Laboratório 3

Instalação de Backdoor em um Servidor Web

Este experimento deve ser feito em duplas (as mesmas formadas no início do semestre). O relatório a ser entregue deve conter os nomes dos participantes, e todos devem colocar o relatório no Moodle.

Objetivo: utilizar a vulnerabilidade de Unicode do experimento anterior para instalar uma backdoor no servidor vulnerável.

1. Inicialize seu computador no Windows, e vá para a máquina virtual do Windows XP. Todo o experimento deve ser feito na máquina virtual. Como diversos serviços de rede serão utilizados, garanta que o firewall do Windows permita a passagem destes serviços**. Importante**: a máquina virtual XP deve estar conectada em modo bridge, e não em modo NAT. Confira se o número IP da máquina virtual é da forma 10.67.10xx.yyy (se for 192.xxx.xxx.xxx, você está em modo NAT).

2. Obtenha o programa NetCat, versão Windows (utilize a Internet para isto). Anote o url de onde você obteve o Netcat, e qual a versão. **Observação:** como o NetCat é considerado um programa daninho, utilizado por invasores, é possível que o anti-vírus da máquina impeça o seu uso. Se isto ocorrer, desabilite a varredura em tempo real do anti-vírus.

3. Obtenha e instale um servidor de TFTP para o Windows (dica: tftpd32). Anote o url de onde você obteve o servidor, qual seu nome, e qual a versão. Ative este servidor na sua máquina, e verifique como ele funciona.

4. Utilizando a vulnerabilidade do Unicode, transfira um arquivo de imagem qualquer (mas pequeno...) da sua máquina para o diretório do seu grupo (o mesmo que você utilizou no experimento passado), usando o **cliente de tftp da máquina invadida** (analise o funcionamento do tftp para ver como fazer isto a partir de uma linha de comando). Anote qual comando de tftp deve ser utilizado, e como você realizou isto no servidor vulnerável (qual url). **Observação:** execute o comando tftp diretamente, e não através do cmd.exe. Se você usar o cmd.exe do servidor, ficará restrito às limitações impostas ao cmd.exe.

5. Repita o passo anterior, mas desta vez para transferir o NetCat para o servidor. Anote como você fez isto.

6. Analisando o funcionamento do NetCat, ative-o para funcionar como um servidor na porta 10000+número do seu grupo. A partir da sua máquina, conecte-se a este servidor. Anote quais os comandos de ativação do NetCat como servidor e como cliente.

7. Tendo estabelecido uma conexão bem sucedida, chame o professor para avaliação do funcionamento.

8. Poste um arquivo de relatório no Moodle, informando:
1) de onde você obteve a versão do NetCat (url).
2) de onde você obteve o servidor de tftp (url).
3) qual o nome do arquivo de imagem que você transferiu para o diretório do seu grupo.
4) qual o comando de tftp que você utilizou para transferir os arquivos.
5) quais os comandos utilizados para ativar o NetCat como servidor e como cliente.