Progettino 1
Corso di Sicurezza

Alessio Lucciola
Matricola 1823638

2 aprile 2021

Contents

1 Introduzione

Il seguente progetto prevedeva di crackare il maggior numero di password a partire da un file dei valori hash, utilizzando un qualsiasi strumento.

2 Approccio

Per svolgere questo progetto ho deciso di utilizzare John The Ripper, un software *open source* i cui punti di forza sono la possibilità di agire combinando diverse modalità di cracking e l'autorilevamento di password in hash. Sono state provate diverse modalità, via via sempre più accurate, per cercare di trovare il maggior numero di password.
Inizialmente ho utilizzato la modalità "single crack" con la quale, in breve tempo, sono riuscito a trovare 31 occorrenze (dove 30 sono utenti con password "NO PASSWORD").
Successivamente sono passato alla "wordlist mode". Sono partito con poche wordlist di piccole dimensioni per testare la fattibilità di questo metodo, riuscendo a trovare svariate password. Visto l'esito positivo, ho iniziato a scaricare altre note wordlist di dimensioni sempre maggiori (ad esempio all.lst di Openwall) andandole poi a testare. Queste mi hanno permesso di rivelare un buon numero di password.
Sono poi passato al metodo brute-force "incremental". Prima di tutto, ho avviato un ciclo con parametri "–min-length=5 –max-length=6" che mi ha permesso di scovare buona parte delle password da cinque e sei caratteri. Ho poi effettuato un altro ciclo su password di 7 caratteri ma ho deciso di abbandonare questo metodo perchè troppo dispensioso. Ho quindi iniziato ad applicare varie maschere che hanno accorciato notevolmente i tempi di ricerca ed ho iterato questo metodo anche per le password di otto caratteri. L'obiettivo delle maschere era quello di trovare password con un pattern predefinito (ad esempio parole di sette caratteri con un numero alla fine). Alcune maschere hanno avuto un buon esito permettendomi di trovare, in maniera abbastanza veloce, alcune password. Sono state testate svariate maschere anche in base alla struttura delle password già trovate in precedenza (alcuni esempi di comandi con maschere si trovano nella lista dei comandi).
Ho infine provato ad utilizzare il metodo "prince" con la wordlist "rockyou.lst", su password di 7 e 8 caratteri, utilizzando i parametri "–prince-elem-cnt-min=1 –prince-elem-cnt-max=2".
I test sono stati svolti principalmente utilizzando il charset "alnum" (caratteri alfanumerici). Alcuni test sono stati svolti con altri charset in modo da includere anche caratteri speciali.

In totale, combinando i vari metodi, sono state trovate **102 password** (su 114).

3 Lista delle password

Qui di seguito, una tabella di terne username, password in chiaro, la rispettiva versione hash e il numero del comando con il quale la password è stata scoperta:

	Username	**Password**	**Versione Hash**	**Comando**
1	zjjyl	zhang123	FoncLBJBak4J2	3
2	zjie	NO PASSWORD		1
3	zhonggu	bowang	aGhUv.z.0aSXs	9
4	yuxm	yuheng	rlS/YAKc9KhaM	2
5	yanc	NO PASSWORD		1
6	xiangcai	NO PASSWORD		1
7	wutao	wwwwww	ASad7icrMKkos	2
8	wenxinqi	this6811	pX2.yYDEMKSBw	8
9	weizh	NO PASSWORD		1
10	wanfei	llchen12	3YV/IUiVwDVHo	3
11	vpetrov	NO PASSWORD		1
12	tuefel	Thebone5	bb5WG8oLJOkyM	3
13	tsljz	ljz5865	kRSzwSCu39p9.	10
14	tianshi	cpre532	NKYidjg81QZSw	11
15	tdinman	tme3garp	z8aQQXPzVQaNw	14
16	surendra	ultimate	JjXqf52ZB2uVs	2
17	stony	kiesha	4xKMtR0/TlcYg	9
18	sherli	new65596	smpjBCeZNc3V.	5
19	ratnakar	NO PASSWORD		1
20	preungsa	alissara	QNPt0rtcOqVHg	2
21	prasad	poruri	skc9rL5TEkaBQ	2
22	plcui	peilian	f1hDinAwKcMNc	2
23	pivanov	acmahi2	vYRlGAiUcTAOQ	3
24	phan	hp1215	/jqVvYA/m4M2o	9
25	pferdig	NO PASSWORD		1
26	parikh	s8390	nA3P8SQtbNA0A	9
27	norules	zen2zach	fFdxLoH4/Rkew	14
28	nishi	qwer123	f9kEW9DnuhRAk	3
29	naumaz	nm542	qzFcZ3btxgsdA	9
30	mmeiners	vortex	e7hvcqLV0YUmQ	2
31	ljh	NO PASSWORD		1
32	lchill	fosteck	wKZMDUqnhfcYA	2
33	kwhitake	b1llet20	PQ/I3C99cfbcY	8
34	krishna	NO PASSWORD		1
35	jwcarter	dorothy	HpUlZlNIV6TH2	2
36	jaalex	lind1ber	oMNCdIjRcJgQg	13
37	hagens	jeremey	EwsR4wcQ9mCtw	2

38	freds	311bliss	goAVEUtPbFVdc	5
39	fanp	ffffff	xOBJK020QFPMo	2
40	daimj	nianzhen	E0GeYx.9dkRes	4
41	creynold	miss69a	2W/IOXfPmVYaw	15
42	chenfeng	NO PASSWORD		1
43	c1zhu	NO PASSWORD		1
44	C1zavesk	st23bc	6VDfiJNHJWjZA	9
45	c1vander	NO PASSWORD		1
46	C1stockh	lastclas	zYAPRhE0EvYhI	2
47	C1steph2	not4me	ge6liK2Vq3aco	9
48	C1steph1	hilander	jyJRC.Oa9fn0Q	4
49	c1stavro	jam1mer	8Xh0uHo2LKdOY	8
50	C1sowads	NO PASSWORD		1
51	C1smith	NO PASSWORD		1
52	C1rolfes	ranger	9tyDMjBEb0VM6	2
53	C1reynol	NO PASSWORD		1
54	C1ray	niloy1ra	R/ANeRa8bpyhY	12
55	c1ray	NO PASSWORD		1
56	c1rasper	NO PASSWORD		1
57	C1rasmus	karl9544	ihhR6n2aFUyag	16
58	C1rapp	tigers	E8n1y32c.rokw	2
59	C1phan	security	iPGAYh7UQyrP6	2
60	c1pender	passme	U.0mgW/1TJXps	2
61	c1patric	NO PASSWORD		1
62	C1obrado	C1obrado	lRERnUQ/HrStU	1
63	C1muegge	Stuka1	14b0ve3npkLLg	9
64	C1marotz	Ilv32Jas	lh7rgQfngXKX6	8
65	c1maddef	NO PASSWORD		1
66	C1luttre	shadow	31QyV/P1F.Qcw	2
67	C1lualle	kicker51	R7GRVeQkxHGAw	7
68	C1little	christin	/PBiubaP4vV/Q	2
69	c1liss	NO PASSWORD		1
70	C1leung	NO PASSWORD		1
71	C1kumar	pvpvzm	pI4J5TtF5PDEE	5
72	C1klopp	NO PASSWORD		1
73	C1jacobo	noogie.	YG7sgFjyVjLgE	3
74	c1hovre	mack66y	IHcr1bcr31Dg6	15
75	C1harris	merlin1	CNK/cFsoYuldM	4
76	c1gonzal	rhette	y8y/b6iwz0.wI	9
77	c1gessne	NO PASSWORD		1
78	c1franko	NO PASSWORD		1
79	C1fitzge	NO PASSWORD		1
80	C1fell	Feller98	A.1SXAwxwtkuw	8

81	C1feldka	cpre532	3KECvQDnmCIMg	11
82	C1elkhat	nsk1115	ctCD2jHdQwO/s	5
83	c1dube	kitotoki	tC86Zvr12gl9U	3
84	C1diaz	NO PASSWORD		1
85	c1deng	NO PASSWORD		1
86	c1delsey	murdoch	UYWQaUAOaq54c	3
87	C1dean	bailey	TFQwXXPUC2PQI	3
88	C1dawson	cuse123	T2HvAD2AvLmeQ	10
89	C1corbet	ash1dog	PhvQwp0O2y73g	6
90	c1cheram	NO PASSWORD		1
91	C1canton	tavy2ner	nY7juyYKK60ws	13
92	C1caldej	NO PASSWORD		1
93	C1anders	javat1ze	yov58b5qxeqOw	12
94	C1albata	bara824	2KTn9bkZgU9QI	3
95	C1adair	superman	4ksmQIt8tD5uc	2
96	bsmith1	ukv930	mHEpEuk8EKfn2	9
97	bowang	cpre532	AdAvT/LLjeQL6	11
98	bork	moreno	yvTPsIMgxaaRs	4
99	binzhu	another	Wl4BjRtBq86u6	2
100	bin_lin	zhuoyang	YD.oUzn6Thavk	4
101	asokt	NO PASSWORD		1
102	aruna	akka1508	ngddzm/Plxlt2	6

4 Lista dei comandi (con tempo di esecuzione)

Qui di seguito è presente una lista dei comandi utilizzati per trovare le password. Ho inserito **solamente** i comandi che mi hanno permesso, in un tempo ragionevole, di trovare almeno una password. Ogni comando è stato eseguito per almeno 30/40 minuti, dopo i quali la ricerca è stata interrotta (nel caso in cui non sia stata scoperta alcuna nuova password). Sotto ad ogni comando è presente il relativo tempo di esecuzione e le password trovate in quel lasso di tempo.
Lista dei comandi:

1. john –single "file/passwd"
   Tempo: 31g 0:00:00:45

2. john –wordlist=="files/all.lst" "files/passwd"
   Tempo: 20g 0:00:01:13

3. john –wordlist="files/rockyou.lst" "files/passwd"
   Tempo: 10g 0:00:02:08

4. john –wordlist="files/realuniq.lst" "files/passwd"
   Tempo: 5g 0:00:10:49

5. john –wordlist="files/pwned.lst" "files/passwd"
   Tempo: 4g 0:00:17:45

6. john –wordlist="files/openwall_all.lst" "files/passwd"
   Tempo: 2g 0:00:1:27

7. john –wordlist="files/10_million_password_list.txt" "files/passwd"
   Tempo: 1g 0:00:2:31

8. john –wordlist="files/xsukax-Wordlist-All.txt" "files/passwd"
   Tempo: 5g 0:00:34:59

9. john.exe –incremental –min-length=5 –max-length=6 –fork=12 "files/passwd"
   Tempo: 10g 0:02:48:34

10. john.exe –incremental –min-length=7 –max-length=7 –fork=12 "files/passwd"
    Tempo: 2g 0:02:19:02

11. john.exe –incremental –mask=?l?l?l?l?d?d?d –fork=12 "files/passwd"
    Tempo: 3g 0:00:36:45

12. john.exe –incremental –mask=?l?l?l?l?l?d?l?l –fork=12 "files/passwd"
    Tempo: 2g 0:01:13:55

13. john.exe –incremental –mask=?l?l?l?l?d?l?l?l –fork=12 "files/passwd"
    Tempo: 2g 0:01:13:55

14. john.exe –incremental –mask=?l?l?l?d?l?l?l?l –fork=12 "files/passwd"
    Tempo: 2g 0:02:01:03

15. john.exe –prince="files/rockyou.lst" –prince-elem-cnt-min=1 –prince-elem-cnt-max=2 –min-len=7 –max-len=7 –fork=12 "files/passwd"
    Tempo: 2g 0:00:02:12

16. john.exe –prince="files/rockyou.lst" –prince-elem-cnt-min=1 –prince-elem-cnt-max=2 –min-len=8 –max-len=8 –fork=12 "files/passwd"
    Tempo: 1g 0:00:14:19

5 Lista delle wordlist

Qui di seguito, la lista delle wordlist utilizzate:

- openwall_all
- rockyou
- pwned-password-2.0
- realuniq
- 10_million_password_list
- xsukax-wordlist
- weakpass-2.0

6 Specifiche Hardware

Qui di seguito, le specifiche della macchina sulla quale è stato svolto il progetto:

- OS: Microsoft Windows 10 Home 64 bit;
- Versione: 10.0.19042 N/D build 19042;
- CPU: Intel(R) Core(TM) i5-10600 CPU @ 3.30GHz (12 CPUs), 3.3GHz;
- Memoria: 16384MB RAM;
- GPU: NVIDIA GeForce GTX 1060 3GB;