CTF Content

Huntress CTF 2025 - 🔍 Webshellz

4d 8h 42m remaining

☀ ☾ 🖵 ✕

Chapters

Systems

Progress

Help

Community

Scoreboard

🔍 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

    flag{03638631595684f0c8c461c24b0879e6}

✓ Correct

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

Submit the flag below: 3 points

    flag{c7ba76c0a4484fe8c135a1195e8d94ed}

✓ 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

    flag{fb4e078a739ac4ce687eb78c2e51aafe}

✓ Correct

← ⏰ More Challenges Tomorrow!   Continue