SOMMAIRE

VII– **Réseaux, Sécurité, SAN**

Interconnecting Cisco Network Devices Part 1 [ICND1]

Objectifs :

Installer, configurer et exploiter un réseau de petite ou moyenne taille, cette formation Cisco officielle prépare à la certification 640-822 (ICND1 : 100-105)

Prérequis

avoir des connaissances de base des réseaux, des compétences de base sur la navigation du système d'exploitation pour PC, Internet .

Participants

administrateurs ré-

Programme

5 jours

Création d'un réseau simple
Explorer les fonctions d'un réseau
Comprendre le modèle de communication Host-to-Host
Introduction des réseaux LANs
Fonctionnement de l'exploitation Cisco IOS
Démarrage d'un Switch
Comprendre le fonctionnement d'Ethernet et d'un Switch
Dépannage des problèmes de commutation liés aux médias

Établissement d'une connectivité Internet
Comprendre le protocole TCP / IP Couche Internet
Comprendre l'adressage IP et la notion de sous-réseaux
Comprendre la couche transport TCP/IP
Explorer les fonctions de routage
Configurer un routeur Cisco 2.6
Explorer le processus de délivrance des paquets
Configurer le routage statique
Apprendre les bases de l'ACLs
Activer la connectivité à Internet

Résumé challenge 1 &2
Etablir une connectivité à Internet
Dépanner une connectivité à Internet

Construire un réseau de taille moyenne
Implémenter les VLANs et Trunks
Routage entre les VLANs
Utiliser un périphérique réseau Cisco en tant que serveur DHCP
Implémenter RIPv2
Présenter les protocoles du routage dynamique

Gestion des périphériques réseau et sécurité
Sécuriser les accès administratifs
Mettre en oeuvre le device hardening
Configurer la journalisation du système de messagerie
Gérer les périphériques Cisco
Licences

Résumé challenge 4 & 5
Implémenter un réseau taille moyenne
Dépanner un réseau de taille moyenne

Présentation de l'IPv6
Présenter les bases IPv6
Configurer le routage IPv6
Configurer le routage statique IPv6

Interconnecting Cisco Network Devices Part 2 [ICND2]

Objectifs :

installer, dépanner et sécurisé un réseau de taille moyenne, y compris la, connexion à un réseau WAN , cette formation Cisco officielle permet de passer l'examen 200-105 (ICND2) ou CCNA Routing and Switching (200-125)

Prérequis

Suivre le cours ICND1

Participants

techniciens et ingénieurs réseaux respon-

Programme

5 jours

Mise en oeuvre des réseaux de taille moyenne
Dépanner la connectivité VLAN
Créer des topologies commutées redondantes
Améliorer les topologies commutées redondantes avec EtherChannel
Comprendre la redondance de niveau 3

Dépannage de la connectivité de base
Dépanner la connectivité du réseau IPv4
Dépanner la connectivité du réseau IPv6

Mise en oeuvre d'une architecture EIGRP
Mettre en oeuvre EIGRP
Dépanner EIGRP
Mettre en oeuvre EIGRP pour IPv6
Résumé challenge
Implémenter et dépanner des réseaux de taille moyenne

Mise en oeuvre d'une architecture OSPF
Comprendre OSPF
Mettre en oeuvre OSPF multi aires IPv4
Mettre en oeuvre OSPFv3 pour IPv6
Dépanner OSPF multi aires

Réseaux WAN – Wide-Area Networks
Comprendre les technologies WAN
Comprendre le protocole point par point
Configurer les tunnels GRE
Configurer Single-Homed EBGP

Gestion des périphériques réseaux
Mettre en oeuvre la gestion et la sécurité des périphériques réseaux
Evolution des réseaux intelligents
Introduction à QOS

Résumé challenge
Implémenter et dépanner les réseaux multi aires

Implementing Cisco Network Security (IINS) , CCNA Network Security

Objectifs :

Maîtriser les concepts de sécurité réseau et d'analyse de risque

Construire une infrastructure réseau sécurisée, Défendre le réseau via les pare-feu Cisco

Mettre en place un VPN, Se préparer à l'examen 640-554 IINS

Prérequis

Ingénieur/ administrateur et technicien réseaux.

Participants

Programme — 5 jours

Introduction aux principes de sécurité réseau

- Les fondamentaux de la sécurité réseau
- Comprendre les stratégies de sécurité avec une approche Life-Cycle

Construire une stratégie de sécurité pour les réseaux Borderless

Protéger l'infrastructure réseau

- Introduction à la protection des réseaux Cisco
- Protéger l'infrastructure réseau avec Cisco Configuration Professional
- Sécuriser le plan de manager sur l'IOS Cisco
- Configurer le AAA avec Cisco Secure ACS (Access Control Server)
- Sécuriser le plan de données sur les switches Catalyst

Sécuriser le plan de données dans les environnements IPV6

Contrôle et maîtrise des menaces

- Planifier une stratégie de contrôle des menaces
- Implémenter des listes de contrôle d'accès pour limiter les menaces
- Comprendre les fondamentaux des pare-feux
- Mettre en oeuvre les stratégies de pare-feux en mode Zone-Based
- Configurer les stratégies de base des pare-feux sur le matériel Cisco ASA

Comprendre les fondamentaux d'IPS · Implémenter Cisco IOS IPS

Connectivité sécurisée

- Comprendre les fondamentaux des technologies VPN
- Introduction aux infrastructures de clés publiques
- Présentation des fondamentaux d'IPsec
- Implémenter les VPN site à site sur les routeurs Cisco IOS

Cisco - Firewall ASA - Mise en œuvre

Objectifs :

Connaître et assimiler les fonctionnalités du firewall Cisco ASA

Avoir une bonne maîtrise de l'installation et de la configuration des firewalls Cisco ASA .

Prérequis

Avoir de bonnes connaissances des réseaux et de la sécurité informatique.

Participants

Ingénieurs, techniciens et administrateurs réseaux et télécoms..

Programme — 5 jours

Introduction aux firewalls

- La technologie pare-feu et les caractéristiques
- L'architecture et les niveaux de sécurité

La configuration et les fonctionnalités

Translation et connexions

- Le NAT statique, dynamique et PAT
- Les connexions établies et les redirections de ports

La configuration DMZ

Liste de contrôle d'accès

- Le filtrage IP
- Le filtrage d'URL
- L'inspection "statefull"

L'inspection applicative

Authentification et autorisations

- L'authentification et les autorisations
- Le protocole RADIUS
- Le protocole TACACS

L'application des ACL

VPN (Virtual Private Network)

- Le VPN site à site via IPSEC
- Le VPN poste à site IPSEC avec client lourd

Le VPN poste à site TLS avec client lége

Routage avec firewall

- Le routage statique et dynamique

Le firewall en mode transparent

Redondance de firewall

- Le mode Failover
- La redondance de configuration

Le mode actif / actif

Opérations de mainte-

Certified Ethical Hacker v9

Objectifs :

vous aider à maîtriser une méthodologie de piratage éthique qui pourra aussi bien être utilisée dans un test d'intrusion que dans une situation de piratage éthique. préparer la certification CeH.

Prérequis

Connaissances basiques de TCP/ IP, Linux et Windows Server .

Participants

Responsables informatique ou de la sécurité

Programme

5 jours

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Hacking Webservers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- Evading IDS, Firewalls and Honeypots
- Cloud Computing

Cryptography

Certifications :

CEHV8 312-50

Computer Hacking Forensic Investigator v8

Objectifs :

Avoir les qualifications nécessaires pour identifier et analyser les traces laissées lors de l'intrusion d'un système informatique par un tiers et pour collecter correctement les preuves nécessaires à des poursuites judiciaires, Se préparer à l'examen CHFI 312-49

Prérequis

CEH v8.

Participants

Professionnels IT chargé de la sécurité

Programme

5 jours

- Module 1 : L'investigation légale dans le monde d'aujourd'hui
- Module 2 : Procédés d'investigation informatique
- Module 3 : Recherche et Saisie de PC
- Module 4 : Preuve numérique
- Module 5 : Procédure "First Responder"
- Module 6 : Laboratoire d'investigation légale
- Module 7 : Comprendre les systèmes de fichiers et les disques durs
- Module 8 : Investigation légale sous Windows
- Module 9 : Collecte de données et duplication
- Module 10 : Retrouver des fichiers et des partitions supprimés
- Module 11 : Investigation légale en utilisant AccessData FTK
- Module 12 : Investigation légale en utilisant EnCase
- Module 13 : Sténographie et investigation légale dans les fichiers d'image
- Module 14 : Application de crackage de mots de passe
- Module 15 : Capture de logs et corrélation d'évènements
- Module 16 : Investigation légale dans les réseaux et utilisation des journaux de logs à des fins d'investigation

Certifications :

CHFIv8 (312-49)

Kaspersky Endpoint Security and Management

Objectifs :

Describe the capabilities of Kaspersky Endpoint Security for Windows and Kaspersky Security Center, Plan and implement an optimal Windows network protection solution .

Prérequis

basic skills in administering Microsoft Windows networks and AD

Participants

Microsoft Windows network administra-

Programme

3 jours

Unit I. Deployment

- Chapter 1. Organizational Issues
- Chapter 2. Installation of Kaspersky Security Center
- Chapter 3. Installation on Computers

Chapter 4. Management of Computer Structure
Unit II. Protection Management

- Chapter 1. Basics of Kaspersky Endpoint Security
- Chapter 2. File System Protection
- Chapter 3. Network Protection
- Chapter 4. Proactive Defence
- Chapter 5. Threat Diagnostics

Chapter 6. Protection Status Diagnostics
Unit III. Control

- Chapter 1. General
- Chapter 2. Application Startup Control
- Chapter 3. Application Privilege Control
- Chapter 4. Device Control

Chapter 5. Web Control
Unit IV. Maintenance

- Chapter 1. License Management
- Chapter 2. Updates
- Chapter 3. Roaming Computer Management
- Chapter 4. Interaction with User
- Chapter 5. Backup and Restore

Chapter 6. Statistics and Reports
Unit V. Advanced Skills

- Chapter 1. Traffic Management
- Chapter 2. Update Agents and Connection Gateways
- Chapter 3. Using Several Administration Servers
- Chapter 4. Managing Administrators

Chapter 5. Special Features

Veritas NetBackup 7.5 for UNIX and Windows: Advanced Administration

Objectifs : advanced NetBackup functionality : deduplication, performance, disaster recovery, virtual machine backups, security. manage Oracle, Microsoft Exchange, and SQL database backups.

Prérequis : three years experience with basic NetBackup administration..

Participants: system administrators, system engineers, technical support.

Programme

4 jours

NetBackup Concepts Review

- Reviewing the NetBackup environment
- Reviewing NetBackup concepts

Reviewing NetBackup administrative interfaces

Managing NetBackup Deduplication

- Introduction to NetBackup deduplication
- Configuring NetBackup media server deduplication
- Configuring client-side deduplication

Managing NetBackup media server deduplication

Improving NetBackup Performance

- NetBackup performance overview
- Isolating bottlenecks
- Addressing bottlenecks
- Tuning NetBackup buffers

Using NetBackup Accelerator

Advanced Disaster Recovery Strategies

- Disaster recovery strategies
- Optimized duplication
- Introduction to Replication Director

Disaster recovery for the NetBackup infrastructure

Using Auto Image Replication for Disaster Recovery

Managing Virtual Machine Backups

Application Backup Concepts

Managing Oracle Backups

Oracle databases

Managing Microsoft SQL Backups