Essa atividade representa a tarefa do quadro Análise do Servidor - Nmap

Data: 09-04-16

Horário dos testes: 30 min

Horário Total: 1 h

**Objetivo:** Utilizar a ferramenta Nmap para descobrir quais portas do servidor

estão abertas e que tipo de atividade pode ser desenvolvida a partir disso.

**Ferramenta:** Nmap é um scanner de portas automatizado que consegue fazer a detecção de portas abertas e o tipo de aplicação rodando no momento em um servidor web.

**Resultados**

**Tentativa 1:**

*comando nmap -Ss -O 192.168.0.58*

1. -Ss é para a ferramenta tentar fazer o scan SYN do tcp.
2. -O é para a ferramenta tentar encontrar o S.O. rodando no momento
3. 192.168.0.58 é o IP onde está hospedada a aplicação.

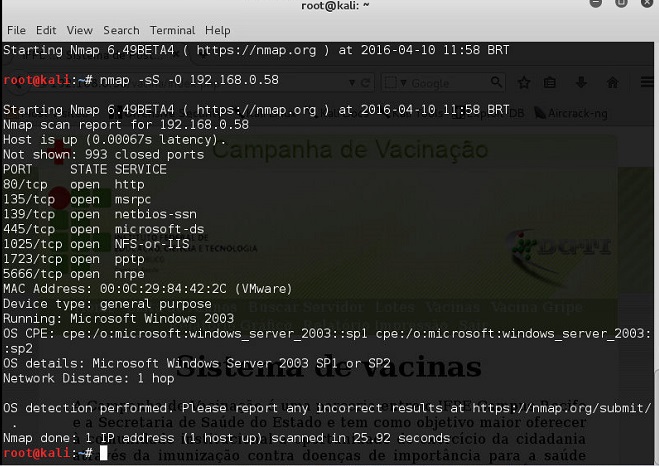
**Resultado:** Erro na ferramenta.

**Tentativa 2:**

*comando nmap -sS -O 192.168.0.58*

1. -sS é para a ferramenta tentar fazer o scan SYN do tcp.
2. -O é para a ferramenta tentar encontrar o S.O. rodando no momento.
3. 192.168.0.58 é o IP onde está hospedada a aplicação.

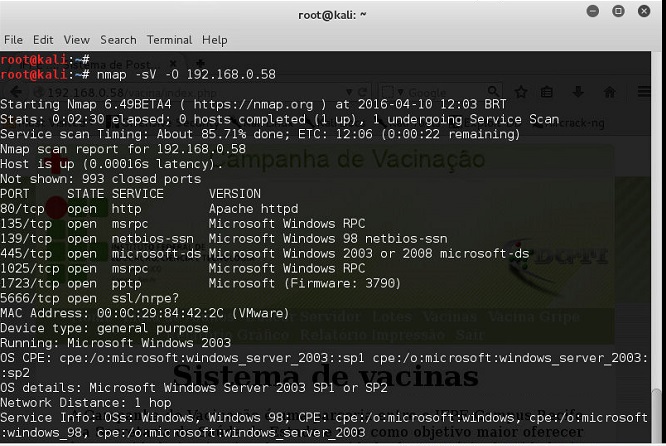
**Resultado:**



**Tentativa 3:**

*comando: nmap -sV -O 192.168.0.58*

1. -sV é para realizar o SYN e buscar a versão do software rodando no momento.
2. -O é para a ferramenta tentar encontrar o S.O. rodando no momento.
3. 192.168.0.58 é o IP onde está hospedada a aplicação.



Serviços:

Microsoft Windows RPC - Ferramenta semelhante ao TeamViewer que conecta o computador criando um esquema de servidor - cliente.

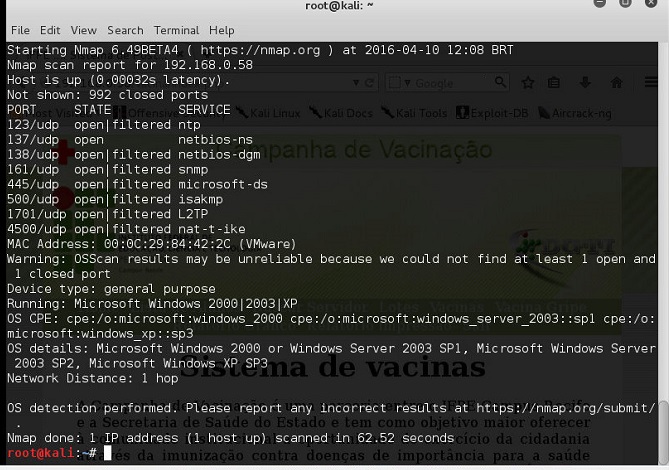
Microsoft Windows microsoft-ds - Ferramenta que auxilia a implantação de imagens em uma distribuição windows.

**Tentativa 4:**

*comando nmap -sU -O 192.168.0.58*

1. -sU é para usar o detector de portas UDP.
2. -O é para a ferramenta tentar encontrar o S.O. rodando no momento.
3. 192.168.0.58 é o IP onde está hospedada a aplicação.

**Resultado:**



Serviços:

ntp - protocolo de sincronização de relógios usando udp

netbios-ns - responsável pelo registro de nomes de aplicação do NetBios

netbios -dgm - serviço de datagrams do NetBios

snmp - gerenciamento de redes.

microsoft-ds - protocolo windows para compartilhamento e impressões de arquivos

isakmp -

L2TP - protocolo de encapsulamento de camada 2, para criar redes vpn privadas.

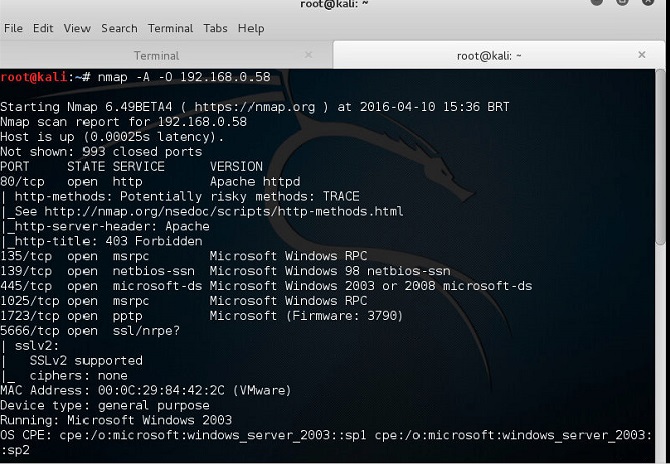
nat-t-like - protocolo de tradução de ips

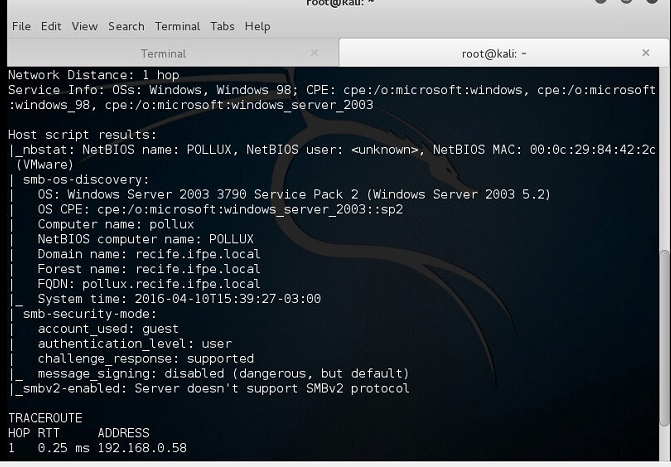
**Tentativa 5:**

*nmap -A -O 192.168.0.58*

1. -A é para usar o tracerouter na requisição.
2. -O é para descobrir o S.O. rodando no momento.
3. 192.168.0.58 é o IP onde está hospedada a aplicação.

**Resultado:**



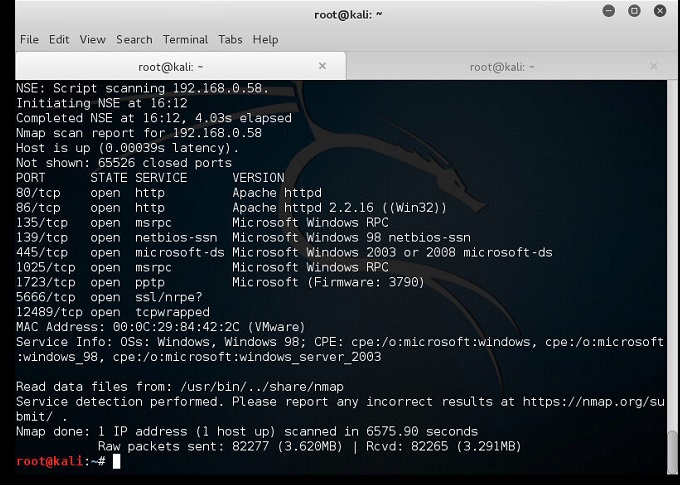


**Tentativa 6**

*nmap -sV -p 1-65535 -O 192.168.0.58*

1. -sV é para realizar o SYN e buscar a versão do software rodando no momento
2. -p para indicar quais portas devem ser usadas no teste, o delimitador é “-”
3. -O é para a ferramenta tentar encontrar o S.O. rodando no momento.
4. 192.168.0.58 é o IP onde está hospedada a aplicação.

**Resultado:**

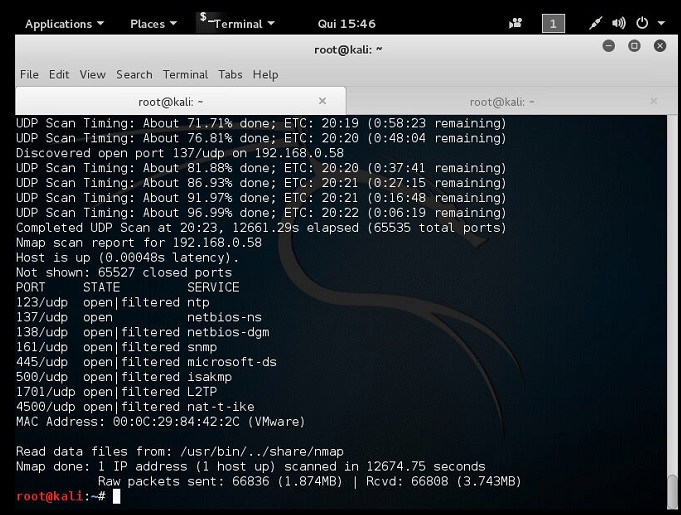


**Tentativa 7**

*nmap -sU -p 1-65535 192.168.0.58*

1. -sU é para usar o detector de portas UDP.
2. -p para indicar quais portas devem ser usadas no teste, o delimitador é “-”
3. 192.168.0.58 é o IP onde está hospedada a aplicação.

**Resultado:**



Referencias

[NTP](https://pt.wikipedia.org/wiki/Network_Time_Protocol)

[NetBios](https://pt.wikipedia.org/wiki/NetBIOS)

[SNMP](https://pt.wikipedia.org/wiki/Simple_Network_Management_Protocol)