Recon & Exploitation

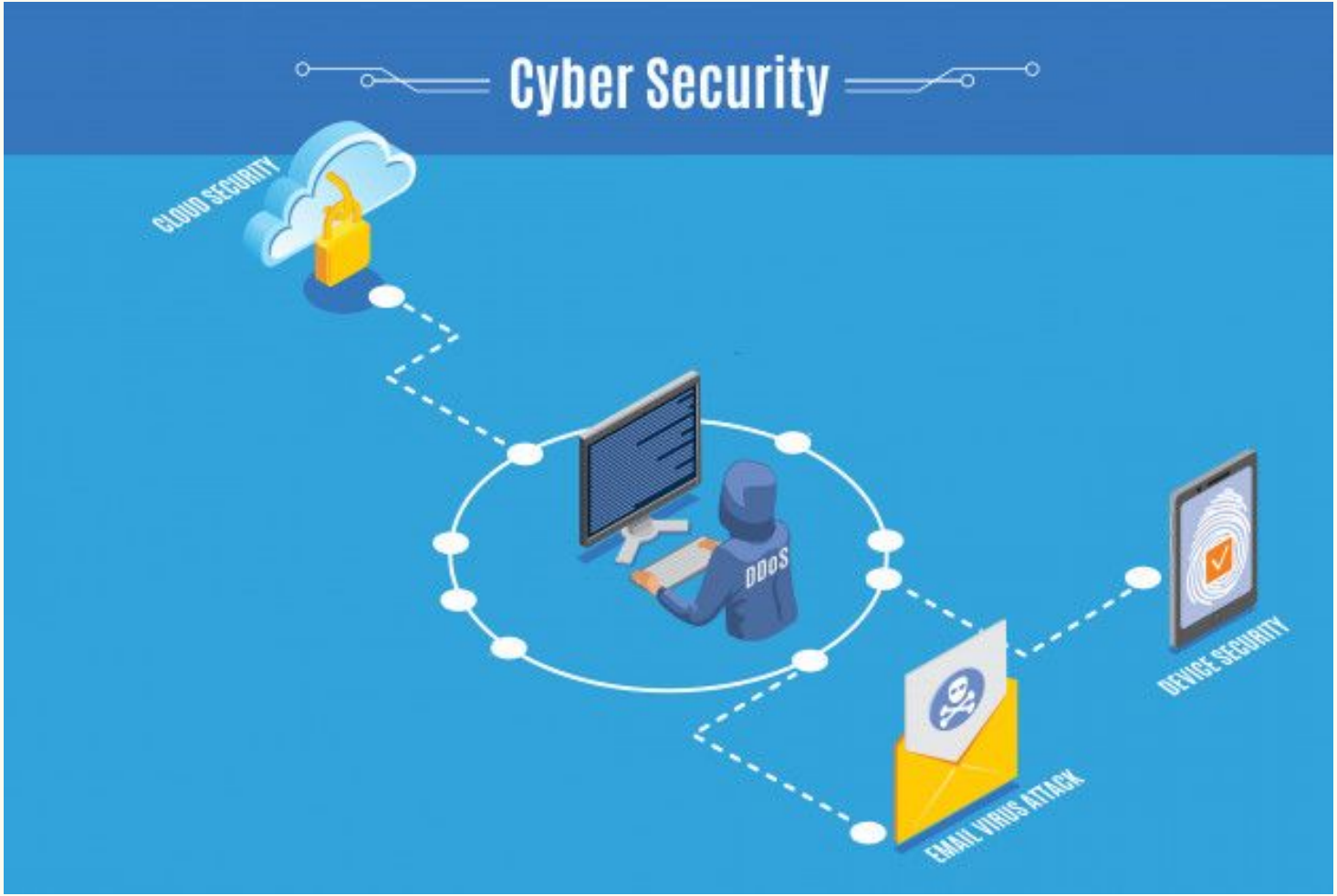
Um pouco mais sobre esses processos

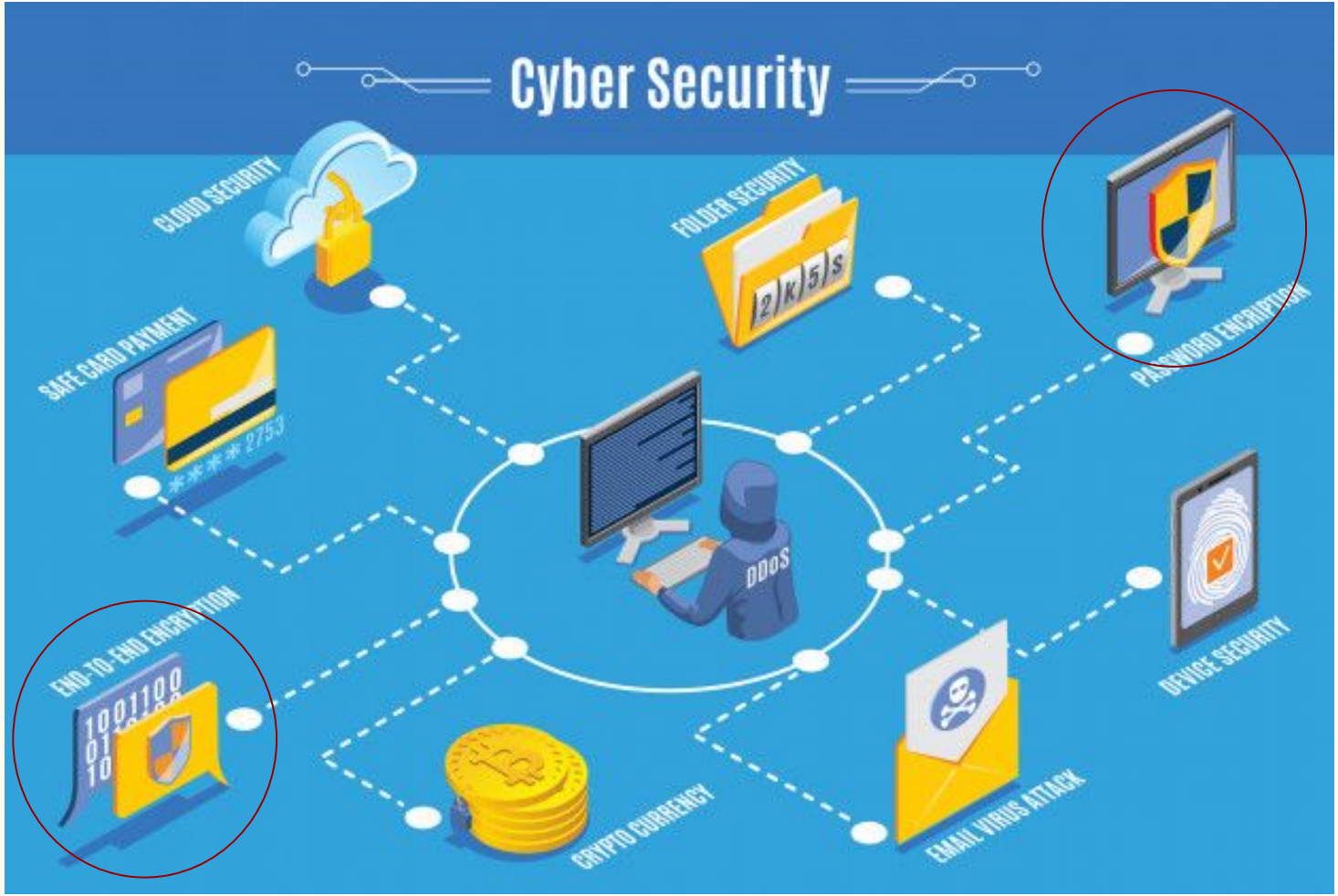
O Cerne do Pentest

- Recon
  - Mapeamento de rede
  - Mapeamento de diretórios
  - Outros serviços
- Exploitation
  - Metasploit
  - SQLMap
- Lab 1
- Lab 2

Reconnaissance


Cyber Security
CLOUD SECURITY
DDoS


Cyber Security
CLOUD SECURITY
DDoS
DEVICE SECURITY
EMAIL VIRUS ATTACK


Cyber Security
CLOUD SECURITY
FOLDER SECURITY
SAFE CARD PAYMENT
DDoS
END-TO-END ENCRYPTION
CRYPTO CURRENCY
EMAIL VIRUS ATTACK
DEVICE SECURITY

Principais Processos de Recon

- Busca por certificados e registros DNS
  - Consulta de Certificados e subdomínios
  - Censys
  - SecurityTrails
  - Google Dorking para busca de subdomínios
  - Amass
- Enumeração das máquinas encontradas
  - Identificação
  - Nmap
  - Existem serviços só para execução de scans
  - Shodan
- Enumeração de diretórios e parâmetros
  - Processo que busca encontrar arquivos sensíveis ou parâmetros utilizados pela página
  - Dirsearch, ffuf, dirb
  - Wappalyzer

Processo de Exploitation

- Uma vez identificado processos ou sistemas vulneráveis, devemos partir para a etapa de exploração.
- Cada processo vulnerável exige um ataque diferente e especializado, para

- SQL Injection
  - sqlmap

- Exploits em Geral
  - Metasploit

Lab 1

Lab 2

Material de apoio:

- Laboratório 1: https://www.vulnhub.com/entry/my-tomcat-host-1,457/
- Laboratório 2: https://www.vulnhub.com/entry/dc-32,312/
- Diversos laboratórios extras
  - https://www.hackthebox.eu/
  - https://tryhackme.com/
- Vídeos sobre essas e outras técnicas de recon
  - https://www.youtube.com/watch?v=p4JgIu1mceI
  - https://www.youtube.com/watch?v=VZrfnUXWCBk
- Curso gratuito de pentest
  - https://desecsecurity.com/curso/curso-pentest-gratuito