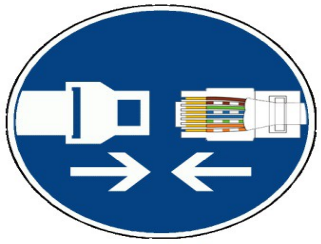


www.seguridadpyme.es

ASISTENCIA TÉCNICA A LA SEGURIDAD INFORMÁTICA EN PYMES

MANUAL FLUNYM0US

CIUDAD AUTÓNOMA DE MELILLA
Consejería de Presidencia y Participación Ciudadana
DIRECCIÓN GENERAL DE LA SOCIEDAD DE LA INFORMACIÓN

Unión Europea
P.O. FEDER 2007-2013
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Flunym0us

Bueno esta herramienta llamada flunym0us, nos servirá para realizar escaneos en websites que tengan el CMS wordpress y Moodle.

1. ***Funcionalidades de Flunym0us 2.0 :***

   - ***Fingerprint de versión de WordPress: Extrae de los archivos "Readme.html" la versión actual instalada de WordPress.***
   - ***Descubrimiento de vulnerabilidades por Path Disclosure en WordPress que dejan expuesta la ruta de instalación.***
   - ***Descubrimiento de versión de plugins instalados en WordPress.***
   - ***Aviso de versiones obsoletas de instalaciones de WordPress.***
   - ***Aviso de versiones obsoletas de instalaciones de plugins en WordPress.***
   - ***Descubrimiento de usuarios registrados.***
   - ***Aumento en la velocidad de análisis gracias al procesamiento en paralelo con múltiples procesos parametrizables.***
   - ***Ocultación de User-Agent por uno aleatorio a través de un diccionario incluido de User-Agents reales.***

2. ***Uso e Instalacion:***

   Descargamos la herramienta: http://code.google.com/p/flunym0us/downloads/list

   Lo dejamos en nuestro escritorio y seguimos los pasos.

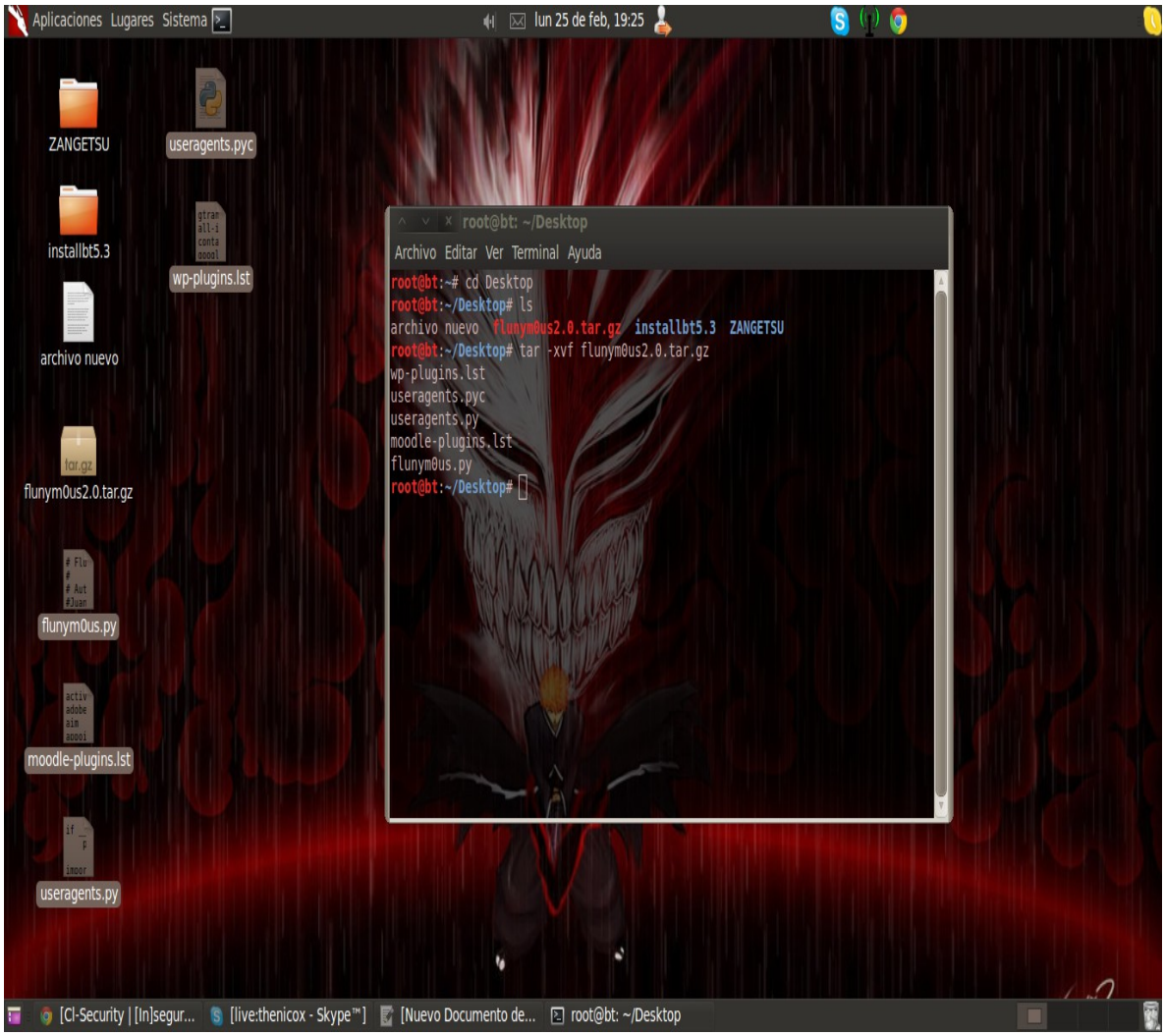
   ## *Primero descomprimir:*

   - ***cd Desktop***
   - ***tar -xvf flunym0us2.0.tar.gz***
   - ***guardamos los archivos en una carpeta, en este caso : flunym0us***
   - ***vamos a la carpeta : cd Desktop/flunym0us***
   - ***python flunym0us.py y tendremos listo para realizar el escaneo.***

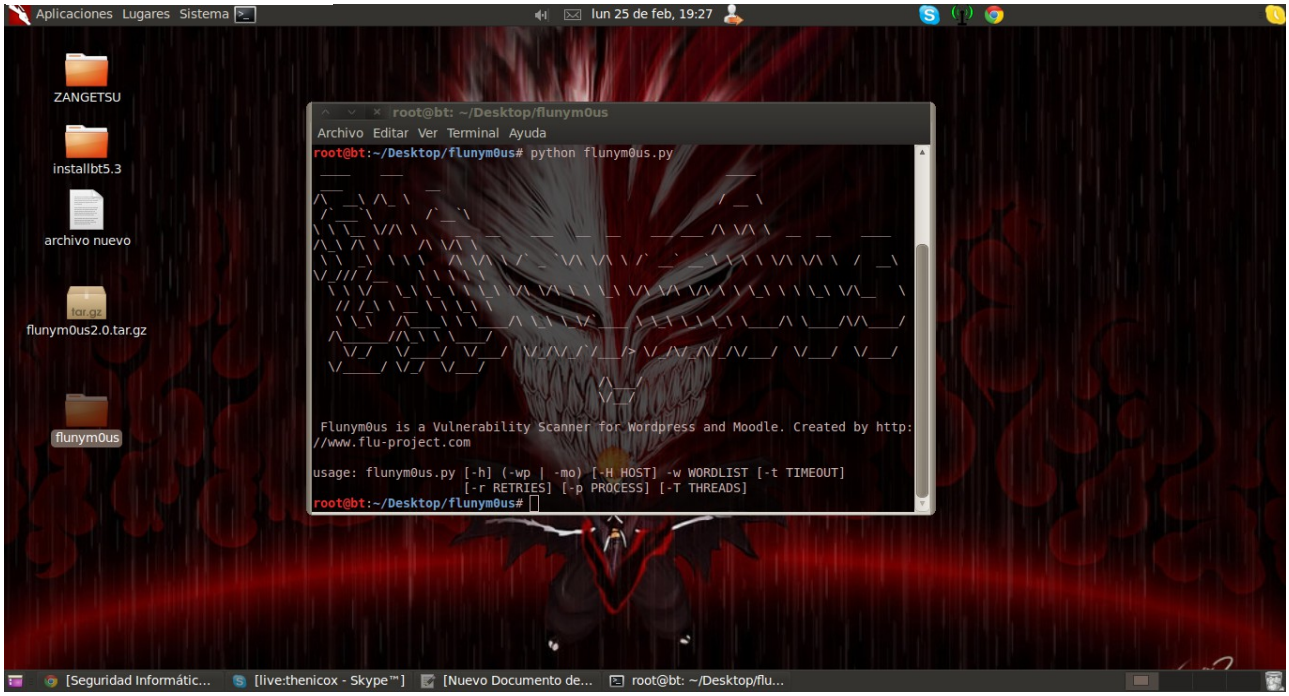
Este proyecto está cofinanciado en un 80% por la Unión Europea a través del Fondo Europeo de Desarrollo Regional (FEDER), en el marco del Programa Operativo FEDER 2007 – 2013 de Melilla, Eje 1,tema prioritario 14.

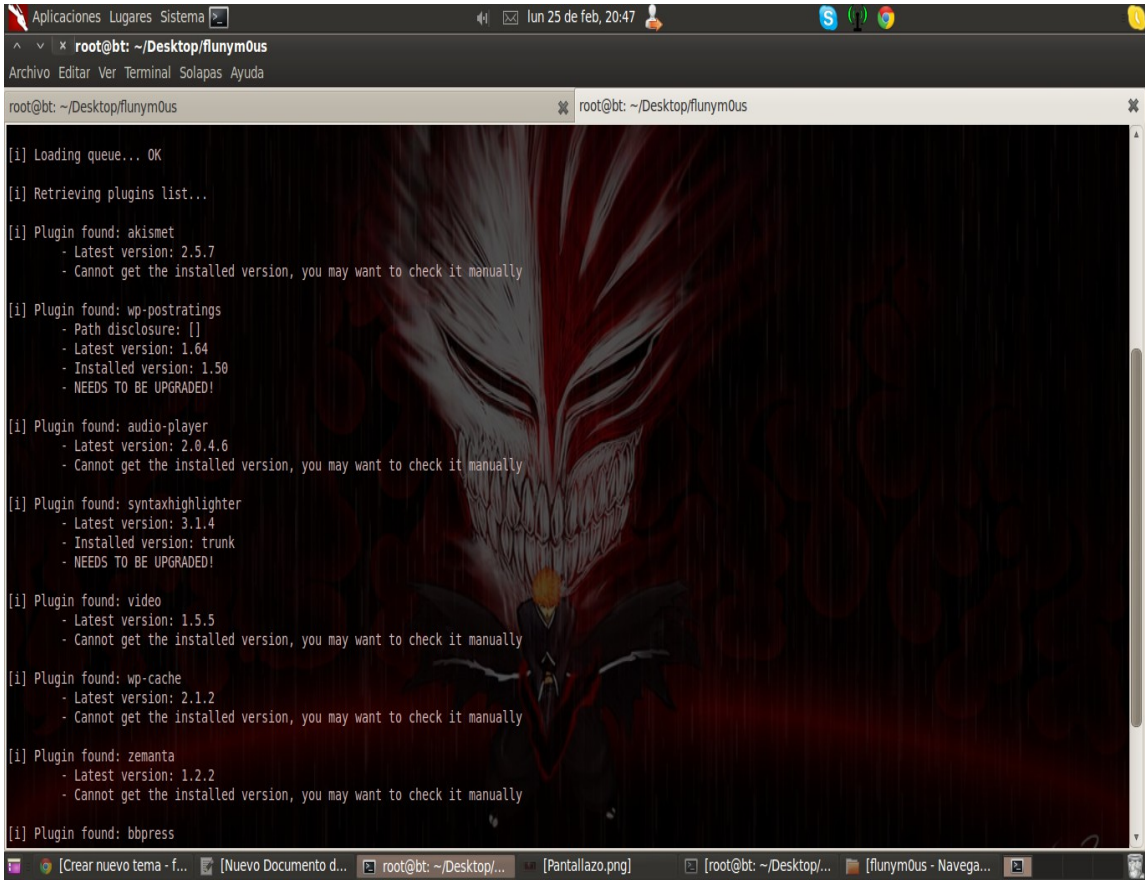
Comandos :

- ***-h, –help: Show this help message and exit***
- ***-wp, –wordpress: Scan WordPress site***
- ***-mo, –moodle: Scan Moodle site***
- ***-H HOST, –host HOST: Website to be scanned***
- ***-w WORDLIST, –wordlist WORDLIST: Path to the wordlist to use***
- ***-t TIMEOUT, –timeout TIMEOUT: Connection timeout***
- ***-r RETRIES, –retries RETRIES: Connection retries***
- ***-p PROCESS, –process PROCESS: Number of process to use***
- ***-T THREADS, –threads THREADS: Number of threads (per process) to use***
- ***Y el comando del ataque: python flunym0us.py -H http://www.target.com -wp -w wp-plugins.lst -t 60 -r 1 -T***

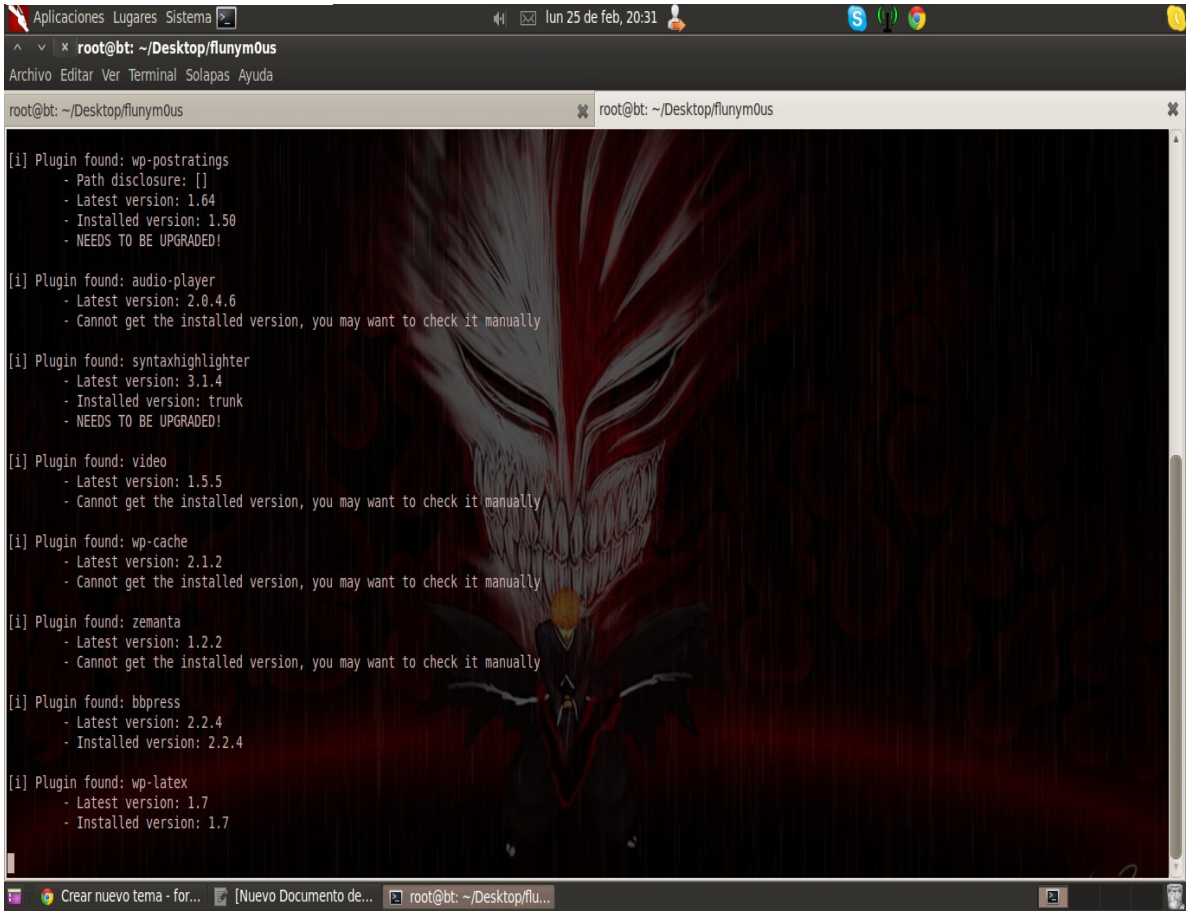


Este proyecto está cofinanciado en un 80% por la Unión Europea a través del Fondo Europeo de Desarrollo Regional (FEDER), en el marco del Programa Operativo FEDER 2007 – 2013 de Melilla, Eje 1,tema prioritario 14.





Este proyecto está cofinanciado en un 80% por la Unión Europea a través del Fondo Europeo de Desarrollo Regional (FEDER), en el marco del Programa Operativo FEDER 2007 – 2013 de Melilla, Eje 1,tema prioritario 14.



http://blackkzangetsu.blogspot.com.es/2013/02/flunym0us-20-herramienta-scan.html

Este proyecto está cofinanciado en un 80% por la Unión Europea a través del Fondo Europeo de Desarrollo Regional (FEDER), en el marco del Programa Operativo FEDER 2007 – 2013 de Melilla, Eje 1,tema prioritario 14.