OS Fingerprinting

~~~~~~

Identificando o Sistema Operacional

~~~~~~

+ Existem várias técnicas para se identificar o sistema operacional, c como:

→ TTL: Cada sistema operacional utiliza um padrão de TTL

- Windows = 128
- Linux = 64
- FreeBSD = 64
- Solaris = 255
- Cisco = 254

→ Análise de Serviços (Remote Desktop [3389] / SSH [22] / Webserver)
→ Implementação da Pilha TCP/IP
→ Enumeração de Serviços Identificados
→ NMAP -O / -A

~~~~~~

+ Os testes de TTL podem ser feitos por meio do seguinte comando

```
for i in $(seq 1 254); do ping -c1 -w1 172.16.1.$i; done
| grep "64 bytes"
```

→ Ao visualizarmos a resposta, o normal é que os TTLs estejam próximos dos esperados para os sistemas operacionais padrão

+ A análise de serviços pode se dar pelos filtros dos arquivos que aprendemos a montar nas aulas passadas
Ex: IIS indica serviço Windows
→ Um grep "Terminal" pode indicar em quais portas está rodando um Microsoft Terminal

+ Para tentar fazer um acesso remoto ao sistema, podemos utilizar a ferramenta rdesktop:

```
rdesktop 172.16.1.140
```

+ Uma outra maneira de procurar identificar o OS (Operational System) é por meio do nmap:

```
nmap -v -O 172.16.1.140 -Pn
```

+ Vale lembrar que todas essas saídas podem ser manipuladas para enganar um atacante.
→ Para editar o tttl, podemos executar:

```
echo "128" > /proc/sys/net/ipv4/ip_default_ttl
```
~~~~~~