sliding_writeup

Table of Contents

1 Sliding Writeup

Group 07, Vuk, Mack, Justin

1.1 Linux

1.1.1 Russian and Roman Generals: fabius_maximus

Found names on wikpedia of generals at https://en.wikipedia.org/wiki/List_of_Roman_generals and https://en.wikipedia.org/wiki/Category:Russian_generals Used python to parse all names and create a word list of all combinations of last names connected (connecters "$" "%" "_") with corresponding first names as well as capitalizing the first letter of a name and the remaining lower case, or all upper, or all lower. Also applying the capitalizations independently to the first and last name. Passed wordlist of all combinations to john the ripper, results was found immediately.

1.1.2 11 Letter Word: flamboyancy

Found all 11 letter long english words at https://www.bestwordlist.com/11letterwords.txt Used python to parse all words and lower case them. Passed wordlist of all words to john the ripper, result was found immediately.

1.1.3 8 digit hex number sans 0x: a5b5ef91

Created custom incremental mode with rules maxLen = 8, minLen = 8, charCount = 16 with a custom charset of fedcba9876543210 Result took 6.5 hours to find, originally ran with uppercase characters, exhausted after 7 hours.

1.1.4 10 letter word with leet substitution: r[-laxation14

Found all 10 letter long english words at https://www.bestwordlist.com/10letterwords.txt Used Python to parse all words and create Lowercase combinations with 1 character leet-substituted with a 2 character combo. Found all 2 character combo leet substitutions at http://www.gamehouse.com/blog/leet-speak-cheat-sheet/ Passed wordlist of combinations to john the ripper and applied custom rule of appending 2 digits at the end. Result found in 10 minutes

1.1.5 13 alpha numeric: No solution found.

Ran john the ripper on incremental mode using alnum (all 62 alphanumeric characters) mode, maxLen = 13, minLen = 13, charCount = 62 . Will run forever until it exhausts all possible combinations or finds solution.

1.2 Windows

1.2.1 Dead Musicians (last decade): PeteSeeger

Found names of dead musicians at https://en.wikipedia.org/wiki/List_of_deaths_in_rock_and_roll and https://en.wikipedia.org/wiki/List_of_pop_musicians_who_died_of_drug_overdose Parsed all names in python to make them all capital and passed wordlist to john the ripper From LM hash got result PETSEE, then created seperate wordlist containing peteseeger and applied john the rippers wordlist rules (–rules). Cracked NT hash immediately.

1.2.2 9 letter word: phrenetic

Found all 9 letter long english words at https://www.bestwordlist.com/9letterwords.txt Parsed all words in python to make them all uppercase and passed wordlist to john the ripper. From LM hash got result PHRENET, then created seperate wordlist containing phrenetic and applied john the ripper wordlist rules Cracked NT hash immediately.

1.2.3 11 letter alpha numeric: YEjhqLyvsEA

Ran john the ripper on incremental method with mode UpperNum(uppercase letters plus digits, for 36 total) From LM hash got result YEJHQLYVSEA, took 30 minutes to crack. Created custom incremental with charset YEJHQLYVSEA yejhqlyvsea, rules maxLen = 11, minLen = 11, charCount = 18(john removes duplicate characters for charCount) NT hash cracked immediately.

1.3 Answer to questions

Linux passwords that required wordlists were fast because wordlists are basically completed passwords that required very little mangling. 8 digit hex number required longer because its an exhaustive search for the password going through all possible combinations of the hex value incrementally. 13 alpha numeric is the toughest, as there is no strategy to lower the amount of possible combinations that it must go through incrementally.

Windows passwords that required wordlists were the easiest, as you just pass all uppercase combinations to crack the lm hash, no mangling required. Once you crack the LM hash, there is a limited amount of mangling required to crack NT hash as you already know what you are looking for. 11 letter alpha took the longest for windows hash, as you had to incrementally go through all combintions to find the corrrect upercase characters to crack LM hash.

Windows passwords are easier to crack because LM hashes contain all uppercase characters, which once cracked narrows down the possibilities of required characters to crack the NT hash. Linux hashes don't have this kind of freedom, so they cannot be narrowed down as well.

Author: Justin Barclay

Created: 2016-11-04 Fri 13:48

Emacs 25.1.1 (Org mode 8.2.10)

Validate