

«Back|Track-[IT]

www.backtrack.it



(c) 2008 brigante
brigante@backtrack.it

Hydra



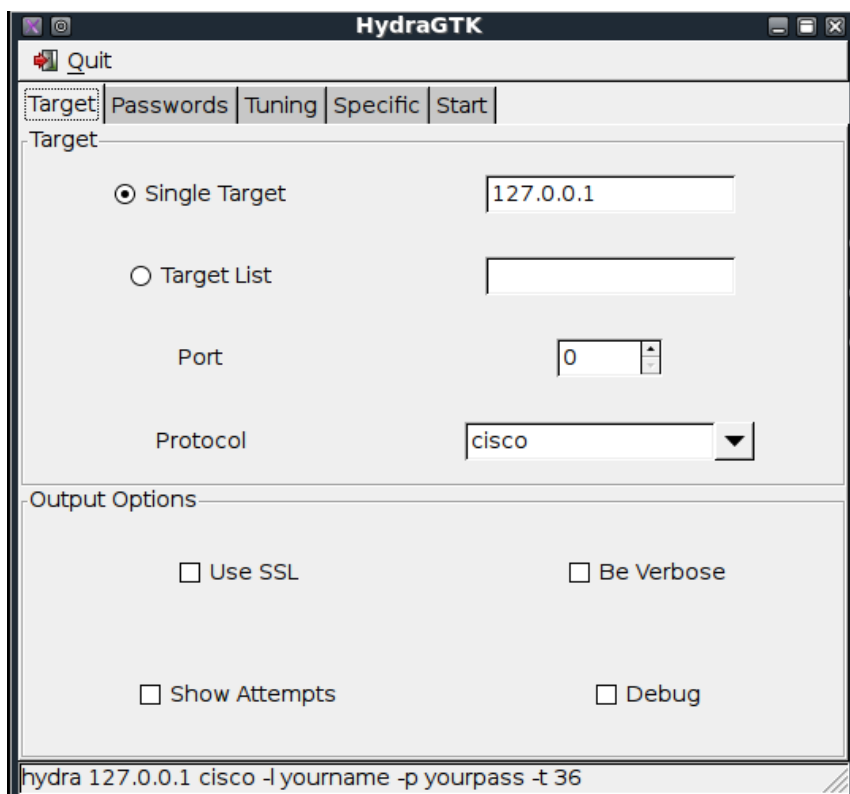
Questo pdf contiene due sezioni, una dedicata all' introduzione – descrizione – ed impiego generale di Xhydra, mentre la seconda descriverà l' uso del tool durante una dimostrazione video, potete vedere il **video** nell' apposita sezione del nostro [portale](#) oppure scaricarlo nella risoluzione originale [1280x800] dal link nella sezione **Privilege Escalation** nel nostro [blog](#).

Passiamo quindi alla prima parte del documento e cioè a parlare e descrivere quest' eccezionale strumento per il login bruteforce qual' è Hydra.

Hydra ed **XHydra** , (ovvero l'Hydra dotato di GUI), è uno strumento per effettuare login-bruteforcing presente in **BackTrack** già dalle primissime release, grazie ai vari tipi di formato in cui viene rilasciato viene utilizzato anche su piattaforme diverse da sistemi GNU/Linux, come ad esempio Windows.

Il nome Hydra, (*il mostro a più teste nato nella mitologia dell' antica Grecia*), ispira già da sé le capacità di questo tool, che infatti può effettuare bruteforce su molti tipi di protocolli, si va dall' HTTP/s fino al FTP, dal TELNET al VNC, dai Router (con delle specifiche sugli apparati CISCO), fino al POP e a vari tipi di database come MYSQL e PostgreSQL.

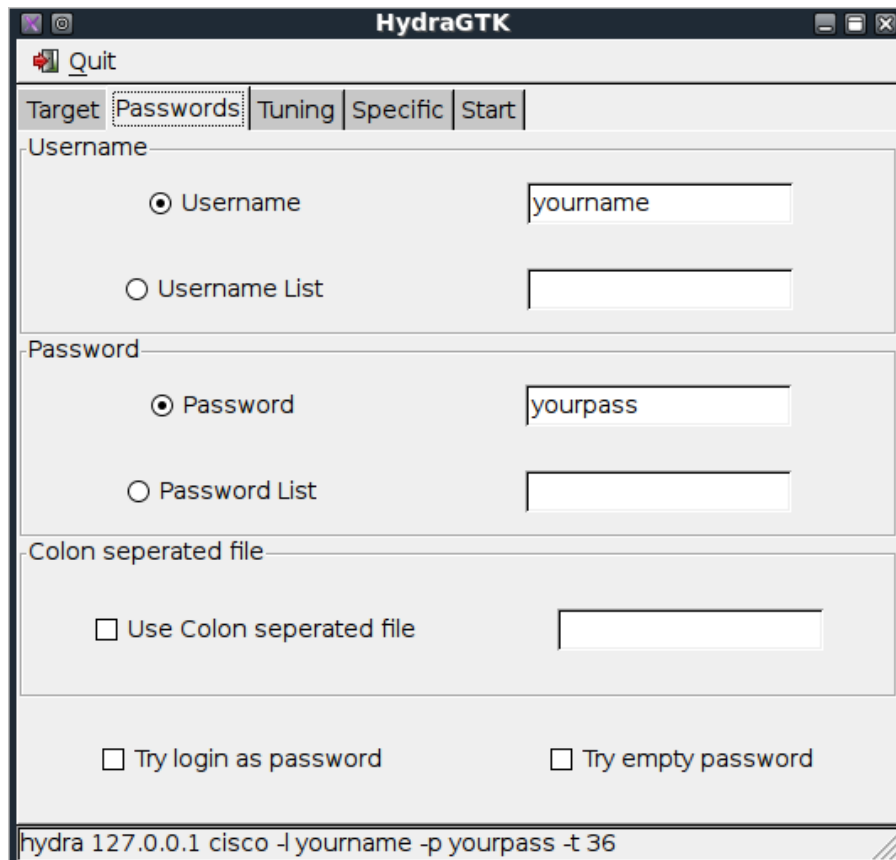
Appena lanciato XHydra si presenta come nell' immagine sottostante...



Come possiamo vedere l' interfaccia di Hydra è davvero molto semplice ed intuitiva, ci presenta le prime opzioni da inserire per il nostro attacco ovvero:

- L' inserimento del o dei nostri Target, possibilità quindi di inserire oltre ad un unico indirizzo IP selezionando l' opzione **Single Target**, una lista di indirizzi in formato ***.txt** con tutti gli IP inseriti uno sotto l' altro. Infatti appena si clicca con il mouse sulla casella corrispondente a **Target List**, ci si aprirà una finestra di ricerca files.
- La porta di lavoro, che bisogn ovviamente scegliere secondo il protocollo che vorremmo sfruttare per il nostro bruteforce.
- Il protocollo, selezionabile da una finestra a comparsa.
- Ed in ultimo le opzioni per l' output che vogliamo l' Xhydra rispetti , come ad esempio la comunicazione del risultato dell' attacco diretto su protocollo **SSL** , l' opzione per mostrare tutti i tentativi di login **Show Attampts** , giusti o rifiutati, la modalità **Be Verbose**, per scorrere con l' output tutta la procedura che Xhydra effettua durante l' attacco.

Nella seconda sezione del nostro tool dovremmo invece inserire le credenziali di login ed indicare ad Xhydra come deve usarle. L' immagine della seconda sezione è la seguente:

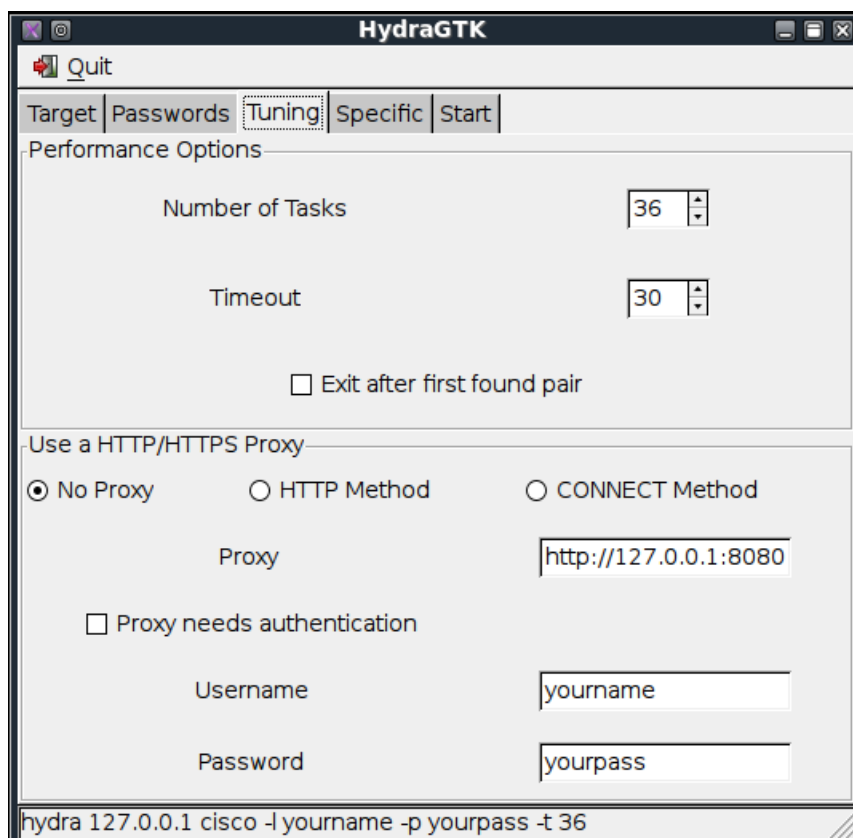


Le credenziali dovranno essere inserite sempre secondo il metodo di scelta , singolo o in file *.txt , si possono avere a disposizione sia le eventuali password che gli username , di conseguenza Xhydra ci mette nelle condizioni di scegliere:

- Single Username
- Username inseriti uno dopo l' altro in un file di testo
- Single Password
- Password inserite in un file di testo

Con la possibilità di provare l' username come password con l' opzione **Try Login as Password** , la possibilità di provare un attacco a password vuota con l' opzione **Try Empty Password** , e di selezionare un file con gli username e con le nostre password inseriti una coppia sotto l' altra ma distribuite in colonne con l' opzione **Use Colon Separated File** e nel modo **username:password**.

Questa invece l' immagine della terza sezione...



Come possiamo vedere dall' immagine sopra Hydra ci chiede i parametri di tuning, ovvero quelle specifiche che servono al programma per eseguire l' attacco secondo determinati tempi e tentativi.

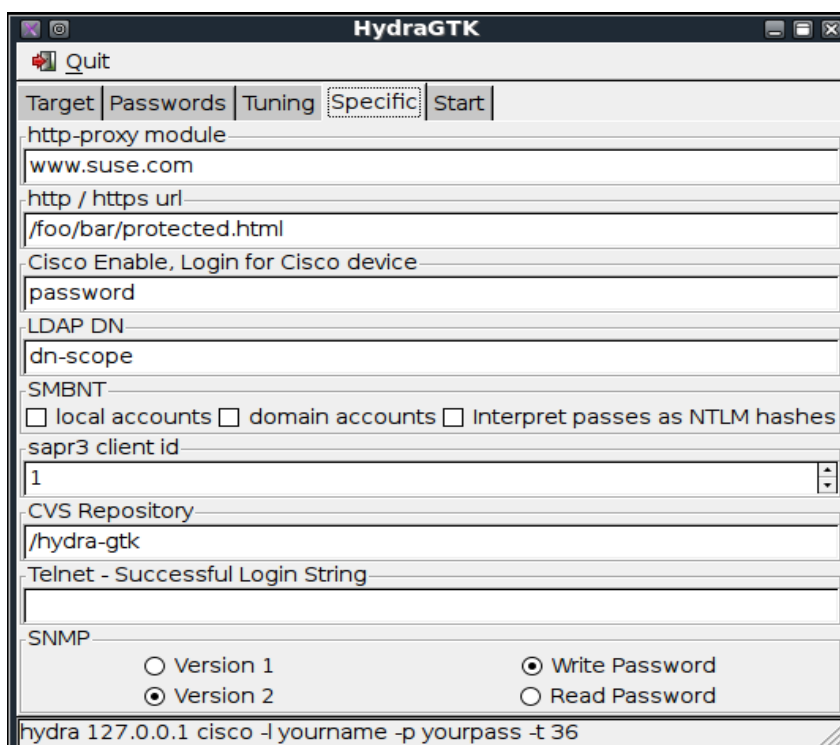
Le opzioni sono:

- **Number of Tasks**, il numero di tentativi da fare
- **Timeout**, il timeout da rispettare secondo i tentativi inseriti precedentemente
- La possibilità di mascherarsi dietro un **Proxy HTTP / HTTPS** inserendo il metodo e l' eventuale **indirizzo del proxy** con rispettive **credenziali** di accesso.

Queste opzioni molte volte vengono saltate nei test, perché appunto di test si tratta e non di veri e propri attacchi, ma in un vero attacco sono sempre e comunque essenziali.

Se ci si trova a dover fare bruteforcing verso un host sconosciuto, quindi in un vero e proprio attacco , onde riuscire vanno settati a dovere il numero di tasks ed il timeout, perché ormai per evadere ad attacchi di questo tipo la maggiorparte dei server, soprattutto quelli di tipo POP3 , dopo un determinato numero di tentativi ti negano l' ingresso e se non immessi Timeout e Tasks per bene in Xhydra ci si ritrova con il programma piantato dopo 3 minuti, ma se si inseriscono a dovere Xhydra offre una copertura formidabile e direi quasi unica nel suo genere.

Passiamo ora alla quarta sezione...



La quarta sezione riguarda come possiamo vedere ancora informazioni su protocolli , sezione Specific , con ancora metodi di autenticazione per **Ldap** per **Proxy** caratteristiche dei Router **CISCO** eccetera.

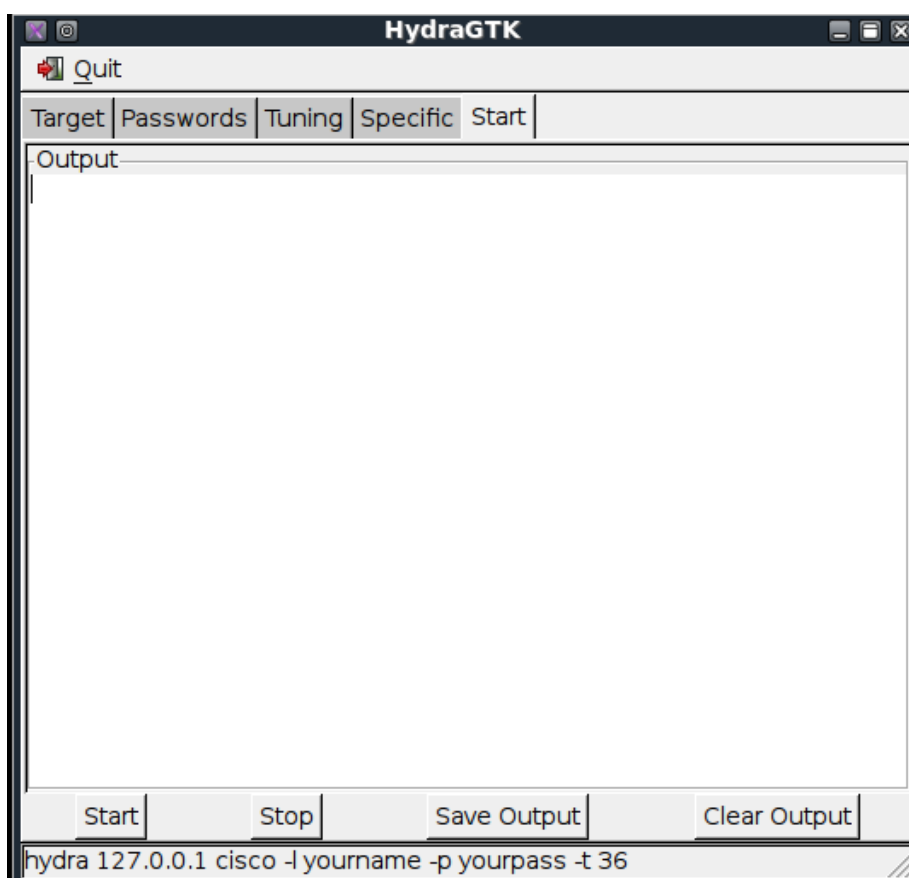
Sono molte opzioni in tutto, rirordiamo però che il bruteforce non è un attacco rapido , ma lento , molto lento , non nel lavoro ma nella riuscita...

Il metodo più rapido nel bruteforcing è sempre quello di raccogliere informazioni sull' host / admin da attaccare per costruirci delle password tramite , (social engeneering) , che poi di solito si va ad aggiungere ad una wordlist generica, questo metodo è essenziale e Xhydra con il metodo precedentemente descritto dei Tasks e del timeout è uno strumento eccellente.

Ovviamente noi dobbiamo vedere con gli occhi di chi l' attacco lo compie, per arrivare ad una difesa che sia la migliore possibile.

Una volta che l' attacco è stato lanciato si possono aspettare ore – giorni e Xhydra ce lo comunicherà nell' ultima sezione della sua GUI, secondo logicamente le nostre opzioni inserite nelle sezioni precedenti.

In questa descrizione naturalmente la sezione è vuota...



Dutante l' inserimento dei dati e delle credenziali nella GUI di Xhydra possiamo vedere nel riquadro in basso dell' interfaccia lo stesso comando che daremo ad Hydra se usato in shell, senza GUI quindi , questo ci fa avere un quadro della situazione anco più chiaro.

Bene per quanto riguarda la descrizione i Xhydra è tutto, chi volesse pprofondire è presente nella pagina apposita [**Video**] del portale un video che dimostra un' attacco brteforce con Xhydra.

Il testo che segue nella seconda parte di questo pdf describe le fasi del video.

PROCEDURA:

- Identificazione sistema attaccante con indirizzo IP ottenuto da **ifconfig**
- scanning dell' host con **nmap** ed opzioni di fingerprinting
- preparazione **wordlist** con inserimento nel mezzo delle password più probabili
- lancio e configurazione di **XHydra**
- Apertura sessione **Telnet** con credenziali otenute dall' attacco

Seguendo il video...

lanciando uno scanning con **nmap** contro il server , con opzioni di *service fingerprinting* , vediamo subito che la porta **23** del server , all' indirizzo **192.168.1.100** è aperta ed utilizzata per il servizio **Telnet** , solito sulla porta 23.

ecco infatti il risultato della scansione...

```
HaCkLaB ~ # nmap -sV -T Aggressive 192.168.1.100 -v
Starting Nmap 4.68 ( http://nmap.org ) at 2008-09-10 13:44 GMT
Interesting ports on 192.168.1.100:
Not shown: 1710 filtered ports
PORT STATE SERVICE VERSION
23/tcp open telnet Microsoft Windows XP telnetd
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn
445/tcp open microsoft-ds Microsoft Windows 2003 microsoft-ds
1027/tcp open IIS?
MAC Address: 00:02:72:61:7B:52 (CC&C Technologies)
Service Info: OSs: Windows XP, Windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.891 seconds
```

Ora per iniziare l' attacco basta crearci un file di testo che poi andremo ad utilizzare come *wordlist* per le nostre eventuali password... ..il file , con estensione ***.txt** , lo metteremo per comodità nel nostro **Desktop** , nel mio caso con il nome **pwd.txt**.

Per avere una wordlist decente ci sono molti mezzi , in **BackTrack** è presente ad esempio **wyd** per la raccolta di specifiche wordlist anche attraverso pagine **HTML**, nel caso specifico di questo video ho scaricato una semplice wordlist in formato ***.txt** ed ho aggiunto nel mezzo una password mia.

Bene , vista la scansione possiamo passare i risultati della stessa a **XHydra** , in questo modo possiamo lanciare l' attacco.

Come potete vedere dal video , appena compilati tutti i campi necessari Hydra inizia a fare i tentativi di login , secondo le impostazioni che noi abbiamo inserito , nel caso del video , ho inserito **50 task** con un timeout di **59 secondi**.

Questo natralmente è sol una dimostrazione, nel caso di un vero attacco avremo dovuto mettere un numeo di tentativi molto inferiore altrimenti il server avrebbe di sicuro bloccato in qualche modo l' accesso da remoto.

Una volta che si vedono i tentativi di Xhydra, si può essere ancor più certi delle credenziali esatte, se si seleziona nella 3^a sezione **Tuning** l' uscita dopo il login esatto: **Exit after first found pair**.

Dopo il lancio e i tentativi, il risultato arriva presto...

```
*** user: Administrator *** password: komintern ***
```

alla prossima ;)

Xhydra è un tool della THC - [TheHacker'sChoice](#)

in BackTrack:

BackTrack->PrivilegeEscalation->PasswordsAttacks->PasswordOnLineAttacks->[X/Hydra](#)



www.backtrack.it

Questo documento è da ritenersi esclusivamente per scopi informativi / didattici, l' autore del testo e coloro che lo ospitano sul proprio spazio non sono responsabili delle azioni commesse da terze parti.

(c)2008 *brigante* for backtrack.it published under [GNU/GPL-v3](http://www.gnu.org/licenses/gpl-3.0.html)