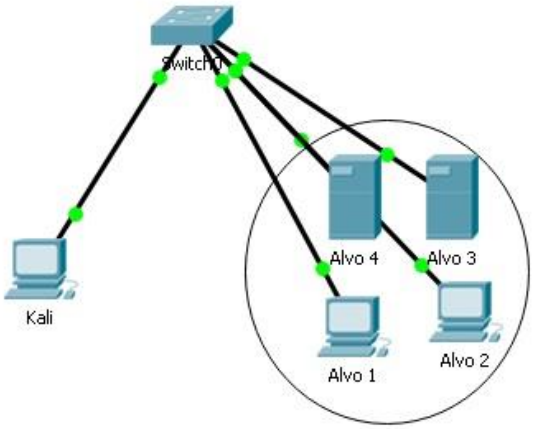
ATIVIDADE - USO DO WIRESHARK (SERVIÇOS DO METASPLOITABLE2):

Nome: Enzo Arrue

Topologia



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):

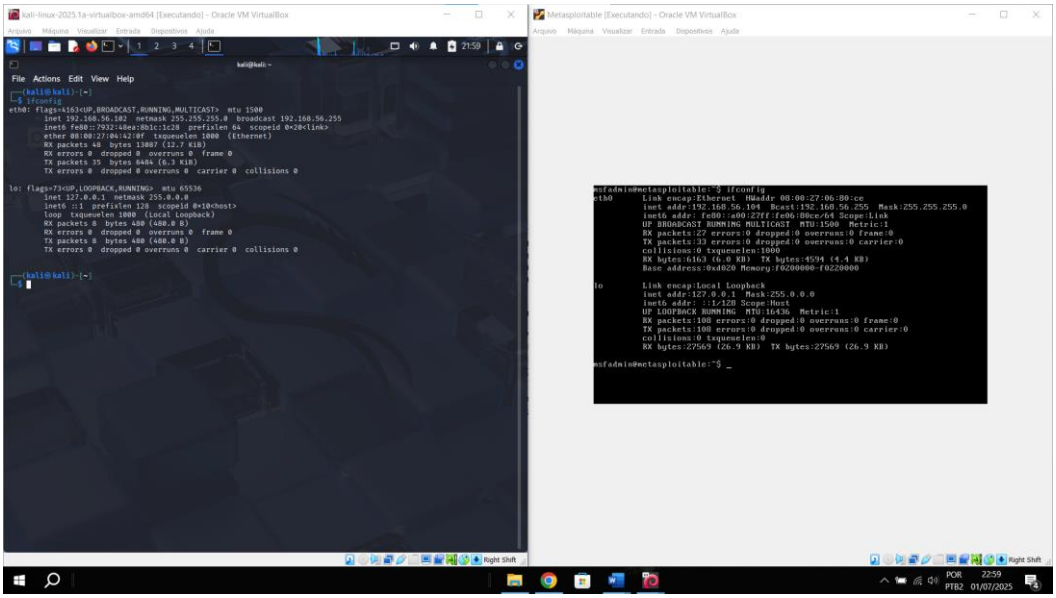
a. Configurando IP e Máscara (manual por linha de comando)
ifconfig -a // verificando todas as interfaces no sistema
ifconfig < interface > <IP > //configuração da rede no Linux
ifconfig eth0 10.32.0.10 netmask 255.255.255.0 //configuração de endereço IP 10.32.0.10 com a máscara 255.255.255.0 usando 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 ´

Tudo configurado em Host-Only 192.168.56.X;



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

1.1. Kali Linux para realização dos testes (vetor de ataque);
1.2. Uma máquina virtual Linux como alvo (Metasploitable2).

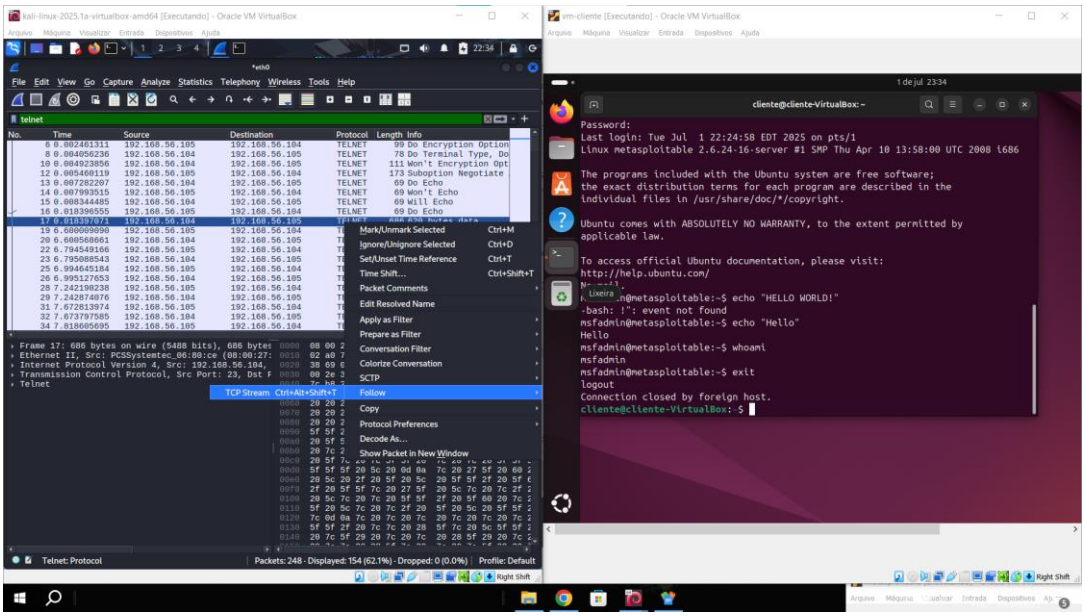
Parte 2 – Captura de um tráfego Telnet (Kali <-> Metasploitable):

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

2.1. Foi feita uma análise com wireshark no kali, observando a conexão via telnet entre uma VM Ubuntu e outra VM Metasploitable

No Ubuntu digitar **telnet IP (por exemplo, telnet 192.168.56.104),** assim como o nome de usuário e senha (**admin/admin**). Assim que estiver acessando o outro computador, digitar:

```
whoami
ls
echo “Hello World!”
```



Digitar Telnet → Follow → TCP Stream (verificar o que está sendo observado).

Descreva e demonstre o que está sendo observado.

No tráfego Telnet capturado, é possível observar que todos os dados trafegam em **texto simples (plain text)**. Isso significa que as **credenciais de login (nome de usuário e senha)** e todos os comandos digitados durante a sessão são visíveis e podem ser facilmente interceptados. No Wireshark, ao seguir o fluxo TCP (Analyse > Follow > TCP Stream), os comandos e respostas do servidor aparecem sem criptografia.

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

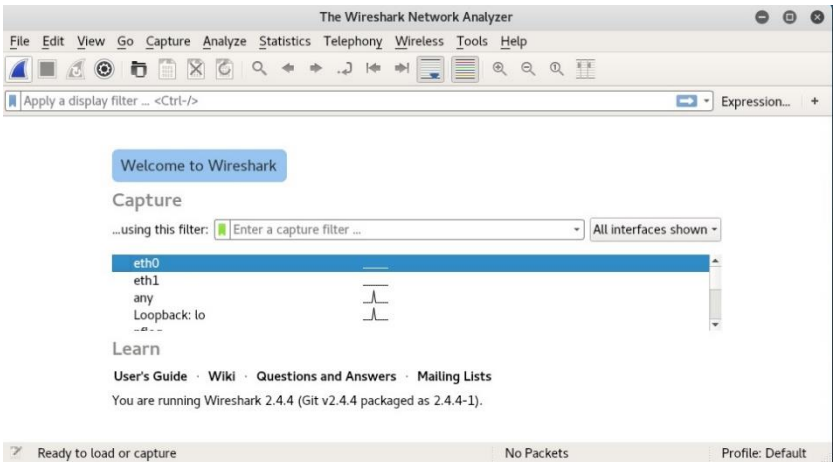
Sim, o Telnet apresenta uma vulnerabilidade crítica devido à **falta de criptografia**, o que permite que atacantes façam captura de pacotes e leiam credenciais e dados sensíveis. Para mitigar esse problema, recomenda-se utilizar o **SSH (Secure Shell)** em vez do Telnet, pois o SSH criptografa os dados transmitidos, garantindo maior segurança.

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

Os Ips são diferentes devido ter dado sequência em outro PC.

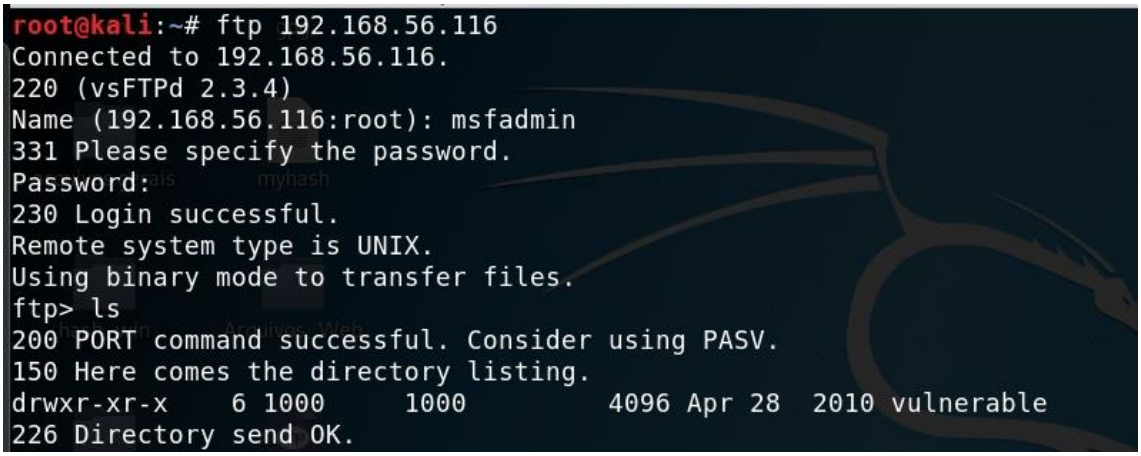
3. Para um cenário **FTP** deve-se acessar ao servidor **FTP (Metasploitable2)**. Considere o seguinte procedimento:

3.1. No Kali iniciar a captura no Wireshark:



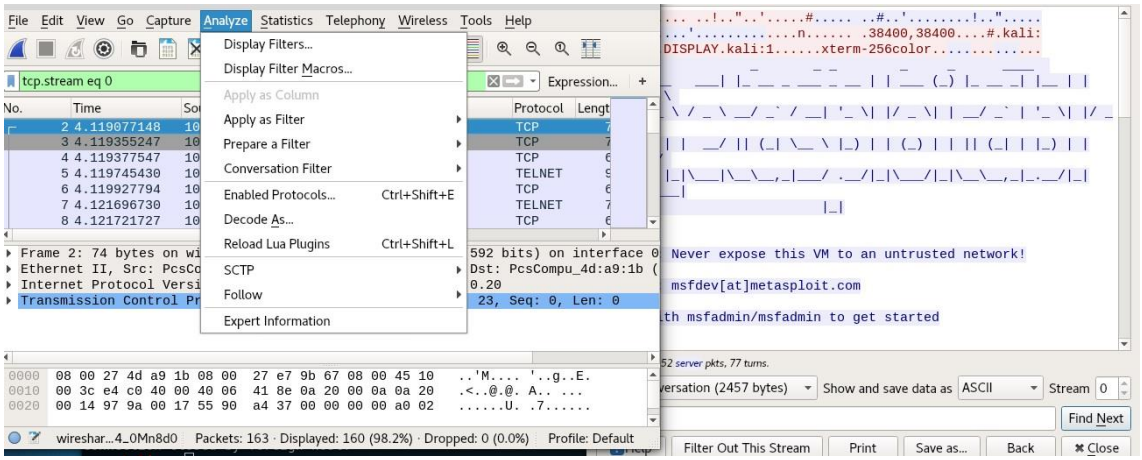
3.2. No Kali digitar **ftp IP (ftp 192.168.56.116),** assim como o nome de usuário e senha (**admin/admin**). Assim que estiver acessando o outro computador, digitar:

```
# ls
# pwd
# help
# exit
```



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

3.3.1. Digitar Analyse → Follow → TCP Stream (verificar o que está sendo observado).



3.3.2. Descreva e demonstre o que está sendo observado.
Durante a captura de tráfego FTP, nota-se que tanto as credenciais (usuário e senha) quanto os arquivos transferidos são transmitidos em texto simples. Isso torna o protocolo vulnerável a ataques de interceptação (man-in-the-middle). O Wireshark revela facilmente essas informações ao seguir o fluxo TCP.

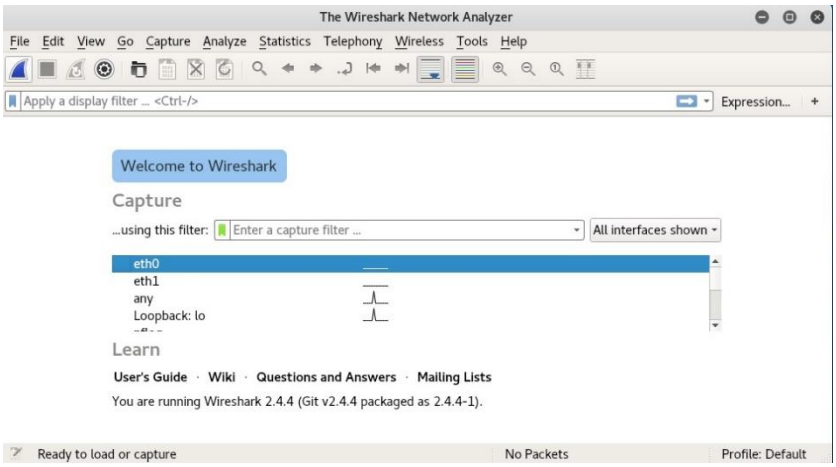
3.3.3. Existe alguma vulnerabilidade nesse serviço? O que pode ser realizado para minimizar o problema pensando em um serviço mais seguro? Justifique.

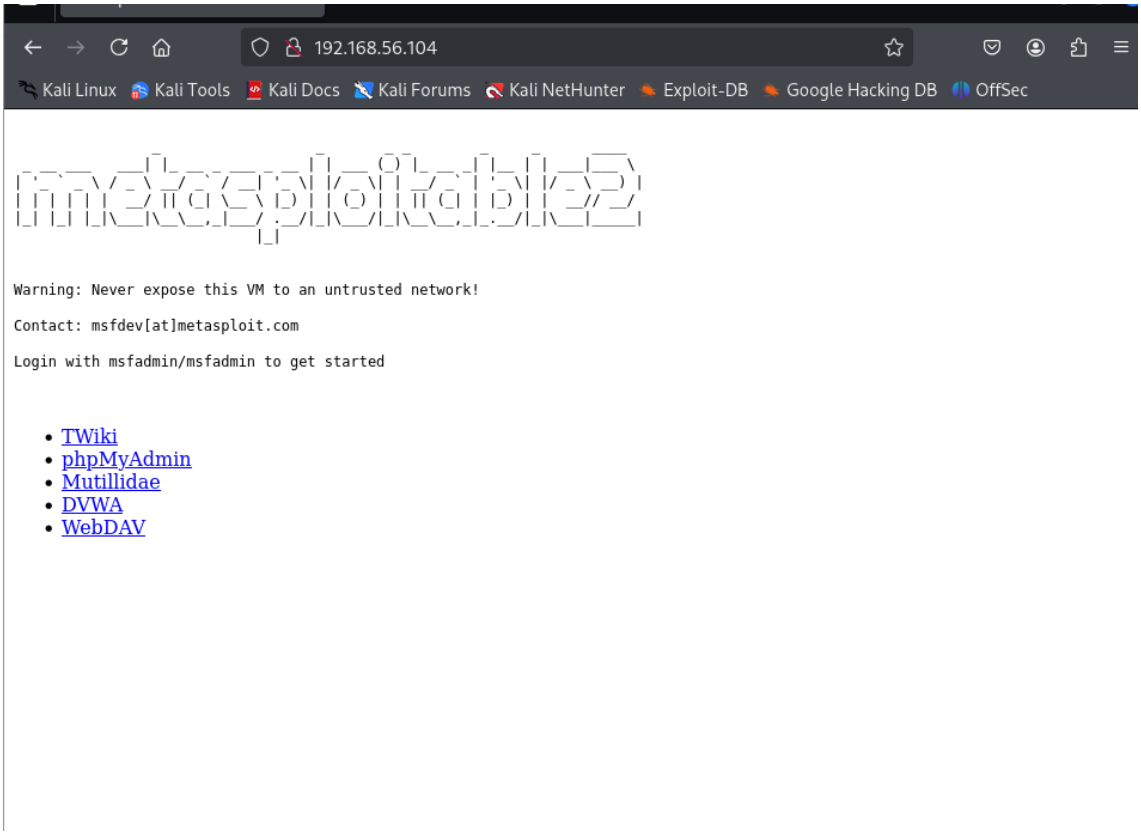
A principal vulnerabilidade do FTP é a falta de criptografia. Para um serviço mais seguro, recomenda-se utilizar o FTPS (FTP Secure) ou o SFTP (SSH File Transfer Protocol), que oferecem criptografia robusta para proteger os dados e as credenciais.

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

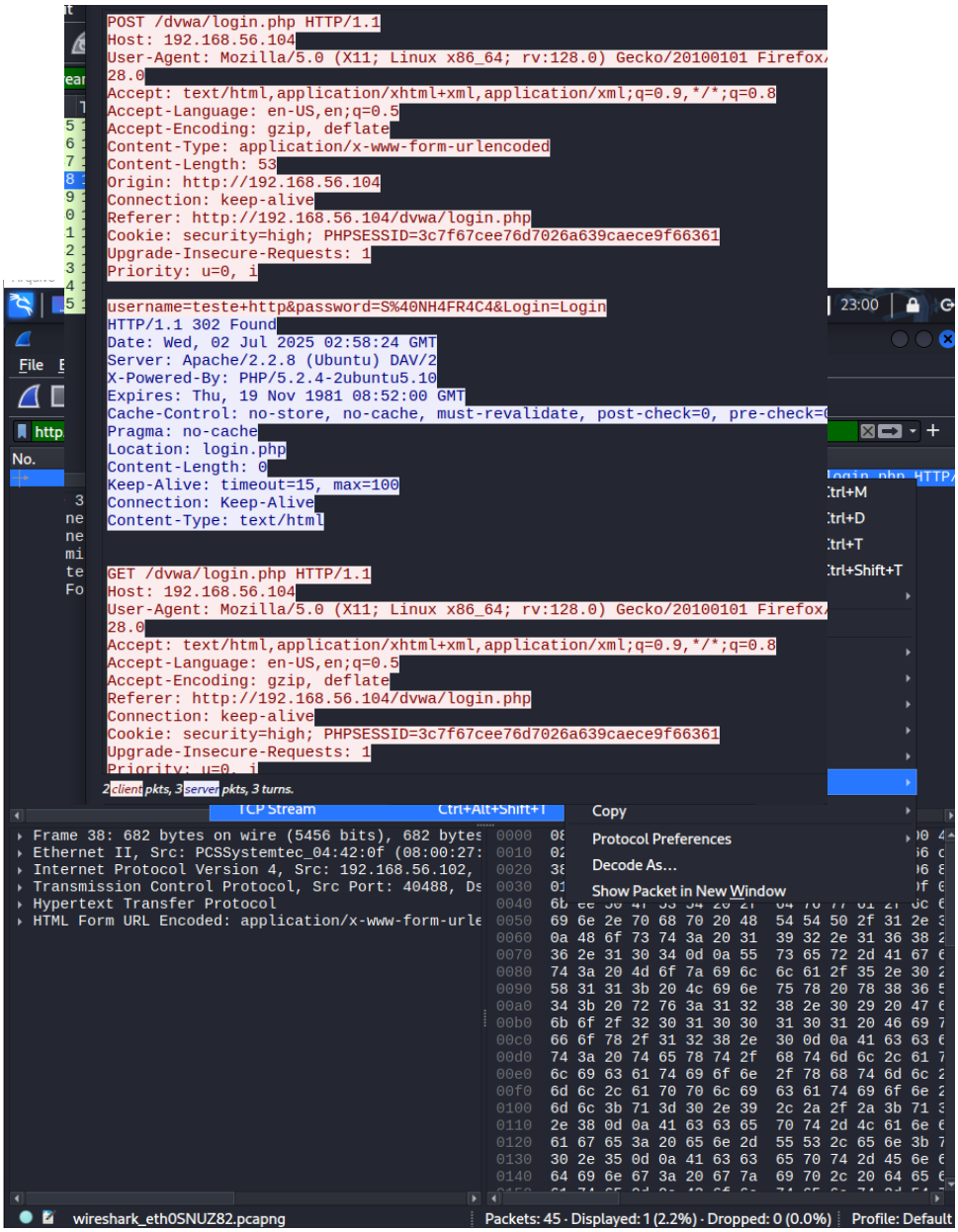
4. Para um cenário **HTTP** deve-se acessar ao servidor **HTTP (Metasploitable2)**. Considere o seguinte procedimento:
4.1. No Kali iniciar a captura no Wireshark:

4.2. No Kali (Firefox), acessar o browser do Metasploitable2 e o endereço IP, deve ser o endereço disponibilizado no modo host only ou no endereço IP configurado:





4.3. Acessar o serviço DVWA:
4.4. Finalizar a captura no Wireshark e realizar a análise offline:


POST /dvwa/login.php HTTP/1.1
Host: 192.168.56.104
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/
28.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: http://192.168.56.104
Connection: keep-alive
Referer: http://192.168.56.104/dvwa/login.php
Cookie: security=high; PHPSESSID=3c7f67cee76d7026a639caece9f66361
Upgrade-Insecure-Requests: 1
Priority: u=0, i
username=teste+http&password=S%40NH4FR4C4&Login=Login
HTTP/1.1 302 Found
Date: Wed, 02 Jul 2025 02:58:24 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=
Pragma: no-cache
Location: login.php
Content-Length: 0
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
GET /dvwa/login.php HTTP/1.1
Host: 192.168.56.104
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/
28.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.104/dvwa/login.php
Connection: keep-alive
Cookie: security=high; PHPSESSID=3c7f67cee76d7026a639caece9f66361
Upgrade-Insecure-Requests: 1
Priority: u=0, i
2 client pkts, 3 server pkts, 3 turns.
TCP Stream
Ctrl+Alt+Shift+T
Copy
Protocol Preferences
Decode As…
Show Packet in New Window
Frame 38: 682 bytes on wire (5456 bits), 682 bytes
Ethernet II, Src: PCSSystemtec_04:42:0f (08:00:27:
Internet Protocol Version 4, Src: 192.168.56.102,
Transmission Control Protocol, Src Port: 40488, Ds
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urle
wireshark_eth0SNUZ82.pcapng
Packets: 45 · Displayed: 1 (2.2%) · Dropped: 0 (0.0%)
Profile: Default

Descreva e demonstre o que está sendo observado.

O tráfego HTTP capturado mostra que os dados trafegam em texto simples, incluindo informações sensíveis, como cookies, credenciais e dados de formulários. Isso permite que qualquer interceptador visualize as informações trocadas entre o cliente e o servidor.

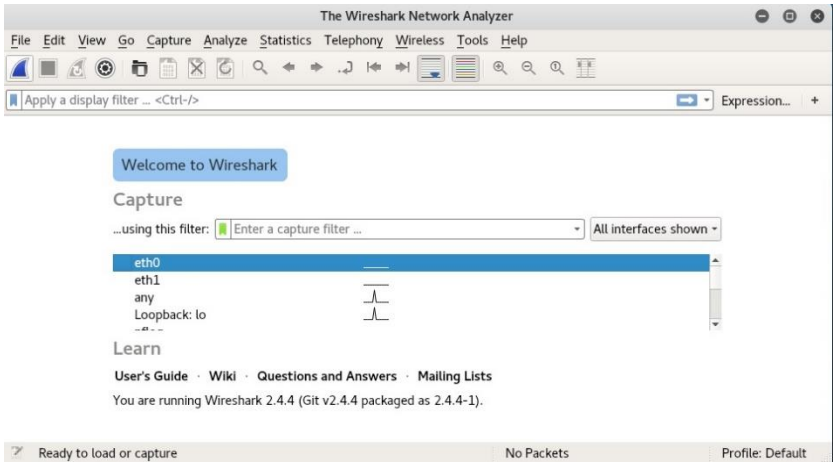
4.4.1. Existe alguma vulnerabilidade nesse serviço? O que pode ser realizado para minimizar o problema pensando em um serviço mais seguro? Justifique.

A vulnerabilidade do HTTP reside na ausência de criptografia, permitindo ataques de interceptação e roubo de informações. Para garantir a segurança, o recomendado é usar HTTPS (HTTP Secure), que utiliza o protocolo TLS/SSL para criptografar a comunicação.

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

5. Para um cenário **SSH** deve-se acessar ao servidor **SSH (Metasploitable).** Considere o seguinte procedimento:

5.1. No Kali iniciar a captura no Wireshark:

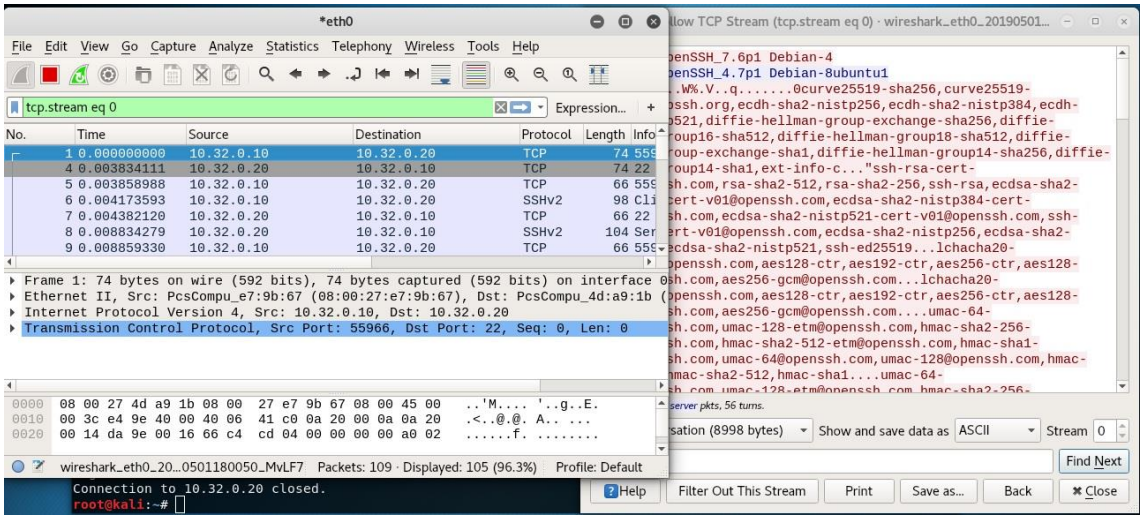


5.2. No Kali digitar **ssh usuario@IP (por exemplo, ssh msfadmin@192.168.56.20) ou usando o IP associado,** assim como a senha (**msfadmin**). Assim que estiver acessando o outro computador, digitar:

```
# ls
# ifconfig
# exit
```

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

5.3.1. Digitar Analyse → Follow → TCP Stream (verificar o que está sendo observado).



5.3.2. Descreva e demonstre o que está sendo observado.

No tráfego SSH capturado, é possível observar que os pacotes estão criptografados, mesmo ao seguir o fluxo TCP no Wireshark. Dessa forma, as credenciais e os comandos não são exibidos de forma legível, garantindo a confidencialidade dos dados.

5.3.3. Existe alguma vulnerabilidade nesse serviço? Esse serviço é considerado seguro? Justifique.

O SSH é considerado seguro justamente por utilizar criptografia robusta (geralmente RSA ou ED25519) para garantir a integridade e a confidencialidade da comunicação. No entanto, ainda podem existir vulnerabilidades relacionadas a chaves fracas ou más práticas de gerenciamento de credenciais, como senhas fracas ou reutilização de chaves.