
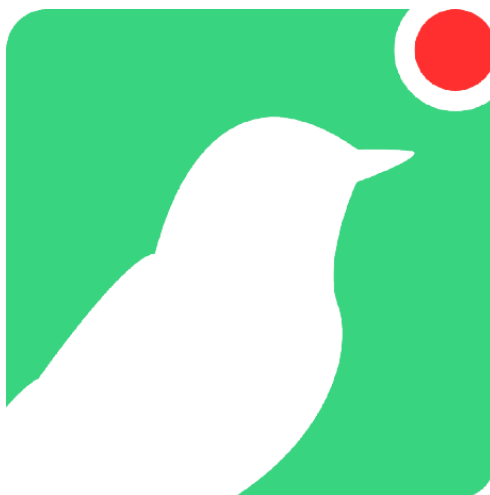


<u>UNIVERSIDAD AUTÓNOMA “TOMAS FRÍAS”</u> <u>CARRERA DE INGENIERÍA DE SISTEMAS</u>				
Materia:	Seguridad de sistemas (SIS-737)			
Docente:	M.Sc. Ing. Javier Alexander Durán Miranda Univ. Aldrin Roger Perez Miranda			Nº Práctica
Auxiliar:				5
Estudiante CI	Sandra choque garnica 8507099			
Grupo:	1	Sede	Potosí	

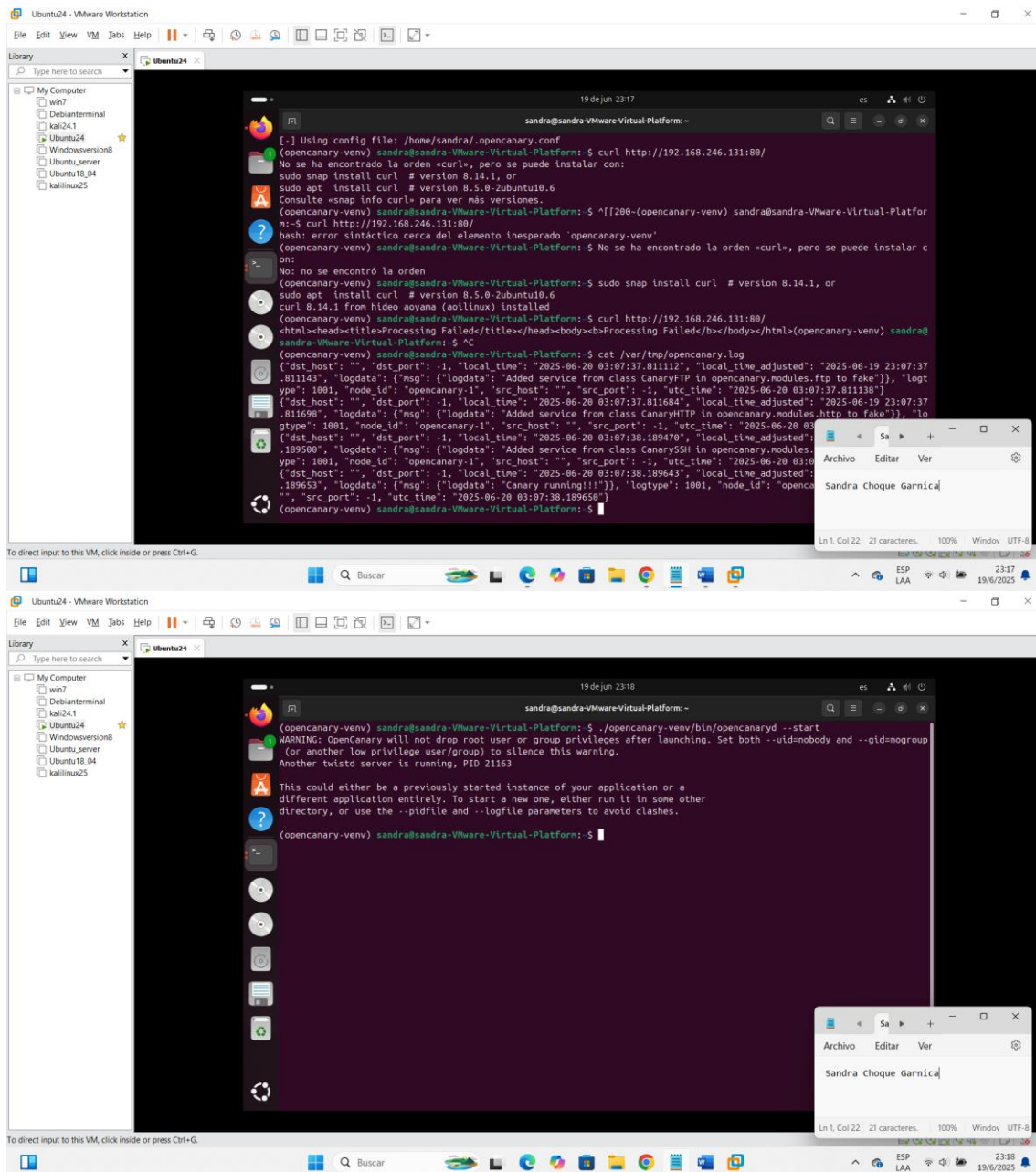
IMPLEMENTACION:

Elegir 1 solo Honeypot de los cuales se muestra en la lista. En el cual deberá también tener configurados los servicios necesarios, para posteriormente demostrar ataques al Honeypot **(50 pts)**

OpenCanary



Muy fácil de configurar (Python)
 Simula múltiples servicios (SSH, HTTP, RDP, MySQL, SMB)
 Guarda logs en formato legible (JSON, Syslog, Splunk)
 Enlace: <https://github.com/thinkst/opencanary>



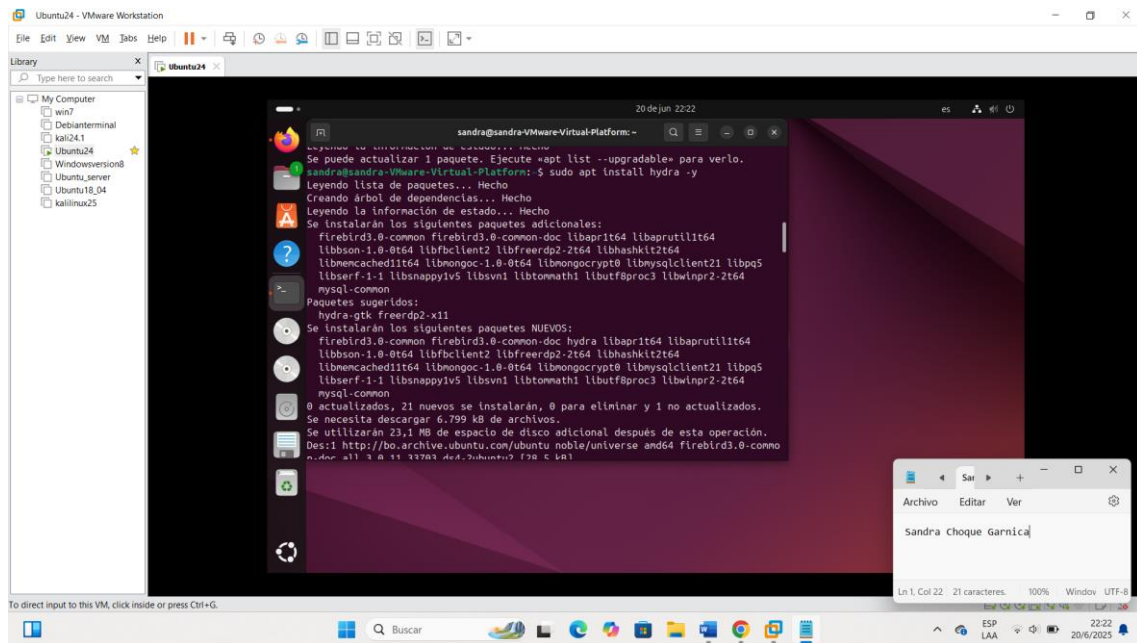
ATAQUE:

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**.

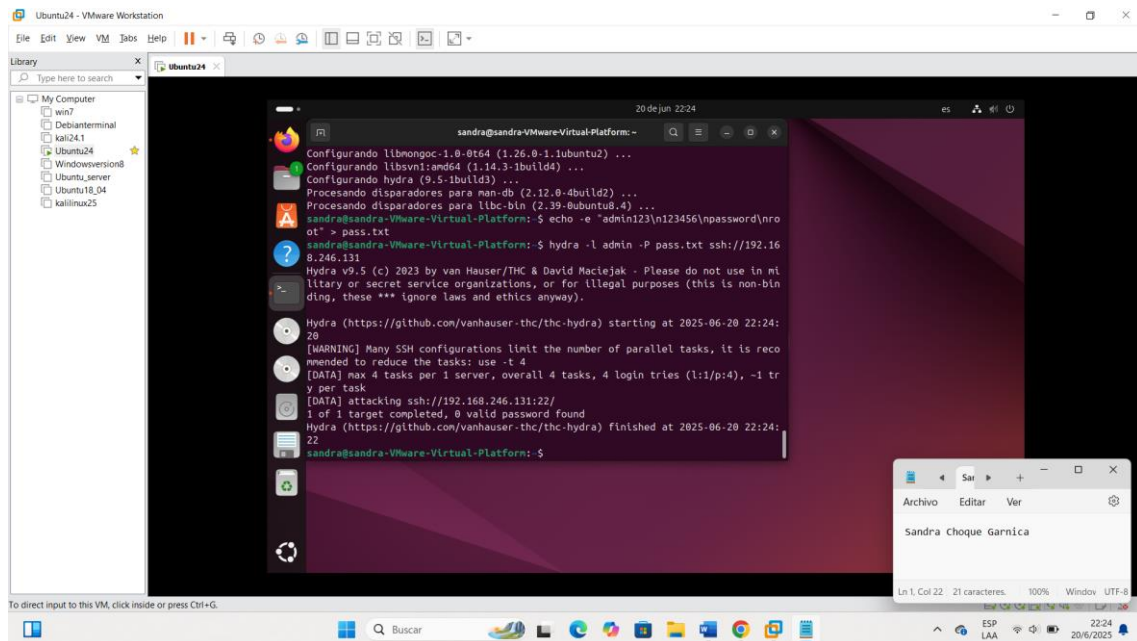
Realiza un ataque de **fuerza bruta** para obtener credenciales (usuario y/o contraseña) contra el entorno **Honeypot**. Puedes usar cualquier herramienta o script.

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. (50 pts)

-instalación de hidra

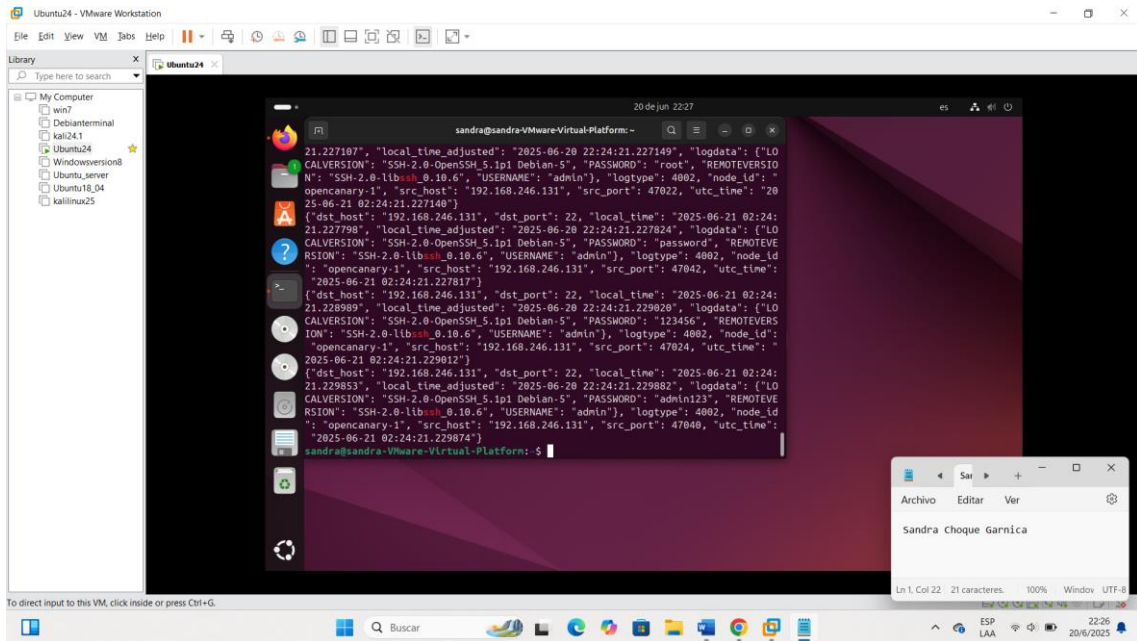


--creamos un archivo de contraseñas



-ejecutamos el ataque en hydra

-ver el ataque de los logs



-ataque detectado

