1. Course Details:

Course Code : ISCS-002
Course Title : SSCP - Systems Security Certified Practitioner
Course Duration : 5 Days

2. Course Overview:

- The (ISC)2 Systems Security Certified Practitioner (SSCP) certification covers seven domains which they describe as 'the compendium of topics pertaining to an Information Systems Security Practitioner', the CBK (Common Body of Knowledge). The SSCP is aimed at security go-to-people, on the front line of a business dealing with technologies employed to protect Information. If you are responsible for implementing and maintaining countermeasures such as Firewalls, Intrusion Detection or Prevention, Anti-Virus solutions or Public Key Infrastructures and you want a certification to attest to your skills and professionalism within Information Security, this is it.

3. Learning Outcomes:

- SSCP maps to just over half of the CISSP required knowledge, so it is great as a precursor or certification path to follow if you intend on obtaining CISSP in the future
- Build a relationship with (ISC)2 and use the many member benefits to manage and improve your career as an Information Security professional
- SSCP allows you to waive one year of the 5 years' experience required to pass CISSP, (other certifications can also allow this)

4. Course Contents:

Testing-Taking Tips and Study Techniques

- Preparation for the SSCP Exam
- Submitting Required Paperwork
- Resources and Study Aids
- Passing the Exam, the First Time

Security Operations and Administration

- Change Control/Configuration Management
- Dual Control, Separation of Duties, Rotation of Duties
- Vulnerability Assessment and Pen-Testing

Access Controls

- Authentication Methods
- Authorization - DAC, RBAC, MAC
- Accounting - Logging, Monitoring, Auditing
- Central/Decentralized and Hybrid Management
- Single Sign-On - Kerberos, Radius, Diameter, TACACS
- Vulnerabilities - Emanations, Impersonation, Rouge Infrastructure, Social Engineering

Cryptography

- Intro/History
- Symmetric
- Asymmetric
- Hashing
- Cryptosystems - SSL, S/MIME, PGP
- PKI
- Cryptanalysis

Malicious Code and Malware

- Layering, Data Hiding, and Abstraction
- Database Security
- OOD
- Mobil Code
- Malware Architecture Problems - Covert Channels + TOC/TOU, Object Reuse
- Network Vulnerabilities

Networks and Telecommunications

- OSI/DoD TCP/IP Models
- TCP/UDP/ICMP/IP
- Ethernet
- Devices - Routers/Switches/Hubs
- Firewalls
- Wireless
- WAN Technologies - X.25/Frame Relay/PPP/ISDN/DSL/Cable
- Voice - PBX/Cell Phones/VOIP

Risk, Response, and Recovery

- Roles and Responsibilities - RACI
- Asset Management
- Taxonomy - Information Classification
- Risk Management
- Policies, Procedures, Standards, Guidelines, Baselines
- Knowledge Transfer - Awareness, Training, Education
- BIA Policy
- BIA Roles and Teams
- Data Backups, Vaulting, Journaling, Shadowing
- Alternate Sites
- Emergency Response
- Required notifications

Analysis and Monitoring

- Ethics - Due Care/Due diligence
- Intellectual Property
- Incident Response
- Forensics
- Evidence
- Laws - HIPAA, GLB, SOX

Final Review and Test Preparations

5. Our Methodology:

- Make coaching and monitoring innovative and using modern
- Media training also using on the go training by using interactive means and focusing on
- The exercises, practical applications and real situations study.
- Live delivery method, instructor-led training.
- Experienced consultant, trainers, and professional.
- Qualified trainer with high-level experience

6. Attendance Reports:

- Send daily attendance reports to trainingdep
- Send full attendance report to training dep. by the end of thecourse
- Attend 100 % from the course days also providedaily
- Issue attendance certificate for participant who attend minimum 80% from the course duration

7. Pre/Post Reports:

- Pre- assessment before starting training.
- Post assessment after finish training
- Full report for the deferent between Pre-& Post assessment

8. Who Should Attend?

- Network Security Engineer
- Security Administrator
- Security Analyst
- Systems Engineer
- Network Administrator
- Systems Administrator
- Security Specialist
- Systems/Network Analyst
- Security Consultant
- Database Administrator