Instituto Federal de Educação, Ciência e Tecnologia do RN
Câmpus Currais Novos
Curso: Tecnologia em Sistemas para Internet
Disciplina: Segurança e Preservação de Dados

Atividade Prática em Laboratório (Roteiro) :: Port Scan (Varredura de Portas)

A atividade consiste em proporcionar ao aluno o contato com a técnica de varredura de portas utilizando a ferramenta NMAP (em ambiente controlado)

1) Baixe o contêiner que será usado para fazer a varredura (docker Linux com Nmap instalado).

```
docker pull ricardokleber/rk_debian12:latest
```

2) Baixe o contêiner que será usado como alvo (docker com o sistema metasploitable2)

```
docker pull ricardokleber/metasploitable2:latest
```

3) Crie um diretório para utilizar nesta prática

```
$ mkdir scan01
```

4) Entre no diretório onde colocará o arquivo de configurações dos contêineres

```
$ cd scan01
```

5) Baixe o arquivo de configuração dos contêineres

```
$ wget https://www.segurancaderedes.com.br/spd/pratica02/docker-compose.yml
```

6) Execute o docker compose para iniciar os contêineres

```
$ docker compose up -d
```

7) Entre no contêiner scan01 via console (executando uma shell bash)

```
$ docker exec -it scan01 bash
```

8) Verifique se o docker scan01 acessa (ping) o docker alvo01

```
$ ping 172.30.0.101
```

9) Realize a varredura de portas padrão do nmap para verificar o número de portas abertas no alvo01

```
$ nmap 172.30.0.101
```

10) Realize agora a varredura de portas do nmap para verificar o número de portas abertas no alvo01 em todas as portas do alvo

```
$ nmap -p- 172.30.0.101
```

11) Utilize agora o nmap individualmente nas portas abertas encontradas para confirmar cada serviço em execução e tentar identificar as versões de cada um deles

```
$ nmap -sT -p 21 -sV 172.30.0.101
```

12) Utilize agora o módulo ‘scripts’ do nmap para verificar se o serviço em execução na porta 21 está vulnerável.

```
$ nmap -sT -p 21 -sV 172.30.0.101 -script=vuln
```