Recover Various Password hashes By Using Cryptanalysis Technique

Shailendra Nigam
Computer Science & Engineering Department
DIET, Kharar Mohali(Punjab) India.

Bhanu Sharma
Computer Science & Engineering Department
BBSBEC, Fatehgarh sahib(Punjab) India

Abstract - This paper is based on literature survey and thoughts. Recover various password hashes by using cryptanalysis technique is used for analyzing the hidden information of the system. This technique is based on rainbow table that are used to retrieve the passwords. Rainbow table is an application of Martin Hellman Algorithm. Diffie-Hellman key exchange (D-H) is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented with in the field of cryptography. The aim of this work is to recover the password hashes in plain text format using cryptanalysis attack.

Keywords:- Hellman Algorithm, Rainbow table, Recover password , Hashes

I. INTRODUCTION

Recover Various Password hashes By Using Cryptanalysis Technique is based on the rainbow table and recovery software tool. Rainbow table usually for a cracking password hashes. In this tables are used in recovering the text password but limited set of characters. Rainbow table solve the collisions problem with the help of ordinary hash chain. Rainbow tables are an application of an earlier, simpler algorithm by Martin Hellman. Recover Various Password hashes By Using Cryptanalysis Technique strategy which option strategy to use is one of the most difficult decisions for an option trader. Some recovery software are available in the market but based on the brute force, dictionary attacks and other technique but I will use the cryptanalysis technique because this technique is based on the rainbow table and provide the information about the password in the plain text format. So I will recover password by using cryptanalysis technique concept with the help of password recovery tool software. Packets contain a lot of useful information about password activity that can be used as a description of the general password behavior. Cain and Abel a useful tool for system and network administrator to capture such kind of network information. Packets are units of data traveling in these computer networks and they can carry all the important information from its source to final destination. Packets also contain a wealth of information about the network infrastructure, topologies and provide the information of network traffic. Password packet analyzer will be very useful to people who have the intention to look into more details of what is actually going on inside the network. This analyzer provides additional information about sniffing which users may find helpful. Packet Analyzer also detects network misuse by internal and external users and also handles the documenting regulatory compliance through logging all perimeter and endpoint traffic. This topic is similar to the network packet analyzer. Network packet analyzer provides the information about the network traffic but in this topic it is also provide the information about recover password as well as provide the information of network traffic. This tool to provide forensics, criminal investigators, security officers and government authorities with the ability to retrieve a variety of passwords stored on a PC.

1. 2 Rainbow Table

- A rainbow table is a lookup table offering a time-memory tradeoff used in recovering the plaintext password from a password hash generated by a hash function
  - Approach invented by Martin Hellman
- The concept behind rainbow tables is simple
  - Make one-way hash functions two way by making a list of outputs for all possible inputs up to a character limit

1. 3 How do Rainbow Tables Work?

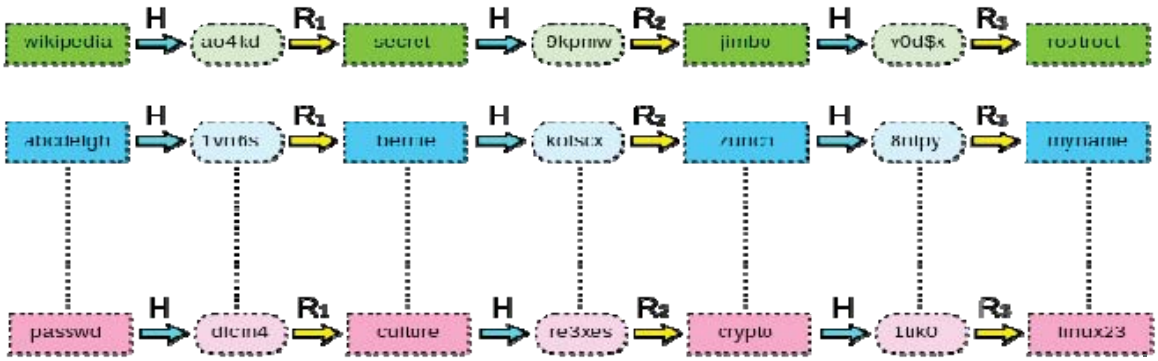

Figure 1.1 Rainbow Tables Working part 1

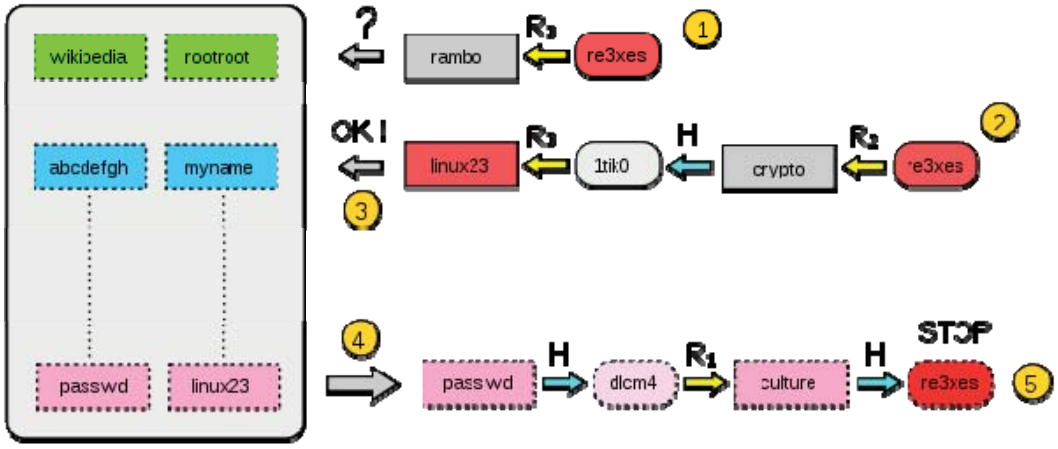

Figure 1.2 Rainbow Tables Working part2

1. 4 Using Rainbow Tables

- You can download your own Rainbow Tables (.rt) and then use a variety of software to test your hash list.
- Tables can vary in size (anywhere from a couple of meg to a couple hundred gb.)
- Rainbow Crack, Ophcrack and Cain and Abel all use .rt files

1.5 Other Information

- Rainbow Tables are Large. A rainbow table set for windows NTHASH exactly 8 characters including only 0-10, a-z, A-Z, and the symbols !* is 134.6GB
- 9+ character rainbow tables can take up terabytes of space.
- Generating rainbow tables requires more time than a brute force attack
- Always “worst case” time complexity.
- Requires access to the password hash

Salting passwords can make the approach unfeasible

II. SYSTEM DESIGN

Existing System

Rainbow tables reduce the difficulty in brute force cracking a single password by creating a large pre-generated data set of hashes from nearly every possible password. Rainbow Tables and Rainbow Crack come from the work and subsequent paper by Philippe Oechslin.1 The method, known as the Faster Time-Memory Trade-Off Technique, is based on research by Martin Hellman & Ronald Rivest done in the early 1980’s on the performance trade-offs between processing time and the memory needed for cryptanalysis. In his paper published in 2003, Oechslin refined the techniques and showed that the attack could reduce the time to attack 99.9%ofMicrosoft's LAN Manager Passwords (alpha characters only) to 13.6 seconds from 101 seconds. Further algorithm refinements also reduced the number of false positives produced by the system. The main benefit of Rainbow Tables is that while the actual creation of the rainbow tables takes much more time than cracking a single hash, after they are generated you can use the tables over and over again. Additionally, once you have generated the Rainbow Tables, Rainbow Crack is faster than brute force attacks and needs less memory than full dictionary attacks. Rainbow Tables are popular with a particularly weak password algorithm known as Microsoft LM hash. LM stands for LAN Manager, this password

algorithm was used in earlier days of Windows and still lives on only for compatibility reasons. By default Windows XP or even Windows Server 2003 keeps the LM hash of your passwords in addition to a more secure hash (NTLMor NTLMv2). This allows for the benefit of backwards compatibility with older operating systems on your network but unfortunately makes the job of password cracking easier if you can obtain the LM hashes instead of the NTLM hashes.

For example Consider the number of possible seven character passwords made exclusively from letters, i.e., no numbers, symbols, etc. For a case-insensitive algorithm (like LAN Manager) this means there's a total of 26 possible values for each character position in the password. Here's how a case-insensitive algorithm's search space compares to one for a case-sensitive algorithm:

Number of possible characters	**Number of possible seven character passwords**
26	26^7 (8,031,810,176 or about 8.0319)
52	52^7 (1,028,071,702,528 or about 1.02812)

So if you have the same CPU, the same memory, and all other factors being equal; the doubling of possible values in the character space will result in, not the doubling of passwords to crack, but an increase a couple orders of magnitude in the number of passwords to crack. So if we assume that LM can use every character on a standard US keyboard it has a character set of 69 possible characters.

Count	**Class**
26	All Letters (Upper and Lower Combination)
10	Digits
10	Shifted Symbols from digit keys
22	Remaining Symbols and their shifted Counter parts
1	Space
----------	----------
69	Total

Case-sensitive algorithms (e.g., the password hashing algorithm on most Unix variants, and Microsoft's NTLM and NTLMv2) give us an additional 26 characters per position, or a character set of 95 possibilities.

To calculate the total number of possible passwords for a given algorithm, you add the total number of passwords for each valid password length (or at least each valid password length for the password space you're searching). LM's maximum effective password length is seven characters for a total search space of 7,555,858,447,479 possible passwords (about 7.55612).

# Characters in password	**Number of possible passwords**
1	69 (69^1)
2	4,761 (69^2)
3	328,509 (69^3)
4	22,667,121 (69^4)
5	1,564,031,349 (69^5)
6	107,918,163,081 (69^6)
7	7,446,353,252,589 (69^7)
==========	==========
	7,555,858,447,479 Total

A case-sensitive algorithm would give us an additional 26 characters, for a total of 95.With the larger character set (but sticking with the seven character password limit for the moment), the total search space is 70,576,641,626,495 possibilities (about 7.05813).

# Characters in password	**Number of possible passwords**
1	95 (95^1)
2	9,025 (95^2)

3	857,375 (95^3)
4	81,450,625 (95^4)
5	7,737,809,375 (95^5)
6	7, 350, 918, 906, 25 (95^6)
7	69,833,729,609,375 (95^7)
==========	
	70,576,641,626,495 Total

So, an algorithm that's case-sensitive has a password search space about nine times larger than Microsoft LAN Manager's

III. Experimental Study

Ophcrack software tool, RainCal software tool, Rainbowcrack-1.5 and Windows Password Recovery software Tools are powerful password auditing tools. The best course of action to protect yourself is to not allow the storage and use of LAN Manager (LM) passwords on your network if you don't absolutely need to and create and enforce a strong password policy that will force the storage and use of passwords as NTLM and not LM. Additionally, the time to compute and space requirements of complex Rainbow Tables should limit the use of them to only determined attackers or auditors. A strong password policy, strong domain security policy, and keeping up with your patches and updates is your best safeguard against password attacks.

Figure 3.1 Oph Crack

Figure 3.2 Oph Crack local SAM with samdump1

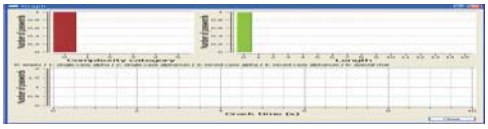

Figure 3.3 Oph Crack Graphical Representation of crack time

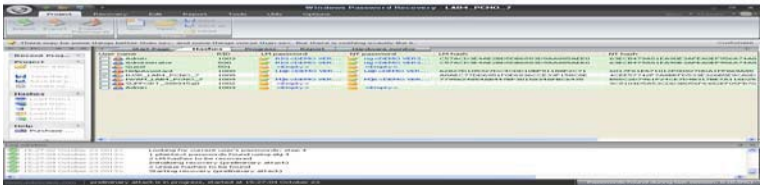

Figure 3.4 Window Password Recovery Tool

Figure 3.5 Window Password Recovery Tool Progress

Figure 3.6 Window Password Recovery Tool CPU & Memory Usage History

Figure 3.7 Window Password Recovery Tool Hash Generator

Figure 3.8 Rainbow Table Generator

Figure 3.9 Rainbow Table Generator Process

Figure 5.10 Rainbow Crack Calculator

IV. RESULTS AND DISCUSSIONS

This work presents the using various software tools for rainbow table. Based on the experimental results it is found that this software tools are not that much good, it covers only less area. Rainbow table is very large so it is very hard to calculate this table because it is a time consuming process. We followed various software's like Ophcrack software tool, RainCal software tool, Rainbowcrack-1.5 and Windows Password Recovery software Tools but did not get any efficient result for this rainbow table because rainbow table works in the form of exponential series because of that this process take more time so some times provide expected result and some time provide unexpected result. We spend lots of time behind this process but did not reach any expected output. We will apply more efficient software and will try to get efficient output

V. FUTURE SCOPE

The Topic Recover Various Password hashes By Using Cryptanalysis Technique with the help of Software Tool is basically based on the cryptanalysis technique and recovery password software performance but future of this topic I will handle all technique like brute force, dictionary attack etc. and also provide the better result of this topic and introduce the new concept of this topic.

REFERENCES

[1] M.E. Hellman, "A Cryptanalytic Time - Memory Trade-Off," IEEE Transactions on Information Theory, vol. 26, pp. 401-406, July 1980.

[2] Harshali Zodpe, Prakash Wani , Rakesh Mehta, *"HARDWARE IMPLEMENTATION OF ALGORITHM FOR CRYPTANALYSIS",* International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013.

[3] Fauzan Mirza ," *Block Ciphers And Cryptanalysis*", Department of Mathematics Royal HollowayUniversity of London.

[4] Michael E. Steurer *," Cryptanalysis of the Hash Function Tiger",* September 6, 2007.

[5] Celine Blondeau and Benot Gerard, "Multiple Dierential Cryptanalysis: Theory and Practice", SECRET Project-Team - INRIA Paris-Rocquencourt Domaine de Voluceau - B.P. 105 - 78153 Le Chesnay Cedex – France.

[6] Amrapali Dhavare, Richard M. Low, Mark Stamp, *"Efficient Cryptanalysis of Homophonic Substitution Ciphers"*.

[7] Paul C. van Oorschot and Michael J. Wiener*," Parallel Collision Search with Cryptanalytic Applications"*, Nortel, P.O. Box 3511 Station C, Ottawa, Ontario, K1Y 4H7, Canada 1996 September 23.

[8] Jennifer Kay," *Cryptanalysis Techniques: An Example Using Kerberos"*, September 1995 School of Computer Science Carnegie Mellon University Pittsburgh, Pennsylvania 15213-3890.

[9] John Kelsey and Bruce Schneier*," MARS Attacks! Preliminary Cryptanalysis of Reduced-Round MARS Variants "*, Counterpane Internet Security, Inc., 3031 Tisch Way, San Jose, CA 95128.

[10] H. Feistel, "Cryptography and computer privacy," Sci. Amer., vol.228, pp. 15-23, May 1973.

[11] Kevin Beaver (January 12, 2010). Hacking For Dummies. ISBN 978-0-7645-5784-2.

[12] Montoro, Massimiliano (2009). "Brute-Force Password Cracker". Oxid.it. Retrieved 13 August 2013.

[13] "Electronic Authentication Guideline". NIST. Retrieved March 27, 2008.

[14] Lakshmi M. and Sankaranarayanan P.E., "Performance analysis of three routing protocols in wireless ad hoc networks", Information technology Journal 5 (1): 114-120, © 2006 Asian Network for Scientific Information.

[15] Sundaram Rajagopalan and Chein-Chung Shen, "What does Using TCP as an Evaluation Tool Reveal about MANET Routing Protocols?", IWCMC'06 © 2006 ACM Journal.