Cyber Sky

# Cyber sky junior Pentester (CSJP)

## This course covers these certificates (eJPT, CEH, OSCP, eCPPT)

## Outline:

- **Footprinting and Reconnaissance**
  - Introduction
  - MetaData extraction
  - Gathering information about target
  - Subdomains
  - Developing tools using python

- **Scanning Networks and Enumeration**
  - Live hosts scanning , OS
  - open ports scanning
  - labs
    - Nmap
    - Python Scapy
  - Services enumeration Samba, FTP, HTTP, SNMP, SMTP, NFS, DNS
  - Nessus
  - IDS Evasion

+(970) 592 094401 info@cyber-sky.org www.cyber-sky.org
USA - 651 N Broad st, Middletown, Delaware 19709
Palestine, 454 Alwehda st Gaza, Gaza strip P840

Cyber Sky

## Password attacks

- Types of password attacks
- Wordlist generator tools
- Hash cracking (Developing tool using python )
- SE toolkit
- John the ripper , hashcat and hydra (kali tools )
- Attacks on custom services

## Web application vulnerabilities

- HTTP/S protocol
- Web service concept
- BurpSuite
- SQL injection
  - Zixem SQL
  - sqlmap
- XSS

  XSS google
- Command Injection
- RCE
- exploit fixing python

+(970) 592 094401 info@cyber-sky.org www.cyber-sky.org
USA - 651 N Broad st, Middletown, Delaware 19709
Palestine, 454 Alwehda st Gaza, Gaza strip P840

Cyber Sky

## System hacking

- Introduction to system hacking
- Metasploit framework
- Buffer Overflow (-٣٢bit and -٦٤bit)

  Introduction to CPU architecture

  Windows BOF

  Linux BOF
- Privilege escalation(Windows and Linux )
- Port redirection and tunneling
- Locating public exploits IOT pentesting
- Metasploitable  Walkthrough
- Cysec ١ machine Walkthrough
- Tr٠ll ١ machine Walkthrough
- Kioptrix ٣, ٢ , ١ and ٤ machines walkthrough
- many of tryhackme machines  walkthroug

## Wireless attacks

- WIFI frames
- Handshake capturing (airodump , aircrack ,aireplay )
- Evil twin attack
- Pure socket WIFI sniffer

+(970) 592 094401 info@cyber-sky.org www.cyber-sky.org
USA - 651 N Broad st, Middletown, Delaware 19709
Palestine, 454 Alwehda st Gaza, Gaza strip P840

Cyber Sky

## IOT pentesting

- Basic fundamental
- Firmware in IOT
- IOT Threat Modeling
- OWASP IOT top ١٠
- Practical side

## Malware attacks

- Types of malwares
- Develop a C&C using python
- Develop simple malware
- browser passwords stealer concept

## Cloud

- Intro to cloud security
- Pentesting ECr
- Pentesting AWS Simple Storage Service Configuring and Securing
- Leveraging AWS Pentesting Tools for Real-World Attacks

+(970) 592 094401 info@cyber-sky.org www.cyber-sky.org
USA - 651 N Broad st, Middletown, Delaware 19709
Palestine, 454 Alwehda st Gaza, Gaza strip P840

## Cryptography

- Intro to cryptography
- Encryption algorithms(AES, RSA, RCɛ, XOR and ᵻDES)
- Developing tools
- CTF

## Active Directory Attacks

- What is Active Directory
- What is the Forest in Active Directory
- The Trust in Active Directory
- Active Directory Domain Services & Authentication
- Active Directory Cloud

## Report Writing

## CTF

+(970) 592 094401 info@cyber-sky.org www.cyber-sky.org
USA - 651 N Broad st, Middletown, Delaware 19709
Palestine, 454 Alwehda st Gaza, Gaza strip P840