INTRODUCTION TO:

Ethical Hacking

The art of legally breaking into computer system

By Mr. Seang Y PHUON
@ January 2025

About Me

- Name: Phuon, Seang Y [Codename: THECyb0rg]
- Titles:
  - Red Team Lead @ Veilron Technologies Pte. Ltd.
  - @ THECyb0rg Lab – a vulnerability research lab
    - Founder, Ethical Hacker, Zer0-Day Hunter
  - Red Team Member @ Synack
  - Yogosha Strike Force @ Yogosha
  - Instructor @ Sunrise Institute
  - Formerly a Cyber Risk Manager @ Deloitte
- Certifications:
  - Certified Ethical Hacker [C|EH – Practical]
  - OffSec Certified Professional [OSCP]
  - Certified Penetration Testing Professional [CPENT]
  - Certified Red Team Operator [CRTO]
  - Certified Red Team Expert [CRTE]
  - Certified Instructor for EC-Council and OffSec
  - Bachelor Degree of Computer Science and Engineering [CSE] – RUPP, Cambodia

Agenda

- Introduction to Cybersecurity
- Introduction to Ethical Hacking
- Hacker's Arsenal
- Hacker’s Playground
- Industry Certifications
- Q&A

INTRODUCTION TO:

Cybersecurity

By Mr. Seang Y PHUON
@ January 2025

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)

@https://www.cisa.gov/news-events/news/what-cybersecurity

Offensive Security

Adopt the attacker’s mindset and simulate attacks against targeted environment/organization.

Defensive Security

Protect the organization from malicious attackers or cyber threats.

@https://assets.bizclikmedia.net

By Mr. Seang Y PHUON
@ January 2025

INTRODUCTION TO:

Ethical Hacking

By Mr. Seang Y PHUON
@ January 2025

Introduction to Ethical Hacking

- Ethical Hacking is the practice of intentionally testing computer systems, networks, or applications to identify and remediate vulnerabilities before the malicious hackers do.
- Authorized permission and approval to assess the security of the target systems.

@https://www.comptia.org/content/articles/what-is-ethical-hacking

Vulnerability Assessment (VA)

The process of identifying vulnerabilities without exploitation attempt on the identified vulnerabilities. This includes manual and automated approaches.

Penetration Testing (PT)

The process of identifying vulnerabilities and exploit the vulnerabilities once identified.

By Mr. Seang Y PHUON
@ January 2025

Hacker's Mindset and Skillset

❑ Soft Skill:

- Curiosity
- Creativity
- Persistence
- Logical and analytical thinking skill
- Think outside the box
- Adaptability and willing to learn new things

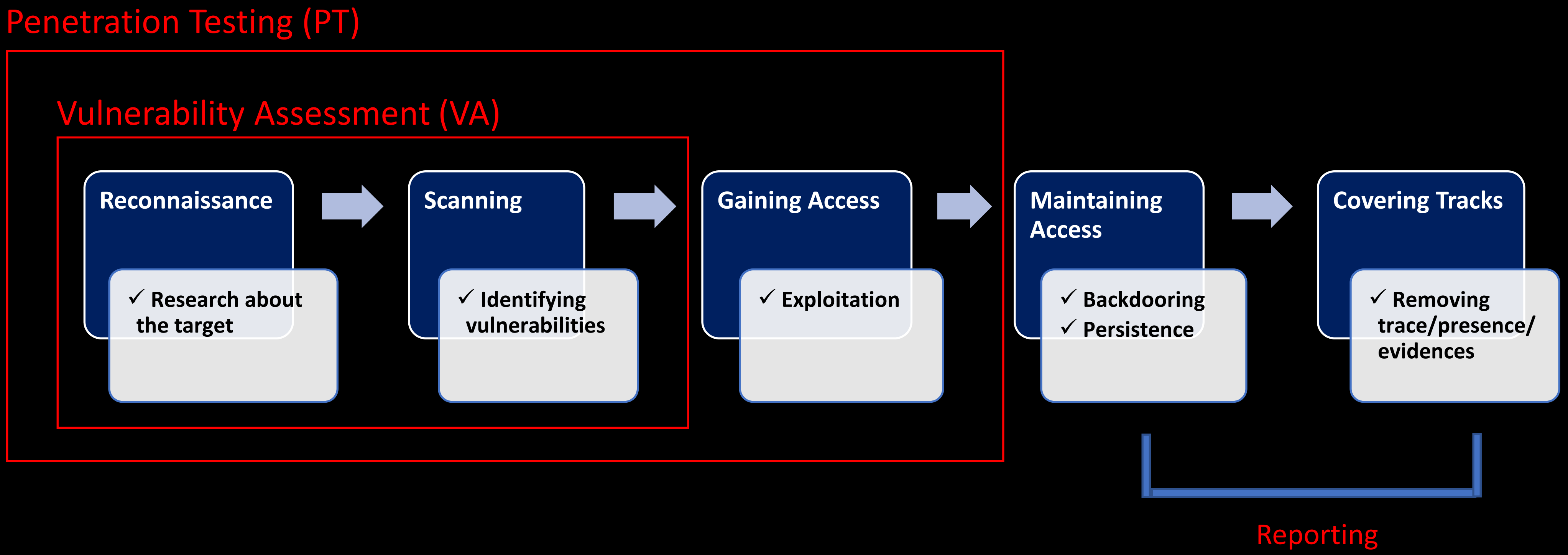
Hacker's Mindset and Skillset

❑ Technical Skill:

- 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.

Hacking Methodologies

The generic methodologies to ethical hacking:



Penetration Testing (PT)

Vulnerability Assessment (VA)

Reconnaissance
- ✓ Research about the target

Scanning
- ✓ Identifying vulnerabilities

Gaining Access
- ✓ Exploitation

Maintaining Access
- ✓ Backdooring
- ✓ Persistence

Covering Tracks
- ✓ Removing trace/presence/ evidences

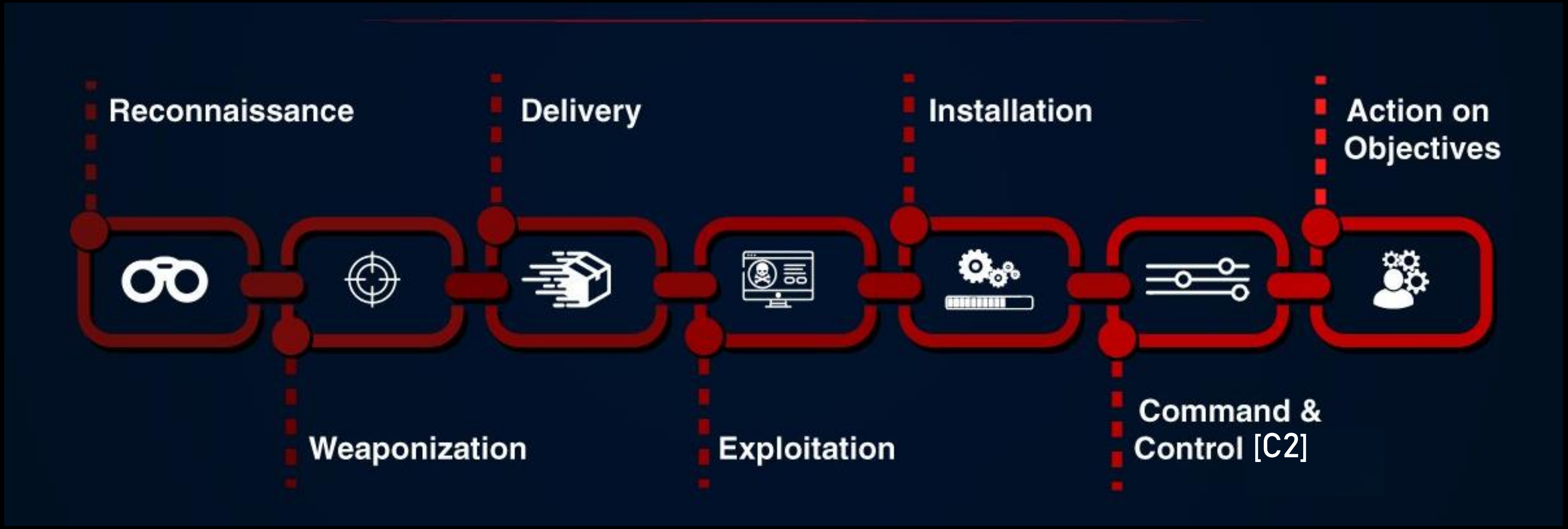
Reporting

@https://www.eccouncil.org/

By Mr. Seang Y PHUON
@ January 2025

Hacking Methodologies

Cyber Kill Chain – APT / Red Team Operations



@https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

By Mr. Seang Y PHUON
@ January 2025

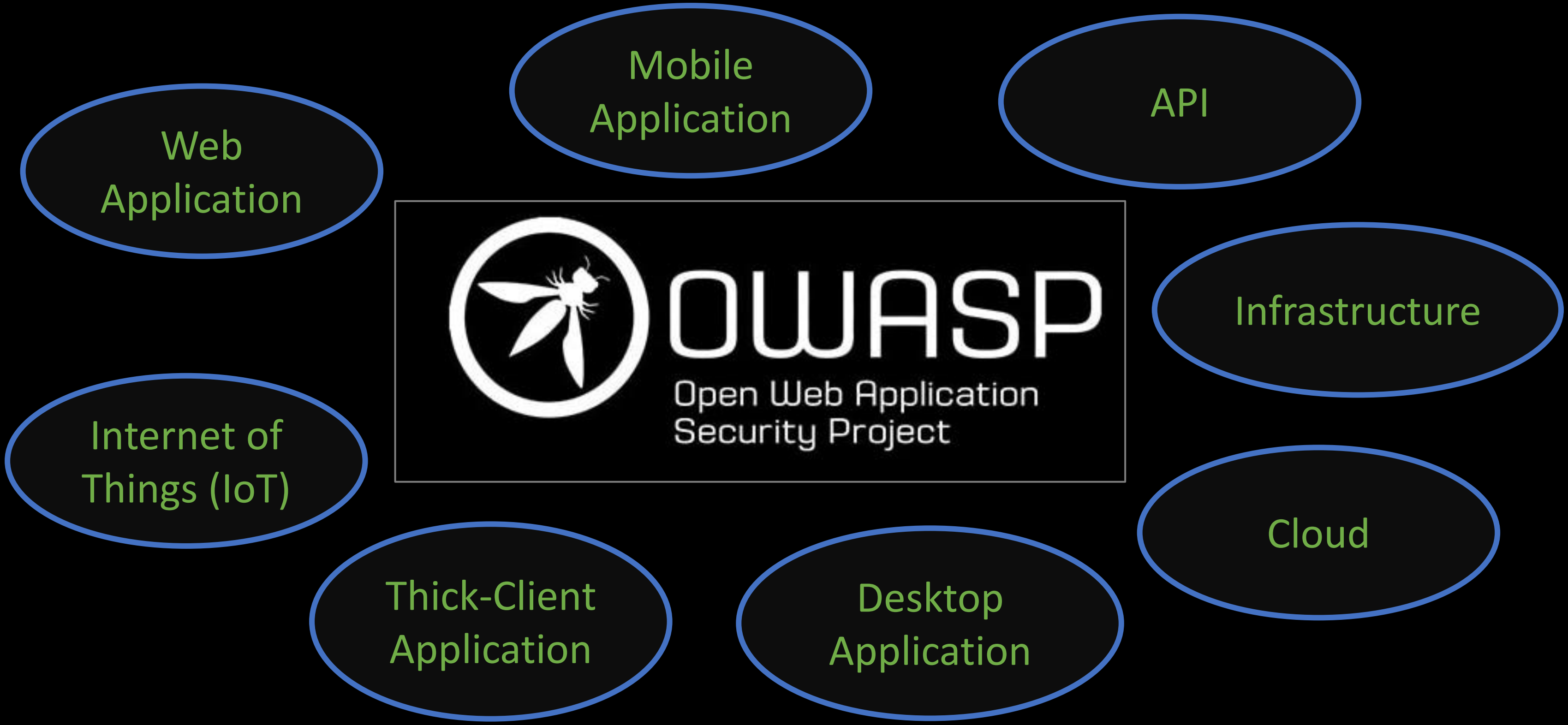
Areas of Penetration Testing

- Network Infrastructure (External Network and Internal Network)
- Web Application
- Mobile Application
- Application Programming Interface (API) / Web Service
- Wireless Network
- Thick-client Application / Desktop Application
- Internet of Things (IoT)
- Physical / Hardware

By Mr. Seang Y PHUON
@ January 2025

Open Web Application Security Project (OWASP) Top 10 Series

OWASP Top 10 Series



Web Application

Mobile Application

API

Infrastructure

Cloud

Desktop Application

Thick-Client Application

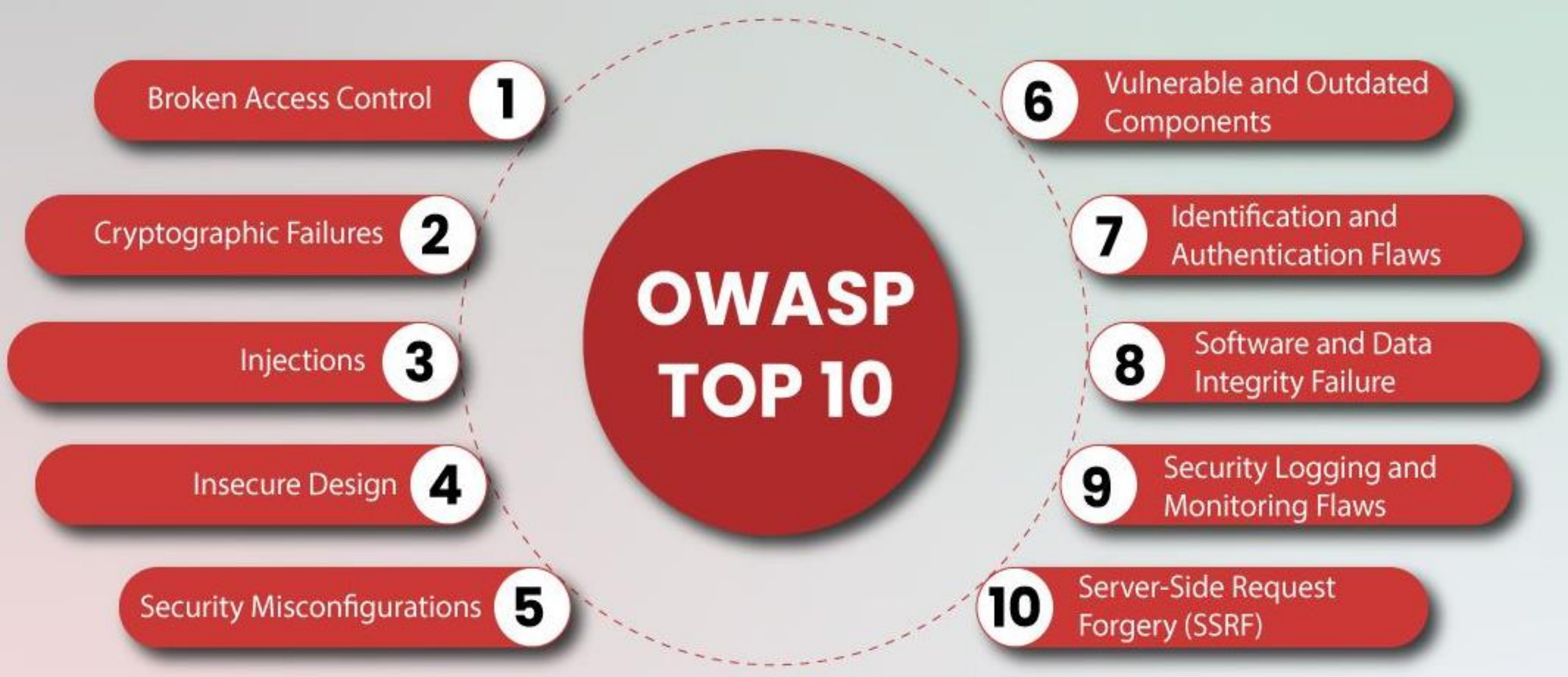
Internet of Things (IoT)

@https://owasp.org/

By Mr. Seang Y PHUON
@ January 2025

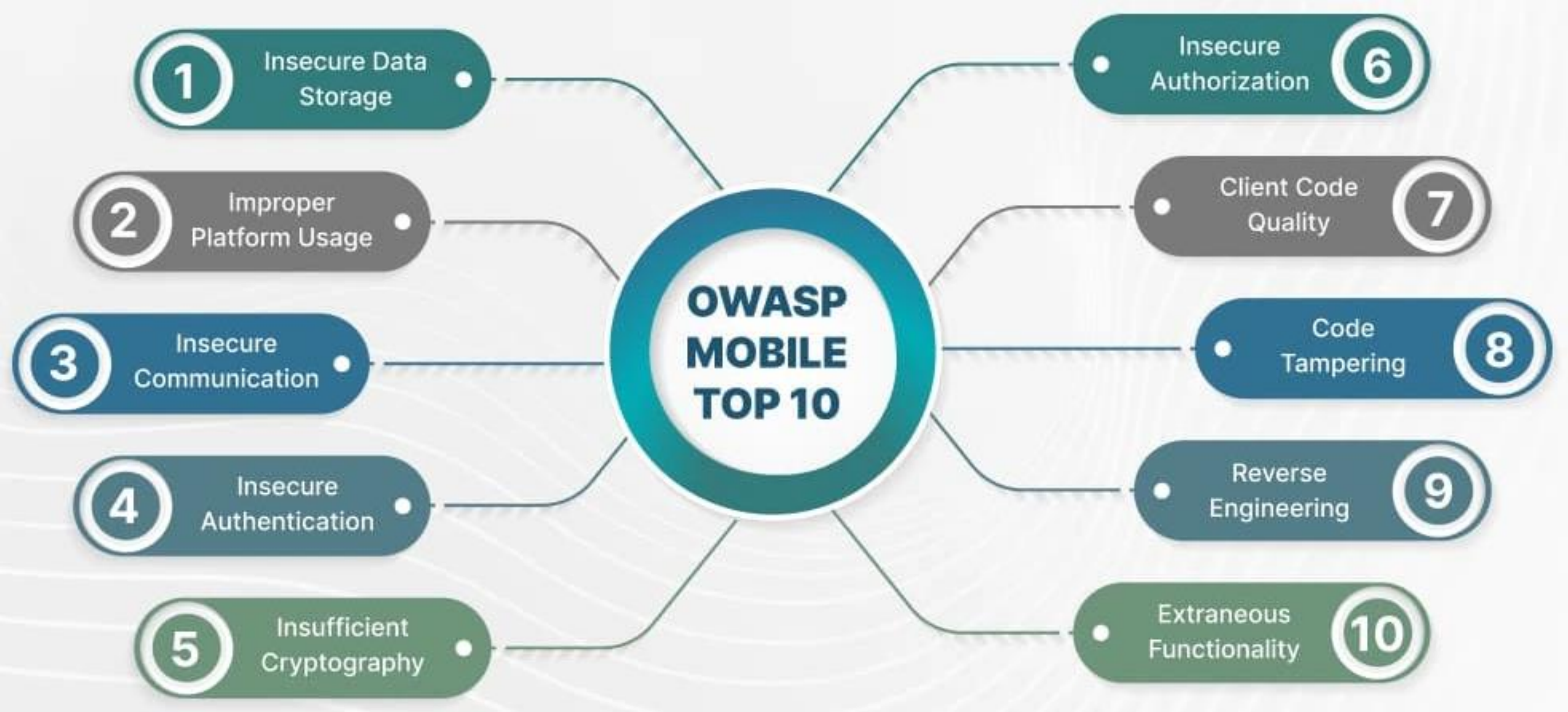
Example of Common OWASP Top 10 Series

OWASP Top 10 – Web Application Security Risks


OWASP
TOP 10
Broken Access Control 1
Cryptographic Failures 2
Injections 3
Insecure Design 4
Security Misconfigurations 5
6 Vulnerable and Outdated Components
7 Identification and Authentication Flaws
8 Software and Data Integrity Failure
9 Security Logging and Monitoring Flaws
10 Server-Side Request Forgery (SSRF)

Example of Common OWASP Top 10 Series

OWASP Top 10 – Mobile Application Security Risks

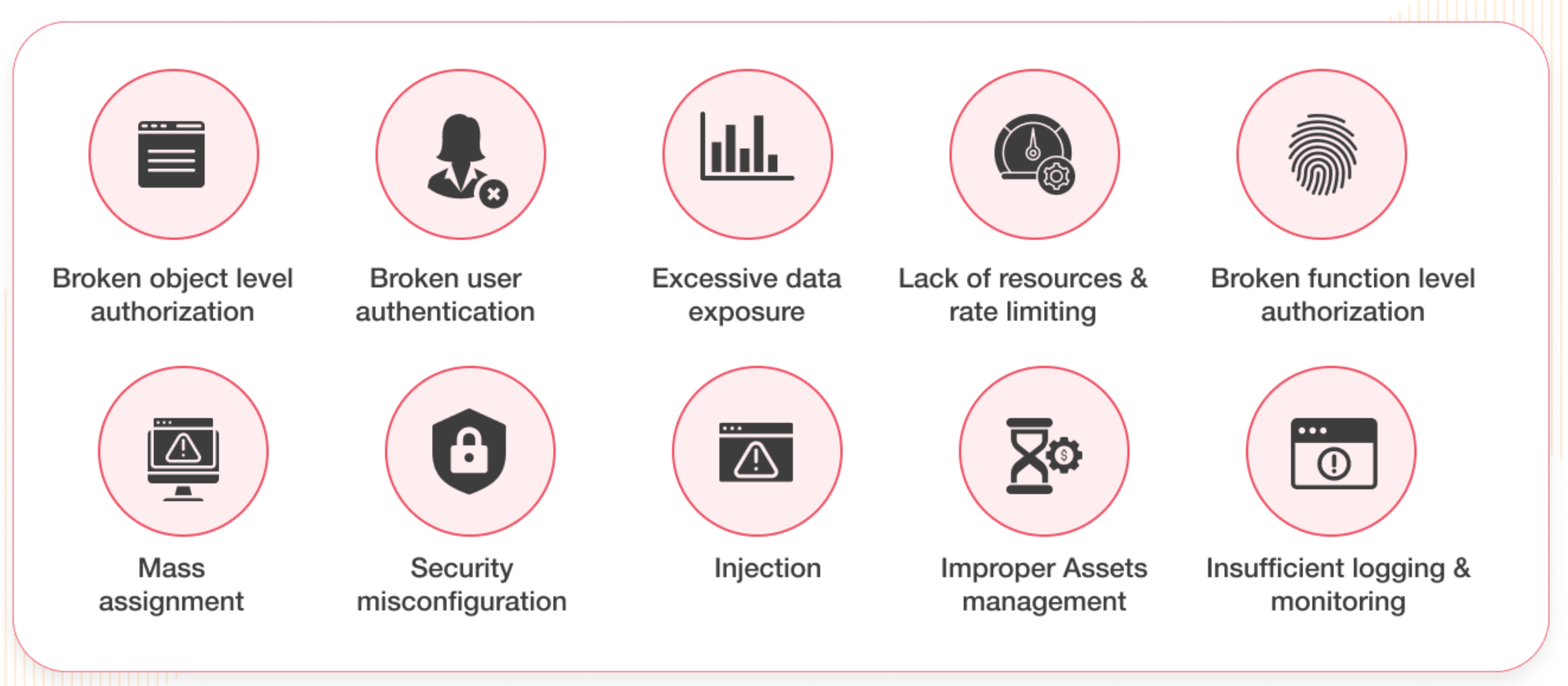


@https://resources.appsealing.com

By Mr. Seang Y PHUON
@ January 2025

Example of Common OWASP Top 10 Series

OWASP Top 10 – API Security Risks



Broken object level authorization

Broken user authentication

Excessive data exposure

Lack of resources & rate limiting

Broken function level authorization

Mass assignment

Security misconfiguration

Injection

Improper Assets management

Insufficient logging & monitoring

@https://www.simform.com

By Mr. Seang Y PHUON
@ January 2025

HACKER’S ARSENAL & INTRODUCTION TO:

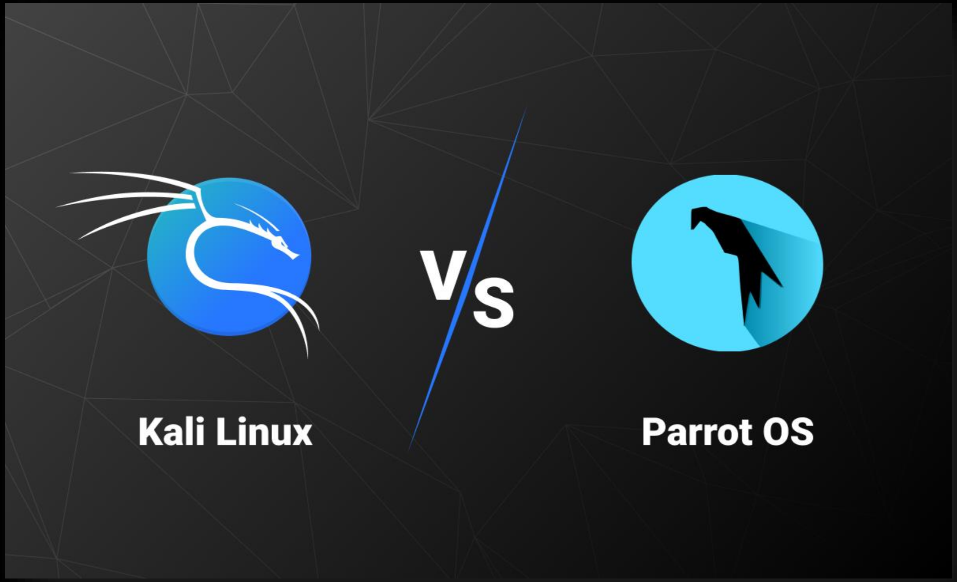
Kali Linux

By Mr. Seang Y PHUON
@ January 2025

Hacker's Arsenal

Operating Systems (OSes) with pre-installed tools used by hackers and security professionals:

- Kali Linux
- Parrot OS
- BlackArch
- BackBox
- Other

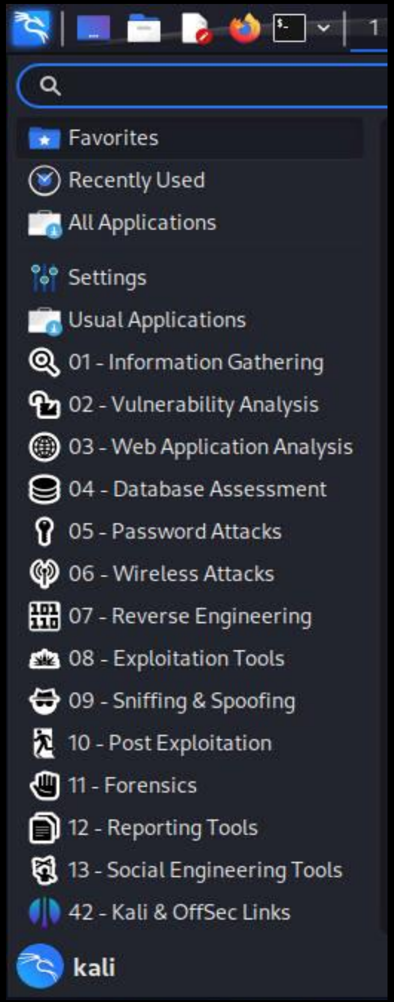


By Mr. Seang Y PHUON
@ January 2025

Introduction to Kali Linux

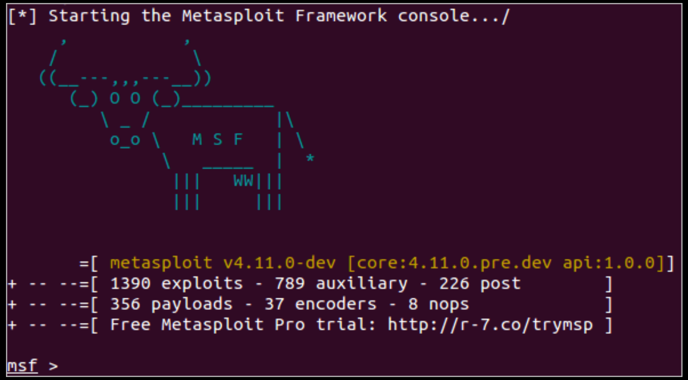
- A Debian-derived Linux distribution designed for digital forensics and penetration testing.
- It is maintained by OffSec..
- A well-known OS used by security professionals.
- Pre-installed tools.

KALI
BY OFFENSIVE SECURITY



Common Hacking Tools

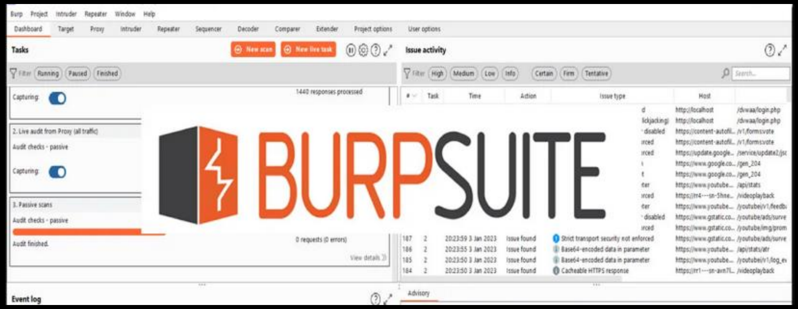
- Nmap
- Metasploit Framework
- Nessus
- Nikto
- Hydra
- CrackMapExec
- Impacket Libraries
- Hashcat
- SQLMap
- Burp Suite
- Wireshark
- Custom Tools from Github Repository



```
[*] Starting the Metasploit Framework console.../
     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||

      =[ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0]]
+ -- --=[ 1390 exploits - 789 auxiliary - 226 post        ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```



Hacking Tools in Action

Hands-On Demo

By Mr. Seang Y PHUON
@ January 2025

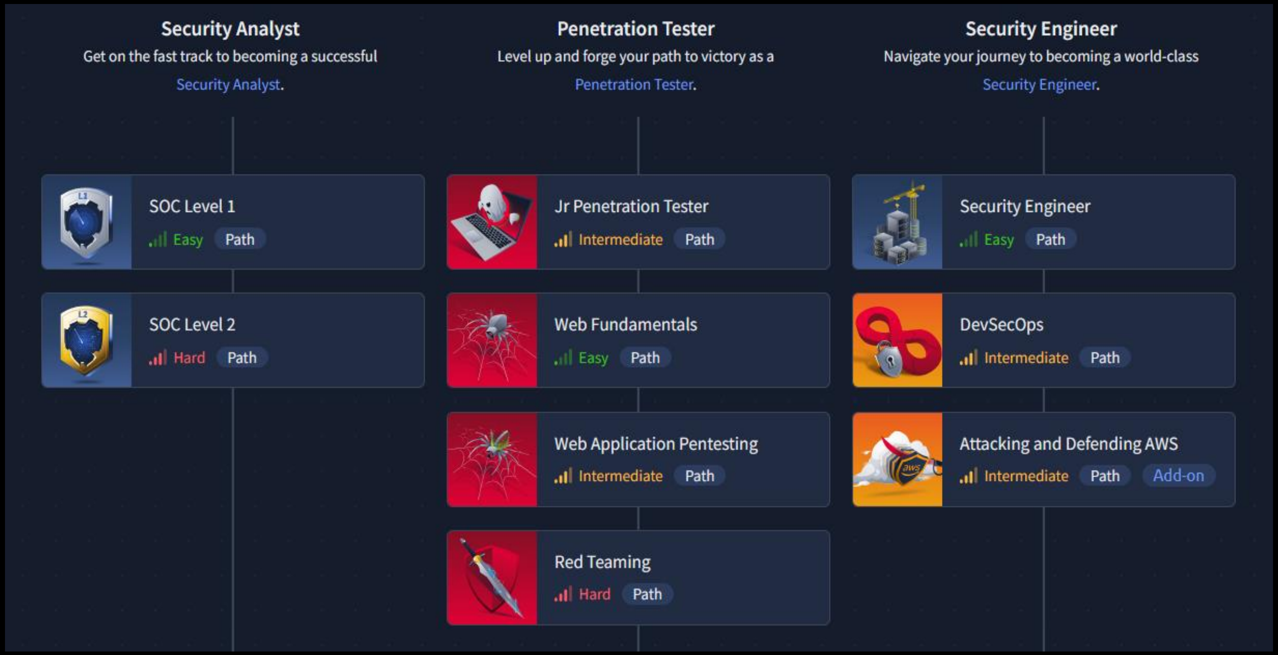
HACKER'S PLAYGROUNDS:

TryHackMe Platform

By Mr. Seang Y PHUON
@ January 2025

Introduction to TryHackMe Platform

- TryHackMe is a beginner-friendly online platform for learning cyber security with hands-on exercises and labs.



Security Analyst
Get on the fast track to becoming a successful Security Analyst.

SOC Level 1
Easy Path

SOC Level 2
Hard Path

Penetration Tester
Level up and forge your path to victory as a Penetration Tester.

Jr Penetration Tester
Intermediate Path

Web Fundamentals
Easy Path

Web Application Pentesting
Intermediate Path

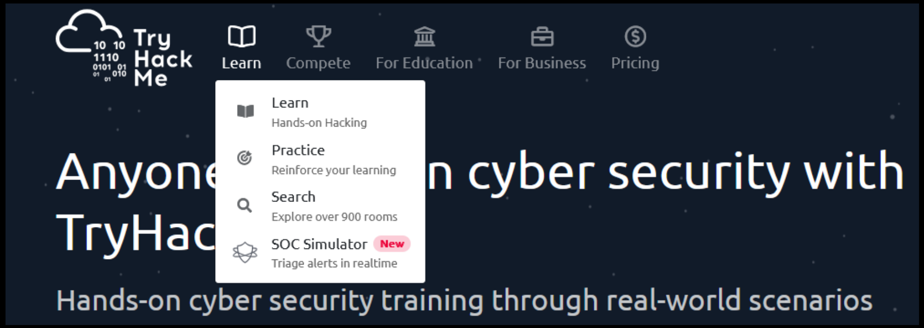
Red Teaming
Hard Path

Security Engineer
Navigate your journey to becoming a world-class Security Engineer.

Security Engineer
Easy Path

DevSecOps
Intermediate Path

Attacking and Defending AWS
Intermediate Path Add-on



Anyone n cyber security with TryHac

Hands-on cyber security training through real-world scenarios

Other Playgrounds

- HackTheBox
- VulnHub
- OverTheWire
- picoCTF
- Root-Me and Others

RECOGNIZED INDUSTRY

Certifications

By Mr. Seang Y PHUON
@ January 2025

Industry Certifications

- CompTIA – Security+, Pentest+
- INE Security / eLearnSecurity – eJPT, eCPPT
- EC-Council – CEH, CPENT, LPT
- Offensive Security (OffSec) – OSCP, OSWE, OSCE3 etc.
- Others: https://pauljerimy.com/security-certification-roadmap

Resources

- https://owasp.org/Top10
- https://tryhackme.com
- https://www.hackthebox.com
- https://ctfsites.github.io
- https://www.vulnhub.com
- https://www.offsec.com/labs
- https://www.exploit-db.com
- https://www.kali.org/get-kali
- https://thehackernews.com
- https://deepai.org

❑ Q & A

❑ ភួន សៀងអ៊ី - Phuon Seang Y

SCAN ME

❑ THECyb0rg Lab

SCAN ME