

UNidad 5

Activity – identify hashing terminology

The screenshot shows a web browser window displaying the Cisco Cybersecurity Essentials interface. The browser's address bar shows the URL: `static-course-assets.s3.amazonaws.com/CyberEss1.1/en/index.html#5.1.1.9`. The page title is "Cybersecurity Essentials".

The main content area is titled "Activity - Identify Hashing Terminology". It features a navigation pane on the left with the following structure:

- Chapter 5: The Art of Ensuring Integrity
 - 5.1 Types of Data Integrity Controls
 - 5.1.1 Hashing Algorithms
 - Activity - Identify Hashing Terminology (selected)

The activity instructions state: "Match each term to its description. Not all terms are used." Below the instructions is a "two-way" button. At the bottom of the instruction box are "Check" and "Reset" buttons.

The main area contains a table with two columns: "Term" and "Description". Each row has a green checkmark in the "Term" column, indicating a correct match.

Term	Description
input	The _____ for a hash can be any length.
output	The _____ for a hash has a fixed length.
one-way	The hash function is _____ and is not reversible.
MD5	The _____ algorithm produces a 128-bit hash value.
SHA	The _____ algorithm can produce up to a 512-bit hash value.
fixity	The fact that one set of bits is identical to the original set of bits establishes _____.
dictionary	A _____ attack uses a file containing common words, phrases, and passwords.
brute-force	A _____ attack attempts every possible combination of characters up to a given length.

At the bottom of the interface is a navigation bar with icons for "Search Pages", "Bookmarks", "Course Index", "Search", "Select Background", and "Help".