Universidad Gerardo Barrios

Comisión de Acreditación de la Calidad de la Educación Superior
UNIVERSIDAD GERARDO BARRIOS (UGB)
ACREDITADA
2024-2029

FACULTAD DE CIENCIA Y TECNOLOGÍA

Asignatura: Seguridad informática.

Docente: Ing. Timotea Guadalupe Menjívar.

Tema: Desencriptando credenciales con Parrot Security.

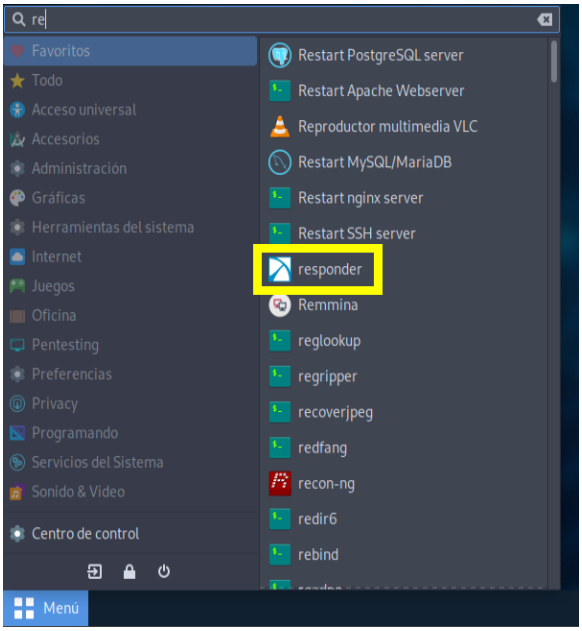
Carrera: Ingeniería en sistemas y redes informáticas.

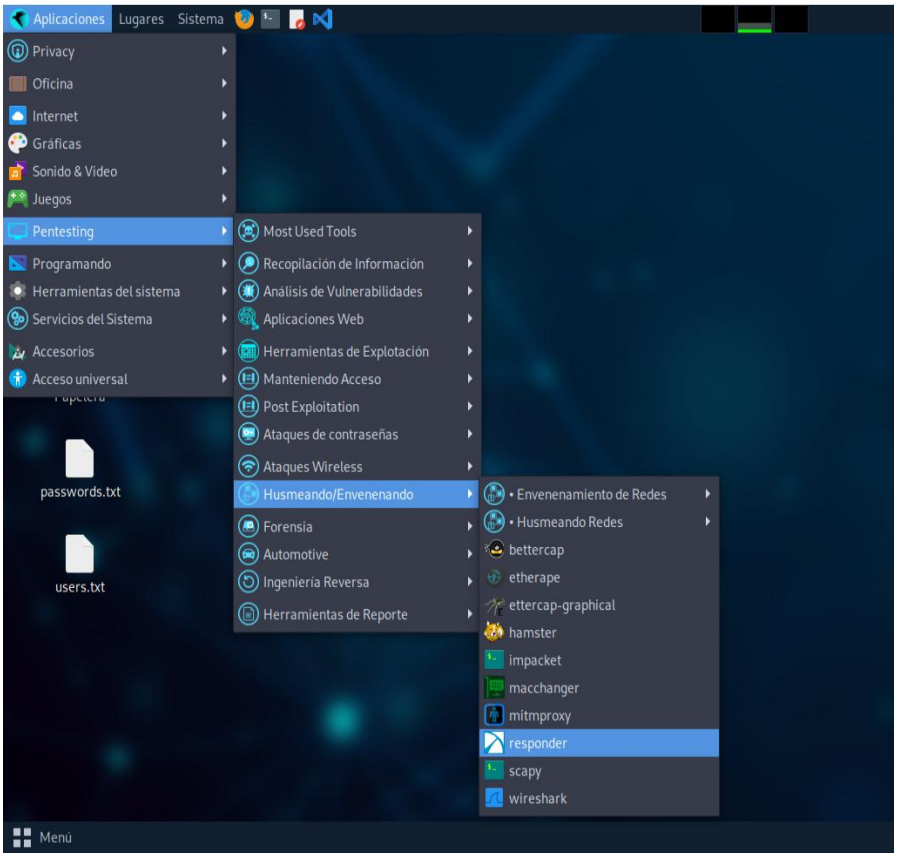
Estudiante: Romeo Alexander Garcia Castillo.

Usulután, miércoles 8 de octubre de 2025.

Para resolver esta práctica usaremos la herramienta **responder.py** la cual puede responder a las consultas LLMNR y NBT-NS, dando su propia dirección IP como destino para cualquier nombre de host solicitado.

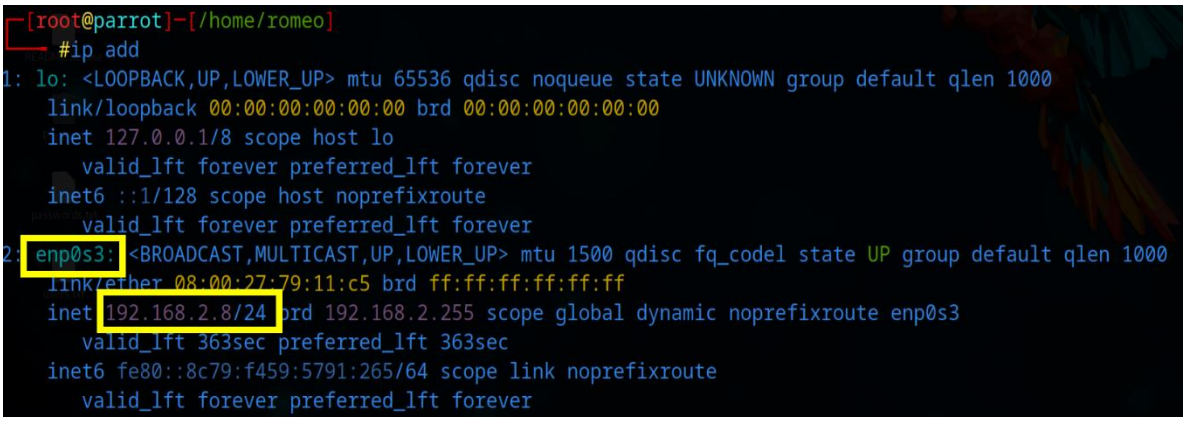
Para utilizar la herramienta, debemos buscarla en el menú de parrot:

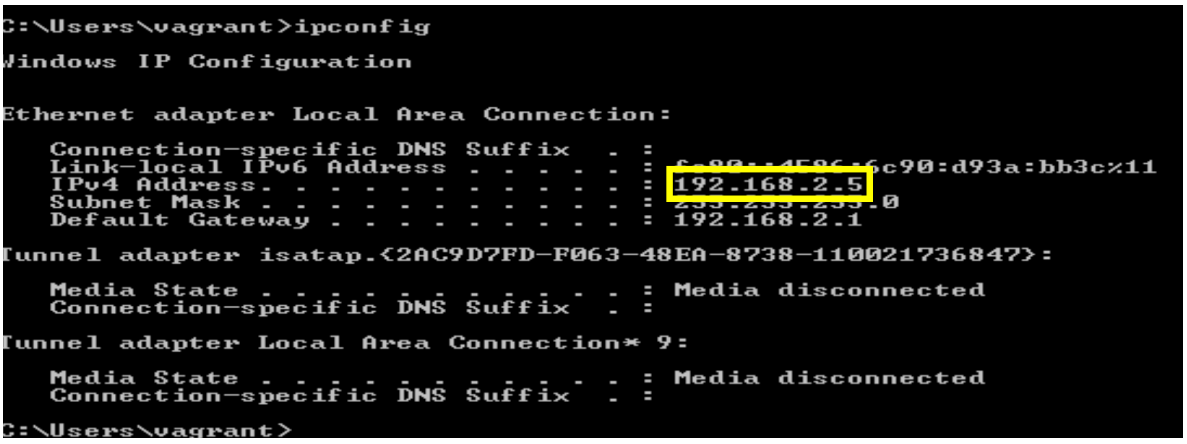




Al abrir muestra la siguiente ventana:

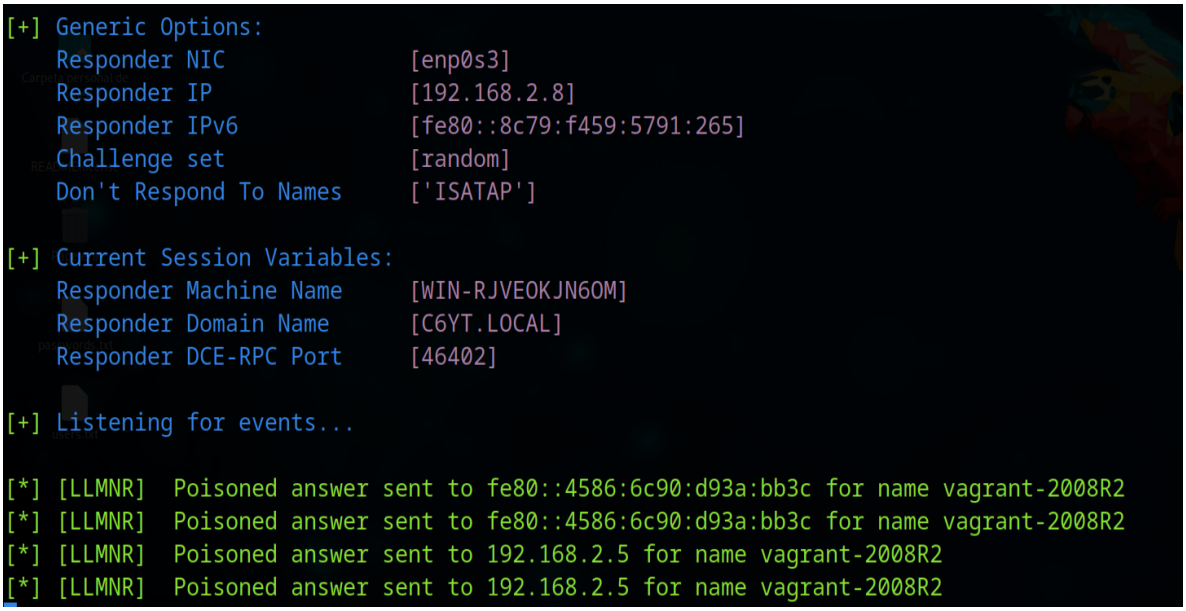
Verificamos que ambas máquinas estén en la misma red.





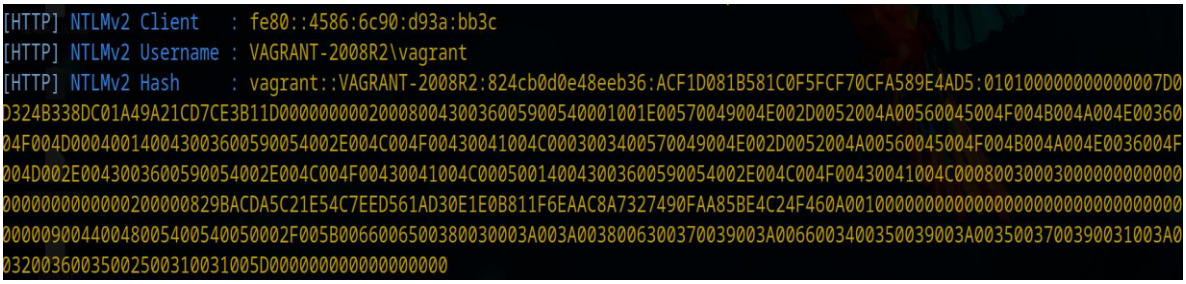
Ejecutamos el comando **responder -I enp0s3.**

Observamos que empieza a escuchar todas las maquinas que están dentro de la red.



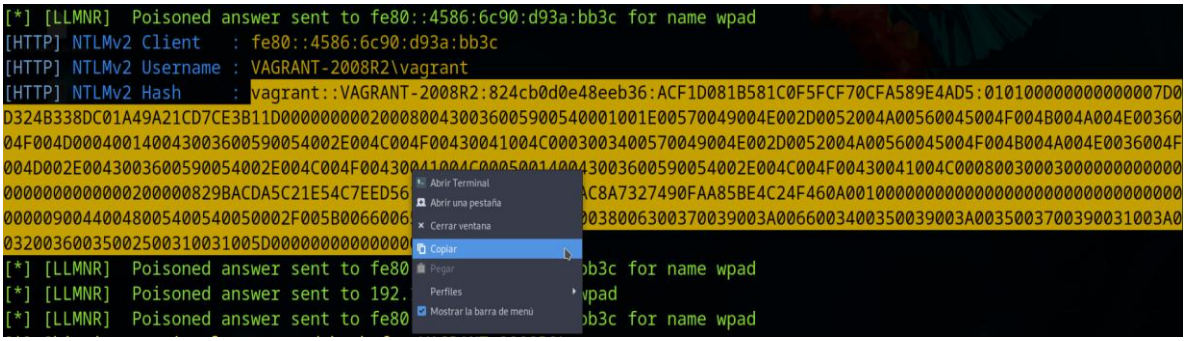
Este proceso toma varios minutos, además se observa que comienza a conocer la red y a detectar los equipos conectados dentro de la misma. Y comienza a infectar. El funcionamiento es como si fuera la BIOS, va obteniendo los usuarios y contraseñas, el tráfico de internet, entre otros de nuestros equipos.

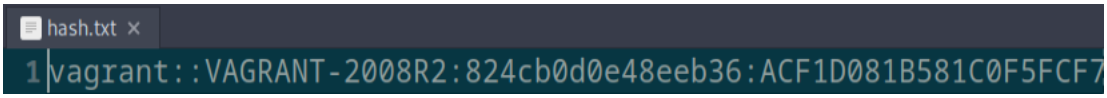
Nos arroja el hash:



Ahora solo queda desencriptar el hash, si esta fuera una red empresarial, podría contener todos los usuarios y contraseñas de las máquinas conectadas. En un escaneo real, esto tarda mucho tiempo.

Procedemos a copiar el hash en un archivo de texto.

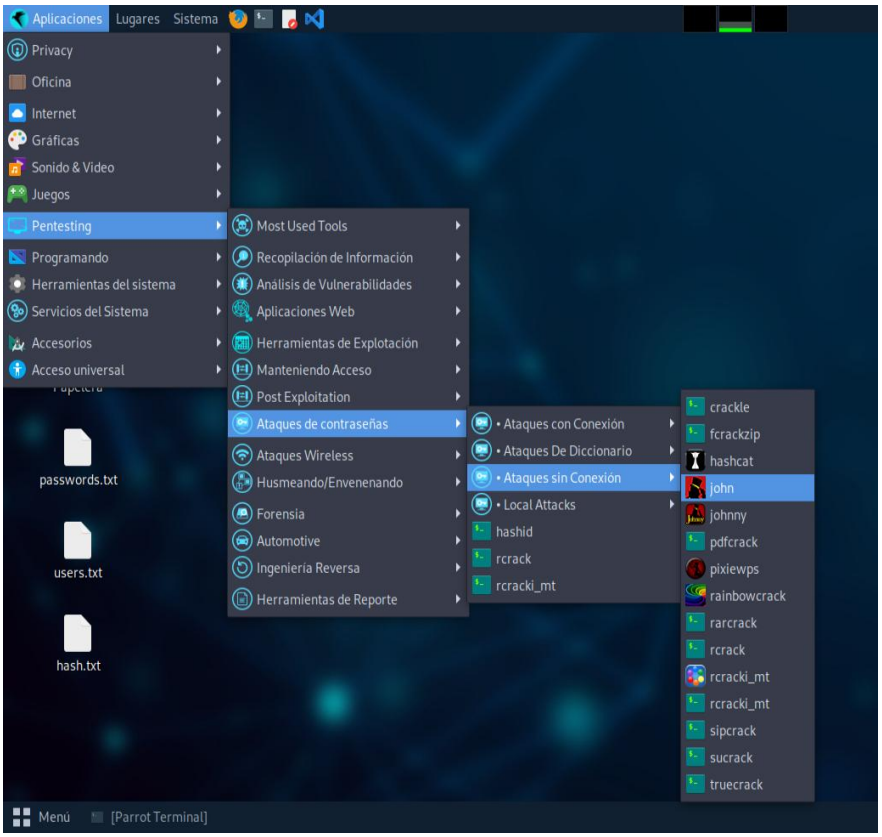




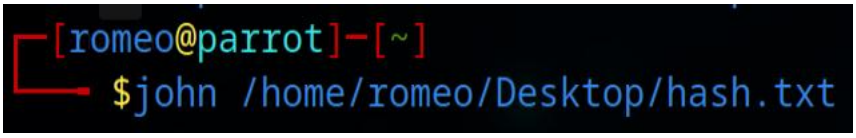
Jhon the Ripper.

Usaremos John the Ripper para desencriptar el hash, está orientado específicamente a crackear contraseñas por fuerza bruta y también por diccionario, es capaz de crackear los hashes de las contraseñas muy rápido

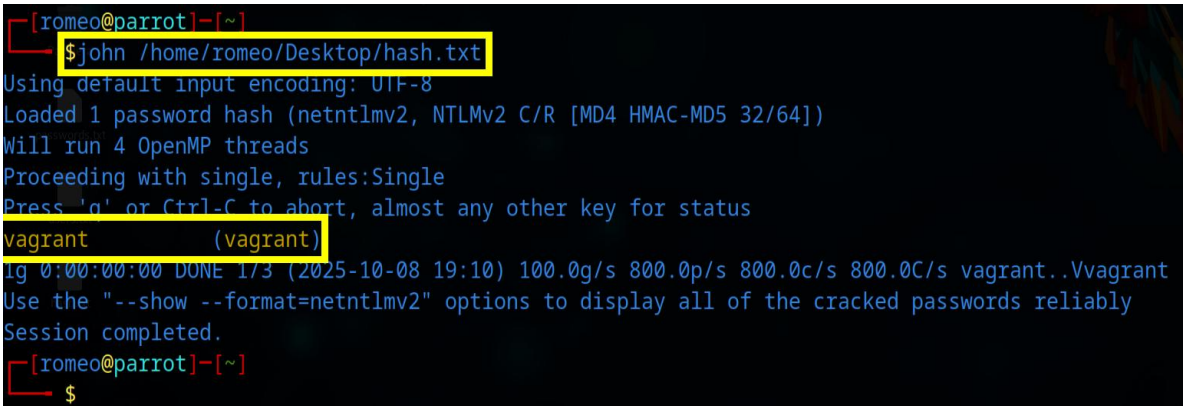
(depende de la potencia del procesador de tu ordenador), y su utilización es realmente sencilla.



Para usar la herramienta, se usa el comando John más **la ruta donde esta el archivo hash,** en este caso está en Desktop.



Muestra el usuario y contraseña asociado:



¿Por qué deshabilitar *Multicast Name Resolution* (LLMNR / mDNS / NetBIOS)?

Porque estos protocolos permiten que clientes resuelvan nombres sin usar DNS centralizado. Un atacante en la misma red puede responder (spoof) a esas peticiones y convencer al equipo víctima de enviar credenciales (p. ej. NetNTLM hashes) a la máquina atacante.

Herramientas como Responder explotan exactamente eso: responden a consultas LLMNR/NBT-NS/mDNS y capturan credenciales que luego se pueden relayar o crackear.

Resultado: exposición de hashes / credenciales, posibilidad de relay a servicios (SMB, HTTP) y escalada lateral en la red.

En resumen: deshabilitar multicast name resolution reduce la superficie de ataque y evita que máquinas confíen en respuestas no confiables dentro de la LAN.