[Un framework de test de intrusión web]

IV OWASP Spain Chapter Meeting
21 Noviembre 2008, Barcelona, España
José Ramón Palanco. Hazent Systems S.L
jose.palanco@hazent.com.

- ¿Qué es w3af?
- ¿Por qué w3af?
- ¿Quién debería conocer este framework?
- Características
- Preguntas

¿Qué es w3af?

¿Qué es w3af?

Web **A**pplication **A**ttack and **A**udit **F**ramework

- Es un framework de test de intrusión web
- Está desarrollado en Python
- Bajo licencia GPLv2
- Tiene funcionalidad de scanner de vulnerabilidades.

¿Por qué w3af?

¿Por qué w3af?

Nos permite compartir know-how

- Buenas herramientas libres (falta sinergia)
- Productos comerciales caros
- Automatiza las tareas repetitivas de pentest

¿Quien debería conocerlo?

¿Quién debería conocerlo?

A todo experto en seguridad web

- Este framework está diseñado para ser utilizado para la auditoría de un entorno web
- Puede utilizarse por expertos en seguridad que no sean necesariamente programadores
- También a investigadores de vulnerabilidades o de productos de seguridad

Características

Características

Los módulos trabajan conjuntamente con la misma información

- Arquitectura modular
- Web 2.0
- Servicios Web
- Perfiles
- Remote File Inclusion Service
- Virtual Daemon

Arquitectura modular

Tipos de plugins

- **discovery**
- **audit**
- **grep**
- **attack**
- **output**
- **mangle**
- **evasion**
- **bruteforce**

Discovery

Descripción

Se ejecutan continuamente enviado su salida a la entrada del siguiente plugin hasta que no se localicen peticiones *fuzeables* u obtener datos para afinar la funcionalidad de los siguientes plugins.. Muchos de los métodos pueden considerarse explotacionec tácticas

Los plugins obtienen información analizando dom en busca de form actions, descubrimiento de métodos HTTP soportados, ficheros con información interesante en path predecibles, información de buscadores, ghdb, google sets, pykto, webspider, HTTP load balancer detection, archive.org..

Audit

Descripción

Obtienen información de los plugin discovery para localizar vulnerabilidades como:

- sqli
- bof
- evali
- command execution
- Xss
- ...

Las vulnerabilidades se almacenan para su posterior posible explotación.

Grep

Descripción

Parsean los response de las peticiones que vamos haciendo en busca de:

- comentarios en código
- emails
- direcciones ip privadas
- code disclosure
- cookies
- idioma
- path disclosure
- ...

Attack

Descripción

Leen información de la base de datos de vulnerabilidades recolectada por los plugins audit para intentar explotarlos.

- mysqlWebShell
- localFileReader
- osCommandingShell
- remoteFileIncludeShell
- sqlmap
- xssBeef
- ...

Output

Descripción

Estos plugins se encargan de generar un tipo y formato de salida:

- console
- gtkOutput
- htmlFile
- textFile
- ...

Mangle

Descripción

Alteran peticiones y respuestas en función de expresiones regulares.

Evasion

Descripción

Nos permiten modificar las peticiones o parte de las peticiones para evadir IDS e IPS.

- mod_security < 2.1.0 bypass
- rndCase
- dndHexEncode
- rndParam

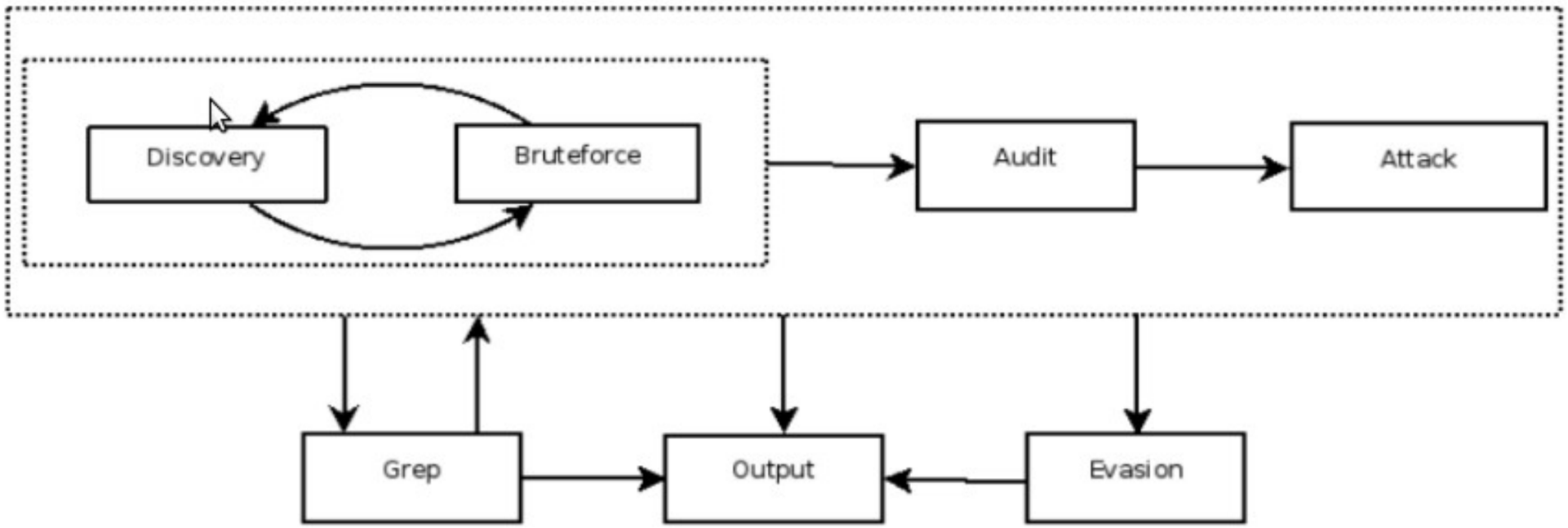
Bruteforce

Descripción

Utilizando información recopilada de los módulos grep, podemos hacer lanzar un ataque de fuerza bruta basicAuth o de formulario. Estas son algunas de las configuraciones:

- passEqUser
- useMailUsers
- useSvnUsers
- useMails
- ...

Arquitectura modular



Web 2.0

Los módulos trabajan conjuntamente con la misma información

- Es posible analizar páginas que uses AJAX (grep)
- Análisis de peticiones para alimentar un fuzzer interno

Servicios Web

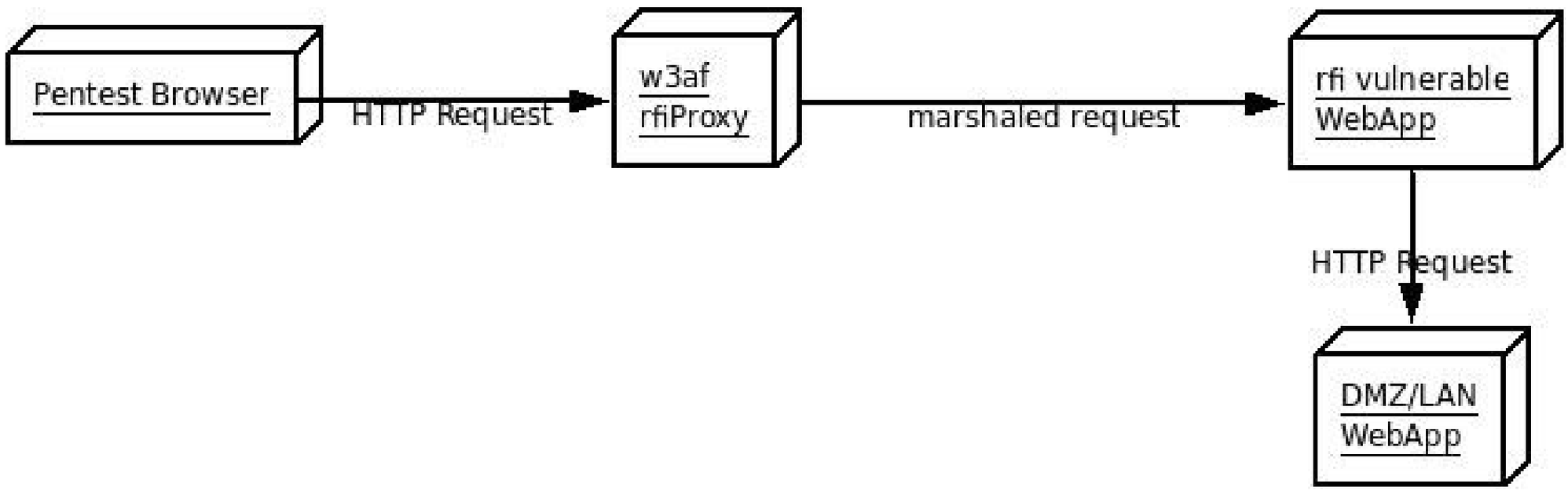
- Descubriemiento de wsdl:
  - discovery.wsdlFinder
  - grep.wsdlGreper
- Todos los audit plugins funcionan para servicios web
- Todos los de exploit deberían funcionar también.
- Para parsear WSDL se usa SOAPpy

Perfiles

- Es posible crear o usar perfiles preconfigurados que cargan una colleción de plugins.
- Perfiles por defecto:
  - OWASP Top 10
  - Fast Scan
  - Full Audit
  - Full Audit Manual Disc
- Podriamos incorporar otros perfiles como PCI DSS. De hecho hay un módulo grep que detecta números de tarjetas de crédito.

Remote File Inclusion Proxy

Aprovechando una vulnerabilidad file inclusion es posible levantar un servidor proxy para lanzar ataques hacia la DMZ o la red interna.

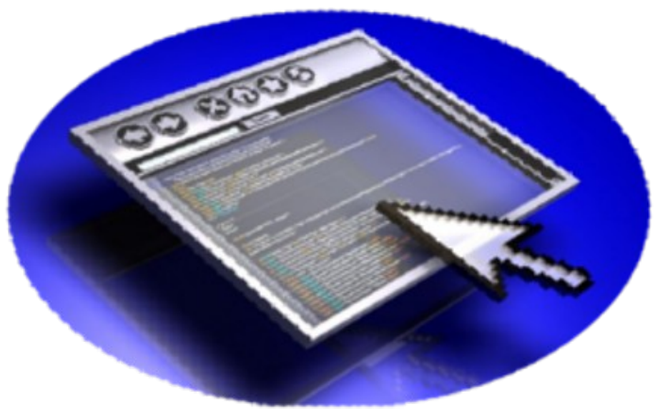


Virtual Daemon

Es posible utilizar payloads de metasploit para explotar vulnerabilidades en aplicaciones web.

Para ello, se ha desarrollado un plugin para metasploit que permite a este último enviar los payloads a través de virtual daemon, un attack plugin que recibe el payload y crea un pequeño ejecutable ELF/PE.

Virtual Daemon



hazent systems

FIN
¿Preguntas?

http://w3af.sf.net