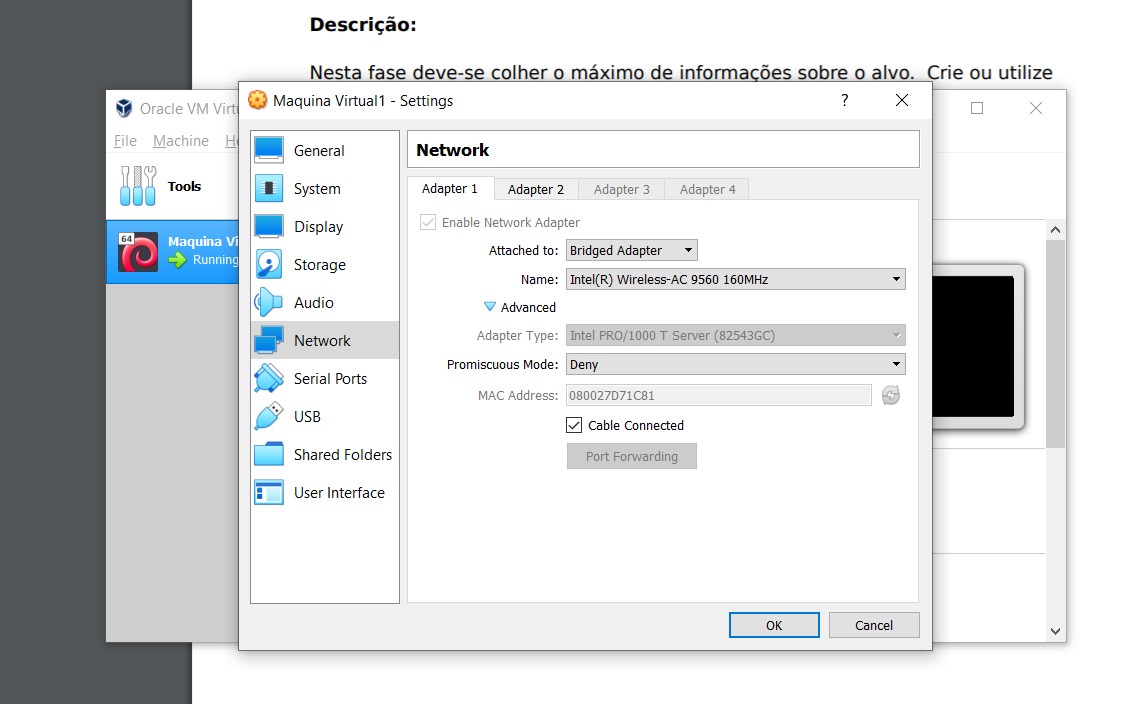
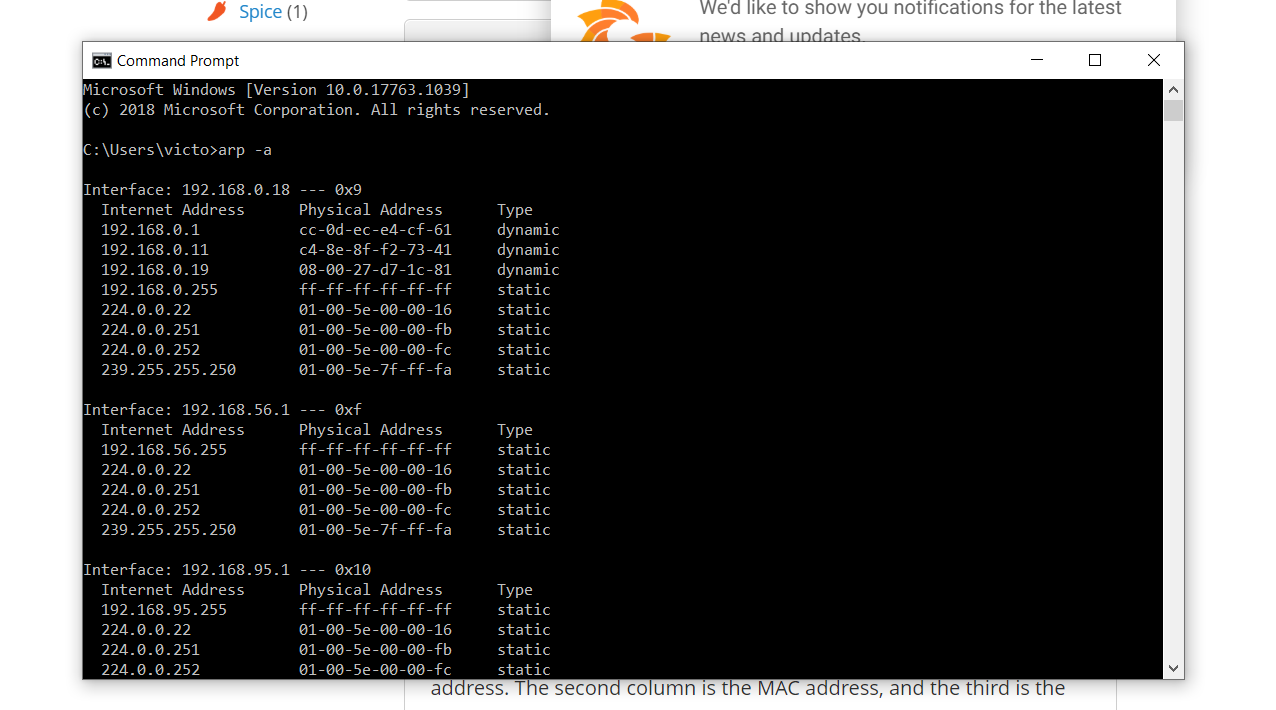
Diário de bordo

**1.1.a :**

Primeiro fui encontrar o MAC Address atribuido ao host da maquina.



Em seguida, tendo obtido o MAC Address, foi possivel descobrir o numero de IP associado:



**1.1.b:**

Usei o comando telnet ip porta para descobrir qual processo estava rodando.

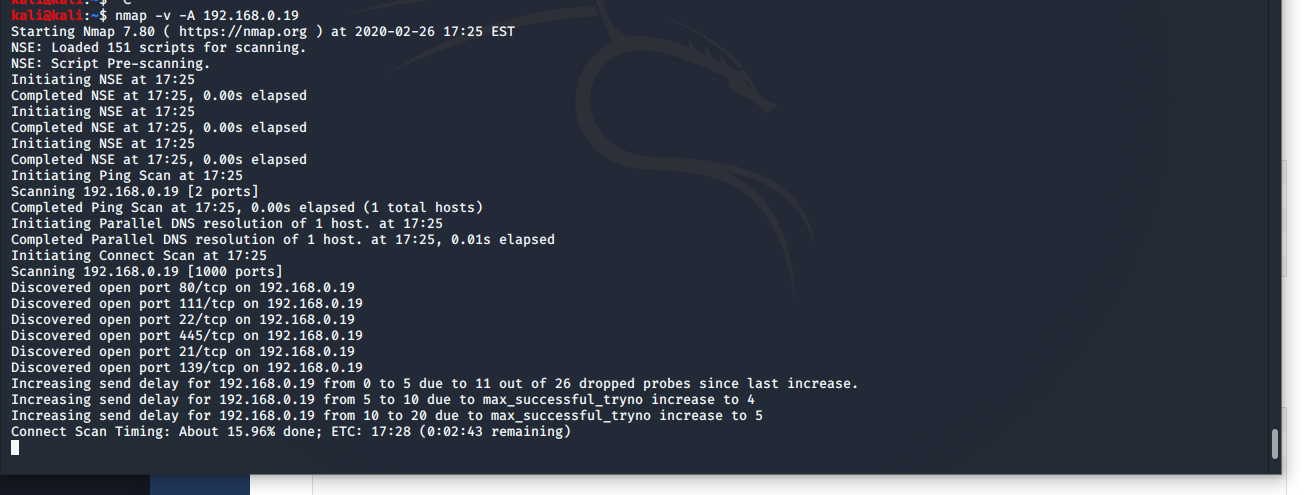


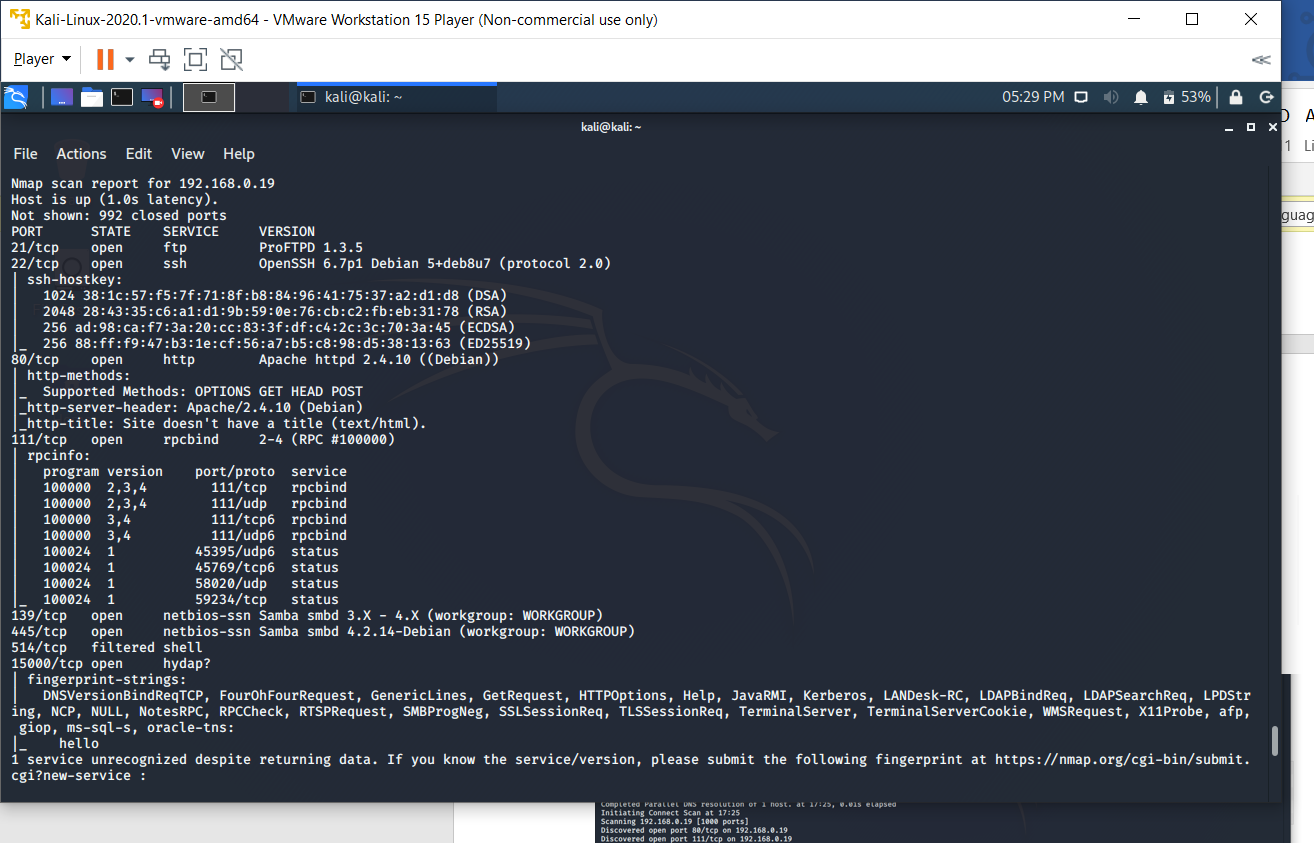
**1.1.c:**

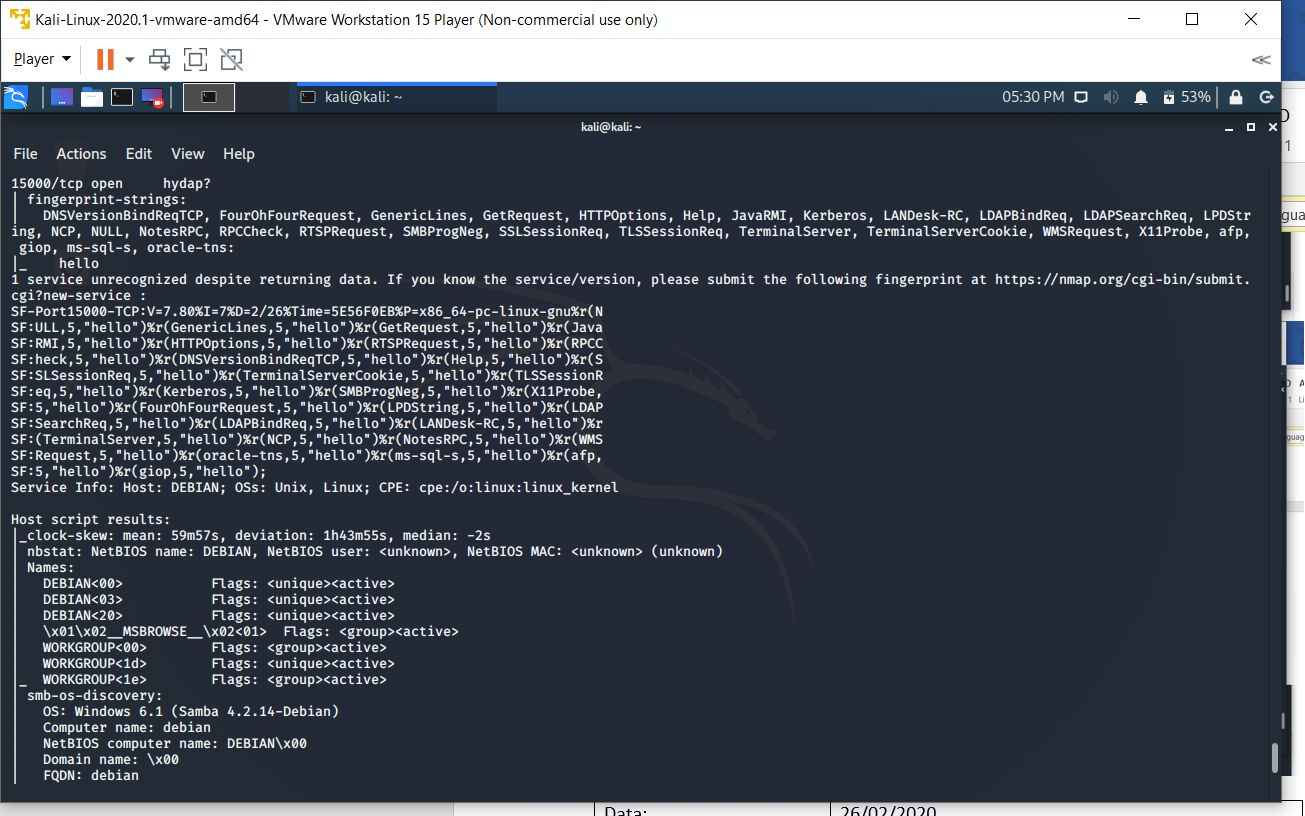
Processo rodando e sistema operacional:

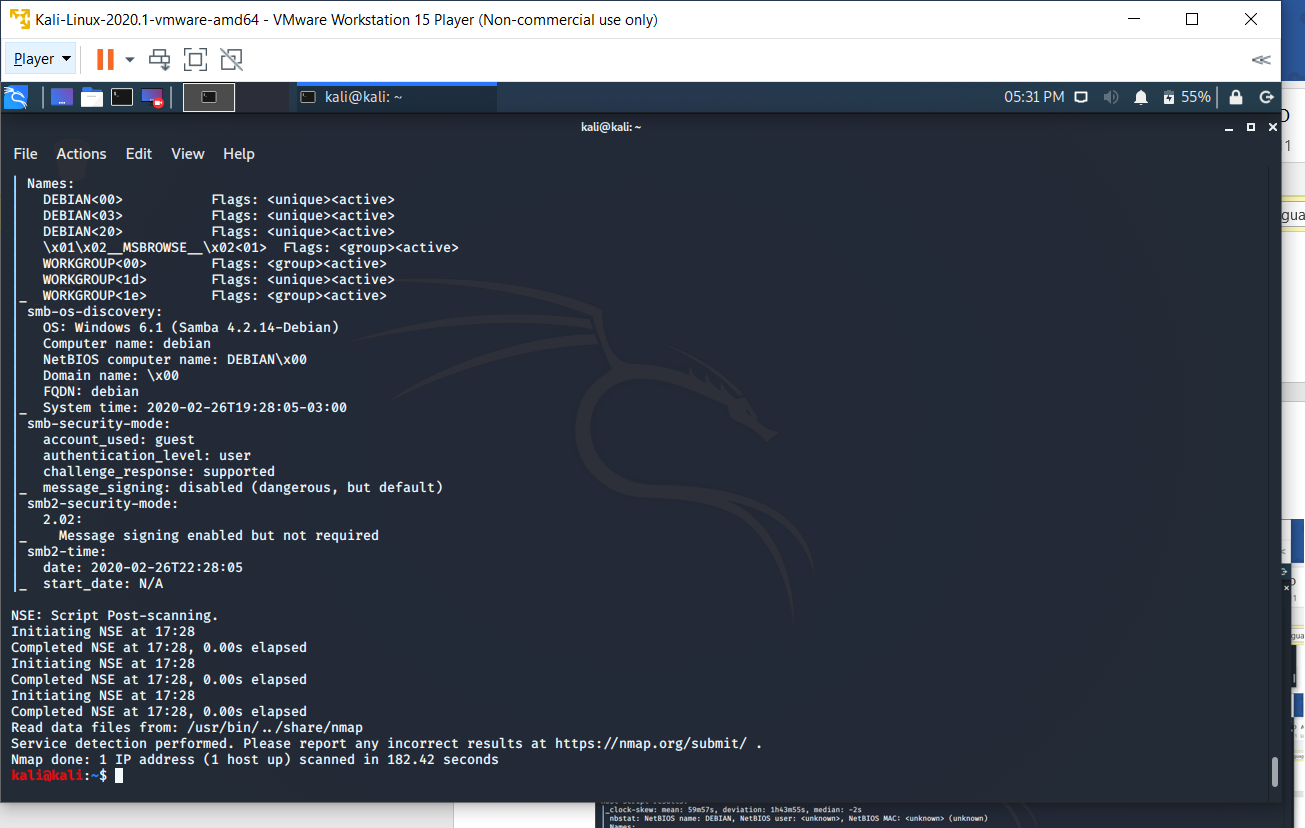


Para habilitar a deteccao do sistema operacional:

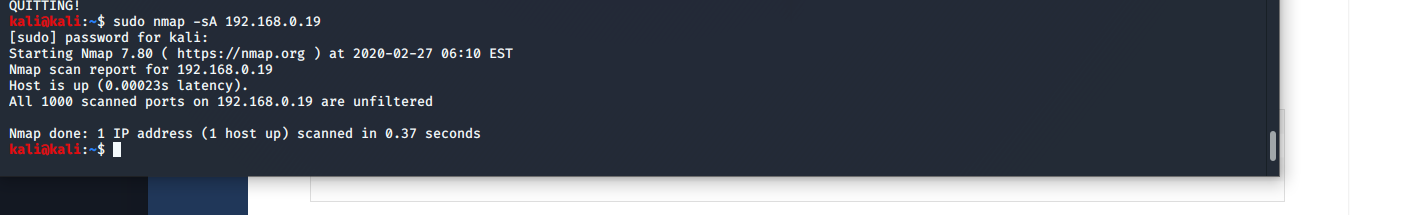






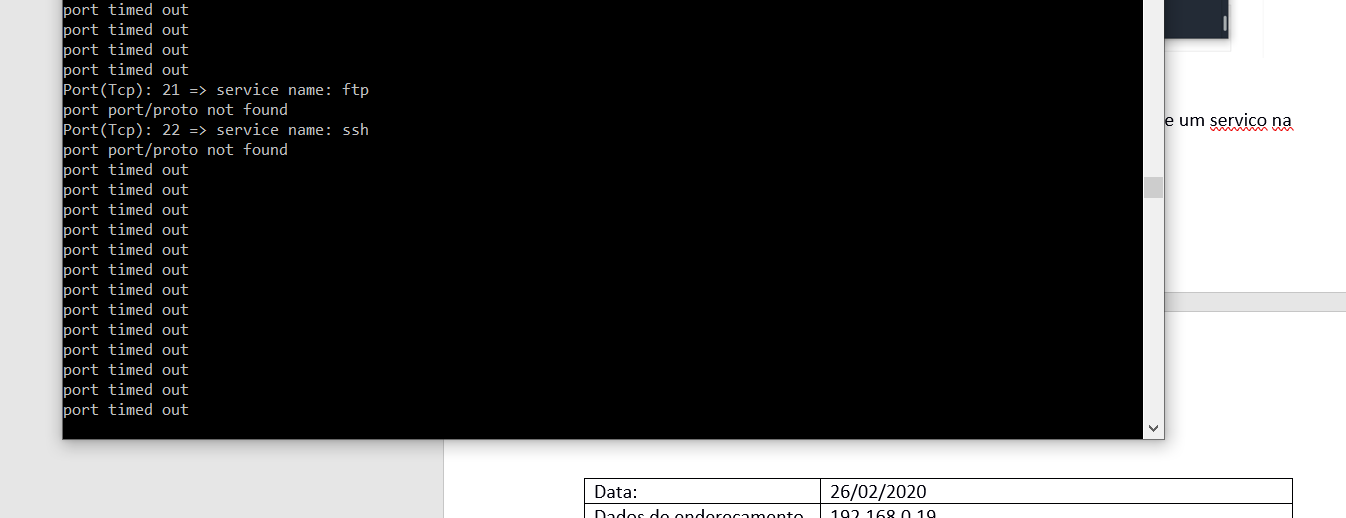


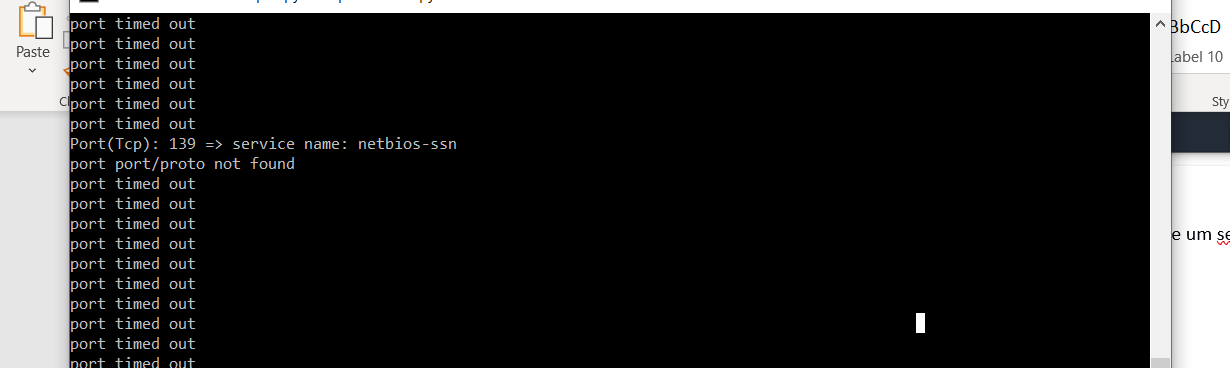
Todas as portas existentes nao sao protegidas por firewall:



**1.1.e:**

Usando a ferramenta desenvolvida, foi possivel descobrir a existencia de um servico na porta 21, 22, 80, 111, 139.





|  |  |  |
| --- | --- | --- |
| Data: | 26/02/2020 | |
| Dados de endereçamento do(s) alvo(s) | 192.168.0.19 | |
|  | | |
| Dados coletados de Rede (Portas/serviços, topologia) | | Comando utilizado |
| 1. Processos: ProFTPD 1.3.5(21), OpenSSH(22), servidor web(80) 2. Portas abertas: 80/tcp, 111/tcp, 22/tcp, 445/tcp, 21/tcp, 139/tcp | | nmap -v -A 192.168.0.19 |
| Dados coletados de aplicação (SO, versões de serviços..) | | Comando utilizado |
| 1. OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0) rodando na porta 22/tcp sendo o tipo de servico ssh. 2. Sistema operacional: Windows 6.1 (Samba 4.2.14-Debian) 3. Site de titulo desconhecido rodando na porta 80 atraves de um servidor apache. | | 1. telnet 192.168.0.19 21 2. nmap -A -p 21 192.168.0.19 |
| Vulnerabilidades | | |
| 1. Todas as portas nao sao protegidas por firewall, o que nao controla o fluxo de dados nem o acesso a elas. | | |
| Exploração | | |
|  | | |
| Outras informações úteis | | |
|  | | |