

Real-World Scenario 6-3: Defending Against the Web Shell

Scenario: One of your associate's websites was hacked into. The associate contacted you to see if you knew anything about a "web shell." The person had found that name within the syntax of one of the "new" files on his web server. Your task is to explain to your associate what is going on, and recommend a solution.

What is the web shell?

How did it get there?

What should your recommendations be?

Real-World Scenario 6-3 Solution

Web shells are programs (known under several permutations: C99, C Shell, Web Shell, Web Shell by Orb, and others) that are installed on the web server by an attacker and are used to remotely access and reconfigure the server without the owner's consent. They are remote access Trojans but are also referred to as backdoors because they offer an alternative way for attackers to access a website.

Most likely, the attacker stole the associate's FTP password. Once the attacker had the password, it was just a matter of uploading the shell. Then the attacker could log in through the new web shell and do just about anything he wanted to the web server. Many of these web shells allow the operator to access them through a proxy, thus hiding the location of the operator. Also, the shell can be bound to specific ports, and the information can be encrypted and hashed.

First, you should recommend increasing password security for all important FTP accounts. Make the passwords as complex as the web server will allow. Remove any unnecessary FTP accounts. Delete the original RAT files and run a full scan of the system, or at the least, restore data from an older backup. Have the associate verify the web host's scanning techniques, or scan web files manually.

Simulation: Complete the simulation "6-3: Defending Against the Web Shell."