Security

Securing Email with Cisco Email Security Appliance

SESA

Version : 3.1
4 Jours

Objectifs

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

- Décrire et administrer l'appliance de sécurité de messagerie Cisco (ESA)
- Contrôler les domaines émetteur et destinataire
- Contrôlez le spam avec Talos SenderBase et anti-spam
- Utiliser des filtres antivirus et anti-épidémies
- Utiliser des politiques de messagerie
- Utiliser des filtres de contenu
- Utiliser des filtres de messages pour appliquer les politiques de messagerie
- Empêcher la perte de données
- Effectuer des requêtes LDAP
- Authentifier les sessions SMTP (Simple Mail Transfer Protocol)
- Authentifier l'e-mail
- Crypter les e-mails
- Utiliser des quarantaines système et des méthodes de livraison
- Effectuer une gestion centralisée à l'aide de clusters
- Tester et dépanner

Public Concerné

- Ingénieurs sécurité
- Administrateurs de sécurité
- Architectes de sécurité
- Ingénieurs d'exploitation
- Ingénieurs réseau
- Administrateurs réseau
- Techniciens réseau ou sécurité
- Gestionnaires de réseau
- Concepteurs de systèmes
- Intégrateurs et partenaires Cisco

Pré-requis

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

- Avoir des connaissances sur les fondamentaux TCP/IP

- Avoir de l'expérience dans la messagerie Internet, incluant SMTP, les formats de messages Internet et les formats de messages MIME
- Le niveau de connaissances de la certification CCNA est recommandé.

Plan du cours détaillé

1. Décrire l'appliance de sécurité de messagerie Cisco
   - 1.1. Présentation de l'appliance de sécurité de messagerie Cisco
   - 1.2. Cas d'utilisation de la technologie
   - 1.3. Fiche technique de l'appliance de sécurité de messagerie Cisco
   - 1.4. Présentation de SMTP
   - 1.5. Présentation du pipeline de messagerie
   - 1.6. Scénarios d'installation
   - 1.7. Configuration initiale de Cisco Email Security Appliance
   - 1.8. Centraliser les services sur une appliance de gestion de la sécurité du contenu Cisco (SMA)
   - 1.9. Notes de version pour AsyncOS 11.x
2. Administration de Cisco Email Security Appliance
   - 2.1. Distribution des tâches administratives
   - 2.2. L'administration du système
   - 2.3. Gestion et surveillance à l'aide de l'interface de ligne de commande (CLI)
   - 2.4. Autres tâches dans l'interface graphique
   - 2.5. Configuration réseau avancée
   - 2.6. Utilisation de Email Security Monitor
   - 2.7. Messages de suivi
   - 2.8. Enregistrement
3. Contrôle des domaines expéditeur et destinataire
   - 3.1. Auditeurs publics et privés
   - 3.2. Configuration de la passerelle pour recevoir des e-mails
   - 3.3. Présentation de la table d'accès à l'hôte
   - 3.4. Présentation de la table d'accès des destinataires
   - 3.5. Configuration des fonctionnalités de routage et de livraison
4. Contrôle du spam avec Talos SenderBase et Anti-Spam
   - 4.1. Présentation de SenderBase
   - 4.2. Anti-spam
   - 4.3. Gérer Graymail
   - 4.4. Protection contre les URL malveillantes ou indésirables
   - 4.5. Filtrage de la réputation des fichiers et analyse des fichiers
   - 4.6. Vérification du rebond
5. Utilisation de filtres antivirus et anti-épidémies
   - 5.1. Présentation de l'analyse antivirus

5.2. Filtrage antivirus Sophos
5.3. Filtrage antivirus McAfee
5.4. Configuration de l'appliance pour rechercher les virus
5.5. Filtres anti-épidémies
5.6. Fonctionnement de la fonction Filtres anti-épidémies
5.7. Gestion des filtres d'épidémie

6. Utilisation des stratégies de messagerie

6.1. Présentation de Email Security Manager
6.2. Présentation des stratégies de messagerie
6.3. Gestion différente des messages entrants et sortants
6.4. Faire correspondre les utilisateurs à une stratégie de messagerie
6.5. Éclatement de message
6.6. Configuration des politiques de messagerie

7. Utilisation de filtres de contenu

7.1. Présentation des filtres de contenu
7.2. Conditions de filtrage du contenu
7.3. Actions de filtrage de contenu
7.4. Filtrer les messages en fonction du contenu
7.5. Présentation des ressources textuelles
7.6. Utilisation et test des règles de filtrage des dictionnaires de contenu
7.7. Comprendre les ressources textuelles
7.8. Gestion des ressources textuelles
7.9. Utilisation des ressources textuelles

8. Utilisation de filtres de messages pour appliquer des stratégies de messagerie

8.1. Présentation des filtres de messages
8.2. Composants d'un filtre de messages
8.3. Traitement du filtre des messages
8.4. Règles de filtrage des messages
8.5. Actions de filtrage des messages
8.6. Numérisation des pièces jointes
8.7. Exemples de filtres de messages d'analyse des pièces jointes
8.8. Utilisation de la CLI pour gérer les filtres de messages
8.9. Exemples de filtres de messages
8.10. Configuration du comportement de scan

9. Prévenir la perte de données

9.1. Présentation du processus de numérisation DLP (Data Loss Prevention)
9.2. Configuration de la prévention de la perte de données
9.3. Stratégies de prévention de la perte de données
9.4. Actions de message
9.5. Mise à jour du moteur DLP et des classificateurs de correspondance de contenu

10. Utilisation de LDAP

10.1. Présentation de LDAP
10.2. Travailler avec LDAP
10.3. Utilisation de requêtes LDAP
10.4. Authentification des utilisateurs finaux de la quarantaine de spam
10.5. Configuration de l'authentification LDAP externe pour les utilisateurs
10.6. Test des serveurs et des requêtes
10.7. Utilisation de LDAP pour la prévention des attaques de récolte d'annuaire
10.8. Requêtes de consolidation d'alias de quarantaine de spam
10.9. Validation des destinataires à l'aide d'un serveur SMTP

11. Authentification de session SMTP

11.1. Configuration d'AsyncOS pour l'authentification SMTP
11.2. Authentification des sessions SMTP à l'aide de certificats clients
11.3. Vérification de la validité d'un certificat client
11.4. Authentification de l'utilisateur à l'aide de l'annuaire LDAP
11.5. Authentification de la connexion SMTP via TLS (Transport Layer Security) à l'aide d'un certificat client
11.6. Etablissement d'une connexion TLS à partir de l'appliance
11.7. Mise à jour d'une liste de certificats révoqués

12. Authentification par courriel

12.1. Présentation de l'authentification des e-mails
12.2. Configuration de la signature DomainKeys et DomainKeys Identified Mail (DKIM)
12.3. Vérification des messages entrants à l'aide de DKIM
12.4. Présentation du Sender Policy Framework (SPF) et de la vérification SIDF
12.5. Vérification des rapports et de la conformité de l'authentification des messages basée sur le domaine (DMARC)
12.6. Détection des e-mails falsifiés

13. Cryptage des e-mails

13.1. Vue d'ensemble de Cisco Email Encryption
13.2. Chiffrement des messages
13.3. Détermination des messages à chiffrer
13.4. Insertion d'en-têtes de chiffrement dans les messages
13.5. Cryptage des communications avec d'autres agents de transfert de messages (MTA)
13.6. Travailler avec des certificats
13.7. Gestion des listes d'autorités de certification
13.8. Activation de TLS sur la table d'accès à l'hôte d'un auditeur (HAT)
13.9. Activation de TLS et de la vérification des certificats à la livraison
13.10. Services de sécurité S / MIME (Secure Internet Multipurpose Internet Extensions)

14. Utilisation des quarantaines système et des méthodes de livraison

14.1. Décrire les quarantaines
14.2. Spam Quarantine
14.3. Configuration de la quarantaine de spam centralisée
14.4. Utilisation de listes fiables et de listes de blocage pour contrôler la remise des e-mails en fonction de l'expéditeur
14.5. Configuration des fonctionnalités de gestion du spam pour les utilisateurs finaux
14.6. Gestion des messages dans la quarantaine de spam
14.7. Stratégie, virus et quarantaines d'épidémies
14.8. Gestion des quarantaines de stratégie, de virus et d'épidémie
14.9. Utilisation des messages dans les quarantaines de stratégie, de virus ou d'épidémie
14.10. Modes de livraison

15. Gestion centralisée à l'aide de clusters

15.1. Présentation de la gestion centralisée à l'aide de clusters
15.2. Organisation du cluster
15.3. Créer et rejoindre un cluster
15.4. Gérer les clusters
15.5. Communication de cluster
15.6. Chargement d'une configuration dans des appliances en cluster
15.7. Les meilleures pratiques

16. Test et dépannage

16.1. Débogage du flux de messagerie à l'aide de messages de test: trace
16.2. Utilisation de l'écouteur pour tester l'appliance
16.3. Dépannage du réseau
16.4. Dépannage de l'écouteur
16.5. Dépannage de la remise des e-mails
16.6. Dépannage des performances
16.7. Problèmes d'apparence et de rendu de l'interface Web
16.8. Répondre aux alertes
16.9. Dépannage des problèmes matériels
16.10. Travailler avec le support technique

17. Les références

17.1. Spécifications du modèle pour les grandes entreprises
17.2. Spécifications de modèle pour les entreprises de taille moyenne et les petites ou moyennes entreprises ou succursales
17.3. Spécifications du modèle d'appliance de sécurité de messagerie Cisco pour les appliances virtuelles
17.4. Forfaits et licences

Laboratoire

- Vérifiez et testez la configuration de Cisco ESA
- Effectuer l'administration de base
- Logiciels malveillants avancés dans les pièces jointes (détection de macros)
- Protection contre les URL malveillantes ou indésirables sous les URL raccourcies
- Protection contre les URL malveillantes ou indésirables dans les pièces jointes
- Gérez intelligemment les messages non analysables
- Exploitez AMP Cloud Intelligence via une amélioration de la pré-classification
- Intégrez Cisco ESA à la console AMP
- Prévenez les menaces grâce à la protection antivirus
- Application de filtres de contenu et d'épidémie
- Configurer l'analyse des pièces jointes
- Configurer la prévention de la perte de données sortantes
- Intégrez Cisco ESA à LDAP et activez la requête d'acceptation LDAP
- Messagerie identifiée par clés de domaine (DKIM)
- Cadre de politique de l'expéditeur (SPF)
- Détection des e-mails falsifiés
- Configurer Cisco SMA pour le suivi et les rapports