

CTF Write-up — Icebound Evidence

Category: Forensics

Points: 50

Author: p3f0rm3r ({x0x} Team)

Description

The challenge asks for the malware framework used in the 2015 cyberattack on Ukraine's power grid.

Solution

I searched online for information about the 2015 Ukraine power grid attack and found that the malware framework used was BlackEnergy.

Flag

atcctf_BlackEnergy

Conclusion

This challenge tests knowledge of major historical cyberattacks and malware used against critical infrastructure.