Network Security Expert

This course is mapped to the Network Security Expert Certification Exam from US-Council.

This is a comprehensive course which covers the nitty gritty of network security. It is a vendor independent course, designed to make the security engineer aware of how exactly security can be built into an organization's network. It gives an in depth understanding of the underlying protocols and mechanisms of network security. The Network Security Engineer would be able to configure firewalls, security policies, NAT, VPNs, IPS / IDS, content security, etc. at the end of this course, irrespective of the vendor, with very little additional platform specific training.

Course Outline

INTRODUCTION TO NETWORKING

- OSI Model
- IP addressing
- Subnetting

NETWORKING DEVICES

- Switches
- Routers
- Access points

NETWORKING PROTOCOLS

- HTTP
- HTTPS
- FTP
- DHCP
- Domain Naming System
- Telnet
- SSH
- NTP
- Syslog

ROUTING AND ROUTING PROTOCOLS

- Static Routing
- Default Routing
- Dynamic Routing Protocols

TROUBLESHOOTING NETWORKS

- ICMP
- SNMP
- Ping
- Trace route
- Sniffers
- Protocol Analysis
- Wireshark
- Syslog analysis

NETWORK SECURITY

- Layer 1 Security
- Layer 2 Security
  - o Vlans
  - o Port security
  - o Wireless Security
- Layer 3 security
  - o Routers with Access lists
  - o Securing Routers
- Device - Role based access
- BNTP
- Log management and log analyses

FIREWALL

- Types of firewalls
  - o Packet filtering
  - o Proxy server
  - o Stateful inspection
- BDesigning Security with Firewalls
  - o Routed mode
  - o Transparent / Bridge mode.
- NAT
  - o Static NAT
  - o Dynamic NAT
  - o PAT

SECURITY POLICY

APPLICATION SECURITY

CONTENT / WEB SECURITY

- URL filtering
- Blacklists and white lists
- Keyword filtering
- Category based filtering

AUTHENTICATION

- RADIUS
- Kerberos
- LDAP

VIRTUAL PRIVATE NETWORKS

- Encryption Algorithms
- Symmetric and Asymmetric cryptography
- Public / Private key Infrastructure (PKI)
- Hash Algorithms
- GRE
- IPSEC
  - o ISAKMP/IKE
  - o Phase 1 Negotiations
  - o Phase 2 Negotiations

  - Main mode and aggressive mode
  - Diffie Hellman Algorithm
  - IPSec SAs and IKE SAs
  - Site to site VPNs
  - Remote access VPNs
  - Troubleshooting VPNs
- SSL

INTRUSION DETECTION / INTRUSION PREVENTION SYSTEMS

- IPS/IDS Signatures
- Custom Signatures
- Fine tuning of Signatures
- Snort

HOST SECURITY

- OS hardening
- Patch management