

Practica Nº5

Nombre: Rafael Antonio Patricio Ayllon

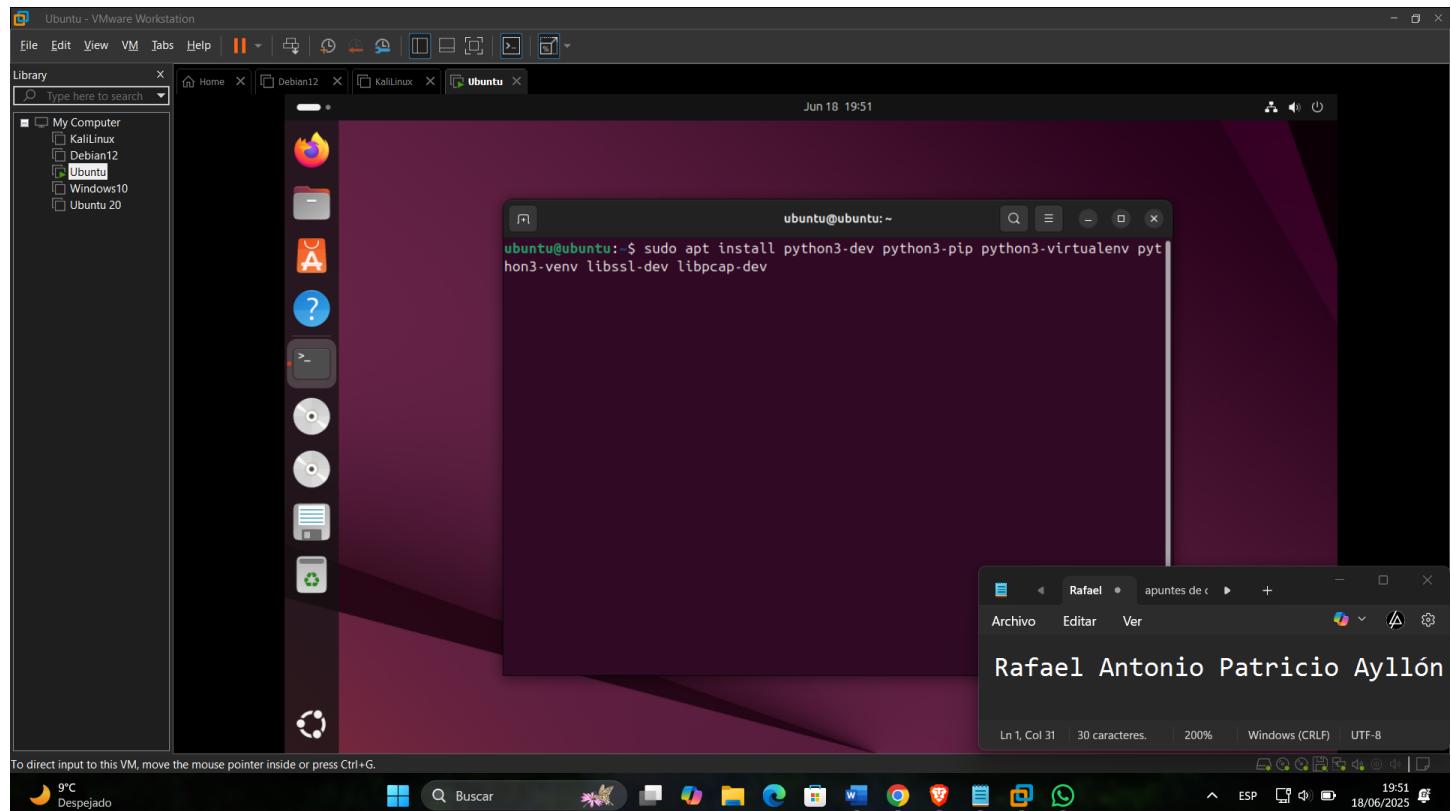
CI: 10473854

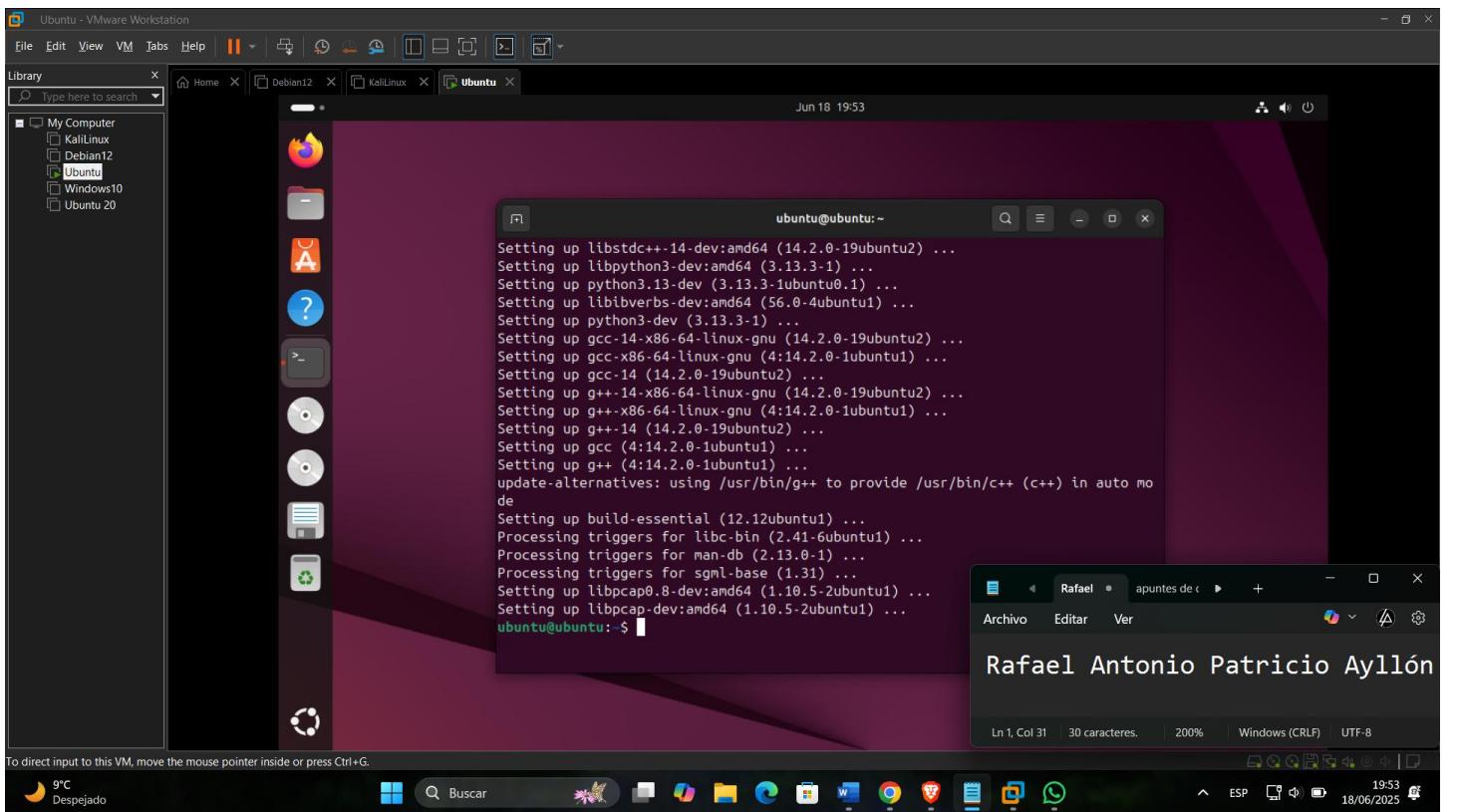
RU: 108771

IMPLEMENTACION:

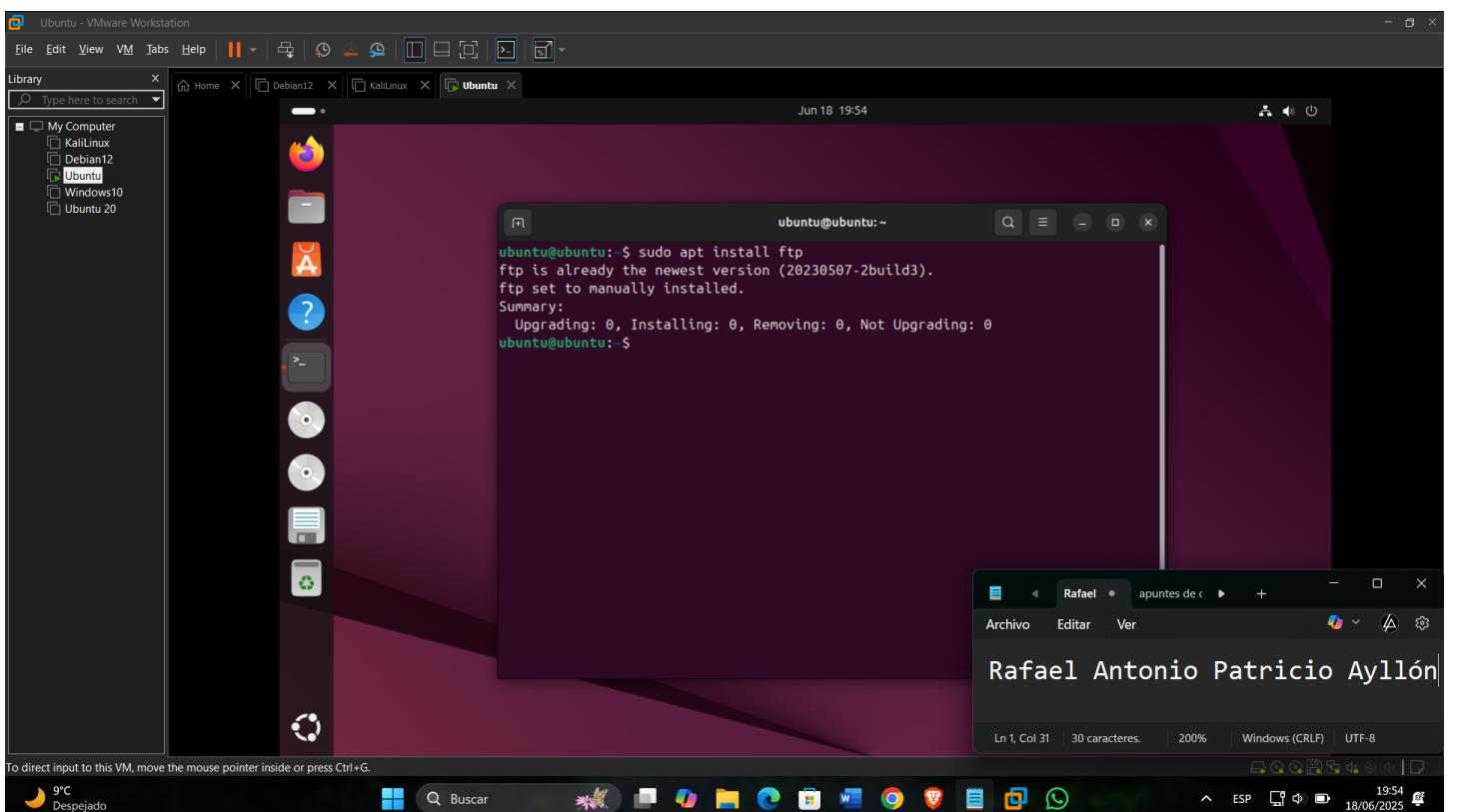
Elegir 1 solo Honeypot de los cuales se muestrra en la lista. En el cual deberá también tener configurados los servicios necesarios, para posteriormente demostrar ataques al Honeypot

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

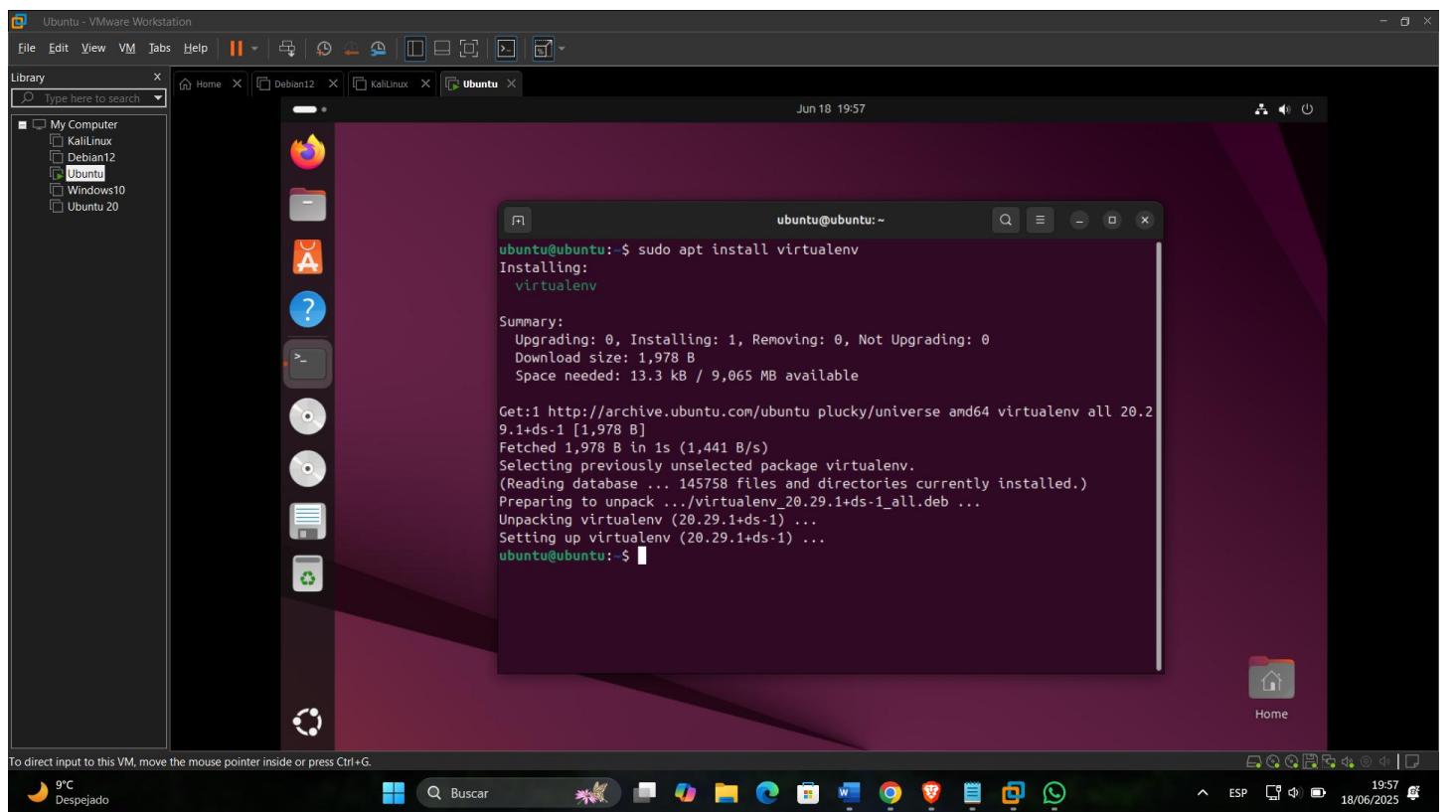




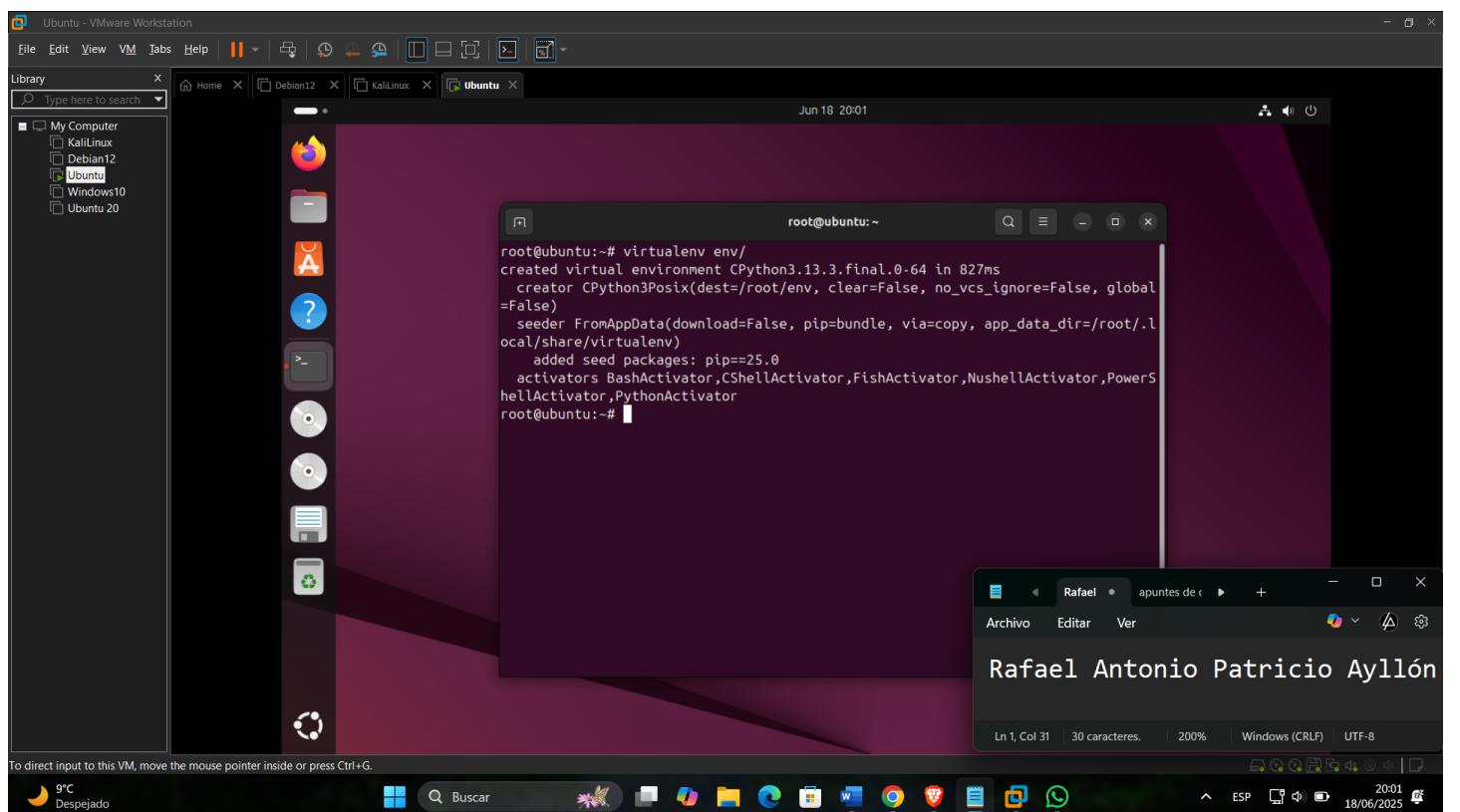
Instalar FTP



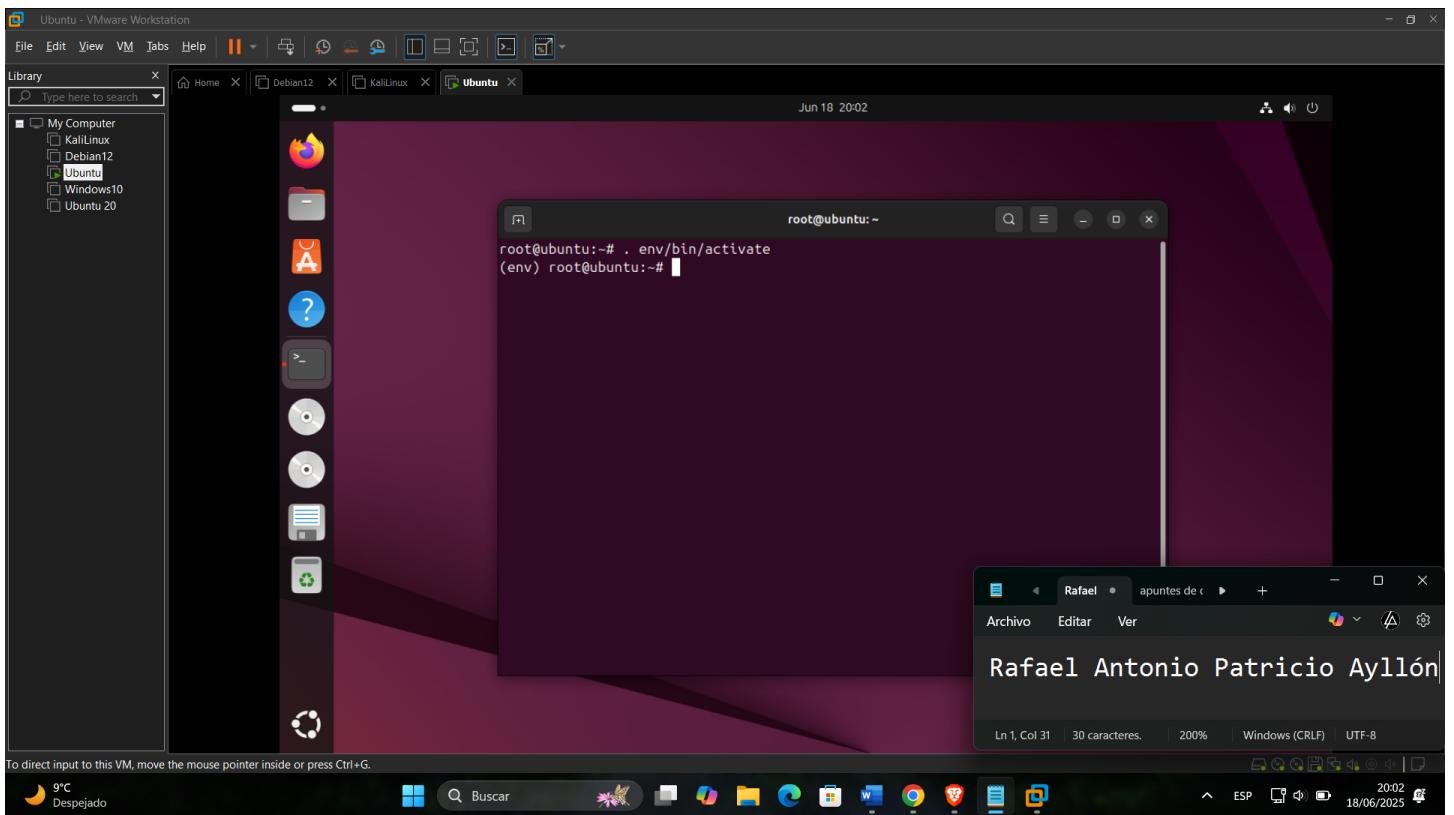
Instalar el virtualizador



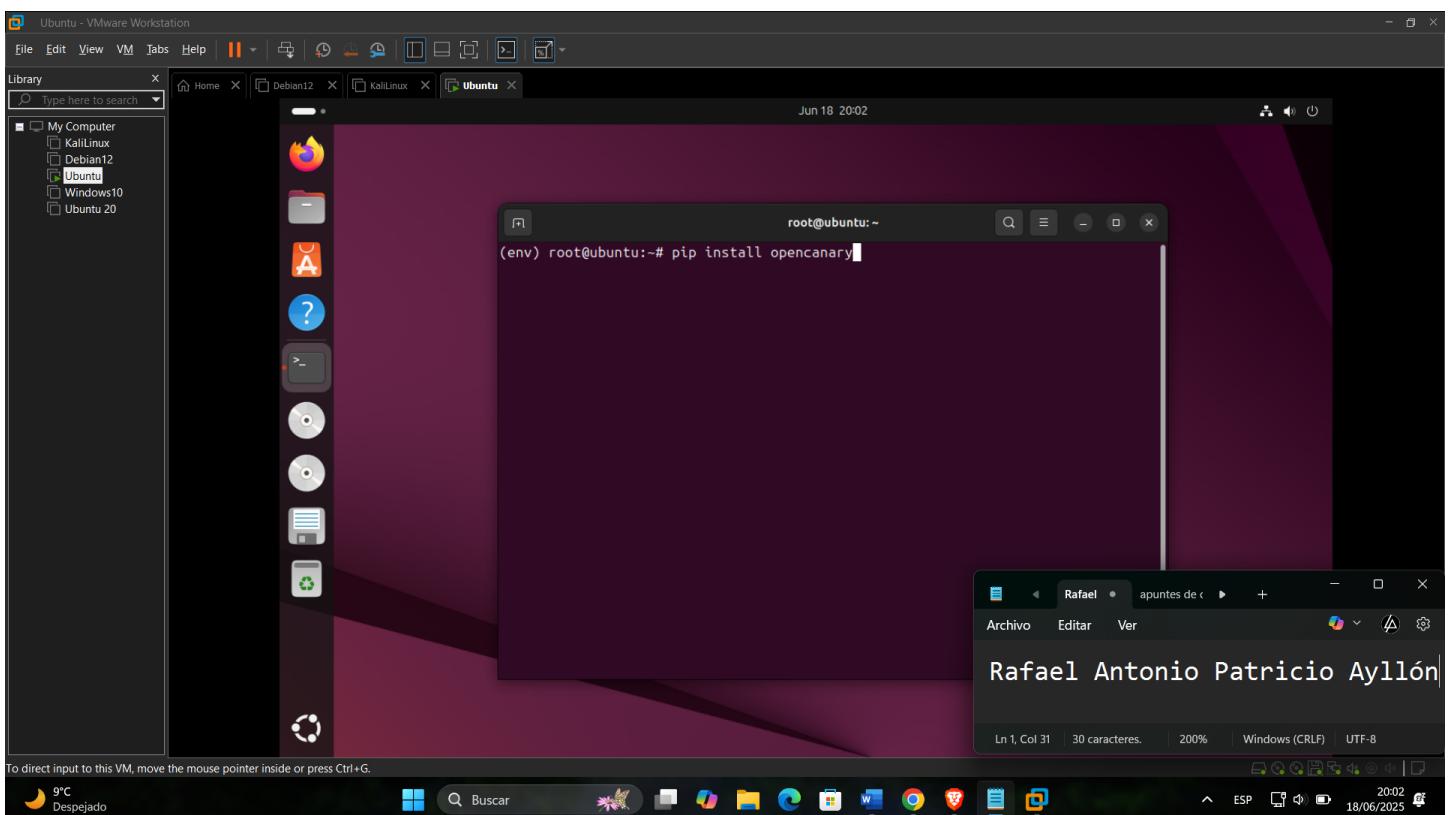
Creamos un entorno virtual

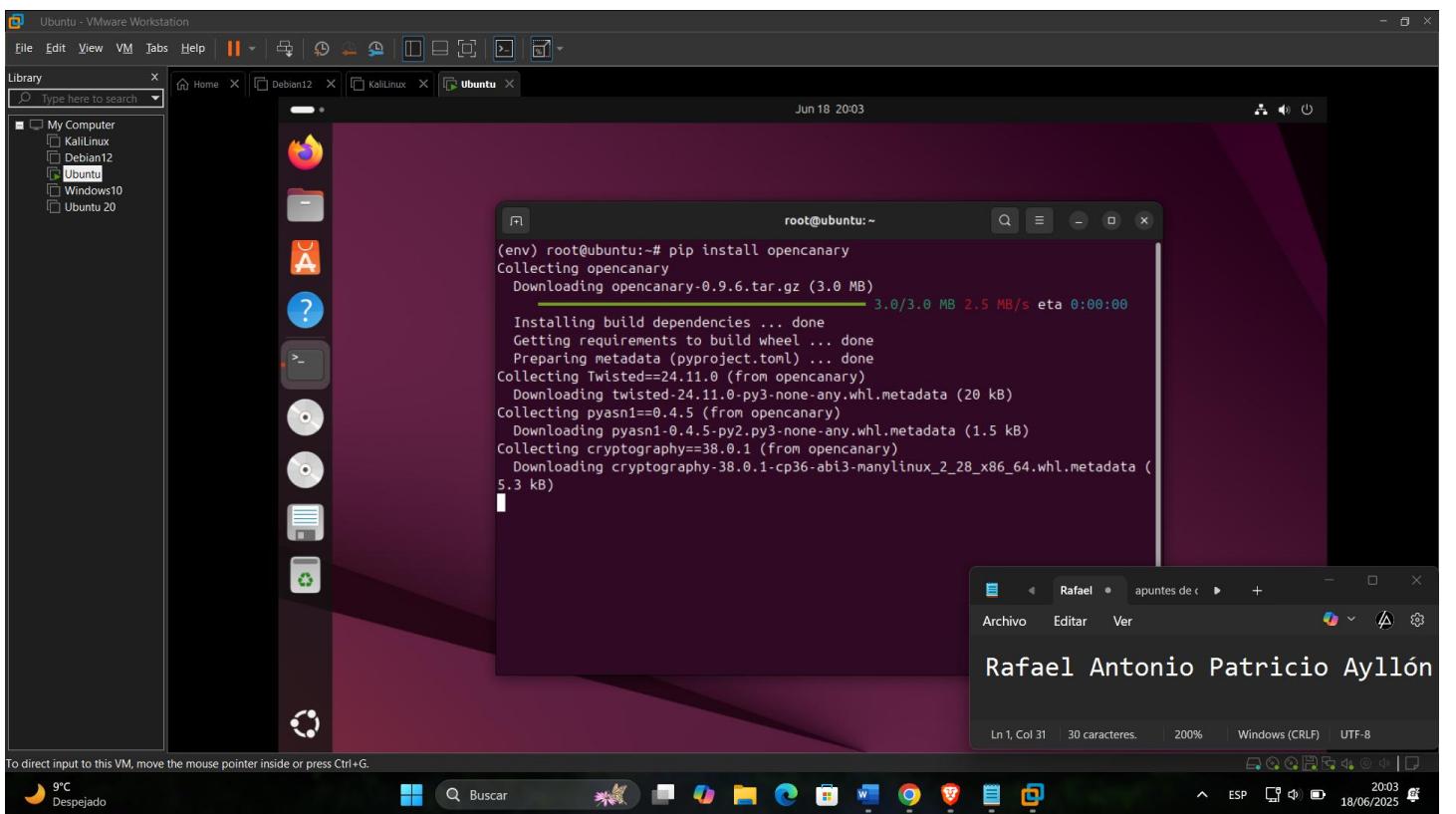


Activamos el entorno virtual

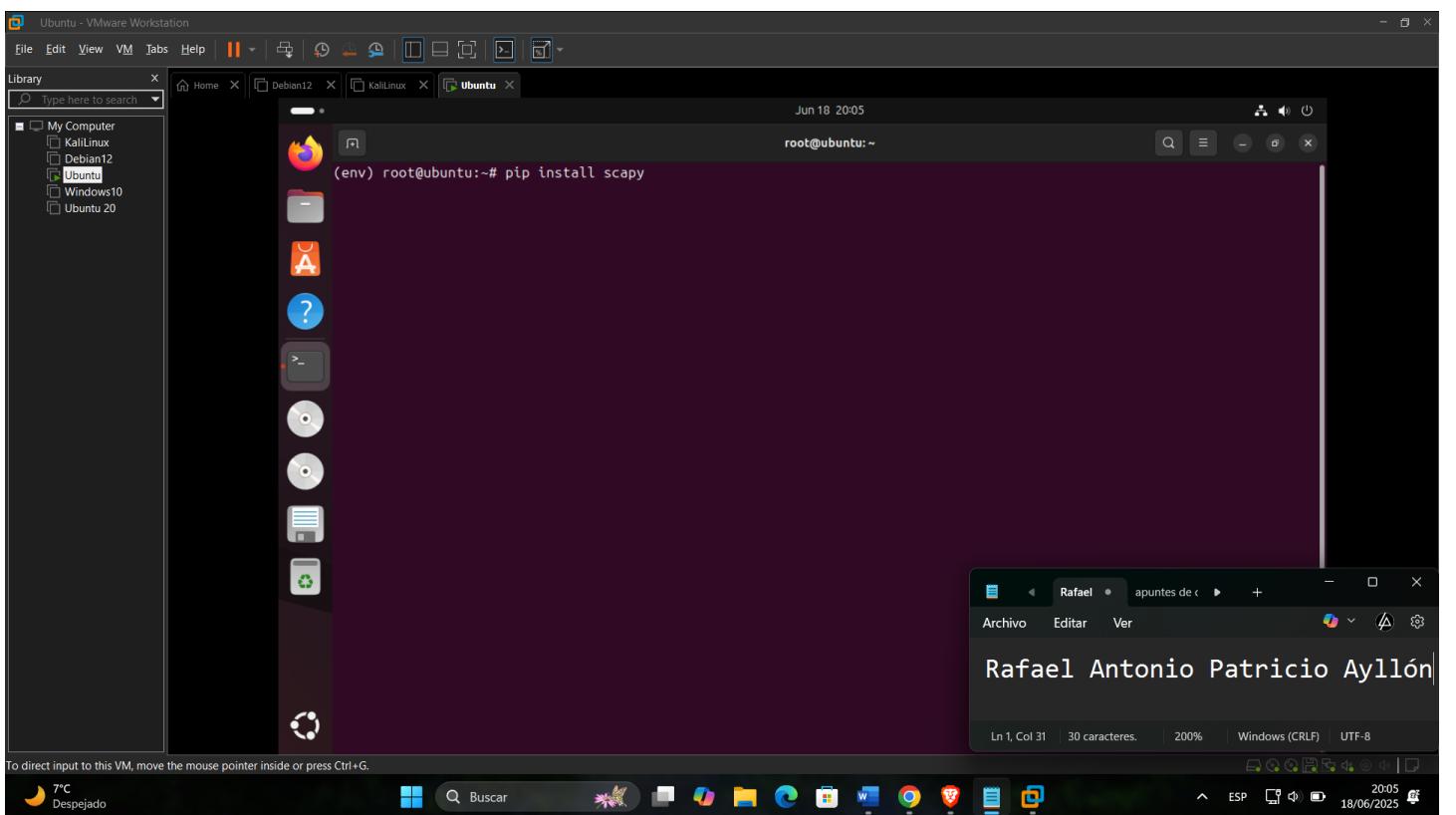


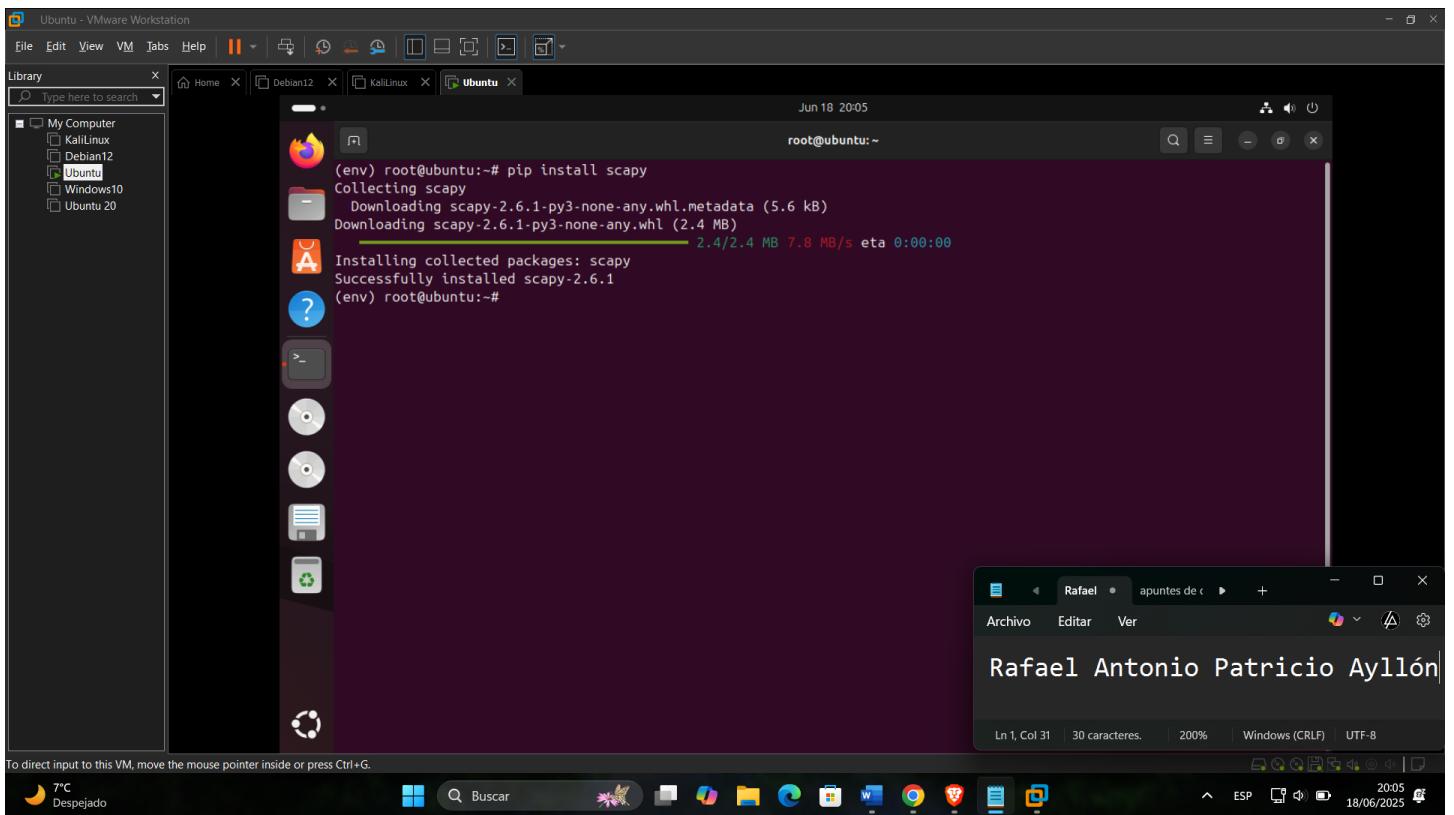
Instalar opencanary



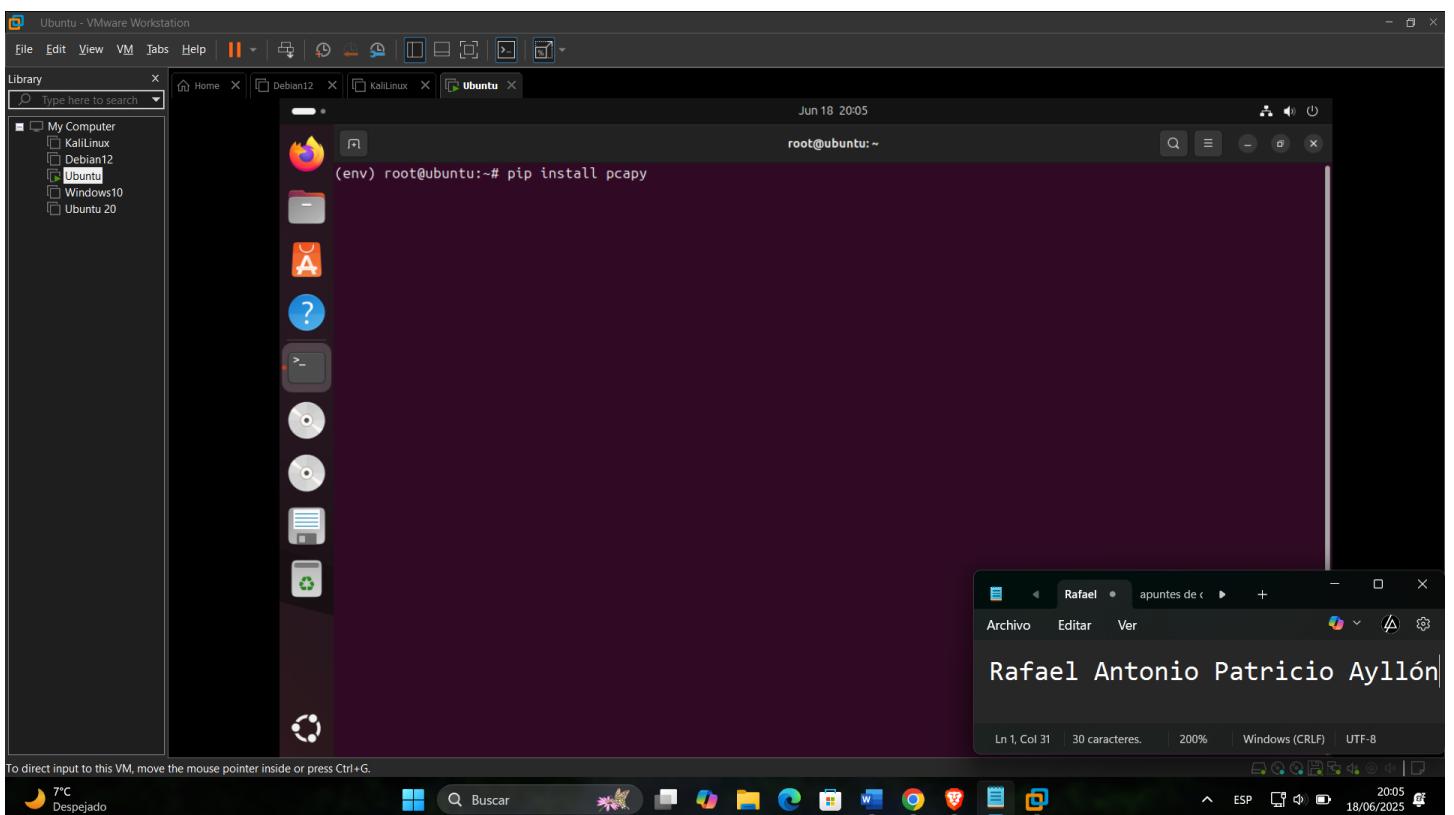


Instalar scapy

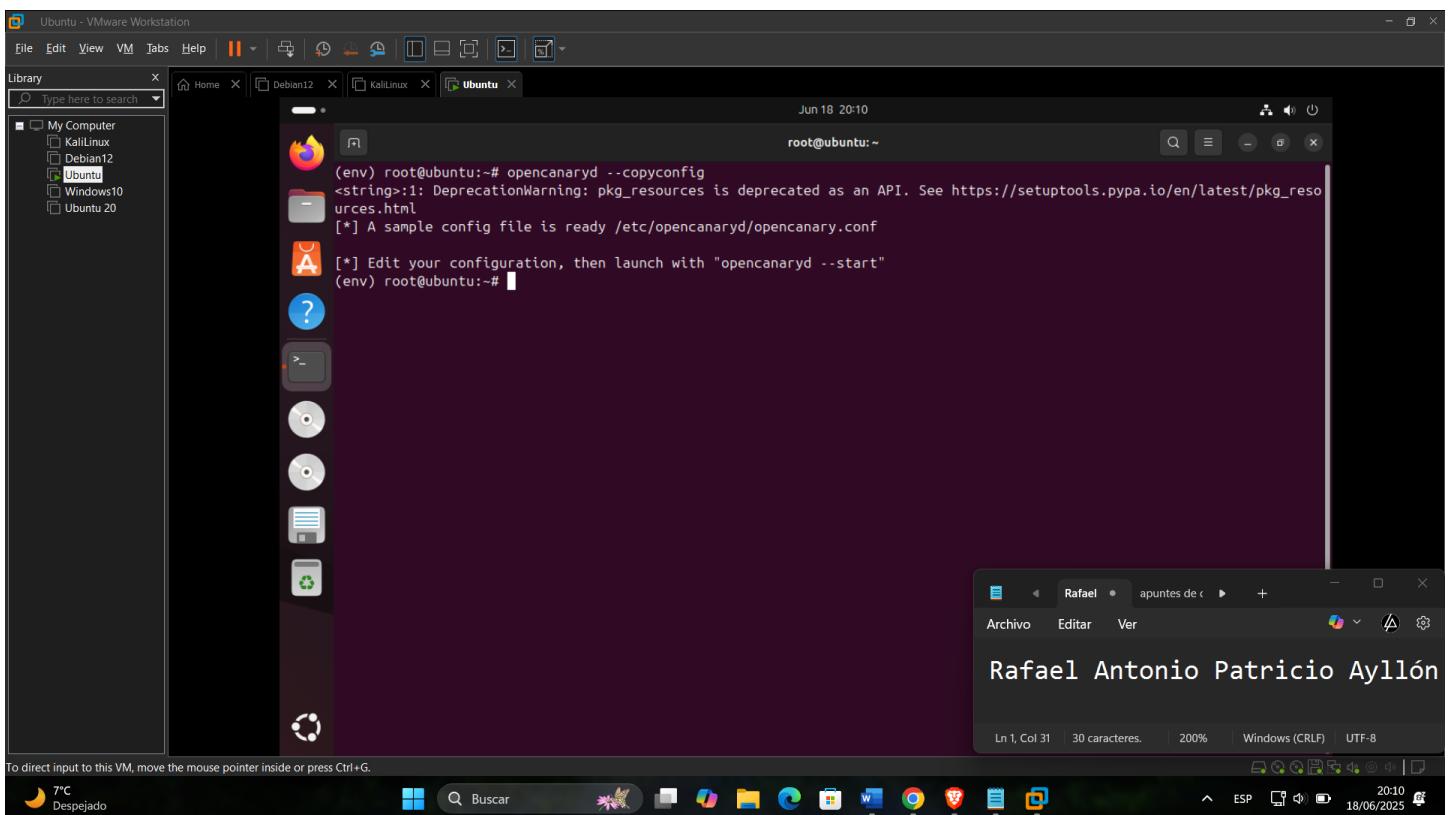
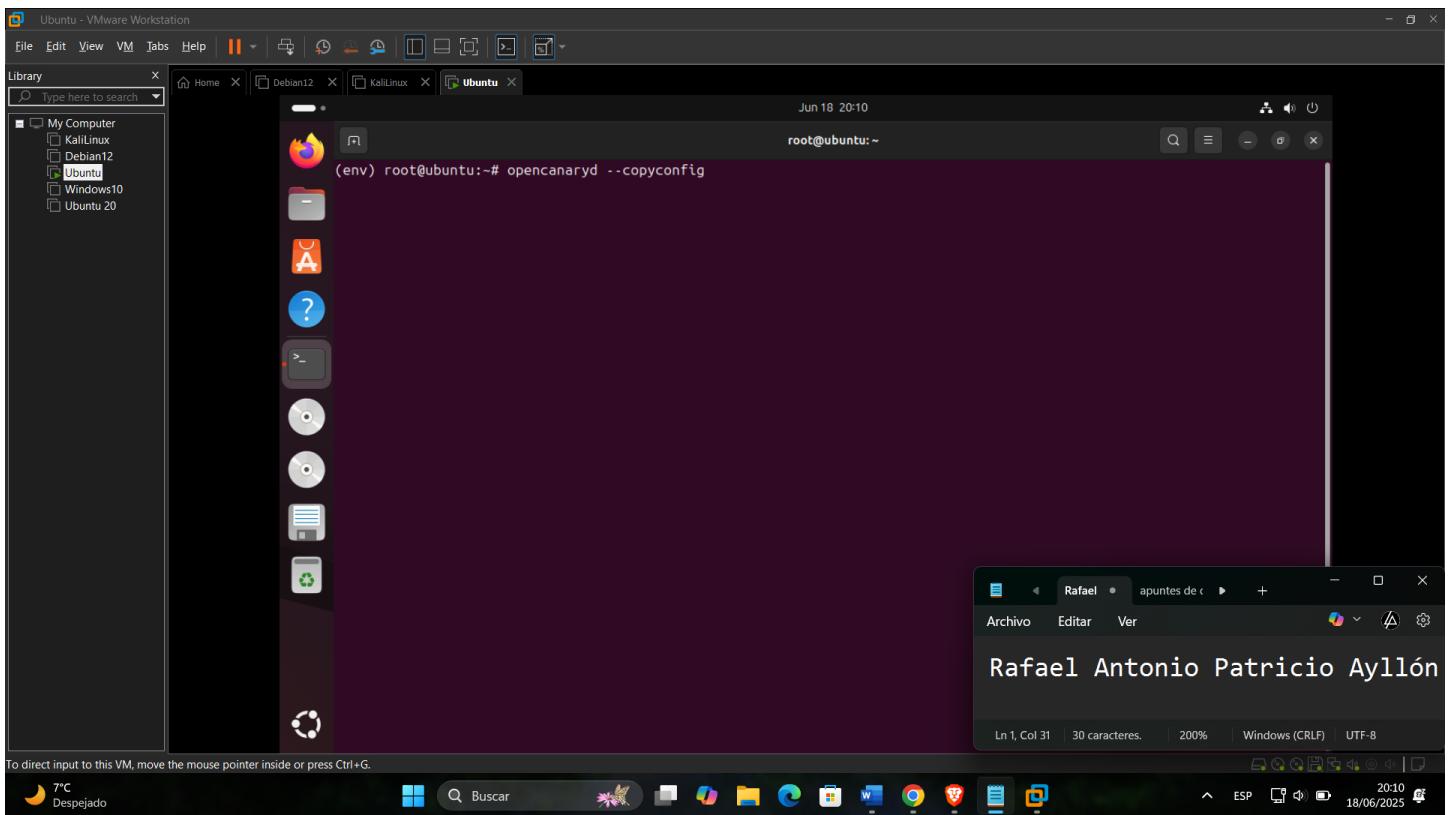




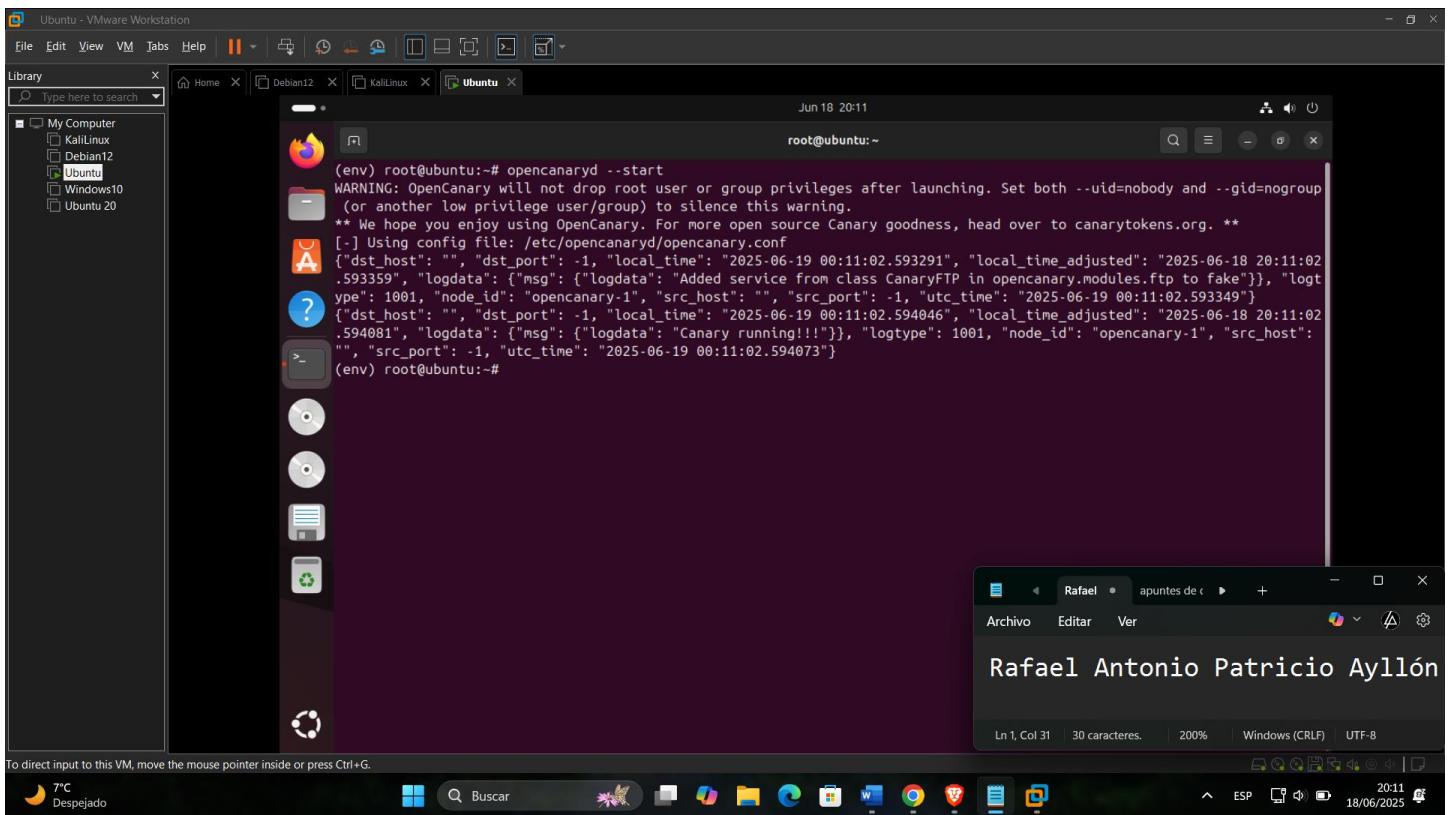
Instalar pcapy



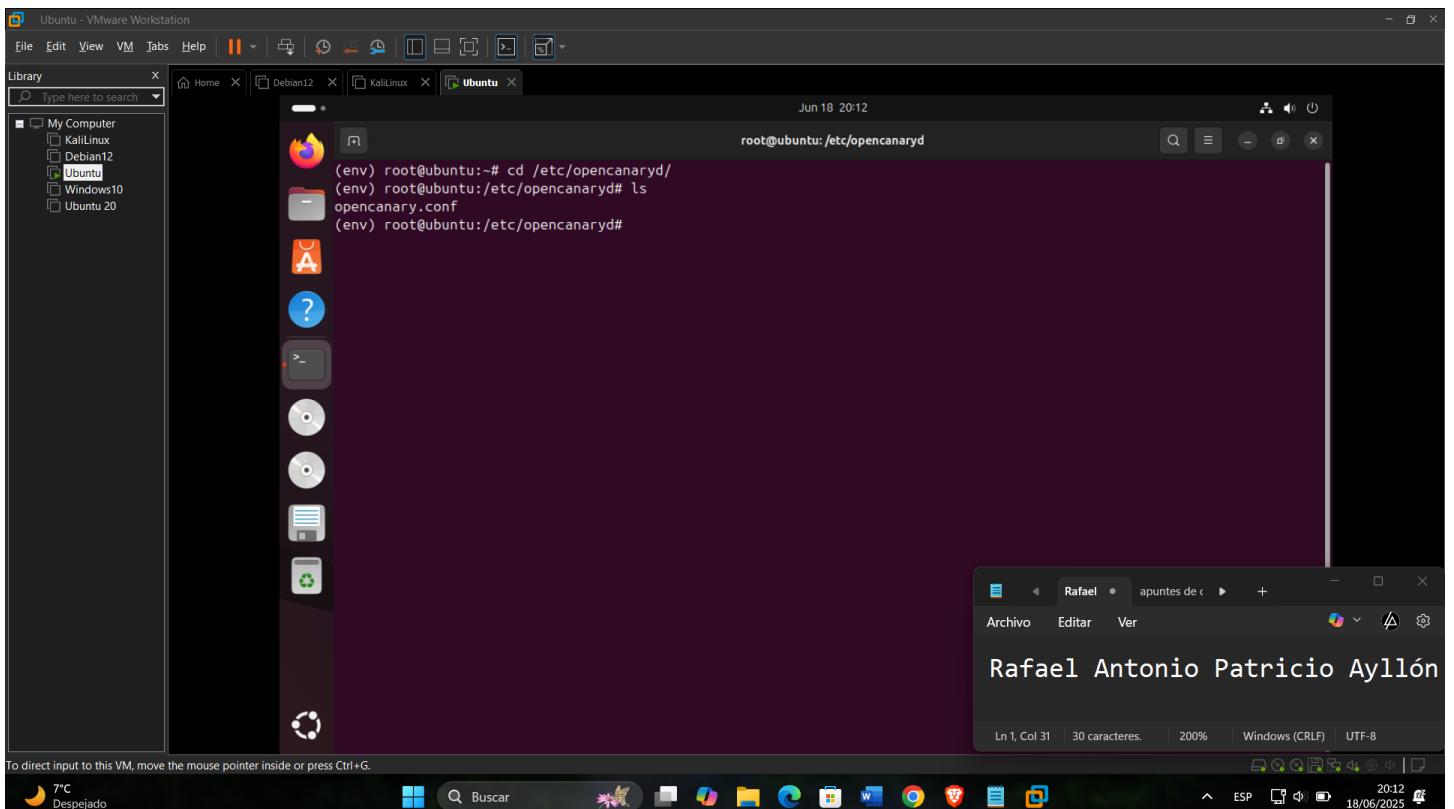
Copiar los archivos de configuración de opencanary



Iniciamos opencanary



Entramos a los archivos de opencanary



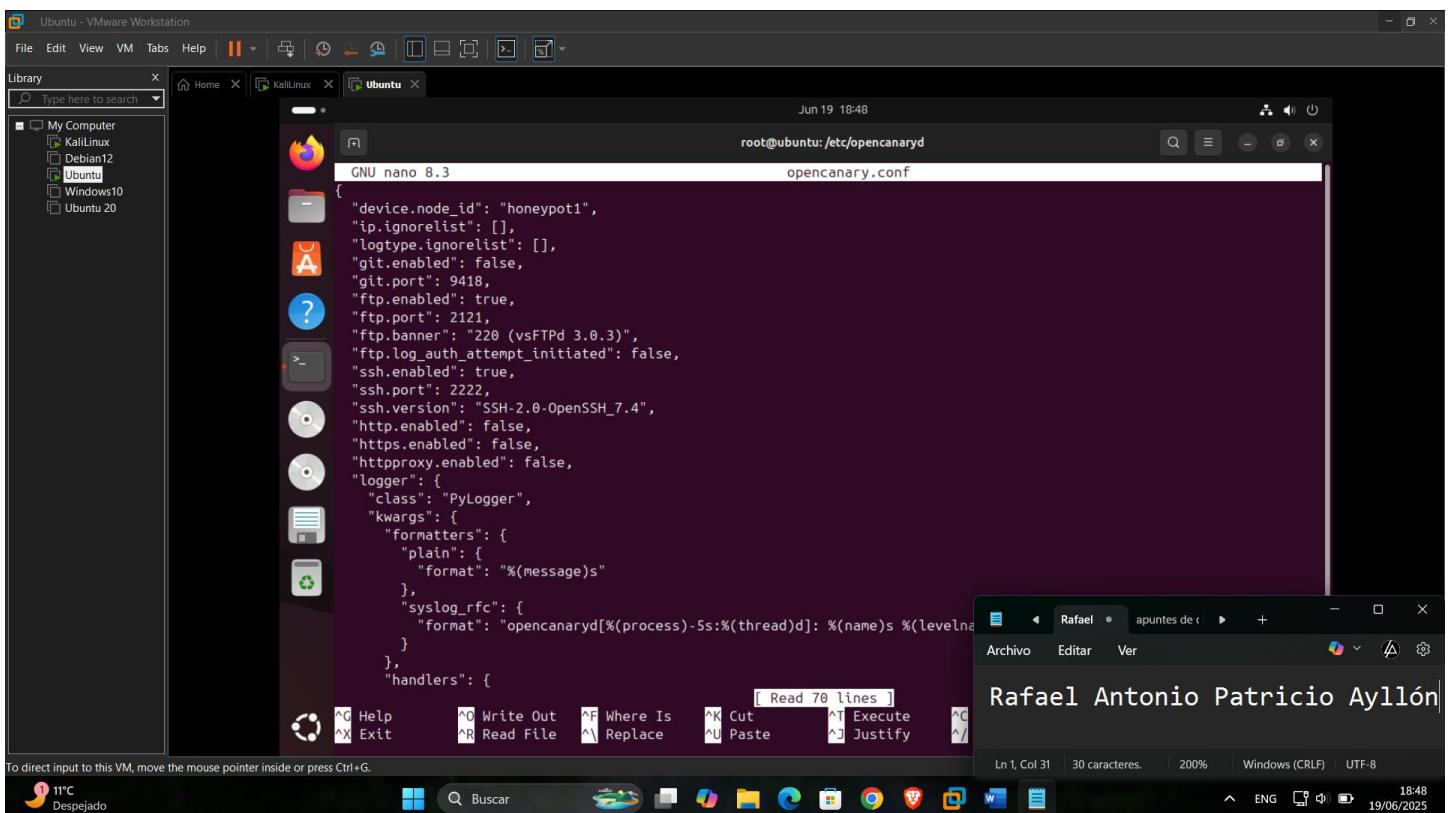
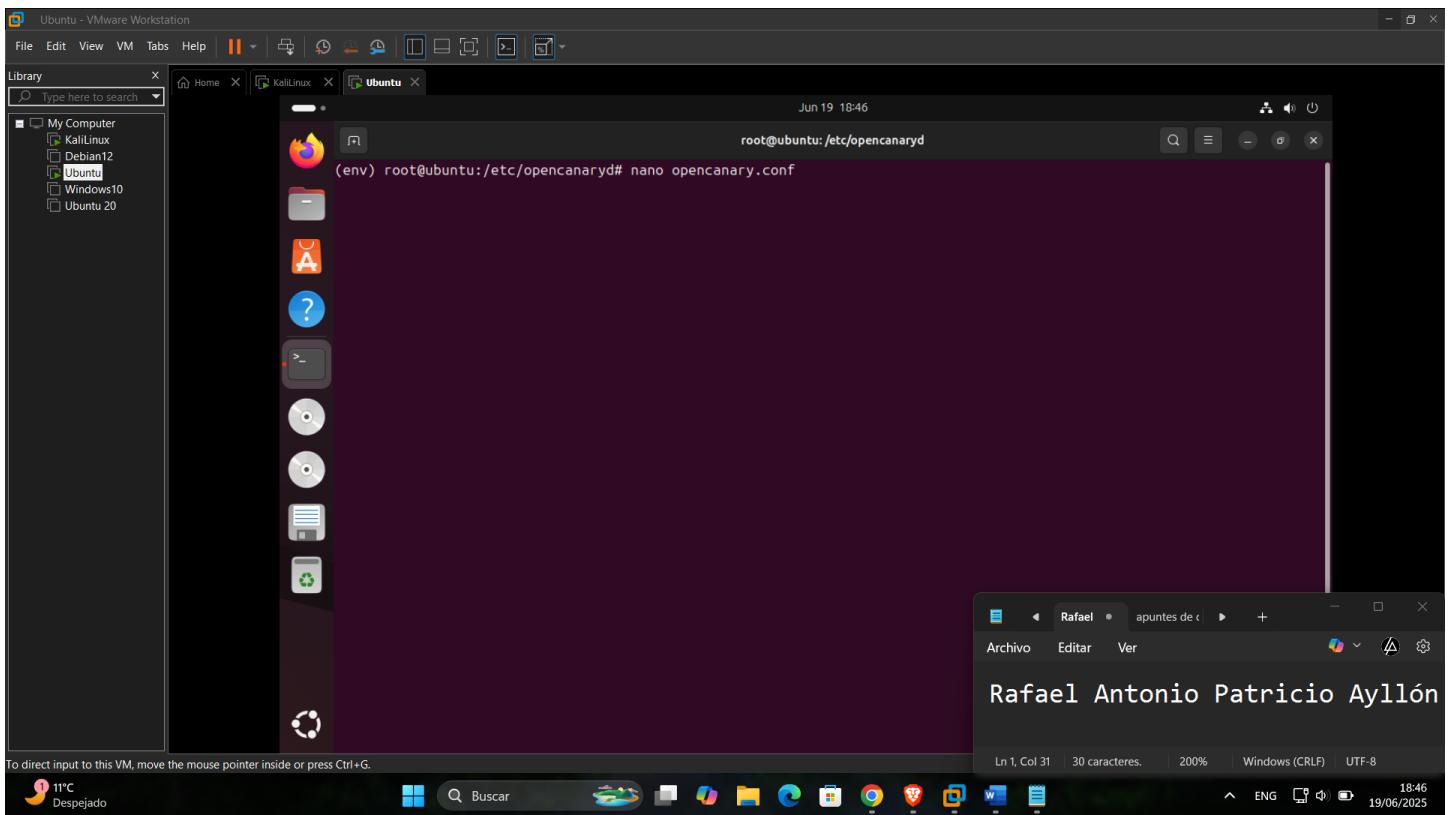
Editar opencanary.conf

{

```
"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"  
            }  
        }  
    }  
}
```

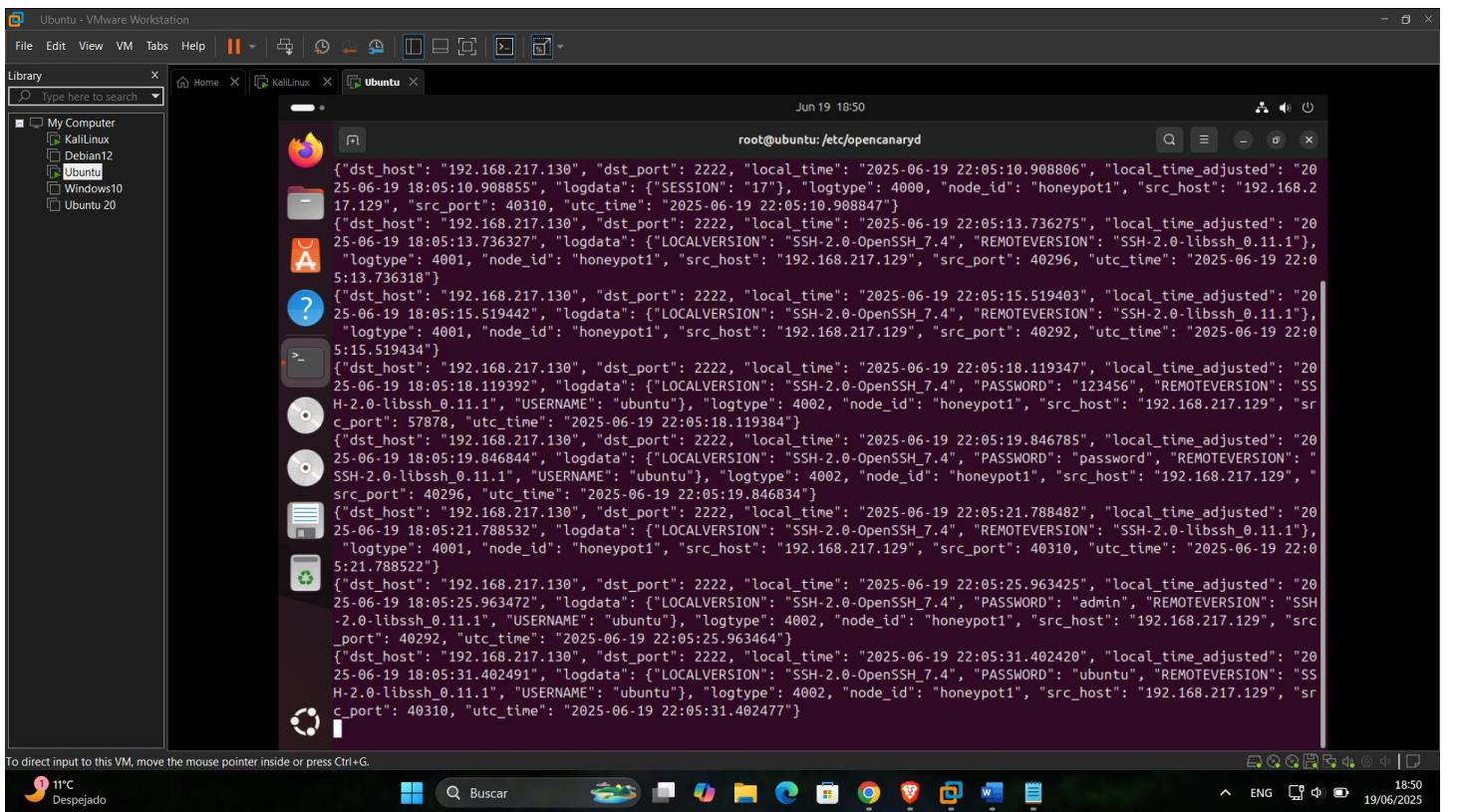
```
},  
"handlers": {  
    "console": {  
        "class": "logging.StreamHandler",  
        "stream": "ext://sys.stdout",  
        "formatter": "plain"  
    },  
    "file": {  
        "class": "logging.FileHandler",  
        "filename": "/var/log/opencanary.log",  
        "formatter": "plain"  
    },  
    "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 verificará 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

Mostrará los puertos abiertos

```
nmap -sV -p 2121,2222 192.168.217.130
```

Creamos un archivo de texto para comprobar usuarios y contraseñas

The screenshot shows a Kali Linux desktop environment with several windows open. The terminal window displays a Hydra password cracking session against a target at 192.168.212.128 port 2222. It also shows an Nmap scan of the same host. A file browser window titled 'My Computer' is visible, showing icons for KaliLinux, Debian12, Ubuntu, Windows10, and Ubuntu 20. A search bar at the top says 'Type here to search'. The status bar at the bottom indicates 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'

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
```

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer KaliLinux Debian12 Ubuntu Windows10 Ubuntu 20

Home KaliLinux Ubuntu

kali@kali: ~

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-19 15:01:14
[ERROR] File for logins not found: usuarios.txt

(kali㉿kali)-[~]
$ ls usuarios.txt contrasenas.txt
ls: cannot access 'usuarios.txt': No such file or directory
ls: cannot access 'contrasenas.txt': No such file or directory

(kali㉿kali)-[~]
$ echo -e "admin\nroot\nnubuntu" > usuarios.txt
echo -e "123456\nadmin\npassword\nnubuntu" > contrasenas.txt

(kali㉿kali)-[~]
$ ls usuarios.txt contrasenas.txt
contrasenas.txt usuarios.txt

(kali㉿kali)-[~]
$ hydra -L usuarios.txt -P contrasenas.txt ssh://192.168.217.130 -s 2222 -t 4 -vv
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these are ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-19 15:02:51
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16 login tries (l:4/p:4), -4 tries per task
[DATA] attacking ssh://192.168.217.130:2222
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://192.168.217.130:2222
[INFO] Successfull, password authentication is supported by ssh://192.168.217.130:2222
[ATTEMPT] target 192.168.217.130 - login "admin" - pass "123456" - 1 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.217.130 - login "root" - pass "root" - 2 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.217.130 - login "admin" - pass "password" - 3 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.217.130 - login "admin" - pass "ubuntu" - 4 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.217.130 - login "root" - pass "123456" - 5 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.217.130 - login "root" - pass "admin" - 6 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.217.130 - login "root" - pass "password" - 7 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.217.130 - login "root" - pass "ubuntu" - 8 of 16 [child 3] (0/0)
[STATISTICS] 0 tries/min, 0 tries in 00:00:01, 0 do in 00:01:01, 4 active
[ATTEMPT] target 192.168.217.130 - login "test" - pass "123456" - 9 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.217.130 - login "test" - pass "admin" - 10 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.217.130 - login "test" - pass "password" - 11 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.217.130 - login "test" - pass "ubuntu" - 12 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.217.130 - login "ubuntu" - pass "123456" - 13 of 16 [child 1] (0/0)
[STATISTICS] 6.50 tries/min, 0 tries in 00:00:01, 0 do in 00:01:01, 4 active
[ATTEMPT] target 192.168.217.130 - login "ubuntu" - pass "password" - 14 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.217.130 - login "ubuntu" - pass "password" - 15 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.217.130 - login "ubuntu" - pass "ubuntu" - 16 of 16 [child 3] (0/0)
[STATUS] attack finished for 192.168.217.130 (waiting for children to complete tests)

1 of 1 target completed, 0 valid password found
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Rafael Antonio Patricio Ayllón

Archivo Editar Ver

Ln 1, Col 31 30 caracteres. 200% Windows (CRLF) UTF-8

11°C Despejado

Buscar

ESP LAA 18:55 19/06/2025

Verificamos los logs de opencanary

Ubuntu - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer KaliLinux Debian12 Ubuntu Windows10 Ubuntu 20

Home KaliLinux Ubuntu

Jun 19 18:55

root@ubuntu:/etc/opencanary

```
{"dst_host": "192.168.217.130", "dst_port": 2222, "local_time": "2025-06-19 22:05:10.908806", "local_time_adjusted": "2025-06-19 18:05:10.908855", "logdata": {"SESSION": "17"}, "logtype": 4000, "node_id": "honeypot1", "src_host": "192.168.217.129", "src_port": 40310, "utc_time": "2025-06-19 22:05:10.908847"} {"dst_host": "192.168.217.130", "dst_port": 2222, "local_time": "2025-06-19 22:05:13.736275", "local_time_adjusted": "2025-06-19 18:05:13.736327", "logdata": {"LOCALVERSION": "SSH-2.0-OpenSSH_7.4", "REMOTEVERSION": "SSH-2.0-libssh_0.11.1"}, "logtype": 4001, "node_id": "honeypot1", "src_host": "192.168.217.129", "src_port": 40296, "utc_time": "2025-06-19 22:05:13.736318"} {"dst_host": "192.168.217.130", "dst_port": 2222, "local_time": "2025-06-19 22:05:15.519403", "local_time_adjusted": "2025-06-19 18:05:15.519442", "logdata": {"LOCALVERSION": "SSH-2.0-OpenSSH_7.4", "REMOTEVERSION": "SSH-2.0-libssh_0.11.1"}, "logtype": 4001, "node_id": "honeypot1", "src_host": "192.168.217.129", "src_port": 40292, "utc_time": "2025-06-19 22:05:15.519434"} {"dst_host": "192.168.217.130", "dst_port": 2222, "local_time": "2025-06-19 22:05:18.119347", "local_time_adjusted": "2025-06-19 18:05:18.119392", "logdata": {"LOCALVERSION": "SSH-2.0-OpenSSH_7.4", "PASSWORD": "123456", "REMOTEVERSION": "SSH-2.0-libssh_0.11.1"}, "logtype": 4002, "node_id": "honeypot1", "src_host": "192.168.217.129", "src_port": 57878, "utc_time": "2025-06-19 22:05:18.119384"} {"dst_host": "192.168.217.130", "dst_port": 2222, "local_time": "2025-06-19 22:05:19.846785", "local_time_adjusted": "2025-06-19 18:05:19.846844", "logdata": {"LOCALVERSION": "SSH-2.0-OpenSSH_7.4", "PASSWORD": "password", "REMOTEVERSION": "SSH-2.0-libssh_0.11.1"}, "logtype": 4002, "node_id": "honeypot1", "src_host": "192.168.217.129", "src_port": 40296, "utc_time": "2025-06-19 22:05:19.846834"} {"dst_host": "192.168.217.130", "dst_port": 2222, "local_time": "2025-06-19 22:05:21.788532", "local_time": "2025-06-19 22:05:21.788532", "logdata": {"LOCALVERSION": "SSH-2.0-OpenSSH_7.4", "REMOTEVERSION": "SSH-2.0-libssh_0.11.1"}, "logtype": 4001, "node_id": "honeypot1", "src_host": "192.168.217.129", "src_port": 40310, "utc_time": "2025-06-19 22:05:21.788522"} {"dst_host": "192.168.217.130", "dst_port": 2222, "local_time": "2025-06-19 22:05:25.963425", "local_time_adjusted": "2025-06-19 18:05:25.963472", "logdata": {"LOCALVERSION": "SSH-2.0-OpenSSH_7.4", "PASSWORD": "admin", "REMOTEVERSION": "SSH-2.0-libssh_0.11.1"}, "logtype": 4002, "node_id": "honeypot1", "src_host": "192.168.217.129", "src_port": 40292, "utc_time": "2025-06-19 22:05:25.963464"} {"dst_host": "192.168.217.130", "dst_port": 2222, "local_time": "2025-06-19 22:05:31.402420", "local_time_adjusted": "2025-06-19 18:05:31.402491", "logdata": {"LOCALVERSION": "SSH-2.0-OpenSSH_7.4", "PASSWORD": "ubuntu", "REMOTEVERSION": "SSH-2.0-libssh_0.11.1"}, "logtype": 4002, "node_id": "honeypot1", "src_host": "192.168.217.129", "src_port": 40310, "utc_time": "2025-06-19 22:05:31.402477"} To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

11°C Despejado

Buscar

ESP LAA 18:55 19/06/2025

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.