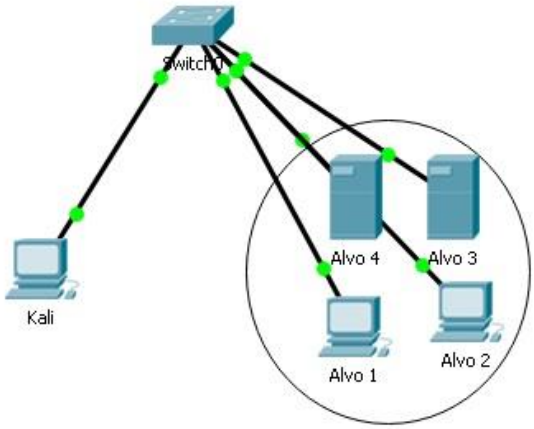
ATIVIDADE DE COLETA DE INFORMAÇÕES – SCANNER DE PORTAS (NMAP OU ZENMAP):

Nome: Enzo Arrue



Objetivos

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

Parte I – Preparando as Máquinas Virtuais:

1. Pode-se usar o serviço do Host Network Manager e placas de rede Host-Only (VirtualBox);

1.1. Kali Linux para realização dos testes (vetor de ataque);

1.2. Uma máquina virtual Linux como alvo (Metasploitable2).

Ambas redes já configuradas em host-only.

Parte II – Resolução do Laboratório:

2. Com a rede montada deve-se realizar os testes (escolher pelo menos 3 serviços para serem analisados na máquina analisada):

2.1. Quais portas e serviços estão abertas na máquina analisada (escolher pelo menos 3 portas para analisar)?

```
└─$ nmap 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 13:51 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:06:80:CE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

2.2. Quais as versões dos serviços escolhidos na máquina analisada?

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -sV -O -p 21,22,80 192.168.56.104

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 14:03 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00071s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
MAC Address: 08:00:27:06:80:CE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.71 ms 192.168.56.104

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.93 seconds
```

2.3. Qual o sistema operacional possivelmente está rodando na máquina analisada?

Trecho obtido do nmap

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 – 2.6.33