分析混合字典攻击中的规则效率

Passcape Software

1 分析混合字典攻击中的规则效率

1.1 摘要

当涉及到密码解密时，混合字典攻击 是一种非常灵活和不可或缺的工具。与 普通字典攻击 不同的是，虽然使用了一种自定义的攻击，但仍然有一组固定的单词变异规则，混合攻击可以根据您的需要完全调整。

许多用户在解密密码时使用自己的密码变异规则，使用不同的设置多次启动混合字典攻击。例如，第一次攻击从快速搜索流行密码的最常用且有限的一组规则开始，然后使用混合攻击规则查找非拉丁密码，然后使用一组完整的规则查找所有可能的组合等进行缓慢攻击。顺便提一下，以下链接提供了600000多条变异规则的完整集合: hybrid_all.ini

1.2 密码生成规则

许多高级研究人员在解密密码时使用他们自己的密码突变规则，用不同的设置启动混合字典攻击几次。例如，第一次攻击从最常用的、有限的规则集开始，用于快速搜索流行的密码，然后是混合攻击，用于定位非拉丁语的密码，然后是慢速攻击，用全套的规则找出所有可能的组合，等等。顺便说一下，超过600000条突变规则的完整集合可在以下链接中找到：hybrid_all.ini

在特定情况下，什么是最有效的规则文件？问题是，有些规则是根据流行的突变规则来搜索密码的，有些则是为了寻找某些类型的密码。比如说，像这些：

overwrite.ini, insert.ini - 搜索替换或插入字符的密码
numbers.ini - 搜索在单词开头或结尾有数字的密码
simple_dates.ini - 搜索带有日期的密码
nonenglish_words.ini - non-Latin 密码的变异
l33t.ini -对于用 leet, 编写的密码，如密码 -> p@$$w0rd
dotcom.ini - 单词末尾的域

1.3 规则的有效性

1.3.1 整体效率

我们试图从一些密码集是特定于某种类型的密码这一事实中抽象出来，并试图评估我们的 Windows Password Recovery tool 所附带的每个规则文件的有效性。我们从Defcon Crack Me if You Can 2010比赛中抽取了30819个NTLM哈希值的列表。然后依次用每一个（一个）集合开始混合攻击，以评估其有效性，检查工作时间等。攻击是使用内置的wpr.pcd词典进行的，该词典由5398185个单词组成。使用的硬件 - Nvidia GTX 1060。下表显示了最有效的集合列表，按发现的最大项目数排序。

Rule-file name	Passwords found	% found	Number of rules	Work time (sec)	Found pwds per rule	Speed (found pwds/sec)
hybrid_all.ini	11248	36,5%	616716	3487	0,02	3,23

Rule-file name	Passwords found	% found	Number of rules	Work time (sec)	Found pwds per rule	Speed (found pwds/sec)
Hashcat_generated2.ini	7552	24,5%	304062	1775	0,02	4,25
nsa.ini	7270	23,6%	123286	552	0,06	13,17
english_words.ini	6758	21,9%	30055	208	0,22	32,49
Hashcat_d3ad0ne.ini	6492	21,1%	35323	189	0,18	34,35
InsidePro-HashManager.ini	5785	18,8%	6469	28	0,89	206,61
yurets.ini	5724	18,6%	74585	394	0,08	14,53
Hashcat_rockyou-30000.ini	5324	17,3%	29999	139	0,18	38,30
Hashcat_T0XlCv1.ini	5130	16,6%	11936	53	0,43	96,79
InsidePro-PasswordsPro.ini	4819	15,6%	3119	16	1,55	301,19
d3adhob0.ini	4764	15,5%	57536	308	0,08	15,47
Hashcat_generated.ini	4531	14,7%	14726	71	0,31	63,82
Hashcat_T0XlC.ini	3687	12,0%	4086	21	0,90	175,57
overwrite.ini	3239	10,5%	3	7	1079,67	462,71
insert.ini	3174	10,3%	3	7	1058,00	453,43
fasthash.ini	2112	6,9%	2943	16	0,72	132,00
Hashcat_T0XlC-insert_00-99_1950-2050_toprules_0_F.ini	2105	6,8%	4015	19	0,52	110,79
megatron-1.ini	1994	6,5%	450	2	4,43	997,00
megatron-2.ini	1804	5,9%	10664	50	0,17	36,08
Hashcat_best64.ini	1661	5,4%	77	1	21,57	1661,00
numbers.ini	1457	4,7%	650	5	2,24	291,40
simple_dates.ini	1300	4,2%	4828	32	0,27	40,63
Hashcat_combinator.ini	1287	4,2%	39	2	33,00	643,50
Hashcat_toggles5.ini	1215	3,9%	4943	26	0,25	46,73

Rule-file name	Passwords found	% found	Number of rules	Work time (sec)	Found pwds per rule	Speed (found pwds/sec)
Hashcat_toggles4.ini	1178	3,8%	1940	10	0,61	117,80
Hashcat_toggles3.ini	1153	3,7%	575	3	2,01	384,33
Hashcat_toggles2.ini	1136	3,7%	120	1	9,47	1136,00
Hashcat_toggles1.ini	1107	3,6%	15	2	73,80	553,50
Hashcat_T0XlC-insert_space_and_special_0_F.ini	1023	3,3%	480	2	2,13	511,50
Hashcat_specific.ini	997	3,2%	176	1	5,66	997,00
Hashcat_Incisize_leetspeak.ini	869	2,8%	15487	120	0,06	7,24
Hashcat_T0XlC-insert_top_100_passwords_1_G.ini	856	2,8%	1600	10	0,54	85,60
nonenglish_words.ini	824	2,7%	4448	82	0,19	10,05
hashcat_ninja_leetspeak.ini	733	2,4%	2047	15	0,36	48,87
Hashcat_leetspeak.ini	704	2,3%	17	2	41,41	352,00
l33t.ini	583	1,9%	1046	11	0,56	53,00
Hashcat_oscommerce.ini	135	0,4%	256	2	0,53	67,50
dotcom.ini	127	0,4%	40	2	3,18	63,50

第一栏显示的是通过给定的规则集找到的密码数量。第二列显示找到的密码数量的百分比。第三列显示文件的规则总数。第四列是验证所有规则所花费的时间。接下来的两列就有点意思了，输出的是最有效的规则。更具体地说，是单个规则发现的密码数量和每秒发现的密码数量。

看到一些规则集（例如insert.ini和overwrite.ini）的显著优势和其他规则集的失败，例如Hashcat_Incisize_leetspeak.ini，相当有趣。但这是可以理解的，考虑到它们主要是为搜索某些类型的密码而设计的。总的来说，这些结果对于那些在恢复密码时面临严格时限的人来说是很有用的。例如，一个很好的平衡规则集是InsidePro-HashManager.ini，它仅用28秒就找到了5785个密码。作为比较，所有突变规则集在使用上述硬件的情况下，在1小时内找到了11248个密码。

1.3.2 十大最佳规则集

前10个最佳规则集(按找到的密码数量排序)

Rule-file name	Passwords found	% found
hybrid_all.ini	11248	36,5%
Hashcat_generated2.ini	7552	24,5%
nsa.ini	7270	23,6%
english_words.ini	6758	21,9%
Hashcat_d3ad0ne.ini	6492	21,1%
InsidePro-HashManager.ini	5785	18,8%
yurets.ini	5724	18,6%
Hashcat_rockyou-30000.ini	5324	17,3%
Hashcat_T0XlCv1.ini	5130	16,6%
InsidePro-PasswordsPro.ini	4819	15,6%

1.3.3 最大的10个规则集

前10个最大的规则集(按规则数量)

Rule-file name	Number of rules
hybrid_all.ini	616716
Hashcat_generated2.ini	304062
nsa.ini	123286
yurets.ini	74585
d3adhob0.ini	57536
Hashcat_d3ad0ne.ini	35323
english_words.ini	30055
Hashcat_rockyou-30000.ini	29999
Hashcat_Incisize_leetspeak.ini	15487
Hashcat_generated.ini	14726

1.3.4 最高效的10个规则集

前10个最有效的规则集(按每条规则找到的密码数量)

Rule-file name	Found passwords per rule
overwrite.ini	1079,67
insert.ini	1058,00
Hashcat_toggles1.ini	73,80
Hashcat_leetspeak.ini	41,41
Hashcat_combinator.ini	33,00
Hashcat_best64.ini	21,57

Rule-file name	Found passwords per rule
Hashcat_toggles2.ini	9,47
Hashcat_specific.ini	5,66
megatron-1.ini	4,43
dotcom.ini	3,18

1.3.5 最快的10个规则集

最快的10个规则集(按找到的密码数量排在第二位)。

Rule-file name	Found passwords in second
Hashcat_best64.ini	1661,00
Hashcat_toggles2.ini	1136,00
Hashcat_specific.ini	997,00
megatron-1.ini	997,00
Hashcat_combinator.ini	643,50
Hashcat_toggles1.ini	553,50
Hashcat_T0XlC-insert_space_and_special_0_F.ini	511,50
overwrite.ini	462,71
insert.ini	453,43
Hashcat_toggles3.ini	384,33