



# **Curso de Hacking ético Master. D**

Ejercicio 9  
Informe sobre Herramientas  
de Explotación

Alumno: Julián Gordon

# Índice

Introducción .....	3
Uso de Nessus para detección de vulnerabilidades .....	5
Uso de Metasploit .....	10
Conclusiones .....	14

# Introducción

Para poder entender los conceptos de Explotación que veremos más adelante, primero debemos saber qué es una vulnerabilidad. Una vulnerabilidad es una debilidad en un sistema, que puede ser explotada para comprometer su seguridad. Estas debilidades pueden surgir debido a errores de diseño, implementación o configuración, creando oportunidades para posibles ataques.

Otro concepto muy importante que debemos saber, es qué es un exploit. Un exploit es un programa, script o conjunto de comandos diseñados para aprovechar una vulnerabilidad o debilidad en un sistema, aplicación o dispositivo, con el objetivo de ejecutar código malicioso, obtener acceso no autorizado ó realizar acciones no previstas por los creadores del sistema. La explotación exitosa de una vulnerabilidad mediante un exploit, puede permitirnos eludir medidas de seguridad, obtener privilegios elevados, acceder a información confidencial ó comprometer la integridad y disponibilidad de un sistema. Los exploits se pueden clasificar en diferentes categorías, como exploits locales y remotos, dependiendo de cómo interactúan con el sistema objetivo y pueden provenir de diversas fuentes, como bases de datos como Exploit-DB, Rapid7-DB y 0day.today.

Los payloads en Metasploit se dividen en tres categorías: Singles, Stagers y Stages. Los Singles son autónomos y completamente independientes, realizando acciones específicas como agregar usuarios o ejecutar programas. Pueden utilizarse sin la necesidad de manejadores de payloads como Metasploit, incluso con herramientas como netcat. Por otro lado, los Stagers establecen una conexión de red entre el atacante y la víctima, siendo pequeños y confiables. Metasploit elige el mejor Stager disponible y recurre a uno menos preferido cuando es necesario. Finalmente, los Stages son componentes de los payloads que se descargan a través de los módulos Stagers. Proporcionan funciones avanzadas sin límites de tamaño, como Meterpreter, Inyección VNC o la Shell 'ipwn' para iPhone

En este informe hablaremos sobre las herramientas de Explotación que utilizamos para hacer los ejercicios anteriores. Explicaremos en detalle, el funcionamiento de Metasploit para explotar las vulnerabilidades que encontramos con Nessus y Nmap y el uso de John the Ripper para romper los hashes que encontramos en nuestras máquinas objetivo.

# Uso de Nessus y Nmap para detección de Vulnerabilidades

Como ya hemos visto en ejercicios anteriores, Nessus y Nmap son herramientas importantísimas para la detección de vulnerabilidades. Gracias a estas herramientas, podemos realizar nuestro paso a paso para lograr explotar estas vulnerabilidades.

Nuestro paso a paso consiste primero en detectar una vulnerabilidad, luego buscar un exploit que nos pueda brindar información importante, para después encontrar el exploit adecuado que nos dé acceso a nuestra máquina objetivo y a través del payload correcto, poder hacernos con el control total de la máquina. A continuación veremos imágenes sobre las vulnerabilidades que encontramos en las máquinas de Metasploitable y Windows Server 2012.

Hosts 1

Vulnerabilities 94

Remediations 6

History 1

Filter

Search Vulnerabilities



94 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Gain a shell remotely	2		
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1		
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1		
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1		
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1		
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2		
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1		
<input type="checkbox"/>	MIXED	...	...	DNS (Multiple Issues)	DNS	5		
<input type="checkbox"/>	MIXED	...	...	Phpmyadmin (Multiple Issues)	CGI abuses	4		
<input type="checkbox"/>	MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	3		
<input type="checkbox"/>	MIXED	...	...	PHP (Multiple Issues)	CGI abuses	3		
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1		
<input type="checkbox"/>	HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1		
<input type="checkbox"/>	HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1		Snooze
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1		

```

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:  *Kali tools* *Kali Docs* *Kali Featime* *Kali NetHunter* *Exploit-DB* *Google Hacking DB* *0nSec* *Hack The Box* *Startin...
| STAT:
| FTP server status:
|   Connected to 10.0.2.15
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230) Password:
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, DSN
|_ssl-date: 2024-01-23T09:24:36+00:00; ~10m16s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp   open  java-rmi      GNU Classpath grmiregistry
1524/tcp   open  bindshell     Metasploitable root shell
2049/tcp   open  nfs           2-4 (RPC #100003)
2121/tcp   open  ftp           ProFTPD 1.3.1
3306/tcp   open  mysql         MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5

```

```
| Thread ID: 9
| Capabilities flags: 43564
| Some Capabilities: Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, SupportsCompression, LongColumnFlag, Speaks41ProtocolNew, ConnectWithDatabase
| Status: Autocommit
|_ Salt: $%+Iotwz"2w">RbwQkGb
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ ssl-date: 2024-01-23T09:24:36+00:00; -10m16s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
6697/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_ http-favicon: Apache Tomcat
|_ http-title: Apache Tomcat/5.5
|_ http-server-header: Apache-Coyote/1.1
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
33590/tcp open mountd 1-3 (RPC #100005)
33939/tcp open java-rmi GNU Classpath grmiregistry
38625/tcp open nlockmgr 1-4 (RPC #100021)
42394/tcp open status 1 (RPC #100024)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 1h04m46s, deviation: 2h30m02s, median: -10m16s
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2024-01-23T04:24:33-05:00
```



# Windows Server 2012 enigma

[← Back to All Scans](#)

Hosts 1 Vulnerabilities 83 Remediations 8 Notes 8 History 3

Filter Search Vulnerabilities 83 Vulnerabilities

<input type="checkbox"/> Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	⦿ ✎
<input type="checkbox"/> CRITICAL	9.8	5.9	Elasticsearch Transport Protocol Unspecified Remote Code Execution	Databases	1	⦿ ✎
<input type="checkbox"/> MIXED	...	...	WordPress (Multiple Issues)	CGI abuses	27	⦿ ✎
<input type="checkbox"/> MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	18	⦿ ✎
<input type="checkbox"/> MIXED	...	...	PHP (Multiple Issues)	CGI abuses	16	⦿ ✎
<input type="checkbox"/> MIXED	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	15	⦿ ✎
<input type="checkbox"/> MIXED	...	...	Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	15	⦿ ✎
<input type="checkbox"/> MIXED	...	...	Apache Httpd (Multiple Issues)	Web Servers	7	⦿ ✎
<input type="checkbox"/> MIXED	...	...	Elasticsearch (Multiple Issues)	CGI abuses	3	⦿ ✎
<input type="checkbox"/> HIGH	8.1	5.9	Elasticsearch ESA-2018-11	CGI abuses	1	⦿ ✎
<input type="checkbox"/> HIGH	7.5	3.6	DNS Server Spoofed Request Amplification DDoS	DNS	1	⦿ ✎
<input type="checkbox"/> MIXED	...	...	SSL (Multiple Issues)	General	46	⦿ ✎
<input type="checkbox"/> MIXED	...	...	SNMP (Multiple Issues)	SNMP	12	⦿ ✎
<input type="checkbox"/> MIXED	...	...	IETF Md5 (Multiple Issues)	General	3	⦿ ✎
<input type="checkbox"/> MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	2	⦿ ✎
<input type="checkbox"/> MEDIUM	5.3		Sensitive File Disclosure	CGI abuses	10	⦿ ✎

Plugin ID: 121041

# Uso de Metasploit

Siguiendo con el paso a paso que hemos aprendido luego de realizar los ejercicios de esta unidad, ahora debemos buscar los exploits que nos puedan servir para explotar las vulnerabilidades anteriores. Esto lo hacemos a través de abrir metasploit y utilizar el comando 'search' seguido del nombre o algún dato de la vulnerabilidad elegida. A continuación veremos 2 imágenes de este proceso.

```
msf6 > search snmp windows
```

```
Matching Modules
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/http/hp_nnm_snmp	2009-12-09	great	No	HP OpenView Network Node Manager Snmp.exe CGI Buffer Overflow
1	exploit/windows/http/hp_nnm_ovwebsnmprsv_uro	2010-06-08	great	No	HP OpenView Network Node Manager ovwebsnmprsv.exe Unrecognized Option Buffer Overflow
2	exploit/windows/http/hp_nnm_ovwebsnmprsv_main	2010-06-16	great	No	HP OpenView Network Node Manager ovwebsnmprsv.exe main Buffer Overflow
3	exploit/windows/http/hp_nnm_ovwebsnmprsv_ovutil	2010-06-16	great	No	HP OpenView Network Node Manager ovwebsnmprsv.exe ovutil Buffer Overflow
4	exploit/windows/http/hp_nnm_snmpviewer_actapp	2010-05-11	great	No	HP OpenView Network Node Manager snmpviewer.exe Buffer Overflow
5	exploit/multi/http/hp_sys_mgmt_exec	2013-06-11	excellent	Yes	HP System Management Homepage JustGetSNMPQueue Command Injection
6	exploit/windows/ftp/oracle9i_xdb_ftp_unlock	2003-08-18	great	Yes	Oracle 9i XDB FTP UNLOCK Overflow (win32)
7	auxiliary/scanner/snmp/snmp_enumshares		normal	No	SNMP Windows SMB Share Enumeration
8	auxiliary/scanner/snmp/snmp_enumusers		normal	No	SNMP Windows Username Enumeration
9	exploit/windows/scada/sunway_force_control_netdbsrv	2011-09-22	great	No	Sunway Forcecontrol SNMP NetDBServer.exe Opcode 0x57
10	post/windows/gather/enum_snmp		normal	No	Windows Gather SNMP Settings

```
Interact with a module by name or index. For example info 10, use 10 or use post/windows/gather/enum_snmp
```

```
msf6 > use auxiliary/scanner/snmp/snmp_enumusers
```

```
msf6 > search elasticsearch
```

## Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/elasticsearch/script_mvel_rce	2013-12-09	excellent	Yes	ElasticSearch Dynamic Script Arbitrary Java Execution
1	exploit/multi/elasticsearch/search_groovy_script	2015-02-11	excellent	Yes	ElasticSearch Search Groovy Sandbox Bypass
2	auxiliary/scanner/http/elasticsearch_traversal		normal	Yes	ElasticSearch Snapshot API Directory Traversal
3	auxiliary/gather/elasticsearch_enum		normal	No	Elasticsearch Enumeration Utility
4	auxiliary/scanner/http/elasticsearch_memory_disclosure	2021-07-21	normal	Yes	Elasticsearch Memory Disclosure
5	exploit/multi/misc/xdh_x_exec	2015-12-04	excellent	Yes	Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

Interact with a module by name or index. For example `info 5`, use `5` or use `exploit/multi/misc/xdh_x_exec`

```
msf6 > use Interrupt: use the 'exit' command to quit
```

```
msf6 > use exploit/multi/elasticsearch/script_mvel_rce
```

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > options
```

Module options (exploit/multi/elasticsearch/script\_mvel\_rce):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	9200	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The path to the ElasticSearch REST API
VHOST		no	HTTP server virtual host
WritableDir	/tmp	yes	A directory where we can write files (only for *nix environments)

Una vez elegimos el exploit que mejor se adecue a la vulnerabilidad que encontramos, lo ejecutamos y si obtuvimos acceso, nos abrirá una sesión de meterpreter de acuerdo al payload que hayamos seleccionado.

Luego de tener una sesión abierta a la máquina de windows server 2012, encontramos un archivo.zip llamado 'rompeme'. Nos lo descargamos en nuestra máquina y al intentar abrirlo para ver que archivos contiene, nos hemos encontrado con una contraseña. Para descifrar esta contraseña utilizamos otra herramienta que se llama John the Ripper. Al ser un archivo .zip debemos transformarlo para que lo pueda leer John the Ripper. Para eso usamos el comando `zip2john + rompeme.zip > rompeme.txt` . Luego utilizaremos un diccionario muy común llamado Rockyou para que John lo descifre, el comando sería el siguiente `'john --wordlist=/usr/share/wordlists/rockyou.txt rompeme.txt'`

Luego usamos el comando `'john --show rompeme.txt'` para ver el password que obtuvimos. A continuación se verán imágenes de todo este proceso.

```
(kali㉿kali)-[~]:/# ping 10.0.2.15
$ zip2john rompeme.zip > rompeme.txt
ver 2.0 rompeme.zip/IRC.log PKZIP Encr: cmplen=356, decmplen=614, crc=8AA635E1 ts=0705 cs=8aa6 type=8
ver 2.0 rompeme.zip/recentServers.xml PKZIP Encr: cmplen=326, decmplen=555, crc=9FC3F862 ts=08A4 cs=9fc3 type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
^C Aborting foreground process in the shell session
(kali㉿kali)-[~]:/# 15: icmp_seq=3 ttl=64 time=0.642 ms
$ john --wordlist=/usr/share/wordlists/rockyou.txt rompeme.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64]) packet loss, time 1999ms
No password hashes left to crack (see FAQ) 945 ms
root@metasploitable:/#
(kali㉿kali)-[~]:/# exit
$ john --show rompeme.txt
rompeme.zip:simpleplan:rompeme.zip:recentServers.xml, IRC.log:rompeme.zip
^C
1 password hash cracked, 0 left CONTRASEÑA ENCONTRADA
```

Con la contraseña 'simpleplan' podemos abrir el fichero rompeme.zip y encontramos dentro un fichero con credenciales que nos sirvieron para vulnerar la máquina de Windows Server 2012.

# Conclusiones

Este informe nos sirvió mucho para fijar nuestros conocimientos sobre todo lo que aprendimos en esta unidad sobre herramientas de explotación. Pudimos analizar vulnerabilidades encontradas con Nessus y Nmap, que son herramientas que venimos usando con frecuencia. Con las vulnerabilidades obtenidas, aprendimos a buscar exploits dentro de Metasploit Framework, para recogida de información (dentro del módulo Auxiliary) y explotación de estas vulnerabilidades (dentro del módulo exploit). También empezamos a usar el módulo de post, que nos sirvió para escalar privilegios y lograr acceso total a nuestras máquinas objetivo. Como hemos comentado en trabajos anteriores ahora ya no solo se trata de analizar las vulnerabilidades que encontremos, sino que empezamos a hacer uso de ellas y vulnerar las máquinas. Esto esta cada vez más interesante y paso a paso seguimos en nuestro camino a convertirnos en profesionales.