2ª Chamada do FIBRE OPEN CALL

HANDS-ON: Ataque de Negação de Serviço (DoS) e Análise de Tráfego

Desenvolvido na Universidade Federal de Juiz de Fora por:
Prof. Dr. Eduardo Pagani Julio - eduardo.pagani@ice.ufjf.br
Prof. Dr. Edelberto Franco Silva - edelberto@ice.ufjf.br

Visão Geral

Neste Tutorial você irá criar um experimento usando o testbed FIBRE, com o objetivo de analisar o tráfego da rede durante uma simulação de um ataque de negação de serviço.

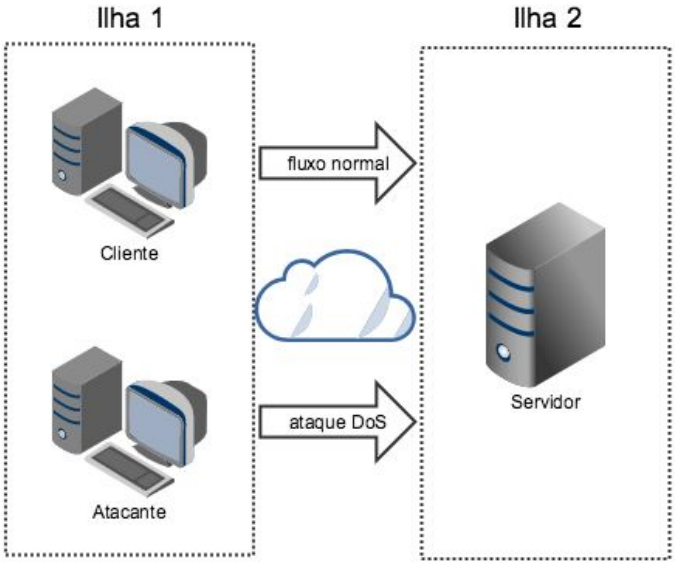
O que você irá aprender

1. Criar máquinas virtuais usando o orquestrador OCF
2. Alocar uma topologia virtual e iniciar um experimento
3. Instalar pacotes para simulação do ataque de DoS
4. Analisar o comportamento do tráfego durante um ataque usando a ferramenta Wireshark

Pré-requisitos

1. Ter uma conta criada em http://portal.rnp.fibre.org.br
2. Estar conectado à VPN do FIBRE (https://fibre.org.br/start-using-fibre/getting-access/)
3. Ter conhecimentos básicos de experimentação (Criar projeto, criar slice: https://fibre.org.br/start-using-fibre/your-first-experiment/ocf-hello-world/)

Topologia



Agenda

1. Preparando o Ambiente

1.1. Criando o *Slice*

Acesse o ***site https://ocf.fibre.org.br/*** e realize ***login*** com seu usuário e senha.

Figura 1: Tela de login no portal FIBRE

Em seu ***dashboard***, selecione o projeto de interesse e crie um ***slice*** para realização do experimento. Caso ainda não tenha criado um projeto, inicie a criação através do botão "***Create***" e preencha o formulário. No seu projeto e no seu ***slice***, adicione dois "***Virtualization Aggregate***" (use duas ilhas diferentes) conforme a Figura 2.

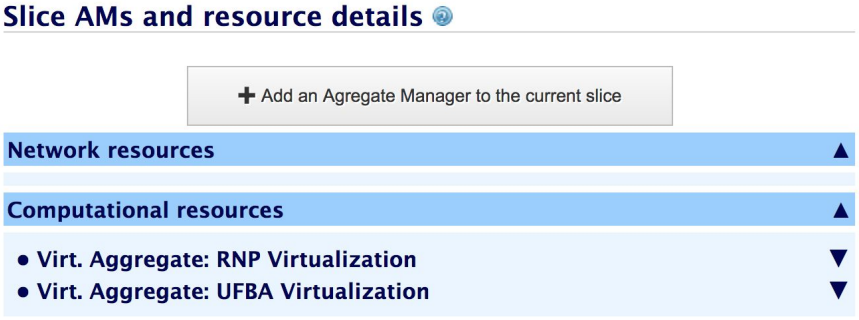


Figura 2: Adição de Dois *Virtualization Aggregates* no Projeto

NOTA: Para a correta execução do experimento é necessário que hajam dois agregadores do tipo "***Virtualization***". Selecione duas ilhas diferentes para melhor visualização do tráfego.

1.2. Criando Máquinas Virtuais

Após adicionados os agregadores, é necessária a criação de três máquinas virtuais: ***cliente, servidor*** e ***atacante***. crie a máquina virtual ***servidor*** em uma ilha, e as outras duas máquinas virtuais (cliente e atacante) na outra ilha.

Para a criação da máquina virtual, selecione um dos recursos disponíveis em uma ilha, por exemplo ***UFBA_whitebox4***, e clique em "***Create VM***". Use os mesmos parâmetros ilustrados na Figura 3 para a criação das três máquinas virtuais, mudando apenas o nome e a localização da máquina virtual.

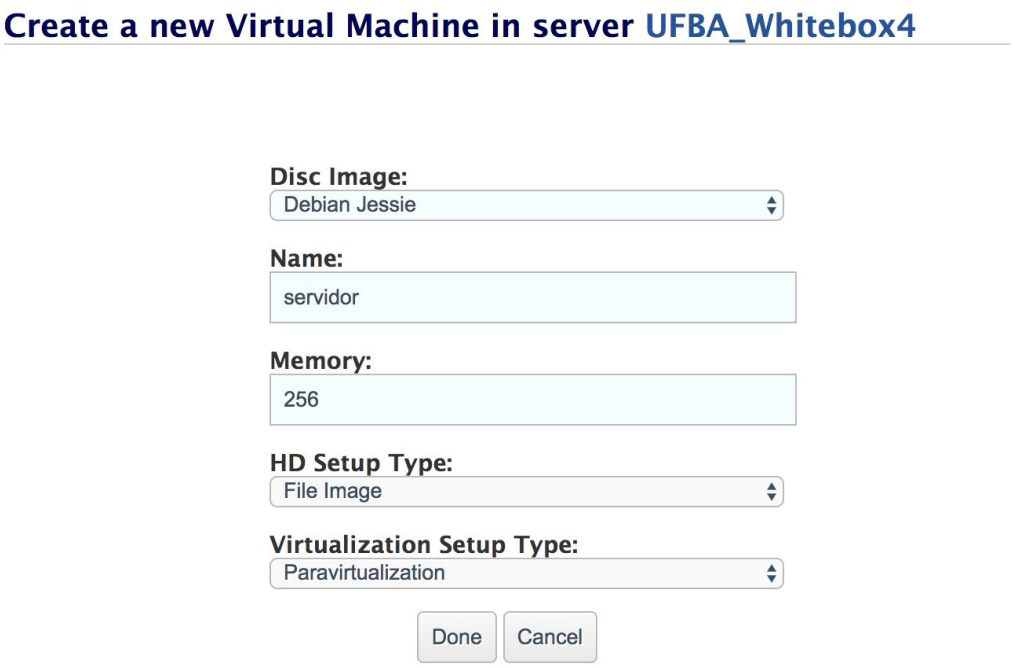


Figura 3: Parâmetros para a Criação de Máquina Virtual

1.3. Iniciando o *Slice*

Após a criação das três máquinas virtuais, clique em "***Start Slice***". Inicie também cada uma das três máquinas virtuais clicando em "***Start***".

2. Experimento

Com as 3 máquinas virtuais em execução, faça acesso remoto em cada uma e prepare o ambiente para o experimento.

2.1. Instalação dos softwares

Para o experimento, é necessário a execução dos seguintes comandos na máquinas virtuais para a instalação dos pacotes necessários, conforme descrito na Tabela 1.

Tabela 1: Instalação de Softwares nas Máquinas Virtuais.

atacante	$ su # apt-get update && apt-get install -y hping3
servidor	$ su # apt-get update && apt-get install -y tcpdump
cliente	(nada a instalar)

2.2. Executando o Experimento DoS

Cada máquina no experimento tem a sua função bem definida: o ***cliente***, simulando um tráfego normal com o servidor; o ***servidor***, que atende os clientes e vai sofrer o ataque; e o ***atacante***, com o objetivo de inundar o servidor.

No ***cliente***, usaremos a versão cliente do ***software*** iperf, que será usado para simular um tráfego com o ***servidor.***

No ***atacante***, será usado o ***software*** hping3, usado para simular um ataque de inundação de pacotes (***flood***) ao servidor.

No servidor, ele receberá o tráfego do ***cliente*** (com iperf) e do ***atacante***, além de capturar o tráfego para análise posterior.

Para o início do experimento, serão necessárias **quatro conexões SSH**: **uma** com o ***cliente***, **uma** com o ***atacante*** e **duas** com o ***servidor.*** Os comandos que devem ser executados em cada máquina virtual e a ordem de execução, são listados na Tabela 2.

NOTA: Para uma melhor execução do experimento é sugerido que sejam abertas 4 janelas e os comandos sejam todos executados em modo ***root*** (execute o comando ***su*** com a senha ***openflow***). Além disso, deixe digitado todos os comandos nos terminais antes de iniciar. Com todos os comandos digitados e os dados conferidos, execute-os na ordem indicada na Tabela 2. Um exemplo de um ambiente preparado é ilustrado na Figura 4.

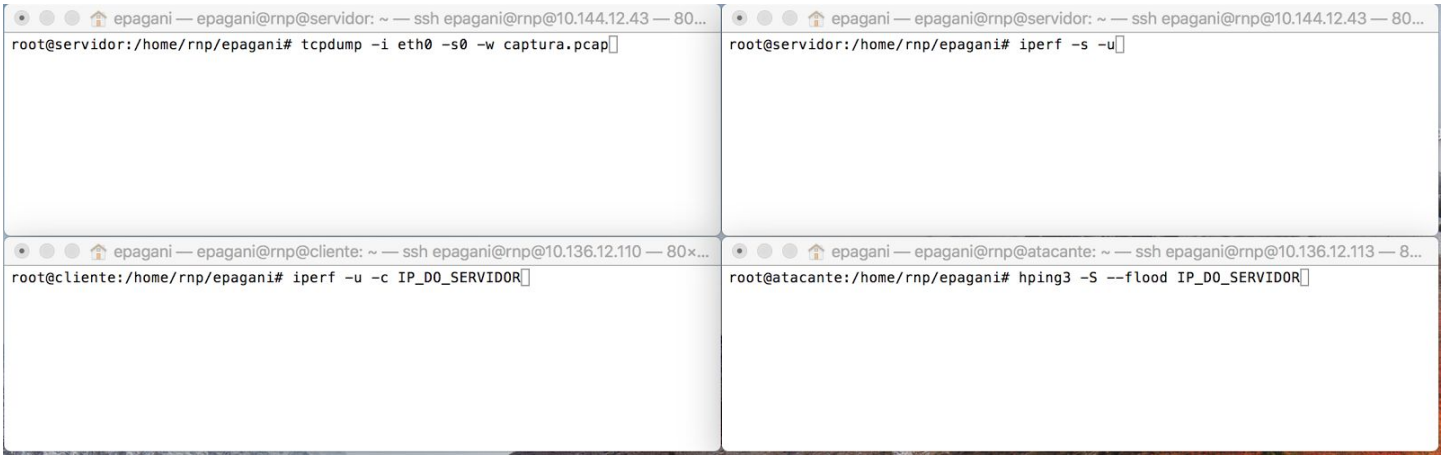


Figura 4: As Quatro Conexões com as Máquinas Virtuais e os Comandos já Digitados

Tabela 2: Ordem de Execução dos Comandos para o Experimento.

ordem	máquina virtual (conexão)	comandos
1	servidor (1)	# tcpdump -i eth0 -s0 -w captura.pcap
2	servidor (2)	# iperf -s -u
3	cliente	# iperf -u -c IP_DO_SERVIDOR
4	atacante	# hping3 -S --flood IP_DO_SERVIDOR
5	atacante	(CONTROL+C, após 5 segundos para parar o ataque)
6	servidor (1)	(CONTROL+C para parar a captura) # tar zcvf captura.tgz captura.pcap

Após a execução dos comandos, será gerado no ***servidor*** o arquivo de ***captura.pcap,*** que deve ser compactado e transferido para uma máquina externa a infraestrutura do FIBRE para a análise.

2.3. Análise dos Dados Coletados

Com o arquivo de captura já transferido para a máquina de análise (use o comando scp para transferir), abra o arquivo com o software ***wireshark***.

No ***wireshark*** é possível visualizar todos os pacotes enviados e recebidos no ***servidor***, visto que a captura foi feita a partir dele, conforme ilustrado na Figura 5.

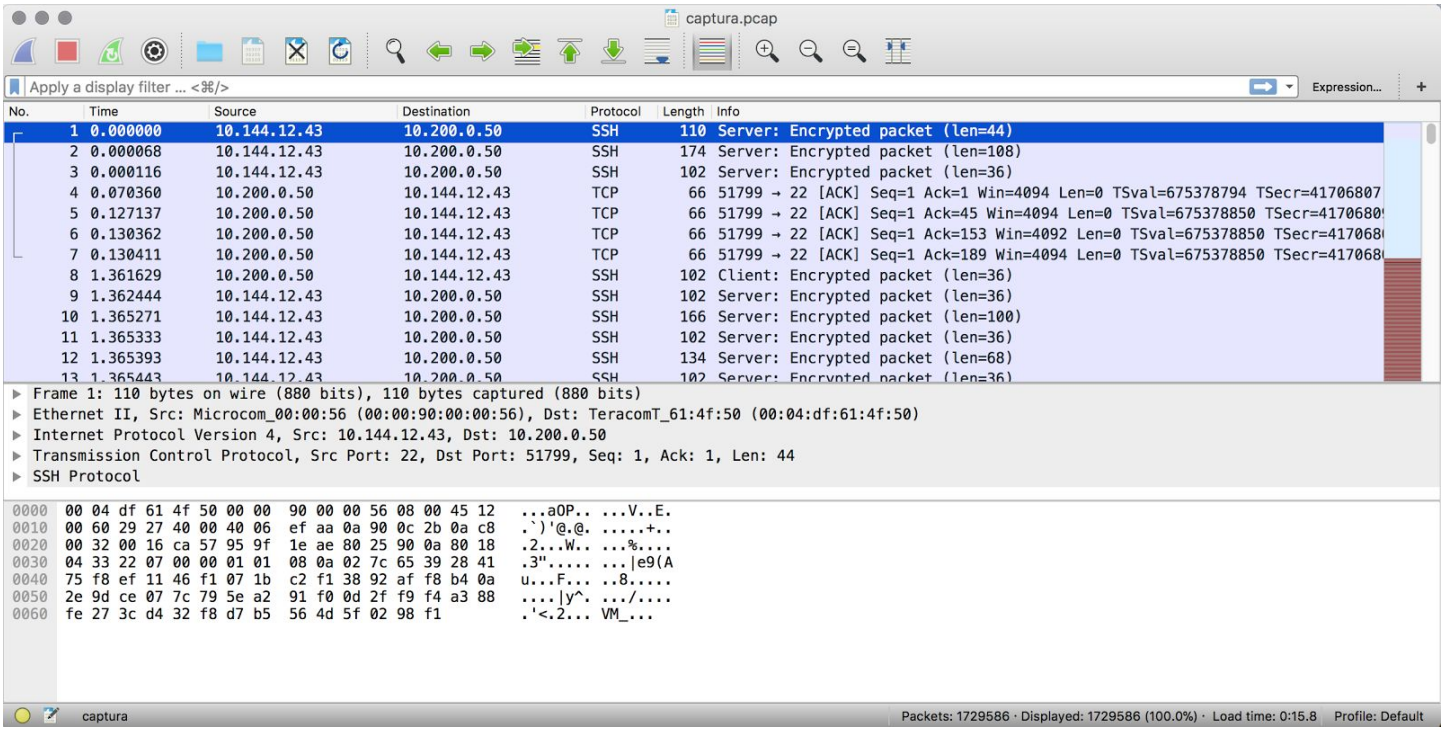


Figura 5: Tela Principal do Wireshark

No exemplo exibido na Figura 5, é possível identificar na barra de ***status*** um total de 1.729.586 de pacotes capturados.

Para a análise gráfica do tráfego, acesse no ***Wireshark*** o menu "***Statistics***", "***I/O Graph***". Para adicionar um novo filtro, use a opção "+". Crie dois novos filtros, conforme a Tabela 3.

Tabela 3: Criação de Filtros no Wireshark.

Name	***Display Filter***	***Style***	***Demais op- »es***
cliente	ip.addr == IP_do_cliente	Line	Default
atacante	ip.addr == IP_do_atacante	Line	Default

Após a criação dos filtros é possível aplicá-los para a criação dos gráficos. Crie 4 gráficos diferentes, com os parâmetros listados na Tabela 4.

Tabela 4: Parâmetros para a Criação de Gráficos.

Gráfico #	**Filtros Marcados**	***Log scale***
1	cliente	
2	atacante	
3	***All Packets*** + cliente + atacante	