quick Guide, 2021) Tijekom izviđanja, etički haker pokušava prikupiti što je moguće više podataka o ciljnom sustavu, slijedeći sedam koraka -prikupljanje početnih informacija, određivanje raspona mreže, identifikacija aktivnih strojeva(računala, mobiteli,…), otkrivanje otvorenih portova i pristupnih točaka, određivanje koji operativni sustav radi, otkrivanje aktivnosti u portovima i mapiranje mreže. Samo izviđanje se dijeli na aktivno, u kojem izravno komuniciraš s računalnim sustavom radi prikupljanja informacija i pasivno izviđanje u kojem nisi izravno povezan s računalnim sustavom.

## Skeniranje

U ovom procesu napadač počinje aktivno ispitivati ciljani stroj ili mrežu radi utvrđivanja ranjivosti. Alati koji se koriste u ovom procesu su Nessus, Nexpose i NMAP.

Postoje tri vrste skeniranja u etičkom hakiranju. To su skeniranje portova koje uključuje skeniranje cilja radi traženja informacija poput otvorenih portova, živih sustava, raznih usluga pokrenutih na hostu, skeniranje ranjivosti pod koju spada provjeravanje ciljanih slabosti ili ranjivosti koje se mogu iskoristiti (obično se radi uz pomoć automatiziranih alata) i mrežno mapiranje u koje se ubraja pronalaženje topologije mreže, usmjerivača, poslužitelja „firewall“-a te informacija o hostu, u to pripada i crtanje mrežnog dijagrama s dostupnim podacima (takva karta služi kao vrijedan podatak tijekom cijelog procesa hakiranja) (Ethical Hacking; Phases of Hacking, 2020)

### Dobivanje pristupa

U tom se procesu ranjivost nalazi i pokušavate je iskoristiti kako biste ušli u sustav. Primarni alat koji se koristi u ovom procesu je Metasploit. Etički hakeri nakon što uđu u sustav, povećaju privilegiju na razinu administratora kako bi mogli instalirati aplikaciju ili izmijeniti i sakriti podatke kao što bi zlonamjerni haker napravio.

### Održavanje pristupa

To je proces u kojem je haker već dobio pristup sustavu. Nakon što dobije pristup, haker instalira neka stražnja vrata kako bi ušao u sustav kada mu zatreba pristup u ovom vlasničkom sustavu u budućnosti. Metasploit je preferirani alat u ovom procesu. Većina zlonamjernih crackera i hakera za ovu fazu koriste trojanske konje, viruse i ostali „maleware“.

### „Brisanje staza“

Ovaj proces je zapravo neetička aktivnost. To se odnosi na brisanje dnevnika svih aktivnosti koje se odvijaju tijekom procesa hakiranja. Svaki haker uvijek briše sve aktivnosti koje je radio tako da u kasnijem razdoblju nitko ne može pronaći nikakve tragove koji vode do slabih točka u sustavu. Što uključuje brisanje vrijednosti „log“-ova, izmjenu vrijednosti registra i deinstaliranje svih aplikacija koje je haker koristio te brisanje svih mapa koje je stvorio.

### Izvještavanje poslodavca

Izvještavanje je posljednji korak dovršetka procesa etičkog hakiranja. Ovdje Etički haker sastavlja izvješće sa svojim nalazima i poslom koji je obavljen, kao što su upotrijebljeni alati, stopa uspjeha, pronađene ranjivosti i procesi iskorištavanja. (Tutorials Point, Ethical Hacking - Quick Guide, 2021)

## Uloga Etičkog hakiranja u Zaštiti Podataka

Etički hakeri mogu biti neovisni vanjski konzultanti, zaposleni u tvrtki specijaliziranoj za simulirane uvredljive usluge „cyber“ sigurnosti, ili mogu biti interni zaposlenici koji štite web stranicu ili aplikacije tvrtke.

Poznavanje sadašnjih metoda i alata napada uvjet je za sve ove mogućnosti zapošljavanja, međutim od internog etičkog hakera može se zahtijevati blisko poznavanje samo jednog softvera ili vrste digitalne imovine.

Iako je relativno nov u sigurnosnoj industriji, jedna prednost koju interni crveni tim može pružiti je ta što će tim nužno imati intimnije razumijevanje o tome kako su izgrađeni njihovi vlastiti sustavi i aplikacije nego nezavisni konzultant. Ovo unutarnje znanje daje crvenom timu prednost, sve dok po njihovom mišljenju ne mogu postati kratkovidni. Pravim

napadačima trebale bi godine da ponove tu prednost. Smatra se da su interni timovi jeftiniji i od stalne uporabe konzultantske tvrtke.

S druge strane, korist koju vanjski etički haker može pružiti je svjež pogled na prepoznavanje ranjivosti koje unutarnji tim može zanemariti. Čak i organizacije koje zapošljavaju interni crveni tim mogu povremeno ugovoriti vanjskog etičkog hakera kako bi pružile svjež pogled na svoju obranu.

Za bilo kojeg vanjskog pružatelja uvredljivih sigurnosnih usluga posebno je važno dobiti pismenu dozvolu od klijenta prije početka bilo kakvih uvredljivih aktivnosti. Ovo dopuštenje treba detaljno opisati sustave, mreže, aplikacije i web stranice koje će biti uključene u simulirani napad. Nemojte povećavati opseg usluge bez dodatnog pisanog dopuštenja za to.

U skladu s korištenjem boja u industriji za razgraničenje između različitih uloga i funkcija „cyber“ sigurnosti, postoje etički hakerski angažmani bijele kutije, crne kutije i sive kutije. Angažman u bijeloj kutiji je kada sigurnosni stručnjak dobije što je moguće više informacija o ciljnom sustavu i aplikaciji. To omogućuje simuliranom napadu da ide široko i duboko, vrlo brzo tražeći ranjivosti za koje bi pravom lošem glumcu trebalo jako dugo vremena da ih otkriju.

Nasuprot tome, angažman u crnoj kutiji je kada se etičkom hakeru ne daju unutarnje informacije. Ovo pobliže odražava okolnosti stvarnog napada i može dati vrijedan uvid u to kako bi pravi vektor napada mogao izgledati. Kao što naziv implicira, angažman u sivoj kutiji tada označava simulaciju napada u kojem je napadač već prošao perimetar i možda je proveo neko vrijeme unutar sustava ili aplikacije.

Mnoge tvrtke traže pomoć od sve tri vrste angažmana zajedno s internim i vanjskim etičkim hakerima. Ova varijacija primijenjenog znanja može pružiti najbolji uvid u to koje se zaštite moraju primijeniti, ali je i mnogo skuplje za poduzimanje.

Posjedovanje etičkih hakerskih vještina i znanja korisno je za mnoge druge sigurnosne uloge.

Ove su vještine od vitalnog značaja za analitičare mrežne sigurnosti i mrežne inženjere. Ljubičastim timovima potrebni su ljudi s napadačkim sposobnostima. Razvojni programeri za sigurnost aplikacija imaju koristi od razumijevanja uvredljivih metoda i alata. Istraživači sigurnosti, općenito poznati kao lovci na kukce, uvelike ovise o svom znanju napadačke taktike. Mnogi uspješni lovci na greške pokazuju razumijevanje koje seže dublje od aplikacijskog sloja do mrežnog sloja i drugih područja koja se mogu iskoristiti.

# Znanje i vještine potrebne za etičkog hakera

U skladu sa nekoliko povjerljivim i upućenim izvorima za certifikaciju etičkih hakera kao što su Međunarodno vijeće konzultanata za elektroničku trgovinu (EC-Council) i razne škole za treniranje i podučavanje etičkih hakera ovo su šest osnovnih vještina i potreba radi postajanja etičkim hakerom:

## Naučiti što se sve uključuje i isključuje iz etičkog hakiranja

Prije nego što počnete učiti o bilo čemu treba se upoznati sa osnovnim konceptima predmeta ili discipline. Ista ta pravila vrijede i za etičko hakiranje. Potrebno je znati da je etičko hakiranje pristup obrani sigurnosti sustava i mreže iskorištavanjem postojećih ranjivosti istih. Etički hakeri jačaju sustave i sigurnost mreže identificiranjem slabosti i ispravljanjem odgovarajućim protumjerama. Razumijevanje da etički hakeri slijede iste tehnike kao i crackeri kako bi pronašli ranjivosti sustava i popravili ih, ali svoje usluge nude samo ako su za to legalno zaposleni u nekoj organizaciji.

## Razumijevanje različitih vrsta hakiranja

Shvatiti da je izraz 'hakiranje' kontroverzne prirode i često se razmatra u negativnom kontekstu. Potrebno je primijetiti da postoje različite vrste hakera koje služe različitim svrhama, od zlonamjernih do korisnih. Gdje su hakeri bijelog šešira i sivog šešira korisni i koriste svoje hakerske vještine za etičko hakiranje. Postoje sa druge strane, hakeri s crnim šeširima koji svoje vještine koriste za ilegalne i zlonamjerne aktivnosti.

Poznavanje različitih vrsta hakera pomaže budućim profesionalcima da razumiju svoje granice kao etičkim hakerima i pravne nijanse etičkog hakiranja te pravila kojih se svaki etički haker treba pridržavati.

## Skupovi vještina potrebni za karijeru u etičkom hakiranju

Ne postoji jedna formula za postajanje etičkog hakera. Najviše ovisi o zahtjevima organizacija koje trebaju takve usluge, one stvaraju opis posla i traže vještine u kandidatu po istom. Ali diploma iz računalnih znanosti, informacijskih tehnologija ili matematike može postaviti temelje karijere u etičkom hakiranju.

Također treba imati dobre vještine rješavanja problema, sposobnost podnošenja pritiska i razmišljanje „izvan okvira“. Za karijeru u etičkom hakiranju potrebno je stalno učenje i stalni razvoj. Što se tiče tehničkog aspekta potrebno je imati radno znanje o programskim jezicima kao što su HTML, C/C ++, Python, Java i drugi. Inter personalne vještine potrebne za rad u području etičkog hakiranja su: strast prema samom području tehnološke sigurnosti, snažne komunikacijske vještine, fleksibilnost i inovativno razmišljanje.

## Programiranje i operacijski sustavi

Karijera u etičkom hakiranju zahtijeva dobro poznavanje programskih jezika jer uključuje svakodnevni rad na različitim sustavima. Također je potrebno znati barem osnove o operativnim sustavima kao što su Windows, UNIX, LINUX i IOS.

Živo razumijevanje programskih jezika pomaže etičkim hakerima u identifikaciji programskih grešaka ili ranjivosti. (Advani, 2021) Također pomaže u implementaciji sigurnosnih rješenja gdje je potrebno kodiranje i omogućuje automatizaciju zadataka zajedno s drugim zahtjevima kodiranja.

Temeljito poznavanje funkcionalnosti operacijskih sustava zajedno s odgovarajućim naredbama je od iznimne pomoći u etičkom hakiranju.

## Poznavanje mreže i sigurnosti

Razumijevanje računalnih mreža i koncepata „cyber“ sigurnosti ključno je za karijeru u etičkom hakiranju. Nadahnuti etički haker trebao bi dobro poznavati osnove, kao i napredno znanje o računalnom umrežavanju i sigurnosti. Neki od ovih koncepata uključuju VPN-ove (virtualne privatne mreže), kriptografiju, „firewall“-ove i različite vrste „cyber“ -napada, poput napada DoS (uskraćivanje usluge). Na internetu su dostupne razne knjige, časopisi i internetski tečajevi za učenje o mreži i sigurnosti u svrhu etičkog hakiranja koje mogu osigurati potrebna znanja radi postajanja etičkog hakera.

## Programi obuke i stjecanje certifikata

S porastom potražnje za vještim etičkim hakerima, na tržištu za aspirante predstavljaju se mnogi programi obuke i tečajevi za certificiranje. Potrebno je prijaviti se za program obuke ili kamp za obuku kako bi aspirant poboljšao svoje vještine i prakticirao etičko hakiranje u stvarnom svijetu. Stjecanje certifikata važno je jer dodaje vjerodostojnost i vrijednost profesionalnom profilu kao etičkog hakera. Vrijedna potvrda dobrog instituta može pomoći pronaći posao u velikim tehnološkim divovima. Napredni tečaj računalne sigurnosti Stanforda Great Learning odličan je program certifikacije za one koji žele nastaviti karijeru u etičkom hakiranju. (Advani, 2021)

## Međunarodno priznati certifikati za Etičkog hakera

Da bi postao etički haker potrebno je biti certificiran kao jedan jer ako etički haker nema certifikat lako je zamijeniti planirani i dogovoreni upad za zlonamjerni napad na sustav. Iz tog razloga sigurnosni stručnjaci su odlučili izdavati certifikate od kojih su sedam najpoznatijih i najpriznatijih:

1.“ Certified Ethical Hacking Certification“ koji je jedan od najstarijih, najpopularnijih i najboljih programa certificiranja koji se može pružiti etičkim hakerima. Stjecanje ovog

međunarodno priznatog certifikata znači stjecanje znanja i vještina etičkog hakiranja za kojima je sada ogromna potražnja.

2. „GIAC Penetration Tester“ je druga vrsta certifikata koja uglavnom pokriva dubinske tehničke pristupe provjeri cijelog sustava putem izvješćivanja i opsežnog testiranja.

3. „Offensive Security Certified Professional“ postoji samo oko 10 godina, ali je već stekao dobru reputaciju zbog trajnosti i žilavosti. Ovaj certifikacija dokazuje da njezin nositelj može prepoznati ranjivosti, generirati i mijenjati kod za eksploataciju, iskorištavati hostove i uspješno izvršavati zadatke na ugroženim sustavima u nekoliko operativnih sustava.

4. CREST certifikacijski ispiti i tečajevi široko su prihvaćeni u mnogim zemljama. On „…djeluje kao fokus za napredak najbolje prakse i aktivnosti profesionalnog napretka kroz svoja kolektivna istraživačka djela.“ (7 Ethical Hacking Certifications for Your IT Career, 2020)

5. „Foundstone Ultimate Hacking“ sljedeći je najbolji certifikat. Ovaj certifikat uključuje nauku o primijeni alata i metode koje hakeri koriste u kontroliranom i sigurnom okruženju.

6. „Certified Penetration Testing Consultant“ dolazi nakon prošlog , ali on se bavi podučavanjem budućih profesionalaca odgovornim za sigurnost računalnih sustava.

7. „Certified Penetration Testing Engineer“ je zadnji najpoznatiji certifikat za etičke hakere. Ovo je međunarodno prihvaćena potvrda o kibernetičkoj sigurnosti i smatra se jednom od pet temeljnih vjerodajnica za kibernetičku sigurnost.

# Prevencija i zaštita od hakiranja

Unatoč rasprostranjenosti računalnih hakera, većina se tvrtki oslanja na internet za praćenje svojih financija, naručivanja i održavanja zaliha, provođenje marketinških i PR kampanja, povezivanje s klijentima, uključivanje u društvene medije i obavljanje drugih kritičnih operacija. Unatoč svemu tome još uvijek čujemo u vijestima o masovnim računalnim oštećenjima, čak i u velikim korporacijama sa snažnim sigurnosnim mjerama. U takvom okruženju i mala poduzeća se također mogu često pronaći kao meta, posebno zato što mogu podcijeniti rizik koji postavljaju „cyber“ kriminalci i možda nemaju sredstava za korištenje skupih rješenja za „cyber“ sigurnost. Zato je najbolje da svi korisnici računalnih mreža koriste sve u svojoj sposobnosti i mogućnosti da se zaštite od takvih kriminalnih dijela. Većina sigurnosnih i preventivnih mjera od hakiranja mogu biti: upotreba vatrozida („firewall“ , što je softver osmišljen za stvaranje barijere između podataka korisnika i vanjskog svijeta, također sprječava neovlašteni pristup korisnikovoj mreži i upozoravaju vas na sve pokušaje upada), instaliranje antivirusnih softvera (štite računalo od neovlaštenog koda ili softvera koji može ugroziti operacijski sustav), instaliranje paketa protiv špijunskog softvera(vrsta softvera koji tajno nadzire i prikuplja osobne ili organizacijske podatke, teško ga je otkriti i ukloniti te prikazuje neželjenih oglasa ili rezultata pretraživanja koji vas namjeravaju usmjeriti na određene web stranice, neki bilježe svaki pritisak na tipku za pristup lozinkama i drugim financijskim podacima), korištenje složenih lozinka (najvažniji je način sprječavanja upada u mrežu, najsigurnije lozinke su dugačke i složene), ažurni OS, aplikacije i preglednici (većina ažuriranja uključuje sigurnosne popravke koji hakerima sprječavaju pristup), zanemarivanje neželjene pošte (e -pošte za krađu identiteta mogu oponašati korisnikove prijatelje, suradnike i pouzdane tvrtke), napraviti sigurnosnu kopiju računala(sigurnosno kopiranje podataka ključno je u slučaju da hakeri uspiju probiti sustav i uništiti ga, vanjski hard-disk pruža mogućnost za spremanjem podataka izvan dohvata hakera), ugasite računala i druge strojeve koji su u sustavu te korištenje virtualizacije (omogućuje da pokretanje preglednika u virtualnom okruženju što zaobilazi operacijske sustave samog računala).

Preventiranje hakerskih napada je uvijek posao tvrtke i samog korisnike, a ne samo posao sigurnosnog stručnjaka. Stoga je dobro da se i osiguraju mreže korisnika i tvrtki. Najbolje je da se koriste usmjerivači i postavljanje sigurnih lozinki na sam ruter. Naravno uvijek se može upotrijebiti dvodijelna provjera autentičnosti što uključuje lozinke kao prvu liniju obrane od računalnih hakera, a kao sljedeću sigurnosnu opciju može se zatražiti da se unese brojčani kod (poslan na telefon ili u e-poštu) prilikom prijave. Još jedna korisna sigurnosna mjera je korištenje enkripcije koja je tu samo u slučaju ako su hakeri ušli u sustav radi zaštite informacija na računalu ili u sustavu.

## Zaštita telefona od hakera

Za razliku od računala telefoni su uvijek uz nas i relativno su mobilni u smislu gdje se nalaze. To čini sigurnost telefona lakšom i težom za osigurati. Radi zaštite mobilnih uređaja potrebno je poduzeti različite sigurnosne mjere nego što je potrebno za osiguravanje računala. Najčešća pogreška kod korisnika je to što ostave uključen Bluetooth. Preko Bluetootha je jako lako otvoriti vrata u telefon bez da korisnik zna za to. Korištenje javnih nesigurnih Wi-Fi veza je još jedna česta pogreška i rizik kojem se korisnici izlažu svakodnevno. U te veze se ne vežu osigurane javne mreže koje su povezane sa institucijama već one javne mreže koje nemaju i ne trebaju lozinku. Takve mreže su glavna meta za hakere svih motiva i vještina. Iz takvih problema proizlazi i potreba za sigurnosnom aplikacijom na samom telefonu. Te aplikacije najčešće funkcioniraju po istom principu kao i „firewall“ na računalima, neke od kvalitetnih aplikacija sa takvom funkcijom su Avast, Bitdefender i drugi. Naravno ako kradljivac ili haker uspije doći do fizičkog telefona najbolja sigurnosna mjera protiv gubitka podataka je upotreba boljeg pristupnog koda ili lozinke prije ulaska u sam mobitel. Najbolja lozinka bi bila neka nasumično generirana šestoznamenkasta šifra. (Freedman, 2020)

Nešto što većina korisnika ne smatra prijetnjom svojoj sigurnosti je automatsko dovršavanje i popunjavanje fraza i riječi koje svaki telefon u novije vrijeme ima, ali to je isto jako veliki rizik jer u njemu se mogu zadržavati sve lozinke, korisnička imena i sve e-mail adrese koje su ikad bile zapisane na mobitelu. Što ne označuje samo rizik za hakiranog korisnika već i za sve zapamćene korisnike u tom programu. I na kraju bi bilo najbolje da korisnici često brišu svoju povijest pregledavanja i sama povijest na Internet preglednicima što je korisno samo u slučaju ako je telefon već hakiran. To pomaže u davanju što manje informacija o korisniku koliko je to moguće.

# Sigurnosni alati

Tržište sigurnosnih alata veliko je koliko i samo polje. Odvajanje stotina različitih alata pomaže ih podijeliti u različite kategorije. Prva kategorija su „event managers“. Ovi alati reagiraju na događaje koji se događaju na mrežama koje nadzirete. Oni analiziraju zapisnike na sustavima kako bi otkrili te događaje.

Još jedan od korisnih alata su „packet sniffers“ koji omogućuju dekodiranje paketa dok kopaju po prometu kako bi skenirali njihov teret. „Packet sniffers“ koriste se kada se želi dublje proučiti sigurnosne događaje koji su se događali ili se trenutno događaju.

Sustavi za otkrivanje i sprječavanje upada još su jedna korisna kategorija alata. Mogu izgledati poput vatrozida i antivirusa, ali se uvelike razlikuju po funkciji. Što se tiče tog softvera, uvijek ih se treba smatrati kao granicom mreže koji je tu radi otkrivanja nedopuštenih aktivnosti. (Maurushat, 2019) Naravno, ne može se svaki alat kategorizirati zbog toga koliko su specifični po pitanju funkcije i dizajna. Međutim, oni mogu biti vrlo

korisni u mnogim različitim situacijama. Vrlo je teško odrediti koji su alati bolji od drugih u različitim kategorijama zbog različitih namjena koje mogu imati. Većina alata uvelike se međusobno razlikuju i nije moguće reći da je jedan apsolutno bolji od drugog. Što znači da je teško odabrati alate za svaki posao, ali evo nekoliko često korištenih alata koje uvijek morate imati na umu pri preuzimanju posla.

# Zaključak

U konačnici etičko hakiranje je nastalo više iz potrebe prema i radi sigurnosti korisnika i kompanija. Iako nisu sva hakiranja zlonamjerna izrazito je potrebno implementirati barem vanjske suradnike sigurnosne stručnjake. Vrijednost i potreba etičkih hakera je vidljiva u svim aspektima tehnološke sigurnosti i privatnosti. Oni su ti koji sprječavaju crackere sa zloćudnim i kriminalnim motivima i namjerama. U današnjici sve je više prihvaćeno da crackeri postoje i da njihove stalno razvijajuće metode nije moguće u potpunosti iskorijeniti. Tu ulaze etički hakeri sa svojim metodama i stručnošću gdje oni pomažu tvrtkama da uoče svoje prijestupe u sigurnosti i da pomognu istima osigurati da se takvi prijestupi ne ponove u tom obliku. Potreba za etičkim hakerima je sve veća jer ima sve više i više dostupnosti i proširenosti rada na računalima. Što kao posljedicu sa sobom vuče sve više nesigurnosti u računalne sustave jer ima sve više nemoralnih i kriminalnih crackera. Etički hakeri nisu samo linija obrane između korisnika i crackera već i preventivna mjera od krađe bilo to krađa korisničkih informacija ili samog novca korisnika. Tvrtke koje zapošljavaju etičke hakere razumiju potrebu korisnika da se osjećaju sigurno u svom virtualnom okruženju. Ali naravno nisu samo korisnici u pitanju već i same korporacije i tvrtke koje zapošljavaju etičke hakere. Velika odgovornost je stavljena na leđa etičkih hakera jer oni svojim radom uspiju zaštititi podatke prije nego što bi neki cracker uspio doći do bilo kakvog utjecaja na sustav. Iako su metode koje implementiraju etički hakeri identične crackerima i njihovim napadima na sustav oni svojim znanjem i vještinama osiguravaju da nema nikakvih prodora i napada na sustave koje osiguravaju. Etičko hakiranje glavni je ključ učvršćivanja mrežne sigurnosti i jedna je od najtraženijih vještina svakog stručnjaka za tehnološku sigurnost. Etički hakeri obučavaju se u tom polju radi testiranja je li je mreža organizacije izložena, slaba ili ranjiva na napade crackera.

# Bibliografija


*7 Ethical Hacking Certifications for Your IT Career*. (2020). Dohvaćeno iz PrepAway: https://www.prepaway.com/certification/7-ethical-hacking-certifications-for-your-it-career/

*A complete guide to becoming an ethical hacker*. (20. lipanj 2021). Dohvaćeno iz Cyber Security Guide: https://cybersecurityguide.org/resources/ethical-hacker/

Advani, V. (2021). *How To Start A Career In Ethical Hacking*. Dohvaćeno iz My Great Learning: https://www.mygreatlearning.com/blog/how-to-start-a-career-in-ethical-hacking/

Erickson, J. (2008). *Hacking The art of exploitation.* San Francisco: No starch press.

*Ethical Hacking; Phases of Hacking*. (2020). Dohvaćeno iz Grey Campus: https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking

Freedman, M. (13. Listopad 2020). *18 Ways to Secure Your Devices From Hackers*. Dohvaćeno iz Business News Daily: https://www.businessnewsdaily.com/11213-secure-computer-from-hackers.html

*How to make a career in ethical hacking*. (10. srpanj 2020). Dohvaćeno iz Geeks for Geeks: https://www.geeksforgeeks.org/how-to-make-a-career-in-ethical-hacking/

*JavaTpoint, Types of Hackers*. (2021). Dohvaćeno iz JavaTpoint: https://www.javatpoint.com/types-of-hackers

Lichstein, H. (1963). Telephone hackers active. *The Tech*, 1.

Malwarebytes. (2020.). *Resources: Hacking*. Dohvaćeno iz Malwarebytes: https://www.malwarebytes.com/hacker/

Maurushat, A. (2019). Ethical Hacking. U A. Maurushat, *Ethical Hacking* (str. 7-30). Ottawa: University of Ottawa Press.

Power, K. (17. Kolovoz 2016). *The State of Security*. Dohvaćeno iz Tripwire: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/

Sapp, A. S. (2020). *Infinity Ethical Hacking Learn basic to advance hacks.*

Synopsys. (2021). *Glossary, Synopsys*. Dohvaćeno iz Ethical Hacking, Synopsys: https://www.synopsys.com/glossary/what-is-ethical-hacking.html

*Tutorials Point, Ethical Hacking - Quick Guide*. (2021). Dohvaćeno iz Tutorials Point: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_quick_guide.htm

*Tutorials Point, Ethical Hacking - Tools*. (2021). Dohvaćeno iz Tutorials Point: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_tools.htm

# Sažetak

U ovom radu sagledavala se povijest, razvoj i sadašnjica hakiranja i njegovih opasnosti. Sagledani su razlozi i posljedice nedostatka sigurnosnih stručnjaka za računalne svrhe. Isto tako je i izložen način na koji ljudi mogu biti u rizičnoj skupini u obziru na osigurane ljude ili korporacije te su predložene mjere koje se mogu poduzeti i inicirati radi što veče računalne sigurnosti. Rad se bavi isto tako i sa načinom na koji se može postati stručnjakom za računalnu sigurnost i sa svim uvijetima potrebnim radi što boljeg i stručnijeg profesionalca potrebnim za javnu računalnu sigurnost.



Ključne riječi: hakiranje, računalna sigurnost,etičko hakiranje, crackiranje, računalo, mreža

Abstract

This paper examines the history, development and present of hacking and its dangers. The reasons and consequences of the lack of security experts for computer purposes are considered. It also outlines the way in which people can be at risk with respect to insured people or corporations, and suggests measures that can be taken and initiated to maximize computer security. The paper also deals with the way in which one can become a computer security expert and with all the conditions necessary for the best and most professional professional needed for public computer security.

Keywords: hacking, computer security, ethical hacking, cracking, computer, network