**ESCALAÇÃO DE PRIVILÉGIO**

**INTRODUÇÃO**

Uma vez que se tenha ganho o acesso à máquina-alvo de um teste ou ataque, é importante escalar privilégios tanto quanto possível. Geralmente, se ganha acesso para uma conta de usuário (o usuário de um computador) que tem privilégios restritos. Entretanto, a conta-alvo pode ser a conta do administrador.

Este capítulo cobre os seguintes tópicos:

* Usando *tokens* de personificação
* Ataque de escalação de privilégio local
* Controlando com o *SocialEngineer Toolkit* (SET)
* Coletando dados da vítima
* Apagando ou limpando as pistas
* Criando um *backdoor* persistente
* Ataque *Man-in-the-Middle*

**USANDO TOKENS DE PERSONIFICAÇÃO**

Neste experimento, é personificado um outro usuário sobre uma rede, usando *tokens* de personificação.

Quando um usuário se “loga” em um sistema Windows, é dado um ***token*** de acesso como parte de sua sessão autenticada. A personificação do ***token*** permite-nos escalar privilégios por personificar esse usuário. Uma conta de sistema, por exemplo, pode precisar rodar como um administrador de domínio para manipular uma tarefa específica e, geralmente, põe à parte, sua autoridade elevada quando feita. Pode-se utilizar desta fragilidade para elevar direitos de acesso.

**REQUISITOS**

Os seguintes requisitos precisam ser cumpridos:

* Uma conexão de Internet ou Intranet é requerido para completar esta tarefa.
* Uma máquina-alvo de uma vítima é também requerido.

**COMO FAZER**

Começamos nossa exploração de tokens de personificação, a partir do *shell* do Meterpreter. Neste caso, temos que usar Metasploit para atacar uma máquina, no sentido de ganhar o *shell* do Meterpreter. Pode-se usar um dos experimentos para se ganhar acesso a uma máquina usando Metasploit.

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. Do Meterpreter, pode-se começar o processo de personificação, usando **Incognito**:

meterpreter > use incognito

1. No prompt de Meterpreter, usar o arquivo help para incognito**, executando o comando** help.

meterpreter > help

1. Note que agora surgem várias opções possíveis, sendo uma delas, list tokens (List tokens available under current user contexto).
2. Desejamos obter uma lista de usuários disponíveis que estão correntemente “logados” no sistema-alvo ou que tiveram acesso ao sistema, recentemente. Para tal, executar o comando o comando:

meterpreter > list\_tokens –u

[-] Warning: Not currently running as SYSTEM, not all tokens will be available
 Call rev2self if primary process token is SYSTEM

Delegation Tokens Available

==============================

willie-PC\willie

Impersonation Tokens Available

==============================

No tokens available

meterpreter >

1. No que segue, rodamos o ataque de personificação. A sintaxe para usar é

**impersonate\_token[name of the account to impersonate]**como segue:

meterpreter > impersonate\_token [\\test-pc\willie](file:///%5C%5Ctest-pc%5Cwillie)

1. Se formos bem sucedido, estaremos, agora, usando o sistema corrente, mas, como um outro usuário.

 **CONCLUSÃO**

Neste experimento, nós começamos com uma maquina comprometida (pelo uso anteriormente do **Metasploit** e, então, usamos **Meterpreter** para personificar o *token* de um outro usuário sobre a máquina-alvo. A meta do ataque de personificação é escolher o mais alto nível de um usuário, possível, preferivelmente, alguém que esteja também conectado através de um domínio, e usar a conta desse usuário para ir além dentro da rede.