- ## Courses For Event WT2017 Cybersecurity Ethical Hacking

- Cyber Security Course
- Ethical Hacking

- ## Topics For Ethical Hacking

- Concepts of networking and connecting remote computers using Netcat
- Port Scanning using Nmap, Zenmap and Network Statistics
- Network Services, Wired and Wireless Networks
- Concepts of ARP Spoofing and Man in the Middle Attack
- Practical Demonstration: Man in the Middle Attack using ARPSPOOF
- How to create virus program using metasploit framework
- How to create virus program for victims on internet
- Device Forensics
- Device Forensics on Virtual Devices
- How to take Device dump of a real device
- Server and Website Vulnerability Scanning using Nikto and Owasp ZAP
- Hacking Websites using SQL Injections
- Hiding files using Alternate Data Streams
- Concepts of Firewalls, Intrusion Detection Systems
- Concepts of Proxy Servers

- ## Resources For Ethical Hacking

- Download VMWARE Workstation 10.0.7 for Windows
- Download VMware Workstation 11.1.4 for Linux
- Download Kali 64 bit (2.8 GB)
- Download Kali 32 bit (2.9 GB)
- Download Kali 32 bit (2.9 GB)
- Download Netcat for Windows - nc111nt.zip (password:nc)
- Download NMAP 7.60 for Windows
- Download NMAP 7.60 for Linux 64 x86-64 (64bit)
- Download NMAP 7.60 for MAC OSX
- Download Wireshark for Windows 64 bit

- Download Wireshark for Windows 32 bit
- Download Wireshark for Mac OS 10.6 and Later
- Download WinHex for Windows: Computer Forensics & Data Recovery Software

This course ends on 06 January 2018

Topics For Cyber Security Course

- The OSI Model
- Network Hardware
- IPv4
- IPv6
- TCP and UDP
- Use Common Windows TCP/IP Utilities
- Use Common Linux TCP/IP Utilities
- Configure and Scan for Open Ports
- Network Services
- Wired and Wireless Networks
- Use Common Wireless Tools
- Internal and External Networks
- Cloud Concepts
- Cloud Service Models
- Virtualization
- Cloud Security Options
- Topology, Service Discovery, and OS Fingerprinting
- Reviewing Logs
- Packet Capturing
- Capture FTP and HTTP Traffic
- Network Infrastructure Discovery
- E-mail and DNS Harvesting
- Social Engineering and Phishing
- Acceptable Use Policy
- Data Ownership and Retention Policy
- Data Classification Policy

- Password Policy
- Threat Overview
- Threat Classification
- Personally Identifiable Information
- Payment Card Information
- Intellectual Property
- Data Loss Prevention
- Prevent Data Storage on Unencrypted Media
- Scope of Impact
- Stakeholders
- Role-based Responsibilities
- Incident Communication
- Host Symptoms and Response Actions
- Network Symptoms and Response Actions
- Application Symptoms and Response Actions
- Incident Containment
- Incident Eradication
- Lessons Learned
- OEM Documentation
- Network Documentation
- Incident Response Plan/Call List
- Incident Documentation
- Chain of Custody Form
- Change Control Processes
- Types of Reports
- Service Level Agreement
- Memorandum of Understanding
- Asset Inventory
- SDLC Phases
- Secure Coding
- Security Testing
- Host Hardening

This course ends on 13 January 2018