Varreduras de rede

Cassiano Peres

DIO Tech Education Analyst

cassiano-dio

peres-cassiano

Objetivo Geral

Neste curso vamos mapear a nossa rede, encontrando dispositivos e portas abertas.

Pré-requisitos

Conhecimento prévio em linhas de comando Linux facilita o aprendizado.

Percurso

Etapa 1 O que é varredura de rede?

Etapa 2 Encontrando dispositivos com NMap

Etapa 3 Encontrando portas abertas com NMap

Percurso

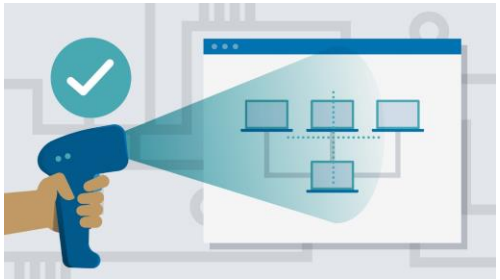
Etapa 4 Varrendo a rede com o Shodan

Etapa 1

O que é varredura de rede?

Introdução

Nesta aula vamos conhecer o que são as varreduras (ou *scan*) de rede e seus perigos relacionados.



Varreduras de rede

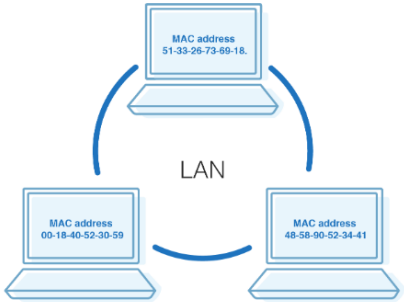
É uma técnica de busca minuciosa em redes, com o objetivo de identificar computadores ativos e coletar informações como, serviços disponibilizados e programas instalados.

Varreduras de rede

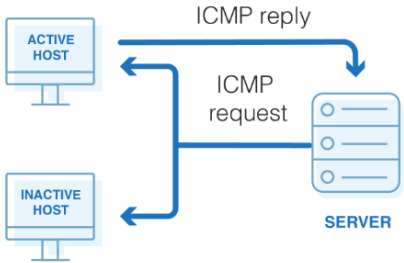
A Network Scan:

1 Discovers active hosts on the network

2 Uses Address Resolution Protocol (ARP) at the subnet level



3 Or uses Internet Control Message Protocol (ICMP) for a wider reach



Tipos de varreduras

- **Portas**: listar portas e serviços;
- **Redes**: listar endereços de IP;
- **Vulnerabilidades**: listar vulnerabilidades conhecidas.

Técnicas de varreduras

- **ICMP;**
- **TCP;**
- **UDP.**

Varredura e enumeração

A etapa de **varredura** busca encontrar as vulnerabilidades, sem maiores detalhes, enquanto a etapa de **enumeração** traz mais detalhes a respeito do sistema invadido.

Conclusão

Nesta aula exploramos a teoria por trás da varredura e enumeração em redes de computadores.

Etapa 2

Encontrando dispositivos com NMap

Introdução

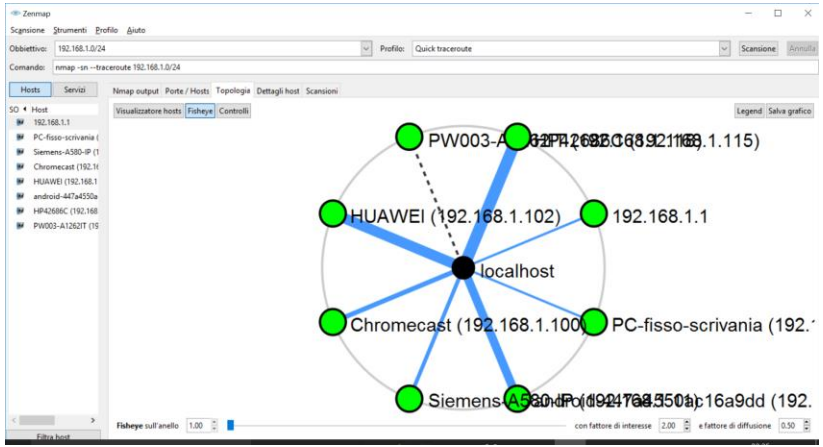
Nesta aula vamos aprender a mapear dispositivos conectados a uma rede utilizando o Nmap.

Nmap

É uma ferramenta gratuita e de código aberto usada para busca de vulnerabilidades, varredura de portas e mapeamento de rede.

Nmap

Possui versões com UI (Zenmap) e CLI.




```
[vivek@nixcraft-wks01 ~]$ sudo nmap -F 192.168.2.254
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 21:13 IST
Nmap scan report for router (192.168.2.254)
Host is up (0.00027s latency).
Not shown: 96 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 00:08:A2:0D:05:41 (ADI Engineering)

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
[vivek@nixcraft-wks01 ~]$
```

Nmap

O coração do Nmap é a varredura de portas, onde os usuários designam uma lista de alvos em uma rede sobre os quais desejam obter informações.

Prática

Vamos instalar e testar o Nmap para varreduras em nossa rede.

Etapa 3

Encontrando portas abertas com NMap

Introdução

Após a busca de dispositivos em nossa rede, vamos econtrar as portas disponíveis.

Técnicas

- **ICMP;**
- **TCP;**
- **UDP.**

Varredura com NMap

```
root@ubuntu:~# nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-25 14:14 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.071s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91f
f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
root@ubuntu:~#
```

Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)