EC-COUNCIL NETWORK SECURITY ADMINISTRATOR

DURATION: 5 DAYS

COURSE OVERVIEW

This course looks at the network security in defensive view. The ENSA program is designed to provide fundamental skills needed to analyze the internal and external security threats against a network, and to develop security policies that will protect an organization's information. Students will learn how to evaluate network and Internet security issues and design, and how to implement successful security policies and firewall strategies. In addition, they will learn how to expose system and network vulnerabilities and defend against them.

TARGET AUDIENCE

System administrators, Network administrators and anyone who is interested in network security technologies.

COURSE OBJECTIVES

The ENSA 312-38 exam will be conducted on the last day of training. Students need to pass the online Pro metric exam to receive the ENSA certification.

COURSE CONTENT

Module: Fundamentals of Network

Module: Network Protocols

Module: Protocol Analysis

Module: IEEE standards

Module: Network Security

Module: Security Standards Organizations

Module: Security Standards

Module: Security Policy

Module: Hardening Physical Security

Module: Network Security Threats

Module: Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS)

Module: Firewalls

Module: Packet Filtering and Proxy Servers

Module: Bastion Host and Honeypots

Module: Securing Modems

Module: Troubleshooting Network

Module: Hardening Routers

Module: Hardening Operating Systems

Module: Patch Management

Module: Log Analysis

Module: Application Security

Module: Web Security

Module: E-mail Security

Module: Authentication: Encryption, Cryptography and Digital Signatures

Module: Virtual Private Networks

Module: Wireless Network Security

Module: Creating Fault Tolerance

Module: Incident Response

Module: Disaster Recovery and Planning

Module: Network Vulnerability Assessment

COURSE PREREQUISITES

This course is a prerequisite for the CEH program.