Security

Implementing and Operating Cisco Security Core Technologies

SCOR

Version : 1.0
5 Jours

Objectifs

A l'issue de ce cours, le stagiaire sera en mesure d'atteindre ses objectifs :

- Décrire les concepts et stratégies de sécurité de l'information au sein du réseau
- Décrire les attaques TCP / IP, les applications réseau et les points de terminaison courantes
- Décrire comment diverses technologies de sécurité réseau fonctionnent ensemble pour se prémunir contre les attaques
- Mettre en œuvre le contrôle d'accès sur l'appliance Cisco ASA et le pare-feu Cisco Firepower nouvelle génération
- Décrire et implémenter les fonctions et fonctions de sécurité de base du contenu de messagerie fournies par Cisco Email Security Appliance
- Décrire et implémenter les fonctionnalités et fonctions de sécurité du contenu Web fournies par Cisco Web Security Appliance
- Décrire les capacités de sécurité de Cisco Umbrella®, les modèles de déploiement, la gestion des politiques et la console Investigate
- Présenter les VPN et décrire les solutions et algorithmes de cryptographie
- Décrire les solutions de connectivité sécurisée de site à site de Cisco et expliquer comment déployer les VPN IPsec point à point basés sur l'interface de tunnel virtuel Cisco IOS® (Cisco IOS®) et le VPN IPsec point à point sur le Pare-feu Cisco ASA et Cisco Firepower nouvelle génération (NGFW)
- Décrire et déployer des solutions de connectivité d'accès distant sécurisé Cisco et décrire comment configurer l'authentification 802.1X et le protocole EAP (Extensible Authentication Protocol)
- Fournir une compréhension de base de la sécurité des terminaux et décrire la protection avancée contre les logiciels malveillants (AMP) pour l'architecture des terminaux et les fonctionnalités de base
- Examiner diverses défenses sur les appareils Cisco qui protègent le plan de contrôle et de gestion
- Configurez et vérifiez les contrôles du plan de données des couches 2 et 3 du logiciel Cisco IOS
- Décrire les solutions Cisco Stealthwatch Enterprise et Stealthwatch Cloud
- Décrire les bases du cloud computing et des attaques cloud courantes et comment sécuriser l'environnement cloud

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

Public Concerné

- Ingénieur sécurité
- Ingénieur réseau
- Concepteur de réseau
- Administrateur réseau
- Ingénieur Systèmes
- Ingénieur conseil en systèmes
- Architecte de solutions techniques
- Gestionnaire de réseau
- Intégrateurs et partenaires Cisco

Pré-requis

Avant de suivre ce cours, le stagiaire doit posséder les compétences et les connaissances suivantes :

- Compétences et connaissances équivalentes à celles acquises dans le cours de mise en œuvre et d'administration des solutions Cisco (CCNA ®) v1.0
- Connaissance des réseaux Ethernet et TCP / IP
- Connaissance pratique du système d'exploitation Windows
- Connaissance pratique des réseaux et des concepts Cisco IOS
- Familiarité avec les bases des concepts de sécurité réseau
- Implementing and Administering Cisco Solutions (CCNA)

Plan du cours détaillé

1. Décrire les concepts de sécurité de l'information *
   1.1. Présentation de la sécurité des informations
   1.2. Actifs, vulnérabilités et contre-mesures
   1.3. Gérer les risques
   1.4. Évaluation de la vulnérabilité
   1.5. Comprendre le système Common Vulnerability Scoring System (CVSS)

2. Décrire les attaques TCP / IP courantes *
   2.1. Vulnérabilités TCP / IP héritées
   2.2. Vulnérabilités IP
   2.3. Vulnérabilités ICMP (Internet Control Message Protocol)
   2.4. Vulnérabilités TCP
   2.5. Vulnérabilités du protocole UDP (User Datagram Protocol)
   2.6. Surface d'attaque et vecteurs d'attaque
   2.7. Attaques de reconnaissance
   2.8. Attaques d'accès
   2.9. Attaques de l'homme du milieu

2.10. Attaques par déni de service et déni de service distribué
2.11. Attaques de réflexion et d'amplification
2.12. Attaques d'usurpation d'identité
2.13. Attaques DHCP (Dynamic Host Configuration Protocol)

3. Décrire les attaques d'applications réseau courantes *
   3.1. Attaques par mot de passe
   3.2. Attaques basées sur le système de noms de domaine (DNS)
   3.3. Tunneling DNS
   3.4. Attaques basées sur le Web
   3.5. Amortissement HTTP 302
   3.6. Injections de commandes
   3.7. Injections SQL
   3.8. Scriptage intersite et falsification de demande
   3.9. Attaques par courrier électronique

4. Décrire les attaques de point de terminaison courantes *
   4.1. Débordement de tampon
   4.2. Malware
   4.3. Attaque de reconnaissance
   4.4. Accès et contrôle
   4.5. Accès via l'ingénierie sociale
   4.6. Accès via des attaques basées sur le Web
   4.7. Kits d'exploitation et rootkits
   4.8. Escalade de privilèges
   4.9. Phase de post-exploitation
   4.10. Angler Exploit Kit

5. Décrire les technologies de sécurité réseau
   5.1. Stratégie de défense en profondeur
   5.2. Défendre à travers le continuum d'attaque
   5.3. Présentation de la segmentation du réseau et de la virtualisation
   5.4. Présentation du pare-feu dynamique
   5.5. Présentation de Security Intelligence
   5.6. Normalisation des informations sur les menaces
   5.7. Présentation de la protection contre les logiciels malveillants en réseau
   5.8. Présentation du système de prévention des intrusions (IPS)
   5.9. Présentation du pare-feu nouvelle génération
   5.10. Présentation de la sécurité du contenu des e-mails
   5.11. Présentation de la sécurité du contenu Web
   5.12. Présentation des systèmes d'analyse des menaces
   5.13. Présentation de la sécurité DNS
   5.14. Présentation de l'authentification, de l'autorisation et de la comptabilité
   5.15. Présentation de la gestion des identités et des accès
   5.16. Présentation de la technologie de réseau privé virtuel

5.17. Présentation des facteurs de forme des périphériques de sécurité réseau

6. Déployer le pare-feu Cisco ASA

6.1. Types de déploiement Cisco ASA
6.2. Niveaux de sécurité de l'interface Cisco ASA
6.3. Objets et groupes d'objets Cisco ASA
6.4. Traduction d'adresses réseau
6.5. Listes de contrôle d'accès à l'interface Cisco ASA (ACL)
6.6. ACL mondiales Cisco ASA
6.7. Stratégies d'accès avancées de Cisco ASA
6.8. Présentation de la haute disponibilité Cisco ASA

7. Déploiement du pare-feu Cisco Firepower nouvelle génération

7.1. Déploiements Cisco Firepower NGFW
7.2. Traitement et politiques des paquets Cisco Firepower NGFW
7.3. Objets Cisco Firepower NGFW
7.4. Traduction d'adresse réseau (NAT) Cisco Firepower NGFW
7.5. Stratégies de préfiltre Cisco Firepower NGFW
7.6. Stratégies de contrôle d'accès Cisco Firepower NGFW
7.7. Intelligence de sécurité Cisco Firepower NGFW
7.8. Stratégies de découverte de Cisco Firepower NGFW
7.9. Stratégies IPS de Cisco Firepower NGFW
7.10. Stratégies de programmes malveillants et de fichiers Cisco Firepower NGFW

8. Déploiement de la sécurité du contenu des e-mails

8.1. Présentation de Cisco Email Content Security
8.2. Présentation du protocole SMTP (Simple Mail Transfer Protocol)
8.3. Présentation du pipeline de messagerie
8.4. Auditeurs publics et privés
8.5. Présentation de la table d'accès à l'hôte
8.6. Présentation de la table d'accès des destinataires
8.7. Présentation des stratégies de messagerie
8.8. Protection contre le spam et Graymail
8.9. Protection antivirus et anti-malware
8.10. Filtres anti-épidémies
8.11. Filtres de contenu
8.12. Prévention contre la perte de données
8.13. Cryptage des e-mails

9. Déployer la sécurité du contenu Web

9.1. Présentation de l'appliance de sécurité Web Cisco (WSA)
9.2. Options de déploiement
9.3. Authentification des utilisateurs du réseau
9.4. Déchiffrement du trafic HTTP sécurisé (HTTPS)
9.5. Stratégies d'accès et profils d'identification

9.6. Paramètres des contrôles d'utilisation acceptable
9.7. Protection anti-malware

10. Déploiement de Cisco Umbrella *
    10.1. Architecture de parapluie Cisco
    10.2. Déployer Cisco Umbrella
    10.3. Client itinérant Cisco Umbrella
    10.4. Gérer Cisco Umbrella
    10.5. Présentation et concepts de Cisco Umbrella Investigate

11. Expliquer les technologies VPN et la cryptographie
    11.1. Définition VPN
    11.2. Types de VPN
    11.3. Communication sécurisée et services cryptographiques
    11.4. Clés en cryptographie
    11.5. Infrastructure à clé publique

12. Présentation des solutions VPN sécurisées de site à site de Cisco
    12.1. Topologies VPN de site à site
    12.2. Présentation du VPN IPsec
    12.3. Cartes cryptographiques statiques IPsec
    12.4. Interface de tunnel virtuel statique IPsec
    12.5. VPN multipoint dynamique
    12.6. Cisco IOS FlexVPN

13. Déploiement de VPN IPsec point à point basés sur Cisco IOS VTI
    13.1. VTI Cisco IOS
    13.2. Configuration VPN v2 point à point IPsec Internet Key Exchange (IKE) statique

14. Déploiement de VPN IPsec point à point sur Cisco ASA et Cisco Firepower NGFW
    14.1. VPN point à point sur Cisco ASA et Cisco Firepower NGFW
    14.2. Configuration VPN point à point Cisco ASA
    14.3. Configuration VPN point à point Cisco Firepower NGFW

15. Présentation des solutions VPN d'accès sécurisé à distance Cisco
    15.1. Composants VPN d'accès à distance
    15.2. Technologies VPN d'accès à distance
    15.3. Présentation de Secure Sockets Layer (SSL)

16. Déploiement de VPN SSL d'accès à distance sur Cisco ASA et Cisco Firepower NGFW
    16.1. Concepts de configuration de l'accès à distance
    16.2. Profils de connexion
    16.3. Stratégies de groupe
    16.4. Configuration VPN d'accès distant Cisco ASA

16.5. Configuration VPN d'accès à distance Cisco Firepower NGFW

17. Explication des solutions Cisco Secure Network Access

17.1. Accès réseau sécurisé Cisco
17.2. Composants d'accès sécurisé au réseau Cisco
17.3. Rôle AAA dans la solution Cisco Secure Network Access
17.4. Moteur de services d'identité Cisco
17.5. Cisco wisdomec

18. Décrire l'authentification 802.1X

18.1. 802.1X et EAP (Extensible Authentication Protocol)
18.2. Méthodes EAP
18.3. Rôle du service utilisateur d'accès à distance par authentification à distance (RADIUS) dans les communications 802.1X
18.4. Changement d'autorisation RADIUS

19. Configuration de l'authentification 802.1X

19.1. Configuration du commutateur Cisco Catalyst® 802.1X
19.2. Configuration du contrôleur LAN sans fil Cisco (WLC) 802.1X
19.3. Configuration de Cisco Identity Services Engine (ISE) 802.1X
19.4. Configuration Supplicant 802.1x
19.5. Authentification Web centrale Cisco

20. Décrire les technologies Endpoint Security *

20.1. Pare-feu personnel basé sur l'hôte
20.2. Anti-virus basé sur l'hôte
20.3. Système de prévention des intrusions basé sur l'hôte
20.4. Listes blanches et listes noires des applications
20.5. Protection contre les programmes malveillants basés sur l'hôte
20.6. Présentation de Sandboxing
20.7. Vérification de l'intégrité des fichiers

21. Déploiement de Cisco Advanced Malware Protection (AMP) for Endpoints *

21.1. Cisco AMP for Endpoints Architecture
21.2. Cisco AMP for Endpoints Engines
21.3. Sécurité rétrospective avec Cisco AMP
21.4. Trajectoire des périphériques et fichiers Cisco AMP
21.5. Gestion de Cisco AMP pour les points de terminaison

22. Présentation de la protection de l'infrastructure réseau *

22.1. Identification des plans des périphériques réseau
22.2. Contrôles de sécurité du plan de contrôle
22.3. Contrôles de sécurité du plan de gestion
22.4. Télémétrie réseau
22.5. Contrôles de sécurité du plan de données de couche 2

22.6. Contrôles de sécurité du plan de données de couche 3

23. Déploiement des contrôles de sécurité du plan de contrôle *
    23.1. ACL d'infrastructure
    23.2. Contrôle du plan de contrôle
    23.3. Protection du plan de contrôle
    23.4. Sécurité du protocole de routage

24. Déploiement des contrôles de sécurité du plan de données de couche 2 *
    24.1. Présentation des contrôles de sécurité du plan de données de couche 2
    24.2. Atténuation des attaques basée sur le LAN virtuel (VLAN)
    24.3. Atténuation des attaques par le protocole STP (Spanning Tree Protocol)
    24.4. Sécurité portuaire
    24.5. VLAN privés
    24.6. Surveillance du protocole DHCP (Dynamic Host Configuration Protocol)
    24.7. Inspection du protocole de résolution d'adresse (ARP)
    24.8. Contrôle des tempêtes
    24.9. Chiffrement MACsec

25. Déploiement des contrôles de sécurité du plan de données de couche 3 *
    25.1. ACL d'infrastructure antispoofing
    25.2. Transfert de chemin inverse unicast
    25.3. IP Source Guard

26. Déploiement des contrôles de sécurité du plan de gestion *
    26.1. Accès de gestion sécurisé Cisco
    26.2. Protocole de gestion de réseau simple version 3
    26.3. Accès sécurisé aux appareils Cisco
    26.4. AAA pour l'accès à la gestion

27. Déploiement des méthodes de télémétrie du trafic *
    27.1. Protocole de temps réseau
    27.2. Journalisation et exportation des événements de périphérique et de réseau
    27.3. Surveillance du trafic réseau à l'aide de NetFlow

28. Déploiement de Cisco Stealthwatch Enterprise *
    28.1. Présentation des offres Cisco Stealthwatch
    28.2. Composants requis pour Cisco Stealthwatch Enterprise
    28.3. Assemblage de flux et déduplication
    28.4. Composants facultatifs de Stealthwatch Enterprise
    28.5. Stealthwatch Enterprise et intégration ISE
    28.6. Cisco Stealthwatch avec Cognitive Analytics
    28.7. Analyse du trafic crypté Cisco
    28.8. Groupes hôtes
    28.9. Événements et alarmes de sécurité

28.10. Hôte, rôle et stratégies par défaut

29. Décrire les attaques Cloud et Common Cloud *
    29.1. Evolution du cloud computing
    29.2. Modèles de service cloud
    29.3. Responsabilités de sécurité dans le cloud
    29.4. Modèles de déploiement cloud
    29.5. Menaces de sécurité courantes dans le cloud
    29.6. Gestion des correctifs dans le cloud
    29.7. Évaluation de la sécurité dans le cloud

30. Sécuriser le cloud *
    30.1. Approche centrée sur les menaces de Cisco en matière de sécurité réseau
    30.2. Sécurité de l'environnement physique du cloud
    30.3. Sécurité des applications et de la charge de travail
    30.4. Gestion du cloud et sécurité des API
    30.5. Virtualisation de la fonction réseau (NFV) et fonctions de réseau virtuel (VNF)
    30.6. Exemples Cisco NFV
    30.7. Rapports et visibilité des menaces dans le cloud
    30.8. Courtier de sécurité d'accès au cloud
    30.9. Cisco CloudLock®
    30.10. Attaques OAuth et OAuth

31. Déploiement de Cisco Stealthwatch Cloud *
    31.1. Cisco Stealthwatch Cloud pour la surveillance du cloud public
    31.2. Cisco Stealthwatch Cloud pour la surveillance de réseaux privés
    31.3. Opérations dans le cloud de Cisco Stealthwatch

32. Décrire le réseau défini par logiciel (SDN *)
    32.1. Concepts de mise en réseau définis par logiciel
    32.2. Programmabilité et automatisation du réseau
    32.3. Plateformes et API Cisco
    32.4. Scripts de base Python pour l'automatisation

* Cette section est du matériel d'autoformation qui peut être fait à votre propre rythme si vous suivez la version dirigée par un instructeur de ce cours.

Laboratoire

- Configurer les paramètres réseau et NAT sur Cisco ASA
- Configurez les stratégies de contrôle d'accès de Cisco ASA
- Configurez le Cisco Firepower NGFW NAT
- Configurez la stratégie de contrôle d'accès de Cisco Firepower NGFW

- Configurer Cisco Firepower NGFW Discovery et IPS Policy
- Configurez la politique de malware et de dossier de Cisco NGFW
- Configurez l'écouteur, la table d'accès d'hôte (HAT) et la table d'accès de destinataire (RAT) sur l'appliance de sécurité du courrier électronique de Cisco (ESA)
- Configurer les politiques de messagerie
- Configurer les services proxy, l'authentification et le déchiffrement HTTPS
- Appliquer le contrôle d'utilisation acceptable et la protection contre les logiciels malveillants
- Examinez le tableau de bord du parapluie
- Examiner Cisco Umbrella Investigate
- Explorez la protection DNS contre les ransomwares par Cisco Umbrella
- Configurer un tunnel IKEv2 IPsec point à point VTI statique
- Configurez le VPN point à point entre Cisco ASA et Cisco Firepower NGFW
- Configurez le VPN d'accès à distance sur le Cisco Firepower NGFW
- Explorez Cisco AMP for Endpoints
- Effectuer une analyse de point final à l'aide d'AMP pour la console Endpoints
- Explorez File Ransomware Protection par Cisco AMP pour Endpoints Console
- Découvrez Cisco Stealthwatch Enterprise v6.9.3
- Explorez Cognitive Threat Analytics (CTA) dans Stealthwatch Enterprise v7.0
- Explorez le tableau de bord Cisco Cloudlock et la sécurité des utilisateurs
- Explorez Cisco Cloudlock Application and Data Security
- Explorez Cisco Stealthwatch Cloud
- Explorez les paramètres d'alerte, les listes de surveillance et les capteurs Stealthwatch Cloud