1.1.a

Comando: sudo nmap -sP 172.20.10.0/28

Para descobrir o IP do alvo utilizei o comando nmap. A partir desse comando o sistema gerou uma lista com todos os hosts ativos nessa subrede. O ip da maquina foi sinalizado como uma máquina virtual, assim consegui identificar qual era o IP do alvo.

Saída do comando com IP:

Nmap scan report for 172.20.10.3

Host is up (0.00023s latency).

MAC Address: 08:00:27:2B:03:C3 (Oracle VirtualBox virtual NIC)

1.1.b Comando: telnet 172.20.10.3 21

Para descobrir o processo rodando na porta 21 do alvo, utilizei o comando telnet + o ip do alvo + a porta que vai ser analisada. O comando retornou uma saída com o nome do processo sendo executado:

Connected to 172.20.10.3.

Escape character is '^]'.

220 ProFTPD 1.3.5 Server (Debian) [::ffff:172.20.10.3]

1.1.c Comando: sudo nmap -A 172.20.10.3

Utilizando o nmap e o IP do alvo podemos descobrir uma série de informações sobre o alvo como OS, versão, entre outros.   
Saída:  
Host script results:

|\_clock-skew: mean: 59m57s, deviation: 1h43m55s, median: -2s

|\_nbstat: NetBIOS name: DEBIAN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| smb-os-discovery:

| OS: Windows 6.1 (Samba 4.2.14-Debian)

| Computer name: debian

| NetBIOS computer name: DEBIAN\x00

| Domain name: \x00

| FQDN: debian

|\_ System time: 2020-02-27T16:24:56-03:00

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2020-02-27T19:24:56

|\_ start\_date: N/A

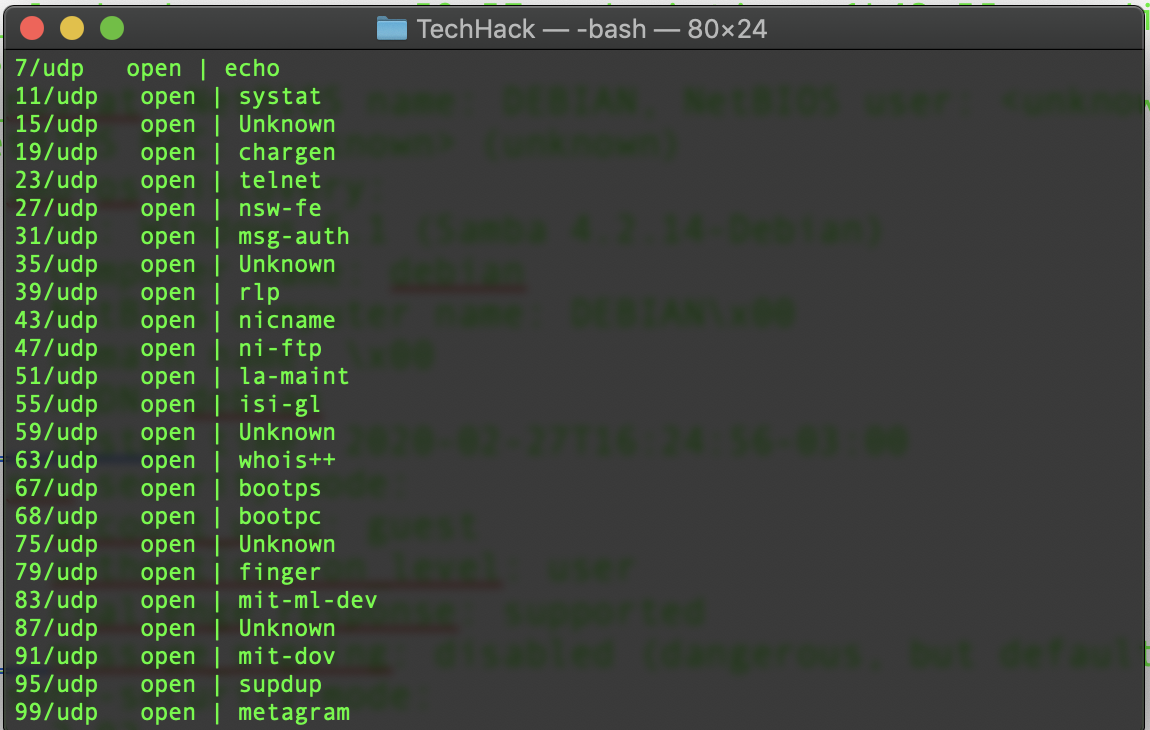
1.1.d Feito, no repositório como portscanner.py

1.1.e Portas abertas no alvo TCP:

Uma imagem contendo captura de tela

Descrição gerada automaticamente

Portas UDP abertas no alvo(1:100, todas demoraria muito):



De modo geral, uma transferência de [arquivos digitais](https://blog.visto.global/armazenar-arquivos-digitais-ferramenta/) se dá quando o servidor FTP de origem envia os dados para o cliente que, então, os transmite para o ponto de destino. Quando há uma conexão de rede lenta, as pessoas tendem a recorrer ao uso de um proxy, que faz o cliente instruir a transmissão diretamente entre dois servidores.

Um hacker pode, facilmente, aproveitar esse tipo de envio e usar o comando PORT para solicitar acesso às portas, passando-se por um intermediário para a solicitação de transferência. Em seguida, o criminoso executa, discretamente, varreduras e, assim, passa a obter acesso aos dados transmitidos pela rede.