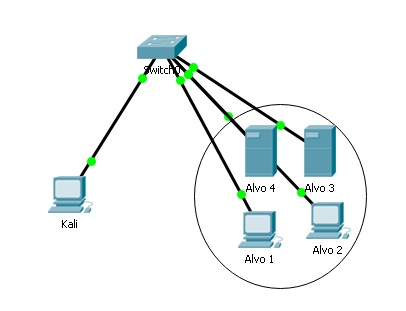
**ATIVIDADE DE COLETA DE INFORMAÇÕES – SCANNER DE PORTAS (NMAP OU ZENMAP):**

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

****

1. Objetivos

Parte 1: Praticar a execução da fase de scanning para coleta de informações (nmap ou zenmap)

Formulário:

nmap –sV 192.168.10.20 (descobrindo serviços TCP)

nmap –sU -T5 192.168.10.20 (UDP com escaneamento rápido)

nmap –sU -p 161 192.168.10.20 (UDP com descobrimento de serviços)

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 -p22 192.168.10.20 (descobrindo o serviço na porta 22, detectando o SO e mostrando possíveis vulnerabilidades do serviço)

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

nmap –T4 –A –v 192.168.56.0/24 (descobre os detalhes dos SOs e serviços com visualização e responde rapidamente)

Uma imagem contendo captura de tela

Descrição gerada automaticamente

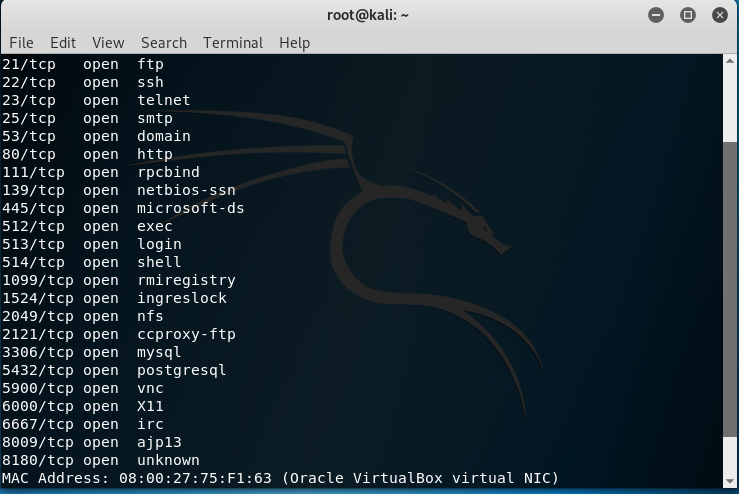
Figura 1: Captura com Zenmap.

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

* 1. Pode-se usar o serviço do Host Network Manager e placas de rede Host-Only (VirtualBox);
  2. Kali Linux para realização dos testes (vetor de ataque);
  3. Uma máquina virtual Windows como alvo (Windows 7);
  4. Uma máquina virtual Linux como alvo (máquina vulnerável a ser escolhida por grupo).

**Parte II – Resolução do Laboratório:**

1. Com a rede montada deve-se realizar os testes (escolher pelo menos 3 serviços para serem analisados em cada sistema operacional), captura de telas e geração de um relatório respondendo as seguintes questões:
   1. Quais foram os hosts detectados?





* 1. Quais portas estão abertas em cada host (escolher pelo menos 3 portas para analisar em cada sistema operacional)?

***Metasploitable –***

***Porta 21/tcp – ftp***

***Porta 22/tcp - ssh***

***Porta 23/tcp - telnet***

***Windows 7 –***

***Porta 135/tcp – msrpc***

***Porta 139/tcp – netbios-ssn***

***Porta 445/tcp – Microsoft-ds***

* 1. Quais serviços estão rodando em cada host (escolher pelo menos 3 serviços para analisar)?

***Metasploitable –***

***ftp – vsftpd***

***ssh – OpenSSH***

***telnet - linux Telnet***

***Windows 7 –***

***Msrpc – Microsoft Windows RPC***

***netbios-ssn – Microsoft Windows Netbios-ssn***

***Microsoft-ds – Windows 7 Professional 7600 microsoft-ds***

* 1. Qual sistema operacional possivelmente está rodando em cada host?

***No metasploitable, possivelmente estão rodando em alguma versão Linux.***

******

***Enquanto o Windows 7 possivelmente esteja rodando em alguma versão do sistema operacional Windows 7.***

**Referência:**

Nmap: <https://nmap.org/>

Zenmap: <https://nmap.org/zenmap/>