Estudo Técnico: Enganando o Atacante

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Serviços Falsos

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ Já vimos em módulos anteriories que se mudarmos a porta padrão de acesso de um serviço qualquer em suas configurações originais e executarmos um scan normal nas portas, o nmap retornará o nome de serviço padrão para aquela porta.

+ Como exemplo, podemos mudar a porta do ssh de 22 (padrão) para 21 (porta padrão do ftp) com o `nano /etc/ssh/sshd_config` e o nmap, caso faça uma varredura comum, vai identificar o serviço ftp como ativo

```
nmap -v -sS -Pn 192.168.1.138
```

```
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
```

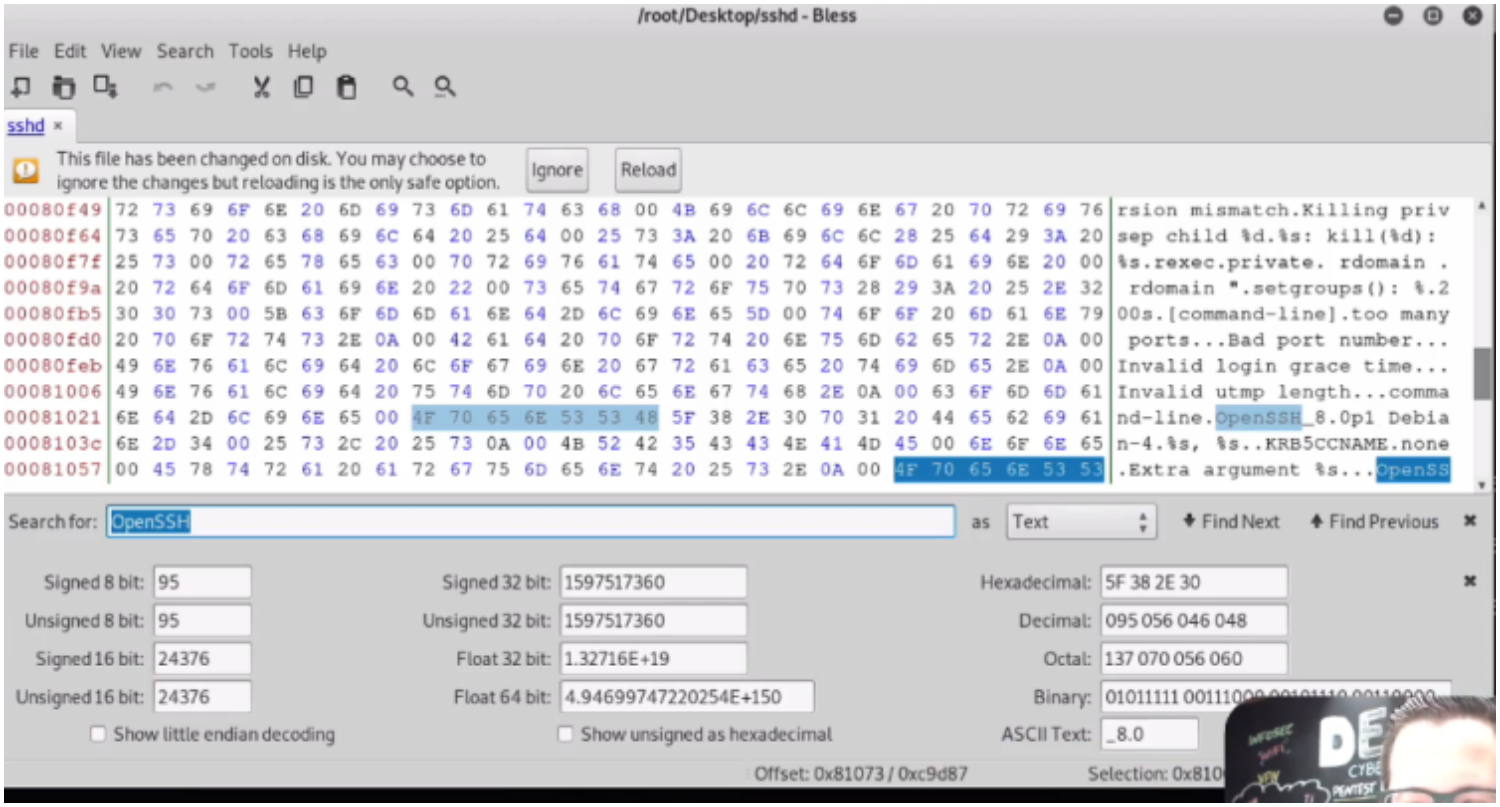
+ Mas caso executemos uma condição de interação com o serviço, poderemos capturar o banner e descobrir que serviço está rodando ali.

```
nmap -v -sV -Pn 192.168.1.138
```

```
PORT   STATE SERVICE VERSION
21/tcp open  ssh     OpenSSH 9.4p1 Debian 1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.58 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

+ O objetivo dessa aula é modificar esse banner nos bytes do protocolo de execução desse serviço

+ Faremos isso por intermédio de uma ferramenta chamada bless



+ Aparentemente ela n existe mais. Mas basicamente abríamos o arquivo sshd que estava localizado na /usr/sbin/sshd e modificávamos as linhas de texto correspondentes ao banner do protocolo. A ferramenta fazia a modificação dos bytes (funciona desde que tenhamos o cuidado de fazer arquivos de mesmo tamanho)

```
bless sshd
```