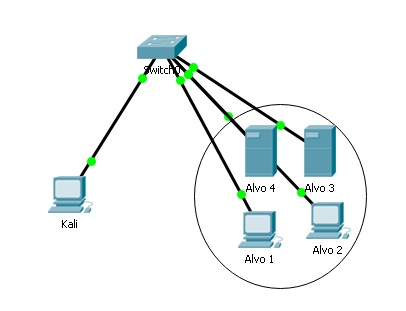
**ATIVIDADE - USO DO NMAP E WIRESHARK:**

**Nome: Igor Correa RA: 15.00588-7**

**Nome: Rodrigo Franciozi RA: 14.04014-0  
Nome: RA:**

1. Topologia
2. Objetivos

Parte 1: Preparando as máquinas virtuais

Parte 2: Praticar a execução da fase de scanning para coleta de informações

Parte 3: Captura e visualização de um tráfego Telnet

Parte 4: Captura e visualização de um tráfego SSH

**Formulário:**

**a. Configurando a Rede no Linux:**

a.1. 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 (a interface pode ser enp0s1 ou outras)

# 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

a.2. Iniciar/para/reiniciar o serviço:

# /etc/init.d/networking start

# /etc/init.d/networking stop

# /etc/init.d/networking restart

a.3. Habilitando/desabilitando interface de rede:

# ifconfig eth0 down

# ifdown eth0

# ifconfig eth0 up

# ifup eth0

**b. Usando o nmap:**

nmap 192.168.10.20 (escaneamento simples de portas e serviços)

nmap –sV 192.168.10.20 (descobrindo serviços TCP)

nmap –A 192.168.10.20 (descobrindo detalhes dos serviços)

nmap –O 192.168.10.20 (detectando o SO)

nmap –O –sV -p22 192.168.10.20 (descobrindo o serviço na porta 22 e detectando o SO)

nmap –O –sV -A 192.168.10.20 (descobrindo os serviços, detectando o SO e mostrando possíveis vulnerabilidades dos serviços)

**Parte I – Preparando as Máquinas Virtuais:**

* 1. Deve-se escolher 3 máquinas virtuais para teste (endereço de rede será substituído pelo RA), por exemplo, 12.00822-9 🡪 12.00.82.29 🡪 12.0.82.0 – endereço de rede). Os endereços IPs serão escolhidos valores que compreendem nessa faixa, por exemplo, 12.0.82.10, 12.0.82.20, 12.0.82.30 e a máscara será 255.255.255.0.
  2. Kali Linux para realização dos testes (vetor de ataque);
  3. Uma máquina virtual Linux como alvo (Metasploitable2).

**Parte 2 – Escaneamento de Portas com o nmap (Kali <-> Metasploitable):**

* 1. Quais portas estão abertas no host (escolher pelo menos 3 portas para analisar)?

**21, 22 e 23.**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Quais serviços estão rodando no host (escolher pelo menos 3 serviços para analisar)?

**FTP, SSH, TELNET.**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

* 1. **Acesse o link e identifique alguns serviços de http e telnet (usuários e senhas padrões dos roteadores):**

http://www.routerpasswords.com

* + 1. Selecione dois fabricantes e identifique os usuários e senhas que ocorrem com maior frequência.

**IBM🡪 usuário mais frequente é “admin” e a senha mais frequente é “admin”**

**CISCO🡪 usuário mais frequente é “amdin” e a senha mais frequente é “admin” e “cisco”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

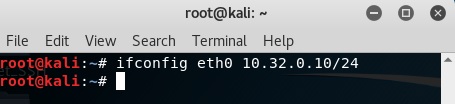
* + 1. O que deve ser evitado nos roteadores usados pelos fabricantes? Justifique.

**Deve ser evitado manter as senhas padrões que vem nos roteadores, pois facilita muito se um hacker tentar entrar na sua rede.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

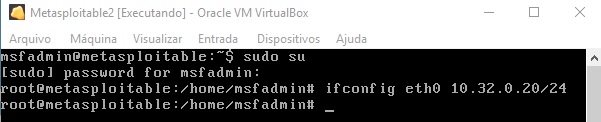
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

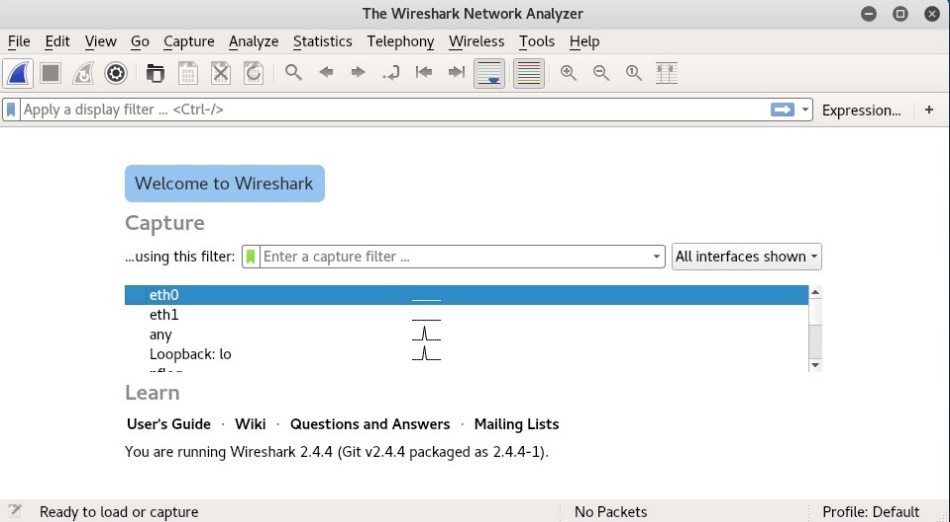
* 1. **Para um cenário Telnet deve-se acessar ao servidor Telnet (Metasploitable2). Considere o seguinte procedimento:** 
     1. Configurando a rede no Kali (Vetor de ataque):



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



* 1. No Kali iniciar a captura no Wireshark:

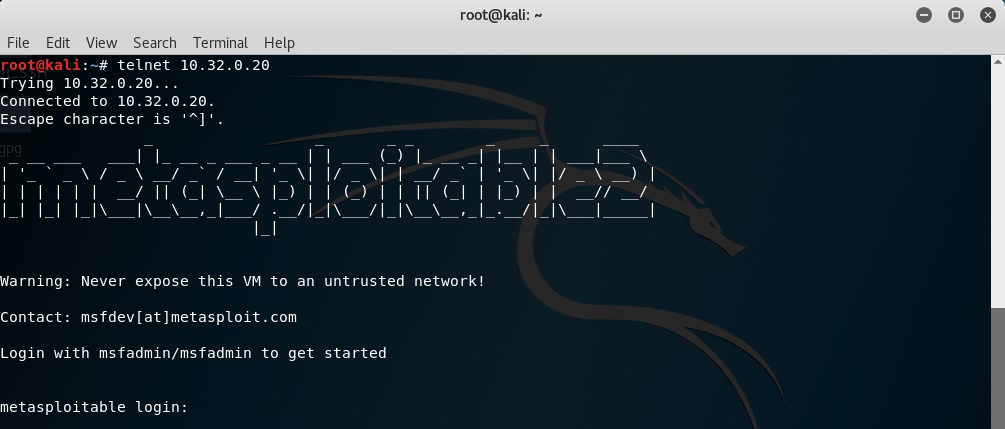
****

* 1. No Kali digitar **telnet IP** **(telnet 10.32.0.20),** assim como o nome de usuário e senha (**admin/admin**). Assim que estiver acessando o outro computador, digitar:

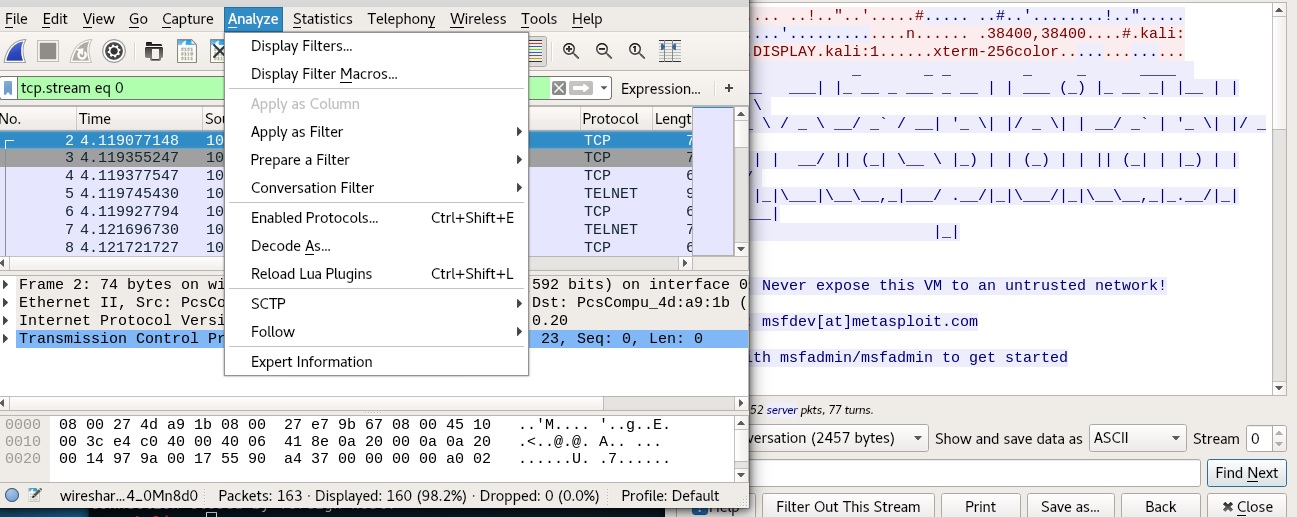
# ls

# 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).



* + 1. Descreva o que está sendo observado.

**Está mostrando todos os comandos e informações que foram digitadas e recebidas no terminal da máquina que está conectando no host.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

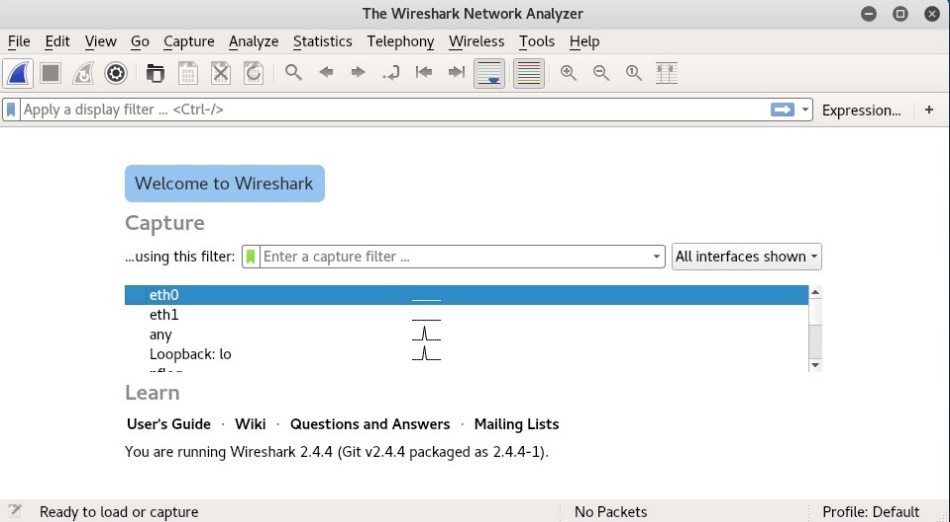
* + 1. Existe alguma vulnerabilidade nesse serviço? O que pode ser realizado para minimizar o problema pensando em um serviço mais seguro? Justifique.

**Sim, as informações passadas não são criptografadas de nenhuma forma, é enviada em texto puro, logo, uma forma de melhorar isso, é criptografar as mensagens antes de mandar.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Parte 4 – Captura de um tráfego SSH com Wireshark (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:

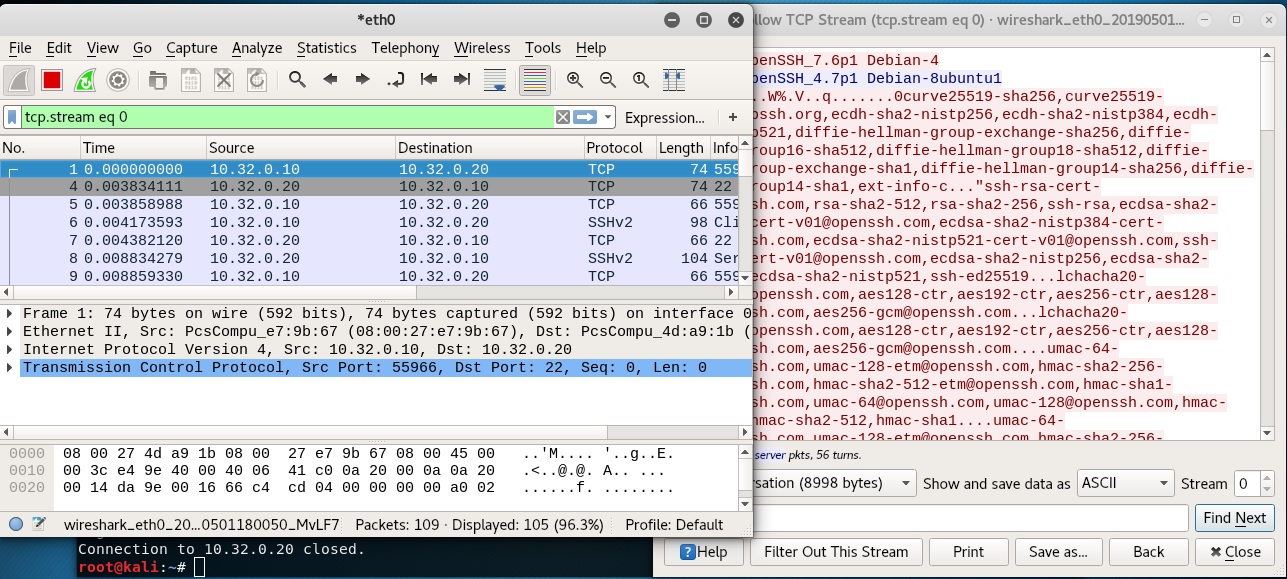
****

* 1. No Kali digitar **ssh usuario@IP** **(ssh msfadmin@10.32.0.20) 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 o que está sendo observado.

**Está mostrando todos os comandos e informações que foram digitadas e recebidas no terminal da máquina que está conectando no host.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

**Sim, existe vulnerabilidade, e ele não é considerado seguro, pois ele passa as informações sem nenhuma criptografia.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Referências:**

1. Nmap:

https://nmap.org

1. Wireshark:

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