Varredura

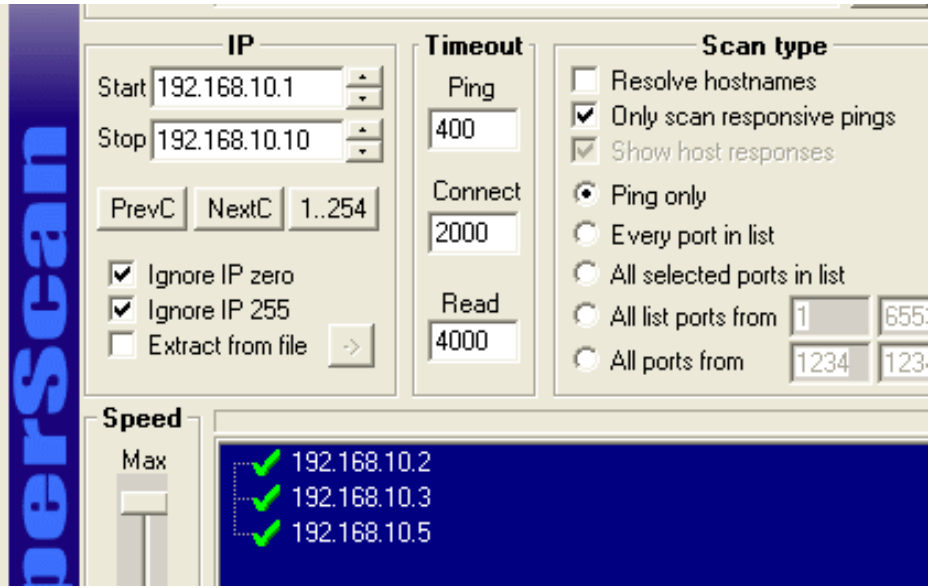
Marcos Flávio Araújo Assunção

Fundamentos de Ethical Hacking

Etapas da Varredura

- Varredura de hosts (endereços IP) na rede
- Varredura de portas (serviços ativos)

Varredura de IPs



- Tem como objetivo descobrir as máquinas ativas da rede
- Ping Sweep
- Softwares: **ping, hping3, nmap (-sV), superscan, etc.**

Varredura de portas

```
root@kali:~# nmap -sn -n 192.168.1.0/24 | grep 192
Nmap scan report for 192.168.1.1
Nmap scan report for 192.168.1.102
Nmap scan report for 192.168.1.109
Nmap scan report for 192.168.1.111
Nmap scan report for 192.168.1.112
Nmap scan report for 192.168.1.107
```

- Exemplo de Ping Sweep com NMAP, filtrando resultado com grep

Varredura de portas

```
C:\>nmap 192.168.10.2

Starting Nmap 4.85BETA3 ( http://nmap.org ) at 201
Brasil
Interesting ports on servidor.falsaempresa.com.br
Not shown: 983 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
```

- Tem como objetivo identificar os serviços ativos no sistema
- Softwares usados: NMAP, Superscan, etc.
- Tipos de varredura: Full, Half-Syn, FIN, ACK, XMAS, NULL, UDP,