Simple Setup for CTFs

and THM/HTB too

whoami

Izdihar Sulaiman

Husband, Father, Avid CTF Player

Principal Consultant @ Swarmnetics 💂



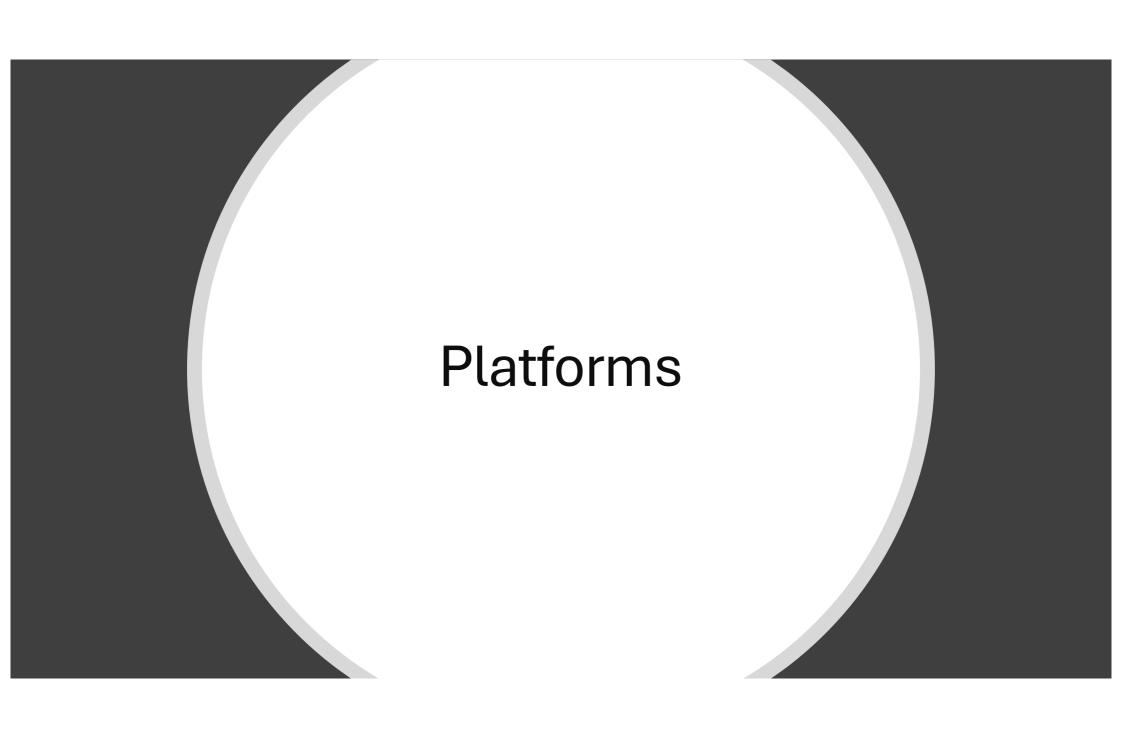
Placed (1/2/3) at CyberBattle CTF 8 out of 9 times 🥯



CVE-2022-40317

CISSP, GXPN, OSEP, OSWE, OSCP, OSWA, OSWP, CRT, CPSA, BSCP, eMAPT, ...

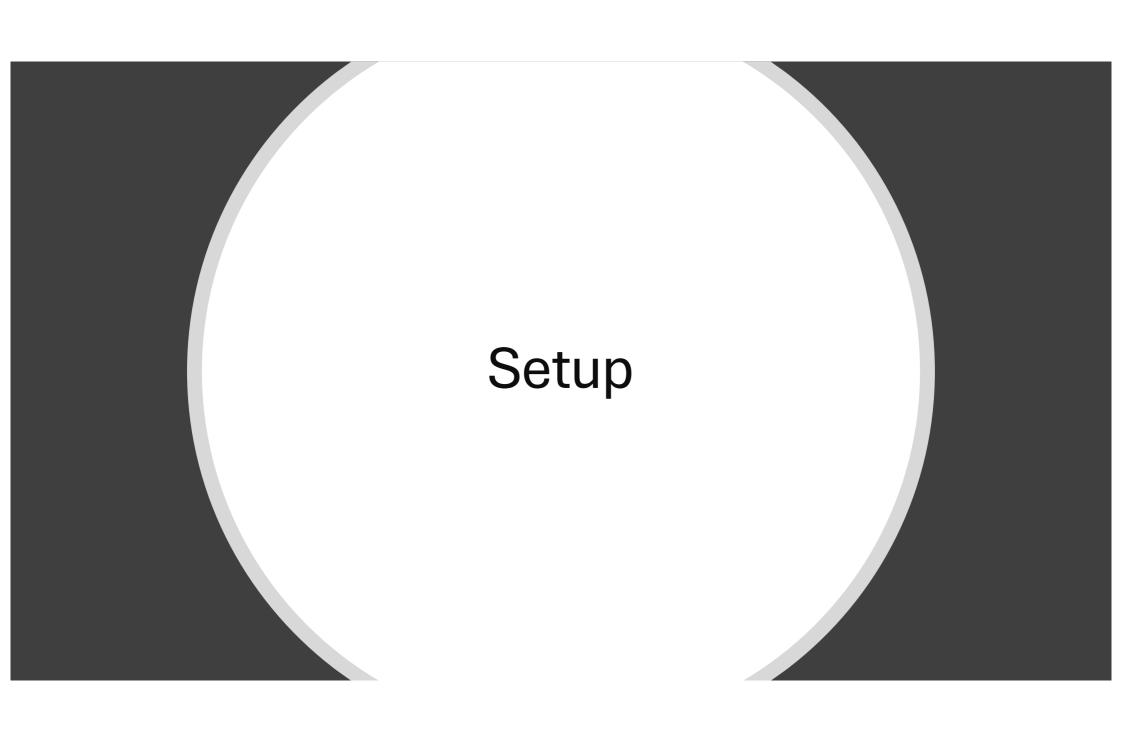
Contact Information => https://izdiwho.com



Capture The Flag

TryHackMe

HackTheBox



Virtual Machine or WSL or Containers

- Hypervisors (VMWare / Parallels / VirtualBox)
 - Kali Linux VM
 - ParrotOS VM
- Windows Subsystem for Linux 2 (Windows)
 - Kali WSL2
- Docker Desktop
 - Kali container
- Orbstack (MacOS)
 - Kali machines



Web Security

Burp Suite (Community Edition) - Web proxy and security testing Developer Tools in Browsers OWASP ZAP (alternative to Burp)

Packet Analysis

- Wireshark Network protocol analyzer
- Tcpdump Command-line packet analyzer

Cryptography

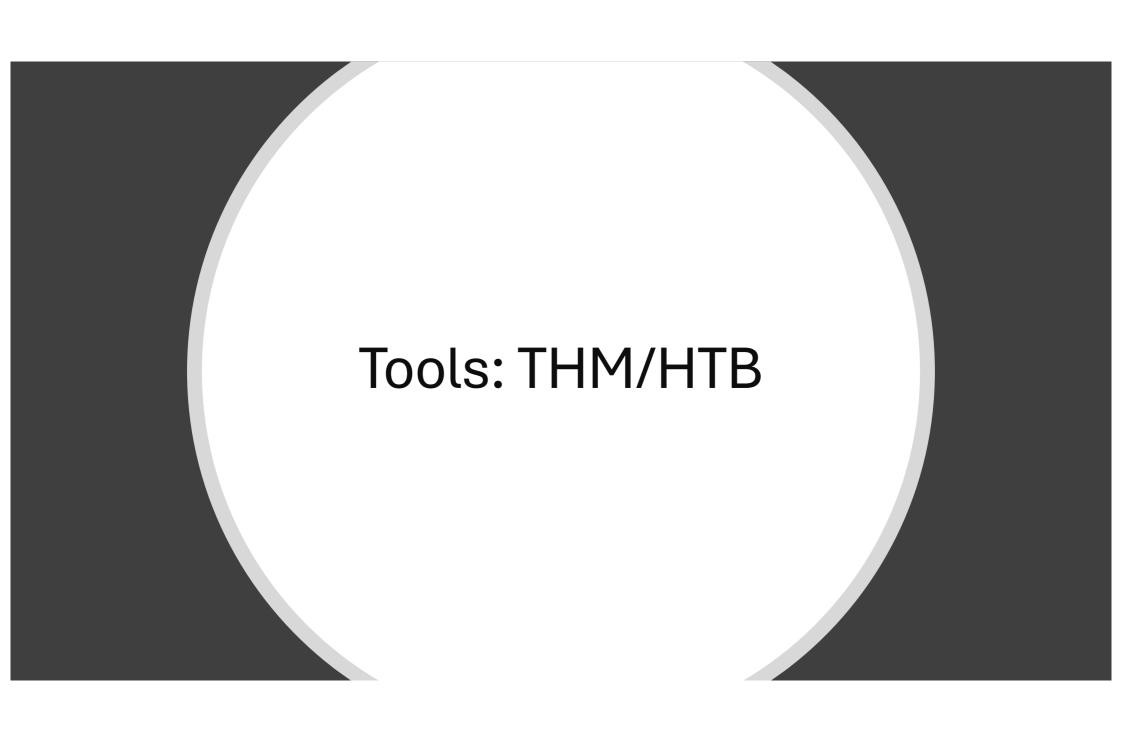
- CyberChef Swiss army knife for encoding/decoding/analysis
- RsaCtfTool RSA cracking tool

Binary Exploitation/Reverse Engineering

- GDB (GNU Debugger) with GEF or PEDA extensions
- Ghidra Software reverse engineering tool
- Radare2 Reverse engineering framework
- IDA Free Disassembler

Digital Forensics

- Volatility Memory forensics
- FTK Imager Disk image creation and analysis
- Autopsy Digital forensics platform
- Exiftool Meta data analysis



Discovery/Recon

- Nmap Network scanning
- Gobuster/Dirbuster Directory enumeration

Bruteforcing

- John the Ripper Password cracking
- Hydra Login brute forcing

Exploitation

- Metasploit Framework Exploitation framework
- Searchsploit Searches ExploitDB for public exploits

Privilege Escalation

• LinPEAS/WinPEAS - Privilege escalation scanners

Others

- NetCat/SoCAT Networking utilities
- Python3 Scripting

