CTF Solvings for OSCP Aspirants

SATHIYANARAYANA S

Product Security Specialist

CTF Challenges

CTFs are gamified security challenges where cybersecurity exercises designed to test participants' skills in areas like

- Web Exploitation
- Network Exploitation
- Binary Exploitation
- Reverse Engineering
- Cryptography
- Forensics
- Steganography

RED TEAM
Examinations

Red Teaming exams validate your ability to simulate real-world cyberattacks. These exams are hands-on and practical, often involving lab environments where you have to exploit low level to high level security mechanisms. They assess your skills in areas like vulnerability exploitation, privilege escalation, and lateral movement within a network.

Benefits of Red Teaming Knowledge

Red teaming knowledge offers several benefits:

- ***Enhanced Security:*** Identifying and addressing vulnerabilities strengthens defenses.
- ***Real-world Simulation:*** Practical experience in simulating cyberattacks mirrors actual threats.
- ***Comprehensive Assessment:*** Thorough evaluations provide insights into security postures.
- ***Proactive Defense:*** Anticipatory measures safeguard against potential breaches.
- ***Skill Development:*** Proficiency in offensive techniques sharpens cybersecurity capabilities.

Common **Red Teaming** Tools & Scripts

Command and Control

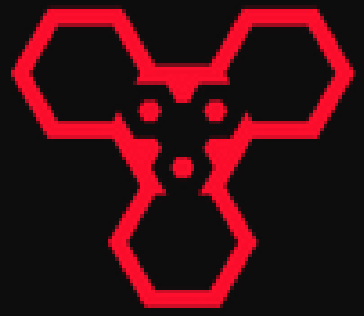
- Cobalt Strike
- Covenant
- SharpC2

Extracting Credentials

- Mimikatz

Obfuscations

- Alcatraz GUI x64 Binary



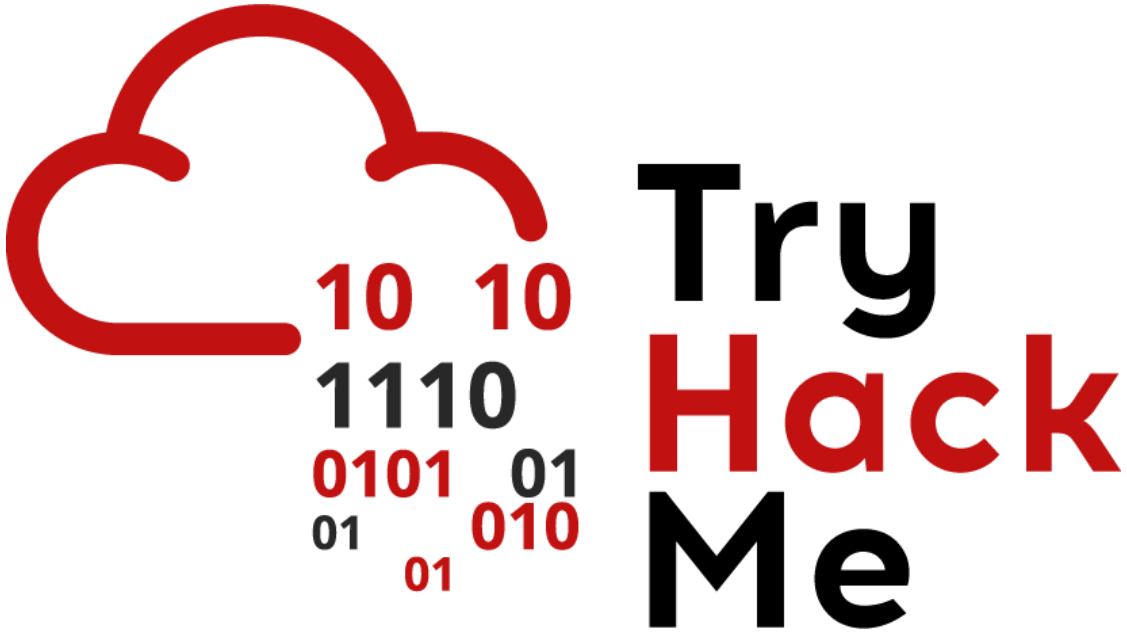
AD Domain Enumeration

- BloodHound

Privilege Escalations

- Win / Lin PEAS
- SweetPotato

Famous CTF Platforms



ANY
questions?