



CTF Content

Huntress CTF 2025 - 🔍 Webshellz

4d 8h 42m remaining



Chapters



Systems



Progress



Help



Community



Scoreboard

> 🏠 Welcome to Huntress CTF

> ♦ Day 31 Challenges

> ♦ Day 30 Challenges

> ♦ Day 29 Challenges

> ♦ Day 28 Challenges

> ♦ Day 27 Challenges

> ♦ Day 26 Challenges

> ♦ Day 25 Challenges

> ♦ Day 24 Challenges

> ♦ Day 23 Challenges

▼ ♦ Day 22 Challenges

🔍 Webshellz ✓

⚙️ NimCrackMe1 ✓

🕒 More Challenges Tomorrow!

> ♦ Day 21 Challenges

> ♦ Day 20 Challenges

> ♦ Day 19 Challenges

> ♦ Day 18 Challenges

> ♦ Day 17 Challenges

> ♦ Day 16 Challenges

> ♦ Day 15 Challenges

> ♦ Day 14 Challenges

> ♦ Day 13 Challenges

> ♦ Day 12 Challenges

> ♦ Day 11 Challenges

> ♦ Day 10 Challenges

> ♦ Day 09 Challenges

> ♦ Day 08 Challenges

> ♦ Day 07 Challenges

> ♦ Day 06 Challenges

> ♦ Day 05 Challenges

> ♦ Day 04 Challenges

> ♦ Day 03 Challenges

> ♦ Day 02 Challenges

> ♦ Day 01 Challenges



Webshellz

Category

Author



Forensics

Ben Folland

Challenge Prompt

The sysadmin reported that some unexpected files were being uploaded to the file system of their IIS servers.

As a security analyst, you have been tasked with reviewing the Sysmon, HTTP, and network traffic logs to help us identify the flags!

📘 NOTE

The password to the ZIP archive is `webshellz`



webshellz.zip
7.42 MB



Something funky is going on with a new account that was created. Can you find the flag? This flag ends with a `6`.

Submit the flag below:

3 points

✓ Correct

There seems to be some Funky Random Program! This flag ends with a `d`.

Submit the flag below:

3 points

✓ Correct

How did the threat actor attempt to gain access to the webshell? This flag ends with a `e`.

Submit the flag below:

4 points

✓ Correct

← 🕒 More Challenges Tomorrow!

Continue