हाइब्रिड डिक्शनरी अटैक में नियमों की कार्यक्षमता का विश्लेषण

© 2017 पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)
पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)

1. हाइब्रिड डिक्शनरी अटैक में नियमों की कार्यक्षमता का विश्लेषण 3

1.1 सार 4

1.2 पासवर्ड जनरेशन नियम 4

1.3 नियमों की कार्यक्षमता 4

1.3.1 समग्र कार्यक्षमता 4

1.3.2 टॉप 10 सर्वश्रेष्ठ नियम-सेट 7

1.3.3 टॉप 10 सबसे बड़े नियम-सेट 7

1.3.4 टॉप 10 सबसे कुशल नियम-सेट 8

1.3.5 टॉप 10 सबसे तेज़ नियम-सेट 8

Index 0

© 2017 पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)

हाइब्रिड डिक्शनरी अटैक में नियमों की कार्यक्षमता का विश्लेषण

1 हाइब्रिड डिक्शनरी अटैक में नियमों की कार्यक्षमता का विश्लेषण

1.1 सार

जब पासवर्ड डिक्रिप्शन की बात आती है, तो हाइब्रिड डिक्शनरी अटैक एक बहुत ही लचीला और अपरिहार्य टूल होता है। एक सामान्य डिक्शनरी अटैक के विपरीत, जो हालांकि एक कस्टम का उपयोग करता है, लेकिन फिर भी शब्द म्यूटेशन नियमों का एक निश्चित सेट है, एक हाइब्रिड अटैक को आपकी आवश्यकताओं के अनुसार पूरी तरह से एडजस्ट किया जा सकता है।

कई यूजर्स पासवर्ड को डिक्रिप्ट करते समय अपने स्वयं के पासवर्ड म्यूटेशन नियमों का उपयोग करते हैं, विभिन्न सेटिंग्स के साथ कई बार हाइब्रिड डिक्शनरी अटैक शुरू करते हैं। उदाहरण के लिए, पहला अटैक लोकप्रिय पासवर्ड को जल्दी से खोजने के लिए सबसे अधिक उपयोग किए जाने वाले और सीमित नियमों के साथ शुरू होता है, फिर गैर-लैटिन पासवर्ड का पता लगाने के लिए एक हाइब्रिड अटैक नियम होता है, और फिर सभी संभावित संयोजनों आदि खोजने के लिए नियमों के पूरे सेट के साथ एक धीमा अटैक होता है। वैसे, 600000 से अधिक म्यूटेशन नियमों का एक पूरा संग्रह निम्नलिखित लिंक पर उपलब्ध है: hybrid_all.ini

1.2 पासवर्ड जनरेशन नियम

कई उन्नत शोधकर्ता पासवर्ड को डिक्रिप्ट करते समय अपने स्वयं के पासवर्ड म्यूटेशन नियमों का उपयोग करते हैं, विभिन्न सेटिंग्स के साथ कई बार हाइब्रिड डिक्शनरी अटैक शुरू करते हैं। उदाहरण के लिए, पहला हमला लोकप्रिय पासवर्ड को जल्दी से खोजने के लिए सबसे अधिक उपयोग किए जाने वाले और सीमित नियमों के साथ शुरू होता है, फिर गैर-लैटिन पासवर्ड का पता लगाने के लिए एक हाइब्रिड हमला होता है, और फिर सभी संभव संयोजन पता लगाने के लिए नियमों के पूरे सेट के साथ एक धीमा हमला होता है। वैसे, निम्नलिखित लिंक पर 600000 से अधिक उत्परिवर्तन नियमों का एक पूरा संग्रह उपलब्ध है: hybrid_all.ini

दी गई स्थिति में सबसे प्रभावी नियम-फाइल क्या है? समस्या यह है कि नियमों के कुछ सेट लोकप्रिय म्यूटेशन के आधार पर पासवर्ड खोजने के लिए बनाए गए थे, अन्य कुछ और प्रकार के पासवर्ड खोजने के लिए। उदाहरण के लिए, इन लोगों की तरह:

overwrite.ini, **insert.ini** - बदले गए या सम्मिलित वर्ण वाले पासवर्ड खोजें
numbers.ini - किसी शब्द के आरंभ या अंत में संख्याओं वाले पासवर्ड खोजें
simple_dates.ini - तिथियों के साथ पासवर्ड खोजें
nonenglish_words.ini - गैर-लैटिन पासवर्ड का म्यूटेशन
l33t.ini - leet में लिखे पासवर्ड के लिए, जैसे पासवर्ड -> p@$$w0rd
dotcom.ini - शब्दों के अंत में डोमेन

1.3 नियमों की कार्यक्षमता

1.3.1 समग्र कार्यक्षमता

हमने इस तथ्य से सार निकालने की कोशिश की कि कुछ सेट एक निश्चित प्रकार के पासवर्ड के लिए विशिष्ट हैं, और हमारे विंडोज पासवर्ड रिकवरी टूल के साथ आने वाले प्रत्येक नियम-फाइल की प्रभावशीलता का मूल्यांकन करने का प्रयास किया। हमने Defcon Crack Me if You 2010 कॉन्टेस्ट से लिए गए 30819 NTLM हैश की एक सूची बनाई है। फिर क्रमिक रूप से उनकी प्रभावशीलता का मूल्यांकन करने, कार्य समय की जांच करने आदि के लिए प्रत्येक (एक) सेट के साथ हाइब्रिड हमला शुरू किया। यह हमला 5398185 शब्दों से युक्त अंतर्निहित wpr.pcd शब्दकोश का उपयोग करके किया गया था। प्रयुक्त हार्डवेयर - Nvidia GTX 1060। नीचे दी गई टेबल सबसे प्रभावी सेटों की सूची दिखाती है, जो अधिकतम संख्या में मिली वस्तुओं के आधार पर क्रमबद्ध होती है।

नियम-फ़ाइल का नाम	पासवर्ड मिले	% मिले	नियमों की संख्या	कार्य समय (सेकंड)	प्रति नियम मिले हुए पासवर्ड्स	स्पीड (पासवर्ड्स मिले/सेकंड)
hybrid_all.ini	11248	36,5%	616716	3487	0,02	3,23
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

नियम-फ़ाइल का नाम	पासवर्ड मिले	% मिले	नियमों की संख्या	कार्य समय (सेकंड)	प्रति नियम मिले हुए पासवर्ड्स	स्पीड (पासवर्ड्स मिले/सेकंड)
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
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_T0XIC-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_T0XIC-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

पहला कॉलम दिए गए नियमों के सेट द्वारा पाए गए पासवर्ड की संख्या को दर्शाता है। दूसरा प्रतिशत में पाए गए पासवर्ड की संख्या प्रदर्शित करता है। तीसरा कॉलम फ़ाइल के लिए नियमों की कुल संख्या दिखाता है। चौथे में, सभी नियमों को

सत्यापित करने में लगा समय। अगले दो कॉलम थोड़े अधिक दिलचस्प हैं और सबसे प्रभावी नियमों को प्रदर्शित करते हैं। अधिक विशेष रूप से, एक नियम के लिए पाए गए पासवर्ड की संख्या और प्रति सेकंड पाए गए पासवर्ड की संख्या।

कुछ सेटों की महत्वपूर्ण श्रेष्ठता (उदाहरण के लिए, insert.ini और overwrite.ini) और दूसरों की विफलता, जैसे कि Hashcat_Incisize_leetspeak.ini को देखना काफी मज़ेदार है। लेकिन यह समझ में आता है, इस बात को ध्यान में रखते हुए कि वे मुख्य रूप से कुछ प्रकार के पासवर्ड खोजने के लिए डिज़ाइन किए गए थे। सामान्य तौर पर, परिणाम उन लोगों के लिए उपयोगी हो सकते हैं जो पासवर्ड रिकवरी करते समय सख्त समय सीमा का सामना करते हैं। उदाहरण के लिए, एक अच्छा संतुलित नियम सेट InsidePro-HashManager.ini है, जिसने केवल **28** सेकंड में **5785** पासवर्ड ढूंढे हैं। तुलना के लिए, सभी म्यूटेशन नियमों के सेट में उपरोक्त हार्डवेयर का उपयोग करके ~ **1 घंटे** के लिए **11248** पासवर्ड मिले।

1.3.2 टॉप 10 सर्वश्रेष्ठ नियम-सेट

टॉप १० सर्वश्रेष्ठ नियम-सेट (पाए गए पासवर्ड की संख्या के आधार पर छाँटा गया)

नियम-फ़ाइल का नाम	पासवर्ड मिले	% मिले
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 टॉप 10 सबसे बड़े नियम-सेट

टॉप 10 सबसे बड़े नियम-सेट (नियमों की संख्या के अनुसार)

नियम-फ़ाइल का नाम	नियमों की संख्या
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 टॉप 10 सबसे कुशल नियम-सेट

टॉप 10 सबसे कुशल नियम-सेट (प्रति नियम पाए गए पासवर्ड की संख्या के अनुसार)

नियम-फ़ाइल का नाम	प्रति नियम पासवर्ड मिले
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
Hashcat_toggles2.ini	9,47
Hashcat_specific.ini	5,66
megatron-1.ini	4,43
dotcom.ini	3,18

1.3.5 टॉप 10 सबसे तेज़ नियम-सेट

टॉप 10 सबसे तेज़ नियम-सेट (दूसरे में पाए गए पासवर्ड की संख्या के अनुसार)

नियम-फ़ाइल का नाम	कितने सेकंड में पासवर्ड मिला
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

© 2017 पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)