5.7 Cracking Passwords

Cracking passwords is not the same as breaking encrypted transmissions. If anyone has successfully cracked a password and particularly the administrator/root password, then any additional security measures are rendered irrelevant.

5.7.1 John the Ripper

John the Ripper is a password cracker which is very popular with both network administrators and hackers.

This product is completely command line–based and has no Windows interface. It enables the user to select text files for word lists to attempt cracking a password. Although John the Ripper is less convenient to use because of its command-line interface, it has been around for a long time and is well respected by both the security and hacking communities.

John the Ripper works with password files rather than attempting to crack live passwords on a given system. Passwords are usually encrypted within a file on the operating system. Hackers frequently try to get that file off the machine and download it to their own system so they can crack it at will. They might also look for discarded media in your dumpster in order to find old backup tapes that might contain password files. Each operating system stores that file in a different place:

- In Linux, it is /etc/passwd and /etc/shadow.
- In Windows 2000 and beyond, it is in a hidden .sam file.

After you have downloaded John the Ripper, you can run it by typing in (at a command line) the word john followed by the file you want it to try to crack:

- john passwd
- john –wordfile:/usr/share/wordlists/rockyou.txt –rules passwd
  Cracked passwords will be printed to the terminal and saved in a file called john.pot, found in the directory into which you installed John the Ripper.

5.7.2 Rainbow Tables

In 1980 Martin Hellman described a cryptanalytic time-memory trade-off that reduces the time of cryptanalysis by using pre-calculated data stored in memory. Essentially, these types of password crackers work with pre-calculated hashes of all passwords available, within a certain character space such as “**a-z”** or “**a-zA-z”** or “**a-zA-Z0-9”** etc. These files are called rainbow tables. They are particularly useful when trying to crack hashes. Due to the fact that a hash is a one-way function, the way to break it is to attempt to find a match. The attacker takes the hashed value and searches the rainbow tables seeking a match to the hash. If one is found, then the original text for the hash is found. Popular hacking tools such as Ophcrack depend on rainbow tables.

5.7.3 Brute Force

This method simply involves trying every possible key. It is guaranteed to work, but very likely to take so long that it is simply unusable. For example, to break a Caesar cipher there are only 26 possible keys, which you can try in a very short time. But consider AES, with the smallest key size of 128 bits. If you tried 1 trillion keys a second, it could take 112,527,237,738,405,576,542 years to try them all.