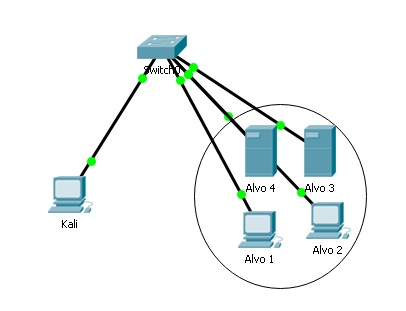
**LABORATÓRIO E ATIVIDADE - CONFIGURANDO SERVIDOR SSH E SFTP:**

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: Preparar as máquinas virtuais

Parte 2: Configuração do Servidor SSH e SFTP

Parte 1 – Preparando as Máquinas Virtuais:

* 1. Escolher o modo **host-only** as duas máquinas virtuais;
  2. Kali Linux para realização dos testes;
  3. Uma máquina virtual Linux como alvo (Metasploitable2).

**Parte 2 – Testes na Máquina Linux (Kali <-> Metasploitable2) – Serviço SSH e SFTP:**

* 1. **1.** Verificar com o nmap os serviços:

nmap IP (usar o endereço IP que estiver disponível no modo Host Only)

**Texto branco sobre fundo preto

Descrição gerada automaticamente**

* + 1. Alterando a porta no servidor (Metasploitable2).

nano /etc/ssh/sshd\_config //editando as configurações no servidor SSH

Ctr+O+enter // salvando

Ctr+W // fechar a edição

Alterando a para **4444**.

* + 1. Configurar o parâmetro **MaxAuthTries 5** no servidor SSH (Metasploitable)
    2. Acessando usuários **msfadmin, user, service**. Desabilitar esses usuários?
    3. Criando um usuário no servidor (criar o usuário com o nome de um dos componentes do grupo - **nome\_usuario**) para conexão via chave pública:

Verificar o usuário que foi criado com o comando no servidor:

cat /etc/passwd

* + 1. Criando o par de chaves (chave pública e chave privada) no Kali e comprovando o envio da chave pública no servidor:

ssh-keygen -t rsa –b 4096 // gerando o par de chaves

ls -l /root/.ssh// verificando o par de chaves

cat /root/.ssh/id\_rsa.pub // visualizando a chave pública

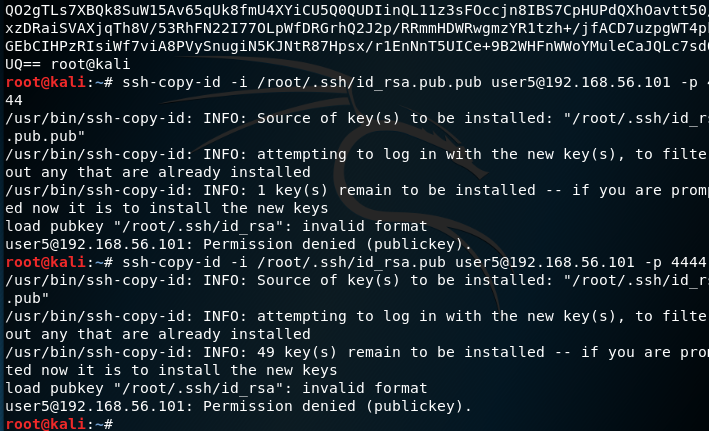
ssh-copy-id -i /root/.ssh/id\_rsa.pub nome\_usuario@192.168.56.116-p 4444 **//** enviando a chave pública para o servidor

cat .ssh/authorized\_keys // verificando a chave pública no servidor

* + 1. Configurando o servidor com a opção **AllowUsers nome\_usuario** (nome de usuário criado no servidor

ssh nome\_usuario@192.168.56.116 -p 4444 // conectando com o usuário criado

* + 1. Gerar os prints de tela comprovando as configurações.



* + 1. Quais as principais vantagens de se usar o serviço ssh se comparado ao serviço telnet? Justifique.

***O Serviço SSH é criptografado, enquanto o Telnet não é sendo assim o Telnet é mais vulnerável do que os Serviços do SSH, justificando a escolha do SSH como mais interessante.***

* + 1. Quais as principais configurações realizadas para garantir uma maior segurança no servidor SSH? Justifique.

***Mudar a porta do serviço SSH, ajustar o numero de tentativas, verificar chaves publicas e permitir usuários em especifico, entre outros fatores que fazem com que dificulte o acesso ao Servico SSH em específico.***

* 1. **Testando o servidor SFTP:** 
     1. Iniciar o Wireshark no Kali e na sequência acessar o serviço SFTP:

sftp -P 4444 nome\_usuario@IP // conectando com o usuário criado na porta 4444

* + 1. Finalizar a captura no Wireshark e realizar a análise offline:

Digitar Analyse 🡪 Follow 🡪 TCP Stream (verificar o que está sendo observado). Realizar o print da tela.



* + 1. Confronte o serviço ftp X sftp. Quais as principais vantagens do sftp se comparado com o ftp? Justifique.

***Os Dados do Serviço SFTP são criptografados, enquanto os serviço FTP não é. Fazendo com que o Serviço SFTP seja uma escolha mais interessante para utilizar em relação as FTP por questões de segurança.***

* + 1. Compare alguns desafios e particularidades das equipes de Pentest e Analista de Segurança nas empresas.

***Os profissionais que trabalham com Segurança Cibernética das empresas precisam configurar seus serviços onlines, nuvem, locais entre outros de maneira segura, utilizando sempre protocolos que utilizam de criptografia de dados, para manter a integridade dos dados a serem transportados***

**Referências:**

1. RFC4250 e RFC4256. The Secure Shell (SSH). Disponível em: [https://www.ietf.org/rfc/rfc4250.txt  
https://www.ietf.org/rfc/rfc4256.txt](https://www.ietf.org/rfc/rfc4250.txthttps://www.ietf.org/rfc/rfc4256.txt%20)