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
- Phising
- Spear phising
- Email hacking and contact spamming

1.2 Phising

Phising sao emails ou mensagens de texto com o objetivo de criar uma sensação de urgencia, curiosidade ou medo nas vitimas.
Essas mensagens depois fazem o alvo revelar informação sensível, clicar em links maliciosos ou cliar em anexos que contêm malware.

1.3 Spear Phising

Um senário de spear phising deve envolver o atacante a fazer-se passar por alguem 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.

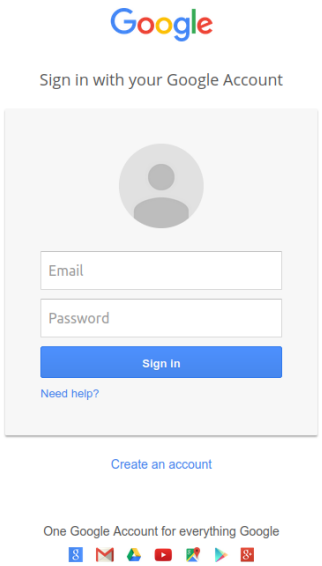
3 Senário 1

sudo setoolkit

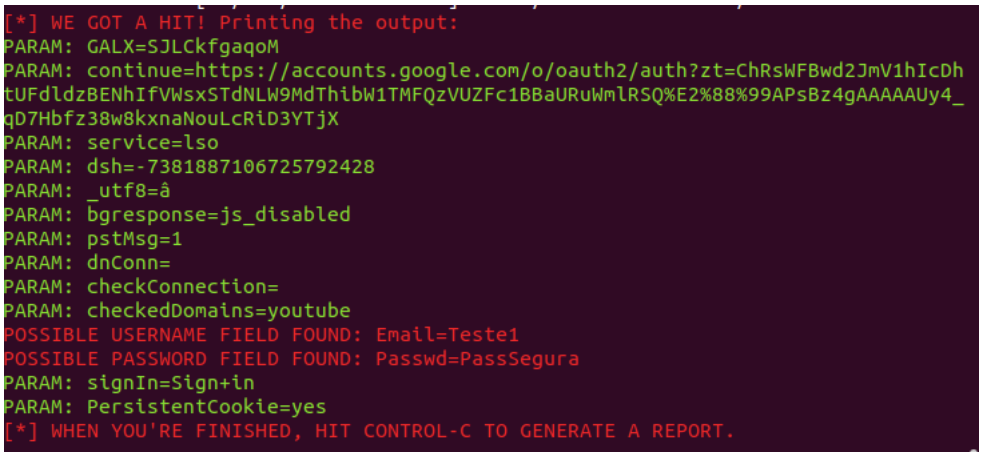
Escolhas feitas na ferramenta:
1) social engineering attacks
2) Website attack vectors
3) Credentials Harvester Attack Method
1) Web templates
Introduzir o IP como
2) Google (pode ser usado outro)

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

Isto é o que o alvo irá ver:



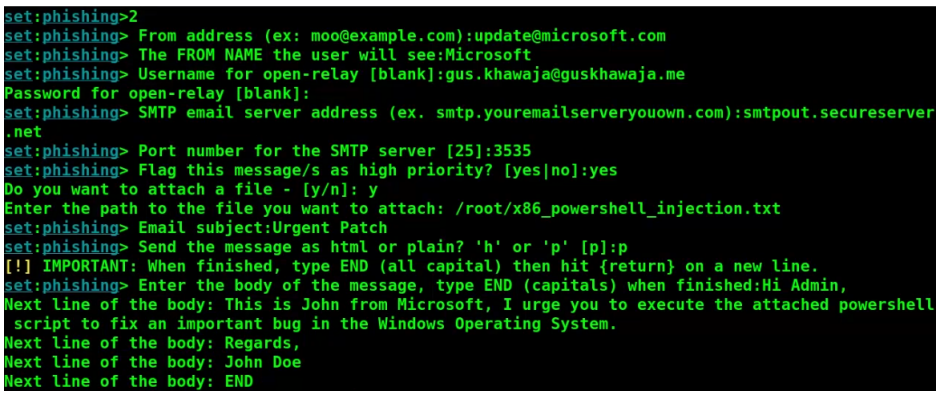
Isto é o que o atacante recebe no seu pc caso o alvo introduza os seus dados:



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 serveror open relay
Preencher a informação, exemplo abaixo:



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 tambem ser usado com o referido no primeiro senário, 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 segunrança e como funciona uma das maneiras mais populares de enganar as pessoas. Aprendemos como os atacantes tentam enganar as suas vitimas mas tambem 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.