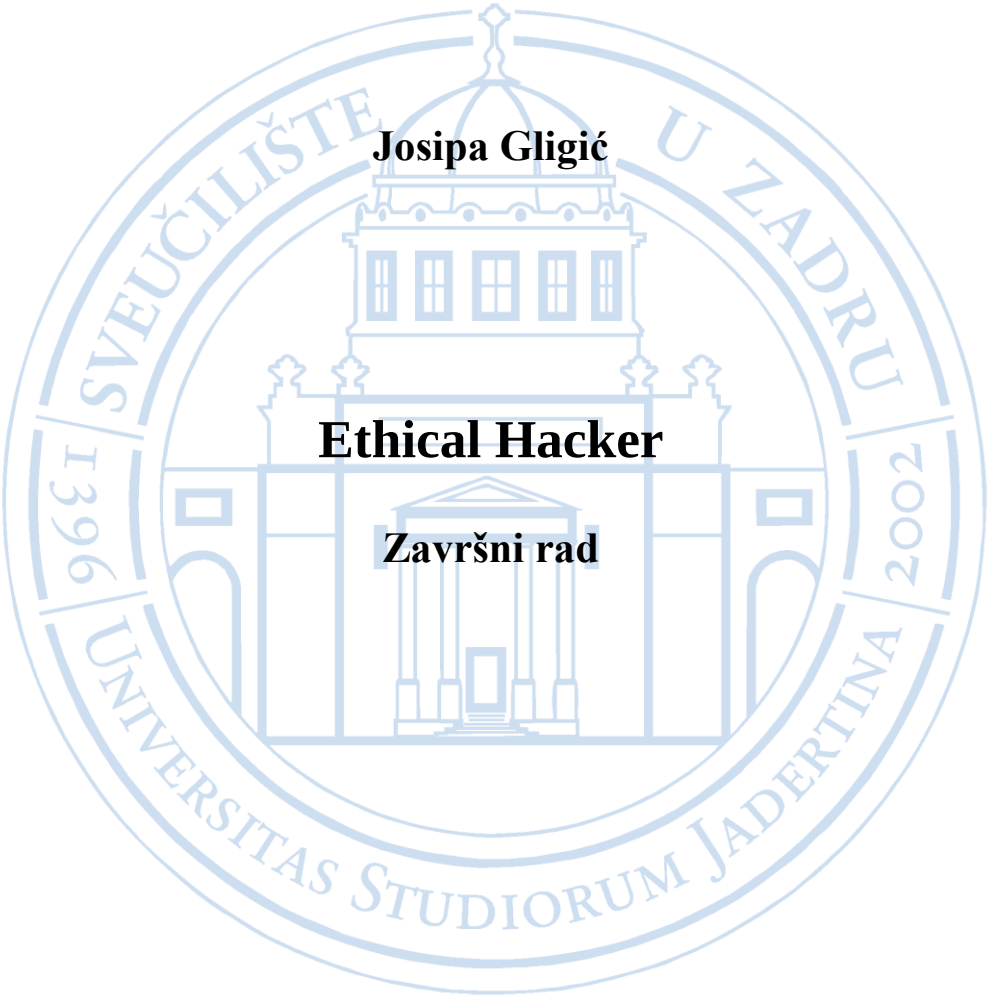
Etički haker

Gligić, Josipa

Sveučilište u Zadru

Odjel za informacijske znanosti
Preddiplomski stručni studij informacijske tehnologije



Josipa Gligić

Ethical Hacker

Završni rad

Zadar, 2023.

Sveučilište u Zadru

Odjel za informacijske znanosti
Preddiplomski stručni studij informacijske tehnologije

Ethical Hacker

Završni rad

Student/ica:
Josipa Gligić

Mentor/ica:
prof. dr. sc. Dino Županović

Zadar, 2023.

Izjava o akademskoj čestitosti

Ja, **Josipa Gligić,** ovime izjavljujem da je moj **završni** rad pod naslovom **Ethical Hacker** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

Izjavljujem da ni jedan dio ovoga rada nije iskorišten u kojem drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Zadar, 22. rujna 2023.

SADRŽAJ

1. UVOD

Razumijevanje važnosti informacijske sigurnosti je temelj uspješnog poslovanja i zaštite osobnih, povjerljivih, privatnih i osjetljivih informacija i podataka. Uspješna zaštita zahtjeva temeljnu provjeru ranjivosti tiskanih, elektroničkih te bilo kojih drugih oblika informacija i podataka. Etičko hakiranje omogućava uspješnost informacijske sigurnosti i zaštitu od zlouporabe, neovlaštenog pristupa, otkrivanja, uništavanja, izmjene ili prekida rada. Etičko hakiranje „White hat“ hakeru omogućava otkrivanja ranjivosti sustava i aplikacija te povratne informacije razvojnim inženjerima i u konačnici poslodavcima izvršavanje izmjena potrebnih za sigurnost i sprječavanje gubitaka različitih vrsta.

Ovaj završni rad sadržava temelje informacijske sigurnosti i etičkog hakiranja. Kroz rad je prikazana njihova uska povezanost te spoznaja svrhe etičkog hakiranja za primjenu uspješne informacijske sigurnosti. Svjesnost o rizicima i ranjivosti podataka u digitalnom svijetu trebala bi biti prva i osnovna točka prije početka korištenja tehnologije. Često pod utjecajem dobrobiti koje pruža digitalni svijet, svakodnevnim olakšavanjem komunikacije, što u osobne ili poslovne svrhe, zanemaruju se opasnosti. Zanemarivanje primjene adekvatne zaštite dovodi do rizika eksploatacije. Svaka interakcija između čovjeka i tehnologije ostavlja trag koji u konačnici tvori identitet. Koristeći neke smjernice i sa osnovnim znanjem o informacijskoj sigurnosti pojedinac štiti svoj identitet.

Etički hakeri pomažu svojim znanjima i vještinama. Nebrojeno se puta u životu dogode situacije koje zbog tehničkog kvara ili zaborava pružaju konkretan uvid koliko su vještine koje posjeduju etički hakeri primjenjive i višestruko korisne. Scenariji, poput vrlo čestog slučaja zaboravljanja lozinke, slučajnog brisanja sadržaja sa računala, slika, pjesama, određenih uspomena. Posao etičkog hakera je prepun izazova. Vrijedan zanat koji zahtjeva puno volje, znatiželje, strpljenja, obuke i predanosti. Završni rad je sažetak i opis različitih tipova hakera te njihovih uloga. Namjena rada je upoznavanje sa osnovnim principima vrlo zahvalnog i zanimljivog zanimanja. Predstavljeni sadržaj opisuje razliku između različitih pojmova, terminologija vezanih uz različite klasifikacije. Alati i primjeri napada koji se svakodnevno događaju i načini predviđanja i sprječavanja. Razvijanje mreže sigurnosti često koristi koncepte dubinske obrane. Slojevite kontrole pristupa u svrhe dodatne zaštite, proizlaze iz iste ili iz različitih kategorija, a njihova implementacija obuhvaća tri glavne kategorije kontrole pristupa (administrativna, logička i fizička).

Potrebno je naglasiti kako je svaki segment u procesu etičkog hakiranja izrazito važan i ključan, kako je ispravno testiranje sustava jedino ono u kojemu je etički haker, uzeo u obzir svaki

segment svog posla, posložio plan, dokumentirao i dao povratne informacije kako bi se pravodobno moglo strukturirati sigurno okruženje, kako za organizaciju tako i za radnike, zaštiti podatke i unaprijediti poslovanje. Unaprjeđenje poslovanja je i educiranje cjelokupne organizacije. Etički hakeri educiraju o svojim pronalascima i izvještavaju o svojim pronalascima, zato je i bitan proces kod same organizacije, pravovremena edukacija radnika i osvještavanje kako bi se proces stvaranja sigurnog okruženja i stabilnog sustava moga odvijati uz što manje rizike i prijetnje. Temeljna svrha završnog rada upravo je upoznavanje kroz različite procese, posao etičkog hakera i šarolikosti tematike koje je potrebno prikupiti i prilagođavati, primjenjivati prilikom obavljanja ovog zanimanja.

Završni rad baziran je na planiranju i opsegu, važnosti i zahtjeva opsega klijenta, onoga kome se pruža usluga osiguranja informacijskog sustava obzirom na scenarije, načine razmišljanja i održavanja profesionalizma i integriteta prilikom etičkog hakiranja, načina prikupljanja informacija, unaprijed predviđenih mogućih scenarija i ranjivosti. Analiza i primjena stečenih znanja u davanju prioriteta rizicima, ovisno o opasnosti koju pružaju i brzini kojom ih se mora otkloniti te pravilno i pravovremeno obavještavanje radi održivosti sigurnosti informacijskih sustava.

2. CILJ I SVRHA ETIČKOG HAKIRANJA

2.1. Informacijska sigurnost

Važnost etičkog hakiranja usko je povezano sa poznavanjem osnova informacijske sigurnosti, prije konkretne definicije etičkog hakiranja i dubinske analize istog razjašnjeni su osnovni pojmovi informacijske sigurnosti, odnosno najbitniji pojmovi i njihove definicije. Spomenut je *C.I.A.* model, temeljni pojam i sažetak svrhe, načina i cilja informacijske sigurnosti .

Tablica 1. C.I.A. model

C	*I*	*A*
CONFIDENTIALITY *TAJNOST*	*INTEGRITY* *INTEGRITET*	*AVAILABILITY* *DOSTUPNOST*
Informacija se smatra tajnom ukoliko je zaštićena od otkrivanja, izlaganja neovlaštenim korisnicima	Informacija posjeduje cjelovitost kada je potpuna i nepromijenjena, kada je u izvornom stanju	Informacija mora biti dostupna autoriziranim korisnicima

Tajnost osigurava pristup isključivo ovlaštenim korisnicima. Zaštitu tajnosti informacija postiže se*: klasifikacijom informacija, zaštitom pohrane, primjenom općih pravila zaštite, obrazovanjem krajnjih korisnika informacija*.

Tajnost informacija je jedna od ključnih značajki današnjih informacijskih sustava (EU i GDPR). Pokušaji promjene izvornog stanja informacije smatraju se narušavanjem njene cjelovitosti, a narušavanje cjelovitosti događa se i u procesu pohrane ili prijenosa informacija nastavno na činjenicu kako određeni dio računalnog Malware-a narušava cjelovitosti informacija. Cjelovitost informacija se štiti stvaranjem hash-a, a hash predstavlja osnovu antivirusne i kriptografske zaštite današnjih računalnih sustava. Autorizirani korisnici moraju imati neometani pristup informacijama te ih primati u traženom obliku, primjerice pristup online bazama znanstvenih i stručnih članaka. Osnovna svrha je evidentiranje svih procesa, događaja unutar štićenog područja. Prate se neovlašteni pokušaji upada, razlozi kvarova dijelova sustava, korištenje računalnih

resursa. Najčešća primjena je putem sistemskih dnevnika (log-ova). Razina praćenja određena je prema potrebama sustava (manje ili više detalja). Redovito predgledavanje dnevnika aktivnosti je ključno kako za otkivanje mogućih nedostataka sustava. Autorizacija je zasnovana na izdavanju autorizacijskih vjerodajnica, odnosno autorizacijskih karta. Izdane autorizacijske vjerodajnice nazivaju se i Single Sign-On (*SSo*) ili Reduced Sign-On. Proces uparivanja autentificiranog entiteta (korisnika) s popisom informacijske imovine i pripadajućim razinama pristupa, najčešće se zasniva na Access Control List (*ACL*). Provodi se *pojedinačno, grupno ili centralno*.

Kontrola pristupa je metoda pomoću koje sustavi određuju pravo i način pristupa zaštićenom dijelu organizacije. Kontrola pristupa zasnovana je na dopuštenjima koja određeni subjekt (osoba ili sustav) posjeduje za pristup određenim objektima (resursima). Definira ako subjekt smije ili posjeduje pristup objektu i na koji način ga koristiti.

Tablica 2. Podjela kontrola pristupa

Obavezna	*Neobavezna*
Funkcija - Organizacijska zaduženja (npr. Voditelj projekta, Sistemski administrator) *Radni zadaci* - Prikupljanje, pohrana podataka u pripremi za projekt *Klasifikacija* - Sve informacije i svi korisnici su kategorizirani sukladno pripadnosti kategoriji prava pristupa podacima	*PEER TO PEER* – Kontrolu pristupa definira korisnik u čijem posjedu se nalaze podaci za razliku od obavezne kontrole pristupa koju definira organizacija

Učinkovita zaštita podataka zahtjeva upravljanje njihovim korištenjem i nakon napuštanja zaštićene okoline. Svaki podatak koji napušta sigurnu okolinu treba sadržavati slijedeće elemente:

- *Kategorizacijske meta-podatke*
- *Kontrolu pristupa*
- *Informacije o pravima pristupa korisnika*

IRM (Information Rights Management) je kombinacija enkripcije i kontrole pristupa ugrađena u dokumente i sam softver. Omogućava pregledavanje dokumenata. Sužava

sigurnosno okruženje na razinu samih podataka i pruža zaštitu podataka svih vrsta medija za pohranu podataka. Štiti mrežnu komunikaciju i baze podataka.

IRM sustav treba posjedovati slijedeće osobine :

1. *Stalna kontrola pristupa podacima*
2. *Enkripcija sadržaja*
3. *Kontrola prava pristupa temeljem provedene autentifikacije*
4. *Offline pristup podacima*
5. *Detaljna kontrola prava pristupa podacima*
6. *Nadzor i izvještavanje*

Pojam informacijske sigurnosti je širok. Navedene su osnovne informacije potrebne za spoznaju svrhe i cilja ovog završnog rada i usku povezanost etičkog hakiranja i informacijske sigurnosti.

2.2. Etičko hakiranje

„I'm still a hacker. I get paid for it now. I never received any monetary gain from the hacking I did before. The main difference in what I do now compared to what I did then is that I now do it with authorization.“ [1][1]

Najjednostavnije rečeno i sažeto, etičko hakiranje uključuje ovlašteni pokušaj neovlaštenog pristupa računalnom sustavu, aplikaciji ili podacima. Uključuje dupliciranje strategija i radnji zlonamjernih napadača. Pruža identifikaciju sigurnosnih propusta i omogućava njihovo rješavanje i sprječavanje zlonamjernih napada.

Etički hakeri, poznati i kao „White hackers“, sigurnosni su stručnjaci koji vrše procjene ranjivosti sustava te ih svojim znanjem pronalaze i otklanjaju. Proaktivno pomažu poboljšanju sigurnosnog položaja organizacije. Dopuštenjem organizacije ili vlasnika IT imovine ciljano vrše napade ali u suprotne svrhe od zlonamjernih napadača.
Ključni koncepti etičkog hakiranja obuhvaćaju 4 protokola kojih se svaki etički haker treba držati kako bi mogao što učinkovitije obavljati svoj posao.

Tablica 3. Osnovni koncepti i protokoli koje bi svaki etički haker trebao slijediti

[1] (Mitnick, n.d.)

Koncept	*Opis*
Legalnost	Prije pristupa i izvođenja sigurnosne procjene odobrava se test.
Definiranje opsega	Određuje se i definira opseg procjene tako da hakiranje ostane u legalnim granicama i unutar odobrenja organizacije.
Prijava ranjivosti	Obavještava se organizacije o svim ranjivostima za zaštitu informacija. Savjetuje se organizacije i saniraju ranjivosti.
Poštivanje osjetljivosti informacija	Etički hakeri pristaju na sporazum, ugovor o ne otkrivanju podataka, uz druge uvjete i odredbe koje zahtjeva organizacija.

RAZLIKE ETIČKIH I ZLONAMJERNIH HAKERA

Etički hakeri svoje znanje i vještine koriste u svrhe osiguranja i poboljšanja tehnologija. Pružaju bitnu uslugu, odnosno ključnu uslugu organizacijama za poboljšanje sigurnosnih uvjeta, pronalaženje ranjivosti i otklanjanje prijetnji. Svojim radom štite tehnologije i onemogućavaju neovlašteni pristup zlonamjernih hakera. Posao etičkog hakera je identifikacija i prijava svake ranjivosti organizacije za koju radi, savjetovanje kako sanirati i uz pristanak organizacije ponavljati proces testiranja radi osiguravanja sustava i potpunog otklanjanja ranjivosti.

Zlonamjerni hakeri pokušavaju neovlašteno pristupiti resursima pojedine organizacije radi financijske dobiti ili osobnog priznanja (pojedinci hakiraju iz dosade, zbog uzdizanja vlastitog ega itd.). Zlonamjernim napadima uništavaju web stranice, ruše pozadinske poslužitelje, narušavaju ugled i uzrokuju financijske gubitke. Iskorištavaju ranjivosti radi vlastite koristi, ne brinu o poboljšanju sustava već iskorištavaju sve sigurnosne propuste unutar organizacije koju napadaju.

Cilj etičkog hakiranja je oponašanje napadača. Početni cilj je izviđanje i prikupljanje što većih količina informacija. Prikupljene informacije koriste se za traženje ranjivosti imovine. Procjena se provodi kombinacijom automatiziranog i ručnog testiranja. Etički hakeri koriste ranjivosti sustava za otkivanje načina koje bi zlonamjerni napadači iskorištavali za ilegalne napade. Najčešće ranjivosti obuhvaćaju injekcijske napade, prekinute autentifikacije i korištenje komponenti sa poznatim ranjivostima te se usmjeravaju na najosjetljivije podatke u svrhu njihove zlouporabe.

Krajnji dio etičkog hakiranja obuhvaća detaljno izvješće. Dokumentiraju se koraci korišteni za kompromitiranje otkrivenih ranjivosti te njihovo otklanjanje ili ublažavanje ovisno o mogućnostima.

Etičko hakiranje ima ograničeni opseg te etički hakeri ne mogu napredovati izvan definiranih granica. Pojedine organizacije omogućavaju etičkim hakerima širi opseg i dopuštenja pristupa sustavu. Pružaju bolji uvid u ranjivosti sustava, ali sve ovisi od organizacije do organizacije, kojim informacijama raspolaže, kojim resursima raspolaže, koliko su osjetljivi podaci i koliko je sama organizacija spremna ovlasti stručnjaka za etičko hakiranje jer je u konačnici najveća prijetnja informacijskoj sigurnosti čovjek. Etički hakeri raspolažu ograničenim resursima te posjeduju vremenski definirane rokove i financijski su ograničeni. Zlonamjerni hakeri djeluju neovisno o proračunu, ovlastima i rokovima. Napadi poput DoS (*Denial of Service*) napada ruše i uskraćuju usluge poslužitelja. Pojedine organizacije, izbjegavaju financijske troškove i ograničavaju etičke hakere u provođenju takvih i sličnih napada, ne razmišljajući pritom o financijskim troškovima u slučaju uspješnih napada zlonamjernih hakera.

„Hakeri razbijaju sustave radi zarade. Prije se radilo o intelektualnoj znatiželji, traženju znanja i uzbuđenja, a sada je hakiranje veliki posao.“ [2][2]

2.3. Sigurnosne prijetnje računalnim sustavima

Mnogobrojne su prijetnje informacijskoj sigurnosti, poput softverskih napada, krađe intelektualnog vlasništva, identiteta, opreme ili informacija, sabotaže i iznuda informacija. Svaka ranjivost koja se može iskoristiti u zlonamjerne svrhe je prijetnja informacijskoj sigurnosti. Informacije su podložne promjenama, trajnim gubitcima koji uzrokuju velike financijske gubitke, reputacijski rizik, izlaganje osobnih informacija te njihovu zlouporaba i iskorištavanje u ilegalne svrhe.

Softverski napadi su najčešći oblik napada. Softverski napadi su naizgled vrlo slični. Njihova sličnost je jedino svrha, a svrha je uništavanje i zlouporaba. Djelovanja pojedinih zlonamjernih softvera se uvelike razlikuju, ovisno koliku i kakvu štetu

[2] (Mitnick, n.d.)

napadač želi napraviti žrtvi napada, koje su napadačeve namjere te koji je razlog napada. Zlonamjerni softveri dijele se u dvije kategorije:

- *Metode infekcije (Infection Methods)*
- *Radnje zlonamjernog softvera (Malware Actions)*

Napredak tehnologije i sve veći broj korisnika pruža hakerima sve veće izazove i mogućnosti eksploatacije i zlouporabe podataka. Svakodnevno raste znanje i povećava se broj dostupnih informacija i alata koje vješti zlonamjerni hakeri iskorištavaju za ilegalne radnje. Etički hakeri sprječavaju i predviđaju takve napade. Sprječavaju napade koristeći se istim metodama kojima bi se koristili zlonamjerni hakeri ali samo za zaštitu sigurnosti informacijskih sustava.

„When solving problems, dig at the roots instead of just hacking at the leaves.“ [3][3]

2.4. Potrebne vještine za etičko hakiranje

„Develop a passion for learning. If you do, you will never cease to grow.“ [4][4]

Etički hakeri trebaju širok raspon računalnih vještina. Najčešće se usmjeravaju i specijaliziraju za određena područja etičkog hakiranja.

Etički hakeri moraju imati navedena znanja i vještine:

- Stručnost u programskim jezicima
- Poznavanje operativnih sustava
- Temeljito poznavanje računalnih mreža
- Temelj u načelima informacijske sigurnosti

Najpoznatiji certifikati etičkih hakera:

- EC Council: Certified Ethical Hacking Certification
- Offensive Security Certified Professional (OSCP) Certification
- CompTIA Security+

[3] (D'Angelo, n.d.)
[4] (D'Angelo, n.d.)

3. TEHNIKE HAKIRANJA

3.1. Kategorije zlonamjernih softvera

Prijetnje informacijskoj sigurnosti su iskorištavanje ranjivosti sustava te napadi koji uključuju korištenje zlonamjernih softvera. Zlonamjerni softveri dijele se u dvije kategorije koje sadrže različite vrste softvera u ovisnosti kojoj kategoriji pripadaju.

Tablica 4. Kategorizacija zlonamjernih softvera

Metode infekcije	*Radnje zlonamjenog softvera*
Virusi	Adware
Crvi	Ransomware
Trojanci	Spyware
Botovi	Scareware
	Zombie
	Rootkit

Virusi se repliciraju povezivanjem sa programom na računalu žrtve, primjerice pjesmama, videozapisima itd., potom putuju po internetu. Prvi virus je otkriven na ARPANET-u.

Crvi se kao i virusi umnožavaju ali se ne vežu na program na računalu žrtve već mrežom putuju sa računala na računalo dok postoji mrežna konekcija. Virusi nemaju takvu mogućnost. Crvi nanose štetu poput zauzimanja prostora na tvrdom disku i na taj način usporavaju rad računala.

Trojanci se konceptualno potpuno razlikuju od virusa i crva. Svrha im je skrivanje unutar softvera koji se čini legitiman. Trojanci se aktiviraju pokretanjem aplikacije. Odrađuju svoj zadatak, ovisno o cilju napada. Primjeri su krađa podataka, izmjena podataka, itd. Omogućavaju „backdoor gateway“, ulaz u sustav i pristup informacijama te manipuliranje sustava bez znanja žrtve.

Bot je napredni oblik crva. Dizajniran je za automatiziranu interakciju putem interneta. Dijele se na dobre i loše. Zlonamjerni bot-ovi parazitiraju kod jednog domaćina (host) te se potom šire na sve domaćine unutar mreže kojima mogu pristupiti i pritom stvaraju zaraženu mrežu zvanu Botnet.

Adware nije toliko zlonamjeran ali krši privatnost korisnika na način da prikazuju oglase na radnoj površini ili unutar programa te daje napadačima pristup interesima korisnika te na taj način korisniku prikazuju relevantne oglase za softvere. Napadači unutar softvera udrađuju zlonamjerni kod i na taj način ugrožavaju sustav korisnika.

Ransomware šifrira datoteke ili zaključava računalo čineći ga potpuno ili djelomično nedostupnim. Prisiljava korisnika / žrtvu da uplati novac, otkupninu u zamjenu za funkcionalno računalo i pristup informacijama unutar datoteka.

Spyware prati aktivnosti na računalu, otkriva i prikuplja podatke. Trojanci, virusi i crvi većinom ispuštaju spyware prilikom pokretanja. Nakon ispuštanja pokreće se automatizmom, sam se instalira i teško ga je otkriti. Najčešći spyware je KEYLOGGER.

Scareware se ugrađuje(„maskira“) unutar softvera poput antivirusa. Prilikom pokretanja softvera izvršava napad, zarazi sustav ili ga potpuno uništi. Slično kao i ransomware, cilj je plašenje žrtve i tjeranje na plaćanje kako bi se sustav popravio.

Zombie ima slično djelovanje kao i spyware. Mehanizam je isti ali svrha mu nije špijuniranje sustava i krađa informacija već naredbe za određene radnje kojima napadač manipulira sustavom.

Rootkit služi za root pristup, odnosno dobivanje administrativnih privilegija u korisničkom sustavu. Administratorski pristup napadaču pruža upravljanje cijelim sustavom i omogućava uzastopne krađe privatnih datoteka i podataka.

Zlonamjerni softveri nisu jedine vrste napada. Alati su koji automatizirano djeluju i postupaju ovisno o napadačevim namjerama. Tehnologija je napredovala i time preglednici i antivirusni softveri pružaju dodatnu zaštitu prilikom korištenja interneta. Načini zaštite su primjeri poput razvrstavanja sigurnih i certificiranih sadržaja unutar baza podataka, upozoravanje korisnika kada pristupaju sadržaju koji nije provjeren, odnosno sadržaju koji je algoritam prepoznao kao sigurnosnu prijetnje. Zlonamjerni softveri se često spominju kao zastarjele metode ali su oni još uvijek aktivni i koriste se u svrhe napada.

Tablica 5. Najčešće teške posljedice napada

Vrsta	*Opis*
Krađa intelektualnog vlasništva	Kršenje autorskih prava, patenata itd.
Krađa identiteta	Djelovanje u svrhu prikupljanja osobnih podataka određene osobe te manipulacija njihovim korisničkim računima, bankovnim računima itd.
Krađa opreme i informacija	Ovakve vrste napada su sve veće zbog sve većeg korištenja mobilnih uređaja i kapaciteta informacija dostupnih unutar baza podataka
Sabotaža	Uništavanje web stranica organizacija kako bi korisnici izgubili povjerenje zbog narušene informacijske sigurnosti
Iznuda informacija	Krađa imovine ili podataka organizacije u svrhu ucjene radi financijske koristi, najčešći zlonamjerni softver koji se koristi za ovakvu vrstu ilegalne radnje je ransomware.

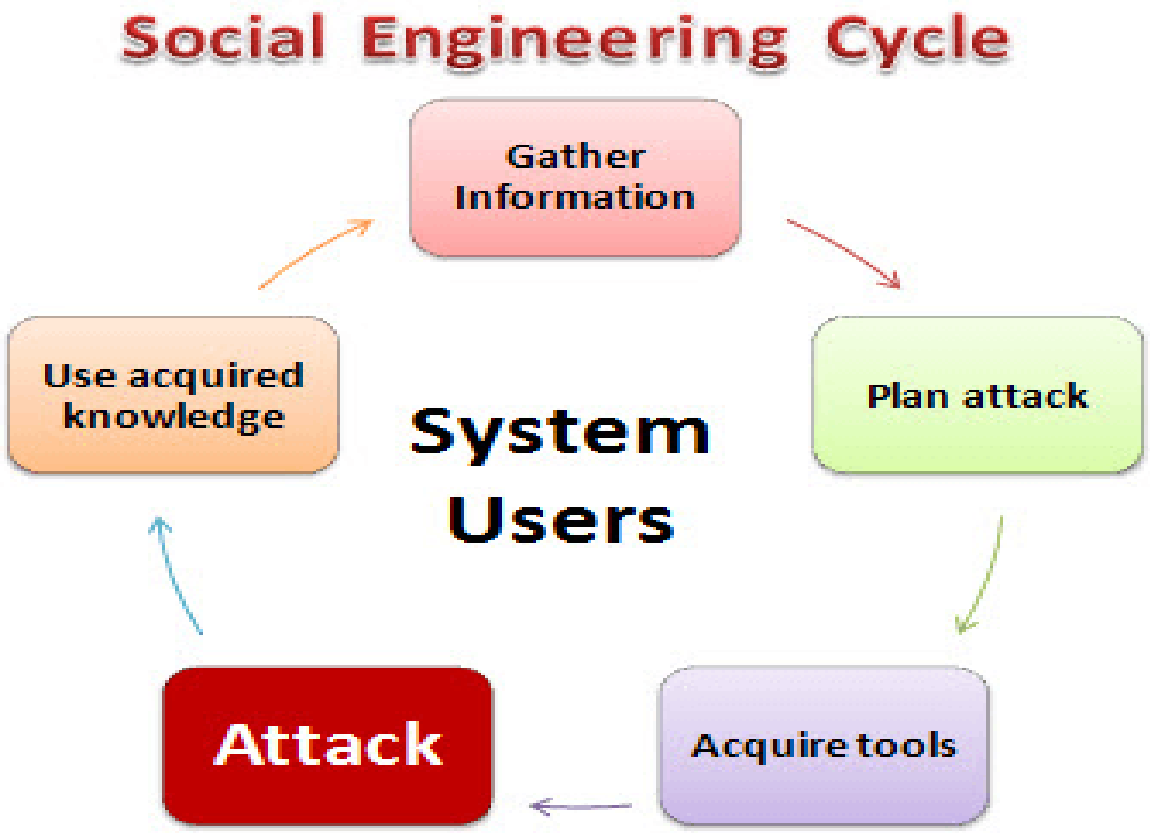
3.2. Social Engineering

"It is impossible to work in information technology without also engaging in social engineering." [5][5]

Socijalni inženjering (Social Engineering) umjetnost je manipuliranja korisnicima računalnog sustava u svrhu otkrivanja osobnih i povjerljivih informacija. Napadač može iskoristiti socijalni inženjering za neovlašteni pristup računalnom sustavu. Socijalni inženjering uključuje aktivnosti poput iskorištavanja ljudske dobrote, navođenja žrtve na uplatu u „humanitarne svrhe“, a u konačnici uplaćeni novac završava

[5] (Lanier, n.d.)

kod napadača kojemu je cilj financijska korist. Iskorištavanje ljudske pohlepe također pripada pojmu socijalnog inženjeringa. Žrtvu se navodi na uplatu nekog novčanog priloga ili otkrivanje osobnih podataka obećanjem kako će na taj način zaraditi novac. Socijalni inženjering obuhvaća i manipuliranje žrtvom obećanjima. Cilj je prikupljanje onoga što je napadaču potrebno od same žrtve. Napadač nudi pristup zgradama sa ograničenim pristupom ili navodi žrtvu na instaliranje softvera koji napadaču daje pristup svim informacijama i cijelom sustavu. Obrana od ovakvih i sličnih napada moguća je edukacijom o najčešćim tehnikama koje se koriste u socijalnom inženjeringu.



Slika 1. Krug napada socijalnim inženjeringom
(https://cdn.guru99.com/images/EthicalHacking/img_social_cycle.png)

Krug predstavlja niz radnji koje napadač vrši za uspjeh prilikom ovakve vrste napada. Prva faza obuhvaća učenje, prikupljanje što većeg broja informacija o žrtvi. Podaci su prikupljeni putem web stranica tvrtke, publikacija, društvenih mreža, internet je ključno sredstvo za prikupljanje takvih informacija jer je sve veći broj korisnika raznih servisa koji olako izlažu svoje osobne informacije u javnosti. Kontaktiranjem žrtve, ostvarivanjem prijateljskog odnosa i dobivanjem povjerenja žrtve napadač može otkriti

što više osobnih informacija od same žrtve. Planiranjem napada razvija se strategija za iskorištavanje informacija. Socijalni inženjering uključuje fazu korištenja alata poput zlonamjernih softvera, preusmjeravanje na „lažne“ web stranice. Završetkom faze kreće novi ciklus. Napadač koristi stečeno znanje i kreira strategiju za iskorištavanje informacija, primjerice za otkrivanje lozinki. Najčešće korištene lozinke su upravo osobni podaci žrtve, njihovi interesi, imena kućnih ljubimaca, imena voljenih osoba, datumi rođenja itd.

TEHNIKE SOCIJALNOG INŽENJERINGA

Iskorištavanje poznanstva sa žrtvom pruža napadaču prikupljanje sve većeg broja informacija o samoj žrtvi te pod maskom prijateljstva zapravo iskorištava žrtvu u svrhe vlastite koristi. Iskorištava se žrtvino povjerenje.

Metode zastrašivanja žrtve uključuju napadačevu manipulaciju ljudskim socio–emocionalnim reakcijama na određene situacije. Metoda zahtjeva poznavanje psihologije i ljudske prirode, takvi napadači su vješti manipulatori. Žrtva nasjeda na metode zastrašivanja i zbog svoje prirodne reakcije na situaciju odaje napadaču informacije radi izbjegavanja eventualnog sukoba.

Lažno predstavljanje obuhvaća trikove i prijevare za prikupljanje privatnih i osjetljivih informacija. Primjeri su lažne e–mail adrese organizacija kojima napadač oponaša iste i navodi žrtvu na otvaranje web stranica koje su naizgled iste kao i stranice organizacije. Prikupljaju podatke poput korisničkog imena i lozinke.

Tailgating je isto tehnika manipulacije, praćenje žrtve u ograničena područja i korištenje raznih psiholoških tehnika za navođenje na pristup zabranjenim područjima.

Iskorištavanje ljudske znatiželje je tehnika kojom napadač ciljano ostavlja, na vidljivim i lako dostupnim mjestima CD, DVD, USB ili bilo koje sredstvo sa malicioznim softverom. Znatiželja je sastavni dio ljudske prirode i žrtva uzima sredstvo zaraze te prilikom pokretanja aktivirati virus ili iz znatiželje otvara neku datoteku koja pokreće virus.

Iskorištavanje ljudske pohlepe je jedna od najučinkovitijih metoda socijalnog inženjeringa. Napadač obećanjem korisniku kako će zaraditi velike količine novca ispunjavanjem obrasca i potvrdom podataka, u konačnici prikuplja podatke o kreditnim karticama, osobne podatke itd.

Većina tehnika socijalnog inženjeringa uključuje manipuliranje ljudskom psihom zato je u svrhu zaštite od takvih napada ključno poznavanje tehnika kojima se napadači služe i znanje za obranu korištenjem raznih sigurnosnih mjera. Prepoznavanje znakova lažnog prijateljstva, reakcije u situacijama zastrašivanja, provjera legitimnosti web stranica koje se posjećuju i poznavanje podataka koje organizacije ne smiju nikada tražiti niti ih se smije ikome odavati svakako su jedne od bitnijih stavki informacijske sigurnosti. Zaštita od iskorištavanja putem ljudske znatiželje iziskuje detaljno skeniranje sredstva na eventualne zlonamjerne softvere prije samog pokretanja, na izoliranom računalu koje ne sadrži osjetljive podatke i čiji eventualni pad sustava neće nanijeti nikakvu štetu. Zaposlenike se mora educirati o prijetnjama informacijskoj sigurnosti, opasnostima i načinima prijevara kojima se služe napadači.

3.3. Kriptografija

Kriptografija je znanost koja proučava i primjenjuje tehnike koje skrivaju pravo značenje informacija na način da se informacije kriptiraju, odnosno pretvaraju u nečitljive formate. Kriptografija također obuhvaća dekriptiranje, tehniku koja iz nečitljivih formata konvertira informacije u izvorno stanje. Predstavljala je sinonim za šifriranje, no u današnjici se uglavnom temelji na matematičkoj teoriji i informatičkoj praksi.

Svrha kriptografije je *povjerljivost*, *integritet*, *neporecivost* i *autentifikacija*. Cilj je zaštita informacije pretvaranjem u nečitljive formate i postizanje povjerljivosti, odnosno sigurne razmjene informacija. Podaci se čuvaju na način da se štiti sam sadržaj od eventualnih izmjena. Izmjene se tehnikama poput hashiranja otkrivaju na vrijeme usporedbom hash-eva. Podaci koji se šalju su neporecivi i time ne daju pošiljatelju mogućnost manipulacije u kasnijim fazama. Autentifikacijom pošiljatelj i primatelj u svakom trenutku potvrđuju svoj legitimitet. Najčešće korištene kriptografske tehnike su kriptografija sa *simetričnim / asimetričnim ključem te hash funkcije.*

"One must acknowledge with cryptography no amount of violence will ever solve a math problem." [6][6]

Tablica 6. Podjela enkripcije podataka prema vrsti

Simetrični ključ	*Asimetrični ključ*	*Hash funkcije*
Pošiljatelj i primatelj dijele 1 ključ koji pošiljatelj koristi za šifriranje (konverziju iz prvotnog stanja u nerazumljivi oblik), a primatelju taj isti ključ služi za dešifriranje podataka (vraćanje poruke u izvorno stanje)	Tehnika asimetričnog ključa, odnosno korištenjem 2 ključa, javnog i privatnog je jedan od najrevolucionarnijih koncepata u posljednjih 300 – 400 godina. Koriste se 2 povezana ključa. Javni ključ se slobodno distribuira, a privatni ključ je jedinstven za korisnika Svrha privatnog ključa je dešifriranje podataka koji su prethodno šifrirani pomoću javnog ključa.	Algoritam ne koristi ključeve. Hash je vrijednost fiksne duljine Izračunava se ovisno o tekstu te ne postoji mogućnost reverzibilnosti. Najčešće se koristi u svrhu zaštite lozinki te za provjeru legitimnosti aplikacija i podataka koje korisnici preuzimaju sa interneta..

Simetrični ključ je zastarjela tehnika i sve se manje koristi jer iako pruža brži prijenos informacija, ranjiva je tehnika zaštite informacija. Asimetrični ključ, kod kojeg je prijenos informacija, odnosno proces razmjene nešto sporiji ali su zato podaci zaštićeniji i teže im je pristupiti. Asimetrični ključ se sve više koristi i mijenja prvotnu tehniku šifriranja simetričnim ključem. Hash funkcije ne služe za razmjenu poruka, odnosno šifriranje i dešifriranje, već samo koriste algoritme za šifriranje radi onemogućavanja konverzije poruke u izvorno stanje, odnosno nema dešifriranja podataka.

3.4. Kripto analiza

Proučavanje tehnika i metoda za prikupljanje saznanja o šifriranim informacijama, bez posjedovanja tajnih podataka potrebnih za dešifriranje naziva se kripto analiza. Obično se proučavaju načini otkrivanja tajnih ključeva.
Korisna je za označavanje svakog pokušaja zaobilaženja drugih tipova kriptografskih algoritama i protokola. Pomoću matematičke analize i kriptografskih algoritama

[6] (Appelbaum, 2012)

uključuje proučavanje „*Side–channel*“ napada. Takvi napadi iskorištavaju slabosti u implementaciji kriptografskih algoritama. Metode kripto analize drastično su se mijenjale kroz povijest radi sve bržeg i sve većeg tehnološkog napretka te promjene ciljeva i svrha korištenja. Jedna od prvih tehnika kripto analize je olovka i papir. Dešifriranje teksta pomoću logičkog razmišljanja, dostupnih informacija te prenošenjem dobivenog teksta olovkom na papiru. Nakon olovke i papira nastali su strojevi, poput britanskih bombi i računala „Colossus“ u Drugom svjetskom ratu, potom sve do naprednih računalnih shema u sadašnjosti.

Najčešće korištene metode razbijanja suvremenih kripto sustava uključuju rješavanje problema čistom matematikom, a najpoznatija takva metoda je *cjelobrojna faktorizacija*. Cilj kripto analize je šifrirani podatak vratiti u izvorno stanje, odnosno u čitljivi tekstualni format.

NAPADI

Klasificiraju se u ovisnosti o vrsti informacija kojima napadač raspolaže Najčešća pretpostavka je kako se napad vrši u svrhu analize te da je na osnovu te svrhe opći algoritam poznat.

“The enemy knows the system” [7][7]

– ekvivalentno Kerckhoffsovom principu.

Pretpostavka se zasniva na iskustvima u praksi, kroz povijest, odnosno na višestrukim primjerima algoritama čija je tajnost narušena principima poput špijunaže, obrnutog inženjeringa, odavanjem tajnih informacija, korištenjem čiste dedukcije, primjer takvog proboja je njemačka Lorenzova šifra i japanska ljubičasta šifra.

[7] (Shannon, n.d.)

Tablica 7. Klasifikacija napada ovisno o vrsti raspoloživih informacija

Vrsta	*Opis*
Šifrirani tekst	Pristup samo zbirci šifriranih tekstova / kodnih tekstova
Dešifrirana i pripadajuća šifrirana poruka	Pristup nizu šifriranih tekstova za koje su poznati odgovarajući dešifrirani tekstovi.
Šifrirani tekstovi koji odgovaraju proizvoljnom skupu otvorenih tekstova	Pristup šifriranom tekstu i proizvoljnom skupu odgovarajućeg dešifriranog teksta.
Iskustvo i naučena znanja	Opsežno znanje iz prijašnjih dešifriranja, korištenje dedukcije i iskustva, znanja i vještina
Povezani ključevi	Poznavanje veze između dva nepoznata ključa (npr. dvije tipke koje se razlikuju u jednom bitu)

POTREBNI RAČUNALNI PARAMETRI ZA USPJEŠAN NAPAD

Postoje tri ključna parametra potrebna za napad. Često je takve parametre teško predvidjeti ali akademski kripto analitičari procjenjuju vrijednosti koje, iako nisu precizne, olakšavaju uvid u veličinu teškoća prilikom kripto analize. Uspjeh samih napada dosta ovisi o parametrima.

Tablica 8. Raspodjela potrebnih informacija za uspješnost napada

Vrsta informacije	*Primjer informacije*
Vrijeme	Broj koraka (npr. Test šifriranja)
Memorija	Količina memorije potrebna za izvođenje napada
Podaci	Vrsta i količina dostupnih dešifriranih tekstova

„Razbijanje šifre jednostavno znači pronalaženje slabosti u šifri koja se može iskoristiti sa složenošću manjom od grube sile (Brute - force)“ [8][8]

Lars Knudsen 1998. godine klasificirao je različite vrste napada na blok – šifre prema kvantitetu i kvaliteti otkrivenih tajnih informacija.

Tablica 9. Klasifikacija napada na blok-šifre prema kvantitetu i kvaliteti otkrivenih informacija (Lars Knudsen, 1988.)

Vrsta	*Opis*
Totalni prekid	Napadač dolazi do tajnog ključa
Globalna dedukcija	Pronalazak funkcionalno ekvivalentnog algoritma za šifriranje i dešifriranje ali bez posjedovanja tajnog ključa
Lokalna dedukcija	Pronalazak dodatnih dešifriranih / šifriranih tekstova koji prije nisu bili poznati
Informacijska dedukcija	Pronalazak podataka o šifriranim / dešifriranim tekstovima koji prije nisu bili poznati
Algoritam razlikovanja	Razlikovanje šifre od slučajne permutacije

Kripto analitičari često za napade koriste oslabljene verzije kripto sustava poput blok–šifri i hash funkcija s uklonjenim rundama. Mnogobrojni napadi su sve teže uspješni dodavanjem rundi u kripto sustave. Uspješnom napadu na *DES, MD5 i SHA- 1* prethodio je napad na oslabljene verzije istih. Često je korištenje nerealnih uvjeta u napadima za otkrivanje slabosti. Jedan od primjera je šifriranje poruka pomoću većeg

[8] (Knudsen & Robshaw, 2011)

broja ključeva. Primjene takvih metoda otkrivaju tek maleni ili gotovo nikakav broj podataka koji mogu biti korisni u stvarnom svijetu prilikom pravih napada. Napadi su primjenjivi samo na oslabljene verzije kriptografskih alata ali u konačnici i na taj način napreduje se ka razbijanju čitavog sustava.

3.5. Algoritmi za šifriranje podataka

MD5(Message – Digest 5)

Ovaj algoritam se koristi za stvaranje 128 – bitnih hash vrijednosti. Primjenjuje se za zaštitu / šifriranje lozinki i provjeru integriteta podataka. Nije otporan na koliziju odnosno poteškoću u pronalaženju dvije vrijednosti koje produciraju jednaku hash vrijednost.

SHA(Secure Hash Algorithm)

Primjenjuje se za generiranje sažetih poruka. Postoje različite inačice ovog algoritma jer su se vremenom uvidjeli nedostaci i postepeno nadograđivali.

SHA – 0 : Proizvodi 120- bitne hash vrijednosti. Ne upotrebljava se jer ima značajne nedostatke.

SHA – 1 : Zamijenio je SHA – 0 te proizvodi 160 – bitne hash vrijednosti. Vrlo je sličan ranijim verzijama MD5 algoritma. Otkrivene su mu kriptografske slabosti zbog kojih ga od 2010. godine ne preporučuju za upotrebu.

SHA – 2 : SHA – 256 i SHA -512 su njegove dvije hash funkcije. SHA – 256 koristi 32 – bitne riječi, a SHA – 512 64 – bitne riječi.

SHA – 3 : Algoritam poznat kao Keccak

RC4

Algoritam grube sile stvara stream šifre. Najčešće se koristi u protokolima poput SSL(Secure Socket Layer) za šifriranje komunikacije putem interneta i WEP(Wired Equivalent Privacy) zaštitu bežičnih mreža.

BLOWFISH

Algoritam za stvaranje simetričnih blokiranih šifri s ključem. Većinom se koristi za šifriranje lozinki i podataka.

„Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin.“ [9][9]

3.6. CrypTool

CrypTool 1 je edukativni alat otvorenog koda za kripto- logičke studije. Alat prilikom otvaranja već sadrži nekakav predefinirani tekst. Zamjenjuje se tekstom koji se šifrira.

ŠIFRIRANJE

Izbornik sadrži *Encrypt / Decrypt* opciju koja otvara padajući izbornik sa opcijama, načinima na koji se želi šifrirati neki tekst, u padajućem izborniku odabirom *Symmetric(modern)* i potom *RC4*, otvara se prozor koji omogućava odabir duljine ključa i polje za unos samog ključa enkripcije. (Npr. Duljina ključa 24 – bita i unos u polje 00 00 00)

DEŠIFRIRANJE

Izbornik sadrži *Analysis* opciju. Odabirom ove opcije otvara se padajući izbornik koji sadrži različite vrste algoritama za šifriranje. Odabirom vrste algoritma kojom se prije šifrirala poruka alat omogućava dešifriranja poruke. Proces zahtjeva određene vještine u procjeni duljine samog ključa kojom se poruka šifrirala. Vrijeme potrebno za ovakvu vrstu napada ovisi o kapacitetu samog računala s kojeg se vrši napad te duljini ključa. Što je duljina ključa veća to je sam proces dešifriranja sporiji.

ANALIZA

Kada je proces analize završen alat daje rezultate u obliku tablice sa kolonama. Ključni podatak pomoću kojeg se otkriva izvorni tekst se nalazi u koloni “Entropy”. Manje vrijednost znači veću točnost rezultata. Odabirom reda, koji je po procjeni, na osnovu „Entropy“ podatka najtočniji i pritiskom tipke *Accept Selection* alat ispisuje krajnji rezultat.

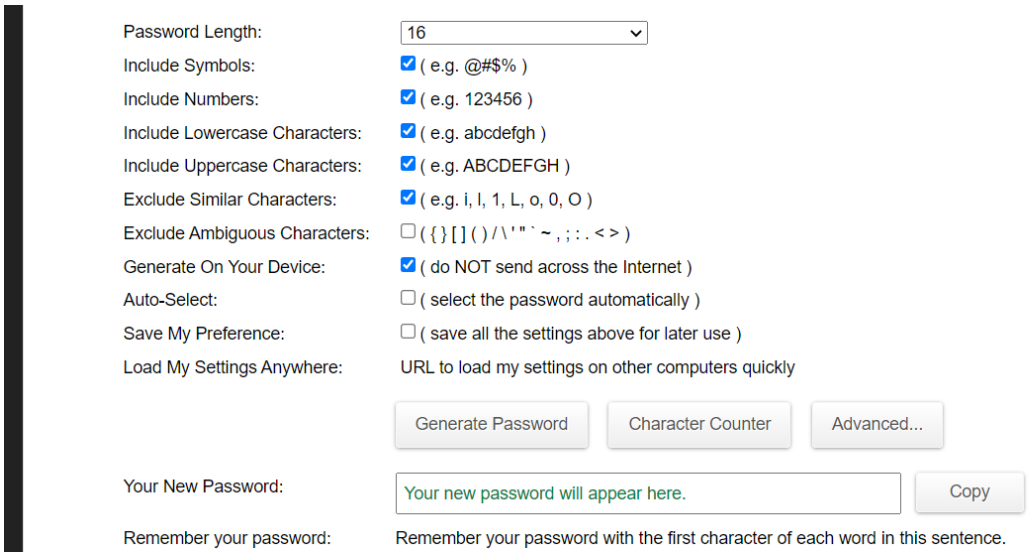
[9] (Neumann, n.d.)

3.7. Krekiranje lozinki aplikacija

Umjetnost dobivanja ispravne lozinke za pristup sustavu pomoću pogađanja lozinki i korištenjem algoritama. Koriste se mnogobrojne tehnike za ostvarivanje krajnjeg cilja, a sam postupak uključuje usporedbu pohranjenih lozinki sa popisom riječi ili tehniku poput algoritama za generiranje podudarajućih lozinki. Lozinke dijelimo u kategorije po jačini. Parametri potrebni za kreiranje što snažnije lozinke su duljina, preporučeno 8 znakova. Složenost je isto bitan parametar, preporučeno je korištenje kombinacije velikih i malih slova, brojki i simbola te zadnji i vrlo bitan parametar je nepredvidivost lozinke, ovaj parametar povezan je uz napad socijalnim inženjeringom. Popularno je korištenje lozinki koje sadrže značajne podatke poput imena kućnih ljubimaca, voljenih osoba, nekih interesa, datum rođenja itd.

„I needed a password eight characters long so I picked Snow White and the Seven Dwarves“ [10][10]

Postoje različite web stranice koje pružaju mogućnost generiranja jake lozinke. Primjer takve stranice je https://passwordsgenerator.net/.
Web aplikacija sadrži DDLB(DropDownListBox) za odabir duljine lozinke, CheckBox–ove. Parametre ukoliko korisnik želi lozinku koja sadrži simbole, brojeve, velika slova, mala slova, bez sličnih znakova i određenih znakova, ukoliko korisnik želi lokalno generiranje lozinke.



[10] (Helm, n.d.)

Cpanel CRM sustav pruža mogućnost provjere jačine lozinke što je isto vrlo koristan alat prilikom odabira i kreiranja lozinke.

KREKIRANJE LOZINKE ŠIFRIRANE MD5 ALGORITMOM

Web aplikacija http://www.md5this.com/ omogućava korisnicima unos hash–a dobivenog šifriranjem lozinke MD5 enkripcijom te dešifriranje lozinke. Lozinke koje navedena aplikacija uspijeva dešifrirati su samo one čija snaga lozinke ne prelazi 50 % ukupne jačine.

Tablica 10. Najčešće tehnike hakiranja lozinki

Tehnika	*Opis*
Dictionary attack	Korištenje popisa riječi za usporedbu sa korisničkim lozinkama
Brute force attack	Korištenje algoritama koji kombiniraju alfanumeričke znakove i simbole
Rainbow table attack	Korištenje unaprijed izračunatog hasha. Primjer je baza podataka koja sadrži pohranjene lozinke šifrirane MD5 algoritmom. Napadač koristi drugu bazu sa najčešće korištenim lozinkama šifriranim MD5 algoritmom i ukoliko napadač pronađe podudaranje uspoređujući baze tada je lozinka otkrivena.
Guess	Pogađanjem često napadači dolaze do lozinki jer koriste najčešće korištene lozinke koje su obično postavljene kao defaultne postavke sustava. Ukoliko takve lozinke nisu na vrijeme promijenjene napadač ima pristup sustavu
Spidering	Većina organizacija upotrebljava u lozinkama sadržaje poput podataka o organizaciji koji su lako dostupni preko društvenih mreža. Napadač prikuplja informacije kako bi dobio popis riječi i tada koristi DICTIONARY ATTACK ili BRUTE FORCE ATTACK u svrhu napada

ALATI

John the Ripper

Pomoću command prompt–a napadač dohvaća lozinku. Pogodan je za napredne korisnike koji se snalaze sa naredbama u command prompt–u. Aplikacija je besplatna

ali popis riječi za dohvat lozinke se mora kupiti. Postoje i open source alternative popisa riječi. Primjer: https://www.openwall.com/john/

Cain & Abel

Dostupan za Windows OS, koristi se za oporavak lozinki za korisničke račune, Network Sniffing itd. Aplikacija ima grafičko sučelje te je vrlo često upotrebljavaju početnici zbog jednostavnosti uporabe. Pomoću aplikacije se izvršavaju Dictionary, Brute force napadi te kriptoanaliza.

Ophcrack

Radi na više operacijskih sustava Linux, Mac OS I Windows. Između ostalih značajki ima ugrađen modul za Brute force napade.

PRIMJER NAPADA CAIN & ABEL APLIKACIJOM

Aplikacija sadrži tipku u obliku plavog + znaka preko koje se radi import hash–a svih lokalnih korisnika. Pritiskom desne tipke miša na određeni korisnički račun pojavljuje se izbornik koji korisniku omogućava odabir vrste napada. Odabirom *Dictionary Attack –> NTML Hashes* otvara se novi prozor sa različitim mogućnostima. Desnim klikom na polje *Dictionary* otvara se izbornik u kojem se odabire opciju *Add to list* i potom pronalazi datoteku sa najčešće korištenim riječima. Pritiskom na tipku *Start*, unutar tekstualnog polja na dnu prozora, ukoliko je korištena neka od najčešće korištenih lozinki, pojavljuje se rezultat i napadač prikuplja informaciju, lozinku korisničkog računa. Vrijeme potrebno za otkrivanje lozinke ovisi o jačini i složenosti lozinke, ukoliko ovakav napad nije uspješan onda napadač može pokušati neke druge napade koje je moguće izvoditi korištenjem ove aplikacije.

3.8. ARP

Protokol za rješavanje adresa (ARP) predstavljen je 2001. godine i opisivalo ga se kao “radnog konja” koji ima mogućnost povezivanja s novim host-om na razini IP–a. Svrha ARP protokola je automatizacija procesa dodavanja novih funkcija bez autorizacije svakog zahtjeva. Temelji se na kontroli pristupa medijima. Svaki korisnik ima jedinstvenu MAC adresu na hardverskoj razini Ethernet mrežnog sučelja (NIC). Brojevi se dodjeljuju tvornički i moguće ih je promijeniti softverom.

ARP je zadužen za prihvaćanje zahtjeva za pridruživanje novog uređaja lokalnoj mreži pružajući IP adrese. Prevodi IP adresu u MAC te šalje zahtjev ako ne zna koju će MAC adresu dodijeliti za IP adresu novog uređaja, zahtjev šalje ostalim uređajima unutar mreže kako bi se dohvatili nedostajući podaci. Štedi vrijeme mrežnim administratorima. Proces se odvija u pozadini ali nosi sa sobom i određene rizike.

ARP NAPADI

Postoje dvije vrste ARP napada: *ARP spoofing* i *ARP poisoning.* Prilikom ARP spoofing-a, odnosno ARP lažiranja, napadač šalje lažne ARP pakete koji povezuju napadačevu MAC adresu sa IP adresom računala koje je već u lokalnoj mreži. Nakon uspješnog ARP spoofing napada, napadač kreće sa ARP poisoning napadom, mijenja ARP tablicu mete sa krivotvorenim MAC adresama. Zaraza se širi i krajnji cilj napada je povezivanje napadačeve MAC adrese sa čitavom lokalnom mrežom te preusmjeravanje cijelog prometa unutar mreže. Napadač prilikom uspješno izvedenog napada može pregledavati podatke prije nego oni dođu do krajnjeg korisnika i tražiti otkupninu kako bi osposobio rad unutar mreže. Man–in– the–middle napad omogućava napadaču manipulaciju gotovo svime unutar mreže osim izmjene podataka prije razašiljanja prema krajnjim korisnicima. Takvi napadi se smatraju jednim od najgorih i najtežih napada. ARP procesi istječu u roku od 60 sekundi ali mrežni zahtjevi mogu trajati i do 4 sata tako da napadači imaju dovoljno vremena za izvršavanje napada.

POZNATE RANJIVOSTI ARP PROTOKOLA

Ciljevi ARP-a prilikom njegovog razvoja bili su postizanje brzine, funkcionalnosti i autonomije, nije se vodila briga o sigurnosti i to ga je učinilo vrlo ranjivim i lakom metom napadača. Kako bi se izveli ARP napadi dovoljno je nekoliko alata i vještina:

- Konekcija / veza: Poveznica na jedan uređaj
- Vještine programiranja: Napadač mora znati zapisati ARP pakete koji se odmah prihvaćaju ili pohranjuju u sustav
- Vanjski alati: *Arpspoof* (slanje lažiranih odgovora)
- Strpljenje: Neki su hakeri brzi dok drugi moraju slati stotine paketa za pristup lokalnoj mreži

Unutar ARP sustava ne postoji nikakva provjera identiteta te na taj način korisnici ne mogu utvrditi jesu li paketi autentični ili od kuda su došli.

PREVENCIJA ARP NAPADA

Napadači koriste predvidljive metode napada poput slanja lažnih paketa i zahtjeva za povezivanjem s lažnim paketom te emitiranje zahtjeva na sva računala u lokalnoj mreži čime napad uspješno završava. Mrežni administratori mogu na dva načina otkriti lažni ARP paket.

Tablica 11. Načini otkrivanja lažnih ARP paketa

Način	*Opis*
Pasivno otkrivanje	Praćenjem prometa i gledanjem ima li nedosljednosti u mapiranju
Aktivno otkrivanje	Ubrizgavanjem krivotvorenih ARP paketa u mrežu koji omogućavaju identificirati slabe točke na sustavu i daju mogućnost brze sanacije i zaustavljanje napada ukoliko je u tijeku. Pisanje vlastitog malicioznog koda za otkrivanje ranjivosti dolazi sa rizicima ali je isto jedan od načina otkrivanja ranjivosti sustava. Ukoliko je protokol strog, lažni alarmi usporavaju pristup, a u suprotnosti ukoliko je protokol sa prevelikim pristupom napadi u tijeku se zanemaruju te se na taj način dobiva lažan osjećaj sigurnosti

Šifriranjem napadač dobije samo nečitljiv tekst, koji bez ključa za dešifriranje ne može pročitati. Sama se šteta, ukoliko dođe do napada, tako ograničava. Potrebno je dosljedno upotrebljavanje šifriranja za zaštitu. Korištenje VPN–a isto je jedan od krucijalnih načina zaštite jer su uređaji međusobno povezani putem šifriranog tunela te se automatski i komunikacija šifrira. Postoje i razne aplikacije za praćenje i nadzor mreže te uočavanje problema s ARP protokolom.

NAJČEŠĆE MJERE PREVENCIJE

- *Arpwatch za Linux:* Nadgledanje aktivnosti Ethernet-a, uključujući promjene IP i MAC adresa. Svakodnevni pristup dnevniku sa vremenskim oznakama kako bi se moglo vidjeti kada je došlo do napada.
- *ARP-GUARD:* Aplikacija skenira mrežu te prepoznaje uređaje koji su u lokalnoj mreži te gradi pravila za kontrolu budućih mrežnih pristupa.
- *XArp:* Alat za otkrivanje napada koji se događaju u pozadini, obavještava čim napad započne kako bi se moglo na vrijeme reagirati i spriječiti napad.
- *Wireshark:* Pomoću grafičkog sučelja vidljivi su svi uređaji i promet unutar lokalne mreže, kako bi njegova primjena bila ispravna potrebne su napredne vještine.
- *Filtriranje podataka:* Upravljanje pristupa mreži traženjem dolaznih i odlaznih paketa. Paketi se zaustavljaju ili propuštaju u ovisnosti o izvorišnim i odredišnim IP adresama port-ova i protokola.
- *Statički ARP:* ARP protokoli se dodaju u pred memoriju i zadržavaju trajno. Trajna su preslika MAC i IP adresa.

3.9. Wireshark

Uređaji komuniciraju putem mreža. Mreže su ili lokalne ili javne. Postoje aplikacije koje dohvaćaju podatke paketa niske razine koji se prenose putem mreže. Napadači analizom tih podataka dolaze do vrijednih podataka i otkrivaju korisnička imena i lozinke. Jedna od takvih aplikacija je Wireshark, aplikacija za analizu mrežnih protokola otvorenog koda. Razvio ju je Gerald Combs 1998. godine, a podržana je od strane globalne organizacije mrežnih stručnjaka i programera koji svakodnevno nastavljaju razvijati i ažurirati nove mrežne tehnologije i metode šifriranja.

Vladine agencije, korporacije, neprofitne organizacije i obrazovne institucije upotrebljavaju ga jer je sasvim siguran za upotrebu, a uvelike im pomaže za proučavanje i rješavanje problema. Najbolji način na koji se može shvatiti mreže je promatranje prometa putem ove aplikacije, promatranje pod mikroskopom.

Wireshark se smije koristiti samo na mrežama gdje postoji dopuštenje za pregled mrežnih paketa jer je izrazito snažan alat za praćenje mreža. Primjeri protokola koji su ranjivi na aplikacije poput Wireshark-a su: Telnet, Rlogin, HTTP, SMTP, NNTP, POP,

FTP, IMAP. Njihova ranjivost je u tome što se informacije ne šifriraju prilikom slanja, već se šalju u izvornom stanju. Korištenjem nekih od ovih protokola, pomoću Wireshark-a je sasvim jednostavno doći do informacije o meti, poput lozinke i korisničkog imena jer se paketi ne šifriraju i pregledavanjem mrežnog prometa pomoću Wireshark-a lozinka i korisničko ime šalju se zapisani u izvornom obliku i tako ih je jednostavno otkriti.

KORIŠTENJE WIRESHARKA ZA DIJAGNOSTIKU MREŽNIH RANJIVOSTI

Alat snima i bilježi mrežnu aktivnost u stvarnom vremenu (sistemsko vrijeme) i omogućava sortiranje i analizu. Važna stavka za što kvalitetniju upotrebu Wireshark aplikacije je planiranje, odnosno određivanja cilja nadzora. Kada je potrebna izolacija i provjera lokalnih uvjeta, praćenjem uključivanja sustava na odgovarajući port pomoću Wireshark-a, moguće je očitati hardverske adrese povezane sa određenim port-om, emitiranje(multicast) promet i promet koji prolazi između port-ova. Ispitivanje na Ethernet priključku koji je izvan lokalne mreže, odnosno nije na Wireshark sustavu zahtjeva zrcaljenje port-ova.

SNIMANJE SUČELJA

Ukoliko je cilj korištenja aplikacije snimanje sučelja aplikacija se koristi na način da se pokreće snimanje mrežnog prometa odabirom tipke *Capture* te potom odabirom *Options* izbornika. Izbornik *Options* omogućuje određivanje željene duljine vremena rada aplikacije te željene količine podataka potrebnih za snimanje prije zaustavljanja sustava.

Pritiskom tipke *Start* aplikacija daje uvid u kretanje mrežnog prometa. Ukoliko nije konkretno specificirano vrijeme zaustavljanja dohvata prometa moguće je u postavkama namjestiti automatsko zaustavljanje. Opcija *Filter* omogućuje isključivanje / uključivanje određene vrste prometa i mrežnih paketa. Aplikacija zapisuje podatke na način da svaki red predstavlja jedan razmijenjeni paket. Svaki paket je moguće detaljno analizirati te dobiti uvid u njegov sadržaj.

Wireshark bilježi podatke unutar memorije. Kod preopterećenja mreže može uzrokovati prekid rada, takvi prekidi se događaju kod predugog rada aplikacije ili kada je ukupna memorija sustava niska. Prevencija eventualnog prekida rada programa zahtjeva prije početka, ovisno o specifikacijama i dostupnim resursima samog sustava, izračunavanje

vremena rada aplikacije. Snimanje sučelja na potpuno zaštićenom Ethernet-u brzine 100 Mbit/s proizvede otprilike 750 MB podataka u minuti.

MREŽNA DIJAGNOSTIKA

P4V klijent je vizualni klijent za „Perforce Helix Core“. Olakšava pristup poslužitelju jer za razliku od P4 klijenta nema potrebe za korištenjem command prompt-a i višestruko je funkcionalan.

Bolji uvid u mrežnu dijagnostiku postiže se povezivanjem P4V klijenta sa Wireshark aplikacijom. Zapisnik P4V klijenta služi kao sažetak aktivnosti te popis redoslijeda izvršavanja naredbi čije su pojedinosti o umrežavanju vidljive pomoću Wireshark-a, najjednostavnije kada su poslužitelj i klijent istovremeno umreženi. P4V klijent se uključuje na način da se u postavkama odabere *Select the Logging heading* i potom opcija *Show P4 reporting commands*, nakon toga treba odabrati *Show P4 command output* i *Enable logging to file*. Završetkom odabira navedenih opcija pritiskom tipke *Select* datoteku je moguće spremiti na željenu lokaciju na računalu.

Praćenjem nefiltriranih izlaza pomoću Wireshark-a moguće je dohvatiti druge mrežne aktivnosti prilikom usporenog rada mreže. Otkrivanje uzroka sporog rada mreže mogče je odabirom opcije *Set View –> Time Display Format –> Seconds Since Previous Captured Packet* . Korisnik ima uvid parametara konkretnog paketa koji kasni. Korisno je jer može pružiti uvid u eventualna mjesta na kojima dolazi do kašnjenja, odnosno paketa koji mogu uzrokovati spori rad mreže. Analizom je moguće dobiti podatke o eventualnim mrežnim greškama i naredbama koje se nepotrebno ponavljaju. Ukoliko se analizom otkrije kako su svi paketi prikazani sa pogreškama kontrolnog zbroja zaglavlja postoji mogućnost da mrežni hardver koristi „Checksum Offload“ te se takve greške zanemaruju.

Mrežna dijagnostika je moguća i usporedbom izlaza problematičnog uređaja sa uređajem koji radi bez problema. Postoji mogućnost da usporeni rad uzrokuju drugi prometi, poput NBNS-a(NetBIOS), TCP ili neke aplikacije.

KORISNE ZNAČAJKE

Odabirom *Edit–>Find Packet–>String–>Packet bytes* te unosom predodređenih naredbi pretražuju se korisničke sinkronizacije i prikazuje vrijeme kada je P4 sinkronizacija pokrenuta sve dok je Wireshark nadzirao mrežni promet.

Korisničke naredbe P4 klijenta imaju predznak „user-“. Jedan od primjera naredbe je user-sync, navedena naredba daje prije navedeni rezultat vezan uz sinkronizaciju.
Najčešće se Wireshark koristi za dijagnosticiranje i rješavanje mrežnih problema poput sporog i slabog web poslužitelja, analize HTTP prometa, kao uvid u naredbe i parametre zaglavlja i parametara protokola prema poslužiteljima te za pregled i analizu odgovora klijentu.

ANALIZA

Expression - Konfiguracija vrste mrežnog sučelja za analizu uz opciju *Filter*
Capture Interfaces - Odabir mrežnog sučelja koje pokazuje probleme
Pokretanje aplikacije – postupak otvaranja programa čiji je rad potrebno analizirati
Capture – Snimanje procesa, opcija *Stop* služi za završetak snimanja
File(Save as) – spremanje datoteke u odabranom formatu i kreiranje zapisa analize

TUMAČENJE ANALIZE

Analiza je kompleksan dio mrežne dijagnostike. Wireshark nudi širok spektar analize te se na kraju jednostavno izgubiti u samim rezultatima. Ključna stvar za dijagnostiku mrežnih problema je prvenstveno izoliranje izvora koji stvara probleme. Jedan od načina izoliranja problema je opcija koju nudi aplikacija *The Statistics–>Conversations* na izlaznom izborniku. Ovisno o protokolu upotrebljava se za detalje kao što su količina prenesenih podataka – *Bytes*, a i za isticanje samo određenih vrsta prometa pomoću opcije *Analyze –> Enabled* i odabirom određenih protokola potrebnih za analizu. Spremanje analize unutar datoteke je bitna stavka jer služi za kasniju upotrebu kod kreiranja proračunske tablice, ukoliko ju se spremi u *.CSV formatu. Usporedba dvije analize, uređaja koji radi bez problema i uređaja koji ima mrežnih problema, izrazito je korisna u samoj dijagnostici.

3.10. Hakiranje Wi-Fi mreže

Wi-Fi mreže su dostupne svima unutar radijusa prijenosa usmjerivača te su iz tog razloga izrazito ranjive na napade. Najranjivije Wi-Fi mreže su javne mreže „hotspots“. Bežične mreže koriste radio valove za povezivanje uređaja sa krajnjim uređajem. Implementacija se vrši na prvom sloju, fizičkom sloju OSI modela.

Pristup mreži omogućava uređaj sa bežičnom mrežom te je potrebno mjesto koje se nalazi unutar radijusa prijenosa pristupne točke bežične mreže. Uređaji većinom sadrže popis dostupnih mreža te jačinu signala i podatak o tome je li mreža javna ili privatna te kojom tehnikom autentičnosti je zaštićena.

NAJČEŠĆE KORIŠTENE TEHNIKE

WEP (Wired Equivalent Privacy)

Razvijen je za IEEE 802.11 WLAN standarde. Namjena mu je osigurati privatnost ekvivalentnu onoj koju pružaju žičane mreže. Radi na principu šifriranja podataka koji se prenose mrežom. Postoje dvije vrste WEP autentifikacije.

- *OSA(Open System Authentication)* odobrava pristup autentifikaciji stanice na temelju već konfiguriranih pravila pristupa
- *SKA(Shared Key Authentication)* šalje šifriranu poruku poslužitelju kojom traži pristup, ključem poslužitelj šifrira poruku i šalje je klijentu, ukoliko se šifrirani odgovor poslužitelja poklapa sa vrijednosti klijenta odobrava se pristup.

WEP kao mjera zaštite bežičnih mjera nije dobro rješenje jer sadrži mnogo sigurnosnih propusta i ranjivosti. Sukladno navedenom sve se manje koristi i zamjenjuje ju se sa WPA koji je otporniji i sigurniji. Svaki projekt ima svoje početke, uspone i padove te ekstinkciju. Svakodnevnim razvojem i tehnološkim unaprjeđenjem razvija se i sigurnost. Stare tehnike se zamjenjuju novima. Svaka od prvotnih tehnika u začetku je napredak i funkcionalno „čudo“ dok joj se ne otkriju ranjivosti i unaprijedi razvojem zakrpa ili pak zamijeni potpuno novim tehnologijama.

Tablica 12. Popis ranjivosti mreža koji eventualno mogu dovesti do neovlaštenog pristupa mreži

Vrsta ranjivosti	*Opis*
CRC32(Cyclic Redundancy Check)	Ovakva provjera integriteta paketa može se ugroziti hvatanjem najmanje dva paketa. Bitovi i kontrolni broj su podložni promjeni od strane napadača te time pružaju napadaču neovlašteni pristup mreži.
RC4	Korištenje ovog algoritma za stvaranje stream šifri još je jedna od ranjivosti iz razloga što niska vrijednost tajnog ključa olakšava njegovo razbijanje. Tajni ključ iznosi 40 – 104 bita te je time maksimalna vrijednost 128 bita, odnosno minimalna 64 bita.
Kombinacije slabih početnih vrijednosti lozinke	Podaci nisu dovoljno šifrirani te su time jednostavniji za dešifriranje. Čini ga ranjivim na „DICTIONARY ATTACK“
Slabo provođenje upravljanja ključevima	Promjena ključeva je vrlo izazovna, pogotovo na velikim mrežama
Početne vrijednosti su višestruko iskoristive	

WPA(Wi-Fi Protected Access)

Sigurnosni protokol koji je razvio Wi-Fi savez u svrhu poboljšanja sigurnosti kada su pronađene ranjivosti WEP-a. Koristi se za šifriranje podataka na 802.11 WLAN-ovima i koristi veće početne vrijednosti, 48 umjesto WEP-ovih 24 bita. Paketi se šifriraju korištenjem vremenskih ključeva.

RANJIVOSTI

- Implementaciju izbjegavanja sudara moguće je prekinuti
- Ranjivost na DoS napade
- Ključevi koji se međusobno dijele unaprijed koriste lozinke što ih čini ranjivim na DICTIONARY napade.

WEP KREKIRANJE

Krekiranje je proces iskorištavanja sigurnosnih slabosti u bežičnim mrežama. WEP krekiranje podrazumijeva iskorištavanje slabosti mreža koje koriste WEP za provođenje sigurnosnih kontrola.

VRSTE PUCANJA

Pasivno – Otkivanje ranjivosti je teško i nema vidljivog učinka na mrežni promet sve do probijanja sigurnosti WEP-a.

Aktivno – Postoji veći učinak i opterećenje mrežnog prometa, lako se otkriva i puno je učinkovitija ranjivost.

Tablica 13. Popis softvera za krekiranje WEP-a

Aplikacija	*Opis*
Aircrack	Alat za hakiranje Wi-Fi lozinki, koristi se za krekiranje i praćenje mrežnog prometa
WEPCrack	Program otvorenog koda za probijanje 802.11 WEP tajnih ključeva. Navedena aplikacija je implementacija FMS napada.
Kismet	Lozinkom na mreži otkriva bežične mreže(vidljive i skrivene), pregledava pakete, otkriva upade na mrežu
WebDecrypt	Koristi aktivne DICTIONARY napade za razbijanje WEP ključeva. Koristi vlastiti generator ključeva i implementira paketne filtre za otkrivanje lozinke

WPA KREKIRANJE

Koristi 256 unaprijed podijeljenih ključeva ili lozinki za provjeru autentičnosti. Kratke i slabe lozinke ranjive su na DICTIONARY napade te druge napade za razbijanje lozinki.

Tablica 14. Popis softvera za krekiranje WPA

Aplikacija	*Opis*
CowPatty	Koristi se za razbijanje unaprijed podijeljenih ključeva pomoću Brute – force napada
Cain & Abel	Koristi se za dekodiranje snimljenih datoteka iz drugih programa za praćenje prometa

VRSTE NAPADA

Sniffing – Presretanje i snimanje paketa koji putuju mrežom koji se pomoću nekih od alata za krekiranje dekodiraju.

Man in the Middle (MITM) – Prisluškivanje mreže i hvatanje osjetljivih informacija.

Denial of Service(DoS) / Distributed Denial of Service (DDoS) – Uskraćivanje mrežnih resura legitimnim korisnicima. Prilikom ovakve vrte napada može biti koristan alat FataJack. DDoS je u principu DoS napad ali meta nije jedan server, jedno računalo, nego više umreženih računala, a cilj i svrha napada je jednaka. Potpuni prestanak rada poslužitelja.

„A man-in-the-middle attack is a type of eavesdropping attack, where attackers interrupt an existing conversation or data transfer. After inserting themselves in the "middle" of the transfer, the attackers pretend to be both legitimate participants.“ [11][11]

Očigledno je da je mogućnost razbijanja ključeva WEP/WPA itekako moguće. Korištenjem aplikacija i hardverskih resursa te strpljenjem. Uspjeh samih napada ovisi i o aktivnosti korisnika mreže koja je meta napada.

[11] (VERACODE, n.d.)

Backtrack je sigurnosni operacijski sustav temeljen na Linux-u. Dolazi u paketu sa raznim sigurnosnim alatima čija je svrha prikupljanje informacija, procjena ranjivosti i izvođenje eksploatacije. Uključuje alate poput: Metasploit, Wireshark, Aircrack-ng, *Ophcrack*. Sadrži baš one alate potrebne za razbijanje ključeva i mrežni pristup.

SIGURNOSNE MJERE ZA ZAŠTITU BEŽIČNIH MREŽA

Jedna od bitnih stavki za zaštitu organizacija od napada je promjena predefinirane lozinke, omogućavanje mehanizama provjere autentičnosti, ograničavanje pristupa mreži samo korisnicima sa registriranim MAC adresama. Važno je osvijestiti koliko je bitno korištenje jakih ključeva koji sadrže kombinacije simbola, brojeva, znakova i time smanjuju mogućnost Dictionary ili Brute force napada. Jaki Firewall je isto od izrazite važnosti te smanjuje mogućnost neovlaštenog pristupa.

PRIMJER HAKIRANJA WI-FI (CAIN & ABEL)

Sučelje sadrži karticu *Decoders*, nakon odabira kartice, lijevim klikom se odabire *Wireless passwords* koji se nalazi u navigacijskom izborniku s lijeve strane. Nakon što su ti koraci dovršeni pritiskom na plavi plus znak, ukoliko korisnik ima pristup lokalnoj mreži, pojavljuju se svi uređaji spojeni u lokalnu mrežu zajedno sa podacima kao što su SSID i lozinka.

Navedeni primjer napada je izvrsna motivacija za ugrađivanje sustava za otkrivanje upada koji onemogućavaju neovlašteni pristup. Organizacije treba osvijestiti o svim rizicima i prijetnjama informacijske sigurnosti te upućivati u štetu ako pravovremeno ne zaštite svoje vlasništvo i informacije, ne ograniče pristup i ne provode sigurnosne mjere.

3.11. DOS – Denial of service

Napad koji onemogućuje žrtvi pristup web stranicama, mreži, elektroničkoj pošti itd. ili pak pristup čini prilično usporenim. Najčešće se provodi na način da se ciljani web poslužitelj pogodi sa previše zahtjeva istovremeno te na taj način poslužitelj ne može odgovoriti na sve zahtjeve mreže. Cilj napada je usporavanje rada poslužitelja ili potpuno rušenje u ovisnosti što je napadačev motiv i želja.

„Human Stupidity, that's why Hackers always win." [12][12]

VRSTE NAPADA

- DoS napad kojeg provodi jedan host.
- DDoS napad kojeg provode više zaraženih uređaja kojima je svima žrtva napada ista. Mreža se preopterećuje slanjem višestrukih paketa istovremeno.

"It is a fairly open secret that almost all systems can be hacked, somehow. It is a less spoken of secret that such hacking has actually gone quite mainstream." [13][13]

Tablica 15. Najčešće vrste napada

Vrsta	*Opis napada*
Ping of death	„*ping*" je naredba koju se koristi za dostupnost mrežnog resursa. Šalje male pakete podataka samo kako bi se potvrdila dostupnost unutar mreže. Ovakva vrsta napada šalje pakete podataka iznad maksimalnog ograničenja (65.536 bajtova) koje TCP/IP dopušta i razbija na male komade koji se šalju poslužitelju. Kako je paket u konačnici veći od onoga što poslužitelj može obraditi dolazi do smrzavanja, rušenja sustava
Smurf	Koristi velike količine ICMP(Internet Control Message Protocol) za ping. IP adresa odgovora je lažna u odnosu na žrtvinu te se svi odgovori šalju žrtvi umjesto IP-a kojeg se koristi kod ping naredbe. Jedna adresa može podržati maksimalno 255 host-ova, a ovakav napad pojačava jedan

[12] (Khelifi, n.d.)
[13] (Kaminsky, n.d.)

	ping 255 puta. Dolazi do onemogućavanja korištenja mreže
Buffer overflow	Međuspremnik je mjesto za pohranu u RAM-u i koristi se za čuvanje podataka tako da ih CPU može manipulirati prije nego što se zapišu na disk. Buffer-i imaju ograničenje veličine. Ovakav napad učitava među spremnik sa više podataka koje može držati te dovodi do prelijevanja među spremnika i oštećenja podataka koje sadrži. (npr. slanje elektroničke pošte s imenima datoteka koje imaju 256 znakova)
Teardrop	Napadač koristi veće pakete koji se razbijaju u fragmente kojima manipulira dok se šalju na način da se međusobno preklapaju i na taj način uzrokuju rušenje žrtve prilikom ponovnog sastavljanja paketa
Syn attack	Koristi rukovanje u 3 smjera za uspostavljanje komunikacije pomoću TCP-a. Žrtvu se preoptereti nepotpunim SYN porukama i uređaj žrtve dodjeljuje memorijske resurse koji se nikada ne koriste te uskraćuje pristup korisnicima.

ALATI

- *Nemesy* generira nasumične pakete. Radi na Windows operacijskom sustavu. Obzirom o kakvoj se aplikaciji radi, ukoliko računalo posjeduje antivirusni program detektirati će ga kao virus.
- *Land and LaTierra* se koristi za IP spoofing i otvaranje TCP veza.
- *Blast*
- *Panther* koristi se za opterećivanje žrtvinog računala UDP paketima.
- *Botnets* je skup kompromitiranih računala koja se koriste u svrhu izvođenja DoS napada

SIGURNOSNE MJERE PROTIV DoS NAPADA

Napadi poput SYN-a iskorištavaju ranjivosti operacijskog sustava. Instalacijom sigurnosnih zakrpi uvelike se smanjuje prilika za izvođenje ovakve vrste napada. Korištenjem sigurnosnih sustava za otkrivanje napada također se pravovremeno otkriva i reagira na eventualne napae u tijeku. Jednostavne DoS napade zaustavljaju antivirusni programi i iz tog razloga ih je bitno imati na uređaju. Konfiguriranjem router-a postavljanjem kontrole pristupa također se sprječava ilegalni pristup mreži.

PRIMJER PING OF DEATH NAPADA

U svrhu izvođenja napada potrebna su dva računala na istoj mreži. Izvođenje samog napada je vrlo jednostavno. Potreban je command prompt i naredba „ipconfig“ za dohvat IP adrese računala žrtve te se potom upisuje naredba:

„ping IP adresa –t |65500 “

Pritiskom tipke Enter na tipkovnici počinju se slati paketi na računalo žrtve, no za uspješan napad je potrebno izvršiti istu naredbu sa više računala.

PRIMJER NAPADA POMOĆU NEMESY ALATA

Nakon uspješnog preuzimanja i instalacije alata potrebno ga je pokrenuti. Sučelje sadrži polja poput Victim IP, Packets: Number, Size, Delay(ms).

Postavke polja:

- Victim IP: IP adresa žrtve
- Number: 0 (beskonačan broj paketa)
- Size: 65000
- Delay(ms): 100

Rezultat ovakvih postavki i pritiska tipke *Send,* slanje je beskonačnog broja paketa sve dok se ne pritisne tipka *Halt* na sučelju.

3.12. Hakiranje Web servera

Svaka interakcija čovjeka i računala bilježi se i prati. Unutar baze podataka moguće je pronaći mnogo informacija poput brojeva računa kreditnih kartica, matičnih brojeva, brojeva mobitela, osobnih informacija raznih vrsta. Njihovo otkrivanje u konačnici, ukoliko napadaču postanu informacije dostupne, izaziva veliku štetu žrtvi i rezultira krađom identiteta.

Poglavlje obuhvaća najbitnije informacije vezane za hakiranje Web servera i prikazuje jednostavnost zavaravanja žrtve i dohvata vrijednih podataka, poput korisničkog imena i lozinke, kada žrtva nije upoznata sa osnovama informacijske sigurnosti.

Web poslužitelj je program za pohranu datoteka, npr. web stranica koji ih čini dostupnima putem mreže, interneta. Zahtjevi web servera su hardver i softver. Najčešća meta napadača je softver, točnije iskorištavanje njegovih ranjivosti za pristup poslužitelju.

„Using the alias cOmrade, Jonathan James hacked several companies. According to the New York Times, what really earned James attention was his hack into the computers of the United States Department of Defense, even more impressive was the fact that James was only 15 at the time.“ [14][14]

RANJIVOSTI WEB POSLUŽITELJA

Zadane postavke

Zadane postavke su jednostavne za pogađanje i lako iskoristive. Postavke uključuju korisnički identifikator i lozinke koje vrlo često sadrže informacije vezane za organizaciju i time olakšavaju izvođenje napada.

Pogrešna konfiguracija operacijskih sustava i mreža

Nedostatak dobre zaštite, jake lozinke uz napadačevo posjedovanje pristupa izvršavanju naredbi na poslužitelju predstavlja sigurnosni rizik jer neovisno o vrsti napada koja se koristi napadaču je dovoljno jako malo vremena za dohvat podataka vezanih za lozinku što u konačnici rezultira neovlaštenim pristupom.

Greške operacijskih sustava i web poslužitelja

Otkrivene ranjivosti operacijskih sustava ili aplikacije također se koriste za dobivanje neovlaštenog pristupa sustavu.

[14] (Kaspersky, n.d.)

Nedostatak informiranosti o procedurama za zaštitu podataka

Neredovito ažuriranje antivirusnih programa, zakrpi, otkrivenih bug-ova u operacijskom sustavu te samog softvera, neorganiziranost vezana za autorizaciju korisnika, odnosno strukturno podijeljene ovlasti u ovisnosti o radnom mjestu, te potpun pristup svim informacijama organizacije za sve zaposlenike također predstavlja ogroman sigurnosni rizik i čini web poslužitelj izrazito ranjivim.

WEB POSLUŽITELJI

Postoje razni tipovi web poslužitelja, neki od najčešće korištenih su Apache, IIS(Internet Information Services), Apache Tomcat, Novell Web Server i IBM Lotus Domino server.

Apache je često korišteni web poslužitelj, najčešće se koristi za Linux OS, većina web stranica izrađenih u PHP-u koristi Apache poslužitelj.

IIS je Microsoft produkt, razvijen je za rad za Windows OS, drugi je najčešće korišten web poslužitelj. Većinom ga koriste asp i aspx web stranice.

Apache Tomcat je najčešće korišten web poslužitelj aplikacija izrađenih u Java programskom jeziku.

VRSTE NAPADA NA WEB POSLUŽITELJE

Zajednički naziv za ovakve vrste napada je "Directory traversal attacks", u prijevodu napadi prolaska imenikom. Iskorištavaju greške web poslužitelja za stjecanje neovlaštenog pristupa privatnim datotekama i direktorijima. Napadači prilikom uspješno izvedenog napada pristupaju osjetljivim i privatnim informacijama te ih imaju mogućnost preuzeti, izvršavati naredbe na poslužitelju, isto tako instalirati zlonamjerne softvere.

Tablica 16. Najčešće korištene tehnike / napadi na web poslužitelje

Metoda	*Opis*
DoS	Ovakva vrsta napada je izrazito teška jer uspješnim napadom daje mogućnost rušenja web servisa te ga također može onesposobiti pristup web servisu ovlaštenim korisnicima
Domain name system hijacking	Napadom se mijenjaju postavke DNS-a te se preusmjeravanja na napadačev web poslužitelj, na taj način se sav promet preusmjerava na pogrešan web poslužitelj
Sniffing	Ukoliko se poslani podaci ne šifriraju napadač ima mogućnost presresti informacije poput korisničkih imena, lozinki itd.
Phishing	Imitacija već postojećih web stranica tvrtke navodi korisnike na upisivanje raznih podataka, promet se potom preusmjerava na napadačev web poslužitelj
Pharming	Kompromitacijom DNS-a vrši se preusmjeravanje prometa na napadačev web servis
Defacement	Napadač koristi web stranice tvrtke i u potpunosti im mijenja sadržaj

ALATI

Metasploit je aplikacija otvorenog koda za razvoj, testiranje i korištenje zlonamjernog koda. Otkriva ranjivosti web poslužitelja. Pomoću aplikacije vrši se kompromitiranje web poslužitelj.

MPack je aplikacija koja podržava MySQL. Radi po principu prikupljanja i preusmjeravanja svog prometa web poslužitelja koji je napadnut.

Zeus pretvara napadnuta računala u bot-ove i zombije, potom ih koristi za daljnje napade. Skupom bot-ova napadač izvodi napade poput DoS napada i slanje neželjene pošte.

Neosplit služi za instalaciju, brisanje i kopiranje programa.

SIGURNOSNE MJERE ZA ZAŠTITU WEB SERVISA

Redovito ažuriranje svih sigurnosnih zakrpi izrazito je bitno. Ranjivosti operacijskih sustava, aplikacija, antivirusnih programa svakodnevno se otkrivaju te otklanjaju u svrhu obrane informacija. Potrebno je sigurno instalirati i konfigurirati aplikacije i operacijske sustave, instalirati sustave za praćenje i skeniranje ranjivosti, alate poput Snort-a, NMap-a, instalacija antivirusnih programa, Firewall-a. Potrebno je promijeniti zadane lozinke i port 21 FTP protokola, ukoliko se koristi, promijeniti u prilagođene priključke i postavke. Postaviti FTP port 5069.

PRIMJER NAPADA

Prvi korak je pronalazak IP adrese web stranice. Postoje određene web stranice koje pomoću alata unosom adrese web stranice otkrivaju IP adresu ("https://www.yougetsignal.com/tools/web-sites-on-web-server/"). Rezultat korištenja ovakvih alata je prikupljanje informacija o IP adresi žrtve i uvid u sve web stranice koje koriste isti web servis kao i žrtva. Skeniranjem pronađenih stranica na ranjivosti koje uključuju izvođenje SQL Injection napada. Kada se pronađe ranjivosti potrebno je u pregledniku otvoriti www.bing.com, u tražilicu se unosi sljedeća naredba:

ip:IP ŽRTVE.php?id=

Rezultat izvršavanja naredbe popis je svih web adresa koje posjeduju istu adresu kao žrtvinu IP adresu. Sljedeći korak je skeniranje pronađenih stranica na SQL Injection ranjivost za neovlašteni pristup. Navedeni link sadrži dk.php datoteku koju se otvara u nekom SQL Injection alatu nakon uspješno dobivenog pristupa:
http://sourceforge.net/projects/icfdkshell/
Pritiskom URL-a unutar Symlink kolone dolazi se do datoteka žrtve što potom omogućuje pristup bazi podataka i kompletnoj manipulaciji, izvođenje raznih napada na web stranice žrtve.

Web poslužitelji su kao svojevrsne škrinje vrijednih i osjetljivih informacija dostupni javnoj domeni te su zbog toga idealne mete napadača. Napadi iskorištavaju pogrešne

konfiguracije operacijskih sustava, web poslužitelja i mreža. Izrazito je bitno poznavati načine zaštite poslužitelja ili pak ublažavanja napada.

3.13. Hakiranje Web stranica

Web stranica / aplikacija temelji se na modelu klijent–poslužitelj. Poslužitelj pruža pristup bazi podataka i radi preko web poslužitelja dok klijent pomoću klijentskih aplikacija pristupa podacima poslužitelja. Najčešći programski jezici koje koriste web aplikacije su: Java, C#, VB.Net, PHP, ColdFusion, Markup jezici itd. Komunikacija s bazom podataka odvija se pomoću MySQL, MS SQL Server, PostgreSQL, SQLite itd. Većina web aplikacija koristi javne poslužitelje kao host-ove te ih to čini ranjivim za napade raznih vrsta.

Tablica 17. Vrste tehnika / napada na Web stranice

Metoda	Opis
SQL Injection	Zaobilaženje algoritama za prijavu, sabotiranje podataka
DoS	Onemogućavanje pristupa resursima
Cross Site Scripting XSS	Ubrizgavanje koda koji se izvršava unutar preglednika klijenta
Cookie / Session Poisoning	Izmjena podataka sesije radi stjecanja neovlaštenog pristupa
Form Tampering	Izmjena podataka unutar same web aplikacije, obrasca, kako bi napadač mogao primjerice puno jeftinije kupiti artikle iz web trgovine
Code Injection	Ubrizgavanje koda koji se izvršava na poslužitelju te omogućuje napadaču backdoor gateway, otkrivanje osjetljivih podataka itd.
Defacement	Izmjena web aplikacije i preusmjeravanje na web aplikaciju napadača koji ovisno o motive ostavlja određenu poruku

PREVENCIJA NAPADA

SQL Injection napad izbjegava se čišćenjem i provjerom korisničkih parametara prije samog slanja parametara bazi na obradu.

DoS napadi se sprječavaju dobrim Firewall-om, pravilnom konfiguracijom mreža i sustavima za otkrivanje upada.

Cross Site Scripting XSS **se** sprječavaju dosljednom provjerom i čišćenjem zaglavlja, prosljeđivanje parametara putem URL-a, skrivanjem vrijednosti također je moguće spriječiti ovakve napade.

Cookie / Session Poinsoning **se** sprječava šifriranjem sadržaja cookie-a, povezivanjem cookie-a s IP adresom klijenta.

Form Tampering se sprječava provjerom i potvrđivanjem korisničkog unosa prije obrade podataka.

Code Injection se sprječava testiranjem svih parametara, a ne samo krajnjeg koda.

Defacement se sprječava provođenjem dobre sigurnosne politike unutar organizacije, pravilnom konfiguracijom sustava i pravovremenim otkrivanjem i uklanjanjem svih ranjivosti.

3.14. SQL Injection

Napad koji truje dinamičke SQL izraze, izraze koji se generiraju za vrijeme izvođenja pomoću parametara iz web obrasca ili URI niza upita, radi na principu komentiranja određenih dijelova izraza i dodavanjem uvjeta koji je uvijek istinit. Iskorištavanjem loše konfiguriranih web aplikacija moguče je izvršavanje zlonamjernog SQL koda. Napadi ovise o vrsti baze podataka koja se koristi.

Postoje različite varijacije SQL Injection napada. Brisanje podataka naredbom DELETE, ažuriranje podataka sa UPDATE, unos podataka putem INSERT naredbe, izvršavanjem određenih naredbi koje uzrokuju instalaciju zlonamjernih softvera, poput Trojanaca, eksploataciju, izvoz osjetljivih podataka na napadačev server, dobivanje podatak za prijavu, no to su samo neki od primjera kojih je mnogo i koji uzrokuju ogromnu štetu žrtvi napada.

Ponekad se za izvršavanje napada koriste određeni alati, aplikacije jer su efikasniji i brži. Primjeri takvih programa su *SQLSmack* i *SQLMap*.

„SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.“ [15][15]

PRIMJER

Uzme li se za primjer obrazac koji pomoću elektroničke adrese i lozinke autorizira korisnika na način da podatke koje je korisnik zapisao šalje u PHP datoteku te ih privremeno sprema tokom sesije u cookie, metoda kojom se šalju podaci je POST što znači da se podaci ne prikazuju u URL-u.

Najčešće se unutar tablice u bazi podataka kolonama daju jednostavni nazivi poput *username, password, email* te tablicu za spremanje tih podataka nazivaju *users*.

Pretpostavkom da meta koristi ta imena u bazi i MD5 algoritam za šifriranje lozinke unosom naredbe:

*SELECT * FROM users WHERE email = 'xxx@xxx.xxx' OR 1 = 1 LIMIT 1 -- '] AND pssword = md5('1234');*

Dodavanjem uvjeta *OR 1 = 1 LIMIT* 1 je uvjet koji je uvijek istinit bez obzira što je napisano za email, dok je *--'] AND* dio početak komentara i time se zanemaruje lozinka, koja god je unesena i SQL naredba dohvaća podatke iz baze. Moguće je napraviti i sljedeće prilikom prijave na neku web stranicu.

- Otvaranje stranice za prijavu neke web aplikacije
- U polje za unos Email adrese se upisuje: xxx@xxx.xxx
- U polje za Password se upisuje: *xxx') OR 1 = 1 --]*

SIGURNOSNE MJERE ZA ZAŠTITU OD SQL INJECTION NAPADA

- Prije izvršavanja dinamičkih SQL naredbi potrebno je provjeriti što je korisnik upisao
- Enkapsulacijom SQL naredbi sav se SQL kod parametrizira
- Unaprijed pripremljene SQL naredbe onemogućavaju manipulaciju SQL kodom i na taj način prvo se kreira SQL naredba, a potom dodaju korisnički parametri.

[15] (imperva, n.d.)

- Provjera najčešće korištenih zlonamjernih dodataka SQL kodu prije pokretanja naredbe
- Ograničena korisnička prava pristupa bazi podataka
- Jednostavni tekstovi eventualnih grešaka koje se pojavljuju, koje ne odaju točnu lokaciju greške već samo upozoravaju korisnika kako je došlo do pogreške u radu aplikacije i kome se mora obratiti.

3.15. Hakiranje Linux operacijskog sustava

Linux je najčešće korišten poslužiteljski operacijski sustav, pogotovo za web poslužitelje. Operacijski je sustav otvorenog koda čime je sav izvorni kod dostupan te mu svatko može pristupiti, ta ga stavka čini manje sigurnim naspram drugih operacijskih sustava. Napadač proučava čitav kod i nailazi na ranjivosti unutar OS-a. Linux ima višestruke mogućnosti upotrebe. Koristi se kao poslužitelj, koristi se na raznim uređajima poput prijenosnog računala, stolnog računala, mobitela i tableta. Upravljanje programima odvija se putem grafičkog sučelja ili nizom naredbi u terminalu. Naredbe za hakiranje Kali Linux-a učinkovitije su od korištenja grafičkog sučelja. Ključno je poznavanje naredbi i njihovog korištenja prilikom izvođenja napada. Internet nudi širok spektar vodiča za učenje hakiranja pomoću Kali Linux-a.

ALATI

Nessus je alat za Ubuntu hakiranje, mijenja postavke konfiguracija skeniranja, zakrpi, mreža itd.

NMap se koristi za praćenje host-ova koji se izvode na poslužitelju te njihovog prometa.

SARA(Security Auditor's Research Assistant) svrha mu je analiza mreže i prometa te praćenje postojanja eventualnih prijetnji poput SQL Injection i XSS napada.

Postoji još mnogo alata ali gore navedeni su jedni od najučinkovitijih i najčešće korištenih.

SIGURNOSNE MJERE ZA ZAŠTITU OD LINUX HAKIRANJA

- Upravljanje zakrpama radi otklanjanja eventualnih grešaka koje napadači iskorištavaju.
- Pravilna konfiguracija operacijskog sustava.
- Onemogućavanje neaktivnih korisničkih imena.
- Promjena zadanih postavki poput uobičajenih lozinki za aplikacije, zadanih korisničkih imena, brojeva port-ova
- Instalacija sustava za praćenje i otkrivanje eventualnih prijetnji, neovlaštenih pristupa i pokušaja napada. Poneki alati automatizacijom sprječavaju napade

3.16. CISSP

CISSP je kratica za „Certified Information Systems Security Professional“ u prijevodu, Certificirani stručnjak za sigurnost informacijskih sustava. Razvio ga je Međunarodni konzorcij za certifikaciju sigurnosti informacijskih sustava poznat kao ISC.

Globalno je priznat standard koji potvrđuje tehničke vještine, praktično iskustvo i znanje stručnjaka za IT sigurnost. Položeni CISSP ispit je često tražen kod kandidata jer im je to određena potvrda da su kandidati dovoljno upućeni u cyber sigurnost te mogu položiti certifikacijski ispit i imati praktično iskustvo i potencijalnu formalnu CISSP obuku.

PREDUVJETI ZA STJECANJE CISSP CERTIFIKATA

Kandidati moraju imati najmanje 5 godina stalnog radnog iskustva u najmanje dvije od osam domena znanja o cyber sigurnosti. CISSP certifikat ne osigurava samo polaganje ispita već postoje određeni koraci koje svaki kandidat mora proći kako bi dobio mogućnost certificiranja. Preporuke su kako bi kandidat trebao biti na nekoj od pozicija poput glavnog službenika za informacijsku sigurnost, direktora sigurnosti, glavnog službenika za informacije, IT menadžera, inženjera sigurnosnih sustava, sigurnosni analitičar, upravitelj sigurnosti, sigurnosni revizor, sigurnosni arhitekt, savjetnik ili mrežni arhitekt.

Priprema za polaganje certifikacijskog ispita moguća je kroz samostalno učenje i učenje korištenjem CISSP-ovih udžbenika, vodiča. Postoje i praktični online ispiti koji uvelike

pomažu u usvajanju znanja i vještina potrebnih za ovaj certifikat. Postoje i tečajevi za obuku CISSP-a koji kandidate pripremaju za konačni certifikacijski ispit.

ZAHTJEVI ZA STJECANJE CISSP CERTIFIKATA

Kandidati moraju proći kroz niz koraka za ispunjavanje preduvjeta, a potom dolaska i do faze stjecanja certifikata u kojoj moraju položiti certifikacijski ispit, ispuniti ugovor o ispitu CISSP-a, pretplatiti se na ISC etički kodeks, odgovoriti na pitanja o kvalifikacijama te primiti potvrdu od ovlaštenog ISC stručnjaka. Zadržavanje certifikata iziskuje godišnje ostvarivanje minimalno 40 bodova za kontinuirano stručno obrazovanje te uplata godišnje naknade od 85 USD.

ISPIT

Sastoji se od 250 pitanja višestrukog izbora te naprednih i inovativnih pitanja kojima se provjerava znanje i razumijevanje kandidata vezano za 8 domena(sigurnost i upravljanje rizicima, sigurnost imovine, sigurnost inženjeringa, sigurnost komunikacija i mreža, upravljanje identitetom i pristupom, procjena i testiranje sigurnosti, sigurnosne operacije i sigurnost razvoja softvera). Ispit traje 6 sati, a rezultati se računaju na ljestvici (min.)700 – 1000(max.) bodova za prolaz. Ispit je dostupan na više jezika, poput engleskog, francuskog, njemačkog, brazilskog, portugalskog, japanskog itd. Dostupan je i u formatu za osobe s oštećenjem vida.

CIJENA

Ispit košta 699 USD iako cijene variraju u ovisnosti o porezu i mjestu pisanja ispita. Ponovno polaganje ispita moguće je uz naknadu od 50 USD, otkazivanje ispita naplaćuje se 100 USD. Certifikat vrijedi 3 godine od uspješno položenog ispita, a produžetak je moguć jedino uz redovito plaćanje godišnje članarine te ispunjenje obveze stjecanja minimalno 40 bodova za stručno godišnje obrazovanje.

OBUKA

Obzirom da se od kandidata očekuje iskustvo i stručno znanje cilj same obuke nije učenje od temelja već usmjeravanje kandidata, pronalaženje slabih točaka u kandidatovom iskustvu i znanju te usmjeravanje ka poboljšanju istog. Procjenjuje se kandidatova upoznatost sa ispitnim materijalima te vještine i znanja iz prije navedenih domena.

DODATNI CERTIFIKATI

Stručnjaci koji već posjeduju CISSP certifikat mogu se opredijeliti za dodatna 3 područja certifikacije kao dodatke već postojećem certifikatu.

CISSP-ISSAP – arhitektura

- Sustavi i metodologije pristupa
- Komunikacija i sigurnost mreža
- Kriptografija
- Analiza sigurnosne arhitekture
- Planiranje kontinuiteta poslovanja povezanog s tehnologijom
- Planiranje oporavka od katastrofe
- Fizička sigurnost

CISSP-ISSEP – inženjering

- Sigurnosni inženjering sustava
- Okvir za certifikaciju i akreditaciju / upravljanje rizicima
- Tehničko upravljanje
- Politike i izdavanja vezana za osiguranje informacija američke vlade

CISSP-ISSMP – upravljanje

- Vodstvo i upravljanje sigurnošću
- Upravljanje životnim ciklusom sigurnosti
- Upravljanje usklađenošću sa sigurnošću
- Upravljanje nepredviđenim situacijama
- Pravo i etika
- Upravljanje incidentima

Ostvarivanje dodatnih certifikata nije moguće bez minimalno dvije godine radnog iskustva u jednoj ili sve 3 navedene domene uz pripadajući CISSP certifikat.
Ovi ispiti traju 3 sata i nude se samo na engleskom jeziku, sastoje se od 125 pitanja višestrukog izbora za ISSAP i ISSMP te 150 pitanja za ISSEP. Cijena im je 599 USD. Nakon polaganja ispita, odnosno ostvarenih minimalno 700 bodova kandidati moraju

proći sličan postupak potvrde kao i kod polaganja samog CISSP ispita. Godišnja naknada za certifikate iznosi 35 dolara te je potrebno ostvariti minimalno 20 bodova godišnje kako bi zadržali certifikat.

3.17. Digitalna forenzika

Proces čuvanja, identifikacije, izdvajanja i dokumentiranja računalnih dokaza koji su iskoristivi na sudu.

Digitalna forenzika je znanost o pronalaženju dokaza iz digitalnih medija poput računala, mobitela, te poslužitelja i mreža. Omogućuje najbolje alate i tehnike za rješavanje kompliciranih slučajeva povezanih s digitalnim tehnologijama. Digitalni forenzičari i etički hakeri na neki način su međusobno povezani, veže ih činjenica da su oboje stručnjaci informacijske sigurnosti što čini te dvije skupine djelatnosti usko povezane. Najjednostavnije je vidljiva njihova povezanost iz primjera same definicije etičkog hakiranja i digitalne forenzike. Digitalni forenzičari kao i etički hakeri imaju ovlasti vršiti određene napade i radnje koje koristi zlonamjeran napadač za ostvarivanje što bolje zaštite i očuvanja podataka. Različitost je u tome što etički hakeri ciljano pronalaze ranjivosti sustava i svrha im je zaštita informacija, aplikacija, njihovo prikupljanje podataka u svrhe je rješavanja problema i što boljeg osiguranja organizacije za koju rade, dok digitalni forenzičari koriste tehnike hakiranja u svrhu prikupljanja podataka, dokaza zločina i njihova uloga nije toliko bazirana na otkrivanju ranjivosti već na iskorištavanju ranjivosti za prikupljanje informacija / dokaznog materijala na sudu.

Digitalni forenzičari i etički hakeri usko su povezanu iako im je krajnji cilj i princip rada nešto drugačiji. Potrebno je za početak razjasniti osnovne činjenice i razlike između digitalnih forenzičara i etičkih hakera.

Tablica 18. Paralelni opis etičkih hakera i digitalnih forenzičara

Etički hakeri	*Digitalni forenzičari*
Koriste svoja znanja i vještine te razne alate za otkrivanje slabosti u računalnom sustavu. Sugeriraju mjere sanacije, obrane i prevencije nakon otkrivanja slabosti sustava. Obučeni su za zaštitu svih vrsta mreža od zlonamjernih napadača. Postepeno se obučavaju za primjenu znanja i vještina, naučenih tokom raznih edukacija, u praksi. Najčešće vježbom na vlastitom računalu, njihov rad je usmjeren na otkrivanje ranjivosti bez nanošenja štete, upoznati su sa svim temeljima hakiranja. Legalno i ciljano vrše napade na sustav oponašajući napadača. Konačno educiraju organizacije kako se obraniti i zaštiti svoje informacije i time smanjiti financijske gubitke, očuvati intelektualno vlasništvo i pružati sigurno korištenje svojih usluga klijentima. Svaka organizacija u svom radnom okruženju treba imati minimalno jednog ovakvog stručnjaka bez obzira o kojoj se djelatnosti radilo.	Paralelno rade na otkrivanju napada na računalni sustav i izvlačenju dokaza u svrhe prijavljivanja zlonamjernog rada napadača višim vlastima. Rade temeljite revizije sustava, analizu i istragu radi utvrđivanja potencijalnih dokaza prijetnje, narušavanja sigurnosti informacija. Prikupljeni dokazi koriste se na sudu u svrhu rješavanja brojnih zločina povezanih s računalom poput krađe ili oštećenja intelektualnog vlasništva, prijevare, krađe poslovnih tajni. Svi prikupljeni podaci korisni su jer su važni u različitim situacijama, poput nelojalnosti zaposlenika, ilegalnih radnji, kršenja uvjeta ugovora, zlouporabe pornografije, prijevare putem elektroničke pošte, krađe dokumenata i uništavanja web stranica. Zadaci digitalnih forenzičara idu u fazama, od identifikacije načina na koji je izveden napada na žrtvu, identifikacije prijetnje, odnosno napadača te prikupljanje svih vrijednih materijala koji u konačnici služe kao dokazni materijal protiv samog napadača. Uspjeh digitalnih forenzičara bazira se na vještinama poput brzog prepoznavanja znakova napada u tijeku, već izvedenog napada, pravilno prikupljanje dokaza kako bi se sve pogreške i tragovi koje je napadač ostavio za sobom, legalni dokazni materijal na sudu.

Zaključno, *digitalni forenzičari* su najkorisniji u zanimanjima poput vojske, policije, agencija za provedbu zakona te svih organizacija kojima poslovanje podliježe velikim financijskim i drugim kritičnim gubitcima.

Potrebno je naglasiti kako bez obzira na eventualne razlike svi imaju isti cilj. Očuvanje važnih podataka poslovne organizacije od zlonamjernih napadača.
Etički hakeri su ograničeni u smislu dosega istraživanja. Njihova svrha je otkrivanje vjerojatnosti zlonamjernih upada te popravljanje slabosti sustava dok s druge strane, digitalni forenzičari imaju nešto više ovlasti i njihov rad ne staje kod identifikacije i otklanjanja ranjivosti već prikupljenim dokaznim materijalima sudjeluju u procesuiranju zlonamjernih hakera na sudu.

3.18. Cybercrime

Cybercrime, u prijevodu kibernetički zločin protupravna je radnja protiv bilo koje osobe koja koristi računalo, njegove sustave te internet i aplikacije koje rade bez povezivanja na mrežu. Cybercrime-om se smatra svaki *namjeran* prekršaj, napad, krađa, te narušavanje informacijske sigurnosti.

PRIMJERI

- Manipulacija računalnim mrežama
- Neovlašteni pristup / izmjena podataka ili aplikacija
- Krađa intelektualnog vlasništva
- Industrijsko špijuniranje
- Pristup ili krađa računalnih resursa
- Pisanje i širenje računalnih virusa, zlonamjernih softvera
- Distribucija dječje pornografije
- Krađa identiteta

VRSTE NAPADA

Stjecanje neovlaštenog pristupa računalnim mrežama i sustavima, korištenje propusnosti mreže i namjerno punjenje elektroničke pošte neželjenim sadržajem, krađa aplikacija kopiranjem originalnog programa i krivotvorenjem u svrhe daljnje distribucije, krađa identiteta i navođenje uređaja na imitaciju drugog računala za pristup privilegijama koje posjeduje mreža.

ALATI

Kali Linux

Posebno dizajniran program za digitalnu forenziku i penetracijsko testiranje. Otvorenog je koda te ga održava i financira „Offensive Security".

Ophcrack - Služi za krekiranje hash-a. Pruža sigurno grafičko sučelje i omogućuje pokretanje na više platformi.

EnCase - Slikanje i pregledavanje podataka sa tvrdih i prijenosnih diskova.

SafeBack - Osnovna funkcija mu je preslikavanje tvrdih diskova zasnovanih na Intel-u na druge tvrde diskove.

Data dumper - Forenzički alat koji koristi command prompt, dostupan je za UNIX operacijske sustave, ima mogućnost točne kopije diskova prikladne za digitalnu forenzičku analizu.

Md5sum - Koristan je za provjeru ukoliko su podaci uspješno kopirani na drugo mjesto za pohranu podataka.

Cybercrime je sve raširenij pojam obzirom kako je sve veći dio populacije kojoj je dostupno korištenje računala i raznih uređaja čime je sve veća mogućnost manipulacije sustavima i mrežom. Prije samog korištenja računala potrebno je osvijestiti korisnike o svim opasnostima i prijetnjama informacijskoj sigurnosti radi minimalizacije štete kibernetičkog zločina.

3.19. Skeniranje mreže / IP skener

Poznavanjem mete već je obavljena polovica posla potrebna za izvođenje napada, no potrebne su i dodatne vještine i znanja za uspješnost napada. Potrebno je poznavati skeniranje mreže koje obuhvaća identifikaciju aktivnih host-ova, port-ova te usluga koje koristi ciljana aplikacija.

Etičkom hakeru je potrebno prilikom pronalaska ranjivosti sustava pronaći točku sustava koju može pokušati napasti. Mrežnim skeniranjem otkrivaju se sve točke sustava koje je moguće iskoristiti za hakiranje mreže.
Svaka organizacija posjeduje svoju mrežu, bilo jednu ili više lokalnih mreža, međusobno povezanih. Pronalazak ranjivosti mreže ključan je dio pri izvođenju napada.

Tablica 19. Slikovni prikaz mrežnog skeniranja

SKENIRANJE PORT-a
Skeniranje porta je proces pronalaska aktivnih portova na mreži. Skener šalje zahtjeve klijenata portu na ciljanoj mreži, potom pojedinosti o portu šalje kao odgovor klijentu i na taj način aktivni port/ovi postaju vidljivi.
TCP skeniranje SYN skeniranje UDP skeniranje ACK skeniranje Window skeniranje FIN skeniranje
SKENIRANJE RANJIVOSTI
Potrebno je u svrhu otkrivanja ranjivosti mreže identificirati slabosti poput loše napisanog koda ili pogrešne konfiguracije mreže

3.20. Wireshark alternative

Postoji mnogo dostupnih aplikacija za skeniranje mreže. Wireshark se smatra kao najjači alat za mrežno skeniranje, no bitno je spomenuti i njegove alternative koje zbog raznolikosti rada možda više odgovaraju pojedinim korisnicima. Ono što je svim aplikacijama zajedničko, u svrhu upotrebe, kako u etičkom hakiranju tako i u zlonamjernom hakiranju, već je spomenuto praćenje prometa i skeniranje mreže radi otkrivanja ranjivosti.

PRIMJERI

Sljedeći primjeri prikazuju način skeniranja mreže upotrebom Kali Linux-a. Njegove su prednosti već spomenuti alati za hakiranje.

Primjer alternative Wireshark-a je aplikacija NMap.

Primjer prikazuje skeniranje mreže, aplikacija je otvorenog koda i javno dostupna. Skeniranje mreže bez ovlasti je ilegalna radnja ali postoje stranice koje nude svojim korisnicima vježbanje skeniranja poput *„scanme.nmap.org“* koju je organizacija Nmap-a osigurala korisnicima svoje aplikacije. U svrhu skeniranja mreže potrebno je otvoriti terminal i upisati naredbu:

$ nmap –v –A scanme.nmap.org

Izvršenjem naredbe u terminalu Nmap će kao rezultat prikazati sve otvorene port-ove na mreži. Naredba sadrži opciju „v“ koja služi za detaljan ispis i opciju „A“ koja služi za otkrivanje operacijskog sustava.

Primjer skeniranja poslužitelja je pomoću aplikacije Nikto. Testira web poslužitelje na zlonamjerne datoteke i zastarjele aplikacije. Rezultati su iskoristivi za hakiranje mreže. Princip korištenja Nikto je sličan Nmap-u. Otvara se terminal u koji se upisuje naredba:

$ nikto –host scanme.nmap.org

Pokretanjem sljedeće naredbe unutar terminala se prikazuje tekst koji sadrži ime servera kojeg web aplikacija koristi te eventualne postavke koje nisu dobro konfigurirane. Jednostavno rečeno prikazuje zapis svih ranjivosti web stranice.

Primjer skeniranja mreže pomoću već spomenutog alata Nessus neizostavan je dio ovog završnog rada jer se smatra jednim od najjačih dostupnih alata uz Wireshark. Aplikacija ne dolazi u paketu sa Kali Linux pa ju je prije upotrebe potrebno instalirati, postoje dvije verzije ovog alata.

Primjer skeniranja prikazan je pomoću besplatne verzije, za preuzimanje aplikacije potrebna je prethodna registracija. Odabirom verzije aplikacije za Ubuntu preuzima se *.deb datoteka i sprema u datoteku Downloads. Instalacija alata provodi se kroz terminal. Potrebno je u terminalu upisati sljedeće naredbe:

$ cd Downloads

$ dpkg – i IME PREUZETE DATOTEKE (npr. Nessus-8.3.0-ubuntu910_amd64.deb)

Kada je proces instalacije gotov potrebno je pokrenuti Nessus naredbom:

$ /etc/init.d/nessusd start

Poslije pokretanja Nessus-a u terminalu potrebno je otvoriti preglednik i u polje za adresu upisati *//kali:8834/*

Slijedi prijava pomoću podataka kojima se prije preuzimanja registriralo i unos aktivacijskog koda koji je prilikom uspješne registracije poslan na adresu elektroničke pošte. Nessus posjeduje grafičko sučelje te nudi širok spektar alata za skeniranje mreže. Odabirom Basic Network Scan opcije otvara se prozor sa poljima za unos podataka. Potrebno je unijeti ime i opis mrežnog skeniranja te IP adresu mete i potom pritiskom na tipku Save spremiti podatke. Sljedeći korak je pokretanje skeniranja spremljenih podataka. Rezultati skeniranja pokazuju informacije i ranjivosti mreže.

Što se veći broj podataka prikaže skeniranjem mreže to je lakše testirati ranjivosti te je iz tog razloga korisno upotrijebiti više alata prilikom ciljanog skeniranja mreže za dohvat što veće količine informacija.

3.21. Špijuniranje Android / iPhone mobilnih uređaja

Upotreba mobilnih uređaja je u porastu te se time razvija sve više aplikacija za špijuniranje i nadzor pametnih telefona. Prate dolazne i odlazne pozive, SMS-ove, lokaciju. Skrivene su unutar mobilnog uređaja i nije ih moguće otkriti. Neke špijunske aplikacije prate i aplikacije poput WhatsApp-a, Facebook-a, Snapchata.

Najčešće korištene aplikacije sa takvim značajkama:

- *MSpy*
- *UMobix*
- *Hoverwatch*
- *FlexiSPY*
- *Clevguard*
- *MobileSpy*
- *PcTattletale*
- *Spyera*
- *IKeyMonitor*
- *Spyfone*
- *XNSPY*
- *Cocospy*
- *Google Family Link*
- *Spyzie*
- *Truth spy App*
- *APPmia*
- *SpyHuman*
- *Spyier*

- *Spy To Mobile*
- *Mobile Spy*
- *Cerberus Phone Security*

Popis izgleda zastrašujuće, a značajke pojedinih aplikacija nude mnogo opcija od samog špijuniranja do preuzimanja kontrole nad mobilnim uređajem. Najčešće korišteni špijunski softveri su MSpy, uMobix, Hoverwatch, FlexiSPY, Clevguard, MobileSpy, PcTattletale, Spyera. Postavljanje špijunskih softvera zahtjeva fizički pristup meti te je kod nekih potreban i root pristup radi naprednih opcija koje pružaju.

3.22. Pen Test

Simulacija je kibernetičkog napada na računalni sustav za provjeru ranjivosti koje napadači iskorištavaju u ilegalne svrhe. Najčešće se koristi za poboljšanje Firewall web aplikacija(WAF). Uključuje proboj aplikacijskih protokola API-ja, sučelja / poslužitelja u pozadini. Takvim testiranjem otkrivaju se slabosti poput neočišćenog ulaza koji je podložan ubrizgavanju malicioznog koda.
Uvidom u rezultate testiranje dohvaća se konkretna sliku ranjivosti sustava te se rezultate iskorištava za podešavanje WAF-a te poboljšanje općenite zaštite.
Pen Test odvija se u pet faza.

Tablica 20. Popis faza prilikom izvršavanja penetracijskog testiranja

Faza	*Opis*
Planiranje i izviđanje	Opseg i ciljevi testiranja, metode ispitivanja, prikupljanje podataka o sustavu radi boljeg razumijevanja rada mete te potencijalnih ranjivosti
Skeniranje	Poznavanje odgovora na različite pokušaje napada pomoću statičke analize(pregled koda); dinamičke analize(pregledavanje koda u aktivnom stanju, pruža uvid u performanse aplikacije jer se provodi u stvarnom vremenu)
Dobivanje pristupa	Vršenje različitih vrsta napada kako bi se dobio krajnji pristup uređaju
Održavanje pristupa	Otkrivanje ukoliko postoji vremensko ograničenje prisutnosti napadača ili je neograničeno
Analitika rezultata	Izvješće s detaljima vezanim za konkretne ranjivosti koje su pronađene i iskorištene, osjetljivim podacima kojima se moglo pristupiti, vrijeme koje je ispitivač proveo unutar sustava prije nego što je otkriven

METODE ISPITIVANJA

Vanjsko ispitivanje

Cilj je testirati imovinu tvrtke koja je javno vidljiva te na taj način prikupiti što je moguće više podataka.

Interno testiranje

Simulacija zlonamjernog napada poput phishing napada, testiranje zaposlenika.

Slijepo testiranje

Svrha ovog ispitivanja je uvid osoblju za informacijsku sigurnost u sam napad, u stvarnom vremenu. Ispitivač dobije samo naziv mete.

Dvostruko slijepo testiranje

Osoblje informacijske sigurnosti nema predznanja o simuliranom napadu. Nema vremena za jačanje obrane prije samog pokušaja napada.

Ciljano testiranje

Ispitivač i osoblje informacijske sigurnosti rade zajedno i međusobno procjenjuju svoja kretanja. Pomaže pri obuci i usmjeravanju te pruža povratne informacije sigurnosnom timu.

Unatoč postojanju ograničenja Pen testiranja, ono je itekako korisno zbog rezultata analize koji pomažu organizaciji. Uvid u ranjivosti te njihovo pravovremeno otklanjanje, obučavanje osoblja informacijske sigurnosti tako i ostalih zaposlenika, skretanje pozornosti na prijetnje informacijskoj sigurnosti prilikom korištenja računala, suočavanje sa prijetnjama te načini ublažavanja i obrane od destruktivnih napada zlonamjernih hakera i poboljšanje zaštite imovine, financija i informacija koje organizacija posjeduje, sve su to prednosti provođenja ovakve vrste testiranja.

3.23. VPN

VPN(Virtual Private Network), u prijevodu, virtualna privatna mreža omogućuje korištenje zaštićene mrežne veze prilikom korištenja javnih mreža. VPN kriptira promet i prikriva IP adresu te na taj način otežava praćenje aktivnosti unutar mreže, krađu podataka i neovlašteni pristup. Šifriranje se odvija u stvarnom vremenu.

VPN skriva IP adresu preusmjeravanjem putem posebno konfiguriranih udaljenih poslužitelja, na taj način izvor podataka postaje sam VPN i time davatelji internetskih usluga(Internet Service Providers) i treće strane nemaju pristup prometu, odnosno, web stranicama koje se posjećuju, podacima koji se šalju i primaju. Filter je koji pretvara sve podatke u nečitljiv sadržaj i time pristup podacima čini beskorisnim. Posjeduje mnogobrojne prednosti poput navedene enkripcije podataka, prikrivanja lokacije, omogućuje pristup stranicama koje su iz nekog razloga

nedostupne za određena područja baš zbog značajke prikrivanja lokacije, omogućuje siguran i neometan prijenos podataka te smanjuju rizik od curenja podataka.

Ministarstvo obrane je 1960. godine pokrenulo projekte koji su radili na šifriranju podataka mrežne komunikacije i time je započeo proces kreiranja modernih virtualnih privatnih mreža. Prvotno je stvoren ARPANET, mreža za prebacivanje paketa koja je dovela do stvaranja TCP/IP protokola za kontrolu prijenosa, internet protokola. TCP/IP je posjedovao 4 sloja: vezu, internet, transport i aplikaciju. Na drugom sloju mreže i uređaji povezivali su se univerzalnom mrežom te je postojao veliki rizik izloženosti koji 1993. godine tim sa Sveučilišta u Kolumbiji i AT&AT Bell Labs na neki način rješava stvaranjem prve verzije VPN-a, imena *swIPe*, potom postepeno slijedi razvoj novih, sigurnijih VPN-ova i nadogradnja postojećih značajki i protokola.

PREPOZNAVANJE DOBROG VPN-a

Odabir VPN-a nije jednostavan ukoliko se ne pridržava određenih smjernica koje čine VPN pouzdanim i sigurnim. Potrebno je obratiti pozornost na par stvari koje dobar VPN posjeduje i na taj način si olakšati odabir.

Karakteristike dobrog VPN-a:

- *Šifriranje IP adrese* – Skrivanje IP adrese od ISP-a I trećih strana omogućuje slanje i primanje podataka na mreži bez rizika. Podaci su vidljivi samo klijentu i davatelju usluga.
- *Šifriranje protokola* – Svi digitalni tragovi se šifriraju, a među najbitnijim su cookie-i koji posjeduju povjerljive podatke, šifrira se povijest pretraživanja, financijske informacije, pristupi web stranicama.
- *Kill switch* – Ukoliko dođe do iznenadnog prekida veze prekida se VPN. Ukoliko VPN posjeduje funkcionalnost za otkrivanje iznenadnog prekida rada može prekinuti unaprijed odabrane programe smanjujući vjerojatnost ugrožavanja podataka.
- *Two-factor-authentification* – Snažan VPN provjerava svaki pokušaj prijave te može tražiti unos lozinke za slanje koda za prijavu na mobilni uređaj i na taj način otežao ilegalan pristup

Tablica 21. Podjela VPN ovisno o namjeni i karakteristikama

Vrsta	*Opis*
SSL VPN	VPN koji je riješio nedostatak opreme za zaposlenike kako bi se omogućio rad od kuće. Njegova je karakteristika što se korisnici mogu preko svojih privatnih uređaja povezati na stranice za prijavu u svoju organizaciju. Pristup je zaštićen lozinkom i korisničkim imenom.
SITE-TO-SITE VPN	Privatna mreža dizajnirana za skrivanje privatnih intranet-a te omogućavanje pristupa dostupnim resursima ovlaštenim korisnicima. Koristan je u organizacijama kojima je potrebna razmjena određenih podatak između više različitih lokalnih mreža ali bez da imaju pristup jedno drugome. Ciljana razmjena podataka. Najučinkovitiji su unutar i između velikih odjela.
CLIENT-TO-SERVER VPN	Koristi se za sigurno spajanje računala na matični uređaj te omogućava cjelokupan pristup matičnom računalu. Idealan za rad od kuće. Klijent nije povezan s Internetom putem vlastitog ISP-a jer se izravna veza uspostavlja putem VPN pružatelja usluge. VPN nema potrebu šifrirati postojeću VPN vezu jer koristi automatski šifrirane podatke prije nego postaje dostupan korisniku. Pruža veću učinkovitost te univerzalni pristup resursima tvrtke.

3.24. Gledanje blokiranih YouTube sadržaja

Postoji više načina na koje se može pristupiti blokiranim YouTube sadržajima. Najčešće se sadržaji blokiraju zbog ograničenja pristupa internetskim stranicama ovisno o zakonima pojedine države, no postoje načini kako zaobići takva ograničenja bez obzira na kojoj se lokaciji nalazili. Ovo poglavlje obuhvaća šest načina na koje je moguće gledati „zabranjena“ videa.

VPN

Najsigurniji i najbolji način prikrivanja IP adrese što omogućuje zaobilazak pronalaska lokacije i pristup web stranicama i YouTube sadržaju koji je blokiran u ovisnosti u kojoj se državi korisnik nalazi. Sigurnosne značajke pružaju anonimnost te virtualna privatna mreža otvara geografski ograničen sadržaj.

Proxy

Poslužiteljska aplikacija koja korisniku pridjeljuje drugu IP adresu. Djeluje kao posrednik između klijenata i šalje zahtjeve poslužitelja koji odgovaraju. Održava privatnost i služi kao enkapsulacija između više interaktivnih sustava. Mana mu je što usporava rad mreže i ne šifrira aktivnosti.

SmartDNS

Aplikacija koja pruža pristup raznim internetskim kanalima, za korištenje je potrebna ručna promjena adrese koja navodi aplikaciju kako je omogućen pristup mrežnim sadržajima koji su inače blokirani.

Skidanje YouTube videa

Najjednostavnija opcija, potrebno je pronaći neku od web aplikacija koja pomoću poveznice na YouTube sadržaj omogućuje spremanje videa na lokalni uređaj.

Tor

Ukoliko je korisniku potrebna potpuna anonimnost idealno rješenje je Tor preglednik. Koristila ga je SAD vojska jer je potpuno siguran, alat je otvorenog koda i pruža jako

puno mogućnosti sigurnog pregledavanja interneta. Povezivanje s Tor-om jako usporava vezu i ponekad mu je potrebno jako puno vremena za učitavanje sadržaja.

Google translate

Pronalaskom željenog sadržaja na drugom jeziku jednostavno se može upotrijebiti značajka u pregledniku „Translate this page“ i na taj način će se učitavati sadržaj samo s Google prevoditelja te će se zaobići sadržaj blokiran od strane države i institucija.

PRIMJER KORIŠTENJA VPN-a

Instaliranjem nekog od dostupnih VPN-ova i otvaranjem može se izabrati državu na koju se želi povezati. Povezivanjem na odabranu državu YouTube će prikazivati sav sadržaj dostupan unutar te države. Prilikom odabira VPN-a potrebno je obratiti pozornost na njegove sigurnosne značajke jer kod nekih VPN-ova može doći do curenja informacija poput IP adrese.

Otvaranje blokiranih YouTube sadržaja većinom nije ilegalno ali isto tako treba obratiti pozornost na zakone pojedine države jer neke od njih posjeduju određene restrikcije i otvaranje blokiranih sadržaja smatraju ilegalnom radnjom, zato je i najsigurniji način korištenje dobrog VPN-a kako bi se osigurala potpuna anonimnost.

YouTube je blokiran u Kini, Eritreji, Južnom Sudanu, Sjevernoj Koreji, Siriji, Turkmenistanu, Sudanu, Iranu, Armeniji, Indoneziji, Njemačkoj, Turskoj, Ujedinjenim Arapskim Emiratima i Finskoj.

PREUZIMANJE BLOKIRANIH YOUTUBE SADRŽAJA

Spremanje na lokalno računalo blokiranih sadržaja izvedivo je prvotno uključivanjem VPN-a, uspješnost veze putem VPN-a vidi se po samom sadržaju, koji postaje vidljiv. Treba iskoristi neku od web aplikacija koja omogućuje preuzimanje videozapisa i kopirani URL unijeti u polje unutar aplikacije, odabrati kvalitetu i format videa i pritisnuti tipku za preuzimanje sadržaja.

ALTERNATIVE YOUTUBE-a

Postoje alternativne web aplikacije slične YouTube-u koje također omogućuju pregledavanje videozapisa kao što su:

Dailymotion | (https://www.dailymotion.com/)

Vevo | (https://hq.vevo.com/)

Hulu | (https://fxo.co/BtIp?fobs=youtube-alternative)

TEDTalks | (https://www.ted.com/talks)

Facebook Videos | (https://www.facebook.com/videos)

Twitch | (https://www.twitch.tv/)

IGTV | (https://about.instagram.com/blog/announcements/welcome-to-igtv)

Cheddar | (https://cheddar.com/)

BuzzFeed | (https://www.buzzfeed.com/videos)

Bitchute | (https://www.bitchute.com/)

Metacafe | (https://www.metacafe.com/)

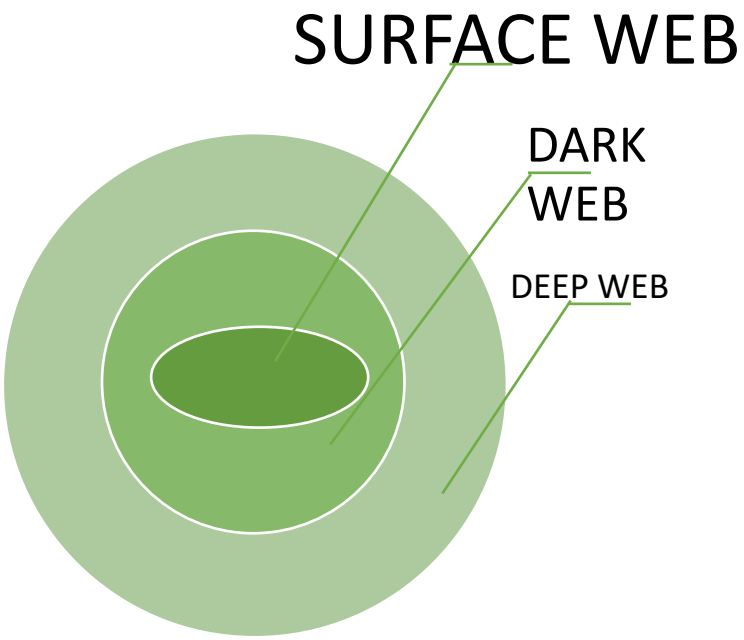
DTube | (https://d.tube/)

Netflix | (https://www.netflix.com/in/)

Vimeo | (https://www.jdoqocy.com/click-9170115-12003468?sid=best-youtube-alternative)

3.25. Deep Web / Dark Web

Internet dijelimo u 3 zasebne kategorije: Surface, Dark i Deep web. Poglavlje se bazira na razlikama između Deep i Dark web-a alije opisan i Surface web u svhu razumijevanja kategorija i zašto je poznavanje istog korisno za etičke hakere.



SURFACE WEB

Vidljiva, indeksirana mreža, svakodnevno korištena, svaki korisnik interneta je dio Surface(površinke) mreže. Mjesto je svakodnevne mrežne aktivnosti i onoga što ljudi smatraju internetom, ali internet je mnogo više od toga. Lakše razumijevanje ove kategorije postiže se vizualizacijom, pomoću sante leda. Santa je vidljiva na površini mora i taj vidljivi dio je Surface Web, dio koji se može razaznati gledajući površinu mora možemo nazvati Dark web-om dok ostatak sante ispod mora koji nije vidljiv promatraču zove se Deep web.

DEEP WEB

Web sadržaj skriven od javnosti tako da ga standardne tražilice ne indeksiraju. Najveća je kategorija novih informacija koja se svakodnevno širi. Ukupna veličina Deep web-a naspram Surface web-a je 1000 – 2000 puta veća. Možemo ga nazvati skupom neindeksiranih web stranica. Obično se koristi u legitimne svrhe koje zahtijevaju anonimnost te mu je moguće pristupiti putem VPN-a.

Koristi se u vojne svrhe, koriste ga i znanstvenici, poslovni ljudi, policija, novinari, zviždači, prosvjednici te skupine za zagovaranje protiv cenzure i stanovnici opresivnih političkih režima. Sporiji je od standardnih tražilica te pretraživanje zahtijeva precizan niz zahtijeva kako bi se dobio adekvatan rezultat. Može izazvati eksploataciju osobnih

podataka koji su inače zaštićeni, ali je koristan za identifikaciju pojedinaca sklonih krađi podataka.

DARK WEB

Odjeljak Deep web-a koji je namjerno skriven od uobičajenih tražilica. Svi su podaci šifrirani te je za pristup potreban softver, odnosno konfiguracija ili autorizacija. Koristi IP adrese koje su maskirane te dostupne samo određenom web pregledniku poput Tor-a, I2P, Freenet itd.

Količinu podataka koju sadržava nije moguće mjeriti i većinom se koristi u ilegalne svrhe te zahtjeva mnogo mjera zaštite prije samog pristupa podacima.

Koriste ga web stranice velikih tvrtki, udruga, trgovačkih organizacija. Koriste se sigurne web stranice zaštićene lozinkom i strogim pristupom samo članovima, koristi se i za tečajeve računalnih i tehnoloških vještina.

Ulazak u Dark web je jednostavan, potreban je dobar VPN i jedan od navedenih preglednika poput Tor-a. Dark web unutar samog URL-a umjesto krajnjeg dijela URL adrese koja sadrži primjerice „.com“ ili „.net“ koristi „.onion“ što omogućava pristup skrivenim dijelovima web-a.

DARKNET

Posjeduje visok stupanj privatnosti jer sadrži razne informacije poput kriminalnih aktivnosti. Najpoznatiji je po nezakonitom i uznemirujućem sadržaju. Moguće je pronaći ukradene informacije, osjetljive informacije, omogućuje kupovinu lozinki za prijavu na hakirane Netflix račune ili određene aplikacije koje se inače plaćaju. Putem darknet-a preprodaje se oružje, droga, kemikalije, dječja pornografija i vrše druge vrste kriminalnih radnji. Moguće je pronaći plaćene ubojice, informacije vezane uz zlostavljanja, trgovinu ljudima, organima itd.

Ukratko, postoje neke značajke koje razlikuju obične web aplikacije od darknet web stranica, a to su već spomenuti dodatak „.onion“ unutar URL i URL često ima kompleksan, skriven naziv, umjesto www.example.com će pisati „xyhduhddidjdi.onion“. Naziva se kodirana struktura imenovanja i koristi se jer je takve adrese teško zapamtiti.

Etičkim hakerima ovo je neiscrpan izvor informacija koje mogu u konačnici prevenirati eventualne napade, upoznati etičkog hakera sa najčešće korištenim tehnikama hakiranja, obrascima kojima se napadači služe, ostaju u toku sa eventualnim novostima i pronalaze

vrijedne informacije radi pravovremenog uklanjanja prijetnji i ranjivosti sustava, mete. Upoznavanje sa načinima, tehnikama i preferencijama zlonamjernih napadača.

3.26. Onion routing

Tehnologija anonimne komunikacije putem računalnih mreža. Unutar onion mreže, poruke koje se razmjenjuju, pakiraju se u slojeve enkripcije, te takva enkripcija asocira na slojeve luka. Prijenos podataka vrši se nizom mrežnih stanica(čvorova) i svaka stanica zadužena je za jedan sloj zaštite. Otkriva se jedino sljedeća destinacija podataka. Kada se posljednji sloj uspješno dešifrira podaci se dostavljaju na odredište. Posljednja mrežna stanica jedina zna sadržaj poslanih podataka ali je pošiljatelj anoniman.

Onion mreža je razvijena u Americi u okviru vojno-pomorskog istraživačkog laboratorija za zaštitu američkih obavještajnih komunikacija, nakon toga razvoj se nastavlja u sklopu agencije za napredne obrambene istraživačke projekte (DARPA) te je patentiran od strane mornarice 1998. godine.

Tor (The onion router) je najpoznatija implementacija onion mreže. Podaci se pakiraju u višestruko- šifrirane slojeve. Router-i znaju samo odredište i ključeve za dešifriranje svog dijela paketa. Podaci su zaštićeni izrazito jakom enkripcijom cijelo vrijeme dok putuju mrežom. Pošiljatelj nasumično izabire skup čvorova te izabrani čvorovi formiraju put slanja. Zbog zaštite anonimnosti čvor ne može znati koji je čvor u lancu pošiljatelj ili posrednik, odnosno je li on sam pošiljatelj ili posrednik, samo zadnji čvor, Exit node, može odrediti svoje mjesto u lancu. Šifrira se uz pomoć asimetrične kriptografije, pošiljatelj ima javni ključ direktorija čvorova i šalje šifriranu poruku na Entry node, uspostavlja se veza i generira tajni kod, proces se nastavlja sve do zadnjeg čvora, podatke prethodnog čvora može dešifrirati samo sljedeći čvor. Najčešće se koriste 3 čvora iako je broj korištenih čvorova u teoriji neograničen, no što je veći broj čvorova to su performanse lošije.

RANJIVOSTI

Analiza frekvencije - Nije se još dogodilo razotkrivanje identiteta korisnika onion mreže jer su za takvo nešto potrebne velike količine resursa, no postoje neki faktori koji mogu olakšati ostvarivanje tog cilja, a to su maliciozni čvorovi koji bilježe sesije u mreži.

Ranjivosti izlaznog čvora – Unatoč višestrukom šifriranju poruka sadržaj je poznat izlaznom čvoru jer on šalje konačan zahtjev primatelju. Zlonamjerni izlazni čvor može prikupiti bitne podatke, poput lozinki, bankovnih računa i sl. Problematika je vrlo slična kao i kod nesigurnih bežičnih mreža te je za rješavanja problema potrebno koristiti end-to-end enkriptirane veze poput SSL protokola. Postoji li šifriranje podataka između pošiljatelja i primatelja krajnji čvor ne može vidjeti originalne podatke.

4. OBAVEZNE INFORMACIJE ZA ETIČKO HAKIRANJE

4.1. Najčešće ranjivosti Web sigurnosti

Tablica 22. Najveće ranjivosti sustava i načini izloženosti riziku

Klasifikacija ranjivosti	*Opis*
Nedostatak strategije na visokoj razini	Nedostatak sigurnosne infrastrukture, najčešća ranjivost malih tvrtki koje smatraju informacijsku sigurnost niskim prioritetom ili pak ne žele uložiti novac kako bi osigurali imovinu i informacije ne računajući kolike bi gubitke u konačnici imali ukoliko netko iskoristi ovakvu vrstu ranjivosti.
Neadekvatna zaštita mreža	Mreže koje nemaju zaštitu daju napadaču jednostavan pristup sustavu. Nakon infiltracije unutar mreže napadači mogu dobiti pristup cjelokupnom sustavu i manipulaciju uređajima unutar mreže.
Nezaštićeni komunikacijski kanali	Ukoliko dolazi do česte razmjene podataka potrebno je te iste podatke na određeni način zaštiti kako ne bi došlo do eksploatacije. Sigurni komunikacijski kanali upravo zato i služe, a djeluju na način da se podaci šifriraju i time smanjuje šteta ukoliko i dođe do napada, jer će napadač jedino moći doći do šifriranih i time nerazumljivih formata
Nepoznate greške	Greške su vrste ranjivosti koje će svaki napadač iskoristi kako bi dobio pristup sustavu. Otkrivanje i sprječavanje svih grešaka je nemoguće ali provjerom postojanja grešaka, odnosno proaktivnim traženjem etički hakeri mogu uvelike poboljšati i otkloniti što više takvih ranjivosti
Zastarjele aplikacije	Redovito ažuriranje hardvera i aplikacija od izrazite je važnosti za zaštitu informacija. Korištenjem zastarjelih sustava i aplikacija ugrožava se

	cjelokupno poslovanje i izlaže velikim financijskim gubitcima
Nedostatak praćenja prometa	Neadekvatnim kontinuiranim praćenjem prometa i ukoliko ne postoji upućenost u najčešće napade koji proizlaze iz ovakve vrste ranjivosti nedostaje mogućnost identifikacije samih napada i pravovremenog sprječavanja istih. Ključno je posjedovati odgovarajuće sustave za praćenje i upozoravanje kako bi se minimalizirala ili u potpunosti spriječila šteta
IoT i više priključnih točaka	Internet of Things(IoT) je sve češće korišten kao i mogućnost višestrukog povezivanja na istu mrežu. Omogućuje veću učinkovitost i produktivnost ali i pruža više točaka ranjivosti
Zaposlenici bez adekvatne edukacije o informacijskoj sigurnosti	Najčešće povrede podataka uzrokuju ljudi i pogreške koje rade neadekvatnim poznavanjem važnosti ključnih stavki informacijske sigurnosti i nepromišljenim radnjama. Najčešće se radi o socijalnom inženjeringu, načinu na koji napadač dohvaća osjetljive informacije od naivnih zaposlenika koristeći se raznim tehnikama. Dovoljna je jedna meta napada(zaposlenik) kako bi se ugrozilo čitavu organizaciju.

4.2.Bug Bounty aplikacije

Programi koji pružaju mogućnost prijavljivanja pronađenih grešaka te zauzvrat nude novčanu nagradu osobi koja otkrije ranjivosti unutar sustava.

Bug Bounty aplikacije najpoznatijih tvrtki:

INTEL
(https://www.intel.com/content/www/us/en/security-center/default.html)

YAHOO
(https://safety.yahoo.com/Security/REPORTING-ISSUES.html)

SNAPCHAT

(https://support.snapchat.com/en-US/i-need-help)

CISCO
(https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html)

DROPBOX
(https://help.dropbox.com/accounts-billing/security/how-security-works)

APPLE
(https://support.apple.com/en-in/HT201220)

FACEBOOK
(https://www.facebook.com/whitehat/)

GOOGLE
(https://www.google.com/about/appsecurity/reward-program/)

QUORA
(https://engineering.quora.com/Security-Bug-Bounty-Program)

MOZILLA
(https://www.mozilla.org/en-US/security/bug-bounty/)

MICROSOFT
(https://technet.microsoft.com/en-us/library/dn425036.aspx)

OPENSSL
(https://www.openssl.org/news/vulnerabilities.html)

VIMEO
(https://vimeo.com/about/security)

APACHE
(https://www.apache.org/security/)

TWITTER
(https://support.twitter.com/articles/477159)

AVAST
(https://www.avast.com/bug-bounty)

PAYPAL
(https://hackerone.com/paypal)

GITHUB
(https://bounty.github.com/)

UBER
(https://eng.uber.com/bug-bounty-map/)

MAGENTO
(https://magento.com/security)

PERL
(http://perldoc.perl.org/perlsec.html#SECURITY-VULNERABILITY-CONTACT-INFORMATION)

PHP
(https://bugs.php.net/report.php?bug_type=Security)

STARBUCKS
(https://www.starbucks.com/whitehat)

AT&AT
(https://bugbounty.att.com/)

LINKEDIN
(https://security.linkedin.com/posts/2015/private-bug-bounty-program)

SHOPIFY
(https://www.shopify.in/whitehat)

WORD PRESS
(https://make.wordpress.org/core/handbook/testing/reporting-bugs/)

ZOMATO
(https://www.zomato.com/security)

TOR PROJECT
(tor-security@lists.torproject.org)

HACKERONE
(https://hackerone.com/bug-bounty-programs)

BUGCROWD
(https://www.bugcrowd.com/bug-bounty-list/)

4.3. Ethical Hacking literatura

„Hacking: The Art of Exploitation“ (Jon Erickson)
https://geni.us/BHGGM

„The Basics of Hacking and Penetration Testing“ (Patrick Engebretson)
https://geni.us/AgFl12

„The Hacker Playbook 2: Practical Guide to Penetration Testing“ (Peter Kim)
https://geni.us/TzleP

„Penetration Testing – A Hands-On Introduction to Hacking“ (Georgia Weidman)
https://geni.us/9lu0fB

„The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws“ (Dafydd Stuttard)
https://geni.us/s1LC

„Hacking: Computer Hacking, Security Testing, Penetration Testing, and Basic Security“ (Gary Hall)
https://geni.us/i4g0

„Computer Hacking Beginners Guide“ (Alan T. Norman)
https://geni.us/mSkPA

„Hackers & Painters: Big Ideas From The Computer Age“ (Paul Graham)
https://geni.us/qucD

„Advanced Penetration Testing: Hacking the World?s Most Secure Networks“ (Wil Allsopp)
https://geni.us/wdDAB

„The Hardware Hacker: Adventures in Making and Breaking Hardware“ (Andre Huang)
https://geni.us/1JTEaqd

„BackTrack 5 Wireless Penetration Testing Beginner’s Guide“ (Packt’s izdavači)
https://geni.us/Jz8yUB

„Hacking: The Underground Guide to Computer Hacking“ (Abraham K White)
https://geni.us/GwG2

„Hacking the Hacker: Learn From the Experts Who Take Down Hackers“ (Roger A. Grimes)
https://geni.us/iApBkY

„Gray Hat Hacking: The Ethical Hacker’s Handbook“ (Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn, Stephen Sims)
https://geni.us/qWRZYIN

„Hash Crack: Password Cracking Manual“ (Joshua Picolet)
https://geni.us/gxM42Ek

„Mastering Hacking (The Art of Information Gathering & Scanning)“ (Harsh Bothra)
https://geni.us/HNId

5. ZAKLJUČAK

Hakiranje je sastavni dio računarstva već desetljećima. Ukratko, za zaštitu mreža i informacijskih sustava koriste se različite vrste kontrola pristupa. Konceptualno ih dijelimo na 7 različitih kategorija.

Kompenzacija – primjenjive u smislu provedbe i podržavanja sigurnosne politike. (Dva ovlaštena zaposlenika kopiraju bazu na eksterni uređaj kako bi se spriječio rizik neovlaštenog pristupa bazi, itd.)

Korektiva – smanjuje se učinak neželjenog događaja predviđanjem eventualne „katastrofe“ i smanjivanjem djelovanja ako i dođe do iste. (Oprema za gašenje požara, antivirusi, itd.)

Detekcija – otkrivanje napada dok su još u tijeku i pravovremeno obavještavanje kako bi se mogle poduzeti mjere prevencije daljnje štete koju mogu prouzročiti. (Sustavi za alarmiranje kod neovlaštenog pristupa osiguranim područjima, itd.)

Odvraćanje – korisne metode koje služe za zaustavljanje kršenja sigurnosnih politika i kodeksa. Mogu se shvatiti i kao metode diverzije.

Usmjeravanje – direktivne kontrole koje se koriste za prisiljavanje na usklađenost sa sigurnosnom politikom i praksama unutar organizacija. (Prakse korištenja mrežnih sustava tvrtke, itd.).

Prevencija – metode kojima se žele spriječiti ili zaustaviti napadi.

Oporavak – metode kojima će se unaprijed odrediti na koji način postupati u slučaju dolaska do neke vrste napada. Treba uzeti u obzir kako pod pojmom napadima, ne misli se samo na neovlašteni pristup „treće strane“, već i prirodna katastrofa, poput primjerice požara, može uzrokovati velike gubitke.

Unaprijed već definiranim metodologijama osigurava se što brži oporavak, sprječavanje i općenitu zaštitu informacijskih sustava. Posao etičkog hakera se zasniva na navedenim kategorijama. Pronalaženje načina primjene tokom ciklusa zaštite i pronalaženja ranjivosti, potrebno je shvatiti kako se sam proces i obujam posla ne svodi samo na hakiranje, već je odgovornost pojedinca vrlo kompleksnija i opsežnija.

Proces redovitih penetracijskih testova, izrazito ključnih za sustave, kod kojih postoji stalna potreba za nadogradnjom i razvijanjem novih softverskih rješenja, provodi se u svrhe što učinkovitije zaštite i održivosti informacijskih sustava.

Kibernetička sigurnost je među glavnim izazovima komercijalnih poduzeća i vladinih institucija u današnjem, sve naprednijem, tehnološkom svijetu. Realnost je kako se društvo

zasniva na internetu. Rastom potrebe za korištenjem raznih tehnoloških alata proporcionalno masovno raste stopa kibernetičkih napada. Standardno korištene tehnike i metode mrežne sigurnosti više nemaju mogućnost sprječavanja vrlo učinkovitih napada i baš se iz tog razloga javlja sve veća potreba za etičkim hakerima. Pravovremeno razotkrivanje opasnosti i slabosti računalnih sustava onemogućava eventualnu iskoristivost ranjivosti u svrhe napada i poboljšava sigurnost poslovanja i industrije. Etički hakeri su prve osobe koje imaju pristup ciljanom sustavu kako bi stručnjaci za sigurnost mogli pravovremeno djelovati i zakrpati sve slabosti sustava.

Tehnike hakiranja i njihova kategorizacija na osnovu područja koje obuhvaćaju svaki segment računarstva:

Hakiranje web stranica – preuzimanje neovlaštene kontrole nad web poslužiteljem i njegovim povezanim softverom.

Hakiranje mreže – prikupljanje informacija o mreži korištenjem raznih alata s namjerom kako oštećenja mrežnih sustava i ometanje rada.

Hakiranje elektroničke pošte – neovlašteni pristup i korištenje bez pristanka vlasnika.

Hakiranje lozinki – proces oporavka tajnih lozinki iz podataka koji su pohranjeni ili preneseni pomoću računalnog sustava.

Hakiranje računala – proces krađe računalnog identiteta i lozinke primjenom metoda hakiranja i dobivanjem neovlaštenog pristupa računalnom sustavu.

Globalno rečeno, svako neovlašteno prikupljanje, iznuda i korištenje informacija u ilegalne svrhe smatra se napadom i kažnjivo je.

PREDNOSTI HAKIRANJA:

- Vraćanje izgubljenih podataka, poput poruka, slika, uspomena, pogotovo u slučaju gubitka lozinke.
- Uspostavljanje odgovarajućih preventivnih mjera za sprječavanje narušavanja sigurnosti.
- Struktura i arhitektura računalnog sustava koja će onemogućiti pristup zlonamjernim napadačima.

NEDOSTACI HAKIRANJA:

- Kršenje sigurnosti
- Neovlašteni pristup sustavu koji sadrži privatne podatke
- Ometanje rada sustava
- Napadi koji onemogućavaju pružanje usluga klijentima
- Napadi na sustav, na pojedinca, krađa, iznuda, itd.

Uzevši u obzir koju štetu i razornost hakiranje može napraviti razvidno je koliko je angažiranje etičkog hakera jedan od ključnih procesa kojeg svaka organizacija prvenstveno treba napraviti ukoliko se ne želi dovoditi u rizik od masovnih financijskih gubitaka te reputacijskih rizika.

Ključni pojmovi vezani uz tematiku uključuju upravljanje rizikom, 3 ključne kontrole, metodologije. Standarde penetracijske testove, konstantno usmjeravanje na rizike i planiranje sprječavanja istih. Rizicima smatramo svaku ranjivost i prijetnju. Mogući scenariji upravljanja rizicima obuhvaćaju i *inherentni rizik,* odnosno, identifikaciju rizika za kojeg nema već postojeće procedure za ublažavanje posljedica. *Rezidualni rizik* je termin kojim se označava vrsta rizika čija se opasnost kalkulira nakon primjene sredstava za ublažavanje. Obzirom na sve navedeno, vidljivo je kako se etičko hakiranje bazira upravo na upravljanju, predviđanju, obrani i sprječavanju različitih vrsta rizika koji su prijetnja informacijskoj sigurnosti.

6. LITERATURA

https://www.synopsys.com/glossary/what-is-ethical-hacking.html

https://www.geeksforgeeks.org/threats-to-information-security/

https://www.guru99.com/ethical-hacking-tutorials.html

https://economictimes.indiatimes.com/definition/cryptography

https://en.wikipedia.org/wiki/Cryptanalysis

https://www.okta.com/identity-101/arp-poisoning/

https://www.varonis.com/blog/how-to-use-wireshark/

https://www.poweradmin.com/blog/how-to-use-wireshark-to-diagnose-network-problems/

https://community.perforce.com/s/article/2956

https://www.guru99.com/learn-sql-injection-with-practical-example.html

https://searchsecurity.techtarget.com/definition/Certified-Information-Systems-Security-Professional

https://www.simplilearn.com/ethical-hacker-or-forensic-investigator-article

https://www.edureka.co/blog/network-scanning-kali-ethical-hacking/

https://www.imperva.com/learn/application-security/penetration-testing/

https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/the-8-most-common-cybersecurity-weaknesses-to-watch-for-in-small-businesses

https://en.wikipedia.org/wiki/Bug_bounty_program

https://hr.wikipedia.org/wiki/Onion_routing

Udemy - Pass the CompTIA Pentest+ (PT0-002) exam on your 1st attempt, includes one full-length Pentest+ practice exam!

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_hacker_types.htm

7. BIBLIOGRAFIJA

[1] Mitnick, K. (n.d.). *Quotes*. Dohvaćeno iz BrainyQuote: https://www.brainyquote.com/quotes/kevin_mitnick_469443?src=t_hacking

[2] Mitnick, K. (n.d.). *Quotes*. Dohvaćeno iz BrainyQuote: https://www.brainyquote.com/quotes/kevin_mitnick_469443?src=t_hacking

[3] D'Angelo, A. J. (n.d.). *Quotes*. Dohvaćeno iz BrainyQuote: https://www.brainyquote.com/quotes/anthony_j_dangelo_105339?src=t_hacking

[4] D'Angelo, A. J. (n.d.). *Quotes*. Dohvaćeno iz BrainyQuote: https://www.brainyquote.com/quotes/anthony_j_dangelo_105339?src=t_hacking

[5] Lanier, J. (n.d.). *TOP 25 SOCIAL ENGINEERING QUOTES*. Dohvaćeno iz AZ QUOTES: https://www.azquotes.com/quotes/topics/social-engineering.html

[6] Appelbaum, J. (2012). U J. Assange, *Cypherpunks: Freedom and the Future of the Internet.*

[7] Shannon, C. (n.d.). *Cryptography Quotes (28 Quotes)*. Dohvaćeno iz goodreads: https://www.goodreads.com/quotes/tag/cryptography

[8] Knudsen, L. R., & Robshaw, M. (2011). Information Security and Cryptography. U L. R. Knudsen, & M. Robshaw, *The Block Cipher Companion* (str. XIV, 270). Springer-Verlag Berlin Heidelberg.

[9] Neumann, J. v. (n.d.). *5 Famous Cryptography Quotes, Explained | Young Coder | Matthew MacDonald | Young Coder*. Dohvaćeno iz MEDIUM: https://medium.com/young-coder/famous-cryptography-quotes-explained-1d0012e03c11

[10] Helm, N. (n.d.). *Top 85 Password Quotes: Famous Quotes & Sayings About Password*. Dohvaćeno iz QUOTES STATS: https://quotestats.com/topic/password-quotes/

[11] VERACODE. (n.d.). *VERACODE*. Dohvaćeno iz VERACODE https://www.veracode.com/security/man-middle-attack

[12] Khelifi, M. A. (n.d.). *Famous 'Hacker Quotes and Sayings' [Updated] — Tech2Hack.* Dohvaćeno iz TECH2HACK: https://www.tech2hack.com/hacker-quotes/

[13] Kaminsky, D. (n.d.). Dohvaćeno iz Wise Sayings: https://www.wisesayings.com/hacker-quotes/

[14] Kaspersky. (n.d.). *Top 10 Most Notorious Hackers of All Time*. Dohvaćeno iz Kaspersky: https://www.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

[15] imperva. (n.d.). *SQL (Structured query language) Injection*. Dohvaćeno iz imperva: https://www.imperva.com/learn/application-security/sql-injection-sqli/

8. SAŽETAK

Rad se bavi pitanjem svrhe i važnosti etičkih hakera i etičkog hakiranja, kao i informacijske sigurnosti koja je usko povezana sa ovim vrlo cijenjenim i potrebnim zanimanjem. Etički hakeri su osobe koje posjeduju skup znanja iz različitih područja informatike radi što učinkovitijeg obavljanja provjere sustava i analiziranja ranjivosti. Krajnji cilj etičkih hakera je povećanje sigurnosti sustava organizacija, prevencija neautoriziranih dohvata podataka, sastavljanje arhitekture i principa, organizacijske strukture i hijerarhije rada sa podacima. Raspodjele ovlasti obzirom na činjenicu kako je čovjek najveća prijetnja informacijskoj sigurnosti. Svojim izvještajima i pronalascima osvještavaju stručnjake iz područja informacijske sigurnosti na što usmjeriti pažnju i koje zakrpe napraviti, odnosno koje su prijetnje i ranjivosti sustava, koliko prijetnja postoji, koji su prioriteti za rješavanje istih i koliko su kritične ranjivosti. Etički hakeri simuliraju napade u određenim granicama, ovisno koliki su im opsezi i dopuštenja dodijeljeni od strane organizacije, odnosno pristup samom sustavu, jer oni nisu zlonamjerni, već rade legalan posao oponašajući nelegalne radnje zlonamjernih hakera. Rad se dotakao različitih tematika usko povezanih uz ovo zanimanje, s kojima se ovi stručnjaci moraju dubinski upoznavati i razumjeti ih radi što efikasnijeg odrađivanja sigurnosnih provjera. U radu su opisane teme poput čestih vrsta napada prilikom hakiranja sustava, posljedica takvih napada i njihove kategorije. Važnost kriptografije i šifriranja podataka te izbjegavanje određenih protokola, opisana je simulacija rada mreže, prolaska paketa te izvođenja nekih od napada pomoću pojedinih alata. Važnost pravovremene prevencije i smanjivanje rizika ovisno o kakvoj se ranjivosti radi, također su spomenuti operacijski sustavi s kojima etički hakeri moraju biti upoznati. Zanimanje opisano u radu iziskuje volju i trud, analitičko razmišljanje, snalažljivost i spremnost na konstantno učenje. Svrha ovog rada je približiti ovo zanimanje i objasniti potrebu za etičkim hakerima i njihovu krucijalnu ulogu unutar organizacije.

PRIJEVOD NASLOVA

Etički Haker

KLJUČNE RIJEČI

Hakeri, Informacijska sigurnost, Tehnike hakiranja, Kriptografija, Digitalna forenzika

POPIS KORIŠTENIH KRATICA

ACL – Access Control List

ARP – Address Resolution Protocol

CPU – Central Processing Unit

CRC32 – Cycle Redundacy Check

CISSP – Certified Information Systems Security Professional

DDLB – Drop Down List Box

DDoS – Distributed Denial of Service

DES – Data Encryption Standard

DNS – Domain Name System

DoS – Denial of Service

FTP – File Transfer Protocol

GDPR – General Dana Protection Regulation

HTTP – Hypertext Transfer Protocol

IMAP – Internet Message Access Protocol

IP – Internet Protocol

IRM – Information Rights Managment

ISC – Internet Systems Consortium

ISSAP – Information Systems Security Architecture Professional

ISSEP – Information Systems Security Engineering Professional

ISSMP – Information Systems Security Management Professional

MAC – Media Access Control

MD5 – Message-Digest Algorithm

MITM – Man In The Middle

NNTP – Network News Transfer Protocol

OSCP – Offensive Security Certified Professional

POP – Post Office Protocol

P4V – Helix Visual Client

RAM – Random Access Memory

SARA – Security Auditor's Research Assistant

SHA – Secure Hash Algorithm

SMTP – Simple Mail Transfer Protocol

SSL – Secure Socket Layer

SSo – Single Sign-On

SYN / ACK – Synchronize / Acknodwledge

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

URI – Uniform Resource Identifier

URL – Uniform Resource Locator

VPN – Virtual Private Network

WEP – Wired Equivalent Privacy

WAF – Web Application Firewall

WPA – Wi-Fi Protected Access

2FA – Two-factor Authentication

9. SUMMARY

The thesis deals with the question of the purpose and importance of ethical hackers and ethical hacking, as well as information security, which is closely related to this highly valued and necessary profession. Ethical hackers are people who possess a set of knowledge from various areas of IT in order to perform system checks and analyze vulnerabilities as efficiently as possible. The ultimate goal of ethical hackers is to increase the security of organization's systems, prevent unauthorized access to data, compile architecture and principles, organizational structure and hierarchy of working with data. Distribution of authority considering the fact that man is the biggest threat to information security. With their reports and findings, they inform experts in the field of information security what to focus attention on and what patches to make, about the threats and vulnerabilities of the system, how many threats exist, what are the priorities for solving them and how critical are the vulnerabilities. Ethical hackers simulate attacks within certain limits, depending on the scope and permissions granted to them by the organization, that is, access to the system itself, because they are not malicious, but do a legal job imitating the illegal actions of malicious hackers. The work touched upon various topics closely related to this occupation, with which these experts must be thoroughly acquainted and understand them in order to perform security checks as efficiently as possible. The thesis describes topics such as common types of attacks when hacking systems, the consequences of such attacks and their categories. The importance of cryptography and data encryption and the avoidance of certain protocols, the simulation of network flow, the packet flow and the execution of some of the attacks using certain tools are described. The importance of prevention in crucial time period and risk reduction, depending on the vulnerability. Also are mentioned operating systems with which ethical hackers must be familiar. The occupation described in this thesis requires will and effort, analytical thinking, resourcefulness and readiness for constant learning. The purpose of this paper is to bring this interest closer and explain the need for ethical hackers and their crucial role within the organization.

TITLE

Ethical Hacker

KEYWORDS:

Hackers, Information Security, Hacking techniques, Cryptography, Digital Forensics