Pwn2Own-CTF

Intentionally Vulnerable Machine

"Capturing the flag by breaking the security"

TEAM MEMBERS

- **Durgesh Sahu**

Bio

Durgesh Sahu

Class - CSE - 6th

Roll no. 301202220065

What ?

What this project is about

Why ?

Vision of this project

How ?

Approach to solve machine

Key Takeaway

What you will have at the end

What is Pwn2Own-CTF ?

- An Operating System designed vulnerable intentionally
- Made vulnerable to practice security, break security
- Contain all phases of ethical hacking
- Project is based on CTF concept where user have to understand the problem/challenge that could be from different domain of Cybersecurity.

CTF ?

- In computer era Capture the flag (CTF) is a type of game that involves solving challenges related to computer security.
- These challenges can be related to different areas of computer security, such as cryptography, web security, and network security.
- The goal of a CTF competition is to find and capture a "flag," which is typically a piece of hidden information or a file.
- Types - Attack Defense, Jeopardy, Boot2Root
- Our project follow the Boot2Root

Boot2Root ?

BOOT2ROOT CTF -

After solving the each challenge user will get flag or hint to solve further challenge thus solving all level of challenge and collecting the flag and reaching to next level eventually user has to get the root flag

Why Pwn2Own-CTF ?

- The aim of this project is to introduce and educate the students to various phases of CyberSecurity in practical way with hands-on experience
- Security is vast field, this project try to let student taste various field of cybersecurity
- The gamification of cybersecurity training eases the learning process
- Out-of-the-box thinking and creative solutions increasing learning for the individual
- get your hands dirty in a safe environment and learn from failure
- It's fun!

Methodology to follow

1. Reconnaissance
2. Scanning/Enumeration
3. Gaining access
4. Privilege escalation
5. Maintaining access
6. Covering tracks/Placing backdoors

What you will learn?

1. Network security
2. Steganography,Forensic
3. Web app security
4. Cryptography
5. Reverse engineering
6. Software/Sys security
7. Google fu :D

Thanks! :)

Project/Machine : https://github.com/Durge5h/College-Project

Write-up : https://0xsegf4ult.github.io/