8.1.2 Introduction to Hacking Facts

One of easiest ways a hacker gains access to a system or network is through passwords. Creating strong passwords and protecting them seems easy enough, but cracking and stealing passwords often leads to success for hackers. One of the main reasons is lack of education. The two simplest and most important safeguards are to teach employees to create strong passwords and to help them understand the importance of secrecy.

This lesson covers the following topics:

- Non-technical password attacks
- Technical password attacks
- RainbowCrack
- Password cracking countermeasures

Non-Technical Password Attacks

The following table describes three non-technical ways a hacker can gain access to passwords.

Attack	Description
Dumpster diving	This non-technical method of attack relies on finding sensitive information that has been discarded in garbage cans, dumpsters, or other unsecure places that a hacker has access to.
Social engineering	The social engineering attack relies on human error. The hacker convinces an employee or other authorized person to give him a password.
Shoulder surfing	This technique involves watching and recording a password, pin, or access code that is being entered by someone in close proximity.

Technical Password Attacks

It's natural for people to want easy-to-remember passwords or to use the same password for multiple systems and websites. A surprising number of people use the password abc123, a pet's name, or a hobby as a password. The weakness in this convenience is that these are all easy for an hacker to guess. The following tables describes common types of technical password attacks.

Attack	Description
Dictionary	In a dictionary attack, word lists, often taken straight from dictionaries, are tested against password databases. Besides all the standard words you find in a dictionary, these lists usually include variations on words that are common for passwords, such as pa$$word. Lists can also include simple keyboard finger rolls like q-w-e-r-t1234. The down side to this attack is this process can take a very long time to crack the passwords. Two common tools for dictionary attacks are Brutus and Hydra.
Brute force	In a brute force attack, every password will eventually be found because its technique is to test every possible keystroke for each single key in a password until the correct one is found. The disadvantages of this type of attack are that it takes a large amount of processing power to execute and it is very time consuming.
Pass the hash	Pass the hash is a hacking technique where an hacker uses an underlying NTML or hash of a user's password to gain access to a server without ever using the actual plain text password. Pass the hash is dangerous to an organization because once a hacker gains access, the entire organization can be compromised very quickly. To execute a pass the hash attack, first, a hacker gains access to an individual computer through malware or another technique. Then the hacker can access the system's memory and find stored hashes from other users that have used that workstation. The hacker can then gain access to other workstations in the network and search each workstation for stored hashes until it finds a hash that gives access to a high-level administrator account. Once that happens, the hacker has access to the entire network as an administrator.
Sniffing	Sniffing is a passive way for a hacker to gain access to an account. The sniffer collects data that is in transit in a LAN. If access is gained on one system in a LAN, then more data can be gathered from data transmissions to any other system in the network. The sniffer runs in the background, making it undetectable to the victim. Sniffing tools include Wireshark, TCPDump, and Recon-ng.
Keylogger	Keystrokes on the computer keyboard are logged or recorded to obtain passwords and other important data. This can be done through either hardware devices or software programs on an individual computer or on a whole network. The user cannot detect the keylogger software, and the information can be recorded before it is encrypted. ▪ A hardware keylogger is a physical device that looks like a regular USB drive. It is installed between a keyboard plug and a USB port. Every stroke of the keyboard is stored on the device, and a hacker has to retrieve it to get the data that is stored. The advantage of this type of keylogger is that it is undetectable by desktop security, as well as antispyware and antivirus programs. The disadvantage is that it is easy to find it because it is physically plugged into the computer. Tools include PC Activity Monitor, RemoteSpy, Veriato, Investigator, and KeyStrokeSpy.

	▪ Software keyloggers are installed through an opened email attachment or remotely through a network. An advantage of this type of keylogger is that it has no memory limitations because the data is stored on a remote computer hard drive.
Rainbow	Rainbow attacks are like dictionary attacks, but instead of endlessly testing dictionary lists, this method uses tables that are precomputed with word lists and their hashes. This is much quicker than a dictionary attack or a brute force attack. When a plain text password is stored, it is processed through a one-way function and converted into a hash. Hashes are then converted into plain text through another one-way function called reduction. This new plain text is not the same plain text that was originally hashed. Passwords often go through this encryption process multiple times, making a chain. Rainbow tables store only the starting plain text and the final hash of these chains. A hacker searches the table for a possible hash and tries to retrieve the password that it was converted from. The rainbow table gets its name from having a different reduction function in each column in the chain. This allows the hacker to quickly crack the password by passing through tables which will work backwards through the chain to identify the original password.

RainbowCrack

RainbowCrack is software that cracks hashes by rainbow table lookup. The rtgen program generates rainbow tables, and the rtsort program sorts them. The following table describes these two programs.

Program	Description
rtgen	rtgen generates rainbow tables based on parameters specified by user. The command line syntax of rtgen program is: **rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index** An example of commands used to generate a rainbow table set with 6 rainbow tables is: rtgen md5 loweralpha-numeric 1 7 0 3800 33554432 0 rtgen md5 loweralpha-numeric 1 7 1 3800 33554432 0 rtgen md5 loweralpha-numeric 1 7 2 3800 33554432 0 rtgen md5 loweralpha-numeric 1 7 3 3800 33554432 0 rtgen md5 loweralpha-numeric 1 7 4 3800 33554432 0 rtgen md5 loweralpha-numeric 1 7 5 3800 33554432 0
rtsort	A rainbow table is an array of rainbow chains. Each rainbow chain has a start point and an end point. The rtsort program sorts the rainbow chains by end point to make a binary search possible. Use the **rtsort .** command to sort all .rt rainbow tables in current directory. Please be aware that after **rtsort**, the command includes a space and then a period.

Program options for rtgen are described in the following table.

Option	Description
hash_algorithm	A rainbow table is hash algorithm specific. A rainbow table for a certain hash algorithm helps to crack only hashes of that type. The rtgen program natively support lots of hash algorithms, like lm, ntlm, md5, sha1, mysqlsha1, halflmchall, ntlmchall, oracle-SYSTEM, and md5-half. In the example above, we generated md5 rainbow tables that speed up the cracking of md5 hashes.
charset	The charset includes all possible characters for the plain text. Loweralpha-numeric is represented by abcdefghijklmnopqrstuvwxyz0123456789, which is defined in configuration file charset.txt.
plaintext_len_min plaintext_len_max	These two parameters limit the plain text length range of the rainbow table. In the example above, the plain text length range is 1 to 7. So plain texts such as abcdefg are likely contained in the rainbow table generated. But plain text abcdefgh with length 8 will not be contained.
table_index	The table_index parameter selects the reduction function. Rainbow tables with a different table_index parameter use different reduction functions.
chain_len	The rainbow chain length. A longer rainbow chain stores more plain texts and requires longer time to generate.
chain_num	The number of rainbow chains to generate. A rainbow table is simply an array of rainbow chains. The size of each rainbow chain is 16 bytes.
part_index	To store a large rainbow table in many smaller files, use a different number for each part, and keep all other parameters identical.

The following table shows the hash types and their possible characters or values.

Hash Type	Possible Values
numeric	[0123456789]
alpha	[ABCDEFGHIJKLMNOPQRSTUVWXYZ]
alpha-numeric	[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
lower alpha	[abcdefghijklmnopqrstuvwxyz]
lower alpha-numeric	[abcdefghijklmnopqrstuvwxyz0123456789]
mix alpha	[abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]
mix alpha-numeric	[abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
ascii-32-95	[!"#$%&'()*+,-./0123456789:;<=>? @ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~]
ascii-32-65-123-4	[!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`{|}~]
alpha-numeric-symbol32-space	[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]

Password Cracking Countermeasures

There are several things you can do to counter password cracking attempts:

- Password salting is a strategy used to make cracking passwords more difficult by adding random bits of data to a password before it is stored as a hash. This is made possible by a one-way function that makes it almost impossible to return the hashed password back to the original password.
- The more complex a password, the harder it is to crack. Use 8 to 12 characters combining numbers, uppercase and lowercase letters, and special symbols.
- Never share your passwords.
- If asked to routinely change your password, do not reuse your current password.
- Never use words from a dictionary as your password.
- Change your passwords every 30 days.
- Never store a password in an unsecure location.
- Never use a default password.
- Never store passwords in a protocol with weak encryption or clear text.
