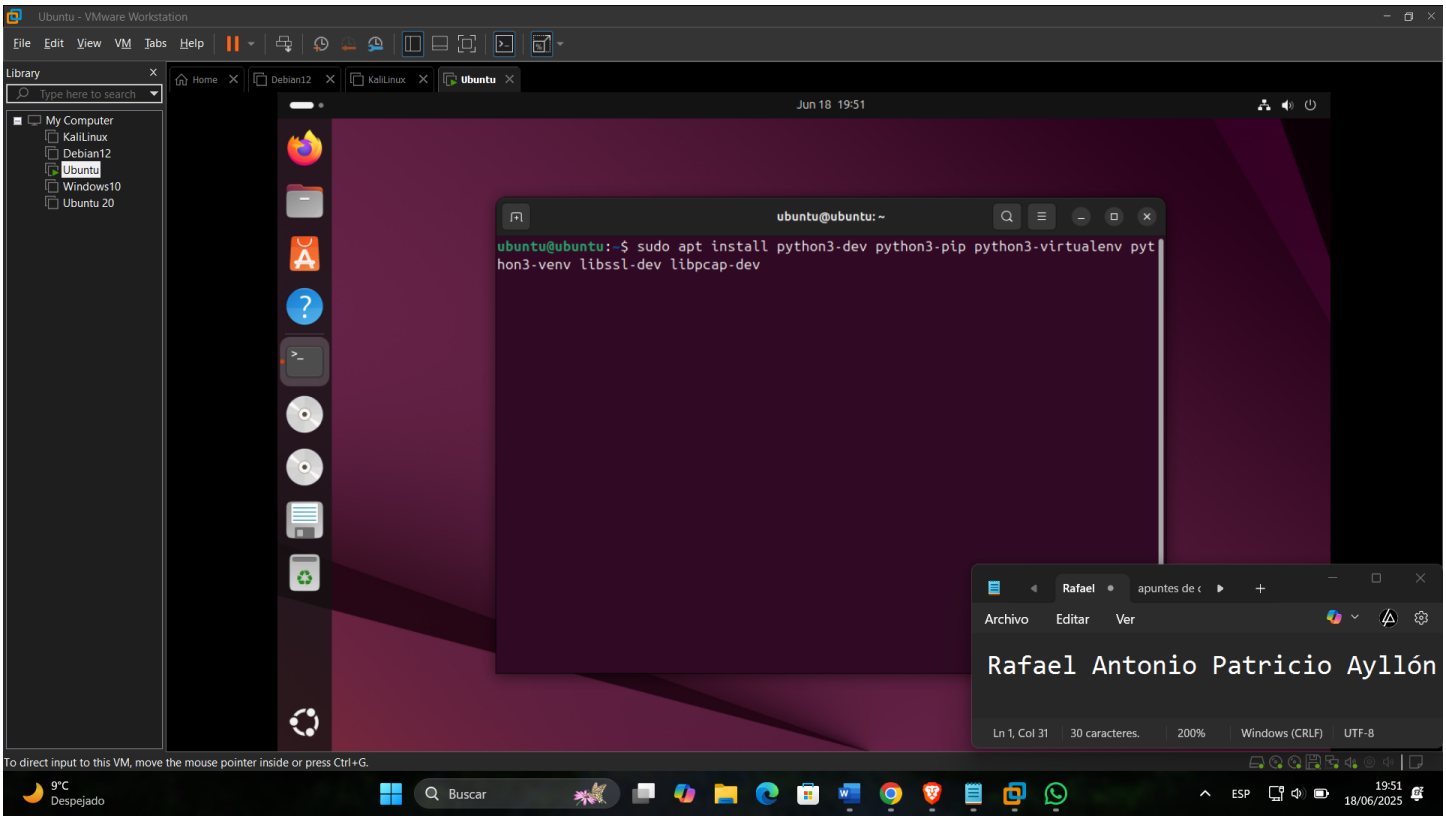
Practica N°5

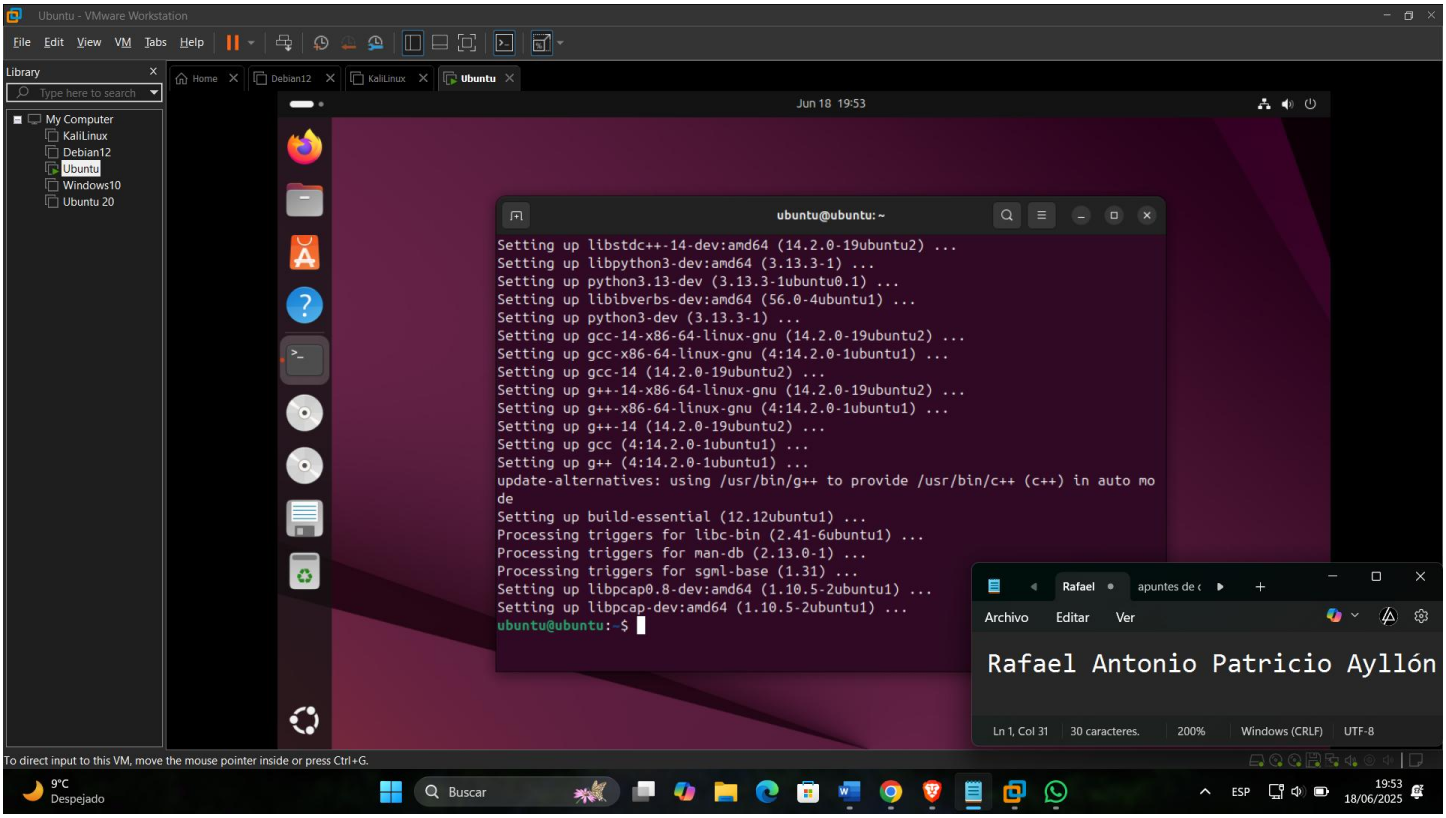
Nombre: Rafael Antonio Patricio Ayllon **CI:** 10473854 **RU:** 108771

IMPLEMENTACION:

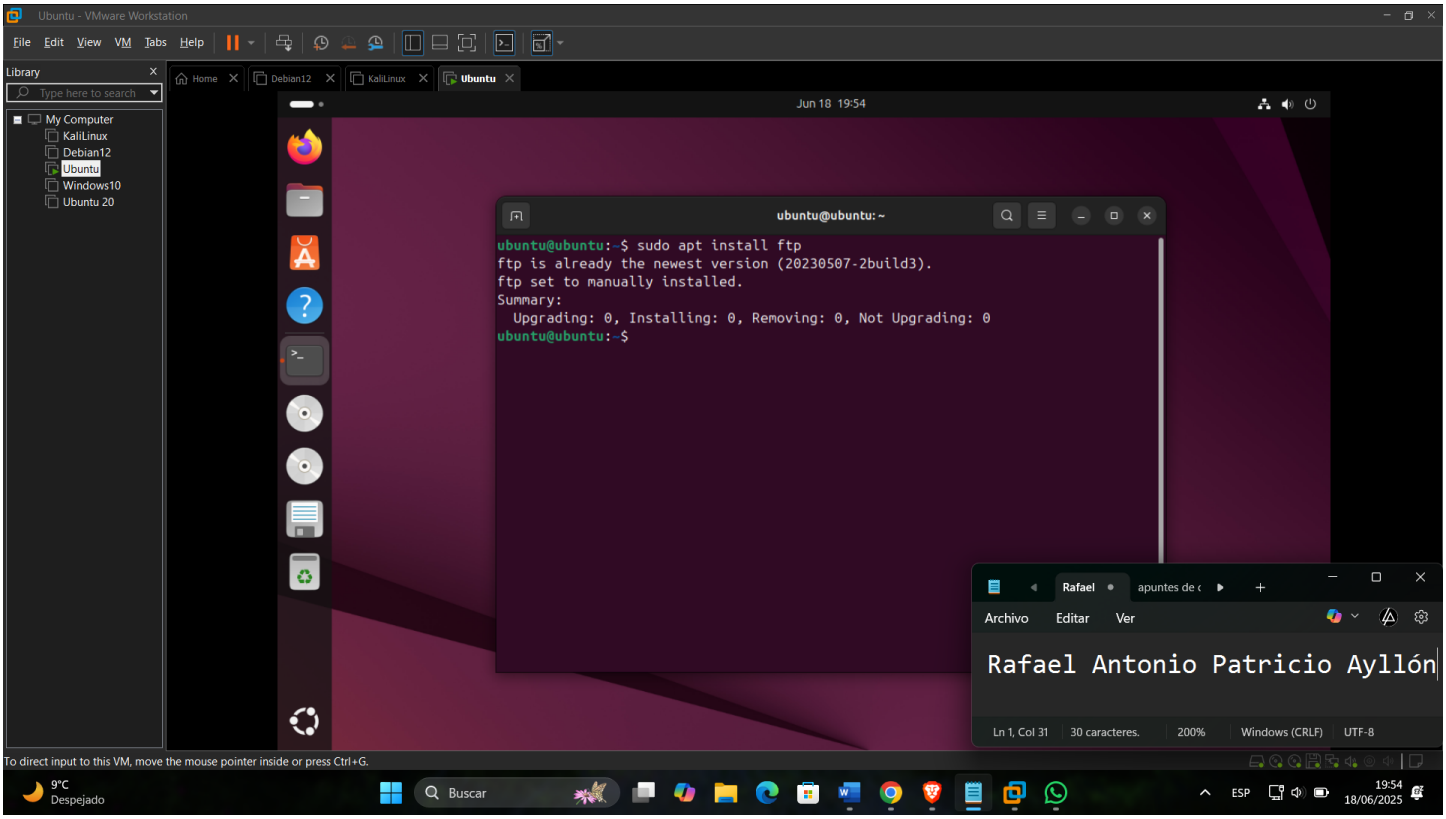
Elegir 1 solo Honeypot de los cuales se muestrra en la lista. En el cual deberá también tener configurados los servicios necesarios, para posteriormente demostrar ataques al Honeypot

Instalamos: sudo apt install python3-dev python3-pip python3-virtualenv python3-venv libssl-dev libpcap-dev

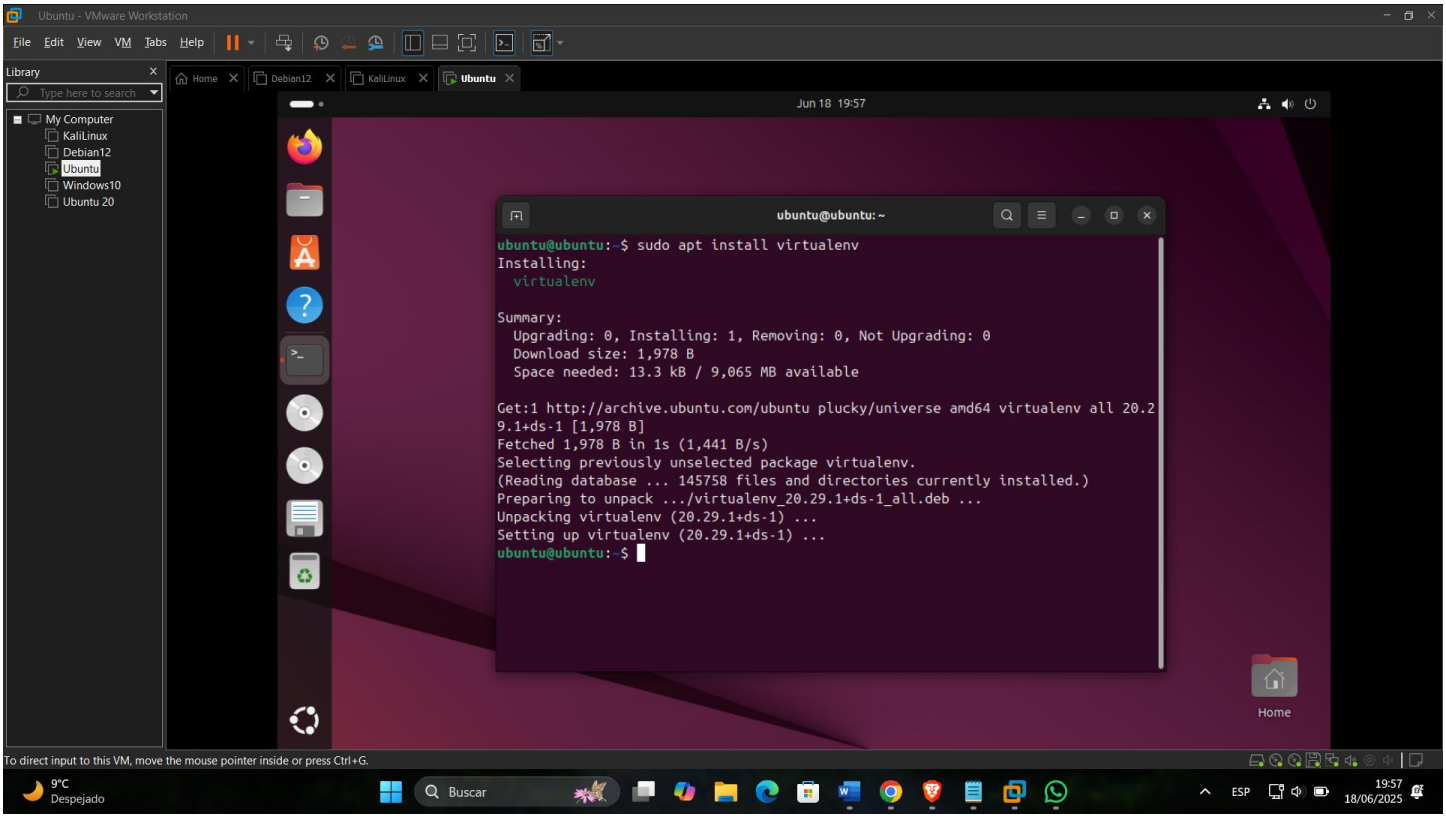




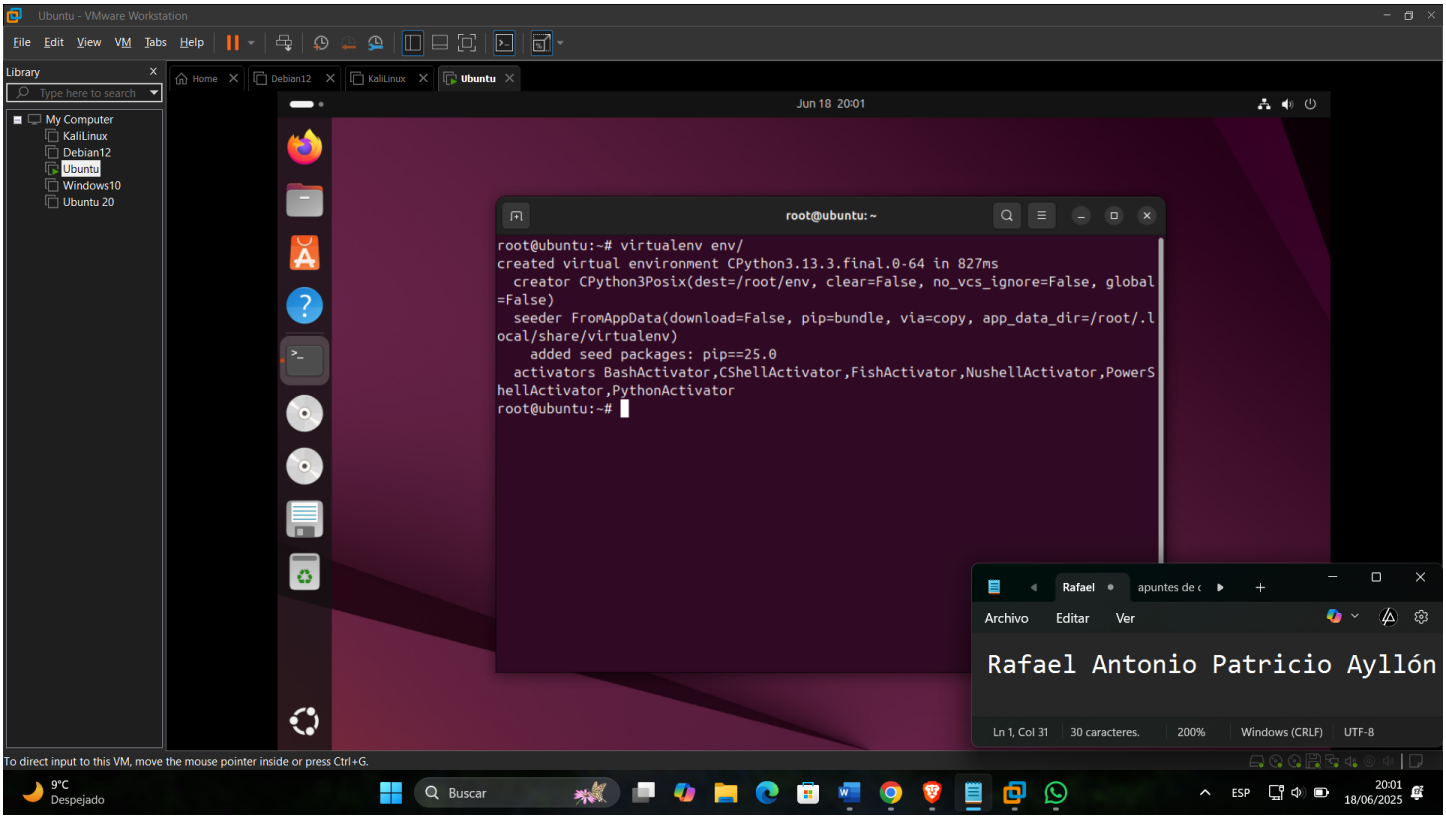
Instalar FTP



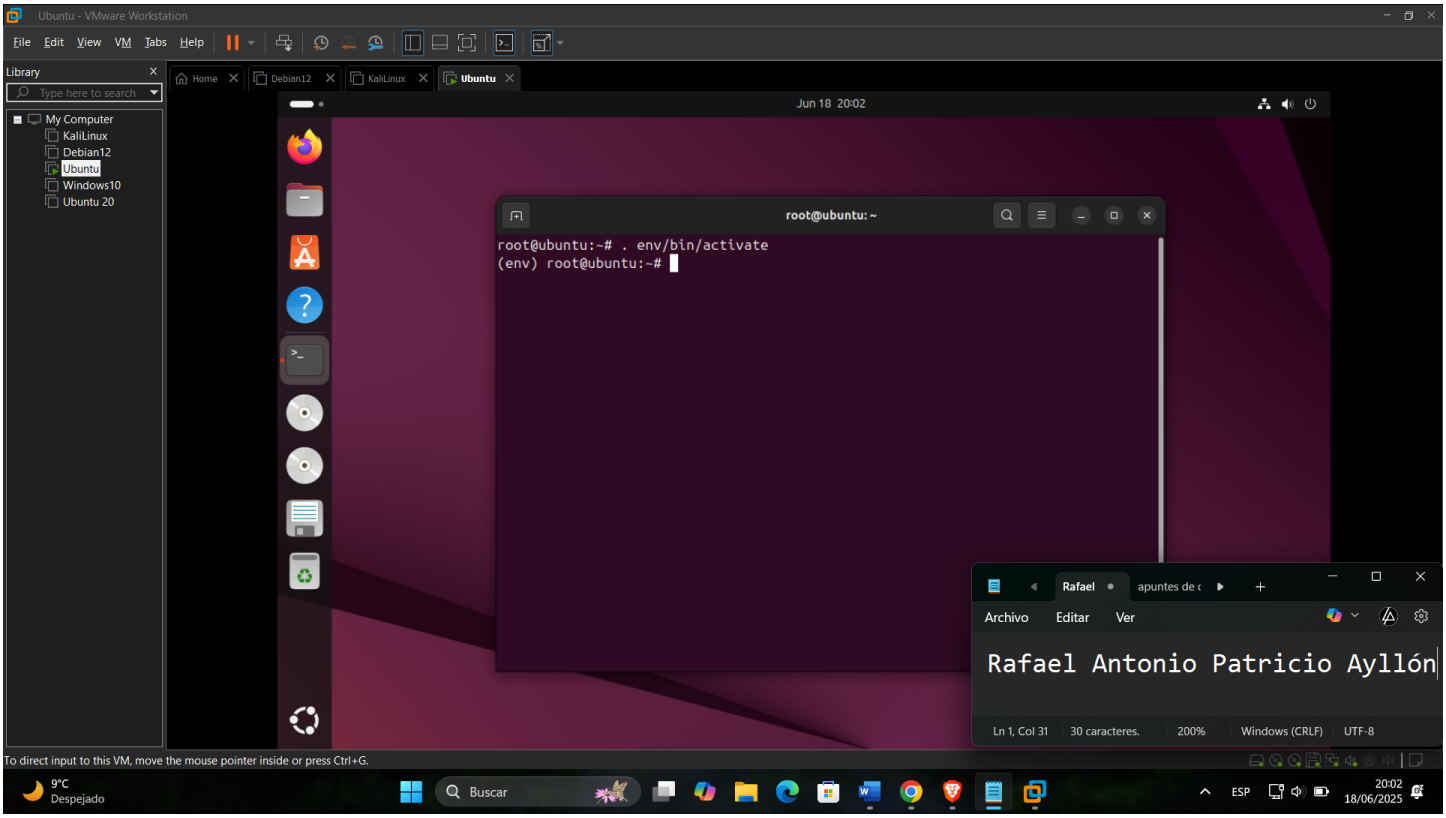
Instalar el virtualizador



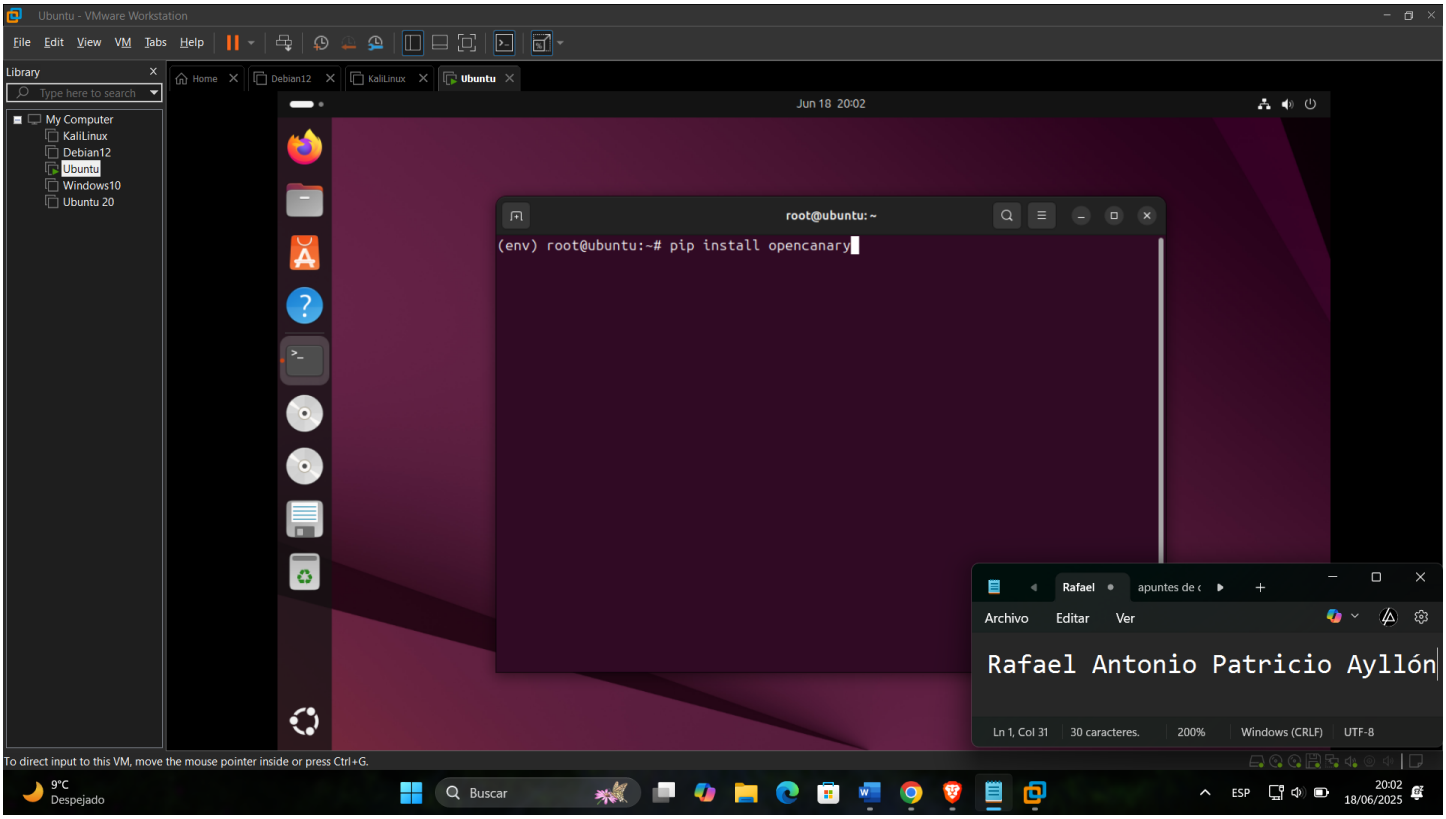
Creamos un entorno virtual

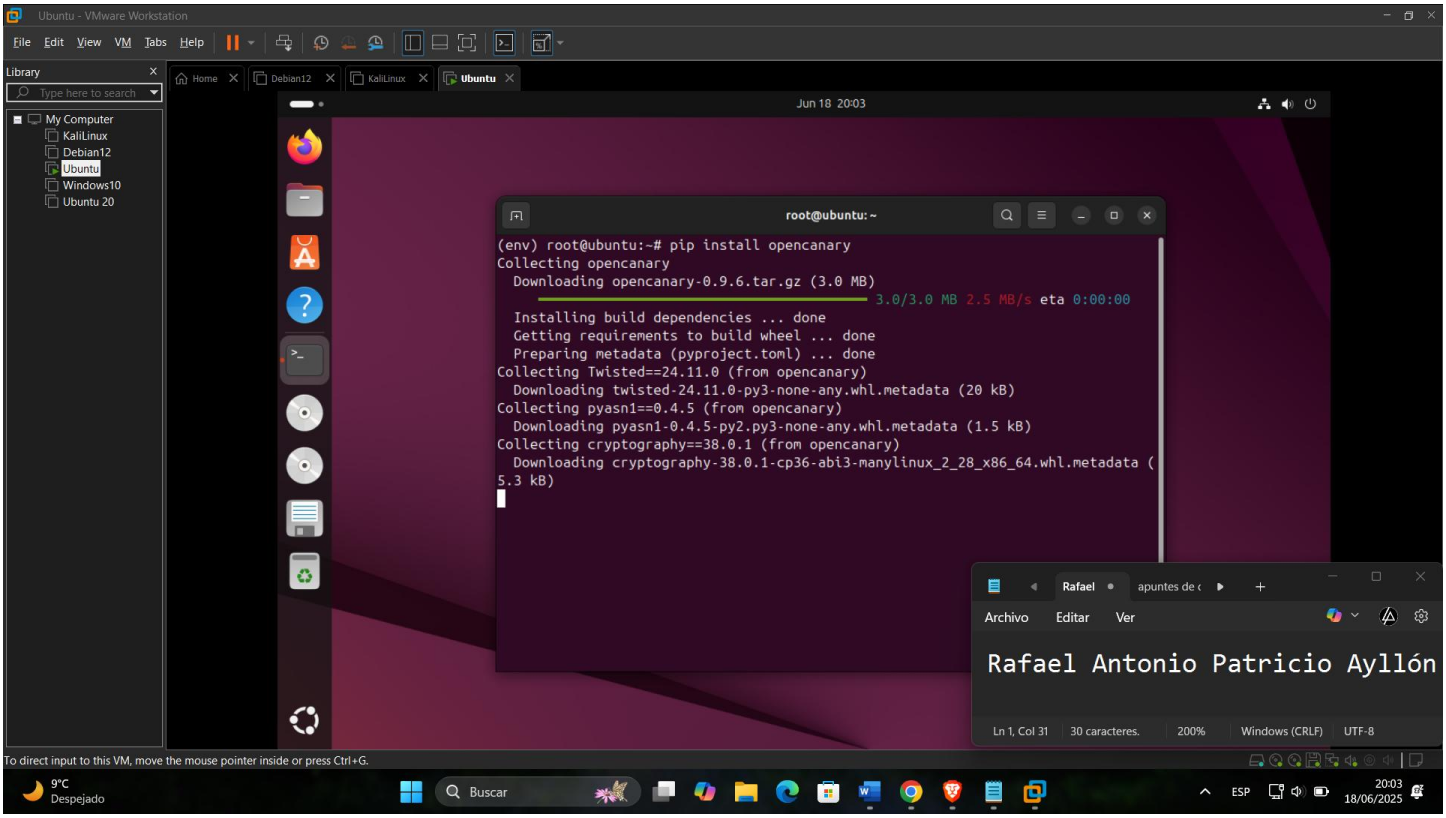


Activamos el entorno virtual

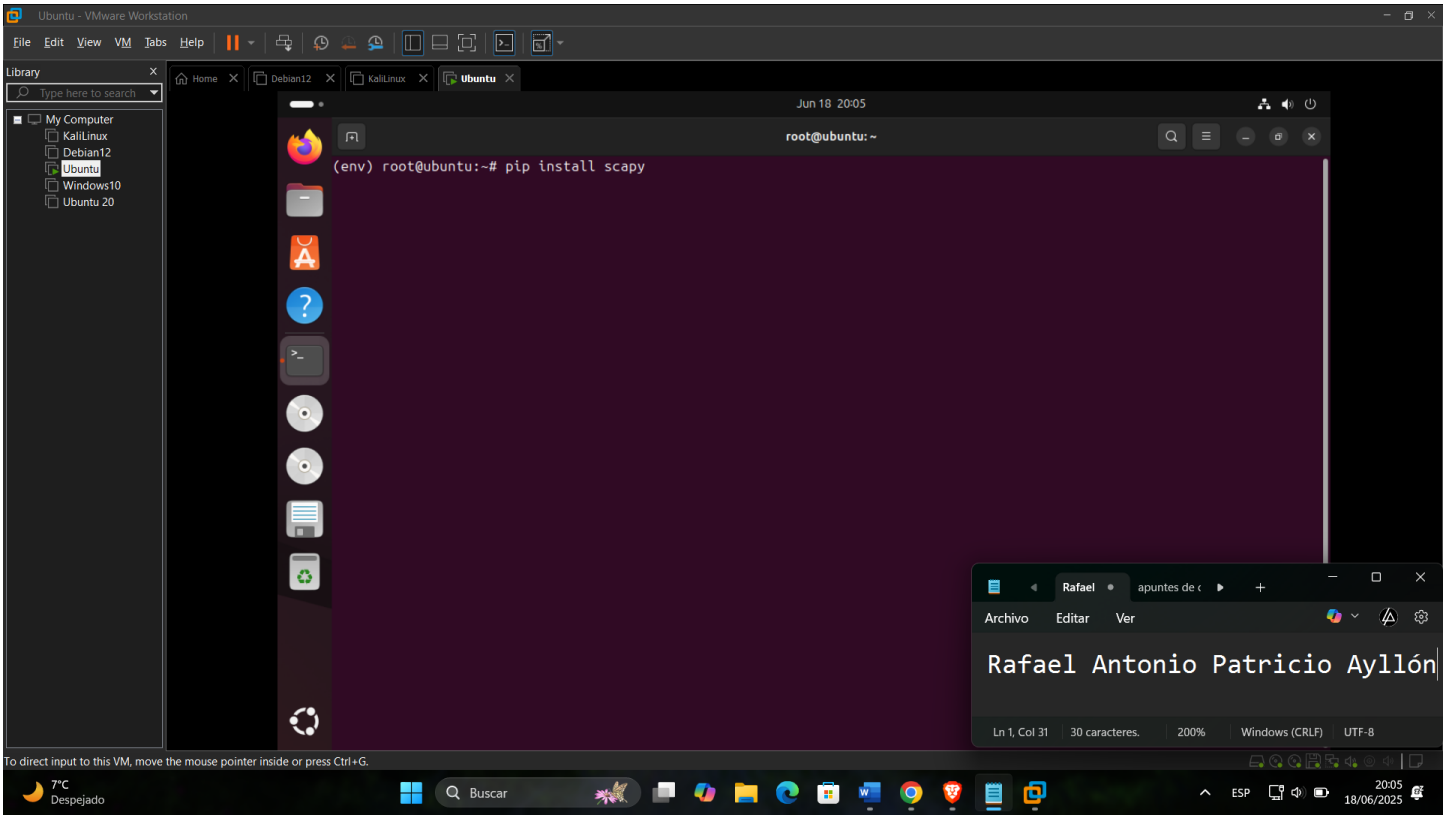


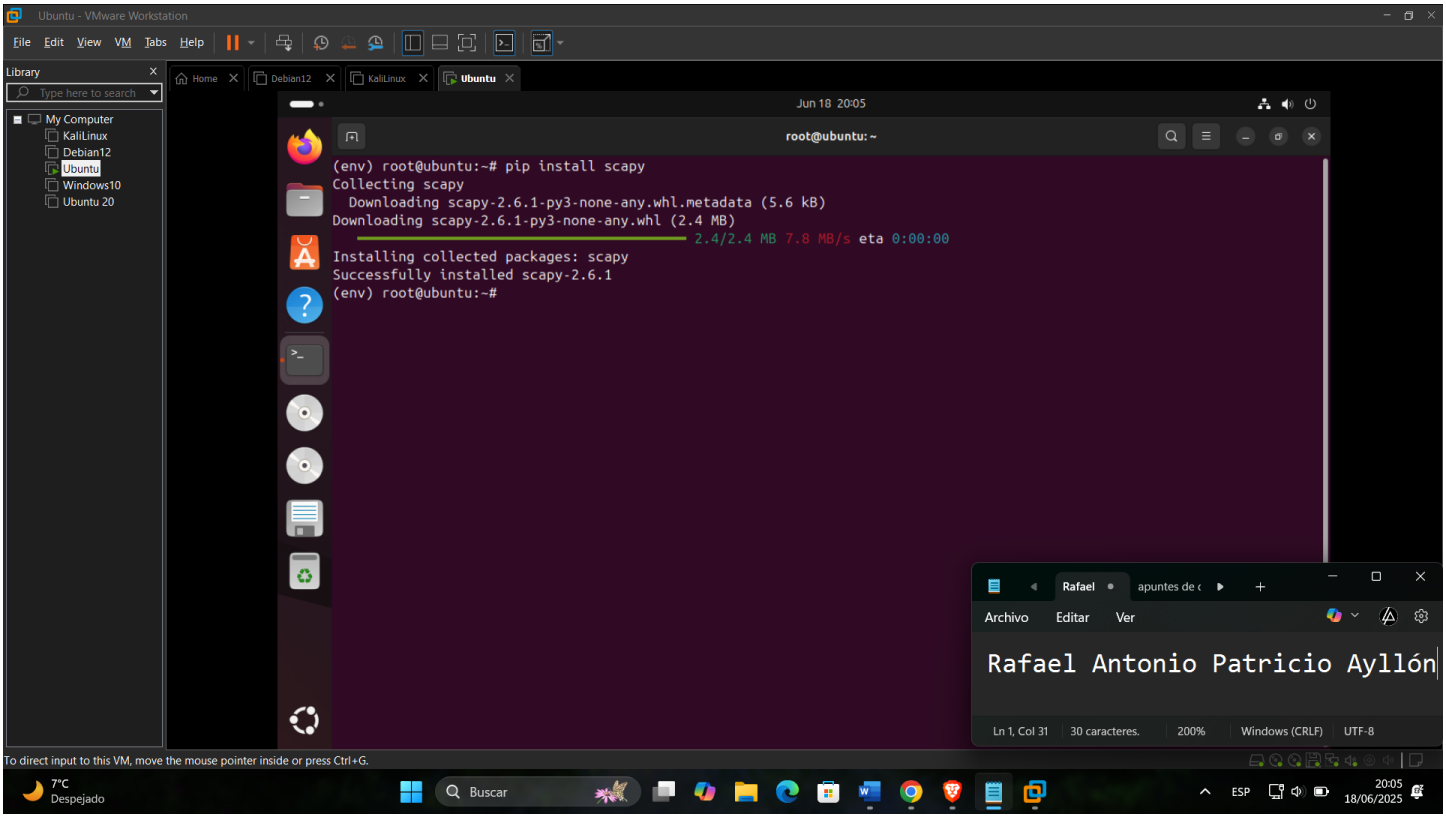
Instalar opencanary



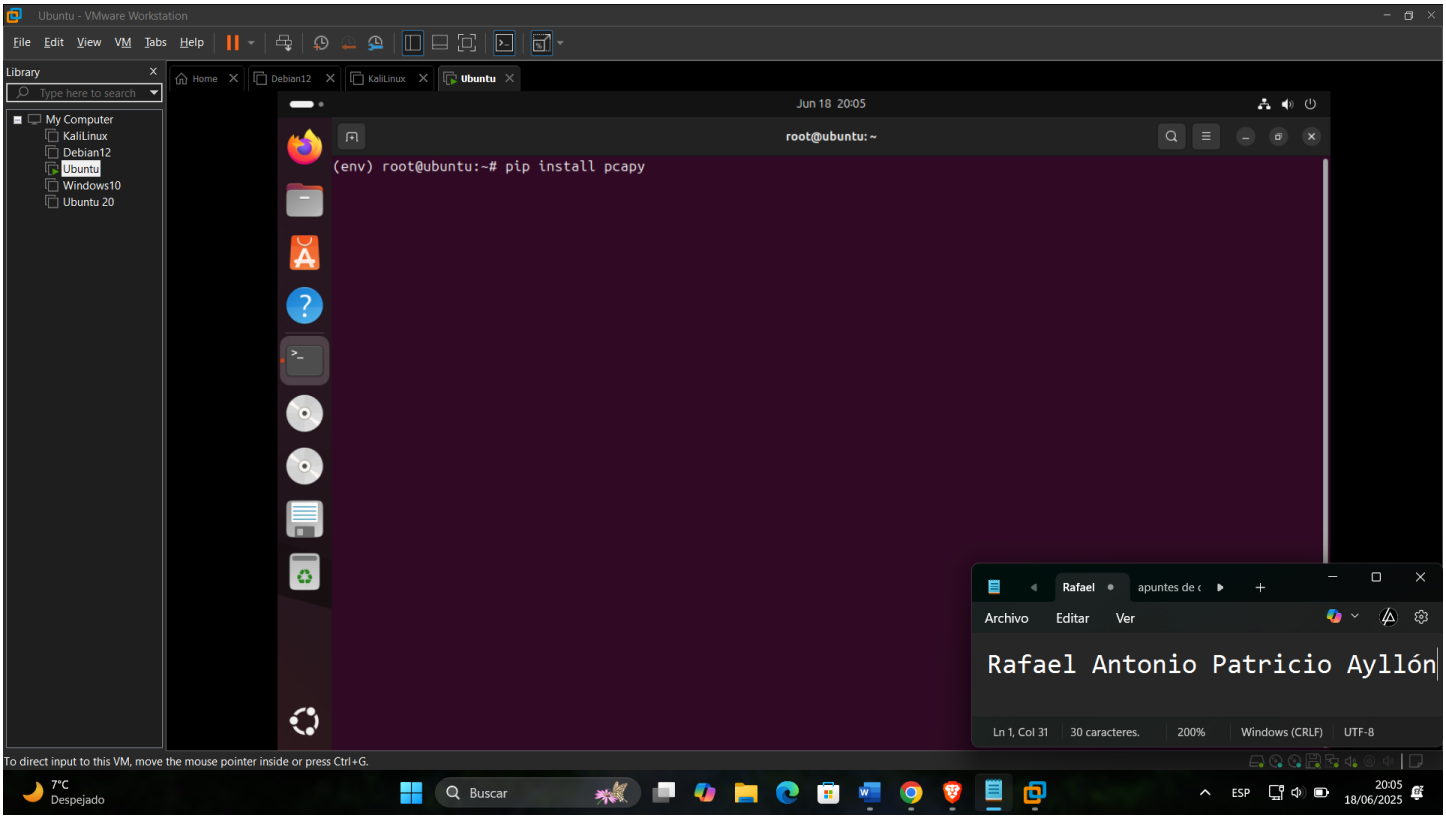


Instalar scapy

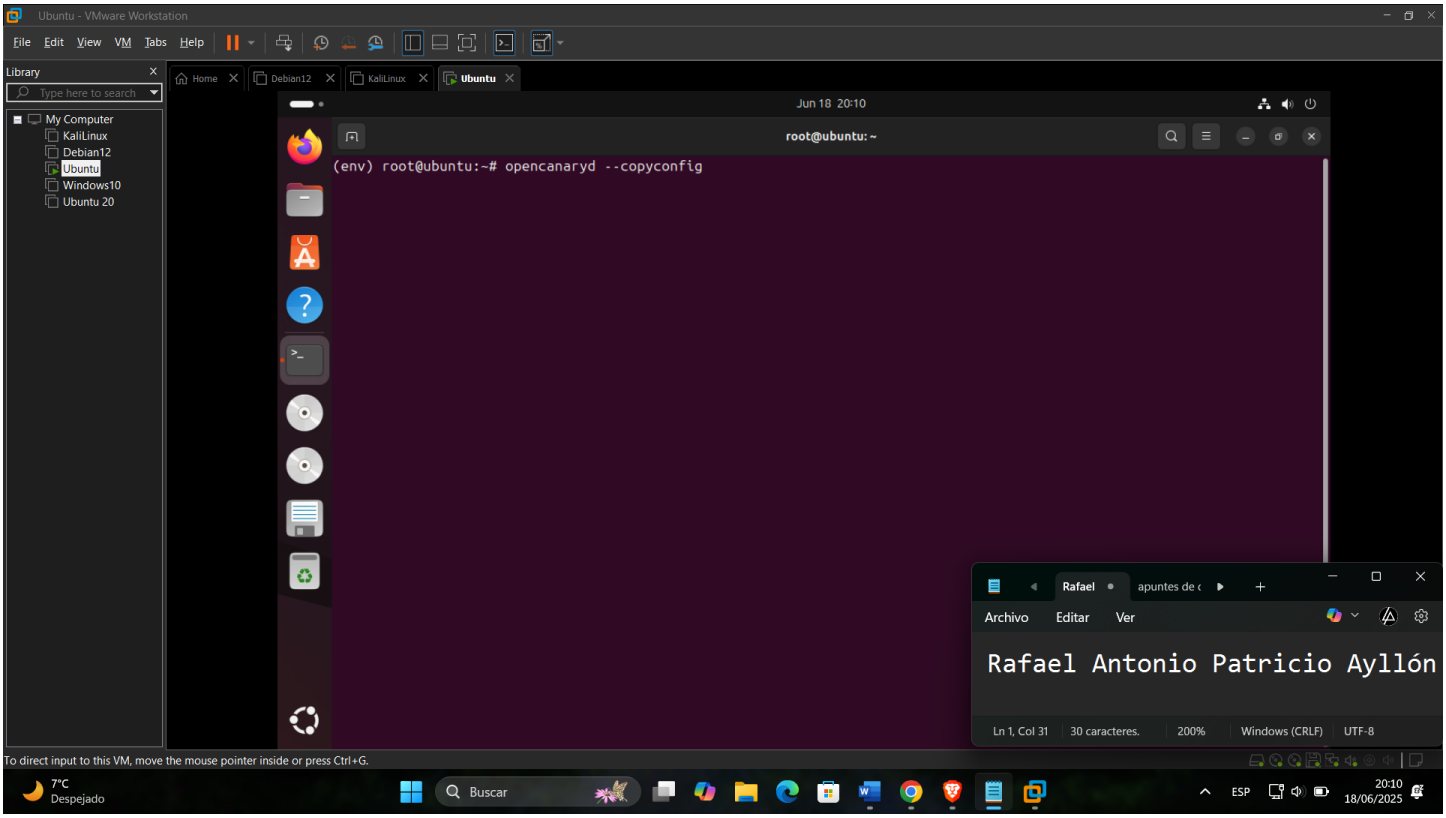


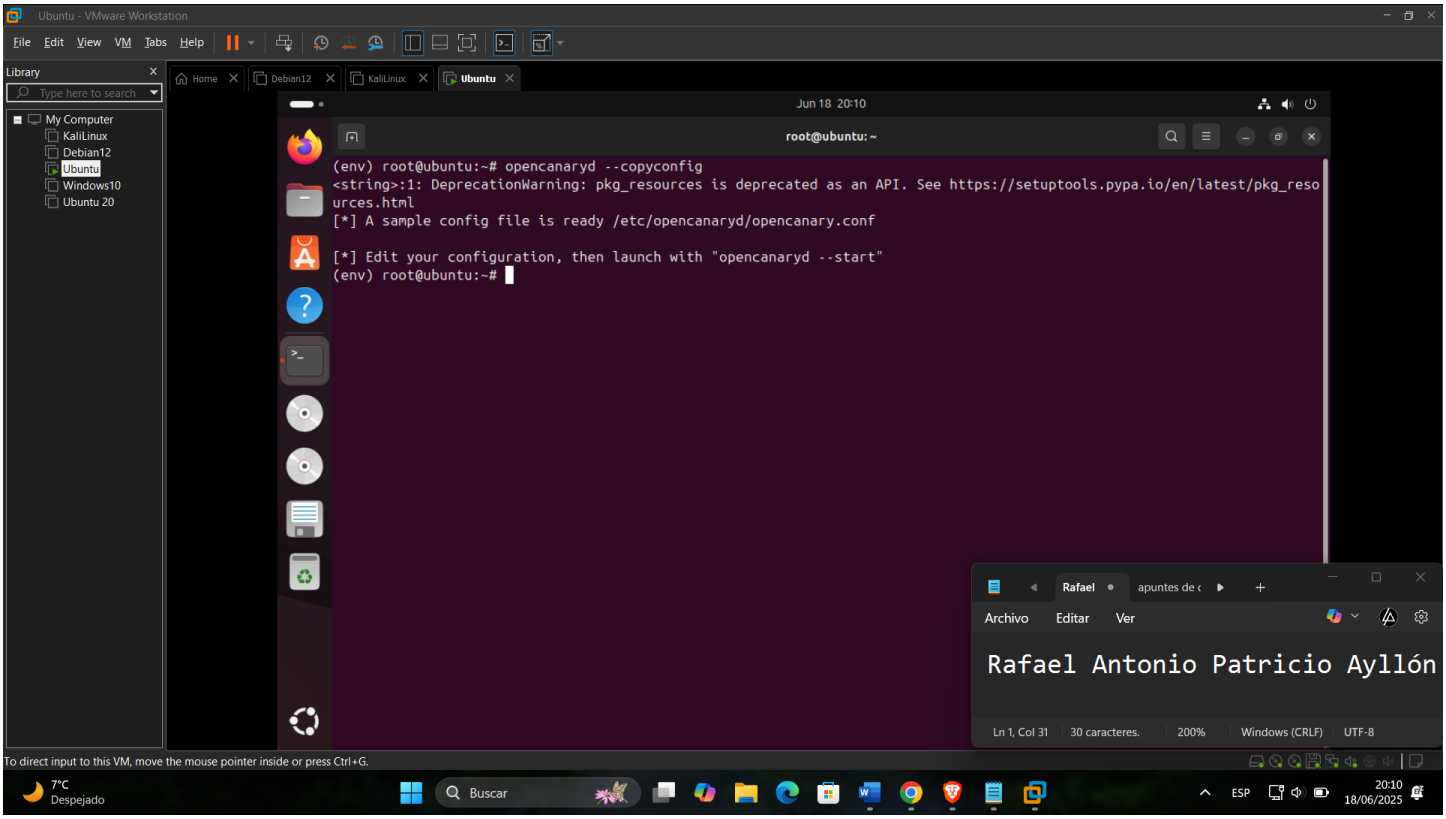


Instalar pcapy

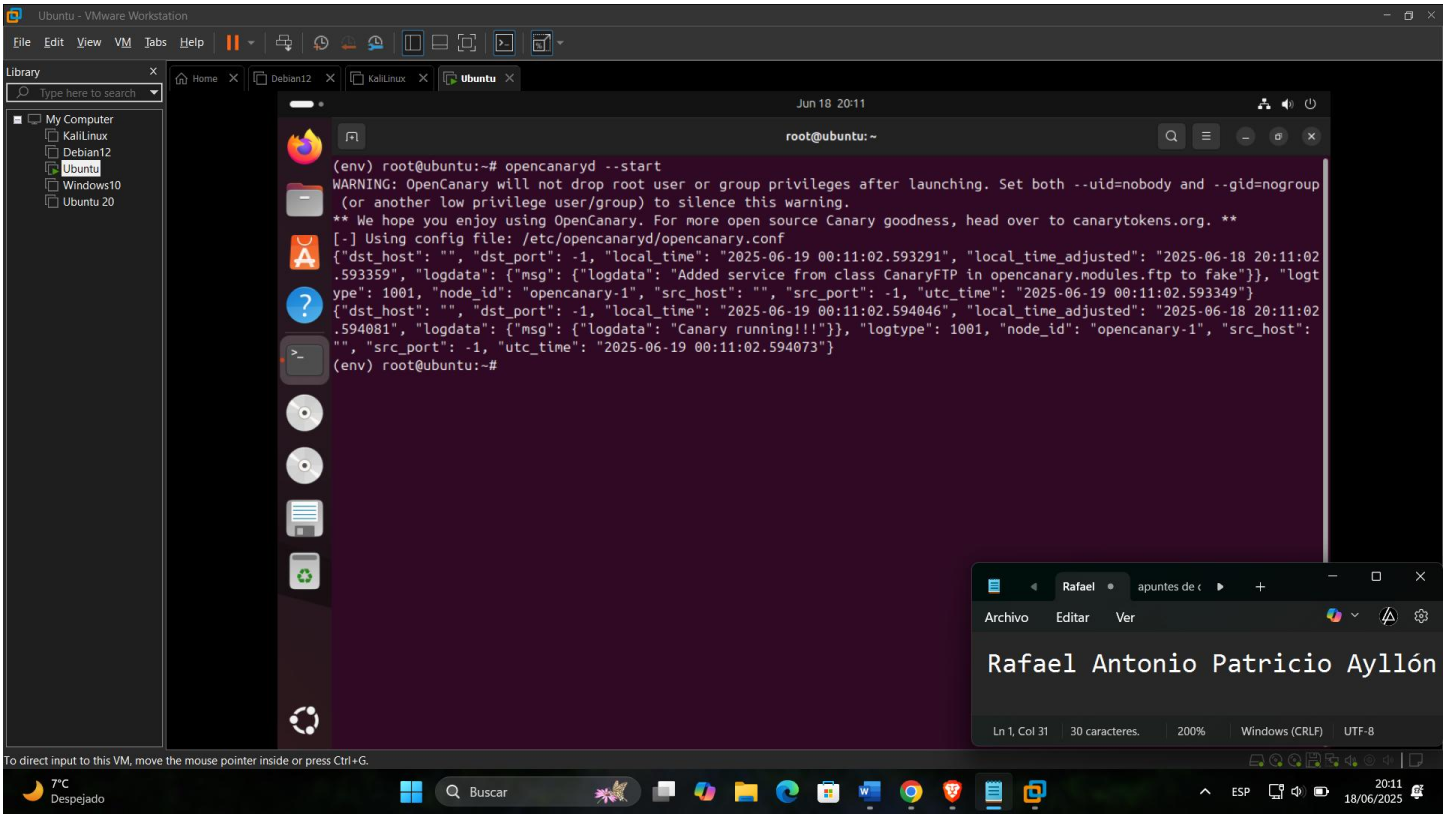


Copiar los archivos de configuración de opencanary

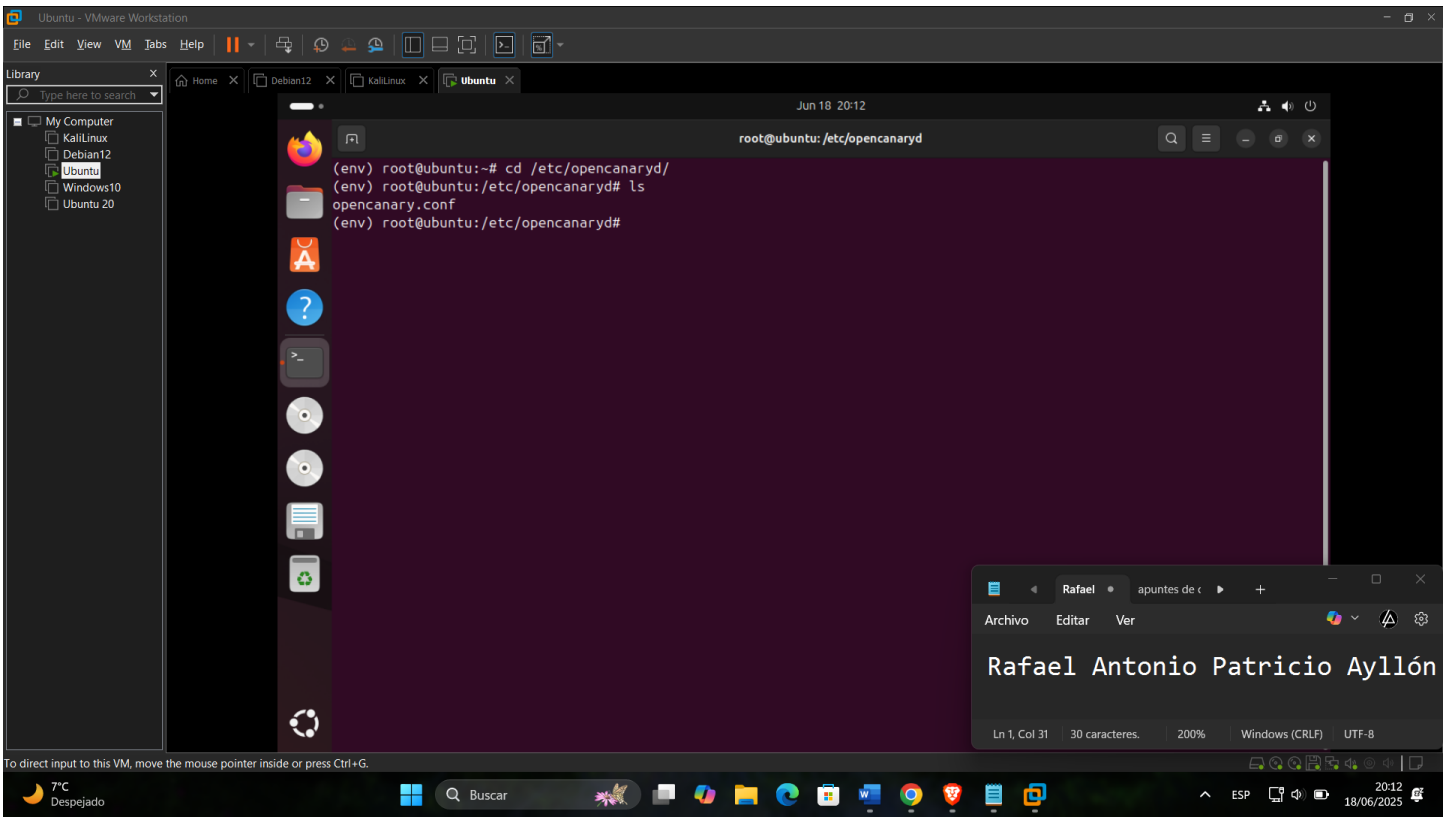




Iniciamos opencanary



Entramos a los archivos de opencanary



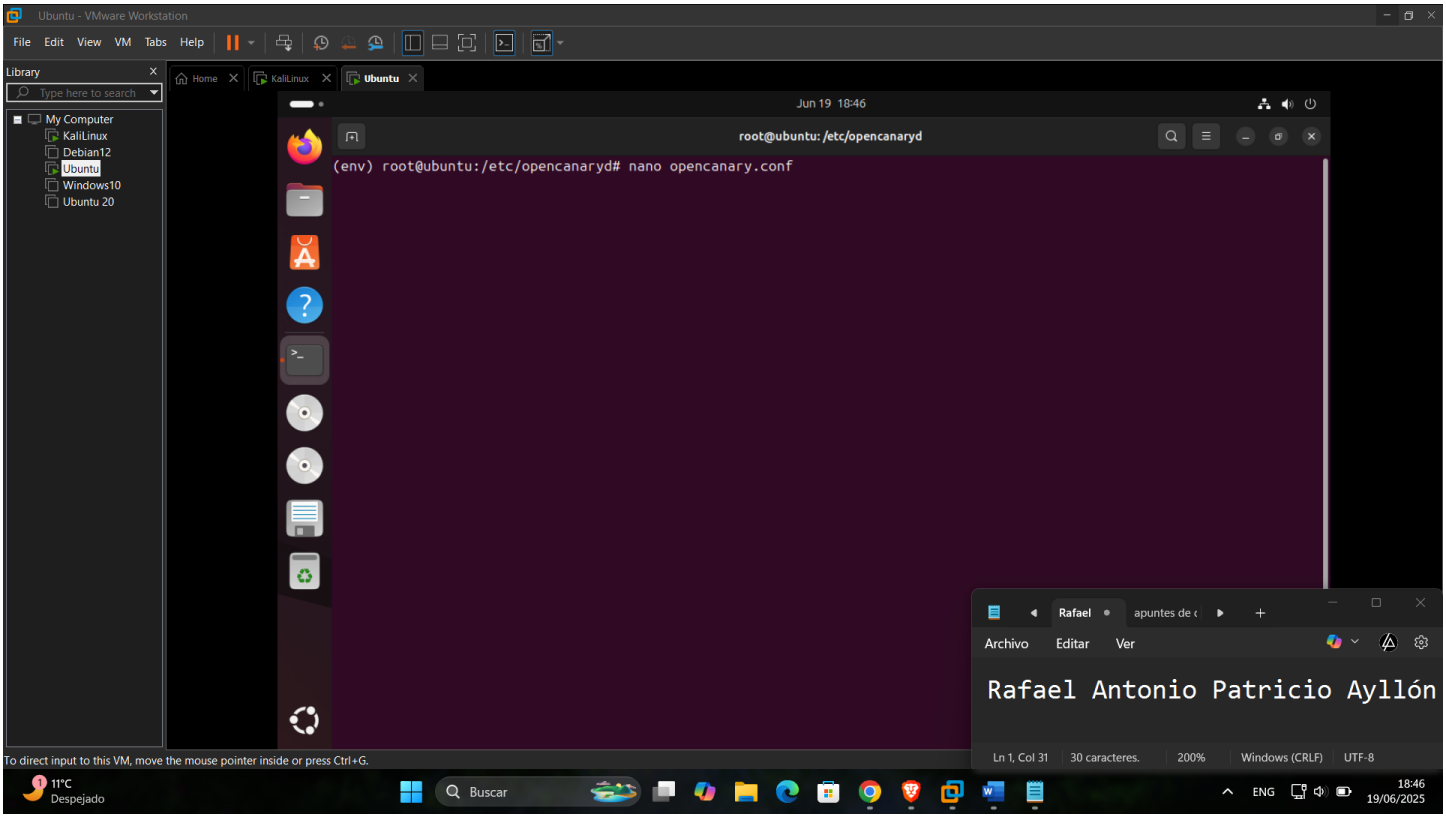
Editar opencanary.conf

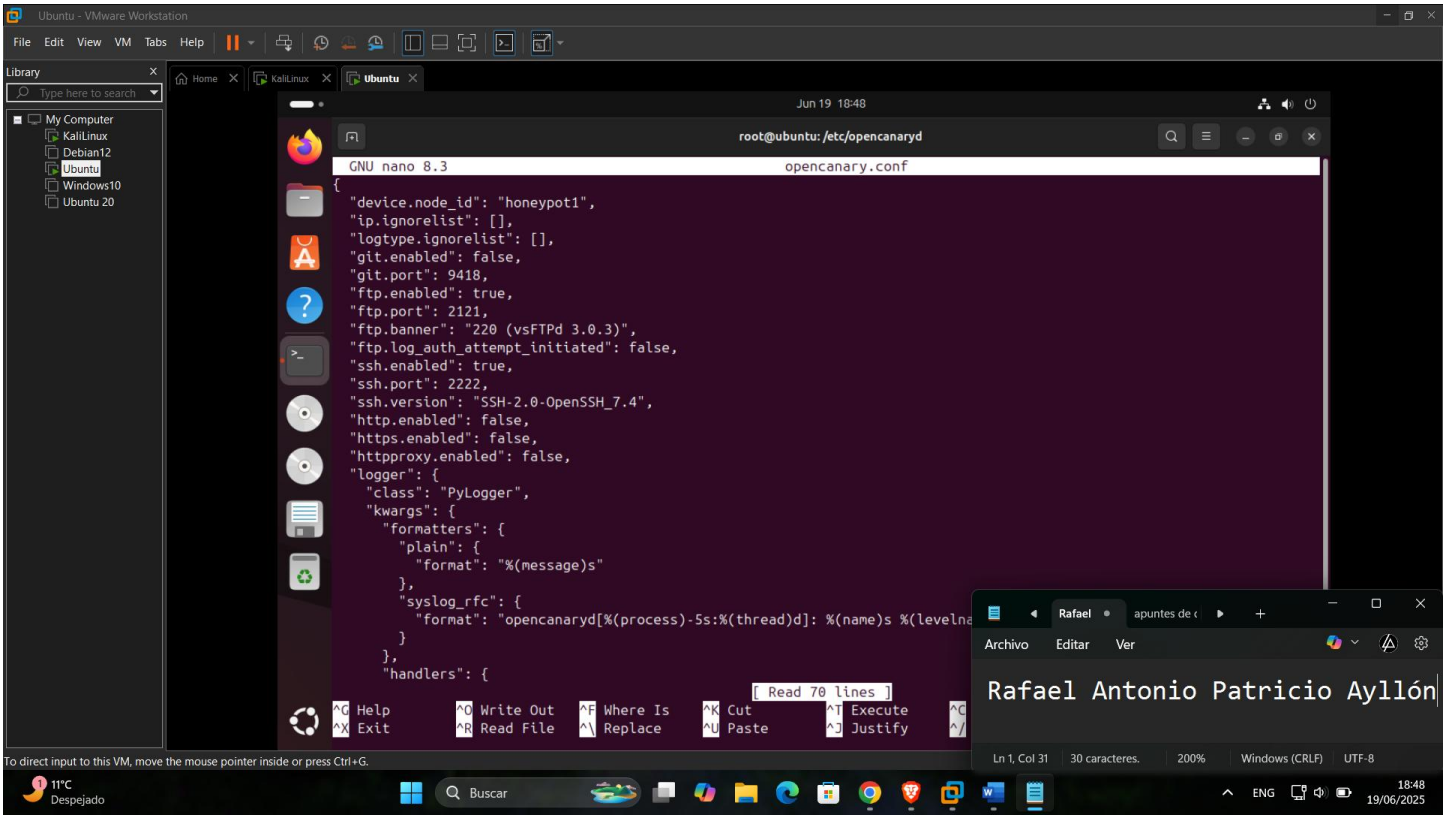
{

```
"device.node_id": "honeypot1",
"ip.ignorelist": [],
"logtype.ignorelist": [],
"git.enabled": false,
"git.port": 9418,
"ftp.enabled": true,
"ftp.port": 2121,
"ftp.banner": "220 (vsFTPd 3.0.3)",
"ftp.log_auth_attempt_initiated": false,
"ssh.enabled": true,
"ssh.port": 2222,
"ssh.version": "SSH-2.0-OpenSSH_7.4",
"http.enabled": false,
"https.enabled": false,
"httpproxy.enabled": false,
"logger": {
  "class": "PyLogger",
  "kwargs": {
    "formatters": {
      "plain": {
        "format": "%(message)s"
      },
      "syslog_rfc": {
        "format": "opencanaryd[%(process)-5s:%(thread)d]: %(name)s %(levelname)-5s %(message)s"
      }
```

```
    },
    "handlers": {
      "console": {
        "class": "logging.StreamHandler",
        "stream": "ext://sys.stdout",
        "formatter": "plain"
      },
      "file": {
        "class": "logging.FileHandler",
        "filename": "/var/log/opencanary.log",
        "formatter": "plain"
      },
      "SMTP": {
        "class": "logging.handlers.SMTPHandler",
        "mailhost": ["smtp.gmail.com", 587],
        "fromaddr": "noreply@mydomain.com",
        "toaddrs": ["seguridad@gmail.com"],
        "subject": "OpenCanary Alert",
        "credentials": ["noreply@mydomain.com", "TUMAIL_APP_PASSWORD"],
        "secure": []
      }
    }
  },
  "portscan.enabled": false,
```

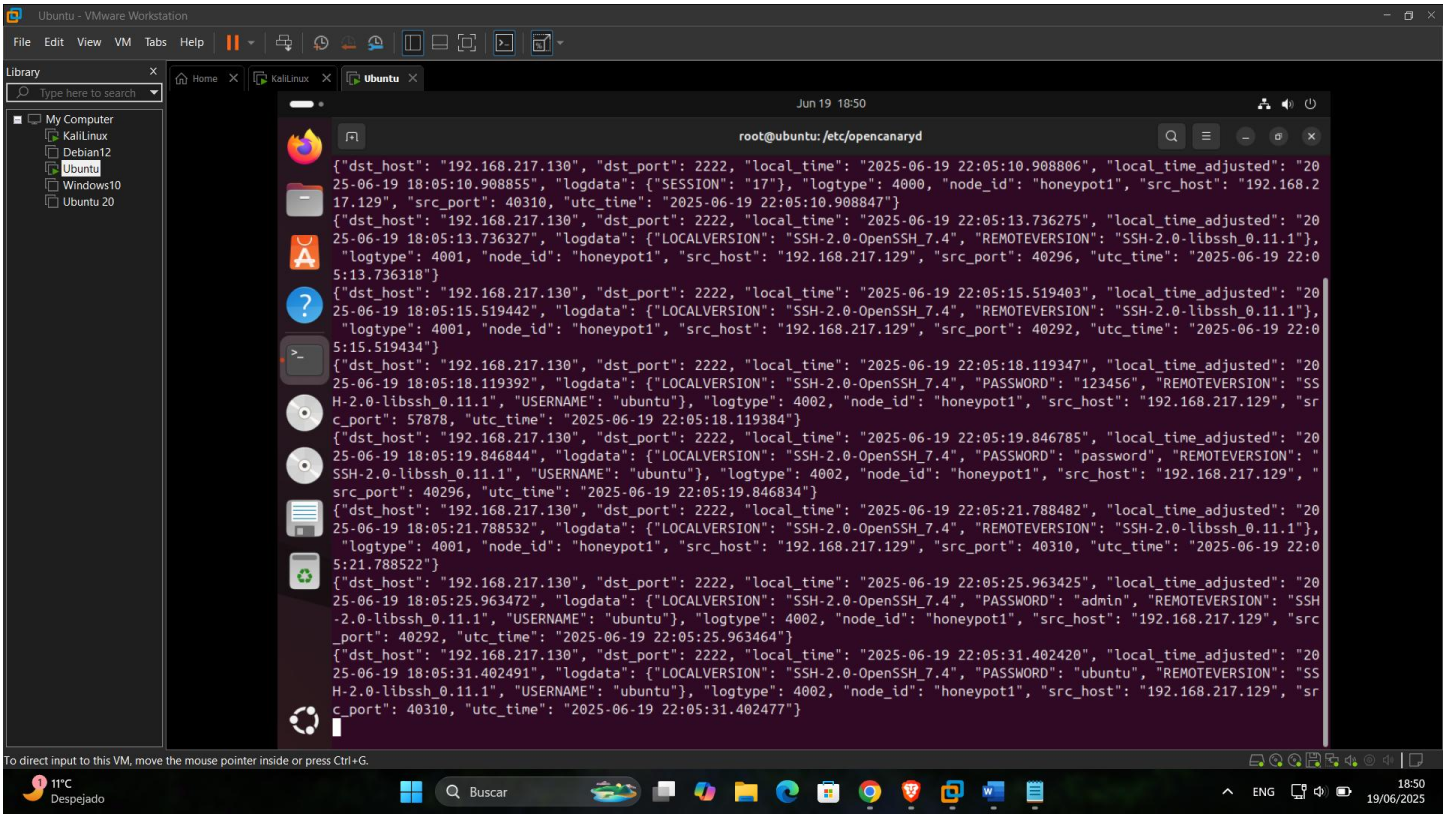
```
  "portscan.ignore_localhost": false,
  "portscan.logfile": "/var/log/kern.log",
  "portscan.synrate": 5,
  "portscan.nmaposrate": 5,
  "portscan.lorate": 3,
  "portscan.ignore_ports": [],
  "smb.enabled": false,
  "mysql.enabled": false,
  "redis.enabled": false,
  "rdp.enabled": false,
  "sip.enabled": false,
  "snmp.enabled": false,
  "ntp.enabled": false,
  "tftp.enabled": false,
  "tcpbanner.enabled": false,
  "telnet.enabled": false,
  "mssql.enabled": false,
  "vnc.enabled": false
}
```





Con este comando se verificara los logs generados:

tail -f /var/log/opencanary.log



ATAQUE:

Demostración de un ataque de fuerza bruta para obtener el usuario y/o contraseña Puede utilizar cualquier herramienta que vea necesaria para los ataques, pero el objetivo debe ser un Honeypot.

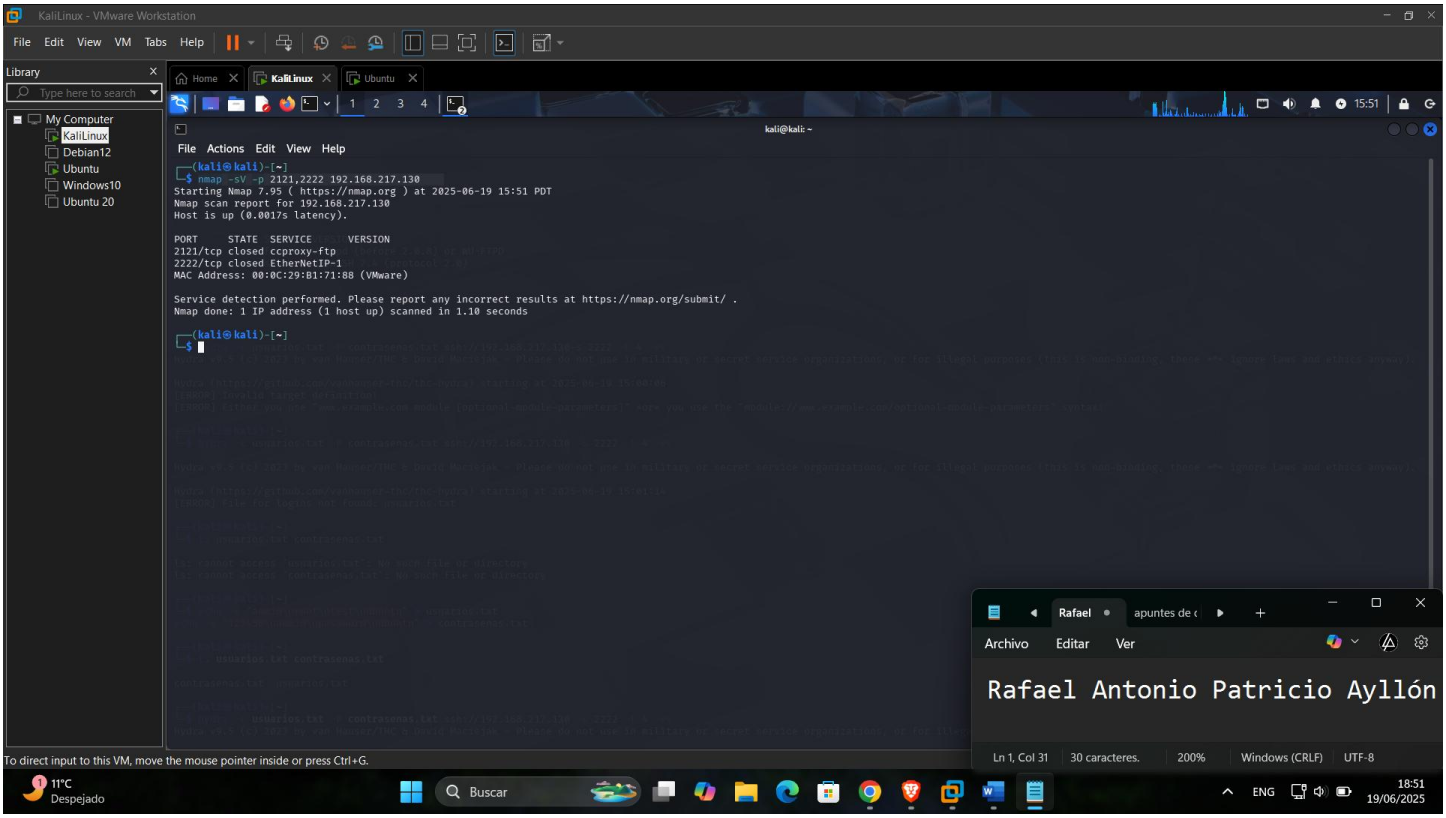
Realiza un ataque de fuerza bruta para obtener credenciales (usuario y/o contraseña) contra el entorno Honeypot. Puedes usar cualquier herramienta o script.

Además, demuestra cómo el Honeypot detecta y registra el ataque: muestra qué script se utilizó, qué credenciales se probaron y cómo se reflejan en los logs del sistema.

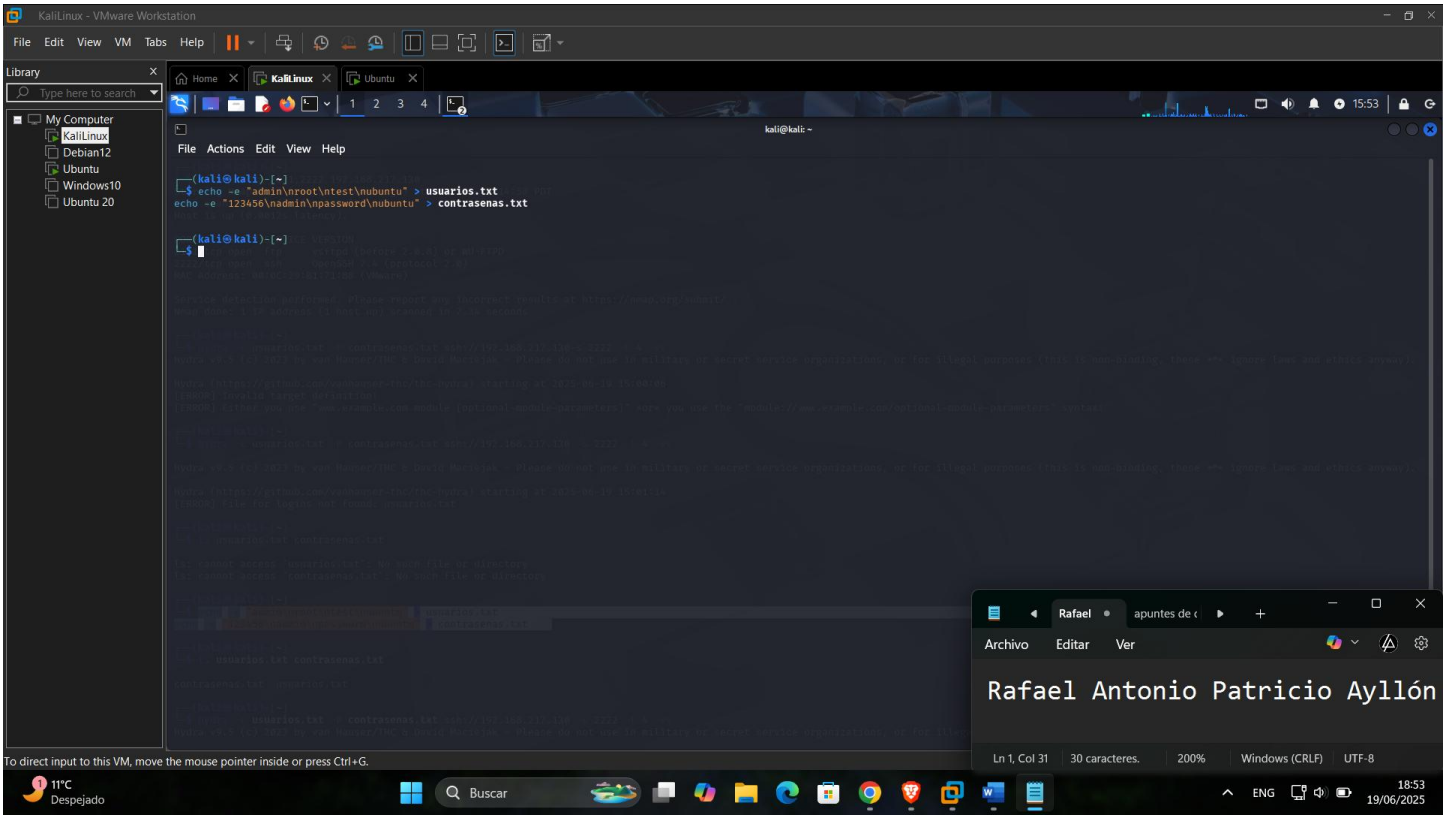
En Kali

Mostrara los puertos abiertos

nmap -sV -p 2121,2222 192.168.217.130

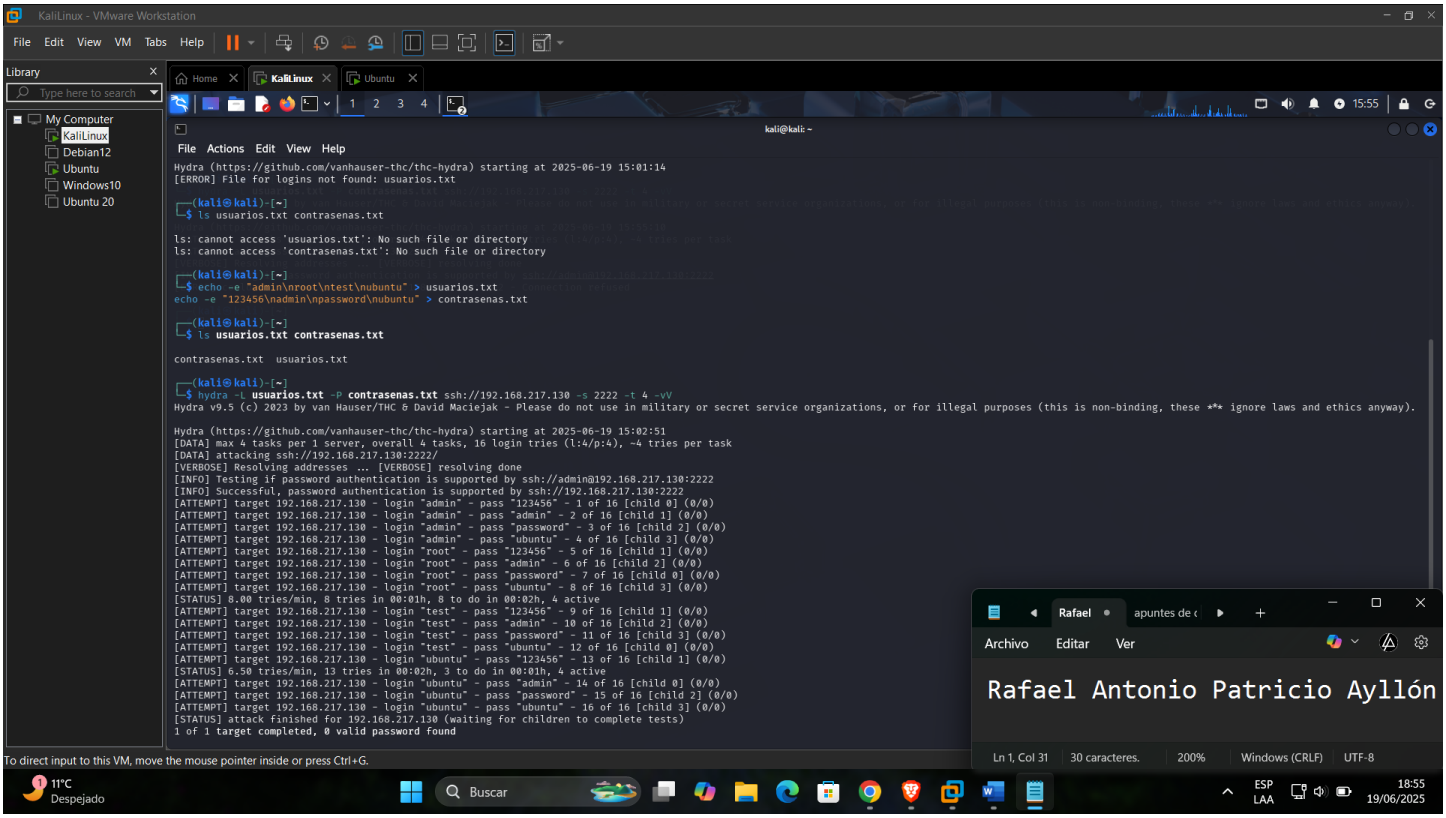


Creamos un archivo de texto para comprobar usuarios y contraseñas

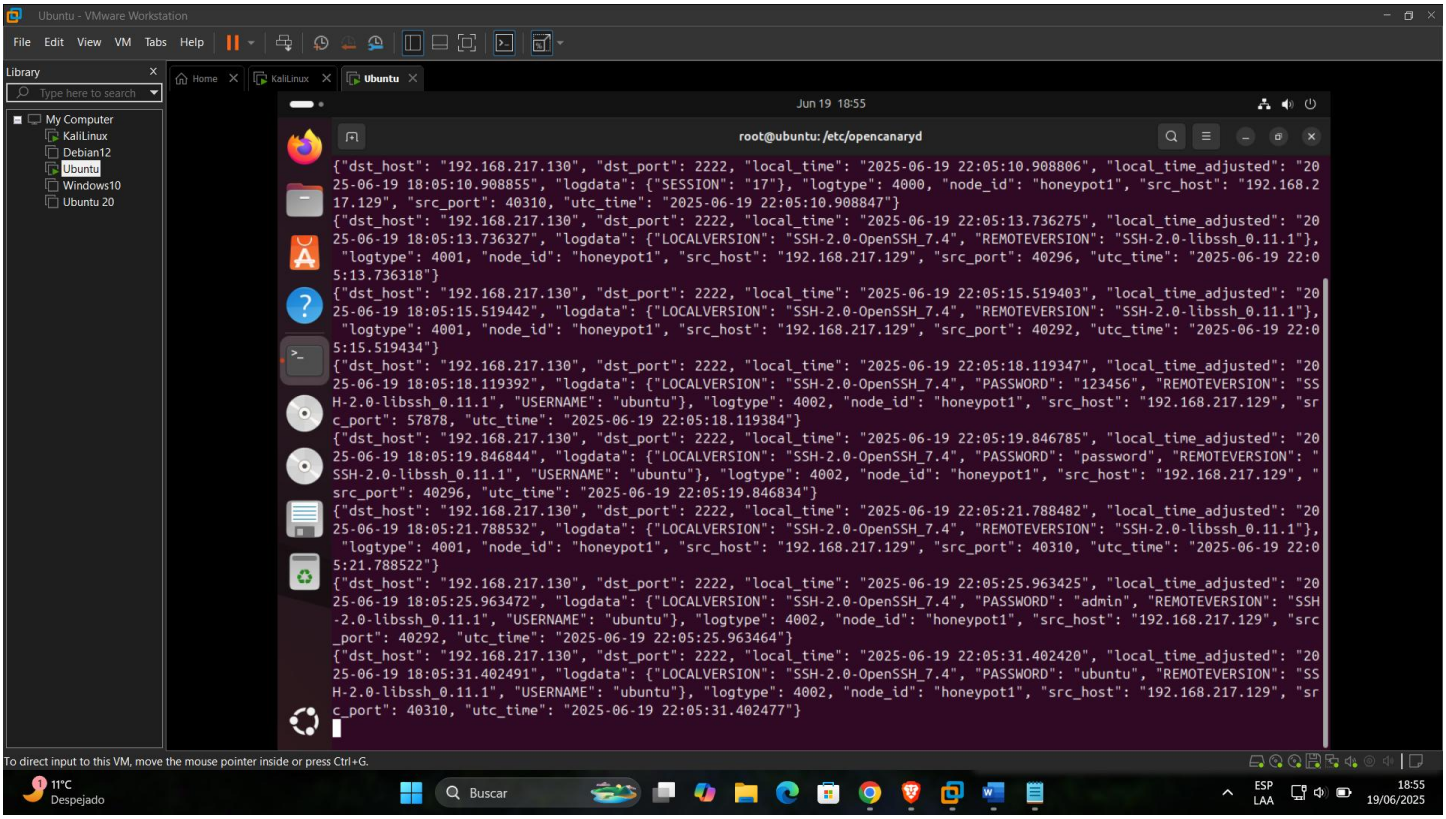


Mediante hydra hacemos el ataque de fuerza bruta

hydra -L usuarios.txt -P contrasenas.txt ssh://192.168.217.130 -s 2222 -t 4 -vV



Verificamos los logs de opencanary



OpenCanary no proporciona acceso SSH real, ni permite que te conectes a una terminal. El servicio de SSH que simula es un honeypot, es decir que acepta conexiones para fingir ser un servidor SSH, pero no da acceso real. Su único propósito es registrar intentos de conexión y autenticación.