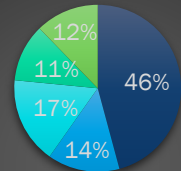**88 HOURS**

Cyber Security?

- Computer security, cybersecurity or information technology security (IT security) is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

Cyber Security

- Ethical Hacking (CEHv11)
- Network System Core Level
- Linux System Core Level
- Windows System Core Level
- CTF

PART1 : Windows System Core Level

Module 1: Installing and configuring domain controllers

- Overview of AD DS
- Overview of AD DS domain controllers
- Deploying a domain controller
- Deploying AD DS
- Deploying domain controllers by performing domain controller cloning
- Administering AD DS

Module 2: Managing objects in AD DS

- Managing user accounts
- Managing groups in AD DS
- Managing computer objects in AD DS
- Using Windows PowerShell for AD DS administration
- Implementing and managing OUs
- Lab : Managing AD DS objects
- Creating and managing groups in AD DS

- Creating and configuring user accounts in AD DS
- Managing computer objects in AD DS
- Lab : Administering AD DS
- Delegate administration for OUs
- Creating and modifying AD DS objects with Windows PowerShell

PART2 : Network System Core Level

Module 1: Building a Simple Network
- Exploring the Functions of Networking
- Understanding the Host-to-Host Communications Model
- Introducing LANs
- Operating Cisco IOS Software
- Starting a Switch
- Understanding Ethernet and Switch Operation
- Troubleshooting Common Switch Media Issues

Module 2: Establishing Internet Connectivity
- Understanding the TCP/IP Internet Layer
- Understanding IP Addressing and Subnets
- Understanding the TCP/IP Transport Layer
- Exploring the Functions of Routing
- Configuring a Cisco Router
- Exploring the Packet Delivery Process
- Enabling Static Routing
- Managing Traffic Using ACLs
- Enabling Internet Connectivity

Module 3 : Implementing DNS
- Implementing DNS servers
- Configuring zones in DNS
- Configuring name resolution between DNS zones
- Configuring DNS integration with Active Directory Domain Services (AD DS)
- Configuring advanced DNS settings

- Lab : Planning and implementing name resolution by using DNS
- Planning DNS name resolution
- Implementing DNS servers and zones
- Lab : Integrating DNS with Active Directory
- Integrating DNS with Active Directory
- Lab : Configuring advanced DNS settings
- Configuring DNS policies
- Validating the DNS implementation
- Troubleshooting DNS

PART3 : Linux System Core Level

- Basics Of Commands
- Navigating directories
- How to get help when needed
- Creating , Copying , Moving , Removing directories and files
- How to edit files with VIM
- Using wildcards to speed up tasks
- Managing users and groups
- Maintaining permissions
- Command redirection and controlling output
- Managing Service
- Networking basics
- Archiving files and directories
- SSH Access
- Download, install, update, and manage software packages from package
- repositories and github

PART4 : Ethical Hacking (CEHv11)

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration

- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing
- Cryptography

PART4:CTF

- Capture the Flag (CTF) is a special kind of information security competitions. There are three common types of CTFs: Jeopardy, Attack-Defence and mixed.

- Jeopardy-style CTFs has a couple of questions (tasks) in range of categories. For example, Web, Forensic, Crypto, Binary or something else. Team can gain some points for every solved task. More points for more complicated tasks usually. The next task in chain can be opened only after some team solve previous task. Then the game time is over sum of points shows you a CTF winer. Famous example of such CTF is Defcon CTF quals.

- Well, attack-defence is another interesting kind of competitions. Here every team has own network(or only one host) with vulnarable services. Your team has time for patching your services and developing exploits usually. So, then organizers

connects participants of competition and the wargame starts! You should protect own services for defence points and hack opponents for attack points. Historically this is a first type of CTFs, everybody knows about DEF CON CTF - something like a World Cup of all other competitions.

- Mixed competitions may vary possible formats. It may be something like wargame with special time for task-based elements (e.g. UCSB iCTF).

- CTF games often touch on many other aspects of information security: cryptography, stego, binary analysis, reverse engeneering, mobile security and others. Good teams generally have strong skills and experience in all these issues.