Certificate Course in Network Security

Course Objective

with Vulnerabilities & Threats all over, this course aims at preparing participants to secure their Computer Networks in various environments like Microsoft, Linux and Cisco

Course Outcomes

On completion of this course the participants will be able to:

- Understand of ethical hacking ethics and legality
- Implement the Foot printing and social engineering, Scanning and enumeration, system hacking
- Identifying of Trojans, back doors, virus and worms, sniffers, Denial of services and session hijacking
- Understand Hacking web servers, web application vulnerabilities
- Implementing Evading IDS honey pots and firewalls, wireless hacking
- Implementing Cryptography, penetration testing methodologies
- Configuring, verifying & troubleshooting a switch with VLANs and interswitch communications
- Implementing an IP addressing scheme and IP services to meet network requirements
- Implementing CBAC and zone-based firewalls, IPS
- Install, Configure of STP, VLAN, Secure layer 2 Switches
- Implement Traffic Control IP tables , NAT, SNAT, DNAT, PAT
- Implement SQUID (proxy server), QOS, Bandwidth, Splitting
- Implementing of Securing - Web, FTP, Open SSH, NFS, Email
- Implementing of IPcop as Firewall Intrusion Detection and Recovery
- Installing and configure AD, group policy, access control, DFS.
- Configure ADCS & PKI deploying a CA hierarchy EFS
- Configure ADRMS, IPSec, NAP, NAT, VPN services.
- Design & Identifying treats to network security
- Implementation and maintaining of TMG

Target Audience

This course is designed for individuals expected to have some hands-on experience with Windows Server, Windows based networking, Active Directory, Anti-Malware products, firewalls, network topologies and devices, and network ports

Teaching Methodology

This course is based on theoretical lessons and delivered in a Classroom atmosphere.

Prerequisites

Graduates / Engineers / Diploma holders with basic Knowledge of Hardware and networking application used

Duration : 10 Weeks (5 days a week , 6 - 8 hours per day)

Batch 1 – 03-07-2017 to 09-09-2017

Batch 2 – 11-09-2017 to 18-11-2017

Course Outline

Network Essentials

- Networking Essentials, LAN, WAN, Protocols
- ISO Model, IP Addressing, Internet, Intranet, Network Cables

Essential of IT Security System

- Introduction to ethical hacking ethics and legality
- Foot printing and social engineering
- Scanning and enumeration, system hacking
- Trojans, backdoors, virus and worms, sniffers
- Denial of services and session hijacking
- Hacking web servers, web application vulnerabilities,
- Evading IDS honey pots and firewalls, wireless hacking
- Cryptography, penetration testing methodologies

Forefront Threat Management Gateway (TMG)

- Installing and Maintaining TMG Server, Enabling Access to Internet Resources
- Configuring TMG as a firewall, Access to Advanced Application & Web Filtering
- Implementing Caching to Browsing & TMG Enterprise Edition

Windows Security

- Overview of AD, group policy, access Control, file system Security.
- Config AD CS overview of PKI deploying a CA hierarchy, EFS.
- Config AD right management services,
- Configuration of IPSec and network access protection.
- Config VPN access, routing and remote access, NAT.
- Designing network security, identifying threats to network Security.

Linux Security

- Traffic Control Iptables, NAT, SNAT, DNAT, PAT
- SQUID (proxy Server), QOS , Bandwidth Splitting
- Internet Security -Web, FTP, OpenSSH, NFS, Email
- IPcop as Firewall Intrusion Detection and Recovery

CCNA Security

- Administrative access, administrative access using AAA & RADIUS. Policy development & implementation.
- CBAC and zone-based firewalls, intrusion prevention system (IPS) using the CLI and SDM.
- Spanning tree, VLAN, securing layer 2 wwitches, VPN using Cisco IOS and SDM, remote access VPN server & client

For more details and procedure to apply for scholarship : **http://www.utltraining.com/itec-scaap/**