**EXPERIMENTO 2**

**ATAQUE DE ESCALAÇÃO DE PRIVILÉGIO LOCAL**

Neste experimento, escalaremos privilégios sobre uma máquina comprometida, anteriormente, através de Metasploit. Escalação de privilégio local permite-nos ganhar acesso a um sistema ou contas de usuário de domínio, utilizando o sistema corrente, no qual estamos ligados.

**REQUISITOS**

Os seguintes requisitos precisam ser cumpridos:

* Uma conexão de Internet ou Intranet é requerido para completar esta tarefa.
* Uma máquina comprometida usando-se Metasploit Framework, de uma vítima é também requerida.

**COMO FAZER**

Inicia-se o processo de realizar um teste ou um ataque de escalação de privilégio local, a partir de um *shell* do **Meterpreter**. Para tal, precisamos usar, anteriormente, o **Metasploit Framework** para atacar uma máquina, no sentido de ganhar o *shell* do **Meterpreter**. Os experimentos anteriores, sobre exploração com **Metasploit**, mostram como se chegar até este ponto.

1. Uma vez que se tenha obtido acesso à máquina de teste (ou da vítima), usando Metasploit com um *payload* do Meterpreter, aguarde pelo prompt do Meterpreter ser mostrado na máquina-alvo.

msf exploit(handler) > sessions –i 1

[\*] Starting interaction with 1 …

meterpreter >

1. No prompt de Meterpreter, vemos o arquivo help para **o** getsystem **executando este com a opção** -h.

meterpreter > getsystem –h

1. Finalmente, rodamos getsystem sem quaisquer atributos:

meterpreter > getsystem

Se estamos tentando ganhar acesso para uma máquina Windows 7, devemos rodar o comando bypassuac antes de executar o comando getsystem . O commando bypassuac permite-nos “by-pass” Microsoft User Account Control.

run post/window/escalate/bypassuac

uac = user account control

1. Assim, podemos ter realizado, bem sucedidamente, um ataque de escalação !!!

**CONCLUSÃO**

Neste experimento, usamos o Meterpreter para realizar um ataque de escalação de privilégio local sobre uma máquina-alvo. Começamos o experimento a partir do *shell* **Meterpreter**. Executamos, então, o comando getsystem, que permite ao **Meterpreter** tentar e elevar nossas credenciais sobre um sistema. Se, bem sucedido, teremos acesso em nível de sistema sobre a máquina-alvo testada.

**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.