_OFFENSIVE SECURITY

The offensive approach to cyber security

@July 2023

❑ About Me

- Name: Phuon, Seang Y
- Title:
  - @ THECyb0rg Lab – a vulnerability research lab
    - Founder
    - Ethical Hacker
    - Zer0-Day Hunter
  - Instructor @ Sunrise Institute, and @ an E-learning Platform
  - Formerly Manager, Cyber Risk @ Global Big-4 Firm
- 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

@July 2023

❑ Agenda

- What is Cyber Security?
- Cyber Security Teams
- Offensive Approaches to Cyber Security
  - Vulnerability Assessment (VA)
  - Penetration Testing (PT)
  - Red Teaming Operations (RTOs)
- Vulnerability Assessment and Penetration Testing Phases
- Red Teaming Operations Cyber Kill Chain
- Malware Development and Defense Evasion
- Q&A

❑ What is Cyber Security ?

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

@July 2023

❑ Cyber Security Team

❑ Offensive Approaches To Cyber Security

- Vulnerability Assessment (VA)
- Penetration Testing (PT)
- Red Teaming Operations (RTOs)

❑ Offensive Approaches To Cyber Security

- Vulnerability Assessment (VA)

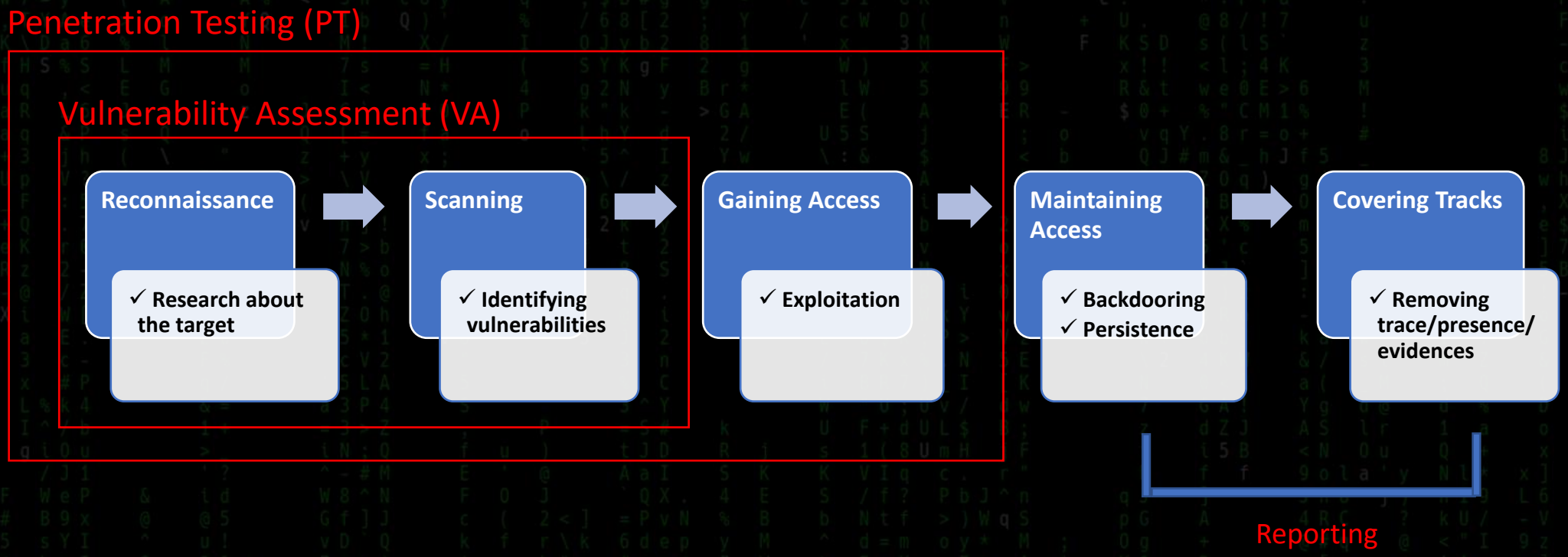
  The process of identifying vulnerabilities without exploitation attempt on the identified vulnerabilities. This includes manual and automated approaches.

❑ Offensive Approaches To Cyber Security

- Penetration Testing (PT)

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

❑ Vulnerability Assessment and Penetration Testing Phases



❑ Offensive Approaches To Cyber Security

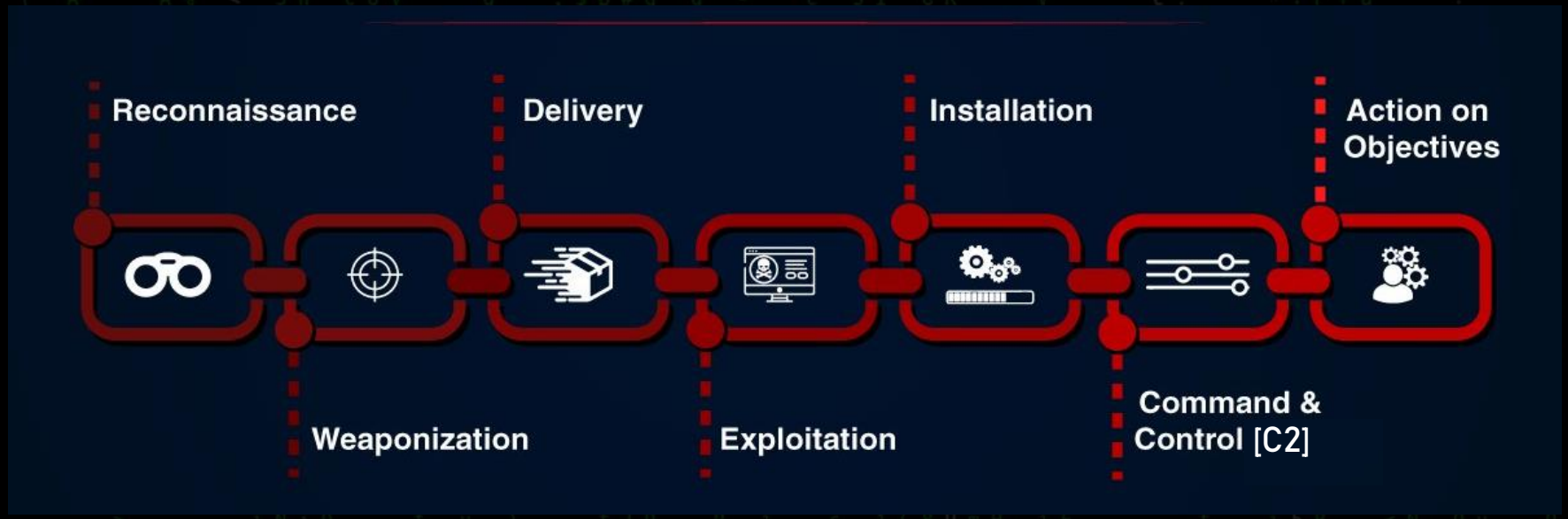
- Red Teaming Operations (RTOs)

  The process to emulate real-world threat actors to measure the effectiveness of people, process, and technology used to defend an environment.

@https://redteam.guide/docs/definition-lexicon/

@July 2023

❑ Red Teaming Operations - Cyber Kill Chain



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

❑ Malware Development and Defense Evasion

- Malware Development

  The art of developing malware or weaponizing malicious payloads to be deployed on target environment bypassing security protections.

@https://www.techtypical.com/wp-content/uploads/was-ist-malware/was-ist-malware-6-1584x797.jpg
@https://logique.s3-ap-southeast-1.amazonaws.com/2020/02/Remove-Trojan-Win32-Occamy-C.jpg

❑ Malware Development and Defense Evasion

- Defense Evasion

  The art of evading and bypassing security software/solutions within the target environment including:

  - Anti-Virus (AV)
  - Endpoint Detect and Response (EDR)
  - Firewalls, IDS/IPS
  - Sandboxes
  - AppLocker/WDAC
  - PowerShell Security: CLM, AMSI, Module Logging etc.

Follow Me on Facebook Pages @:

SCAN ME

- ភួន សៀងអ៊ី - Phuon Seang Y

https://www.facebook.com/phuonseangy

THE CyberORG LAB

SCAN ME

- THECyb0rg Lab

https://www.facebook.com/thecyb0rglab