❑ About Me

- **Name:** Phuon, Seang Y

- **Title:**
  - @ THECyb0rg Lab – a vulnerability research lab
    - Founder
    - Ethical Hacker
    - Zer0-Day Hunter
  - Red Team Member @ Synack
  - Instructor @ Sunrise Institute, @ OneSala E-Learning Platform
  - Formerly Manager, Cyber Risk @ Deloitte

- **Certifications:**
  - Certified Ethical Hacker [C|EH – Practical]
  - OffSec Certified Professional [OSCP]
  - Certified Red Team Operator [CRTO]
  - Certified Red Team Expert [CRTE]
  - Bachelor Degree of Computer Science and Engineering [CSE] – RUPP

❑ Agenda

- Introduction to Cybersecurity

- Offensive & Defensive Security

- Who is Ethical Hacker?

- Hacker's Mindset and Required Skills

- Capture the Flag (CTF)

- Career in Cybersecurity

- Cybersecurity Certifications

- Q&A

❑ Introduction to Cybersecurity

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability (CIA) of information. – CISA (.gov)

❑ Offensive and Defensive Security

- ▪ Offensive Security

  Adopt the <mark>attacker's mindset and simulate attacks</mark> against targeted environment.

❑ **Offensive and Defensive Security**

▪ **Defensive Security**

Protect the target environment from malicious attackers or cyber threats.

❑ Who is Ethical Hacker?

- Ethical Hacker

A cybersecurity professional who uses hacking skills to test the target environment's security with authorization and also known as white-hat hacker or penetration tester.

❑ Hacker's Mindset and Required Skills

▪ **Required Soft Skills**

- Curiosity

- Creativity

- Logical and analytical thinking skill

- Think outside the box

- Adaptability and willing to learn new things

- Persistence

❑ Hacker's Mindset and Required Skills

■ **Required Technical Skills and Knowledges**

- **Operating Systems** – Windows, Linux and other OSes.

- **Networking Skills** – TCP/IP, networking protocols (HTTP/HTTPS, DNS, SSH, FTP etc.)

- **[To up the game] – Programming Languages** – Python, Ruby, C/C++, ASM, web programming languages and technologies etc.

❑ Hacker's Mindset and Required Skills

▪ **Common Areas of Penetration Testing**

- Network Infrastructure (External and Internal Network)

- Web Application

- Application Programming Interface (API)

- Mobile Application

- Wireless Network and others
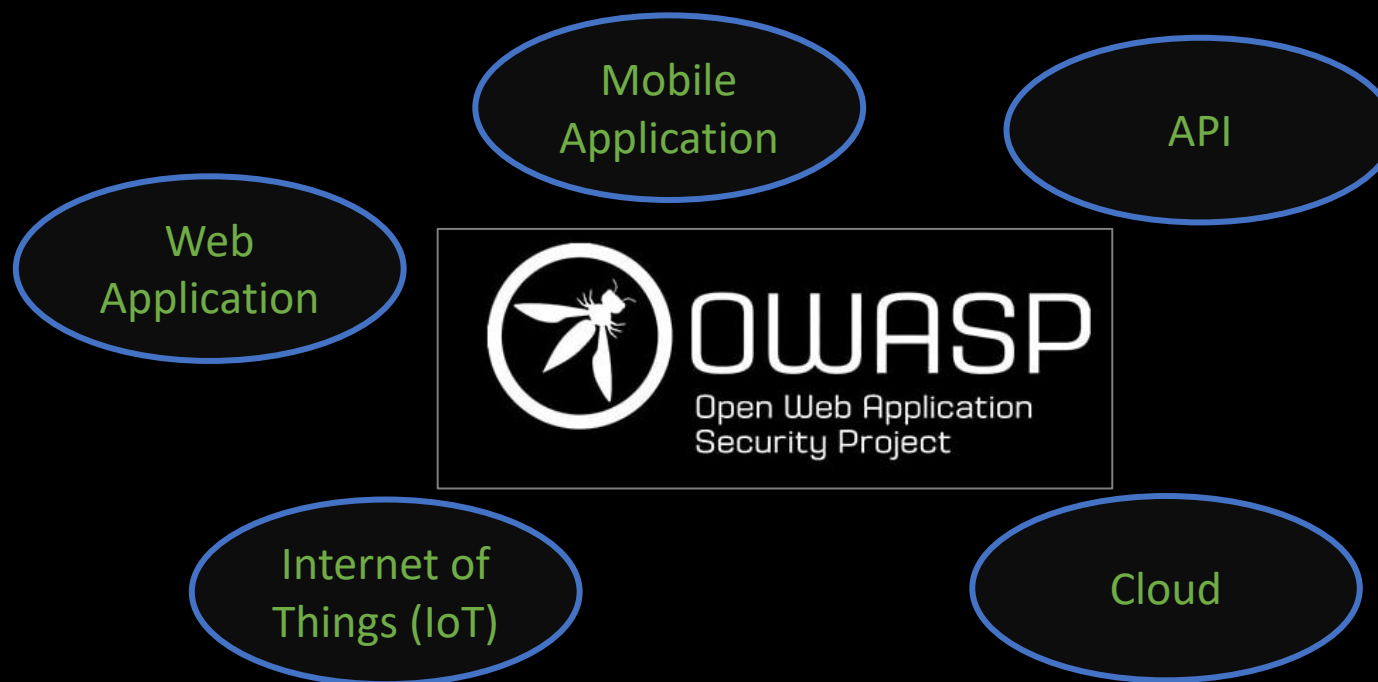
☐ **HACK YOURSELF FIRST !**

MINDSET

SKILLSET

THE CYBORG LAB

@July 2023

❑ Capture The Flag (CTF)

▪ Introduction to CTF

An exercise or competition to **find text strings (flags)** which

are secretly hidden.

❑ Capture The Flag (CTF)

- ■ Types of CTF Challenge

Jeopardy-style CTF:

To solve challenges in various categories including: web, network,

forensics/reverse engineering, PWN/binary challenge and misc.

❑ Capture The Flag (CTF)

■ **Types of CTF Challenge**

Attack/Defense-style CTF:

To **attack opponent's system while protecting yourself** from being

attacked.

❑ Capture The Flag (CTF)

▪ Online CTF Platforms

- TryHackMe

- HackTheBox

- VulnHub

- OverTheWire

- picoCTF

- Root-Me and others

❑ Career in Cybersecurity

- **Cybersecurity Career in Cambodia**
  - o Penetration Tester / Ethical Hacker
  - o Cybersecurity Consultant
  - o SOC Analyst
  - o IT Security Officer
  - o IT Auditor
  - o Incident Response and Digital Forensic Investigator
  - o More

❑ Cybersecurity Certifications

▪ Recognized Certificates in Penetration Testing

- CompTIA – Security+, Pentest+

- eLearnSecurity – eJPT, eCPPT

- EC-Council – CEH, CPENT, LPT

- Offensive Security (OffSec) – OSCP, OSWE, OSCE3 etc.

- Others: https://pauljerimy.com/security-certification-roadmap