

Cybersecurity

• Introduction to cybersecurity

- What is Cybersecurity?
- CIA Triad
- Identification and Authentication, Authorization, and Accounting (AAA)
- Threat Actors
- Malwares
- Common Types of Cybersecurity Attacks
- Social engineering

• Network

- Network Devices
- OSI Model
- TCP/IP
- Protocols
- IP Subnetting
- Network Segmentation
- Zero Trust Security Model
- Firewalls
- Proxies
- VPN
- Wireless Cryptographic Protocols

• Operating Systems

- How Operating Systems Works ?
- Windows 7 / 10 / 11
- Windows Server
 - Active Directory
- Linux

• Web

- How the Web Works ?
 - Client Server Architecture
- HTTP Methods
- HTTP Headers
- Cookies
- HTTP response status codes

• Cryptographic

- Cryptosystem
- Key Exchange
- Encryption
 - Symmetric Algorithms
 - Asymmetric Algorithms
- Hashing
- Steganography

• Virtualization and Cloud Computing

- Virtualization
- Cloud Workloads
- Services Models
- Deployment Models
- Regions and Availability Zones
- Virtual Private Cloud (VPC)
- Security Groups & Policies

• Programing Language

- PHP
- Python
- Javascript
- SQL

• Shell Scripting

- Bash
- Powershell

• Vulnerabilities

- Web Vulnerabilities
 - OWASP TOP 10
- Network Vulnerabilities & Attacks
- Zero-Day
- Third-Party Risks

• Penetration Testing

- What is Penetration Testing ?
- Types of Penetration Testing
- Testing Methodology
- SAST & DAST
- Vulnerability Scans
- Threat Assessment

• Advanced

- Active Directory Attacks
- Reverse Engineering
- Buffer overflow
- Malware analysis

• Must know

- Cyber Kill Chain
- MITRE ATT&ck

• Blue Team & Red Team

- Red Team
 - Red Teaming Methodology
 - Red Teaming Tools
- Blue Team
 - SOC
 - Digital Forensics
 - SIEM / CASB
 - Incident Response
 - Log Management & Analysis
 - Blue Team Tools

• Regulations, Standards, and Frameworks

- What is a Cybersecurity Framework ?
- The NIST Framework
- CIS Benchmarks
- ISO 27001 and ISO 27002
- PCI DSS
- HIPAA
- GDPR

Courses, Books and Cert Path

- Learning platforms
 - LetsDefend
 - Portswigger
 - TryHackMe
 - HackTheBox
- Youtube
 - 13Cubed
 - Computerphile
 - PwnFunction
 - LiveOverflow
 - The Cyber Mentor
 - HackerSploit
 - John Hammond
- Books
 - Cybersecurity For Dummies
 - Social Engineering: The Science of Human Hacking
 - The Art of Invisibility
 - Ghost In The Wires
 - Kali Linux Hacking: A Complete Step by Step Guide by Ethem Mining
 - The Hacker Playbook 3: Practical Guide to Penetration Testing
 - Penetration Testing: A Hands-On Introduction to Hacking
 - Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software
- Certifications Learning Path
 - CCNA
 - CompTIA Network +
 - CompTIA Security +
 - CIAC (GISF)
 - eJPT
 - OSCP