Live

Palestrante: Ariel Chama

Engenharia Social

A Legião The Hackers Security

A engenharia social é um ataque em que explora a vulnerabilidade humana. Este tipo de ataque é muito importante na fase de reconhecimento e é usada para recolher informações sobre o alvo !

Toda e qualquer técnica de persuasão e influência pode ser considerada engenharia social, independentemente de ser ligada à área de informática ou não.

Processo de ataque

- Coleta de informações
- Confiança
- Vetor de ataque
- Execução

Coleta de informações: Coletam-se as informações iniciais relativas ao alvo.

Confiança – Informações mais específicas começam a ser coletadas: usuários mais suscetíveis à execução de programas maliciosos, determinação de qual é a versão do navegador que tal empresa utiliza. Nessa
fase, o atacante deve estabelecer uma relação de confiança com o seu alvo.

Vetor de ataque – Planejamento do tipo de ataque que será efetuado. Pode ser tanto baseado em pessoas como baseado em computadores. Ataques baseados em computadores caracterizam-se por usar meios tecnológicos, como o uso de phishing, sites maliciosos, backdoors etc. Ataques baseados em pessoas caracterizam-se pelo contacto direto, como telefonemas ou, até mesmo, a ida física do atacante à empresa para efetuar o ataque.

Execução – Execução do ataque. Nesse ponto, o atacante já deve ter estabelecido a relação de confiança com a sua vítima para não despertar suspeitas. Do contrário, o ataque vai “Falhar”.

Tipos de engenharia social

- Baseado em pessoas
- Baseado em computadores (Ferramentas, phishing)

Baseado em pessoas: Nesse tipo de engenharia social, as técnicas utilizadas não necessitam do auxílio de programas computacionais. Por exemplo, disfarces, vendedores, vigaristas, vendedores de telemarketing, categorizam-se nesse formato de engenharia social

Baseado em computadores: Nesse tipo de engenharia social, as técnicas utilizadas necessitam do auxílio de programas computacionais. Por exemplo, o phishing e backdoors categorizam-se nesse formato de engenharia social.

A maioria das técnicas de engenharia social consiste em obter informações privilegiadas enganando os usuários de um determinado sistema através de identificações falsas, aquisição de carisma e confiança da vítima. Um ataque de engenharia social pode se dar através de qualquer meio de comunicação. Tendo-se destaque para telefonemas, conversas diretas com a vítima, e-mail e WWW. Algumas dessas técnicas são:

- Vírus que se espalham por e-mail
- Phishing
- Telefonemas
- Isca

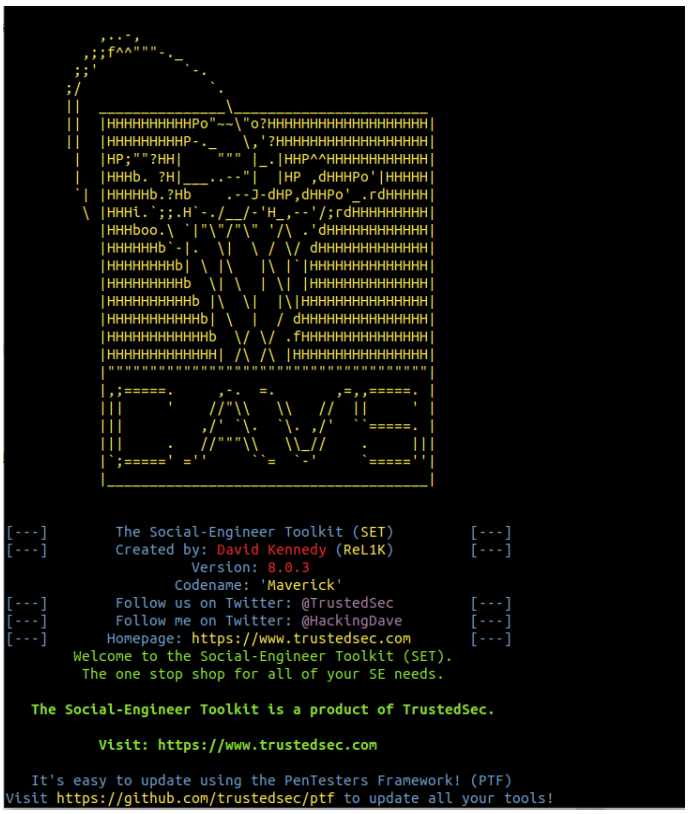
Vírus que se espalham por e-mail: criadores de vírus geralmente usam e-mail para a propagar as suas criações. Na maioria dos casos, é necessário que o usuário ao receber o e-mail execute o arquivo em anexo para que seu computador seja contaminado. O criador do vírus pensa então em uma maneira de fazer com que o usuário clique no anexo. Um dos métodos mais usados é colocar um texto que desperte a curiosidade do usuário. O texto pode tratar de sexo, de amor, de notícias atuais ou até mesmo de um assunto particular do internauta. Um dos exemplos mais clássicos é o vírus I Love You, que chegava ao e-mail das pessoas usando este mesmo nome. Ao receber a mensagem, muitos pensavam que tinham um(a) admirador(a) secreto(a) e na expectativa de descobrir quem era, clicavam no anexo e contaminam o computador. Repare que neste caso, o autor explorou um assunto que mexe com qualquer pessoa. Alguns vírus possuem a característica de se espalhar muito facilmente e por isso recebem o nome de worms (vermes). Aqui, a engenharia social também pode ser aplicada. Imagine, por exemplo, que um worm se espalha por e-mail usando como tema cartões virtuais de amizade. O internauta que acreditar na mensagem vai contaminar seu computador e o worm, para se propagar, envia cópias da mesma mensagem para a lista de contactos da vítima e coloca o endereço de e-mail dela como remetente. Quando alguém da lista receber a mensagem, vai pensar que foi um conhecido que enviou aquele e-mail e como o assunto é amizade, pode acreditar que está mesmo recebendo um cartão virtual de seu amigo. A tática de engenharia social para este caso, explora um assunto cabível a qualquer pessoa: a amizade.

Vou mostrar uma ferramenta muito conhecida, que automatizará os seus ataques em engenharia social, ela é chamada de:

SET (Social Engineering Toolkit)

O SET é uma ferramenta de fácil uso para ataques de engenharia social com base tecnológica. Apresenta opções

como geração de cavalos de Troia, phishing, criação de mídia infectada etc.



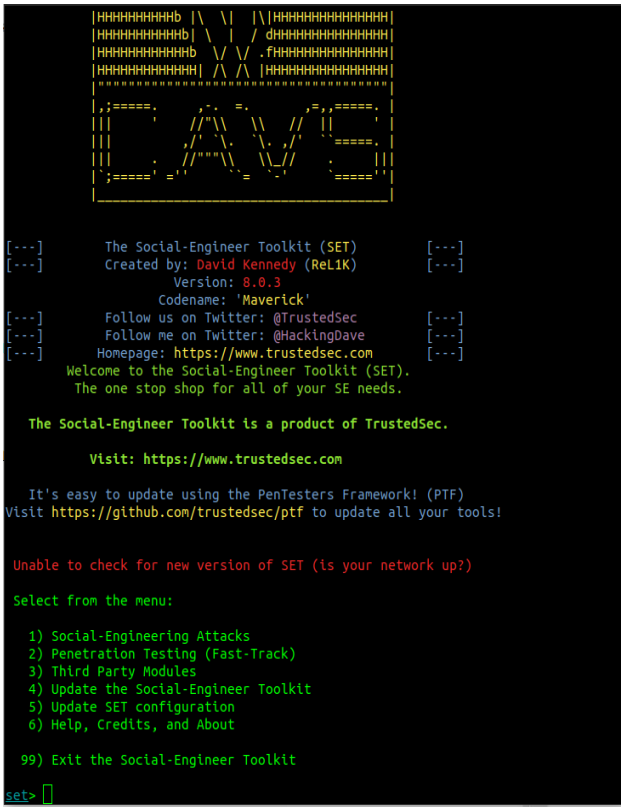


Figura 1- Ferramenta Setoolkit “SET”

OBS: Será explicado sobre uso da ferramenta na live.

GRUPO

Facebook: A Legião The Hackers Security
Github: alegiaothehackersecurity

Palestrante:

Whatsapp: 921964331
Telegram: @arielchama
Facebook: Ariel Chama
Github: arielchama