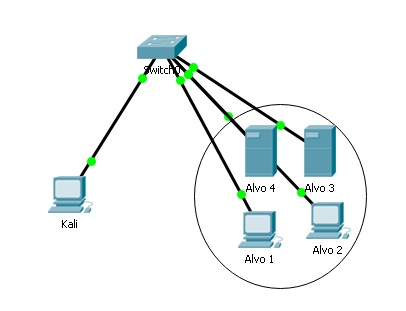
**ATIVIDADE - USO DO WIRESHARK (SERVIÇOS DO METASPLOITABLE2):**

Nome: Luca Zanfelici Fanucchi RA:19.00228-9  
Nome: Bruno Borgiani Tacla RA:19.01821-5  
Nome: Lucas Reis Azevedo RA:19.02659-5

Nome: Igor Eiki Ferreira Kubota RA:19.02466-5

Nome: Rafael Drewes RA:19.00001-4

1. Topologia
2. Objetivos

Parte 1: Preparando as máquinas virtuais (Rede Interna ou Modo Host Only)

Parte 2: Captura e visualização de um tráfego Telnet

Parte 3: Captura e visualização de um tráfego FTP

Parte 4: Captura e visualização de um tráfego HTTP

Parte 5: Captura e visualização de um tráfego SSH

**1. Formulário (Configurando a Rede no Linux):**

a. Configurando IP e Máscara (manual por linha de comando)

# ifconfig -a // verificando todas as interfaces no sistema

# ifconfig < interface > <IP > //configuração da rede no Linux

# ifconfig eth0 10.32.0.10 netmask 255.255.255.0 //configuração de endereço IP 10.32.0.10 com a máscara 255.255.255.0 usando a interface de rede eth0

# ifconfig eth0 10.32.0.10/24 //configuração de endereço IP 10.32.0.10 com a máscara 255.255.255.0 usando a interface de rede eth0

# ifconfig // verificando endereço que foi configurado no sistema Linux

c. Iniciar/para/reiniciar o serviço:

# /etc/init.d/networking start

# /etc/init.d/networking stop

# /etc/init.d/networking restart

d. Habilitando/desabilitando interface de rede:

# ifconfig eth0 down

# ifdown eth0

# ifconfig eth0 up

# ifup eth0

**Parte I – Preparando as Máquinas Virtuais (Modo Host-Only ou Rede Interna):**

* 1. Kali Linux para realização dos testes (vetor de ataque);
  2. Uma máquina virtual Linux como alvo (Metasploitable2).

**Parte 2 – Captura de um tráfego Telnet (Kali <-> Metasploitable):**

1. Para um cenário **Telnet** deve-se acessar ao servidor **Telnet (Metasploitable2)**. Considere o seguinte procedimento:
   1. Configurando a rede no Kali (Vetor de ataque):

Texto branco sobre fundo preto

Descrição gerada automaticamente

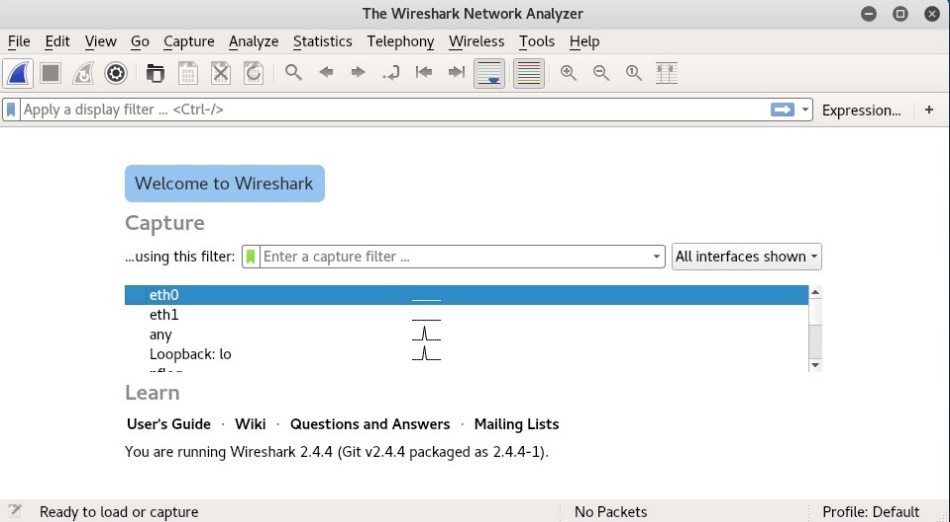
* 1. Configurando a rede no Metasploitable2 (Máquina Alvo):



Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

* 1. No Kali iniciar a captura no Wireshark:

****

* 1. No Kali digitar **telnet IP** **(por exemplo, telnet 192.168.56.20),** assim como o nome de usuário e senha (**admin/admin**). Assim que estiver acessando o outro computador, digitar:

# ls

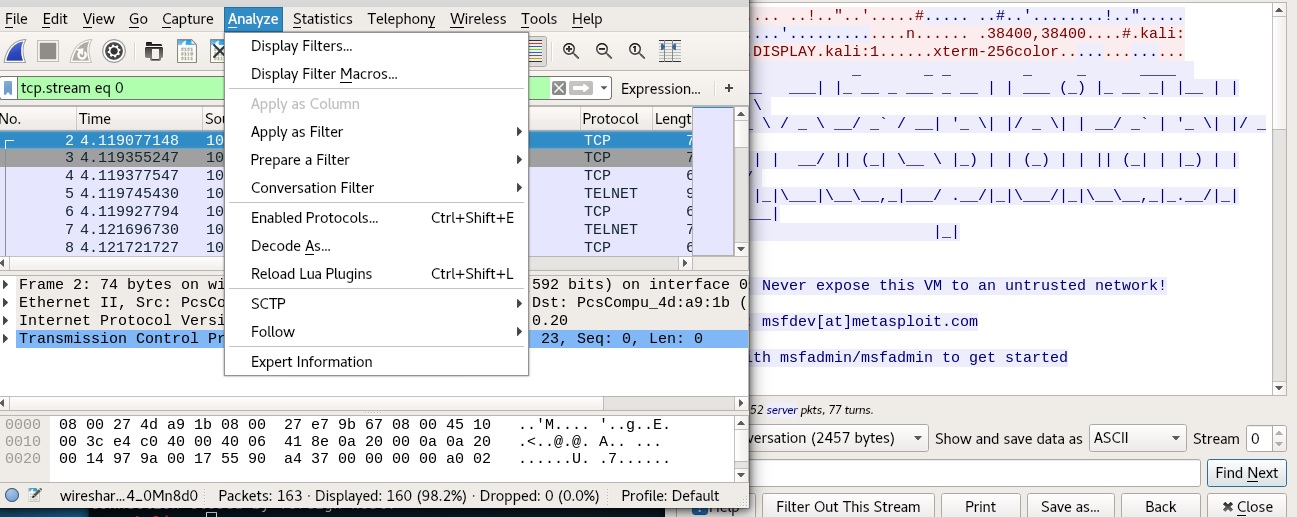
# ifconfig

# exit

**Texto branco sobre fundo preto

Descrição gerada automaticamente**

* 1. Finalizar a captura no Wireshark e realizar a análise offline:
     1. Digitar Analyse 🡪 Follow 🡪 TCP Stream (verificar o que está sendo observado).



* + 1. Descreva e demonstre o que está sendo observado.

***Todo o Tráfego de dados do metasploitable foi transmitido em texto puro, ou seja, todos os comandos que foram digitados pelo usuário, o nome de usuário digitado, a senha e tudo que tenha sido feito até a conexão ter sido terminada.***

* + 1. Existe alguma vulnerabilidade nesse serviço? O que pode ser realizado para minimizar o problema pensando em um serviço mais seguro? Justifique.

***Por estar em texto puro, é uma vulnerabilidade bem grande, uma vez em que um hacker que tenha acesso a uma das maquinas(podendo estar conectado à mesma rede da maquina alvo) possa obter as informações por meio de programas com o WireShark. Uma possibilidade para minimizar esse problema é a utilização de criptografia de dados.***

**Parte 3 – Captura de um tráfego FTP (Kali <-> Metasploitable):**

1. Para um cenário **FTP** deve-se acessar ao servidor **FTP (Metasploitable2)**. Considere o seguinte procedimento:
   1. Configurando a rede no Kali (Vetor de ataque):

Texto branco sobre fundo preto

Descrição gerada automaticamente

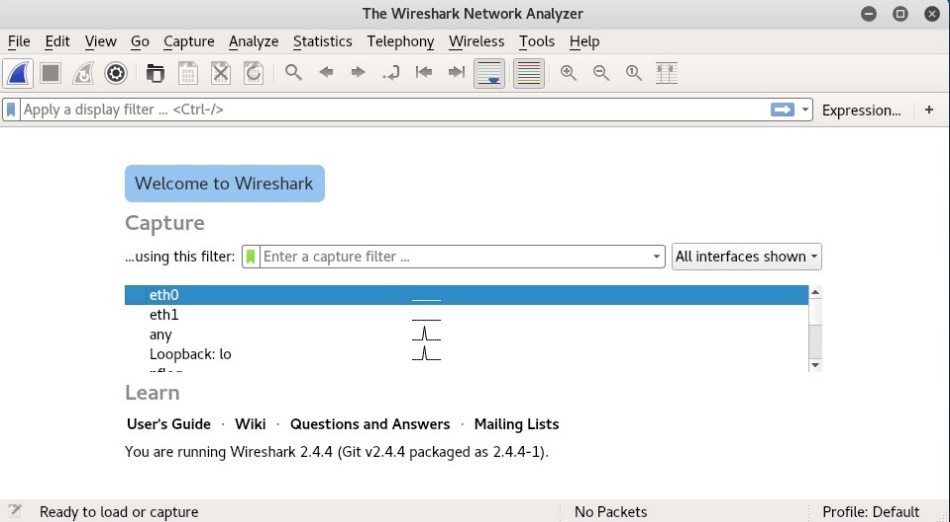
* 1. Configurando a rede no Metasploitable2 (Máquina Alvo):



Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

* 1. No Kali iniciar a captura no Wireshark:

****

* 1. No Kali digitar **ftp IP** **(ftp 192.168.56.20),** assim como o nome de usuário e senha (**admin/admin**). Assim que estiver acessando o outro computador, digitar:

# ls

# pwd

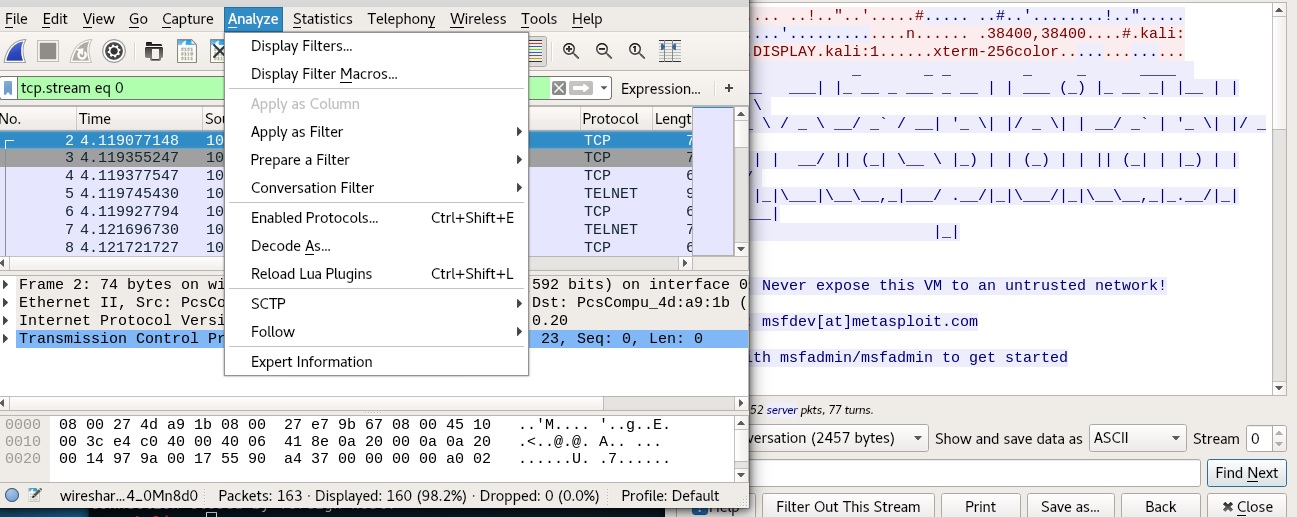
# help

# exit

**Texto branco sobre fundo preto

Descrição gerada automaticamente**

* 1. Finalizar a captura no Wireshark e realizar a análise offline:
     1. Digitar Analyse 🡪 Follow 🡪 TCP Stream (verificar o que está sendo observado).



* + 1. Descreva e demonstre o que está sendo observado.

***O WireShark foi capaz de obter o nome de usuário utilizado, a senha utilizada, todos os comandos que foram digitados pelo usuário, além de todos os dados que foram trocados, tudo isso estando em texto puro.***

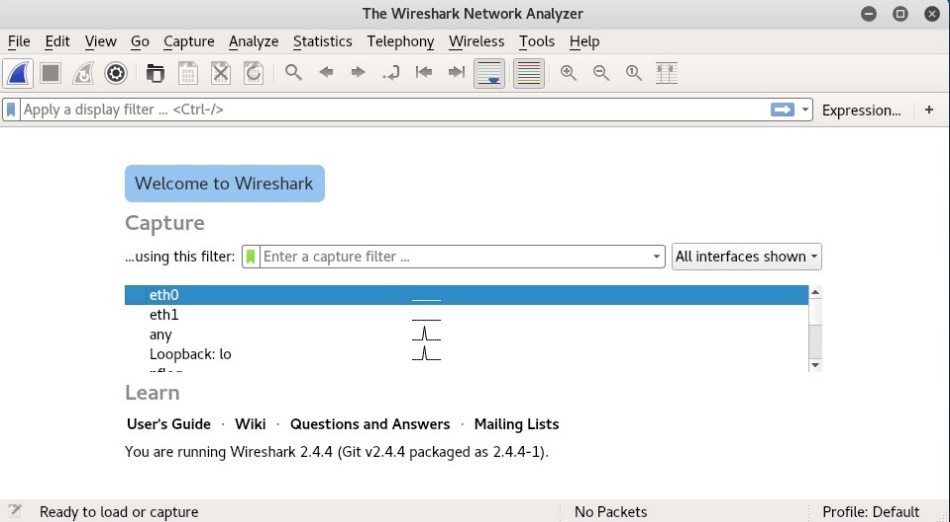
* + 1. Existe alguma vulnerabilidade nesse serviço? O que pode ser realizado para minimizar o problema pensando em um serviço mais seguro? Justifique.

***Sim, embora o FTP use códigos em seus protocolos, o WireShark foi capaz de obter os dados em forma de texto puro, o que indica uma enorme vulnerabilidade. Para minimizar esse problema, deveria ter sido feito uma criptografia nos dados que utilizam do FTP, mantendo-os seguro e não acessíveis por programas como o WireShark.***

**Parte 4 – Captura de um tráfego HTTP (Kali <-> Metasploitable):**

4. Para um cenário **HTTP** deve-se acessar ao servidor **HTTP (Metasploitable2)**. Considere o seguinte procedimento:

4.1. No Kali iniciar a captura no Wireshark:

****

* 1. Tela de celular com texto preto sobre fundo branco

     Descrição gerada automaticamenteNo browser do Kali (Firefox), acessar o endereço IP, deve ser o endereço disponibilizado no modo host only ou no endereço IP configurado:

4.3. Acessar o serviço DVWA:

Tela de celular com texto preto sobre fundo branco

Descrição gerada automaticamente

4.4. Finalizar a captura no Wireshark e realizar a análise offline:

* + 1. Digitar Analyse 🡪 Follow 🡪 TCP Stream (verificar o que está sendo observado).

Descreva e demonstre o que está sendo observado.

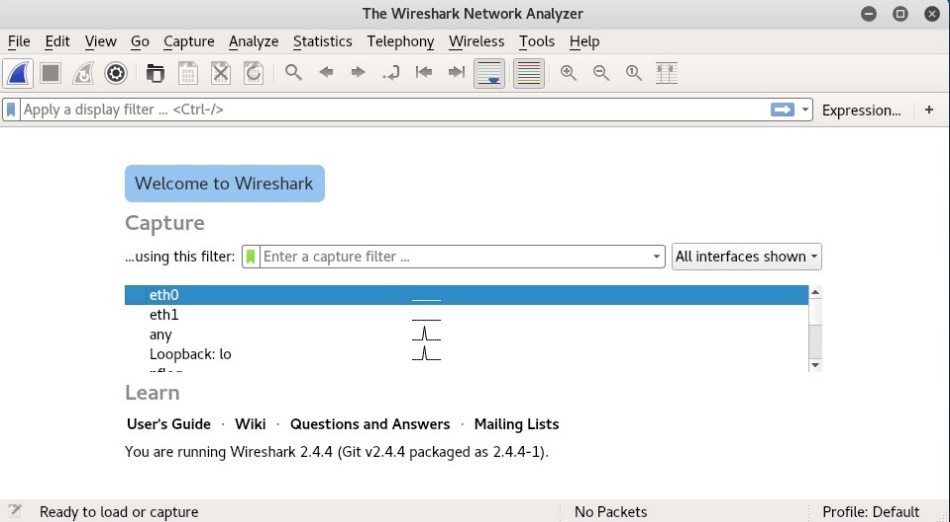
***Pode observar-se através do WireShark, que os nomes de usuário e senha utilizadas no site do Serviço DVWA foram obtidos, o que demonstra que mesmo o HTTP possui vulnerabilidades, já que o método POST mantém como puro texto.***

* + 1. Existe alguma vulnerabilidade nesse serviço? O que pode ser realizado para minimizar o problema pensando em um serviço mais seguro? Justifique.

***Sim, embora o método GET seja mais eficaz que os 2 serviços observados anteriormente, o método POST ainda permite a obtenção de dados que sejam utilizados em sites e serviços. Para minimizar esse problema o método POST teria de utilizar de uma criptografia de dados para que hackers não possam obter as informações por meio de programas como o WireShark.***

**Parte 5 – Captura de um tráfego SSH (Kali <-> Metasploitable):**

1. Para um cenário **SSH** deve-se acessar ao servidor **SSH (Metasploitable).** Considere o seguinte procedimento:
   1. No Kali iniciar a captura no Wireshark:

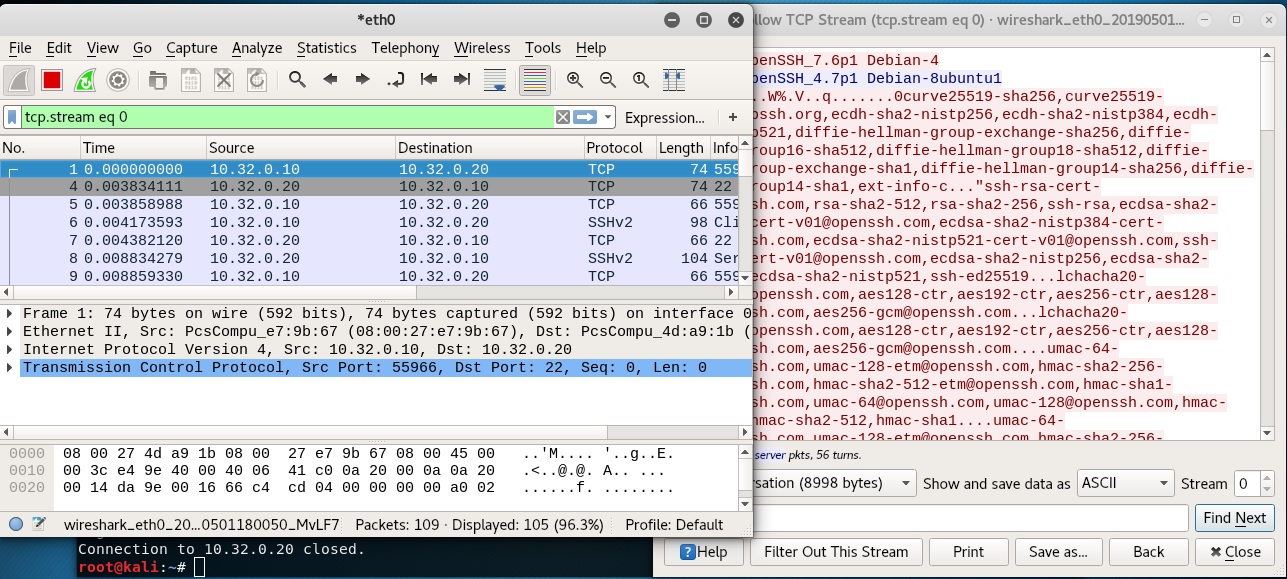
****

* 1. No Kali digitar **ssh usuario@IP** **(por exemplo, ssh msfadmin@192.168.56.20) ou usando o IP associado,** assim como a senha (**msfadmin**). Assim que estiver acessando o outro computador, digitar:

# ls

# ifconfig

# exit

* 1. Finalizar a captura no Wireshark e realizar a análise offline:
     1. Digitar Analyse 🡪 Follow 🡪 TCP Stream (verificar o que está sendo observado).
     2. Descreva e demonstre o que está sendo observado.

***Aos abrirmos a janela de análise do TCP Stream pelo WireShark, observa-se que não é encontrado texto puro mais, encontra-se uma mensagem de texto toda bagunçada o que indica que o texto passou por uma criptografia, e que os dados estão seguros.***

* + 1. Existe alguma vulnerabilidade nesse serviço? Esse serviço é considerado seguro? Justifique.

***O serviço é considerado Seguro, uma vez que o texto passa por uma criptografia, e ele não pode ser obtido por meio de programas como o WireShark. O serviço SSH é amplamente utilizado em serviços da Nuvem, demonstrando uma menor vulnerabilidade, já que os serviços em nuvem são bem populares entre os desenvolvedores WEB hoje em dia.***

**Referências:**

1. Wireshark:

[https://www.wireshark.org](https://www.wireshark.org/)

2. Telnet:

<https://en.wikipedia.org/wiki/Telnet>

<https://cmdref.net/os/linux/command/telnet.html>

3. FTP:

<https://en.wikipedia.org/wiki/File_Transfer_Protocol>

<https://www.howtoforge.com/tutorial/how-to-use-ftp-on-the-linux-shell/>

4. SSH:

<https://en.wikipedia.org/wiki/Secure_Shell>

<https://lzone.de/cheat-sheet/SSH>

<https://www.ssh.com/ssh/command/>