

TECHNOLOGY'S WEAKNESS

Jared R. Greene, CISSP, CCNP, CCDP

From this assessor's perspective, one of the biggest hurdles that security professionals face is customer awareness and education as it relates to new technologies for hacking and network penetration. Many times, the customer's self assessment process lacks the scope and breadth to be effective against threats posed by current technologies. The compromise of even the lowest-level user's credentials can be the breaking point for the entire network's security infrastructure. The use of more advanced technologies for assessments is predicated by the proliferation of tools like Rainbow Tables. Although Rainbow Tables are not a new technology, their use and availability are increasing at an exponential rate. These inexpensive (sometimes free) tools are gaining use and acceptance in the hacking arena and their use can have staggering results.

Of significant importance to password complexity assessment is the use of Cryptanalysis Attacks. A cryptanalysis attack is the testing of a specific encrypted hash against every possible combination of character set. The difference between a Brute Force attack and Cryptanalysis attack is that all of the possibilities for decryption are already generated and the desired encrypted hash is simply cross-referenced from an index and identified in a matter of minutes. At their inception, the decryption of an LM (LAN Manager networking standard) or NTLM (Microsoft NT implementation of LM standard) password hash would have taken months or even years to accomplish. With tools available on the Internet today, passwords of significant complexity (even in excess of 14 characters) can now be cracked by the thousands in less than half an hour. Almost anyone, even those with limited computing knowledge, can harvest and decrypt all of the passwords on a network in a matter of minutes with the use of these tools. The widespread proliferation and availability of Rainbow Tables across the Internet poses a real threat to network security integrity.

This simple password cracking matrix can be used to gauge the effectiveness of passwords under the current technologies for password assessments. This matrix will allow you to judge how quickly a hacker or assessor can break your password with the current cracking methodologies. We will compare several different password configurations in this exercise based on the following parameters:

- LM and NTLM Passwords with all numbers
- LM and NTLM Passwords with all letters (Lowercase)
- LM and NTLM Passwords with all letters (Uppercase)
- LM and NTLM Passwords with letters and numbers (Mixed case)
- LM and NTLM Passwords with letters, numbers and 14 symbols (Mixed case)

Note: Passwords with less than 6 characters are not considered in this analysis because there is no need to discuss a password of that simplicity. Even the most complex passwords containing only 5 characters can be brute forced in less than 2 hours and are not worthy of analysis.

Note: The time necessary to perform and successfully complete a dictionary attack is directly proportional to the computer's ability to read and compare dictionary files against the hashes and the size and length of the dictionary files used in the attack. The computer utilized was an HPnx9500 with dual P4 processors with 1GB of ram operating Cain 2.5 on a Windows 2000 SP4. Your time and results may vary, but as a rule of thumb, it's about 1.5 hrs per gig of dictionary files.

Brute forcing: LAN Man hashes	Brute force	Rainbow Tables
6 digit pass with all numbers	1 second	28 minutes
6 digit pass with all letters (Lower or upper)	4 minutes	28 minutes
6 digit pass with letters and numbers (Mixed case)	10 hours	28 minutes
6 digit pass with Mixed Alpha and 14 symbols	1.54 days	28 minutes
7 digit pass with all numbers	9 seconds	28 minutes
7 digit pass with all letters (Lowercase)	1.5 minutes	28 minutes
7 digit pass with letters and numbers (Mixed case)	27.4 days	28 minutes
7 digit pass with Mixed Alpha and 14 symbols	113 days	28 minutes

8 digit pass password with all numbers	1.2 minutes	28 minutes
8 digit pass with all letters (Lowercase)	1.6 days	28 minutes
8 digit pass with letters and numbers (Mixed case)	4.6 years	28 minutes
8 digit pass with Mixed Alpha and 14 symbols	23.5 years	28 minutes
9 digit pass with all numbers	11 minutes	28 minutes
9 digit pass with all letters (Lowercase)	57 minutes	28 minutes
9 digit pass with letters and numbers (Mixed case)	378 years	28 minutes
9 digit pass with Mixed Alpha and 14 symbols	2370 years	28 minutes
10 digit pass with all numbers	2.6 Hours	28 minutes
10 digit pass with all letters (Lowercase)	4.8 years	28 minutes
10 digit pass with letters and numbers (Mixed)	23481 years	28 minutes
10 digit pass with letters and numbers (Mixed)	182000 years	28 minutes
11 digit pass Mixed Alpha and 14 symbols	1.724533e+007 years	28 minutes
12 digit pass Mixed Alpha and 14 symbols	1.01826e+009 years	28 minutes
13 digit pass Mixed Alpha and 14 symbols	8.07159e+010 years	28 minutes
14 digit pass Mixed Alpha and 14 symbols	6.09418e+012 years	28 minutes

As you can see, technologies for cracking passwords have significantly surpassed the encryption methods available for protecting them. Even a "significantly" complex password of greater than 14 characters containing numbers, letters, symbols and spaces can be decrypted with 99.77% accuracy in just a matter of minutes.

As we strive to educate our customers on how to secure their "last line of defense", we must first become educated ourselves. As new technologies become available in the art of hacking and penetration testing, our policy recommendations for password complexity must change at a rate that meets or exceeds current technologies. The role of a security assessor or auditor is to identify risks and vulnerabilities and, then, to provide guidance on strategies for their mitigation.

Jared R. Greene is a Senior Systems Engineer for The Saturn Partners, Inc. with over a dozen years of network security experience in testing, analysis and business continuity planning. He can be emailed at jared.greene@saturnpartners.com