Socijalni inženjering kao metoda otkrivanja povjerljivih informacija

Kelam, Ivana

Master's thesis / Diplomski rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University Department for Forensic Sciences / Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:227:562560

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

SOCIJALNI INŽENJERING KAO METODA OTKRIVANJA POVJERLJIVIH INFORMACIJA

IVANA KELAM

Split, rujan 2018.

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

SOCIJALNI INŽENJERING KAO METODA OTKRIVANJA POVJERLJIVIH INFORMACIJA

MENTOR: doc.dr.sc. TONI PERKOVIĆ

IVANA KELAM

346/2016.

Split, rujan 2018.

Rad je izrađen u Sveučilišni odjel za forenzične znanosti,
pod nadzorom doc. dr. sc. Toni Perković,
u vremenskom razdoblju od 8.1.2018. do 30.8.2018.

Datum predaje diplomskog rada: 30. kolovoza 2018.
Datum prihvaćanja rada: 4. rujna 2018.
Datum usmenog polaganja: 17. rujna 2018.
Povjerenstvo: 1. Prof. dr. sc. Dinko Begušić
2. Prof. dr. sc. Josip Kasum
3. Doc. dr. sc. Toni Perković

Sadržaj

1. UVOD

U današnje vrijeme eksponencijalnog razvoja digitalnih tehnologija, stanovništvo svakim danom postaje sve više svjesnije sveobuhvatnih prijetnji računalnoj sigurnosti. Te prijetnje su neovlašteno presretanje informacija, neovlašteno mijenjanje informacija, izlaganje podataka neovlaštenim osobama, te uništavanje hardvera, softvera i/ili informacija za koje postoje sigurnosne mjere zaštite povjerljivosti, integriteta i dostupnosti. [1]

Najveću prijetnju predstavlja način narušavanja računalne sigurnosti koji zaobilazi ljudske sposobnosti za obranu. Takvi načini iskorištavaju najslabiju kariku računalnog sustava. To nije niti hardver, niti softver, već je to čovjek, te se upravo iskorištava prirodna ljudska sklonost povjerenju. Neki autori dijele računalni sustav na tri dijela: hardver, softver i *wetware* ili ljudska komponenta sustava. Većina ljudi se fokusira upravo na prva dva dijela kako bi ih unaprijedili i zaštitili najviše što je moguće. No, napadač može zaobići hardver i softver i vrlo lako prevariti ljudsku komponentu. Iz toga se vidi da je ljudska komponenta postala važan faktor u računalnoj sigurnosti. [2]

Upravo zbog toga se istraživanje računalne sigurnosti proširilo od čiste tehnološke orijentacije do toga da se nastoji razumjeti i objasniti uloga ljudskog ponašanja i djelovanja u sigurnosnim propustima. [1]

Cilj ovoga rada je detaljnije istražiti upravo takve napade na računalnu sigurnost, obuhvaćeni pod nazivom socijalni inženjering, njegove metode i načine napada, kao i mjere zaštite, budući da je konstantno educiranje ključna stavka u zaštiti od socijalnog inženjeringa. Dodatni cilj je i pokušati izvesti napad u kontroliranom okruženju kako bi se pokazalo koliko je lako provesti takve napade, budući da su svi materijali sa uključenim detaljnim uputama dostupni na internetu. Cilj je pokazati kako se javno dostupnim alatima može saznati lozinka Wi-Fi mreže korisnika. Također, pokazati ćemo kako se korisnik, odnosno njegov uređaj jednostavno može preusmjeriti ili povezati na Wi-Fi mrežu napadača, te ćemo pokazati koje sigurnosne implikacije mogu nastati.

1.1. SOCIJALNI INŽENJERING

Postoje brojne definicije i različita objašnjenja socijalnog inženjeringa.

Socijalni inženjering je umjetnost izvlačenja povjerljivih informacija psihološkom manipulacijom žrtve. To je strateški napad koji ovisi o ljudskoj interakciji, složen sustav prevara, koji izvlači od pojedinaca lozinke, podatke bankovnog računa i slično. [3] Naziva se još i znanost manipuliranja, netehnološki način neautoriziranog pristupa informacijama ili računalnom sustavu. To je upotreba trikova, uvjeravanja, lažnog predstavljanja, emocionalne manipulacije i zloupotrebe povjerenja. [4]

Kombinirajući sve te definicije možemo jednostavno reći da je socijalni inženjering, umjetnost ili znanost vještog manevriranja osobom kako bi ona poduzela nekakvu radnju, koja može, a i ne mora biti u njenom najboljem interesu. [5]

Neki socijalni inženjering vide kao jednostavnu prevaru za dobivanje besplatnih predmeta, drugi kao alat kojeg koriste kriminalci ili prevaranti, dok treći to smatraju znanošću. Kako god bilo, socijalni inženjering se koristi svakodnevno, koriste ga obični ljudi u svakodnevnim situacijama. Uzmimo za primjer dijete koje pokušava dobiti slatkiše, zaposlenika koji traži povišicu, ali nažalost i kada kriminalci i prevaranti pokušavaju navesti svoje žrtve na otkrivanje informacija koje ih mogu učiniti ranjivima. Kao i svaki alat, socijalni inženjering nije dobar ili loš, već samo alat koji ima mnogo različitih primjena. [5]

Osnovni ciljevi socijalnog inženjeringa su isti kao i kod hakiranja općenito: dobivanje neovlaštenog pristupa sustavu ili informacijama kako bi se počinila prevara, upad u mrežu, industrijska špijunaža, krađa identiteta, ili kako bi se jednostavno narušio sustav ili mreža. [6]

Kevin Mitnick, nekada jedan od najpoznatijih hakera, a danas poznati američki stručnjak za računalnu sigurnost, otkrio je da ljudi, kada im se postavi pitanje na pravi način, lakše pružaju potrebne odgovore. Socijalni inženjering uspijeva upravo zbog toga što ljudi funkcioniraju na način da vjeruju da su svi ostali s kojima komuniciraju uglavnom iskreni. Postavljajući naizgled nedužan zahtjev na način koji se tada čini sasvim razumnim, napadač može prikupiti upravo informacije koje mu trebaju. [4]

1.2. OBRASCI PROVEDBE NAPADA

Iako je svaki napad socijalnim inženjeringom drukčiji od drugog i svaki je jedinstven na svoj način, postoje nekakvi uobičajeni obrasci koji se nalaze u svakom od tih napada. Ti se obrasci

mogu podijeliti u četiri faze koje su prisutne u svakom od njih: prikupljanje podataka, razvoj odnosa, iskorištavanje i provedba. [7]

1. Prikupljanje podataka: U prvoj fazi se identificira žrtva ili žrtve skupljajući različite podatke o njima iz različitih izvora, što može biti kroz javne dokumente, ciljanu web-stranicu, fizičku interakciju i dr. Prikupljanje podataka je nužno kada se napada pojedinačna žrtva. [8] Jednom prikupljene informacije se mogu iskoristiti za daljnji razvoj odnosa sa žrtvom ili s bilo kim drugim koji može dovesti do uspješno provedenog napada. Neki od podataka koji su potrebni za daljnje napade su: telefonski imenik, datumi rođenja, organizacijski grafikoni i dr. [9]
2. Razvoj odnosa: U drugoj fazi slijedi uspostaviti odnos sa žrtvom kako bi se započeo razgovor ili bilo koji drugi način kako bi se što više otkrilo o samoj žrtvi. Razvijajući taj odnos napadač se postavlja u položaj od povjerenja kojeg će u daljnjem tijeku napada iskoristiti. [8]
3. Iskorištavanje: Treća faza ima za glavni cilj uspostaviti što jaču vezu između napadača i žrtve kako bi nastavili dijalog čime bi se prvotni plan približio što više cilju. Žrtva može biti toliko izmanipulirana od strane „pouzdanog“ napadača da otkrije npr. lozinku ili da izvrši neku radnju. S ovom fazom može završiti napad, ili dovesti do sljedeće faze, a to je provedba prvotnog glavnog napada. [9]
4. Provedba napada: Posljednja faza je provedba samog finalnog napada. Nakon što žrtva ispuni sve zadatke napadača, provedeni napad je gotov. [8]

1.3. DVA TIPA NAPADA: USMJERENI NA OSOBE TE PREKO TEHNOLOGIJA

U napadu usmjerenom na osobe napadač direktno komunicira sa žrtvom s ciljem dobivanja osjetljivih informacija. U ovakvom tipu napada broj žrtvi je ograničen budući da postoji manje načina i mogućnosti da napad obuhvati veći broj žrtava u usporedbi napadom koji se provodi koristeći se nekim oblikom tehnologije. Napadi preko tehnologija se izvode uz pomoć različitih sustava, računala, mobilnih uređaja i slično, te se koriste različitim softverima za dobivanje željenih informacija. [7]

1.4. DVA PRISTUPA NAPADU: FIZIČKI I PSIHOLOŠKI

Napadači imaju dva osnovna pristupa napadu, fizički i psihološki.

Fizički pristup uključuje nekakav oblik djelovanja kojeg napadač izvodi da bi najčešće prikupio podatke o žrtvi. Na primjer tu spada radno mjesto, kada napadač jednostavno ušeta u nekakvu tvrtku ili organizaciju i pretvara se da je radnik na održavanju ili nekakav konzultant koji ima pristup toj zgradi. Kada uspije ući unutar zgrade i ureda jednostavno traži informacije koje u tom trenutku može pronaći, a koje su mu potrebne. [6] Napadači također jednostavno nazovu određenu tvrtku i metodom uvjeravanja izvuku lozinke korisnika. Iako se takve metode čine pomalo smiješnima, zapravo su izuzetno učinkovite, te olakšavaju napade koji se ne bi mogli provesti na nekakav drugi način. [10]

Tehnički pristup možemo svrstati kao podvrstu fizičkog pristupa. Najčešće se napadi izvode preko interneta, gdje su društvene mreže postale važan izvor podataka. Postoje i različiti alati i softveri koji omogućuju skupljanje i sistematiziranje svih podataka sa različitih web-stranica. [7]

Psihološki pristup spada u najvažniji aspekt uspješno provedenog napada socijalnim inženjeringom. Kako bi povećali šanse za uspjeh, napadači pokušavaju razviti odnos s žrtvom oslanjajući se na socio-psihološke tehnike. [7] Napadači često pokušavaju utjecati na žrtve na način da izazivaju jake emocije kod njih, kao što su strah ili uzbuđenje, također pokušavaju uspostaviti prijateljski odnos sa žrtvom i stvoriti osjećaj povjerenja i privrženosti. [1]

Napadači se oslanjaju na prirodne ljudske osobine i sklonosti, kao što su:

- Autoritet: ljudi imaju sklonost izvršavanju zahtjeva ukoliko ih postavi osoba koja im je nadređena, odnosno ukoliko vjeruju da je podnositelj zahtjeva osoba koja ima autoritet, ili koja je autorizirana postaviti takve zahtjeve. Primjer takvog napada je kada se napadač pokušava maskirati u osobu s autoritetom iz IT odjela. [11] Autoritet se može koristiti i za izazivanje straha, kada ljudi u strahu slušaju zapovijedi kako bi izbjegli negativne posljedice kao što su gubitak privilegija ili nečega od vrijednosti, kako bi izbjegli kaznu, poniženje ili osudu. Napadači se oslanjaju upravo na strah od autoritativne naredbe. No, neki ljudi na autoritet reagiraju skeptično i pokušavaju mu se oduprijeti. Kada se napadači koriste autoritetom kako bi izazvali strah ili prijetnju, oni

koji poslušnije reagiraju na autoritet će prije izvršiti napadačeve zahtjeve od onih koji su skeptičniji i prkosniji. [1]

- Sviđanje: ljudi su skloni izvršavanju zahtjeva ukoliko se podnositelj zahtjeva prezentirao kao simpatična osoba, koja ima slične interese, vjerovanja ili stavove kao i žrtva. Kroz razgovor, napadač uspijeva naučiti više o hobijima ili interesima žrtve, zatim se pretvara da dijele te iste hobije ili interese. Pokušat će oponašati svoju žrtvu kako bi što više stvorio izgled sličnosti. [11]

  Ljudi imaju sklonost izvršavanju zahtjeva kako bi se svidjeli onima koji se njima sviđaju. Stoga napadači pokušavaju steći povjerene uspostavljanjem prijateljskog odnosa sa žrtvom. Ljudi uobičajeno vjeruju onima koji im se sviđaju, i obrnuto, sviđaju im se oni kojima vjeruju. Vjeruju u one koje percipiraju kao vjerodostojne zbog njihove stručnosti ili sposobnosti. Na primjer, ljudi mogu biti uvjereni od strane poznatog glumca ili košarkaškog igrača da kupe nekakve uređaje, određenu hranu ili nešto samo zato što im se ta osoba sviđa. [1]
- Reciprocitet: ljudi automatski udovoljavaju zahtjevu kada im je obećano nešto zauzvrat. Taj dar može biti materijalna stvar, savjet ili pomoć oko nečega. Kada netko učini nešto za drugoga, taj osjeća potrebu da mu uzvrati tu uslugu. Jedan od najučinkovitijih načina da se utječe na ljude da udovolje zahtjevu jest dati nekakav dar ili pomoć koji stvara uzvratnu obvezu. Primjer takvog napada je kada zaposlenik neke organizacije primi poziv od osobe koja tvrdi da radi u IT odjelu te organizacije. Pozivatelj objašnjava kako su računala u cijeloj organizaciji zaražena virusom koji antivirusni program nije prepoznao te da može uništiti sve datoteke na zaraženom računalu. Žrtvi ponudi da će joj pomoći proći kroz sve korake kako bi se spriječila šteta. Nakon određenih koraka, upozori zaposlenika da mora promijeniti i lozinku, te mu se ponudi da mu on to sve riješi, a zaposlenik ga ne odbija, budući da smatra da je on upravo taj za kojeg se predstavlja te mu vjeruje i dopušta promjenu lozinke zbog dosadašnje pomoći. [11]
- Odanost/Dosljednost: Odanost se definira kao stav koji vodi do upornog djelovanja i prilično je stabilna ljudska osobina. Odanost možemo podijeliti na više tipova odanosti temeljeno na situaciji i ciljanoj žrtvi. Normativna odanost dolazi iz recipročne razmjene sa žrtvom, gdje će netko uložiti još veći napor i izvršiti radnju zbog toga što je to uobičajeno ili ima obvezu prema tom. U smislu informacijske sigurnosti, ljudi će ponekad otkriti povjerljive podatke onima za koje se osjećaju obavezni zbog svoje odanosti. Dugotrajna odanost je proizvod percepcije ulaganja, npr. novca, vremena i

truda, gdje s prekidom te aktivnosti može doći do nekakvog gubitka ili troška. Ljudi su donijeli svoju odluku, i održavaju svoju dosljednost u tu odluku. Emocionalna odanost uzrokuje da ljudi ulažu napor i poduzimaju radnje u zamjenu za zadovoljstvo koje proizlazi iz emocionalnih veza sa ciljem. [1]

Kod dosljednosti riječ je da ljudi imaju sklonost da nakon što su obećali da će nešto napraviti, ustraju u svom naumu, kako ne bi ispali nepouzdani. Najbolje je ovu osobinu objasniti na primjeru, napadač kontaktira relativno novog zaposlenika i savjetuje ga kako da se pridržava sigurnosnih pravila i postupaka. Nakon raspravljanja o nekoliko sigurnosnih pravila, napadač zatraži od korisnika lozinku kako bi potvrdio da li se radi o lozinci koja je lagana ili teška za probiti. Kada mu otkrije svoju lozinku, napadač mu daje različite savjete i preporuke za buduću lozinku koja će biti teža za probiti. Žrtva prati njegove upute i zbog prethodnog obećanja da će se pridržavati pravila stvara novu, težu lozinku te ju prosljeđuje napadaču kako bi ovaj provjerio da li je u skladu sa sigurnosnim pravilima. [11]

- Društvena prihvaćenost: ljudi imaju tendenciju da ispune zahtjev ukoliko misle da to rade i drugi. Radnje drugih su prihvaćene kao potvrda da je njihovo ponašanje točno i odgovarajuće. Primjer je kada se napadač predstavlja da provodi anketu i navodi sve zaposlenike koji su sudjelovali u anketi. Žrtva, vjerujući da su i drugi napravili anketu, pristaje sudjelovati. Napadač u takvom slučaju može postaviti niz pitanja i izvući potrebne podatke iz žrtve. [11]
- Nestašica: ljudi su skloni ispunjavanju zahtjeva kada vjeruju da je traženi objekt teško za pronaći te da se i drugi natječu za njega ili je dostupan samo u kratkom periodu vremena. Primjer je kada napadač pošalje email navodeći da će prvih 500 zaposlenika koji se registriraju na novu web-stranicu organizacije osvojiti kino ulaznice za novi film. Zaposlenici koji ne sumnjaju u istinitost maila se registriraju, tako što navedu korisničko ime i lozinku, a napadač to iskoristi za svoj daljnji naum. [11]
- Želja da budu od pomoći: nastoji se uvijek da je korisnik zadovoljan. Najbolji način za dobru ocjenu poslovanja je da korisnici dobiju dobre odgovore od onih koji im trebaju pomoći, a to može dovesti do otkrivanja previše informacija. [12]
- Sklonost povjerenju: u ljudskoj je prirodi da se vjeruje drugoj osobi sve dok ova ne pokaže suprotno. Ukoliko se napadač predstavi kao osoba od povjerenja, žrtva uglavnom prihvaća tu činjenicu, ne sumnjajući u nju. [12]

Nedovoljno povjerenje može rezultirati paranojom, nepotrebnom napetošću, dok s druge strane pretjerano povjerenje može dovesti do prevare, smanjene učinkovitosti i nesposobnosti. Napadači koriste različite tehnike kako da postignu povjerenje kod žrtve, npr. izigravaju usamljenost, potrebu za prijateljstvom, stvarju osjećaj sličnosti s potencijalnom žrtvom, a sve kako bi se steklo povjerenje. [1]

- Strah od upadanja u nevolju: ljudi se boje negativne reakcije nadređenih ukoliko npr. provjera identiteta određene osobe traje malo dulje vrijeme ili se određeni službenik na to uvrijedi, pa se često znaju dogoditi i propusti u tom pogledu; [12]
- Prečicom do rješenja: često su ljudi lijeni pa tako lozinke ostavljaju na papiriću kraj kompjutera ili nekakve važne materijale ostavljaju na vidljivom mjestu. [12]

Najuspješniji napadi su kada se kombiniraju svi pristupi zajedno. Najbolji primjer je kada napadači iskorištavaju ljudsku znatiželju pa ostave USB sa malicioznim softverom na njemu, na mjestu gdje će ga žrtva uočiti, a njezina znatiželja potaknuti da ga pokrene na svojem računalu i na taj način zarazi računalo virusom koji je na tom USB-u. Riječ je o kombinaciji fizičko-tehničkog pristupa, te psihološkog. [7]

1.5. TEHNIKE NAPADA

Tri su različite tehnike socijalnog inženjeringa:

1. uvjeravanje: pokušaj da žrtva udovolji neprikladnom zahtjevu, da učini nešto što nije po pravilima. Na primjer, kada napadač traži korisničko ime i lozinku predstavljajući se kao ovlaštena osoba smatra se da to spada pod dimenziju uvjeravanja. Pod ovim se smatra da se određene psihološke karakteristike iskorištavaju, kao što su lijenost, povjerenje, strah, pohlepa. [13]

   Najbolji primjer iz svakodnevnog života su političke kampanje, zatim reklamne poruke koje tjeraju na kupnju nečega što i nije potrebno i na što potrošači nisu mislili potrošiti svoj novac. Sposobnost uvjeravanja se smatra najvažnijom karakteristikom koju napadači socijalnog inženjeringa mogu posjedovati. [2]

   Postoje dvije metode uvjeravanja: direktna metoda i sekundarna, odnosno indirektna metoda. U direktnoj metodi napadači jednostavno pitaju žrtvu za informacije. Često

ovakav način i ne funkcionira, no ukoliko ne prođe na ovaj način, napadač se sprema za sistematični pristup kako bi dobio što želi. Ulažu svoje vrijeme kako bi razvili odnos sa žrtvom te na taj način dobili informacije. U sekundarnoj metodi napadači će potencijalnu žrtvu učiniti osjetljivom, tako što će već na samom početku žrtvi izazvati nekakvu snažnu emociju poput straha ili uzbuđenja. [12]

2. prevara/izmišljanje: ova tehnika nije da utječe na žrtvine stavove, uvjerenja, odnosno da iskorištava njezine karakteristike i izravno ju nasamari, već da stvara lažnu ulogu napadača te lažnu situaciju. U usporedbi s uvjeravanjem, ova tehnika je više obmanljiva i manje uočljivija iz perspektive žrtve. Također, prevara/izmišljanje ne dovodi izravno u iskušenje ili postavlja zahtjeve, već napadač preuzima ulogu kameleona koji može mirno i potiho obavljati svoj napad, a da ga nitko ne primijeti. [13]

   Pretvaranje u nadređenu osobu je jedna od najčešćih situacija ove tehnike napada, a razlog je upravo zbog želja zaposlenika da budu prikazani u najproduktivnijem svijetlu te da se iskažu pred svojim nadređenim. Najopasniji slučaj prevare i izmišljanja je kada se napadač maskira u osobu iz tehničke podrške, jer žrtve imaju dozu povjerenja u njih, te mu daju podatke bez da posumnjaju u identitet tehničara. Također, pretvaranje kao novi zaposlenik je vrlo opasna situacija, budući da su ljudi skloni pomoći novopridošlom kolegi, te na taj način dovesti cijelu organizaciju u opasnost. [2]

3. prikupljanje podataka: svaki napad zahtjeva određeno znanje o meti napada. Prikupljanje podataka prije samog napada je jedan od važnijih dijelova socijalnog inženjeringa. Koriste se tehnike kao što su open source informacije, surfanje preko nečijeg ramena, phishing napadi, prisluškivanje i dr. [13]

Svaka od ovih tehnika se rijetko kad događa samostalno sama za sebe, već je više vjerojatno da će se tehnike od svake primjenjivati simultano. Na primjer, napadačev zahtjev službi za podršku da mu se dodijeli nova lozinka, iako nema korisničko ime ili ID, te priča da će upasti u probleme ako ne pristupi svom emailu što prije, spada u uvjeravanje, ali i u prevaru/izmišljanje. Tehnika prikupljanja podataka je već obavljena prije samog zahtjeva. [13]

2. NAČINI IZVRŠAVANJA NAPADA

2.1. PHISHING NAPADI

Phishing napadi nastoje pristupiti važnim informacijama, kao što su korisničko ime, lozinka ili bankovni podaci, predstavljajući se kao vjerodostojan entitet u elektroničkoj komunikaciji. U takvim napadima, kako bi povećali vjerojatnost uspjeha, napadači pokušavaju predstaviti sebe na način da im žrtva povjeruje i prihvati ih kao vjerodostojne entitete, kao što je na primjer banka. Napadač uglavnom svoj plan započinje izradom web-stranice koja izgleda potpuno isto kao i originalna stranica, no s razlikom u URL putanji. Glavni cilj phishing napada je iskoristiti lažnu vezu koja se pošalje najčešće putem emaila, koji sadrži poveznicu na bankovnu stranicu ili neku drugu ustanovu. Napadač nastoji iskoristiti stranice koje su privlačne žrtvi i koje će joj okupirati pažnju. Kada se žrtva spoji, nastoji izvući sve podatke koji će mu biti potrebni da izvrši svoj napad do kraja. [14]

Phishing napadi se provode na različite načine, jedan od njih je i manipulacija URL nizom. Na primjer, poveznica „http://www.mojabanka.primjer.com“, zapravo vodi na web-stranicu „primjer.com“ na odjeljak „mojabanka“, a žrtva bi klikom na takvu poveznicu pomislila da će pristupiti stranici „mojabanka.com“, odjeljak „primjer“. Također, upotrebom sidra unutar URL niza, žrtvu se usmjeri na lažnu stranicu. Na primjer, poveznica „http://hr.wikipedia.org/wiki/Primjeri“ izgleda kao da će korisniku usmjeriti na članak „Primjeri“, ali klikom na nju preusmjerava nas na neku drugu stranicu. Postoje različiti načini manipulacije poveznicama i preusmjeravanja na lažne web-stranice, no moguće je provesti i phishing napade na način da se žrtvi pošalje lažni email, koji ga upućuje da nazove određeni broj, a kada nazove, žrtva misli da je u kontaktu sa svojom bankom ili nekim drugim vjerodostojnim entitetom, te može biti prevarena pa otkriti povjerljive informacije.
Moguće je žrtvu navesti i na originalnu web-stranicu, no upotrebom skočnih prozora (eng. *pop-up windows*) navesti ju da upiše svoje korisničko ime i lozinku. [15]

Postoji nekoliko potkategorija phishing napada, kao što su:

1. Vishing napadi

   Vishing napad je napad iskorištavanjem VoIP tehnologije, koja omogućuje prijenos zvučne komunikacije preko interneta. Sam termin „vishing“ je kombinacija riječi

„voice“ i „phishing“. [16] Ovakav tip napada je privlačan napadačima zbog raznih razloga, kao što je mogućnost obavljanja poziva bilo kojem telefonskom broju s bilo kojeg dijela svijeta, mogućnost prevare lažnim predstavljanjem, niske cijene poziva i dr. [17]

2. Spear phishing napadi

   Spear phishing napadi su identični phishing napadu s razlikom da se cilja točno jedan pojedinac, ili točno određena organizacijama. Uglavnom nisu pokrenuti od strane nasumičnih hakera, već napadača koji ciljaju na financijsku dobit, otkrivanje poslovnih tajni ili nekakvih vojnih informacija. Za razliku od phishing napada, napadači spear phishingom prethodno prikupljaju informacije o ciljanoj žrtvi. Te se informacije koriste za personalizaciju napada. [18]

3. Pharming napadi

   Pharming napad preusmjerava sav promet usmjeren nekoj ranjivijoj web-stranici na drugu, lažnu web-stranicu, te putem te lažne stranice ostvaruje pristup računalu i podacima. [19]

4. Smishing napadi

   Smishing napad se provodi putem SMS poruka preko mobilnog uređaja kako bi se na uređaju ostavio mamac te otkrili osobni podaci. U današnje vrijeme pametnih telefona, kada većina mobilnih uređaja ima brzu internetsku vezu, smishing napadi imaju iste rezultate kao da se izvodio klasičan phishing napad putem emaila. [20]

2.2. STVARANJE SCENARIJA (eng. *PRETEXTING*)

Pretexting napad stvara i koristi istiniti ili izmišljeni scenarij kako bi se povećala mogućnost da će ciljana žrtva otkriti informacije ili izvršiti radnje koje vjerojatno i ne bi u običnim okolnostima. Sofisticirani primjer pretexting napada je obrnuti socijalni inženjering. Riječ je o načinu kada napadač stvara scenarij u kojem je on izvor informacija koje žrtvi trebaju, te ona pristupa napadaču. [3] Napadač stvori scenarij gdje je on osoba koju će zaposlenici pitati za određene informacije. Ukoliko je dobro istražio i pripremio se, napadač reverznim socijalnim inženjeringom ima povećane šanse za dobiti potrebne informacije od zaposlenika. Tri su dijela reverznog socijalnog inženjeringa: sabotaža, oglašavanje i pomaganje. Najbolji primjer je sljedeće: napadač sabotira mrežu određene organizacije, što prouzrokuje problem. Zatim se

oglasi kao odgovarajuća osoba za rješenje tog problema, a zatim kada dođe popraviti problem zahtjeva određene informacije od zaposlenika i tako dobije ono što je otpočetka i želio, a zaposlenici i organizacija nikada ni ne saznaju da je bila riječ o napadu, jer im je mreža stvarno popravljena. [6]

Pretexting je više od samog stvaranja laži, u nekim se slučajevima stvore potpuno novi identiteti, koji se zatim koriste u manipulaciji za dobivanje informacija. Ovakva vrsta napada ne znači da napadač mora smisliti samo jedan scenarij u jednom napadu, potrebno je da stvara različite scenarije kako bi pokrio sva područja i uspješnije izveo napad. Za uspješno stvaranje scenarija potrebno je dobro istraživanje i prikupljanje podataka kako bi se mogao napraviti kvalitetan scenarij. Na primjer, imitiranje tehničke podrške nema smisla, ukoliko ciljana žrtva ne koristi vanjsku tehničku podršku. Za dobru provedbu scenarija, napadač treba prethodno provesti puno vremena vježbajući i usavršavajući svoju ulogu. Slijedeća načela čine suštinu pretexting napada:

- što se više prethodnog istraživanja napravi veća je vjerojatnost uspješno provedenog napada,
- koriste se dijalekti i izrazi za određenu sredinu gdje se napad provodi,
- što je scenarij jednostavniji, veća je vjerojatnost uspjeha,
- scenarij se treba pojaviti spontano,
- treba se pružiti logičan zaključak. [5]

2.3. IGRANJE ULOGE

Jedan od uobičajenijih napada socijalnim inženjeringom je stvaranje, odnosno upotreba lažnih ovlasti. To može biti jednostavno tiskanje krivotvorenih posjetnica, krivotvorenih identifikacijskih kartica ili znački. U današnje vrijeme postalo je prelagano doći do alata i softvera za ovakve namjene. Napadač ne mora uvijek stvoriti skroz realne lažne kartice ili značke, ukoliko može dobro iznijeti priču koja ide s tim. Jedan od stvarnih primjera je kada je napadač stvorio jednostavnu značku sa simbolom za recikliranje na zelenoj plastičnoj podlozi. Uputio se u ciljanu organizaciju kao predstavnik inspekcije za provjeru o recikliranju. Kada su ga zaštitari zaustavili, predstavio se kao inspektor te da bi organizacija mogla dobiti kaznu zbog nepropisnog recikliranja. Zbog straha od kazne, organizacija je od tada svaki dan odvajala papir od ostatka smeća, a napadač je svaki dan skupljao taj papir, te ga iščitavao i tražio informacije koje su njemu bile potrebe za budući napad. Njegov napad je bio toliko uspješan da je mogao

doći i otići iz organizacije kad je god poželio, budući da se osoblje naviklo da ga svakodnevno vidi. [21]

Oponašanje dostavljača predstavlja jedan od napada igranja uloge. Efektivan je, jednostavan napad, no najteži dio je upravo dobivanje potvrde o ovlasti i isprava kako bi napadač uvjerio druge osobe da je on vjerodostojni entitet. Za uspješno provođenje ovakvog tipa napada, napadač mora dobro poznavati tko i kada vrši dostavu u ciljanu organizaciju, pribaviti sve isprave, dokumente, uniformu dostavljača, odrediti vrijeme napada kako bi se mimoišao sa stvarnim dostavljačem te naravno, pridobiti povjerenje zaposlenika. Slična je stvar i sa provođenjem napada tehničke podrške. Napadač nastoji zavarati zaposlenike tehničke podrške ciljane organizacije kako bi dobio pristup mrežnim resursima i računalima organizacije. [15]

2.4. SURFANJE PREKO RAMENA

Ovakav način napada uključuje napadača koji jednostavno potajno gleda dok žrtva upisuje svoje korisničko ime i lozinku. Napadač se nakon toga može jednostavno vratiti poslije i prijaviti se kao korisnik u sustav, te ga na taj način ugroziti. Razvoj prijenosnih računala te bežičnih mreža dovelo je do toga da većina ljudi koristi kafiće, restorane i zračne luke, kao mjesta na kojima mogu nesmetano obavljati svoj posao. No, jednostavnim pronalaskom pozicije u kojem može promatrati žrtvu, napadač može prikupljati informacije koje mu mogu koristiti u budućim napadima. Druga varijanta ovog načina napada je jednostavno slušati javne razgovore između zaposlenika, budući da ljudi često raspravljaju o osjetljivim i povjerljivim informacijama na javnim mjestima poput restorana uz pretpostavku da ih nitko ne sluša, odnosno ne obraća pažnju na njih. [21]

2.5. KOPANJE PO SMEĆU

Ovaj način napada spada među najdraže načine napadačima. Riječ je o oslanjanju na činjenicu da većina ljudi ne razumije vrijednosti informacija kojih se rješavaju. Većina zaposlenika i ne razmišlja kada bace npr. telefonski imenik organizacije. Napadač može pronaći taj telefonski imenik i iskoristiti ga za lažno predstavljanje putem telefona, budući da sada ima sve telefonske brojeve i imena koji su važni za organizaciju. U smeću se također pronađu osjetljive i povjerljive informacije, poput organizacijskih grafikona, bilješki, kalendari sastanaka,

događanja i odmora, imena ili lozinke za prijavu i sl. Korištenjem informacija koje pronađe u njima, napadač može iskoristiti za svoje buduće napade na ciljanu organizaciju. Najbolja praksa organizacijama bi bila da se svi papirnati proizvod unište, umjesto da se bace. [21]

2.6. NAPAD IZMAMLJIVANJEM

Izmamljivanje suptilno izvlači potrebne informacije tijekom na prvi pogled normalnog razgovora. Izmamljivanje može uključivati prethodno smišljen scenarij ili priču kako bi se objasnilo zašto se određena pitanja uopće postavljaju. Neki napori za izmamljivanje mogu biti prilično agresivni, maštoviti ili uključivati opsežno planiranje. [22]

Biti u stanju učinkovito koristiti napad izmamljivanjem znači da napadač može oblikovati pitanja koja privlače ljude i potiče da se krenu ponašati na način na koji napadač upravo i želi. Napadači unaprjeđuju svoje vještine izmamljivanja preoblikujući svoje riječi i pitanja, a samo istraživanje, odnosno prikupljanje podataka može dovesti do toga da žrtva odgovara na sva pitanja i zahtjeve koje joj se postave. Izmamljivanje funkcionira zbog više razloga:

- većina ljudi ima potrebu biti pristojna, posebno prema strancima,
- ukoliko neka osoba primi pohvalu ili kompliment, više će se upustiti u razgovor s tom osobom, a samim tim i otkriti više informacija,
- većina ljudi reagira ljubazno ukoliko se druga osoba pokaže zanimanje ili zabrinutost za njih. [5]

Kao i kod svakog napada, prethodno prikupljanje informacija je ključno za uspjeh samog napada. Vrlo važni aspekt kod provođenja izmamljivanja su izrazi lica tijekom razgovara. Ukoliko su napadačeve riječi mirne i žrtva se aktivirala u razgovoru, a sam govor tijela napadača ili njegovi izrazi lica su nezainteresirani, to može utjecati na raspoloženje žrtve, a da ona to i ne primijeti. [5]

2.7. MAMAC

Mamac je vrsta napada slična Trojanskom konju, a može koristiti fizičke medije poput USB-a, te se oslanja na znatiželju ili pohlepu žrtve. Slično je phishing napadu, no razlikuje se u tome

što se žrtvi obećava nekakva stvar kao poticaj da se uhvati na mamac. Nudi se besplatna glazba, filmovi, ukoliko se prijave npr. na određene web-stranice. Može se provesti na način da napadač zaražene uređaje distribuira među zaposlenicima, nadajući se da će se povezati s mrežom ciljane organizacije. Takvi uređaji mogu biti predstavljeni kao promotivni pokloni, nagrade za sudjelovanje u anketi i na druge slične načine. [23]

3. MJERE I NAČINI ZAŠTITE

Zaštita od napada socijalnog inženjeringa nije jednostavna kao zaštita hardvera ili softvera. Ne postoji sustav zaštite koji se može privezati za zaposlenike ili obične korisnike kako bi bili sigurni od metoda socijalnog inženjeringa. [5]

Metode zaštite možemo podijeliti na metode zaštite organizacija i metode zaštite običnih korisnika.

3.1. METODE ZAŠTITE ORGANIZACIJE

Napadi socijalnim inženjeringom se vrlo lako provode i teško se obraniti od njih, budući da se oslanjaju na ljudski faktor. Većina ljudi su uglavnom spremni pomoći te vjeruju da se takve vrste napada njima ne mogu dogoditi, a kada budu prevareni nisu ni svjesni toga. Zabrinjavajuća je činjenica da je veliki postotak napada socijalnim inženjeringom proveden upravo od osobe unutar organizacije. Stoga, najbolja obrana protiv socijalnog inženjeringa započinje obrazovanjem. Što više zaposlenika razumije takvu vrstu prijetnje i na koji se način provodi, to je vjerojatnije da će se oduprijeti takvom napadu i prijaviti takvu vrstu aktivnosti. Organizacija mora iskoristiti niz tehnika kako bi osigurala odgovarajuću zaštitu svoje imovine. Ta zaštita mora uključivati podizanje svijesti o sigurnosti educiranjem svojih zaposlenika i osoblja, identifikaciju i zaštitu povjerljivih informacija, tehničku regulativu i sigurnosnu politiku organizacije. [21]

3.1.1. PODIZANJE SVIJESTI O SIGURNOSTI EDUCIRANJEM ZAPOSLENIKA

Od velike je važnosti da svi zaposlenici u organizaciji razumiju potencijalne prijetnje, znaju osnovne sigurnosne procedure i sigurnosnu politiku organizacije. Primjer podizanja svijesti o sigurnosti je i jednostavno informiranje zaposlenika da nitko nikada iz organizacije neće pitati za njihove lozinke. [21]

Zaposlenike je potrebno upoznati i sa posljedicama napada socijalnim inženjeringom. Dobar program obuke mora biti raznolik, potrebno je proći kroz što više mogućnosti i alata kako bi se što više postiglo povećanje svijesti i razumijevanje prijetnji. [15]

Četiri načina podizanja svijesti o sigurnosti:

- napraviti formalno dokumentiranu sigurnosnu politiku i politiku obuke zaposlenika,
- pružiti osnovnu obuku o sigurnosti svim zaposlenicima unutar organizacije,
- osigurati specifičnu obuku individualnim zaposlenicima koji imaju važnu ulogu i koji imaju pristup značajnim informacijama unutar organizacije,
- dokumentirati, pratiti i ponavljati periodično obuke podizanja svijesti i obuke o sigurnosti za svo osoblje. [21]

Podizanje svijesti o sigurnosti nije samo kratkotrajni program kroz koji se prođe jednom godišnje. Riječ je o stvaranju sigurnosne kulture i skupa standarda koju svaka osoba treba koristiti cijeli život. [5]

3.1.2. IDENTIFIKACIJA I ZAŠTITA POVJERLJIVIH INFORMACIJA

Vrlo je bitno da svaka organizacija identificira važne i povjerljive informacije kojima raspolaže. Mora se osigurati pravilna klasifikacija svih informacija. Također, sam pristup povjerljivim informacijama mora biti ograničen samo za one koji imaju pravo pristupa tim informacijama. Dobro promišljena i implementirana politika upravljanja identificiranjem, zaštitom i pravom pristupa određenim informacijama može uvelike ublažiti napade na organizaciju. [21]

3.1.3. TEHNIČKA REGULATIVA I SIGURNOSNA POLITIKA

Mudro implementirana tehnička regulativa može dosta otežati napadačima socijalnog inženjeringa da provedu uspješni napad. Tehnička regulativa uključuje razdvajanje dužnosti, kompleksnost lozinki, više faktorsku autentifikaciju, vatrozid, sustave za otkrivanje napada i drugo. Dobro dokumentirana sigurnosna politika ključni je dio obrambene strategije. [21]

Potrebno je provesti sigurnosnu provjeru za svakog novog zaposlenika kako bi se utvrdilo da ne predstavlja sigurnosnu prijetnju organizaciji. Potrebno je provesti mjere zaštite od virusa i drugih zlonamjernih prijetnji. Provođenje politike o lozinkama je jedno od ključnih u zaštiti od socijalnog inženjeringa. Bitno je naučiti zaposlenike da ne koriste iste lozinke za različite namjene, da ne dijele nikada lozinku s drugima, da ne koriste osobne podatke za smišljanje lozinke, kao ni da to ne budu prejednostavne lozinke. Važno je naučiti ih da lozinke nikada ne

zapisuju i ostavljaju na vidljivom mjestu, te da je lozinku potrebno promijeniti s vremena na vrijeme. Bitno je svakom zaposleniku osigurati jedinstveni identifikator koji će odrediti prava pristupa za svakog zaposlenika pojedinačno. Tako da ako napadač sazna identifikator nekog zaposlenika ima pravo pristupa samo određenim dijelovima, dok je ostatak zaštićen. [15]

3.2. METODE ZAŠTITE OBIČNIH KORISNIKA

Svaka osoba koja se koristi internetom u opasnosti je da postane žrtvom socijalnog inženjeringa. Najveći problem je što većina ljudi smatra da se tako nešto njima ne može dogoditi. Stoga je potrebno provoditi edukaciju i običnih korisnika, no to i nije toliko lagano kao obuka zaposlenika unutar organizacije, pa se edukacija običnih korisnika može provoditi kroz različite reklamne poruke, objavljivanjem vijesti o provedenim napadima ili na bilo koji drugi način kako bi se utjecalo na obične korisnike te podigla njihova svijest o sigurnosti na internetu općenito.

Prateći određene indikatore napada može se i običan korisnik zaštiti te ne postati žrtvom, a to su:

- ukoliko netko stvara veliki osjećaj hitnosti kako bi natjerao na donošenje brzih odluka, treba biti sumnjičav,
- obratiti pozornost na osobu koja traži informacije za koje nema pristup ili bi te informacije već trebao znati,
- obavijesti koje su toliko dobre da su nevjerojatne, kao što je obavijest o dobitku na lutriji. [7]

Za sprječavanje napada sa sljedećim stvarima treba postupiti s oprezom:

- ukoliko postoji sumnja da netko pokušava provesti socijalni inženjering, prekinuti svu komunikaciju s tom osobom,
- biti sumnjičav i prekinuti poziv ako treba, ukoliko je osoba koja zove nepoznata,
- ukoliko je primljeni email nepouzdan, odnosno poslan od strane nepoznatog pošiljatelja, a ne postoji povjerenje u poruku, potrebno je takav email izbrisati. [7]

Svaki obični korisnik interneta može poduzeti sljedeće mjere zaštite:

- online transakcije obavezno se provode preko web lokacija koje sadrže *https* protokol, te uvijek provjeravati da li je ta web-stranica sigurna,
- nikada se osobni podaci ne smiju otkrivati preko telefona, pogotovo nepoznatom pozivatelju ili preko web-stranica koje nisu sigurne,
- nikada ne kliknuti na poveznice, preuzimati datoteke ili otvarati privitke od nepoznatog pošiljatelja,
- biti oprezan sa poveznicama na web obrasce koji traže osobne podatke, čak iako izgleda da email dolazi od legitimnog izvora. Upravo su phishing stranice identične replike legitimnih web-stranica,
- korisnici društvenih mreža ne smiju vjerovati u svakoga i potrebno je da samo ograničene informacije o sebi pružaju. Bilo bi dobro ne objavljivati npr. kućne fotografije, raspored godišnjih odmora. Nikada ne bi smjeli kliknuti na poveznice ili videa nepoznatog podrijetla kao i nikada ne preuzimati nepouzdane aplikacije,
- usvojiti odgovarajuće sustave zaštite poput filtra za neželjenu poštu, antivirusni softver i nastojat provoditi konstantna ažuriranja, [3]
- potrebno je biti sumnjičav za bilo koju email poruku koja hitno zahtjeva osobne financijske podatke ili prijeti ukidanjem online računa ukoliko se nešto ne napravi,
- napadači obično traže podatke kao što su lozinka, korisničko ime, broj kreditne kartice i sl., što prave organizacije koje te podatke imaju i traže nikada to neće činiti online,
- prevarantski email neće biti personaliziran, već će započeti sa „Dragi korisniče,...“, dok su poruke od legitimnih entiteta uglavnom personalizirane,
- redovite promjene lozinki su potrebne za sve online račune, [8]
    - lozinke su često prva crta obrane protiv uljeza. Najjednostavniji su način, kao i najjeftiniji od specijalnih kartica ključeva, uređaja za skeniranje otiska prsta i sl. No, iako su najčešće korišteno sredstvo zaštite, vrlo lako se mogu probiti. Za sprječavanje napada na lozinku potrebno je stvoriti jake lozinke. Potrebno je da lozinke budu dovoljno duge, budući da je teže probiti lozinku kako ona ima više znakova. Općenito je pravilo da lozinke sadrže barem jedno veliko slovo, malo slovo, brojeve, specijalne znakove kao što su $, ?, &, te nestandardne znakove poput µ, £, Æ. [24]
    - također, izbjegavati stavljanje iste lozinke za sve račune koji se koriste.

3.3. VIRTUALNA PRIVATNA MREŽA (VPN)

Jedan od načina zaštite od presretanja prometa preko interneta, odnosno neovlaštenog pristupa povjerljivim informacijama je korištenje virtualne privatne mreže. Virtualna privatna mreža za prijenos podataka i međusobnu komunikaciju najčešće koristi internet, a privatnost se osigurava primjenom odgovarajućih sigurnosnih mehanizama, poput enkripcije i tuneliranja. Budući da je promet između uređaja i mreže kriptiran, ostaje privatan i zaštićen cijelo vrijeme prijenosa. Virtualnu privatnu mrežu je najbolje zamisliti kao siguran tunel između uređaja i odredišta koje se na internetu posjećuje. Računalo se spoji sa VPN poslužiteljem, koji može biti bilo gdje, od SAD-a, Britanije, Francuske, Tajlanda i drugo. Prilikom korištenja VPN mreže spajanjem na javnu Wi-Fi mrežu, napadačima će teško biti ukrasti podatke prijave ili preusmjeriti računalo na lažnu web lokaciju. Također, teško će im biti saznati i koje stranice se uopće posjećuju. Ukoliko i dobiju uvid u lokaciju odakle se pristupa nekoj web stranici, vidjeti će web lokaciju VPN poslužitelja. VPN je dobar način zaštite vlastite privatnosti i osiguranja podataka koji mogu biti izloženi različitim vrstama napada. [25]

3.4. Tor (The Onion Router)

Tor je sustav koji nam omogućuje sigurno i anonimno korištenje interneta, pretraživanje i objavljivanje web stranica, korištenje svih sustava koji koriste protokole građene na TCP protokolu. Radi se o slojevitoj enkripciji, što znači da se podaci ponovno enkriptiraju i po nekoliko puta za svaki prolaz kroz nasumice odabrane čvorove. Relejni krugovi se resetiraju svakih 10 minuta nasumičnim odabirom, te se akcije ne mogu povezati. Osim toga, predstavlja i platformu koja omogućuje izgradnju novih aplikacija s ugrađenim mogućnostima zaštite privatnosti korisnika i različitim sigurnosnim elementima. Sigurnost i anonimnost prometa preko interneta se osigurava sprečavanjem analiziranja ostvarenog mrežnog prometa. Komunikacija se preusmjerava unutar distribuirane mreže poslužitelja, tzv. onion poslužitelja, čime se korisnika štiti od web stranica koje neovlašteno sakupljaju podatke o posjetiteljima, od napadača koji pokušavaju steći pristup potencijalno osjetljivim podacima pa čak i od samih onion poslužitelja. Tor mreža štiti od analize prometa, oblika nadzora internet aktivnosti koji omogućuje utvrđivanje izvorišta i odredišta komunikacije. Kako bi se onemogućila analiza prometa, transakcije se unutar Tor mreže distribuiraju preko većeg broja posrednika od kojih ni

jedan ne poznaje izvorište, a niti odredište paketa. Umjesto izravnog slanja podataka od pošiljatelja prema primatelju, oni se šalju preko većeg broja nasumično odabranih poslužitelja. Tor sustav korisnicima omogućuje i zaštitu privatnosti, odnosno skrivanje njihova identiteta. [26]

Lako je primijetiti da i Tor i virtualna privatna mreža imaju istu primarnu funkciju – pružiti zaštitu anonimnosti na internetu i zaobići vatrozid. Za vrhunsku privatnost mogu se koristiti zajedno preko VPN-a koji ima mogućnost „Tor over VPN“ konekcije. [27]

4. PROVOĐENJE NAPADA

Provođenjem kontroliranih napada nastojat će se pokazati koliko je lako doći do besplatnih alata i softvera za provedbu različitih napada socijalnog inženjeringa, te koliko se uz pomoć tih alata lako mogu provesti jednostavni, ali učinkoviti napadi, a da nije ni potrebno preveliko predznanje. Provedeni napadi izvršeni su isključivo za potrebe ovoga rada, te se sve odvijalo u kontroliranom okruženju. Prvi program kojim se proveo napad obuhvaća otkrivanje lozinke Wi-Fi mreže, drugi program stvara vlastitu lažnu pristupnu točku te prisluškuje promet spojenog korisnika, dok treći stvara lažnu web-stranicu.

4.1. PROBLEM LOZINKI

Digitalni trag korisnika interneta se širi i obuhvaća sve, od društvenih mreža, financijskih podataka te podataka pohranjenih u oblaku, a često samo jedan račun podupire sigurnost cijelog identiteta, a to je email adresa. Sve je to ugroženo ukoliko se otkrije email lozinka ili se saznaju odgovori na pitanja za oporavak lozinke. Jednom otkrivena, napadač može resetirati sve lozinke žrtve na drugim uslugama koje koristi, preuzeti sve njezine podatke, obrisati podatke i sigurnosne kopije, ili se lažno predstavljati kao žrtva. [28]

Najveći je problem u samom korisniku, ljudi stvaraju slabe lozinke, ponovno ih upotrjebljuju na više web mjesta, dijele informacije na društvenim mrežama i nenamjerno klikaju na poveznice koje mogu biti maliciozne i preuzeti zlonamjerni softver ili virus. Napadaču je jednostavan uvid u lozinku prilika za otkrivanje svih drugih računa koje taj korisnik ima, te mogućnost otkrivanja svih podataka o žrtvi za zlonamjernu upotrebu. [29]

Zbog različitih načina kako koristimo internet, lako je shvatiti neke lozinke manje važnima od drugih. Međutim, svaka je lozinka važna jer napadač lako spoji sve informacije koje su pohranjene online i iskoristiti ih za svoju dobit. Složene metode otkrivanja koje koriste postaju sve lakše dostupnima i sve više učinkovitijima. Najveće greške korištenja lozinki su sljedeće:

- korištenje slabe lozinke: lozinka se smatra slabom ukoliko se može pogoditi. Slabe lozinke su uobičajeni izrazi, korištenje vlastitog imena i prezimena, datuma rođenja, ili korištenje izraza „lozinka“ ili „p@ssw0rd“. Primjeri slabih lozinku su još i: 123456, qwerty, admin, abc123, hello i dr.

- upotreba iste lozinke za svaki pojedinačni račun: ukoliko napadač otkrije jednu lozinku za jedan račun, tada može pristupiti svim drugim računima koje ta žrtva ima. Također, upotreba istog uzorka za sve lozinke je riskantna. Napadač može otkriti strukturu jedne lozinke, što povećava šanse da otkrije lozinke za druge račune.
- otkrivanje lozinke drugima: tu se uključuje i prijavljivanje na javnim računalima, čuvanje bilješki sa zapisanom lozinkom, ili jednostavno otkrivanje lozinke prijateljima ili drugima. [30]
- zamjena brojeva za slova: naizgled efektivan način, no lako ga je otkriti, budući da danas postoje različiti softveri za detektiranje takvih načina. Primjer zamjene je zamjena slova E sa brojem 3, slova O sa brojem 0, slova I sa brojem 1 i dr.
- korištenje lozinke koja je prekratka: dok je prije lozinka od pet do šest znakova bila smatrana dugom lozinkom, danas postoje softveri koji takvu lozinku mogu probiti u kratkom vremenu. Stoga, danas se dugom smatra lozinka od 12 znakova i više.
- korištenje iste lozinke, no sa samo jednom promjenom: ovo se odnosi kada korisnik smatra da je promjenom samo jednog znaka unutar lozinke, stvorio kompletno novu lozinku. Softveri danas to lako prepoznaju i vrlo lako probiju. Primjer je kada korisnik ima lozinku koja glasi: „lozinka1“, a za drugi račun, ili na tom istom računu promijeni lozinku u: „lozinka2“. [31]

4.1.1. Wireless Local Area Network

WLAN (eng. *Wireless Local Area Network*) skraćenica je za bežičnu lokalnu mrežu, a predstavlja računalnu mrežu koja povezuje jedno ili više računala pomoću bežične tehnologije, pomoću elektromagnetskih valova koji su smješteni između radio valova i infracrvenih valova, frekvencije od 2,4 GHz do 5,8GHz. Osnovni elementi bežične mreže su:

- bežična mrežna kartica: osigurava osnovnu mrežnu komunikaciju, odnosno brine se za adresiranje unutar WLAN, i identificira klijenta ili pristupnu točku,
- pristupna točka: korisnicima bežičnih uređaja omogućuje pristup mreži,
- stanice: spajaju se na pristupne točke; uređaji poput računala, pametnih telefona i sl.,
- BSS – Basic Service Set: osnovni element mreže, a čine ga dvije ili više stanica,

- BSSID – Basic Service Set Identifier: identifikator mreže; kod infrastrukturnog BSS-a (kada sve stanice komuniciraju preko pristupne točke) riječ je o fizičkoj MAC adresi pristupne točke,
- SSID – Service Set Identifier: predstavlja naziv mreže od minimalno 32 ASCII znaka. [32]

Postoje 3 glavna standarda koji služe za zaštitu WLAN prometa: WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*) i WPA2.

- WEP: prvi standard za zaštitu podataka i definiran je unutar standarda IEEE802.11. Riječ je o simetričnom algoritmu koji koristi isti tajni ključ za enkripciju i dekripciju. Ključevi su standardnih duljina od 64, 128 i 256 bita. WEP enkripcija koristi RC4 algoritam za kriptiranje, te se kriptira bit po bit.
- WPA: koristi kao i WEP RC4 algoritam za enkriptiranje, ali je poboljšan TKIP protokolom koji služi za dinamičko mijenjanje ključeva u vrijeme korištenja sustava.
- WPA2: standard koji ne koristi RC4 algoritam već AES, napredni enkripcijski standard. [33]

Handshake je pojam koji se koristi za opis procesa jednog računala koji uspostavlja vezu s drugim računalom ili uređajem. Handshake je često korak potvrđivanja veze, brzine ili autorizacije računala koje se pokušava povezati s njom. [34]

4.1.2. Fluxion

Fluxion je alat koji automatizira proces stvaranja lažne pristupne točke blizanca kako bi uhvatio WPA/WPA2 lozinke. Fluxion je mješavina tehničkog dijela napada i socijalnog inženjeringa koji nasamaruje žrtvu da preda Wi-Fi lozinku. Baziran je na programima koji su već dio Kali Linux distribucije, kao što su *aircrack-ng, mdk3, hostapd* i dr. Riječ je o napadu socijalnim inženjeringom koji koristi zlonamjernu lažnu pristupnu točku blizanca, integrirani zastoj, te funkciju hvatanja handshake-a kako bi se nasamario korisnik. Za razliku od drugih sličnih programa, Fluxion provjerava točnost WPA/WPA2 lozinke, i pruža samo one lozinke koje su ispravne za tu ciljanu bežičnu mrežu.

Fluxion je jedinstveni alat koji koristi WPA handshake, ne samo da kontrolira ponašanje stranice za prijavu, već i ponašanje čitave skripte. Zaustavlja originalnu pristupnu točku, stvara lažnu pristupnu točku blizanca, privlačeći odspojenog korisnika na ponovno spajanje, ali na lažnu točku. Prikaže se lažna forma za prijavu gdje se mora unijeti lozinka za nastavak. Ovaj alat koristi uhvaćeni handshake kako bi provjerio unesenu lozinu i nastavlja jedino ako je unesena lozinka točna. Ovaj napad je najučinkovitiji kada je usmjeren žrtvi koja nije tehnološki upućena. Osjetljive pristupne točke sa sustavom za otkrivanje upada mogu otkriti i pokušati se obraniti od napada blokirajući IP adresu napadača kao odgovor na integrirani zastoj. [35]

Glavna prednost ovog alata je da mu nije potreban rječnik lozinki kao ni napad uzastopnim pokušavanjem (eng. *brute-force attack*) za otkrivanje lozinki.

Osnovni koraci kroz koje napad prolazi:

- skeniraju se sve bežične mreže u krugu zlonamjernog računala, te se odabire od ponuđenih ciljana žrtva,
- aktivira se *Handshake Snooper* napad te se uhvati handshake (ukoliko već postoji prethodno uhvaćen handshake, unese se samo putanja do *.cap* datoteke),
- aktivira se *Captive Portal* napad,
- stvara se lažna pristupna točka blizanac, koja je potpuno ista kao i originalna,
- svi zahtjevi DNS serveru se usmjeravaju na napadača,
- stvara se *Captive Portal* za unos lozinke,
- svi klijenti se odspajaju automatski sa svoje pristupne točke i spajaju na lažnu,
- svi se zahtjevi *Captive Portalu* provjeravaju sa prethodno uhvaćenim handshake-om,
- napad završava čim se uhvati točna lozinka. [36]

Prvu fazu napada, a to je hvatanje handshake-a pokazati ćemo na drugi način kako se može uhvatiti. Riječ je o korištenju alata *Aircrack-ng* koji je već integriran u Kali Linux distribuciji.

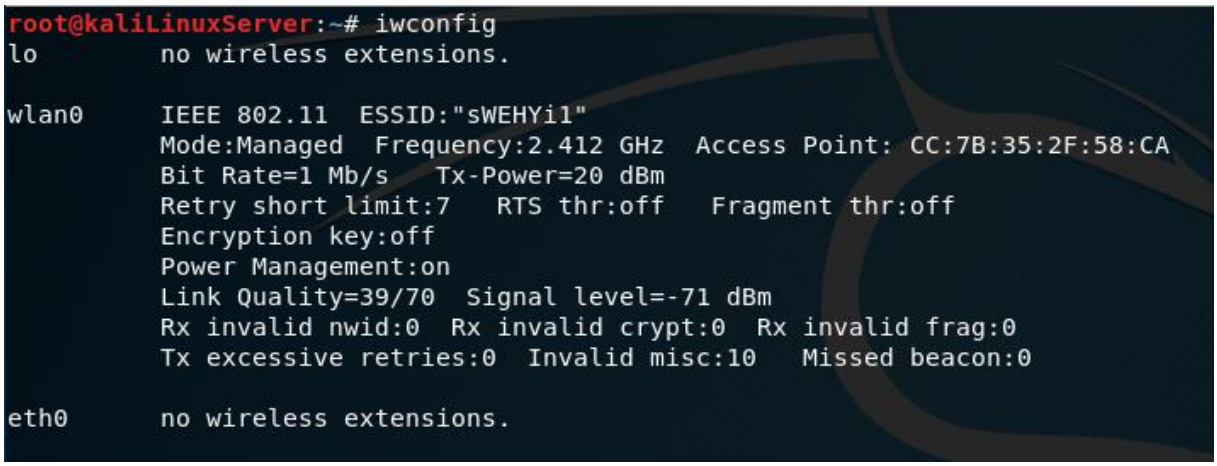
4.1.2.1. Aircrack-ng

Aircrack-ng je naziv za skup besplatnih alata za procjenu sigurnosti bežične mreže. Može pratiti mrežni promet, probijati WEP, WPA/WPA2 lozinke te analizirati bežične lokalne mreže. Podržan je i na Windows operacijskim sustavima i na Linux operacijskim sustavima, no preporuča se upotreba na Linux sustavima jer se na Windowsima može naići na brojna ograničenja koji su posljedica samog operacijskog sustava. [37]

Korištenjem ovog alata pokazat ćemo kako se može uhvatiti handshake, te na taj način otkriti lozinka ciljane žrtve. Korištena je Kali Linux distribucija, koja već sadrži *Aircrack-ng* programski paket. Osnovni koraci kroz koje ćemo proći:

- mrežnu karticu ćemo postaviti u monitor način rada,
- pokrenut ćemo u terminalu naredbu „airodump-ng“ s filtrom za BSSID žrtve,
- koristit ćemo „aireplay-ng“ naredbu u terminalu za deautentifikaciju žrtve s mreže,
- naredbom u terminalu „aircrack-ng“ pokušat ćemo saznati lozinku.

Započinjemo na način da postavimo mrežnu karticu u monitor način rada, što znači da mrežna kartica može prisluškivati svaki paket. U normalnom načinu rada prisluškivati će pakete koji su upućeni samo svom računalu. Prisluškujući sve pakete, omogućeno je hvatanje handshake-a. Naredba „iwconfig“ prikazuje nam listu bežičnih sučelja.

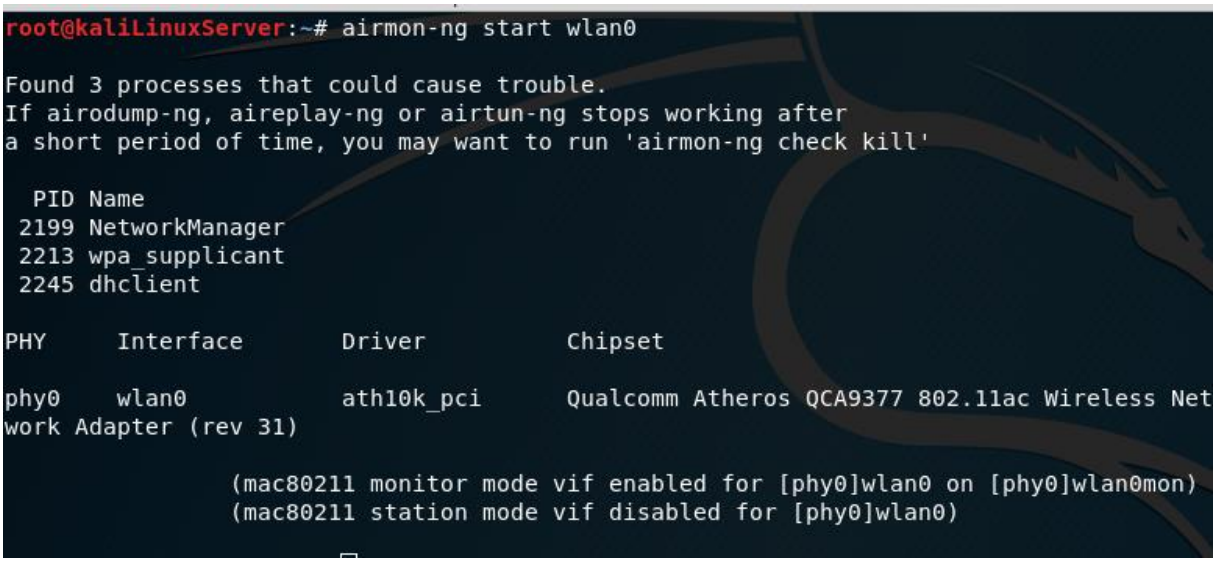


Slika 1: Korištenje naredbe „iwconfig“ za prikaz bežičnih sučelja

Za provjeru da li bežična kartica računala uopće i podržava monitor način rada, može se lako provjeriti korištenjem naredbe „iw list“ u terminalu:

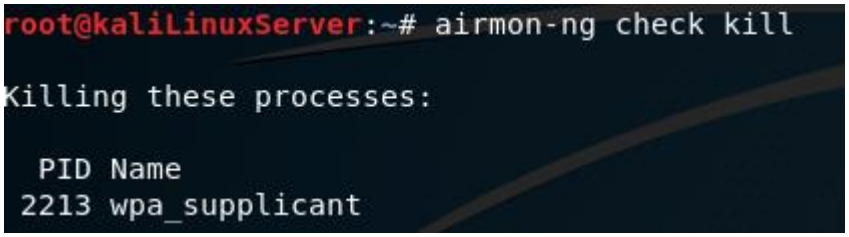
Slika 2: Korištenje naredbe „iw list“ koja pokazuje sve načine rada korištene bežične kartice računala

Vidimo da je naše bežično sučelje *wlan0,* kojeg ćemo staviti u monitor način rada. *Airmon-ng* skripta iz *Aircrack-ng* skupine alata omogućuje stavljanje u monitor način rada. Parametar *start* označuje upravo to da se bežično sučelje *wlan0* postavi u monitor način rada. Za vraćanje u normalni način rada, koristi se parametar *stop*.



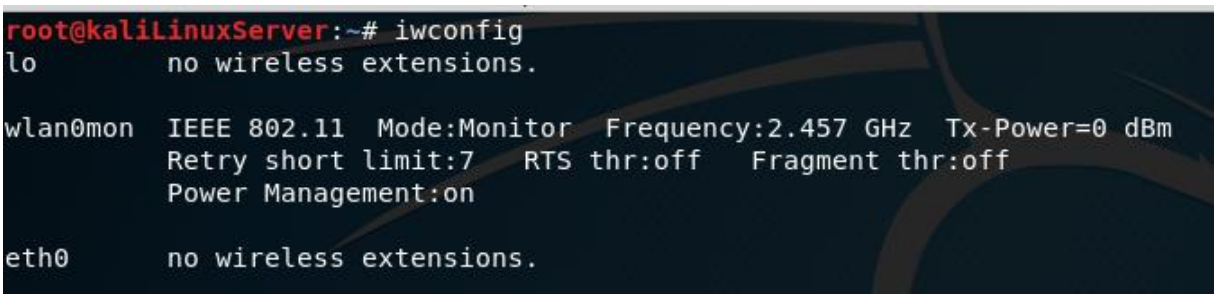
Slika 3: Korištenje naredbe „airmon-ng“ za stavljanje bežične kartice u monitor način rada

Vidimo da je bežična kartica postavljena u monitor način rada, te joj je dodijeljeno sučelje *wlan0mon*. Budući da je javljeno upozorenje kako neki već pokrenuti procesi mogu prouzrokovati probleme, naredbom „airmon-ng check kill“ zaustavljamo te procese.



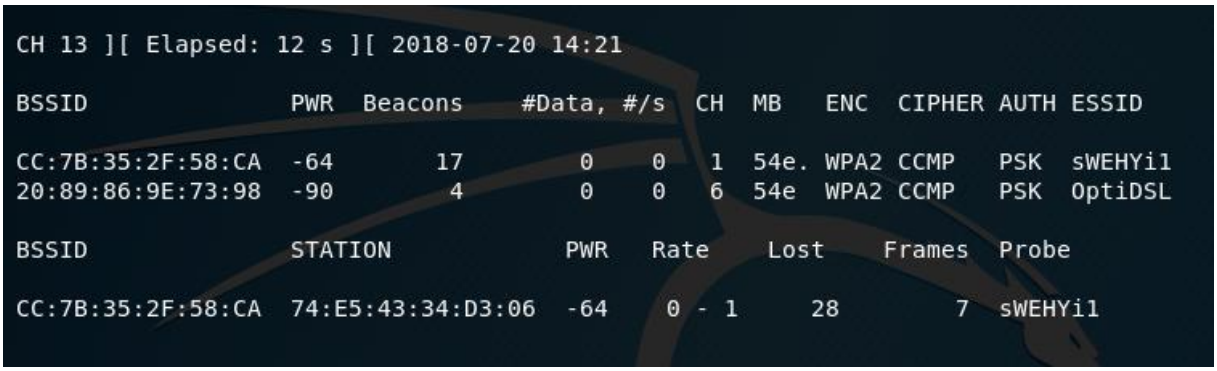
Slika 4: Korištenje naredbe „airmon-ng check kill“ za zaustavljanje procesa koji mogu prouzrokovati probleme u daljnjem radu

Ponovnom upotrebom naredbe „iwconfig“ vidimo da nam je sučelje promijenilo naziv u *wlan0mon,* te da je sad postavljen u monitor način rada.



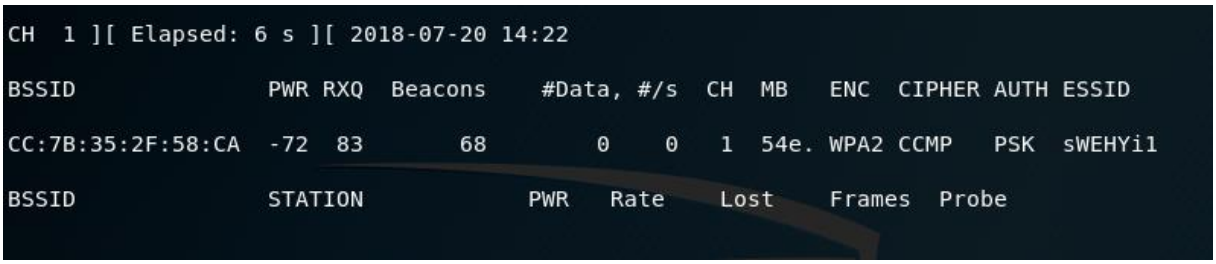
Slika 5: Prikaz da je sučelje u monitor načinu rada upotrebom naredbe „iwconfig“

Korištenjem naredbe „airodump-ng wlan0mon“ dobijemo ispis informacija o svim bežičnim mrežama koje se nalaze u blizini računala s kojeg smo i pokrenuli naredbu.



Slika 6: Prikaz ispisa naredbe „airodump-ng wlan0mon“

Airodump-ng zapisuje prikupljene pakete u datoteke *.cap* formata koju ćemo koristiti poslije za otkrivanje lozinke, kao i druge datoteke različitih formata. Nakon što pronađemo ciljanu žrtvu, u našem slučaju riječ je o pristupnoj točki *sWEHYi1*, zaustavljamo provođenje naredbe, odnosno prisluškivanje mrežnog prometa sa kombinacijom tipki *CTRL+C*. Dodavanjem parametara naredbi „airodump-ng“, možemo preusmjeriti snimanje mrežnog prometa na samo ciljane pristupne točke. Ubaciti ćemo parametre *-c*, što nam označava kanal na kojem se nalazi ciljana pristupna točka, zatim parametar *-w*, što nam je naziv datoteke u koji će se spremiti snimljeni podaci o mrežnom prometu ciljane pristupne točke, te parametar *--bssid* koji je MAC adresa ciljane pristupne točke. Rezultat naredbe: „airodump-ng -c 1 -w TestF –bssid CC:7B:35:2F:58:CA wlan0mon“, prikazan je na sljedećoj slici.



Slika 7: Prikaz rezultata naredbe koja omogućuje prikaz podataka ciljane pristupne točke

Naredba *„aireplay-ng“* služi za ubacivanje paketa u bežičnu mrežu te na taj način generira mrežni promet. Parametar *--deauth* šalje pakete deautentifikacije jednom ili više klijenata koji

su trenutno povezani s pristupnom točkom. Broj 100 označava da će se ti zahtjevi poslati 100 puta. Parametar *-a* definira MAC adresu pristupne točke.

```
root@kaliLinuxServer:~# aireplay-ng --deauth 100 -a CC:7B:35:2F:58:CA wlan0mon -
-ignore-negative-one
14:52:52  Waiting for beacon frame (BSSID: CC:7B:35:2F:58:CA) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
14:52:52  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:52  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:53  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:53  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:54  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:54  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:55  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:55  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:56  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:56  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:57  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:57  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:58  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:58  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:59  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:59  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:52:59  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:53:00  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
14:53:00  Sending DeAuth to broadcast -- BSSID: [CC:7B:35:2F:58:CA]
```

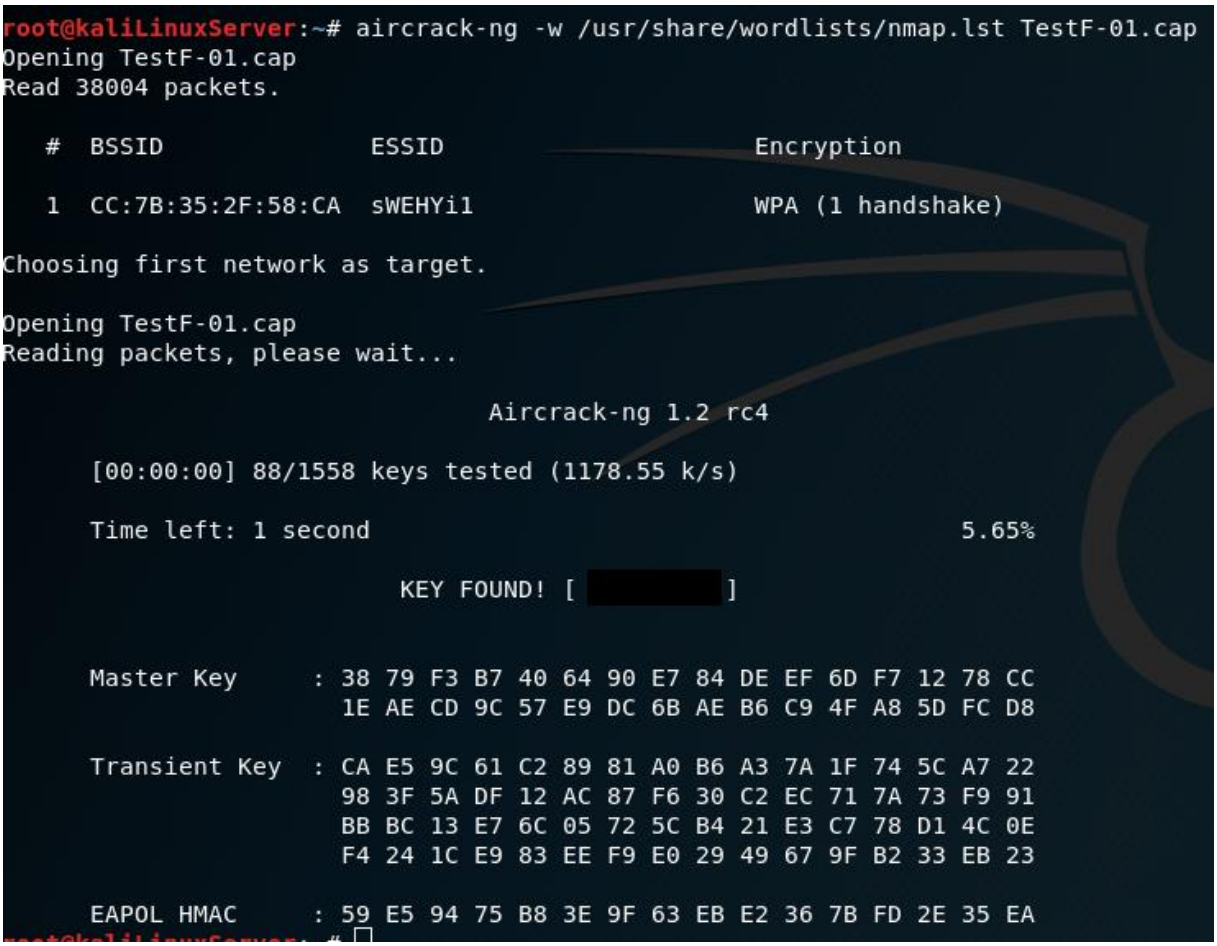
Slika 8: Prikaz rezultata naredbe koja šalje deautentifikacijske pakete

Prethodnu naredbu „airodump-ng“ ne gasimo u terminalu, već nakon provedene posljednje naredbe slanja deautentifikacijskih paketa čekamo kada će nam se u tom terminalu gdje se prisluškuje mrežni promet pokazati da je uspješno uhvaćen WPA handshake, što vidimo u desnom gornjem rubu sljedeće slike.

```
CH  1 ][ Elapsed: 1 min ][ 2018-07-20 14:54 ][ WPA handshake: CC:7B:35:2F:58:CA

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

CC:7B:35:2F:58:CA  -70 100     1076    17722   27   1  54e. WPA2 CCMP   PSK  sWEHYi1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

CC:7B:35:2F:58:CA  9C:4F:CF:85:D8:99  -30    0 - 1e     0        4
CC:7B:35:2F:58:CA  24:4B:81:18:16:06  -53    0e- 9e   224      249  sWEHYi1
CC:7B:35:2F:58:CA  08:3D:88:26:87:77  -51    0e- 0      0       94
CC:7B:35:2F:58:CA  74:E5:43:34:D3:06  -56    0e- 0e     4    17361
CC:7B:35:2F:58:CA  90:E7:C4:A4:25:AC  -64    0e- 1      0       12
CC:7B:35:2F:58:CA  BC:76:5E:E8:CA:76  -77    0e-24      0      130
```

Slika 9: Prikaz da je handshake uhvaćen

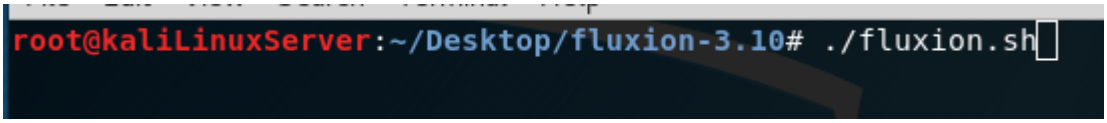
Naredbom *„aircrack-ng“* te korištenjem parametara *-w*, koji nam označava putanju rječnika odakle će se pokušati probiti lozinka, te same *.cap* datoteke u koju je iz prethodno provedenih koraka spremljen handshake, dobijemo sljedeći rezultat. Budući da je riječ o testnom napadu, u rječnik lozinki upisana je i lozinka ciljane nam žrtve, mreže *sWEHYi1*, stoga nam je i rezultat uspješan. No, to samo znači da se lozinke kao što je već spomenuto, npr. *1234*, *qwerty*, *password* i druge mogu s lakoćom probiti.



Slika 10: Prikaz da nam je lozinka uspješno otkrivena

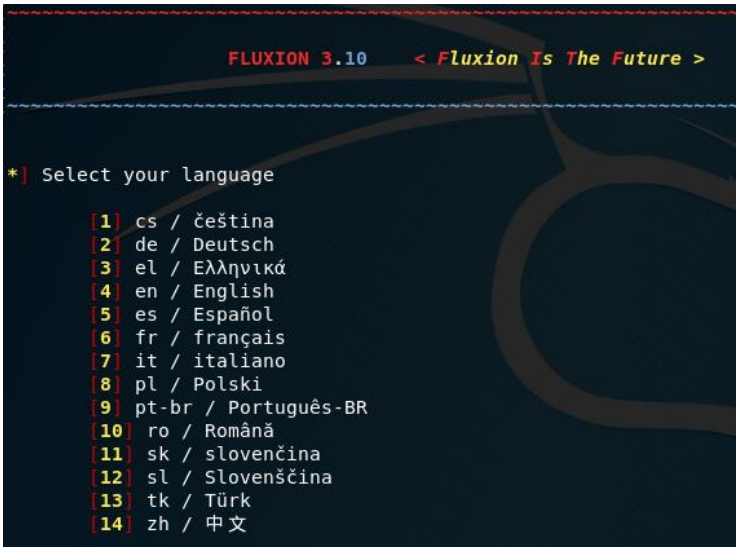
4.1.3. Provedba napada korištenjem programa Fluxion

Korištenje programa Fluxion započinjemo tako da korišteno bežično sučelje postavimo u monitor način rada kako je prethodno opisano. Sam program pokrećemo u terminalu naredbom „./fluxion.sh„.



Slika 11: Pokretanje programa Fluxion

Nakon što je program uspješno pokrenut otvori se izbornik odabira jezika, te smo odabrali engleski jezik.

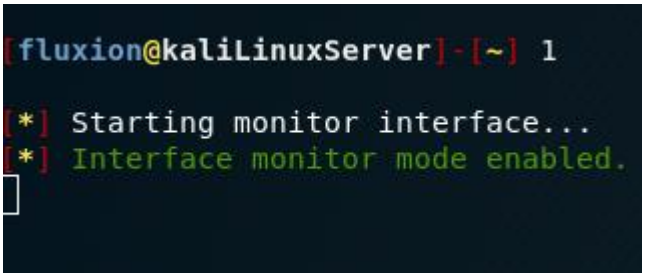


Slika 12: Početni izbornik programa Fluxion za odabir jezika

U sljedećem koraku nudi nam se izbornik za odabir bežičnog sučelja koje ćemo koristiti. Odabiremo onaj koji smo prethodno stavili u monitor način rada.

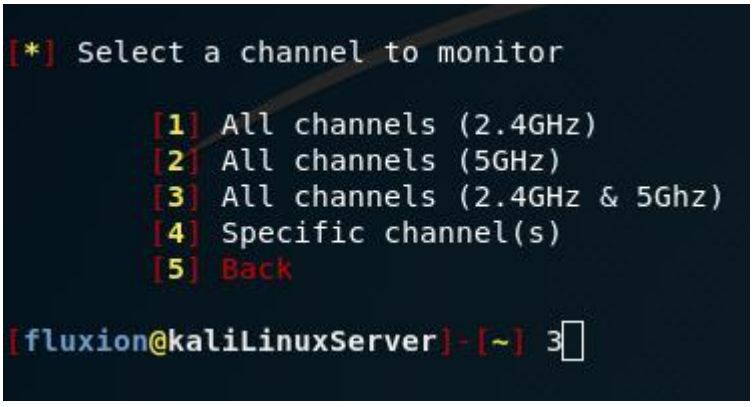
Slika 13: Izbornik programa Fluxion za odabir bežičnog sučelja

Odabirom željenog sučelja program javlja poruku ukoliko je sve u redu, odnosno da li je to sučelje ispravno postavljeno u monitor način rada kako bi se moglo nastaviti s napadom.



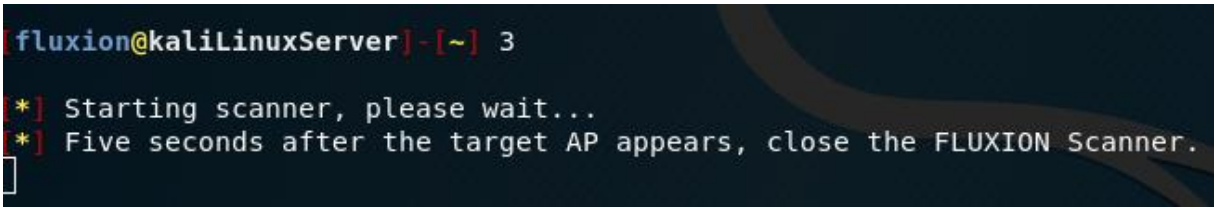
Slika 14: Poruka programa Fluxion kako je odabrano sučelje ispravno i spremno za nastavak napada

Odabir kanala na kojem će se prisluškivati promet. Mi odabiremo sve kanale u rasponu frekvencija od 2,4GHz do 5GHz.



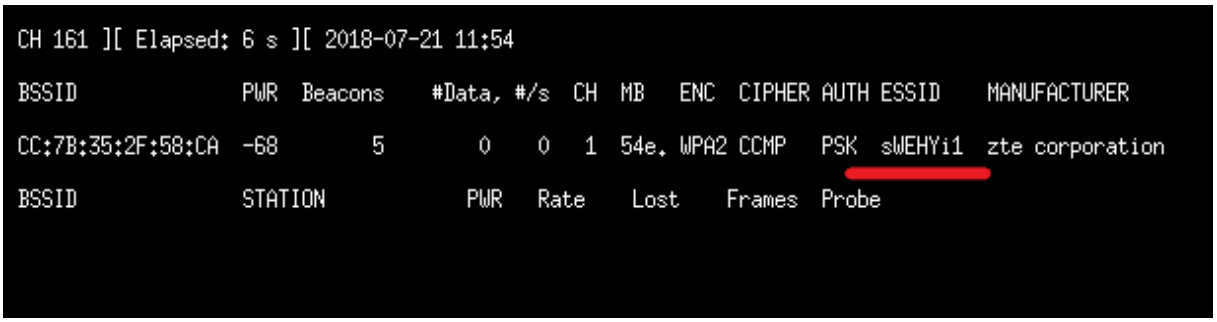
Slika 15: Izbornik programa Fluxion koji će se kanali prisluškivati

Zatim se pokreće prisluškivanje prometa, kojih sve bežičnih mreža ima u krugu od zlonamjernog računala. Kada se ugleda ciljana žrtva, odnosno njena bežična mreža, kombinacijom tipki *CTRL+C* se zaustavlja skeniranje.



Slika 16: Pokretanje skenera za traženje bežičnih mreža u okolini

Kada smo ugledali ciljanu mrežu, testna bežična mreža naziva *sWEHYi1*, zaustavljamo skeniranje i nastavljamo s izvođenjem napada.



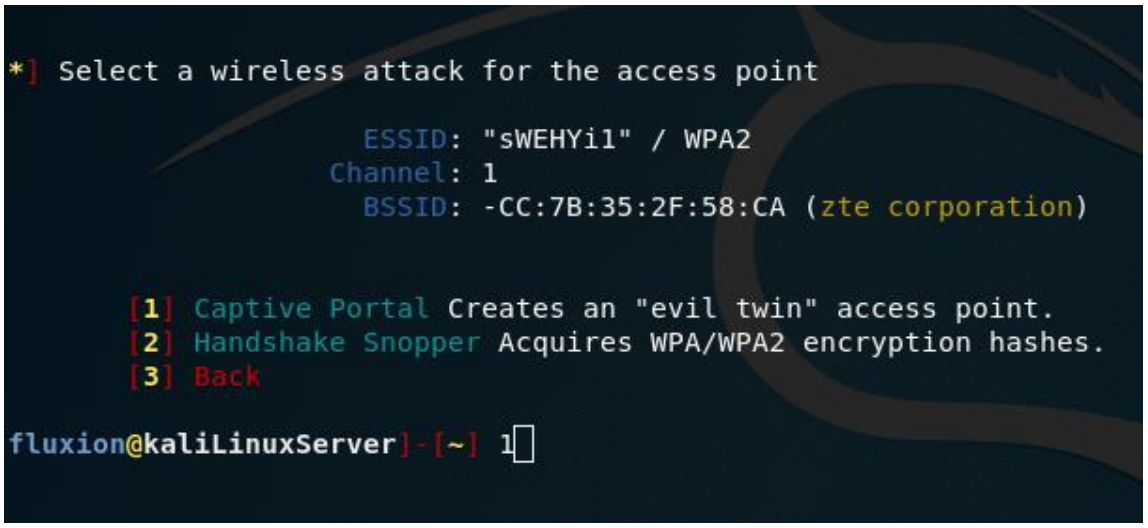
Slika 17: Pronađena je ciljana mreža te se zaustavlja skeniranje

Zatim nam program nudi popis svih mreža koje je uspio uhvatiti, a mi odabiremo našu žrtvu.

Slika 18: Popis mreža koje je program Fluxion uspio skenirati

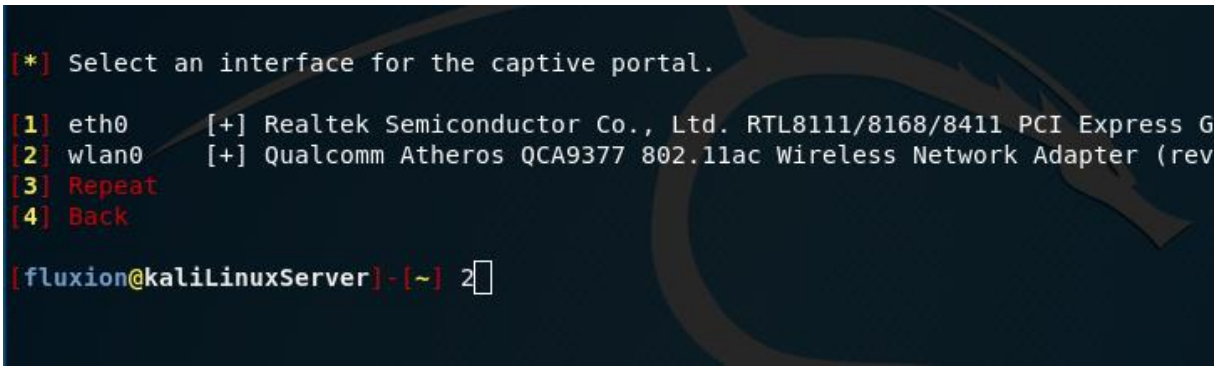
Budući da smo handshake uhvatili na način opisan u prethodnom poglavlju, taj dio napada preskačemo i idemo direktno na *Captive Portal* napad.

Captive Portal predstavlja prozore koji se pojavljuju kada se želimo priključiti na nekakvu javnu pristupnu točku. To može biti „Uvjeti korištenja“ prozor gdje moramo kliknuti da pristajemo na to ili ne, ukoliko pristupamo knjižničnoj pristupnoj točki može nam se pojaviti *Captive Portal* prozor za unos knjižničnog korisničkog računa, a ponekad se čak mora pogledati nekakav kratki video prije nego dobijemo pristup internetu. Sve navedeno se naziva *Captive Portal* prozori. *Captive Portali* su krivci za niz sigurnosnih problema, posebno kada je riječ o *https* web-stranicama. *Https* ima za cilj spriječiti presretanje prometa, izmjenu i lažno predstavljanje treće strane. A *Captive Portali* upravo funkcioniraju na taj način, presreću i mijenjaju vezu između korisnika i web-stranice koju se pokušava posjetiti. Pristupom nekim stranicama osiguranim *https* protokolom, web preglednik će izbaciti upozorenje o nepouzdanoj vezi te lažnim certifikatima za tu stranicu. No, upravo takva neobjašnjiva upozorenja za stranice koje su do tada bile sigurne, mogu uzrokovati da korisnik izignorira upozorenje o sigurnosti. [38]



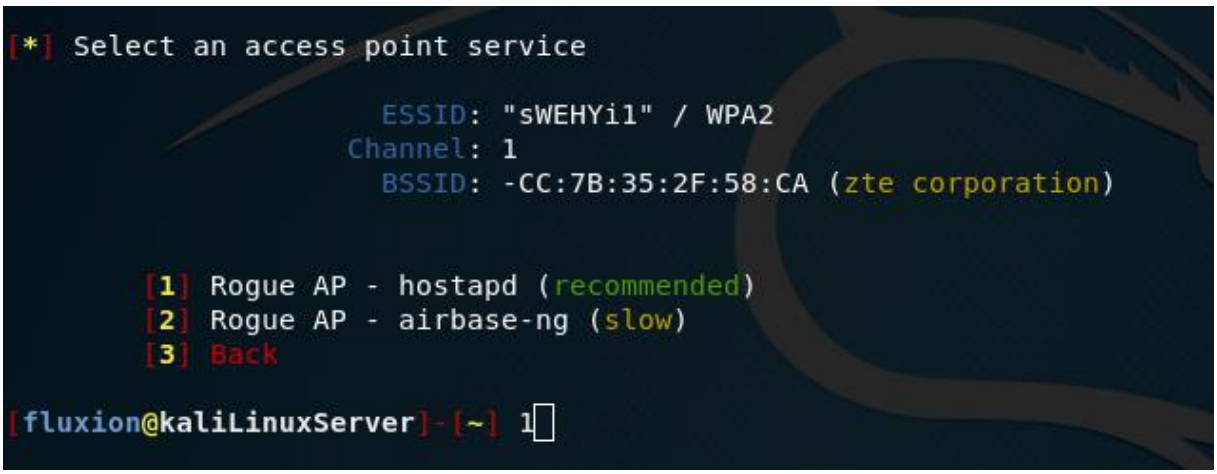
Slika 19: Izbornik programa Fluxion za odabir Captive Portal napada ili Handshake Snopper napada

Odabiremo bežično sučelje za provedbu napada, mi odabiremo *wlan0* sučelje koje je u monitor načinu rada.



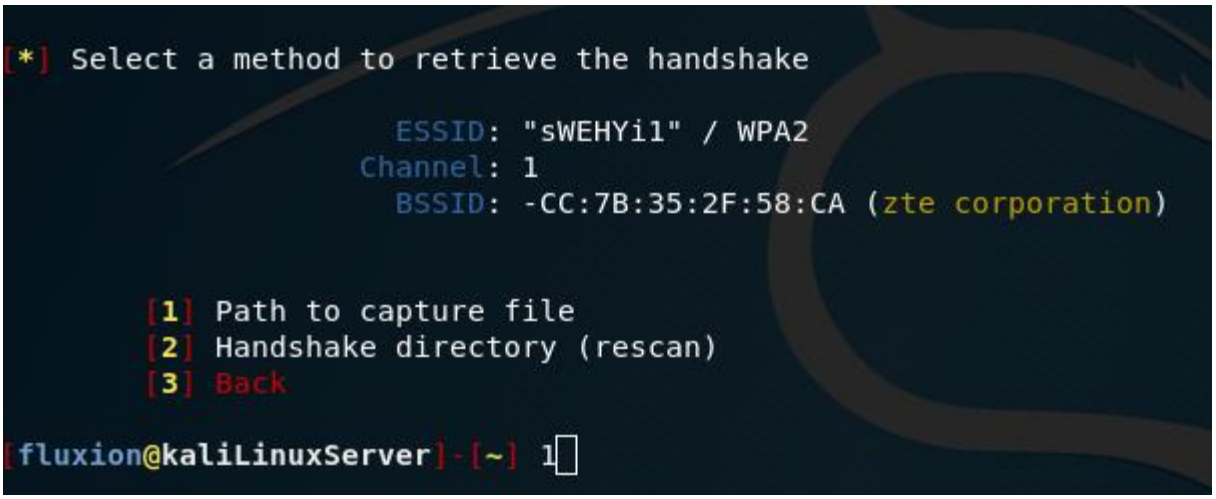
Slika 20: Odabir sučelja za provedbu Captive Portal napada

Sljedeći korak nam je odabir načina na koji će se stvoriti lažna pristupna točka, odabiremo prvi, preporučeni način. Riječ je o *hostapd* načinu. *Hostapd* je vrsta *deamon* programa koji je pokrenut u prostoru memorije namijenjenoj korisničkim aplikacijama (eng. *user space*), a služi za stvaranje bežične pristupne točke i autentifikacijske poslužitelja. *Deamon* program je vrsta programa kojem je svrha raditi u pozadini, obavljati nekakav zadatak, bez interakcije korisnika.



Slika 21: Odabir hostapd načina stvaranja lažne pristupne točke

Budući da je handshake uhvaćen, odabiremo unos putanje do *.cap* datoteke u kojoj je spremljen.



Slika 22: Izbornik za hvatanje handshake-a ili upis putanje do već uhvaćenog

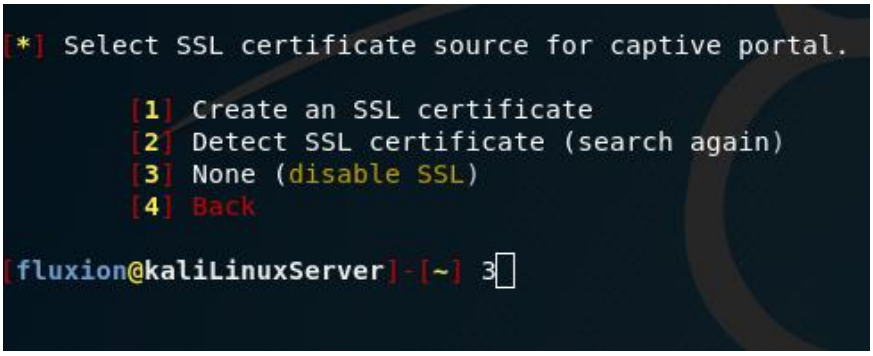
Unosimo putanju gdje smo prethodno spremili *.cap* datoteku sa uhvaćenim handshake-om.

Slika 23: Unos putanje do .cap datoteke u kojoj je spremljen handshake

Budući da smo handshake uhvatili koristeći se *aircrack-ng* skupinom alata odabiremo i *aircrack-ng* metodu za verifikaciju handshake-a.

Slika 24: Izbornik programa Fluxion gdje biramo metodu verifikacije uhvaćenog handshake-a

Zatim odabiremo SSL certifikat za Captive Portal napad. Mi odabiremo da nema SSL certifikata. SSL (eng. *Secure Sockets Layer*) je transportni TCP/IP protokol za održavanje sigurne komunikacije na internetu između klijenta i poslužitelja. Koristi algoritme za enkripciju kako bi svi razmijenjeni podaci ostali nečitljivi napadaču. SSL certifikat je dio programskog koda koji se instalira na poslužitelju te omogućuje sigurnost komunikacije u skladu sa SSL protokolom. Za prepoznavanje sigurne web-stranice, odnosno da li je zaštićena SSL certifikatom, prepoznat ćemo po njenom URL, koji će započeti sa *https://*. [39]



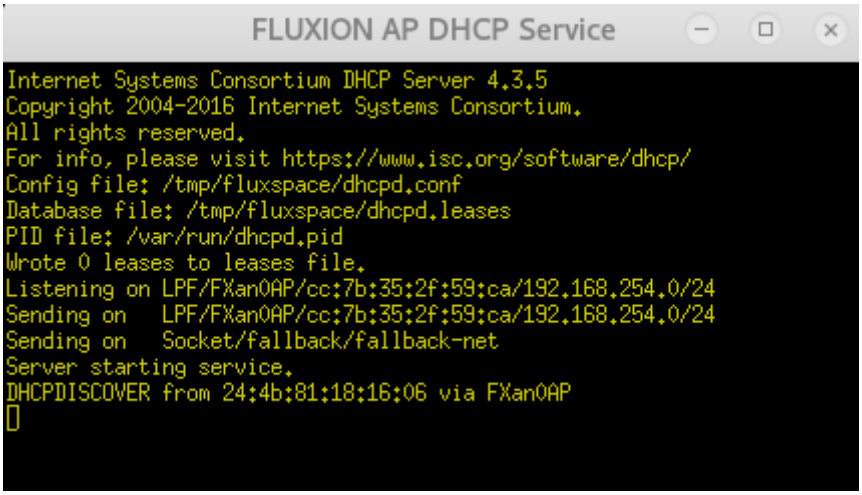
Slika 25: Izbornik programa Fluxion za izbor SSL certifikata

Odabiremo *emulated* za vrstu internet povezivanja. Riječ je o načinu ponašanja upravo kao i ciljana mreža, djelotvorno potpuna replikacija druge mreže.

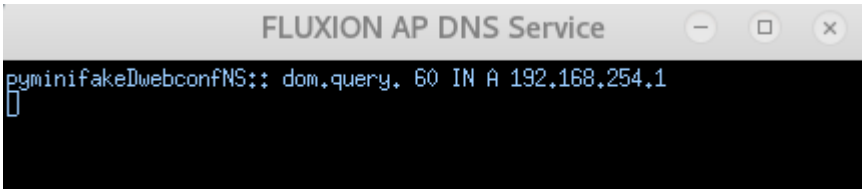
Slika 26: Izbornik programa Fluxion za odabir tipa povezivanja na internet za lažnu pristupnu točku

Zatim nam se nudi izbornik za odabir jezika za *Captive Portal*. Odabrati ćemo engleski jezik, te se time aktivira napad.

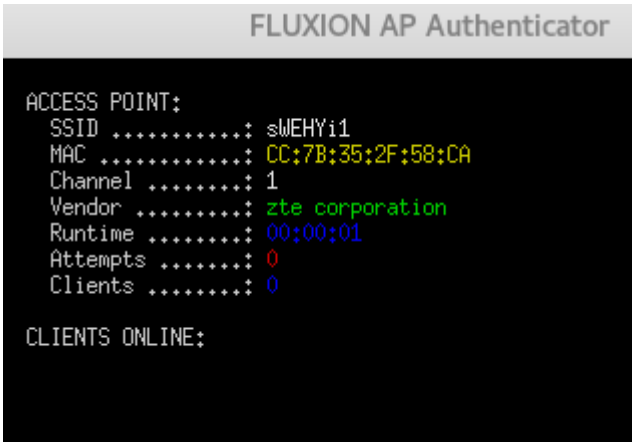
Pokretanjem napada otvaraju se sljedeći prozori koji prikazuju različite informacije o novostvorenoj pristupnoj točki:



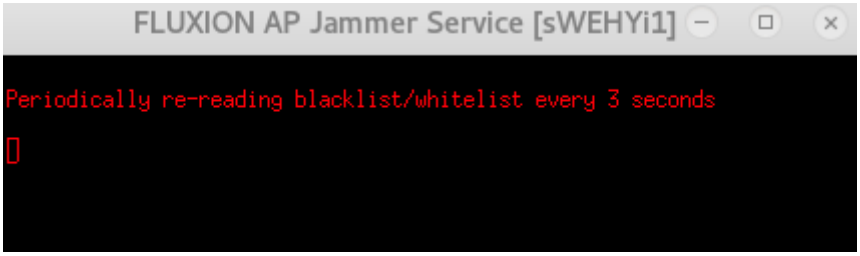
Slika 27: Prozor za DHCP zahtjeve



Slika 28: Prozor za DNS zahtjeve

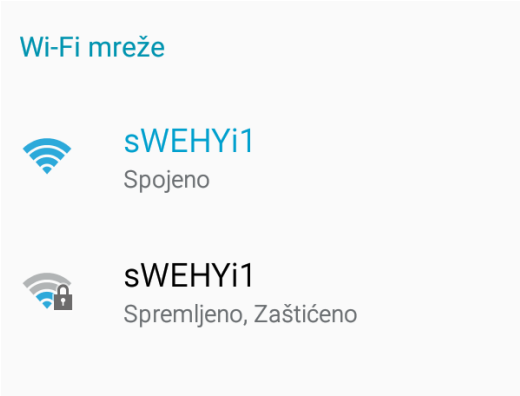


Slika 29: Prozor za izvješće o statusu



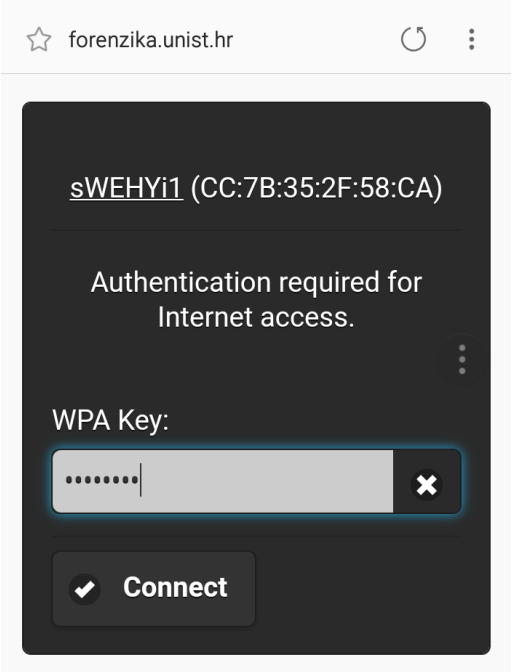
Slika 30: Prozor deautentifikacije korisnika sa originalne pristupne točke

Sljedeće slike prikazuju što se odvija na žrtvinom uređaju, u ovom slučaju riječ je o pametnom telefonu koji je već bio spojen na *sWEHYi1* mrežu. Prva slika prikazuje Wi-Fi postavke mobilnog uređaja. Žrtva to ne primjećuje, nema nikakvih naznaka da je odspojena sa originalne pristupne točke i spojena na lažnu. Sve dok sama žrtva ne uđe u Wi-Fi postavke ne primjećuje promjene. Vidimo da nam je žrtva spojena na lažnu pristupnu točku koja se identično zove, ali vidimo i da je takva pristupna točka otvorenog tipa, dok je žrtva odspojena sa svoje originalne pristupne točke.



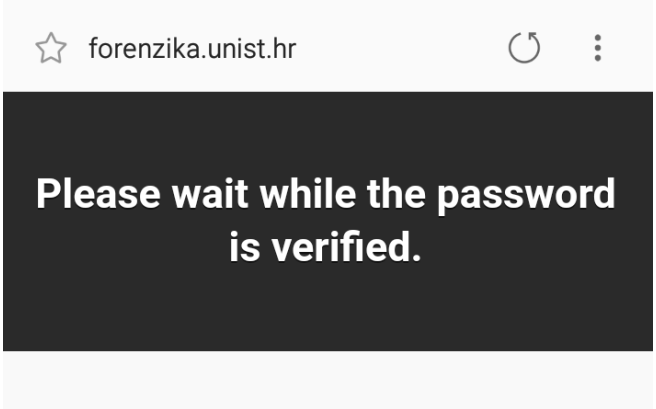
Slika 31: Prikaz Wi-Fi postavki na žrtvinom uređaju

Kada žrtva uđe u internet preglednik, npr. ovdje vidimo prikaz ulaska na web-stranice Odjela za forenzične znanosti, pokaže se prozor kao na sljedećoj slici. Osoba koja nema tehnološkog znanja i koja ne posumnja u ovo, upisuje lozinku.



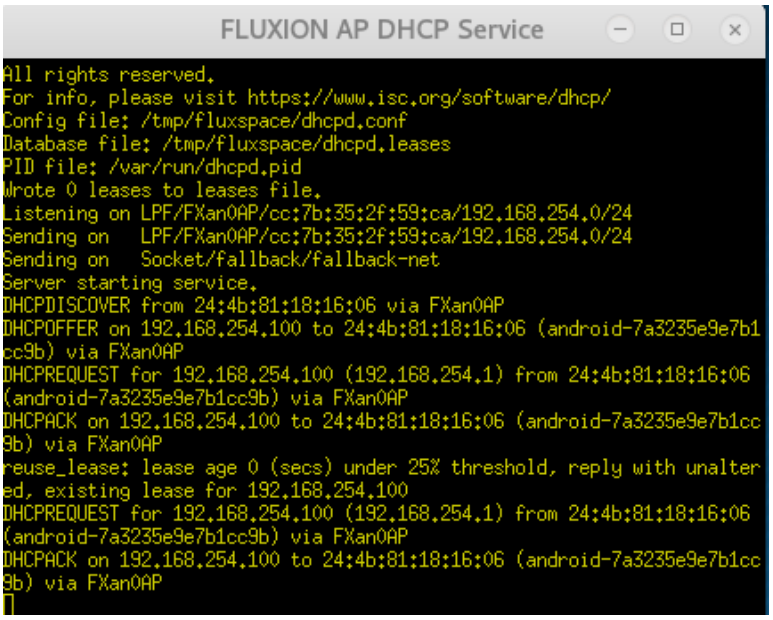
Slika 32: Prikaz Captive Portala na internet pregledniku žrtvinog uređaja

Žrtvi se nakon što utipka lozinku pojavljuje sljedeći prozor koji nastavlja s radom, čim se na napadačevom uređaju prekine izvršavanje napada.

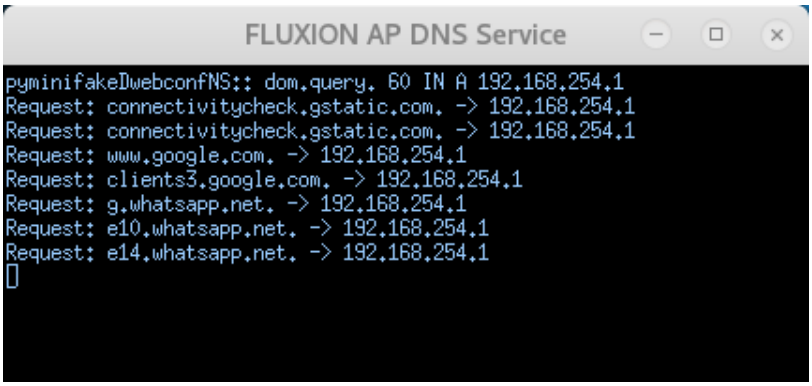


Slika 33: Prikaz na žrtvinom uređaju nakon što unese točnu lozinku

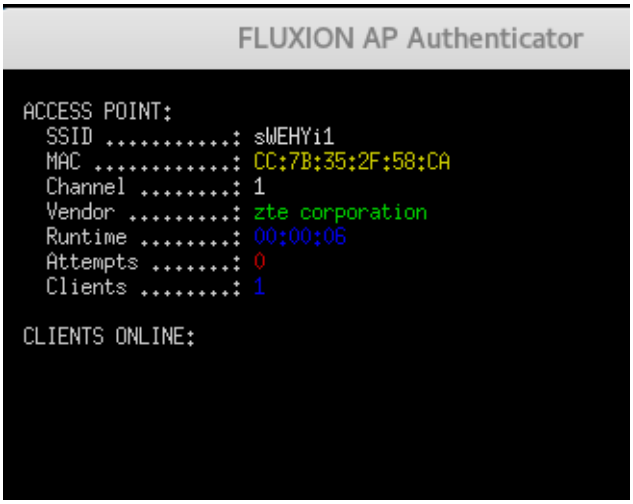
A na napadačevom računalu se događa sljedeće:



Slika 34: Prozor za DHCP zahtjeve nakon što se žrtva spojila na lažnu pristupnu točku

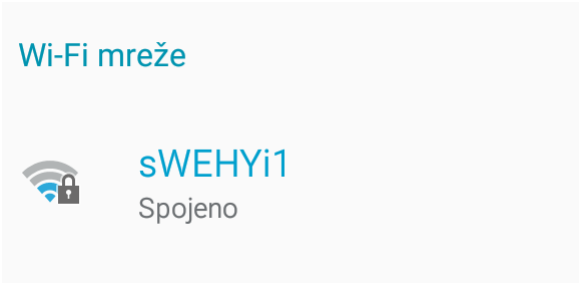


Slika 35: Prikaz prozora DNS zahtjeva nakon što se žrtva spojila na lažnu pristupnu točku

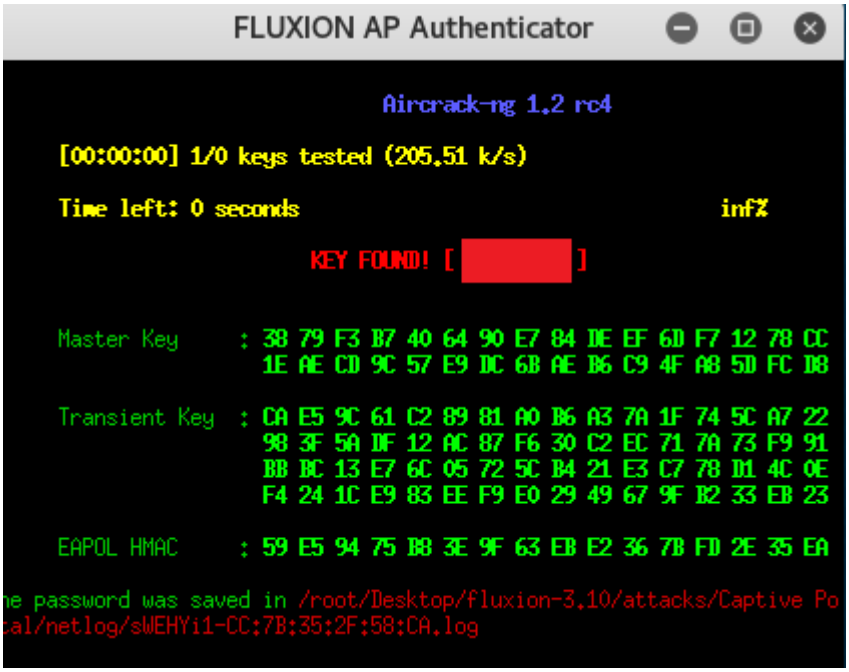


Slika 36: Prozor za izvješće o statusu

Nakon što je napad proveden, žrtva je ponovno automatski spojena na originalnu pristupnu točku, a napadaču se pokaže uhvaćena lozinka.



Slika 37: Nakon provedenog napada lažna pristupna točka je nestala, te je žrtva ponovno vraćena na originalnu



Slika 38: Program nam javlja da je lozinka uspješno uhvaćena

Napad je gotov, program sam sve zatvori.

Slika 39: Nakon završenog napada program sve pokrenute procese zaustavlja i gasi

4.2. PROBLEM LAŽNIH PRISTUPNIH TOČKI

Dvije su glavne vrste mreža, bežična kada su računala spojena bez fizičke veze, te žična kada su računala fizički povezana mrežnim kabelima. Da bi se više računala bežično povezalo u mrežu potreban je dodatni uređaj koji će vršiti usmjeravanje komunikacije među računalima, a to je pristupna točka (eng. Access Point) . Bežična mreža je mnogo više ranjivija u usporedbi sa žičnom, te se mogu provesti i aktivni i pasivni napadi. Pasivni napadi su takva vrsta napada koji ne utječu na ponašanje mreže, već jednostavno njuškaju po mreži i mogu dovesti do aktivnih napada. Aktivni napadi utječu na normalno ponašanje mreže, a najpoznatiji su man-in-the-middle napad i denial-of-service napad. Lažna pristupna točna je savršena za provedbu napada socijalnog inženjeringa. Riječ je o uređaju sa istim standardima koji koriste normalna računala i uređaji, te se legitimni korisnik poveže na lažnu pristupnu točku budući da ne zna razliku između legitimne i lažne. Napadači ovakvim napadom ne moraju gubiti vrijeme na probijanje lozinke, žrtva je već autentificirana na mreži i aktivna, stoga napadač samo može slušati promet bez znanja žrtve o tom. Lažne pristupne točke mogu biti raspoređene svugdje, od kolodvora, bolnica, fakulteta. Kada su takve točke nezaštićene s lozinkom, veliki broj ljudi će se pokušati spojiti upravo na njih. [40]

Ovakav tip napada iskorištava ljudsku želju za besplatnim pristupom internetu. Softver potreban za provedbu je dostupan besplatno na internetu, a mnogo podataka prolazi kroz bežične mreže u obliku nekriptiranih tekstualnih nizova. [41]

4.2.1. WiFi-Pumpkin

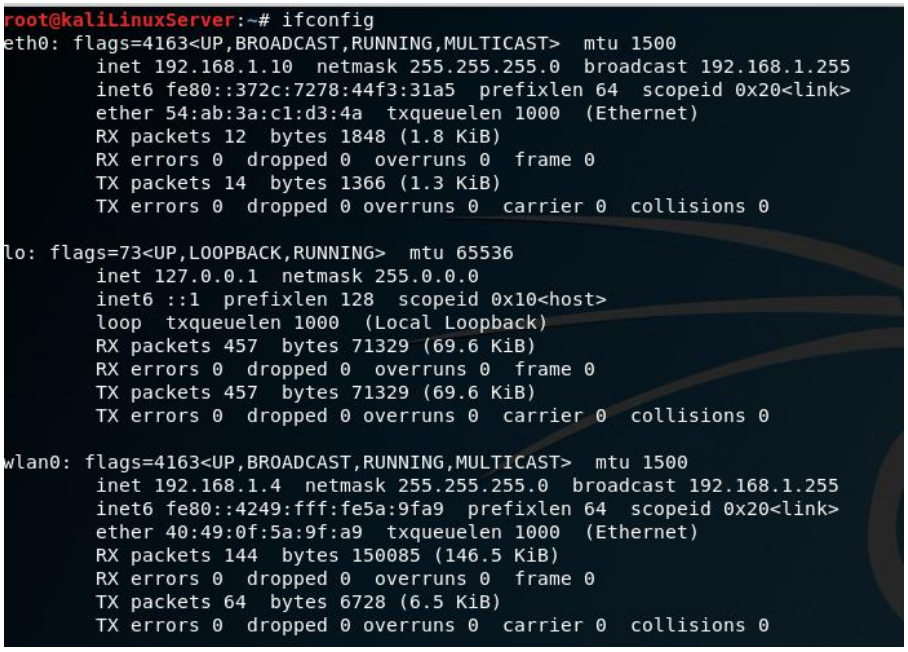
WiFi-Pumpkin je alat za stvaranje lažne pristupne točke, prosljeđujući legitiman promet za i od žrtve. Pruža uslugu bežičnog spajanja na internet, ali prisluškuje promet svih spojenih na lažnu pristupnu točku. Riječ je o vrlo kompletnom okviru za pregled Wi-Fi sigurnosti, a popis značajki je velik: od stvaranja lažne pristupne točke, deautentifikacijskih napada na klijentove pristupne točke, napadi Windows ažuriranjem, hvatanje slika u prometu i dr. [42]

4.2.2. Provođenje napada korištenjem programa WiFi-Pumpkin

Za uspješno korištenje programa potrebna su nam dva bežična sučelja. Jedno ćemo koristiti za stvaranje lažne pristupne točke, a drugo će biti spojeno na internet i koristit će nam za pružanje internet usluge lažnoj pristupnoj točki.

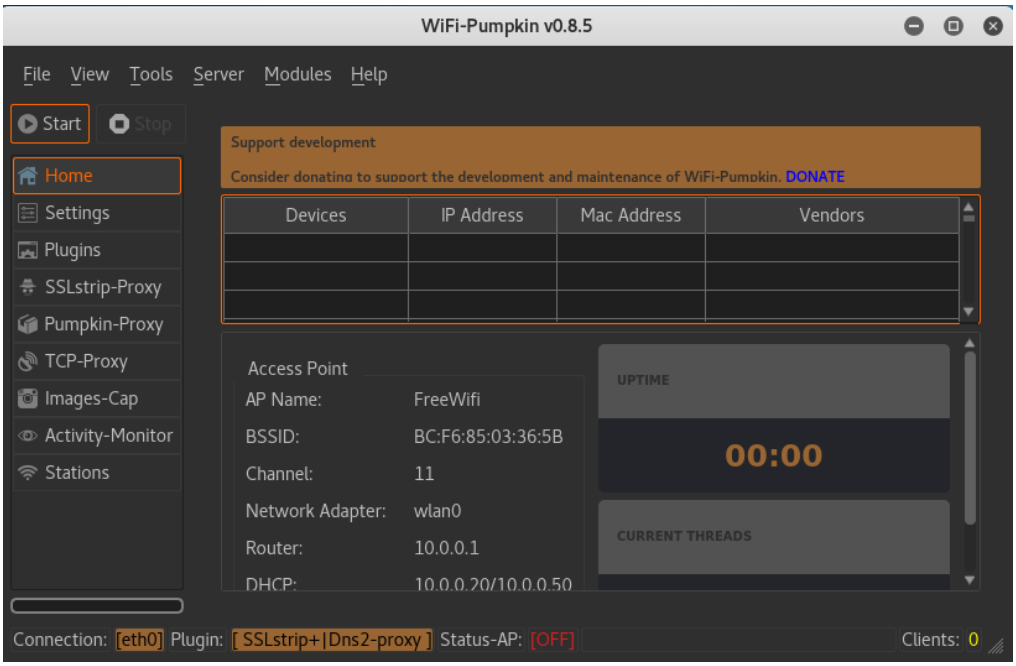
Korištenjem naredbe „ifconfig“ možemo vidjeti aktivne konfiguracije mrežnih sučelja određenog sustava. *eth0* je Ethernet sučelje. *lo* je specijalno mrežno sučelje koje sustav koristi za komunikaciju sa samim sobom. *wlan0* je bežično sučelje.

Za potrebe provođenja napada koristimo *eth0* sučelje koje će nam služiti za spajanje na internet, te bežično *wlan0* sučelje koje će nam služiti za lažnu pristupnu točku.



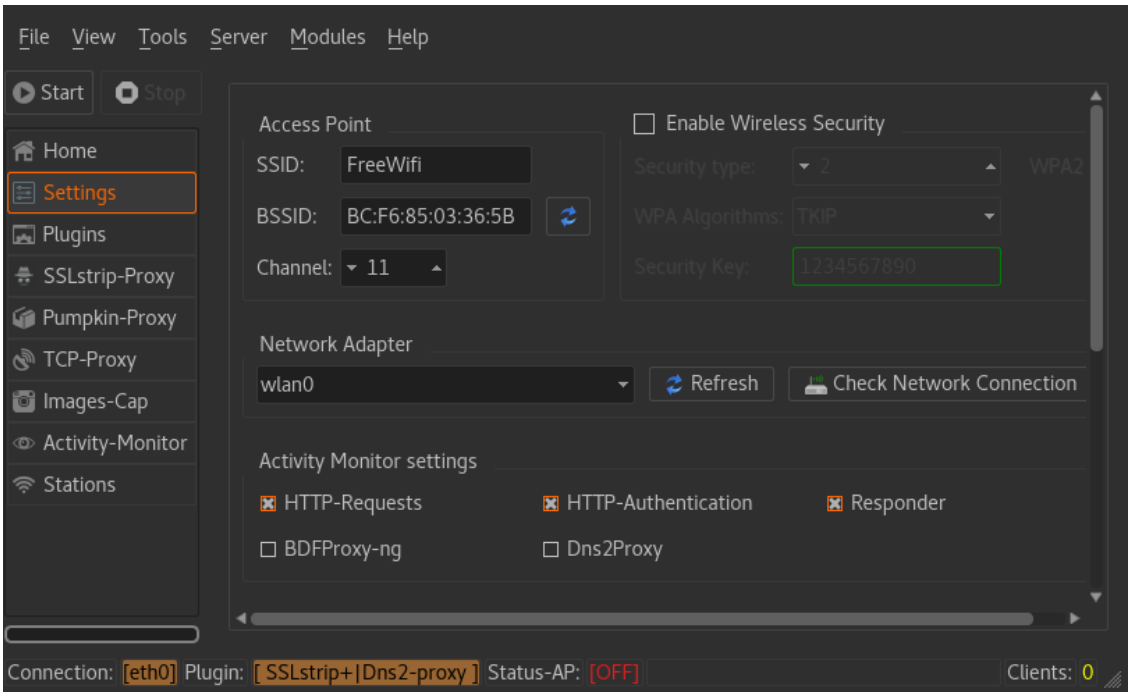
Slika 40: Prikaz aktivnih mrežnih sučelja u sustavu

Nakon upisa naredbe za pokretanje programa u terminalu, otvara nam se GUI sučelje, što je i jedna od značajki programa. Grafičko korisničko sučelje (eng. *Graphical user interface*) koristi prednosti računalne grafike kako bi rad na računalu i korištenje programa bilo jednostavnije i lakše. Na slici ispod vidimo kako izgleda početni zaslon odmah nakon pokretanja programa.



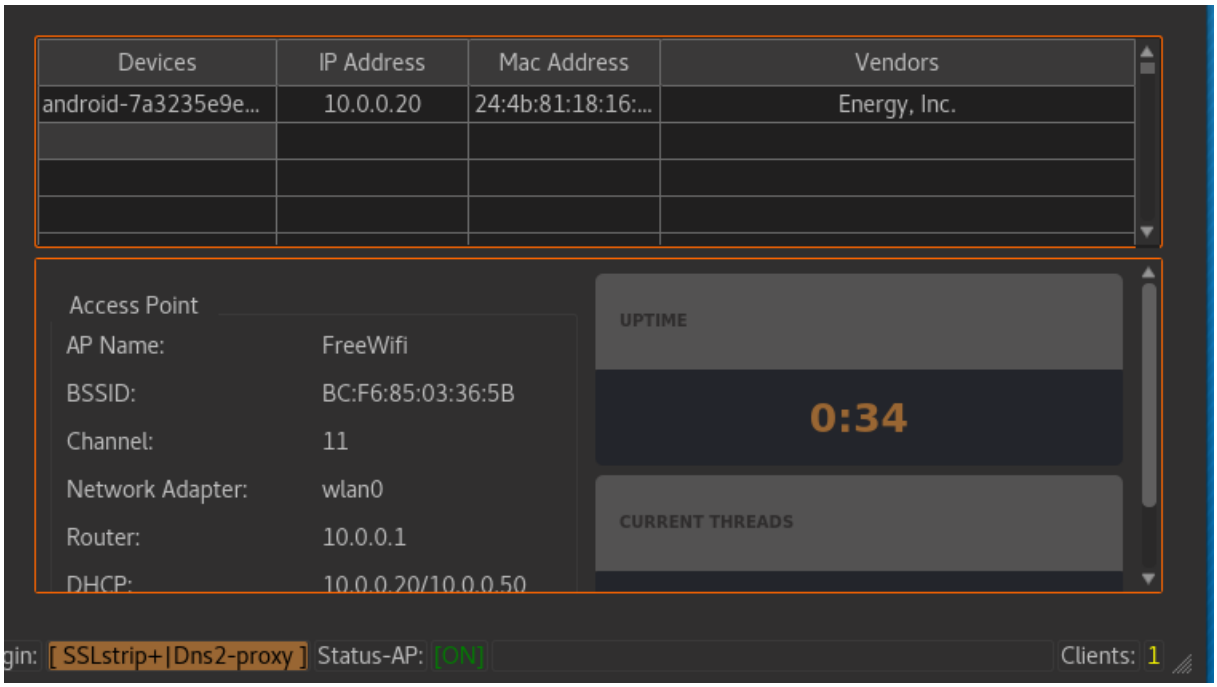
Slika 41: Početni zaslon programa WiFi-Pumpkin

Kada odemo u odjeljak za postavke vidimo da možemo mijenjati i postavljati različite značajke lažne pristupne točke. Postavili smo njezin naziv u „FreeWifi“, te smo isključili značajku za postavljanje lozinke na tu mrežu, odnosno naša mreža je otvorenog tipa. Možemo vidjeti i da je već postavljeno *eth0* sučelje za povezivanje na internet, te *wlan0* sučelje za stvaranje lažne pristupne točke.



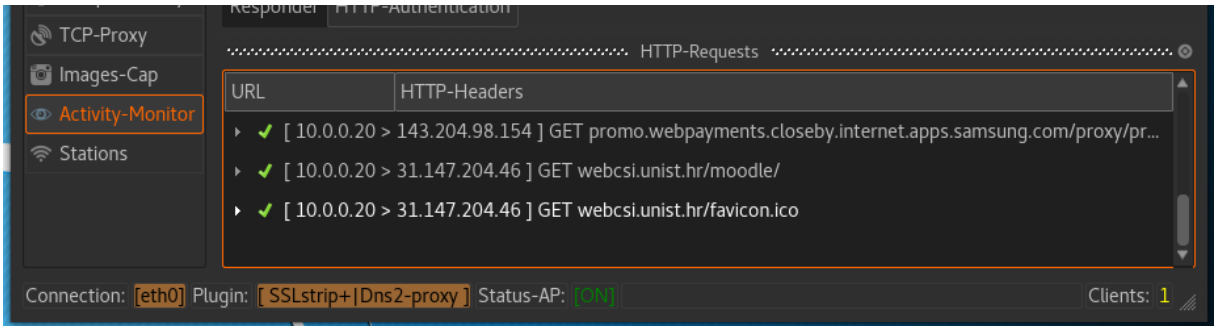
Slika 42: Prikaz osnovnih postavki

Klikom na Start pokrenuli smo našu pristupnu točku. Na početnom zaslonu možemo stalno vidjeti status pristupne točke, koliko je vremenski aktivna i dr. Kada se netko spoji na našu lažnu pristupnu točku, u donjem kutu početnog zaslona vidimo prikaz broja spojenih klijenata, a u tablici možemo vidjeti i o kojem je uređaju riječ, njihove IP i MAC adrese.



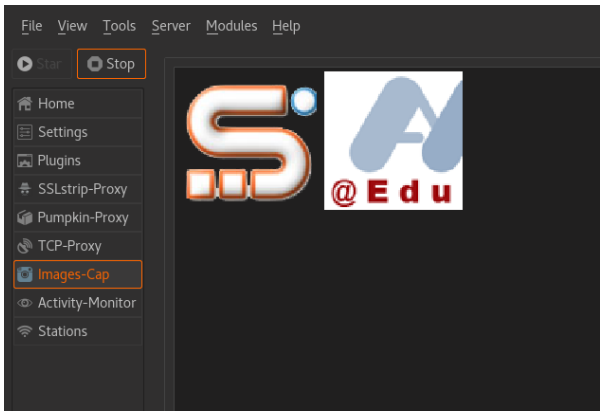
Slika 43: Prikaz podataka o spojenoj žrtvi

U odjeljku Activity-Monitor možemo pratiti na koja se sve web mjesta spaja žrtva.



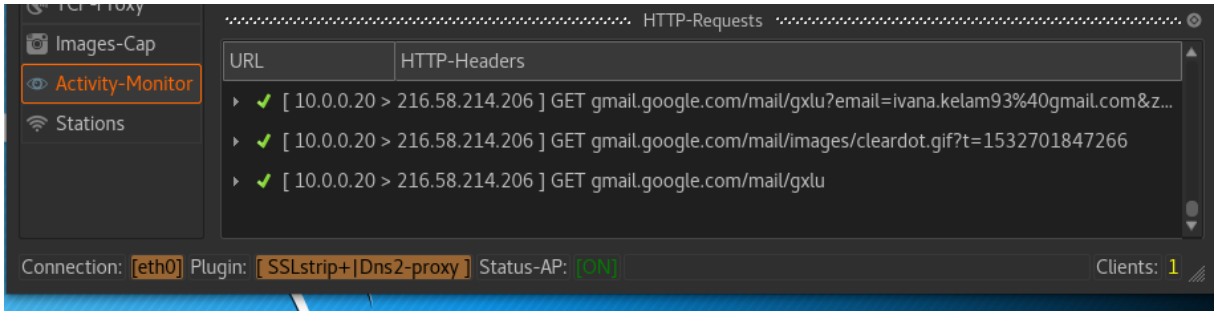
Slika 44: Prikaz Activity-Monitor odjeljka

Također, u odjeljku Images-Cap možemo vidjeti koje je slike program uspio uhvatiti sa web-stranica na koje se žrtva spajala.



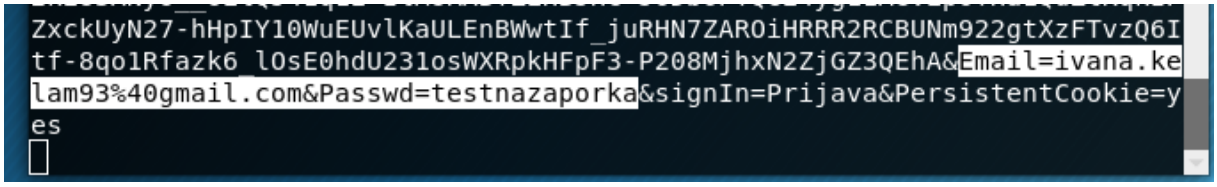
Slika 45: Prikaz Images-Cap odjeljka

U Activity-Monitor odjeljku vidimo da je žrtva pristupila Gmail stranici te koju je email adresu koristila za prijavu.



Slika 46: Vidimo da je žrtva posjetila Gmail stranicu

U terminalu se prikazuju svi podaci o tome koje stranice žrtva posjećuje, koja korisnička imena i lozinke koristi. Kada smo u Activity-Monitor odjeljku vidjeli da se žrtva spaja na Gmail uslugu, u terminalu potražimo je li uhvaćena i lozinka. Na slici ispod vidimo u moru podataka i uhvaćeno korisničko ime i lozinku.



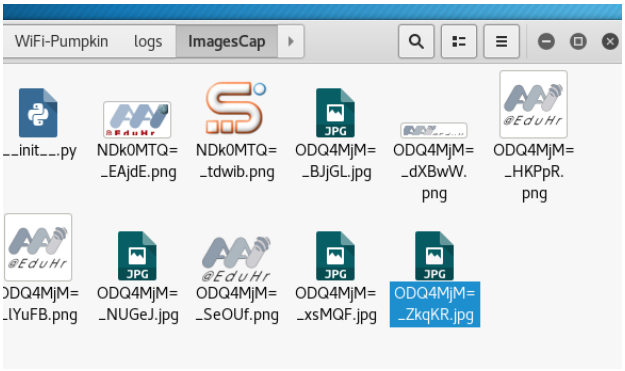
Slika 47: Uhvaćena lozinka i email

Po završetku izvršavanja programa u *url.log* datoteci možemo pronaći popis svih web mjesta koje je žrtva posjetila, izlistano redoslijedom po datumu i vremenu pristupanja.

```
2018-07-27 16:29:31,710 : [ 10.0.0.20 > 31.147.204.103 ] GET forenzika.unist.hr/
2018-07-27 16:29:32,694 : [ 10.0.0.20 > 31.147.204.103 ] GET forenzika.unist.hr/
2018-07-27 16:29:34,715 : [ 10.0.0.20 > 143.204.98.154 ] GET promo.webpayments.closeby.internet.apps.samsung.com/proxy/
2018-07-27 16:30:03,224 : [ 10.0.0.20 > 31.147.204.46 ] GET webcsi.unist.hr/moodle/
2018-07-27 16:30:03,504 : [ 10.0.0.20 > 31.147.204.46 ] GET webcsi.unist.hr/favicon.ico
2018-07-27 16:30:16,673 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/
2018-07-27 16:30:16,937 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/
2018-07-27 16:30:16,986 : [ 10.0.0.20 > 143.204.98.76 ] GET promo.webpayments.closeby.internet.apps.samsung.com/proxy/p
2018-07-27 16:30:17,059 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/
2018-07-27 16:30:17,493 : [ 10.0.0.20 > 216.58.214.205 ] GET cuentas.google.com/ServiceLogin?service=mail&passive=true&
cobx&nui=5&btmpl=mobile&emr=1&osid=1
2018-07-27 16:30:17,649 : [ 10.0.0.20 > 216.58.214.205 ] GET cuentas.google.com/ServiceLogin?
e=true&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&ss=1&scc=1&ltmpl=ecobx&nui=5&btmpl=mobile&emr=1&osid=1
2018-07-27 16:30:18,798 : [ 10.0.0.20 > 216.58.214.195 ] GET webssl.gstatic.com/accounts/ui/avatar_2x.png
2018-07-27 16:30:18,802 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/images/cleardot.gif?t=1532701819172
2018-07-27 16:30:25,831 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/gxlu?email=ivana.kelam93%40gmail.com
2018-07-27 16:30:25,832 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/images/cleardot.gif?t=1532701826381
2018-07-27 16:30:26,569 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/gxlu?email=ivana.kelam93%40gmail.com
2018-07-27 16:30:26,625 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/gxlu
2018-07-27 16:30:34,294 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/gxlu?email=ivana.kelam93%40gmail.com
2018-07-27 16:30:34,300 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/images/cleardot.gif?t=1532701834845
2018-07-27 16:30:35,108 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/gxlu
2018-07-27 16:30:39,876 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/gxlu?email=ivana.kelam93%40gmail.com
2018-07-27 16:30:46,714 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/gxlu?email=ivana.kelam93%40gmail.com
2018-07-27 16:30:46,727 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/images/cleardot.gif?t=1532701847266
2018-07-27 16:30:47.601 : [ 10.0.0.20 > 216.58.214.206 ] GET gmail.google.com/mail/gxlu
```

Slika 48: Prikaz url.log datoteke

Također, u ImagesCap mapi spremljene su sve slike koje je program uspio uhvatiti prilikom spajanja žrtve na različita web mjesta.



Slika 49: Prikaz ImagesCap mape

4.3. PROBLEM DRUŠTVENIH MREŽA

Postoji rastuća povezanost između društvenih mreža i socijalnog inženjeringa, zbog obilja osobnih i poslovnih informacija koje se nalaze na tim društvenim mrežama. Različiti su problemi koje su organizacije iskusile vezano uz društvene mreže: zaposlenici koji dijele previše informacija, kako privatnih tako i poslovnih, gubitak povjerljivih informacija, te veća izloženost spornim situacijama. Tu su još naravno i gubitak u smislu smanjene produktivnosti zaposlenika te povećan rizik izlaganja virusu ili malicioznom softveru. [43]

Najčešće zapažene ugroze organizacija možemo podijeliti u tri grupe:

- reputacijske,
    - najteži izazov je sačuvati reputaciju organizacije. Ona može biti narušena ukoliko se organizacija prikaže kao nesposobna, npr. ukoliko je preko društvene mreže napadač proširio virus i na korisnike, partnere i ostale koji su u doticaju sa organizacijom. Na društvenim mrežama je najčešći oblik napada da se korisnika navodi da odobri pristup osobnim podacima nekoj aplikaciji ili da se klikne na poveznicu koja sadrži maliciozni softver. Naposljetku, zaposlenici su ključni za održavanje reputacije organizacije, i kao takvi najbolja prilika za napadača.
- pravne,
    - primarni pravni rizici uključuju: privatnost, sigurnost, intelektualno vlasništvo i medijski sadržaj. Bilo koja povreda navedenog koja proizlazi iz društvenih mreža može prisiliti organizaciju da preuzme pravnu odgovornost za nastalu štetu. Napadači se mogu infiltrirati u društvenu mrežu te manipulirati zaposlenicima koji mogu otkriti povjerljive podatke. Napadač može dovesti organizaciju u problem povrede prava intelektualnog vlasništva ukoliko objavi informacije koje pripadaju drugoj organizaciji na društvenoj mreži organizacije žrtve. Osim toga, mogu otkriti poslovne tajne poslovnih partnera organizacije te sve izložiti javno, što će organizaciju dovesti u druge različite pravne probleme.
- operativne
    - korištenje društvenih mreža za poslovnu upotrebu predstavljaju veliki rizik za cijeli sustav organizacije, budući da zaposlenik koji bezazlenim klikom na poveznicu preuzme maliciozni softver ugrožava cijelu organizaciju. [43]

Razvojem društvenih mreža socijalni inženjering je postao još veća opasnost, jer umjesto napada na ciljanu tvrtku ili organizaciju, preko Facebook profila, Twitera i dr., žrtvom mogu postati obični ljudi, a većina ljudi i ima nekakav profil na nekoj društvenoj mreži. Na prvi pogled bezazlena lista prijatelja na društvenoj mreži može dosta toga otkriti o korisniku. Osim toga, postao je trend imati što veću listu prijatelja, iako se većina ljudi zapravo i ne poznaje. Na društvenim mrežama korisnici najčešće pišu što trenutno rade, kada su na putovanju, što planiraju. Objavljuju fotografije koje sadrže i privatne podatke, prikaz članova obitelji, interijera kuće. Sve to olakšalo je napadačima provedbu socijalnog inženjeringa. Napadači se odluče za žrtvu, prate ju preko društvenih mreža, traže potrebne podatke, a čak uz pomoć metapodataka iz samih slika moguće je doći i do točnih koordinata gdje je snimljena, te se iz svega toga može napraviti detaljna skica i plan napada. [44]

4.3.1. Weeman

Za prikaz na koji način napadač može uhvatiti lozinku žrtvine društvene mreže, koristit ćemo program Weeman. Žrtva koja nije tehnološki upućena, neće odmah ili uopće neće primijetiti promjene na stranici društvene mreže na koju se prijavljuje. Hvatanjem lozinke napadač može otkriti osobne informacije o žrtvi.

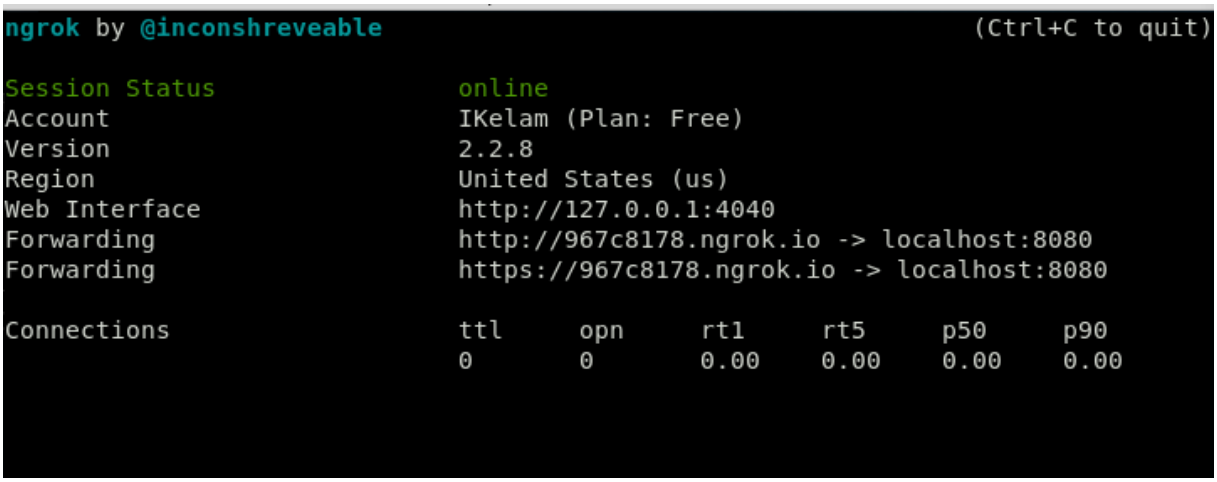
Weeman je jednostavna Phython skripta koja stvara lažne web-stranice identične originalnima.

4.3.2. Provođenje napada korištenjem programa Weeman

Prije pokretanja samog programa u terminalu smo upisali naredbu koju vidimo na sljedećoj slici, a ona nam izlaže web poslužitelja našeg uređaja na port 80 na internet. Port u TCP/IP i UDP mrežama predstavlja krajnju točku logičke veze, a broj porta označuje njegovu vrstu. Tako se broj 80 koristi za HTTP promet. Ngrok je softver koji omogućuje pristup preko interneta Web serveru koji se pokreće na lokalnom računalu.

Slika 50: Naredba za postavljanje porta 80

Kada se Ngrok softver pokrenuo, vidimo stanje, povezanost i ostale informacije.



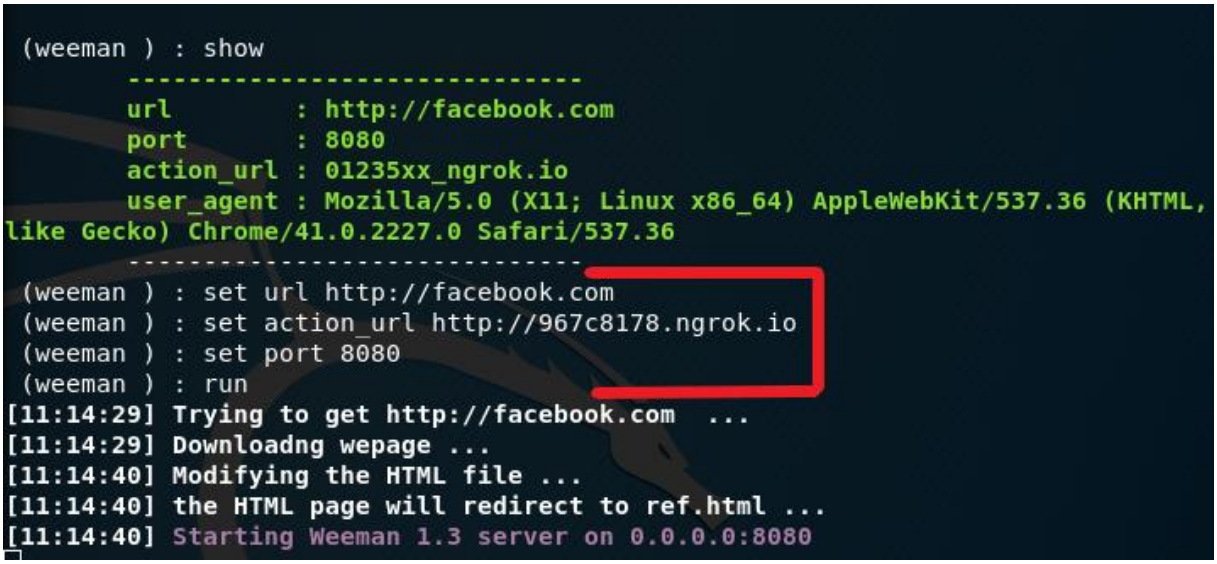
Slika 51: Pokrenut softver Ngrok

Zatim krećemo sa pokretanjem programa Weeman. U terminalu upisujemo naredbu „chmod +x weeman.py“ koja jednostavno znači da navedenu Python skriptu napravi u izvršnu datoteku. Zatim pokrećemo sam program naredbom „python weeman.py“.

Slika 52: Pokretanje Weeman programa

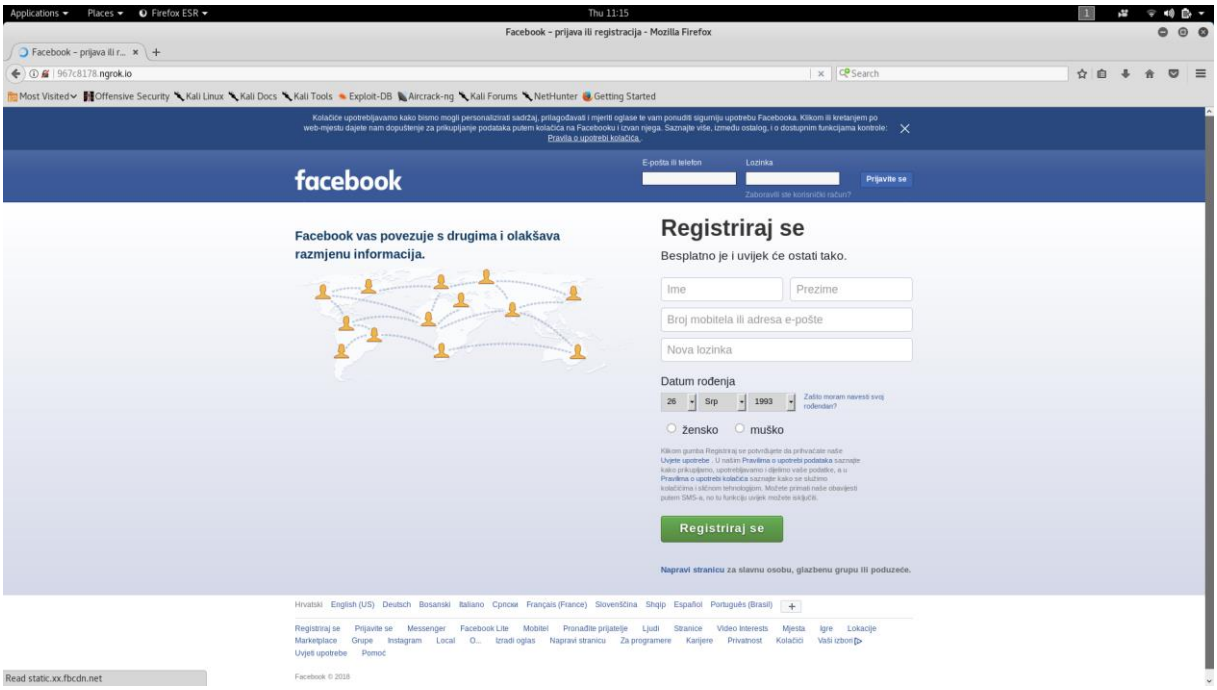
Upisom naredbe „show“ možemo vidjeti koje atribute prima program i kako ih koristiti. Zatim smo započeli sa našim unosom.

- set url http://facebook.com – postavili smo da klonira Facebook društvenu mrežu
- set action_url http://967c8178.ngrok.io – postavili smo da se klonirana stranica pokrene na našem localhostu
- set port 8080 – postavili smo na port 80
- run – pokretanje izvršenja naredbi.



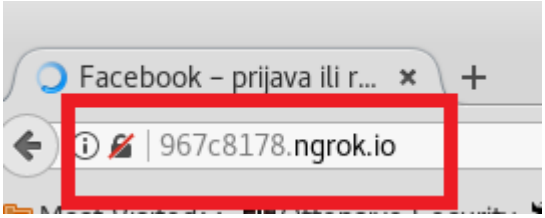
Slika 53: Naredbe za pokretanje napada

Kada je program javio da je sve postavljeno u redu, kliknemo na link *http://967c8178.ngrok.io* i vidimo da nam klonirana stranica izgleda identično kako i originalna. Naravno, promjena se jedino primijeti u gornjem lijevom vrhu stranice, gdje se upisuje URL stranice.



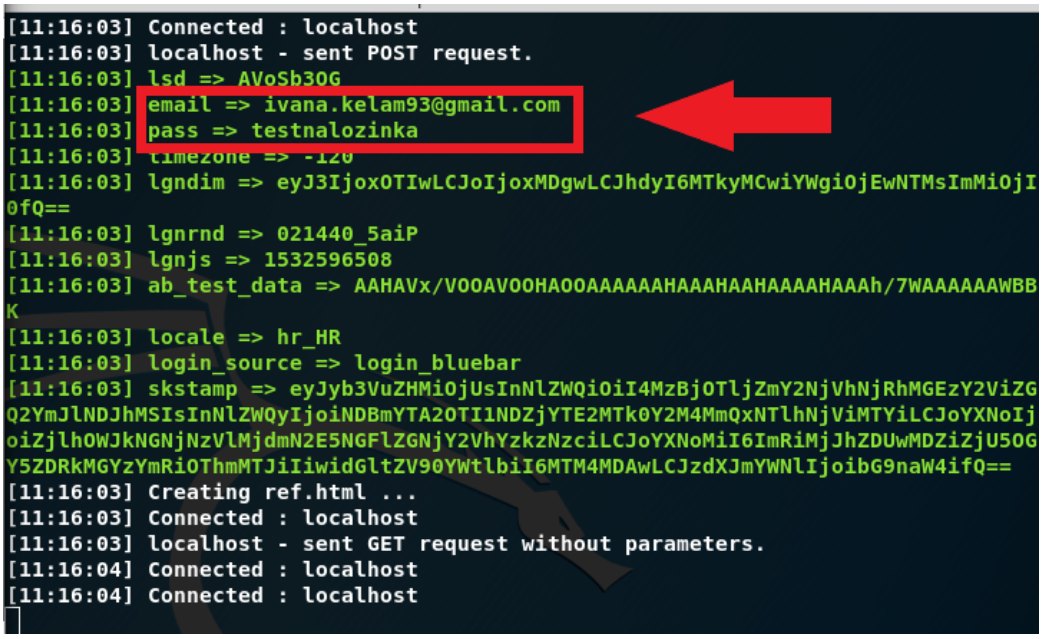
Slika 54: Prikaz kako izgleda klonirana stranica klikom na taj link

Na slici ispod vidimo jedinu promjenu na kloniranoj stranici.



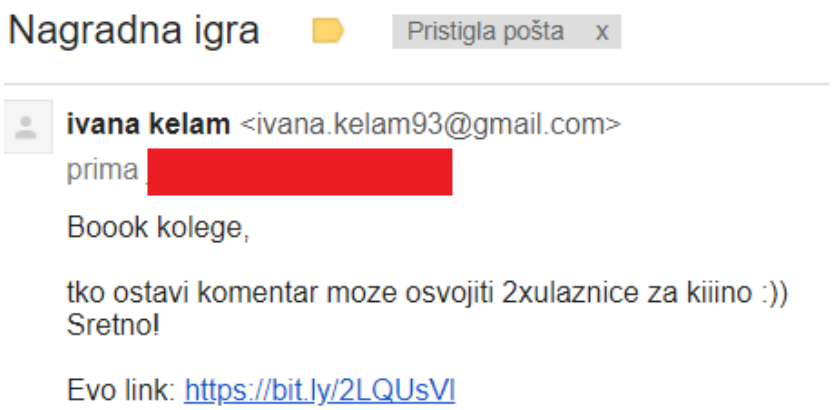
Slika 55: Približeni prikaz URL polja na toj stranici

Nakon unosa korisničkog imena i lozinke na kloniranoj stranici u terminalu nam se pojavljuje sljedeće:



Slika 56: Prikaz u terminalu: uhvaćeno korisničko ime i lozinka

Napadači mogu nasamariti žrtvu na mnogo načina koristeći se ovim programom. Na primjer, napadač ima za cilj nasamariti zaposlenike određene tvrtke. Na neki drugi način uspije saznati emailove zaposlenika, te im svima pošalje email slično kao na slici ispod.



Slika 57: Prikaz na koji način se može zloupotrijebiti

Korištenjem besplatne stranice za smanjivanje URL-a „bitly“ maskirali smo naš zlonamjerni URL da izgleda pristupačnije i manje sumnjivije žrtvi. Ona žrtva koja ne posumnja u ispravnost emaila klikne na poveznicu, prijavi se na lažnoj Facebook stranici, a napadač prikupi korisničko ime i lozinku.

5. ZAKLJUČAK

Napadi socijalnim inženjeringom prisutni su u svim područjima života, ali osobito u području računalne sigurnosti. Napadači ne moraju biti isključivo računalni stručnjaci, to mogu biti različiti prevaranti koji jednostavno psihološkim manipulacijama prevare žrtvu za dobivanje pristupa određenim informacijama. Ljudski faktor je neminovan u računalnom sustavu, ali je isto tako i najtanja karika u sigurnosti tog računalnog sustava. Nema direktnog načina kako se boriti protiv ovakve prijetnje, ali educiranjem ljudi se može podići svijest da je opasnost od socijalnog inženjeringa sveprisutna. Organizacije mogu svoje zaposlenike educirati redovito, provoditi sigurnosnu politiku i sigurnosne procedure. Dok se obične korisnike može educirati putem reklamnih poruka, u školama, primjerima stvarnih napada.

Provedbom kontroliranih napada u ovome radu pokazalo se da je danas prejednostavno doći do malicioznih softvera i alata, pa tako i za provedbu socijalnog inženjeringa. Prvi program kojim smo proveli napad obuhvaća otkrivanje lozinke Wi-Fi mreže, a riječ je o Fluxion programu. Fluxion je alat koji automatizira proces stvaranja lažne pristupne točke blizanca te nasamaruje žrtvu da preda Wi-Fi lozinku. Drugi program je naziva WiFi-Pumpkin, a stvara vlastitu lažnu pristupnu točku, pruža uslugu bežičnog spajanja na internet te prisluškuje promet spojenog korisnika. Treći program stvara lažnu web-stranicu, a tim smo prokazali na koji način napadač može uhvatiti lozinku žrtvine društvene mreže. Koristili smo program Weeman, koji je jednostavna Phython skripta koja stvara lažne web-stranice identične originalnima.

Granice pojedinih vrsta napada su vrlo proširive i još uvijek neistražene do samog kraja. Sve nam to upućuje da je potrebno biti što oprezniji prilikom korištenja interneta, odnosno spajanjem na otvorene Wi-Fi mreže, primitka sumnjivog emaila, paziti na sumnjive poveznice na koje mislimo kliknuti i ostalo.

6. LITERATURA

1. Workman M. Gaining access with social engineering: An empirical study of the threat. Information Systems Security. 2007;16(6):315-31.

2. Socijalni inženjering 2006. [cited 2018. 3.5.]. Edicija dokumenata iz područja informacijske sigurnosti]. Available from: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-172.pdf.

3. Jain A, Tailang H, Goswami H, Dutta S, Sankhla MS, Kumar RJIJoCE. Social Engineering: Hacking a Human Being through Technology. 2016;18(5):94-100.

4. Thompson ST. Helping the hacker? Library information, security, and social engineering. Information Technology Libraries. 2006;25(4):222-5.

5. Hadnagy C. Social engineering: The art of human hacking: John Wiley & Sons; 2010.

6. Granger S. Social engineering fundamentals, part I: hacker tactics. Security Focus. 2001;18.

7. Koyun A, Al Janabi E. Social Engineering Attacks. Journal of Multidisciplinary Engineering Science and Technology. 2017;4(6):7533-8.

8. Hasan M, Prajapati N, Vohara S. Case study on social engineering techniques for persuasion. International journal on application of graph theory in wireless ad hoc networks and sensor networks. 2010;2:17-23.

9. Allen M. Social engineering: A means to violate a computer system. SANS Institute, InfoSec Reading Room. 2006.

10. Winkler IS, Dealy B, editors. Information Security Technology? Don't Rely on It. A Case Study in Social Engineering. USENIX Security Symposium; 1995.

11. Mitnick KD, Simon WL. The art of deception: Controlling the human element of security: John Wiley & Sons; 2011.

12. Peltier TR. Social engineering: Concepts and solutions. Information Security Journal. 2006;15(5):13-21.

13. Tetri P, Vuorinen J. Dissecting social engineering. Behaviour & Information Technology. 2013;32(10):1014-23.

14. Dadkhah M, Sutikno T, Jazi MD, Stiawan DJT. An introduction to journal phishings and their detection approach. 2015;13(2):373-80.

15. Napredne tehnike socijalnog inženjeringa [cited 2018. 7.6.]. Edicija dokumenata iz područja informacijske sigurnosti]. Available from: https://www.cis.hr/www.edicija/Naprednetehnikesocijalnoginenjeringa.html.

16. Ollmann G. The vishing guide. IBM Global Technology Services. 2007.

17. Socijalni inženjering putem VoIP tehnologije [cited 2018. 7.6.]. Edicija dokumenata iz područja informacijske sigurnosti]. Available from: https://www.cis.hr/www.edicija/SocijalniinenjeringputemVoIPtehnologije.html.

18. Rouse M. Spear phishing. 2010. [cited 2018. 8.6.]. Available from: https://searchsecurity.techtarget.com/definition/spear-phishing.

19. Pharming: Wikipedia, The Free Encyclopedia; [cited 2018. 8.6.]. Available from: https://en.wikipedia.org/wiki/Pharming.

20. Yeboah-Boateng EO, Amanor PM. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing Information Sciences. 2014;5(4):297-307.

21. Applegate SD. Social engineering: hacking the wetware! Information Security Journal: A Global Perspective. 2009;18(1):40-6.

22. Elicitation [cited 2018. 9.6.]. Available from: https://www.social-engineer.org/wiki/archives/Elicitation/Definition_of_Elicitation.htm.

23. Nadeem MS. Mailfence Blog [Internet]2015. Available from: https://blog.mailfence.com/what-is-baiting-in-social-engineering/.

24. Tovstukha I, Laaneots U. Prevention Strategies For Social Engineering. University of Tartu Institute of Computer Science [Internet]. Available from: https://courses.cs.ut.ee/MTAT.03.246/2013_spring/uploads/Main/essay07.pdf.

25. Paul I. How—and why—you should use a VPN any time you hop on the internet 2017. [cited 2018. 30.8.]. Available from: https://www.techhive.com/article/3158192/privacy/howand-whyyou-should-use-a-vpn-any-time-you-hop-on-the-internet.html.

26. Tor - mreža za anonimnost [cited 2018. 30.8.]. Edicija dokumenata iz područja informacijske sigurnosti]. Available from: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-07-197.pdf.

27. Oare A. Tor ili VPN – Koji je sigurniji 2018. [cited 2018. 30.8.]. Available from: https://hr.wizcase.com/blog/tor-ili-vpn-koji-je-sigurniji/.

28. Thomas K, Li F, Zand A, Barrett J, Ranieri J, Invernizzi L, et al., editors. Data breaches, phishing, or malware?: Understanding the risks of stolen credentials. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security; 2017: ACM.

29. A study of password habits among American consumers. 2012. [cited 2018. 10.6.]. Available from: https://www.csid.com/2012/09/consumer-password-habits-unveiled/.

30. Huth A, Orlando M, Pesante L. Password security, protection, and management. United States Computer Emergency Readiness Team. 2012.

31. Keeper Security Blog [Internet]2016. Available from: https://keepersecurity.com/blog/2016/08/22/8-most-common-password-mistakes/.

32. Tuđan M. Testiranje sigurnosnih propusta standardnih protokola u bežičnim IEEE 802.11 mrežama: University North. University centre Varaždin. Department of Electrical Engineering.; 2015.

33. Bajtl S. Bežične mreže: University of Pula. Department of Information and Communication Technologies.; 2015.

34. Handshake [cited 2018. 21.7.]. Available from: https://www.computerhope.com/jargon/h/handshak.htm.

35. Cracking Wifi Without Bruteforce or Wordlist in Kali Linux 2017.1. [Full Guide]. [cited 2018. 21.7.]. Available from: https://null-byte.wonderhowto.com/forum/fluxion-cracking-wifi-without-bruteforce-wordlist-kali-linux-2017-1-full-guide-0178727/%20.

36. FluxionNetwork/fluxion [cited 2018. 21.7.]. Available from: https://github.com/FluxionNetwork/fluxion/blob/master/README.md.

37. Aircrack-ng [cited 2018. 22.7.]. Available from: https://www.aircrack-ng.org/doku.php?id=Main.

38. Gebhart G, Hoffman-Andrews J. How Captive Portals Interfere With Wireless Security and Privacy [cited 2018. 10.8.]. Available from: https://www.eff.org/deeplinks/2017/08/how-captive-portals-interfere-wireless-security-and-privacy.

39. THE ULTIMATE GUIDE What is SSL, TLS and HTTPS? [cited 2018. 1.8.]. Available from: https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-https.

40. Kamboj H, Singh G. Fake Access Point Detection and Prevention Techniques. Journal of P2P Network Trends and Technology (IJPTT). 2013.;3(2):34-6.

41. Stealth Attack Types: Fake WiFi Access Points [cited 2018. 12.6.]. Available from: https://www.bankvaultonline.com/faqs/stealth-attacks-fake-wireless-points/.

42. WiFi-Pumpkin [cited 2018. 2.8.]. Available from: https://github.com/P0cL4bs/WiFi-Pumpkin.

43. Wilcox H, Bhattacharya M, Islam R. Social Engineering through Social Media: An Investigation on Enterprise Security. International Confenerence on Applications and Techniques in Information Security; Berlin, Heidelberg: Springer; 2014. p. 243-55.

44. Bača M, Ćosić J. Prevencija računalnog kriminaliteta. Policija i sigurnost. 2013.;22(1):146-58.

7. SAŽETAK

Socijalni inženjering kao metoda otkrivanja povjerljivih informacija

Današnje prijetnje računalnoj sigurnosti su mnogobrojne i raznovrsne. Socijalni inženjering jest jedna vrsta napada na računalnu sigurnost. Riječ je o neautoriziranom pristupu informacijama ili cijelom računalnom sustavu manipuliranjem žrtvom. Povjerljive informacije se izvlače načinima psihološke manipulacije, upotrebe trikova, uvjeravanja, lažnog predstavljanja ili zloupotrebe povjerenja.

Cilj ovoga rada bilo je detaljnije istražiti socijalni inženjering, njegove metode i načine napada, kao i mjere zaštite. Dodatni cilj je bio i pokušati izvesti napad u kontroliranom okruženju kako bi se pokazalo koliko je lako provesti takve napade, budući da su svi materijali sa uključenim detaljnim uputama dostupni na internetu.

Provedeni napadi izvršeni su isključivo za potrebe ovoga rada, te se sve odvijalo u kontroliranom okruženju. Prvi program kojim se proveo napad obuhvaća otkrivanje lozinke Wi-Fi mreže, a riječ je o Fluxion programu. Fluxion je alat koji automatizira proces stvaranja lažne pristupne točke blizanca kako bi uhvatio WPA/WPA2 lozinke, mješavina je tehničkog dijela napada i socijalnog inženjeringa koji nasamaruje žrtvu da preda Wi-Fi lozinku. Drugi program je naziva WiFi-Pumpkin, a stvara vlastitu lažnu pristupnu točku, pruža uslugu bežičnog spajanja na internet te prisluškuje promet spojenog korisnika. Treći program stvara lažnu web-stranicu, a tim je prikazano na koji način napadač može uhvatiti lozinku žrtvine društvene mreže. Koristio se program Weeman, jednostavna Phython skripta koja stvara lažne web-stranice identične originalnima.

Provedbom kontroliranih napada pokazalo se da se jednostavno i besplatno putem interneta može doći do softvera i alata koji su uspješni u otkrivanju povjerljivih informacija. Sve nam to upućuje da je potrebno biti što oprezniji prilikom korištenja interneta, odnosno spajanjem na otvorene Wi-Fi mreže, primitak sumnjivog emaila, paziti na sumnjive poveznice na koje mislimo kliknuti i ostalo, te da je potrebno podignuti svijest među običnim korisnicima interneta, putem reklama, educiranjem u školama i dr. Organizacije i tvrtke moraju shvatiti da je konstantno educiranje njihovih zaposlenika o opasnostima interneta i socijalnog inženjeringa bitno te da na taj način smanjuju rizik od napada na samu organizaciju.

Ključne riječi: socijalni inženjering, napadi, povjerljive informacije, sigurnost, lozinke, pristupne točke, društvene mreže.

8. SUMMARY

Social engineering as a method of revealing confidential information

Modern threats to computer security are many and varied. Social engineering is one kind of computer security threat. It's about unauthorized access to information or the entire computer system by manipulating the victim. Confidential information is extracted by psychological manipulation, the use of tricks, persuasion, false representation or abuse of trust.

The aim of this paper was to investigate social engineering, its methods and ways of attack as well as the protection measures. An additional goal was to try run an attack in a controlled environment to show how easy it is to take such attacks, as all the materials with detailed instructions included are available on the Internet.

The attacks were carried out solely for the purpose of this work, and everything was done in a controlled environment. The first program involves detecting a Wi-Fi password, which is a Fluxion program. Fluxion is a tool that automates the process of creating a fake twin access point to capture WPA / WPA2 passwords, a blend of a technical part of the attack and social engineering that tricks the victim to hand over the Wi-Fi password. The second program is WiFi-Pumpkin, and it creates its own fake access point, provides wireless connectivity to the Internet, and intercepts the traffic of the connected user. The third program creates a fake web page and that program shows us how the attacker can catch the password of the victim's social network. It is program called Weeman, a simple Phython script that creates fake web pages identical to the original.

By implementing controlled attacks, it has been shown that software and tools that are successful in revealing confidential information can be accessed easily and free through the Internet. All this tells us that it is necessary to be extremely cautious when using the Internet, ie by connecting to an open Wi-Fi network, receiving suspicious emails, the suspicious links that we think click and the other, and raising awareness among ordinary Internet users, through advertising, education in schools, etc. Organizations and businesses need to realize that constantly educating their employees about the dangers of Internet and social engineering is important and thus reducing the risk of attacking the organization itself.

Keywords: social engineering, attacks, confidential information, passwords, security, access points, social networks.

9. ŽIVOTOPIS

Ivana Kelam rođena je 9.9.1993. u Splitu.

Osnovnoškolsko obrazovanje stekla je u Osnovnoj školi knez Trpimir u Kaštel Gomilici u razdoblju od 2000. do 2008. godine.

Srednju školu upisuje 2008. godine, Ekonomsko-birotehnička škola Split, smjer ekonomist.

Fakultetsko obrazovanje započinje 2012. godine, kada upisuje Fakultet elektrotehnike, strojarstva i brodogradnje u Splitu, smjer računarstvo te završetkom stječe naziv sveučilišna prvostupnica inženjerka računarstva.

Diplomski studij upisuje 2016. godine na Odjelu forenzičnih znanosti, smjer Forenzika i nacionalne sigurnosti.

U sklopu studiranja na Odjelu forenzičnih znanosti sudjeluje na Festivalu znanosti 2017. godine u osmišljavanju, pripremi i provedbi radionice „Identifikacija osobe – mogućnosti kroz vrijeme“, te 2018. godine u osmišljavanju, pripremi i provedbi edukativne igre „Escape Room: Tragovima forenzike“.

10. IZJAVA O AKADEMSKOJ ČESTITOSTI

SVEUČILIŠTE U SPLITU

Sveučilišni odjel za forenzične znanosti

Izjava o akademskoj čestitosti

Ja, _____Ivana Kelam_____, izjavljujem da je moj diplomski rad pod naslovom _____Socijalni inženjering kao metoda otkrivanja povjerljivih informacija_____

rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovoga rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ičija autorska prava.

Izjavljujem da nijedan dio ovoga rada nije iskorišten u ijednom 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.

Split, _____

Potpis studenta/studentice: _____