Sources d'identité de l'hôte

Les rubriques suivantes fournissent des informations sur les sources d’identité des hôtes :

- Présentation : collecte des données de l’hôte, à la page 1
- Exigences et conditions préalables pour les sources d'identité de l'hôte, à la page 2
- Déterminer les systèmes d’exploitation hôtes que le système peut détecter, à la page 2
- Identification des systèmes d’exploitation hôtes, à la page 3
- Empreintes personnalisées, à la page 3
- Données d’entrée de l’hôte, à la page 12
- Analyse Nmap, à la page 19

Présentation : collecte des données de l’hôte

Pendant que le système Firepower surveille passivement le trafic qui traverse votre réseau, il compare des valeurs d’en-têtes de paquets spécifiques et d’autres données uniques du trafic réseau avec des définitions établies (appelées *empreintes*) pour déterminer les renseignements sur les hôtes de votre réseau, notamment

- le nombre et les types d’hôtes (y compris les périphériques réseau comme les ponts, les routeurs, les équilibreurs de charge et les périphériques NAT)
- les données de base de topologie du réseau, y compris le nombre de sauts entre le point de découverte sur le réseau et les hôtes
- les systèmes d’exploitation fonctionnant sur les hôtes
- les applications sur les hôtes et les utilisateurs associés à ces applications

Si le système ne peut pas identifier de système d’exploitation d’hôte, vous pouvez créer des empreintes client ou serveur personnalisées. Le système utilise ces empreintes pour identifier les nouveaux hôtes. Vous pouvez mapper les empreintes avec les systèmes dans la base de données sur les vulnérabilités (VDB) pour permettre l’affichage des renseignements sur la vulnérabilité appropriés chaque fois qu’un hôte est identifié à l’aide de l’empreinte personnalisée.

Remarque En plus de collecter les données de l’hôte à partir du trafic réseau surveillé, le système peut collecter les données de l’hôte à partir des enregistrements NetFlow exportés, et vous pouvez activement ajouter des données d’hôte à l’aide des analyses Nmap et de la fonctionnalité d’entrée de l’hôte.

Exigences et conditions préalables pour les sources d'identité de l'hôte

Prise en charge des modèles

Tout.

Domaines pris en charge

N’importe quel, à l’exception de la prise d’empreintes personnalisées, qui est uniquement utilisée par Domaine enfant.

Rôles utilisateur

- Admin
- Discovery Admin (administrateur de découverte), à l’exception des données tierces et des mappages personnalisés.

Déterminer les systèmes d’exploitation hôtes que le système peut détecter

Pour savoir quels systèmes d’exploitation exacts le système peut détecter, consultez la liste des empreintes disponibles qui s’affiche pendant le processus de création d’une empreinte de système d’exploitation personnalisée.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur **Créer une empreinte personnalisée**.

Étape 4 Affichez les listes d’options dans les listes déroulantes de la section **Mappages des vulnérabilités** du système d’exploitation. Ces options correspondent aux systèmes d’exploitation pour lesquels le système peut enregistrer des empreintes.

Prochaine étape

Au besoin, consultez Identification des systèmes d’exploitation hôtes, à la page 3.

Identification des systèmes d'exploitation hôtes

Si le système n'identifie pas correctement le système d'exploitation de l'hôte (par exemple, s'il apparaît dans le profil d'hôte comme Inconnu ou est mal identifié), essayez les politiques ci-dessous.

Procédure

Essayez l'une des politiques suivantes :

- Vérifiez les paramètres de conflit d'identité de découverte de réseau.
- Créez une empreinte personnalisée pour l'hôte.
- Exécutez une analyse Nmap sur l'hôte.
- Importez des données dans la cartographie du réseau à l'aide de la fonction d'entrée d'hôte.
- Saisissez manuellement les renseignements sur le système d'exploitation.

Empreintes personnalisées

Le système comprend les *empreintes* du système d'exploitation que le système utilise pour identifier le système d'exploitation sur chaque hôte qu'il détecte. Cependant, il arrive que le système ne puisse pas identifier un système d'exploitation hôte ou l'identifie mal parce qu'aucune empreinte n'existe qui correspond au système d'exploitation. Pour corriger ce problème, vous pouvez créer une *empreinte personnalisée,* qui fournit un modèle de caractéristiques de système d'exploitation unique pour le système d'exploitation inconnu ou mal identifié, pour fournir le nom du système d'exploitation à des fins d'identification.

Si le système ne peut pas correspondre au système d'exploitation d'un hôte, il ne peut pas identifier les vulnérabilités de l'hôte, car le système calcule la liste des vulnérabilités de chaque hôte à partir de l'empreinte de son système d'exploitation. Par exemple, si le système détecte un hôte exécutant Microsoft Windows, le système dispose d'une liste de vulnérabilités Microsoft Windows qu'il ajoute au profil d'hôte de cet hôte en fonction du système d'exploitation Windows détecté.

Par exemple, si plusieurs périphériques de votre réseau exécutent une nouvelle version bêta de Microsoft Windows, le système ne peut pas identifier ce système d'exploitation ni mapper les vulnérabilités aux hôtes. Cependant, sachant que le système comporte une liste de vulnérabilités pour Microsoft Windows, vous pouvez créer une empreinte personnalisée pour l'un des hôtes afin de permettre d'identifier les autres hôtes exécutant le même système d'exploitation. Vous pouvez inclure un mappage de la liste de vulnérabilités pour Microsoft Windows dans l'empreinte pour associer cette liste à chaque hôte qui correspond à l'empreinte.

Lorsque vous créez une empreinte personnalisée, la centre de gestion répertorie l'ensemble des vulnérabilités associées à cette empreinte pour tous les hôtes exécutant le même système d'exploitation. Si l'empreinte personnalisée que vous créez ne comporte aucun mappage de vulnérabilité, le système utilise l'empreinte pour attribuer les informations sur le système d'exploitation personnalisé que vous avez fournies dans l'empreinte. Lorsque le système détecte un nouveau trafic en provenance d'un hôte détecté précédemment, le système met à jour l'hôte avec les nouvelles informations d'empreinte. le système utilise également la

nouvelle empreinte pour identifier tout nouvel hôte à l'aide de ce système d'exploitation lors de sa première détection.

Avant de créer une empreinte personnalisée, vous devez déterminer pourquoi l'hôte n'est pas identifié correctement afin de décider si la empreinte personnalisée est une solution durable.

Vous pouvez créer deux types d'empreintes avec le système :

- Les empreintes du client, qui identifient les systèmes d'exploitation en fonction du paquet SYN que l'hôte envoie lorsqu'il se connecte à une application TCP sur un autre hôte du réseau.
- Les empreintes du serveur, qui identifient les systèmes d'exploitation en fonction du paquet SYN-ACK que l'hôte utilise pour répondre à une connexion entrante à une application TCP en cours d'exécution.

Remarque Si les empreintes du client et du serveur correspondent au même hôte, l'empreinte du client est utilisée.

Après avoir créé les empreintes, vous devez les activer pour que le système puisse les associer aux hôtes.

Sujets connexes

Création d'une empreinte personnalisée pour les clients, à la page 6
Création d'une empreinte personnalisée pour les serveurs, à la page 9

Gestion des empreintes

Après la création et l'activation d'une empreinte, vous pouvez la modifier pour apporter des changements ou ajouter des mappages de vulnérabilité.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés). Si le système attend des données pour créer une empreinte, il actualise automatiquement la page toutes les 10 secondes jusqu'à ce que l'empreinte soit créée.

Étape 3 Gérez vos empreintes personnalisées :

- Activate/Deactivate : active ou désactive une empreinte comme décrit dans Activation et désactivation des empreintes, à la page 5.
- Create : pour créer des empreintes comme décrit dans Création d'une empreinte personnalisée pour les clients, à la page 6 et Création d'une empreinte personnalisée pour les serveurs, à la page 9.
- Edit : modifiez une empreinte comme décrit dans Modification d'une empreinte active, à la page 5 et Modification d'une empreinte inactive, à la page 6.
- Delete : cliquez sur **Supprimer** ( ) à côté de l'empreinte que vous souhaitez supprimer, puis cliquez sur **OK** pour confirmer. Vous ne pouvez supprimer que les empreintes désactivées.

Activation et désactivation des empreintes

Vous devez activer une empreinte personnalisée pour que le système puisse l'utiliser pour identifier des hôtes. Une fois la nouvelle empreinte activée, le système l'utilise pour identifier à nouveau les hôtes détectés précédemment et de nouveaux hôtes.

Si vous souhaitez cesser d'utiliser une empreinte, vous pouvez la désactiver. La désactivation d'une empreinte empêche son utilisation, mais la conserve sur le système. Lorsque vous désactivez une empreinte, le système d'exploitation est marqué comme inconnu pour les hôtes qui utilisent cette dernière. Si les hôtes sont détectés à nouveau et correspondent à une empreinte active différente, ils sont ensuite identifiés par cette empreinte active.

La suppression d'une empreinte la supprime complètement du système. Après avoir désactivé une empreinte, vous pouvez la supprimer.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur le curseur à côté de l'empreinte que vous souhaitez activer ou désactiver.

Remarque L'option d'activation n'est disponible que si l'empreinte que vous avez créée est valide. Si le curseur n'est pas visible, essayez à nouveau de créer l'empreinte.

Modification d'une empreinte active

Si une empreinte est *active*, vous pouvez modifier son nom, sa description, l'affichage personnalisé du système d'exploitation et y mapper des vulnérabilités supplémentaires.

Vous pouvez modifier le nom, la description, l'affichage du système d'exploitation de l'empreinte et y mapper des vulnérabilités supplémentaires.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur **Edit** (✎) à côté de l'empreinte que vous souhaitez modifier.

Étape 4 Modifiez le nom de l'empreinte, la description et l'affichage personnalisé du système d'exploitation, si nécessaire.

Étape 5 Si vous souhaitez supprimer un mappage de vulnérabilité, cliquez sur **Delete** à côté du mappage dans la section **Pre-Defined OS Product Maps** de la page.

Étape 6 Si vous souhaitez ajouter des systèmes d'exploitation pour le mappage des vulnérabilités, sélectionnez le **produit** et, le cas échéant, **la version majeure, la version mineure, la version** de **révision, la version**, la **version**, le **correctif** et l' **extension**, puis cliquez sur **Add OS Defined (ajouter une définition** de système d'exploitation).

Le mappage de vulnérabilité est ajouté à la liste **Mappages de produits de système d'exploitation prédéfinis**.

Étape 7 Cliquez sur **Save** (enregistrer).

Modification d'une empreinte inactive

Si une empreinte est *inactive*, vous pouvez modifier tous les éléments de l'empreinte et la soumettre de nouveau à Cisco Secure Firewall Management Center. Cela inclut toutes les propriétés que vous avez spécifiées lors de la création de l'empreinte, telles que le type d'empreinte, les adresses IP et les ports cibles, les mappages de vulnérabilité, etc. Lorsque vous modifiez une empreinte inactive et que vous la soumettez, elle est soumise de nouveau au système et, s'il s'agit d'une empreinte client, vous devez renvoyer le trafic au périphérique avant de l'activer. Notez que vous ne pouvez choisir qu'un seul mappage de vulnérabilité pour une empreinte inactive. Après avoir activé l'empreinte, vous pouvez mapper des versions et des systèmes d'exploitation supplémentaires à sa liste de vulnérabilités.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur **Edit** (✎) à côté de l'empreinte que vous souhaitez modifier.

Étape 4 Apportez les modifications nécessaires à l'empreinte :

- Si vous modifiez une empreinte client, consultez Création d'une empreinte personnalisée pour les clients, à la page 6.
- Si vous modifiez une empreinte serveur, consultez Création d'une empreinte personnalisée pour les serveurs, à la page 9.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si vous avez modifié une empreinte client, n'oubliez pas d'envoyer le trafic de l'hôte au périphérique qui recueille l'empreinte.

Création d'une empreinte personnalisée pour les clients

Les empreintes du client identifient les systèmes d'exploitation en fonction du paquet SYN qu'un hôte envoie lorsqu'il se connecte à une application TCP en cours d'exécution sur un autre hôte du réseau.

Si centre de gestion n'a pas de contact direct avec les hôtes surveillés, vous pouvez spécifier un périphérique géré par centre de gestion et qui est le plus proche de l'hôte pour lequel vous souhaitez utiliser les empreintes lorsque vous spécifiez les propriétés d'empreinte du client.

Avant de commencer le processus d'empreinte, procurez-vous les informations suivantes sur l'hôte pour lequel vous souhaitez saisir vos empreintes :

- Le nombre de sauts de réseau entre l'hôte et le centre de gestion ou le périphérique que vous utilisez pour obtenir l'empreinte. (Cisco vous recommande fortement de connecter directement le centre de gestion ou le périphérique au sous-réseau auquel l'hôte est connecté.)
- L'interface réseau (sur le centre de gestion ou le périphérique) connectée au réseau sur lequel l'hôte réside.
- Le fournisseur réel du système d'exploitation, le produit et la version réelle de l'hôte.
- Accès à l'hôte afin de générer du trafic client.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur **Créer une empreinte personnalisée**.

Étape 4 Dans la liste déroulante des **périphériques**, choisissez centre de gestion ou le périphérique que vous souhaitez utiliser pour recueillir l'empreinte.

Étape 5 Saisissez le **Nom de l'empreinte**.

Étape 6 Saisissez une **Description de l'empreinte**.

Étape 7 Dans la liste **Type d'empreintes**, choisissez **Client**.

Étape 8 Dans le champ **Target IP Address** (adresse IP cible), saisissez l'adresse IP de l'hôte pour lequel vous souhaitez relever les empreintes.

Notez que l'empreinte sera uniquement basée sur le trafic en provenance et à destination de l'adresse IP de l'hôte que vous spécifiez, et non sur les autres adresses IP de l'hôte (le cas échéant).

Étape 9 Dans le champ **Target Distance** (Distance de la cible), saisissez le nombre de sauts dans le réseau entre l'hôte et le périphérique que vous avez choisis précédemment pour recueillir l'empreinte.

Mise en garde Il doit s'agir du nombre réel de sauts de réseau physique vers l'hôte, qui peut être différent du nombre de sauts détectés par le système.

Étape 10 Dans la liste **Interface** (interface), choisissez l'interface réseau connectée au segment de réseau où se trouve l'hôte.

Mise en garde Cisco vous recommande de ne **pas** utiliser l'interface de détection sur un périphérique géré pour la prise d'empreintes pour plusieurs raisons. Tout d'abord, la prise d'empreintes ne fonctionne pas si l'interface de détection est sur un port de portée. En outre, si vous utilisez l'interface de détection sur un périphérique, le périphérique arrête de surveiller le réseau pendant le temps nécessaire pour recueillir l'empreinte. Vous pouvez, cependant, utiliser l'interface de gestion ou toute autre interface réseau disponible pour effectuer la collecte d'empreintes. Si vous ne savez pas quelle interface est l'interface de détection de votre appareil, consultez le *Guide d'installation* du modèle que vous utilisez pour la prise d'empreintes.

Étape 11 Si vous souhaitez afficher des informations personnalisées dans le profil d'hôte pour les empreintes des hôtes (ou si l'hôte pour lequel vous souhaitez connaître les empreintes ne réside pas dans la section **Mappages de vulnérabilités** du système d'exploitation), choisissez **Use Custom OS Display** (utiliser l'affichage personnalisé du système d'exploitation) et indiquez les valeurs que vous souhaitez afficher pour les éléments suivants :

- Dans le champ **Vendor String** (Chaîne du fournisseur), saisissez le nom du fournisseur du système d'exploitation. Par exemple, le fournisseur de Microsoft Windows serait Microsoft.
- Dans le champ **Product String** (Chaîne du produit), saisissez le nom de produit du système d'exploitation. Par exemple, le nom de produit pour Microsoft Windows 2000 serait Windows.
- Dans le champ **Version String** (Chaîne de la version), saisissez le numéro de version du système d'exploitation. Par exemple, le numéro de version pour Microsoft Windows 2000 serait 2000.

Étape 12 Dans la section OS Vulnerability Mappings (mappages des vulnérabilités du système d'exploitation), choisissez le système d'exploitation, le produit et les versions que vous souhaitez utiliser pour le mappage des vulnérabilités.

Vous devez préciser les valeurs du **fournisseur** et **du produit** dans cette section si vous souhaitez utiliser l'empreinte pour identifier les vulnérabilités pour les hôtes correspondants ou si vous n'affectez pas d'informations d'affichage personnalisées du système d'exploitation.

Pour mapper les vulnérabilités pour toutes les versions d'un système d'exploitation, spécifiez uniquement les valeurs **Fournisseur** et **Produit**.

Remarque Il se peut que certaines options des listes déroulantes **Version principale**, **Version mineure**, **Version de révision**, **version**, **Correctif** et **Extension** ne s'appliquent pas au système d'exploitation que vous choisissez. En outre, si aucune définition ne figure dans la liste qui correspond au système d'exploitation pour lequel vous souhaitez relever les empreintes, vous pouvez laisser ces valeurs vides. Sachez que si vous ne créez aucun mappage de vulnérabilité de système d'exploitation dans une empreinte, le système ne peut pas l'utiliser pour affecter une liste de vulnérabilités avec les hôtes identifiés par cette dernière.

Exemple :

Si vous souhaitez que votre empreinte personnalisée affecte la liste de vulnérabilités de RedHat Linux 9 aux hôtes correspondants, choisissez **RedHat, Inc.** comme fournisseur, **RedHat Linux** comme produit et **9** comme version principale.

Exemple :

Pour ajouter toutes les versions de PALM OS, vous devez **sélectionnerPalmSource,Inc.** dans la liste des **fournisseurs**, **PALM OS** dans la liste des **produits** et conserver les paramètres par défaut des autres listes.

Étape 13 Cliquez sur **Create** (créer).

L'état indique brièvement `New` (Nouveau), puis passe à `Pending` (en attente), statut où il demeure jusqu'à ce que du trafic soit observé pour l'empreinte. Une fois que le trafic est détecté, il passe à l'état `Ready` (Prêt).

La page d'état des empreintes personnalisées est actualisée toutes les dix secondes jusqu'à ce qu'elle reçoive des données de l'hôte en question.

Étape 14 En utilisant l'adresse IP que vous avez spécifiée comme adresse IP cible, accédez à l'hôte pour lequel vous essayez de créer une empreinte et lancez une connexion TCP avec le périphérique.

Pour créer une empreinte précise, le trafic **doit** être vu par le périphérique qui collecte l'empreinte. Si vous êtes connecté par l'intermédiaire d'un commutateur, le trafic vers un système autre que le périphérique peut ne pas être vu par le système.

Exemple :

Accédez à l'interface Web de centre de gestion de l'hôte dont vous souhaitez créer une empreinte ou SSH dans centre de gestion de l'hôte. Si vous utilisez SSH, utilisez la commande ci-dessous, où localIPv6address est l'adresse IPv6 spécifiée à l'étape 7 qui est actuellement attribuée à l'hôte et DCmanagementIPv6address est l'adresse IPv6 de gestion de centre de gestion. La page d'empreinte personnalisée devrait ensuite se téléverser avec un état « Prête ».

```
ssh -b localIPv6address DCmanagementIPv6address
```

Prochaine étape

- Activez l'empreinte comme décrit dans Activation et désactivation des empreintes, à la page 5.

Création d'une empreinte personnalisée pour les serveurs

Les empreintes du serveur identifient les systèmes d'exploitation en fonction du paquet SYN-ACK que l'hôte utilise pour répondre à une connexion entrante vers une application TCP en cours d'exécution. Avant de commencer, vous devriez obtenir les informations suivantes sur l'hôte pour lequel vous souhaitez relever les empreintes :

- Le nombre de sauts de réseau entre l'hôte et le périphérique que vous utilisez pour obtenir l'empreinte. Cisco vous recommande fortement de connecter directement une interface inutilisée du périphérique au sous-réseau auquel l'hôte est connecté.
- L'interface réseau (sur l'appareil) connectée au réseau sur lequel l'hôte se trouve.
- Le fournisseur réel du système d'exploitation, le produit et la version réelle de l'hôte.
- Une adresse IP qui n'est pas utilisée actuellement et qui est autorisée sur le réseau où se trouve l'hôte.

Astuces Si centre de gestion n'a pas de contact direct avec les hôtes surveillés, vous pouvez spécifier un périphérique géré qui est le plus proche de l'hôte pour lequel vous souhaitez relever des empreintes lorsque vous spécifiez les propriétés du serveur d'empreinte.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur **Créer une empreinte personnalisée**.

Étape 4 Dans la liste des **périphériques**, choisissez centre de gestion ou le périphérique géré que vous souhaitez utiliser pour recueillir l'empreinte.

Étape 5 Saisissez le **Nom de l'empreinte**.

Étape 6 Saisissez une **Description de l'empreinte**.

Étape 7 Dans la liste **fingerprint Type** (Type d'empreinte), choisissez **Server** pour afficher les options d'empreinte du serveur.

Étape 8 Dans le champ **Target IP Address** (adresse IP cible), saisissez l'adresse IP de l'hôte pour lequel vous souhaitez relever les empreintes.

Notez que l'empreinte sera uniquement basée sur le trafic en provenance et à destination de l'adresse IP de l'hôte que vous spécifiez, et non sur les autres adresses IP de l'hôte (le cas échéant).

Mise en garde Vous pouvez capturer des empreintes IPv6 uniquement avec les périphériques exécutant la version 5.2 ou une version ultérieure.

Étape 9 Dans le champ **Target Distance** (Distance de la cible), saisissez le nombre de sauts dans le réseau entre l'hôte et le périphérique que vous avez choisis précédemment pour recueillir l'empreinte.

Mise en garde Il doit s'agir du nombre réel de sauts de réseau physique vers l'hôte, qui peut être différent du nombre de sauts détectés par le système.

Étape 10 Dans la liste **Interface** (interface), choisissez l'interface réseau connectée au segment de réseau où se trouve l'hôte.

Mise en garde Cisco vous recommande de ne **pas** utiliser l'interface de détection sur un périphérique géré pour la prise d'empreintes pour plusieurs raisons. Tout d'abord, la prise d'empreintes ne fonctionne pas si l'interface de détection est sur un port de portée. En outre, si vous utilisez l'interface de détection sur un périphérique, le périphérique arrête de surveiller le réseau pendant le temps nécessaire pour recueillir l'empreinte. Vous pouvez, cependant, utiliser l'interface de gestion ou toute autre interface réseau disponible pour effectuer la collecte d'empreintes. Si vous ne savez pas quelle interface est l'interface de détection de votre appareil, consultez le *Guide d'installation* du modèle que vous utilisez pour la prise d'empreintes.

Étape 11 Cliquez sur **Obtenir des ports actifs**.

Étape 12 Dans le champ **Server Port** (port du serveur), saisissez le port que le périphérique doit choisir pour recueillir l'empreinte avec laquelle initier le contact ou choisissez un port dans la liste déroulante **Get Active Ports** (Obtenir des ports actifs).

Vous pouvez utiliser n'importe quel port de serveur ouvert sur l'hôte (par exemple, 80 si l'hôte exécute un serveur Web).

Étape 13 Dans le champ **Source IP Address** (adresse IP source), saisissez une adresse IP à utiliser pour tenter de communiquer avec l'hôte.

Vous devez utiliser une adresse IP source dont l'utilisation sur le réseau est autorisée, mais qui n'est pas actuellement utilisée, par exemple, une adresse de regroupement DHCP qui n'est pas actuellement utilisée. Cela vous évite de mettre temporairement un autre hôte hors ligne pendant que vous créez l'empreinte.

Vous devez exclure cette adresse IP de la surveillance dans votre politique de découverte de réseau pendant que vous créez l'empreinte. Sinon, les affichages de la cartographie du réseau et des événements de découverte seront encombrés d'informations inexactes sur l'hôte représenté par cette adresse IP.

Étape 14 Dans le champ **Source Subnet Mask** (masque de sous-réseau source), saisissez le masque de sous-réseau pour l'adresse IP que vous utilisez.

Étape 15 Si le champ **Source Gateway** (passerelle source) s'affiche, saisissez l'adresse IP de la passerelle par défaut qui doit être utilisée pour établir une voie de routage vers l'hôte.

Étape 16 Si vous souhaitez afficher des informations personnalisées dans le profil d'hôte pour les hôtes identifiés par empreinte ou si le nom d'empreinte que vous souhaitez utiliser n'existe pas dans la section de définition du système d'exploitation, choisissez **Use Custom OS Display** (utiliser l'affichage personnalisé du système d'exploitation) dans la section d'affichage personnalisé du système d'exploitation.

Fournissez les valeurs que vous souhaitez voir apparaître dans les profils d'hôte pour les éléments suivants :

- Dans le champ **Vendor String** (Chaîne du fournisseur), saisissez le nom du fournisseur du système d'exploitation. Par exemple, le fournisseur de Microsoft Windows serait Microsoft.
- Dans le champ **Product String** (Chaîne du produit), saisissez le nom de produit du système d'exploitation. Par exemple, le nom de produit pour Microsoft Windows 2000 serait Windows.
- Dans le champ **Version String** (Chaîne de la version), saisissez le numéro de version du système d'exploitation. Par exemple, le numéro de version pour Microsoft Windows 2000 serait 2000.

Étape 17 Dans la section OS Vulnerability Mappings (mappages des vulnérabilités du système d'exploitation), choisissez le système d'exploitation, le produit et les versions que vous souhaitez utiliser pour le mappage des vulnérabilités.

Vous devez indiquer un fournisseur et un nom de produit dans cette section si vous souhaitez utiliser l'empreinte pour identifier les vulnérabilités des hôtes correspondants ou si vous n'affectez pas d'informations d'affichage personnalisées du système d'exploitation.

Pour mapper les vulnérabilités pour toutes les versions d'un système d'exploitation, spécifiez uniquement le fournisseur et le nom du produit.

Remarque Il se peut que certaines options des listes déroulantes **Version principale**, **Version mineure**, **Version de révision**, **version**, **Correctif** et **Extension** ne s'appliquent pas au système d'exploitation que vous choisissez. En outre, si aucune définition ne figure dans la liste qui correspond au système d'exploitation pour lequel vous souhaitez relever les empreintes, vous pouvez laisser ces valeurs vides. Sachez que si vous ne créez aucun mappage de vulnérabilité de système d'exploitation dans une empreinte, le système ne peut pas l'utiliser pour affecter une liste de vulnérabilités avec les hôtes identifiés par cette dernière.

Exemple :

Si vous souhaitez que votre empreinte personnalisée affecte la liste des vulnérabilités de RedHat Linux 9 aux hôtes correspondants, choisissez **RedHat, Inc.** comme fournisseur, **RedHat Linux** comme produit et **9** comme version.

Exemple :

Pour ajouter toutes les versions de PALM OS, vous devez **sélectionnerPalmSource,Inc.** dans la liste des **fournisseurs**, **Palm OS** dans la liste des **produits** et conserver les paramètres par défaut des autres listes.

Étape 18 Cliquez sur **Create** (créer).
La page d'état des empreintes personnalisées est actualisée toutes les dix secondes et devrait être téléversée avec un état « Prêt ».

Remarque Si le système cible arrête de répondre pendant le processus de prise d'empreinte, l'état affiche le message `ERROR: No Response` (erreur : pas de réponse). Si vous voyez ce message, soumettez de nouveau l'empreinte. Attendez de trois à cinq minutes (le délai peut varier en fonction du système cible), cliquez sur **Edit** (✎) pour accéder à la page des empreintes personnalisées, puis cliquez sur **Create** (Créer).

Prochaine étape

- Activez l'empreinte comme décrit dans Activation et désactivation des empreintes, à la page 5.

Données d'entrée de l'hôte

Vous pouvez élargir la cartographie du réseau en important des données de cartographie réseau provenant de tiers. Vous pouvez également utiliser la fonctionnalité de saisie de l'hôte en modifiant l'identité du système d'exploitation ou de l'application ou en supprimant des protocoles d'application, des protocoles, des attributs d'hôte ou des clients à l'aide de l'interface Web.

Le système peut concilier des données provenant de plusieurs sources pour déterminer l'identité actuelle d'un système d'exploitation ou d'une application.

Toutes les données, à l'exception des vulnérabilités de tiers, sont supprimées lorsque l'hôte concerné est supprimé de la cartographie du réseau. Pour en savoir plus sur la configuration des scripts ou l'importation de fichiers, consultez *Guide d'API des entrées d'hôte du système Firepower*.

Pour inclure des données importées dans les corrélations d'impact, vous devez mapper les données avec les définitions du système d'exploitation et d'application dans la base de données.

Exigences relatives à l'utilisation de données tierces

Vous pouvez importer des données de découverte à partir de systèmes tiers sur votre réseau. Cependant, pour activer les fonctionnalités où des données de prévention des intrusions et de découverte sont utilisées ensemble, comme les recommandations Cisco, Mises à niveau des profils adaptatifs ou l'évaluation d'impact, vous devez faire correspondre le plus grand nombre d'éléments possible aux définitions correspondantes. Tenez compte des exigences suivantes concernant l'utilisation de données tierces :

- Si vous avez un système tiers qui dispose de données spécifiques sur vos actifs réseau, vous pouvez importer ces données à l'aide de la fonction d'entrée de l'hôte. Cependant, étant donné que les tiers peuvent nommer les produits différemment, vous devez faire correspondre le fournisseur, le produit et les versions tiers avec la définition de produit Cisco correspondante. Après avoir mappé les produits, vous devez activer les mappages de vulnérabilités pour l'évaluation d'impact dans la configuration centre de gestion pour permettre la corrélation d'impact. Pour les protocoles d'application sans version ou sans fournisseur, vous devez mapper les vulnérabilités des protocoles d'application dans la configuration centre de gestion.
- Si vous importez des informations de correctifs émanant d'un tiers et que vous souhaitez marquer toutes les vulnérabilités corrigées par ce correctif comme étant invalides, vous devez associer le nom du correctif du tiers à une définition de correctif dans la base de données. Toutes les vulnérabilités traitées par le correctif seront ensuite supprimées des hôtes où vous ajoutez ce correctif.

- Si vous importez des vulnérabilités de système d'exploitation et de protocole d'application d'un tiers et que vous souhaitez les utiliser pour la corrélation des impacts, vous devez faire correspondre la chaîne d'identification de la vulnérabilité tierce avec les vulnérabilités de la base de données. Notez que bien que de nombreux clients ont des vulnérabilités associées et que les clients sont utilisés pour l'évaluation d'impact, vous ne pouvez pas importer et mapper les vulnérabilités de clients tiers. Une fois les vulnérabilités mappées, vous devez activer les mappages de vulnérabilités tiers pour l'évaluation d'impact dans la configuration centre de gestion. Pour que des protocoles d'application sans informations sur le fournisseur ou la version se mappent aux vulnérabilités, un utilisateur administratif doit également mapper les vulnérabilités des applications dans la configuration centre de gestion.
- Si vous importez des données d'application et que vous souhaitez utiliser ces données pour la corrélation des impacts, vous devez mapper la chaîne de fournisseur de chaque protocole d'application avec la définition de protocole d'application Cisco correspondante.

Sujets connexes

Mappages des produits tiers, à la page 13
Correctifs des mappages de produits tiers, à la page 15
Cartographie des vulnérabilités tierces, à la page 16
Création de mappages de produits personnalisés, à la page 17

Mappages des produits tiers

Lorsque vous ajoutez des données tierces à la cartographie du réseau au moyen de la fonction de saisie de l'utilisateur, vous devez faire correspondre les noms du fournisseur, du produit et de la version utilisés par le tiers aux définitions de produit Cisco. La mise en correspondance des produits avec les définitions de Cisco attribue des vulnérabilités en fonction de ces dernières.

De même, si vous importez des informations relatives à un correctif tiers, comme un produit de gestion des correctifs, vous devez mapper le nom du correctif avec le fournisseur et le produit appropriés et le correctif correspondant dans la base de données.

Mappages des produits tiers

Si vous importez des données d'un tiers, vous devez faire correspondre le produit Cisco au nom du tiers pour attribuer les vulnérabilités et effectuer une corrélation des impacts à l'aide de ces données. La mise en correspondance du produit associe des informations sur la vulnérabilité de Cisco au nom du produit tiers, ce qui permet au système d'effectuer une corrélation des impacts à l'aide de ces données.

Si vous importez des données à l'aide de la fonction d'importation des entrées de l'hôte, vous pouvez également utiliser la fonction AddScanResult pour mapper les produits tiers aux vulnérabilités du système d'exploitation et des applications lors de l'importation.

Par exemple, si vous importez des données d'un tiers qui répertorie Apache Tomcat comme application et que vous savez qu'il s'agit de la version 6 de ce produit, vous pouvez ajouter une carte tierce où :

- **Le nom du fournisseur** est `Apache`.
- **Le nom du produit** est `Tomcat`.
- **Apache** est choisi dans la liste déroulante **Vendor** (Fournisseur).
- **Tomcat** est choisi dans la liste déroulante **Product** (Produit).
- **6** est choisi dans la liste déroulante **Version**

Ce mappage ferait en sorte que toute vulnérabilité d'Apache Tomcat 6 soit attribuée aux hôtes avec une liste d'application pour Apache Tomcat.

Notez que pour les applications sans version ou sans fournisseur, vous devez mapper les vulnérabilités pour les types d'applications dans la configuration Cisco Secure Firewall Management Center. Bien que de nombreux clients soient associés à des vulnérabilités et que les clients sont utilisés pour l'évaluation d'impact, vous ne pouvez pas importer et mapper les vulnérabilités de clients tiers.

Astuces Si vous avez déjà créé un mappage tiers sur un autre Cisco Secure Firewall Management Center, vous pouvez l'exporter, puis l'importer dans ce centre de gestion. Vous pouvez ensuite modifier le mappage importé selon vos besoins.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **User Third-Party Mappings** (Mappages utilisateur tiers).

Étape 3 Vous avez deux choix :

- Create (créer) : pour créer un nouvel ensemble de cartes, cliquez sur **Create Product Map Set**(créer un ensemble de cartes de produit).
- Edit (modifier) : pour modifier un ensemble de cartes existant, cliquez sur **Edit** ( ) à côté de l'ensemble de cartes que vous souhaitez modifier. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Saisissez le **Nom du jeu de mappage**.

Étape 5 Saisissez une **description**.

Étape 6 Vous avez deux choix :

- Créer : pour mapper un produit tiers, cliquez sur **Add Product Map** (ajouter une carte de produit).
- Modifier : pour modifier une carte de produits tiers existante, cliquez sur **Edit** ( ) à côté de l'ensemble de cartes que vous souhaitez modifier. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 7 Saisissez la **chaîne du fournisseur** utilisée par le produit tiers.

Étape 8 Saisissez la **chaîne du produit** utilisée par le produit tiers.

Étape 9 Saisissez la **chaîne de version** utilisée par le produit tiers.

Étape 10 Dans la section Product Mappings (Mappages de produits), choisissez le système d'exploitation, le produit et les versions que vous souhaitez utiliser pour le mappage des vulnérabilités dans les champs **Vendor**, **Product**, **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch** et **Extension** (Fournisseur, Produit,Version majeure, version mineure, Version de révision , Build, Extension).

Exemple :

Si vous souhaitez qu'un hôte exécutant un produit dont le nom est composé de chaînes tierces utilise les vulnérabilités de Red Hat Linux 9, choisissez **RedHat, Inc.** comme fournisseur, **RedHat Linux** comme produit et **9** comme version.

Étape 11 Cliquez sur **Save** (enregistrer).

Correctifs des mappages de produits tiers

Si vous associez un nom de correctif à un ensemble particulier de correctifs dans la base de données, vous pouvez ensuite importer des données à partir d'une application de gestion des correctifs tierce et appliquer le correctif à un ensemble d'hôtes. Lorsque le nom de correctif est importé sur un hôte, le système marque toutes les vulnérabilités traitées par le correctif comme non valides pour cet hôte.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **User Third-Party Mappings** (Mappages utilisateur tiers).

Étape 3 Vous avez deux choix :

- Create (créer) : pour créer un nouvel ensemble de cartes, cliquez sur **Create Product Map Set**(créer un ensemble de cartes de produit).
- Edit (modifier) : pour modifier un ensemble de cartes existant, cliquez sur **Edit** ( ) à côté de l'ensemble de cartes que vous souhaitez modifier. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Saisissez le **Nom du jeu de mappage**.

Étape 5 Saisissez une **description**.

Étape 6 Vous avez deux choix :

- Create (créer) : Pour mapper un produit tiers, cliquez sur **Add Fix Map** (ajouter un mappage de correctifs).
- Modifier : pour modifier une liste de produits tiers existante, cliquez sur **Edit** ( ) à côté de celle-ci. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 7 Saisissez le nom du correctif que vous souhaitez mettre en correspondance dans le champ **Nom du correctif tiers**.

Étape 8 Dans la section **Mappages de produits**, choisissez le système d'exploitation, le produit et les versions que vous souhaitez utiliser pour le mappage de correctifs dans les champs suivants :

- **Fournisseur**
- **Produit**
- **Version majeure**
- **Version mineure**
- **Version de révision**
- **Créer**
- **Correctif**
- **Extension**

Exemple :

Si vous souhaitez que votre mappage attribue les correctifs de Red Hat Linux 9 aux hôtes où le correctif est appliqué, choisissez **RedHat, Inc.** comme fournisseur, **RedHat Linux** comme produit et **9** comme version.

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer la carte de correctifs.

Cartographie des vulnérabilités tierces

Pour ajouter des informations sur la vulnérabilité provenant d'un tiers à la base de données sur les vulnérabilités (VDB), vous devez mapper la chaîne d'identification tierce pour chaque vulnérabilité importée avec tout SVID, Bugtraq ou SID existant. Après avoir créé un mappage pour la vulnérabilité, celui-ci fonctionne pour toutes les vulnérabilités importées vers les hôtes dans la cartographie du réseau et permet la corrélation des impacts pour ces vulnérabilités.

Vous devez activer la corrélation d'impact pour les vulnérabilités tierces afin de permettre la corrélation. Pour les applications sans version ou sans fournisseur, vous devez également mapper les vulnérabilités pour les types d'applications de la configuration Cisco Secure Firewall Management Center.

Bien que de nombreux clients aient des vulnérabilités associées et que les clients soient utilisés pour l'évaluation d'impact, vous ne pouvez pas utiliser les vulnérabilités de clients tiers pour l'évaluation d'impact.

Astuces Si vous avez déjà créé un mappage tiers sur un autre Cisco Secure Firewall Management Center, vous pouvez l'exporter, puis l'importer dans ce centre de gestion. Vous pouvez ensuite modifier le mappage importé selon vos besoins.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **User Third-Party Mappings** (Mappages utilisateur tiers).

Étape 3 Vous avez deux choix :

- Create (créer) : Pour créer un nouvel ensemble de vulnérabilités, cliquez sur **Create Vulnerability Map Set**(créer un ensemble de cartes de vulnérabilités).
- Edit (Modifier) : pour modifier un ensemble de vulnérabilités existant, cliquez sur **Edit** ( ) à côté de l'ensemble de vulnérabilités. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Add Vulnerability Map** (Ajouter une carte de vulnérabilité)

Étape 5 Saisissez l'identification tierce pour la vulnérabilité dans le champ **Vulnerability ID** (ID de la vulnérabilité).

Étape 6 Saisissez une **Vulnerability Description** (Description de la vulnérabilité).

Étape 7 De manière facultative :

- Saisissez un ID de Snort dans le champ de **mappages d'ID de vulnérabilité Snort**.
- Saisissez un ID de vulnérabilité existant dans le champ **Mappages SVID**.
- Saisissez un numéro d'identification Bugtraq dans le champ **Mappage d'ID de vulnérabilité Bugtraq**..

Étape 8 Cliquez sur **Add** (Ajouter).

Sujets connexes

Activation de l'évaluation de l'incidence de la vulnérabilité de la découverte de réseau

Mappages de produits personnalisés

Vous pouvez utiliser des mappages de produits pour vous assurer que les serveurs saisis par un tiers sont associés aux définitions Cisco appropriées. Après avoir défini et activé le mappage de produit, tous les serveurs ou clients sur les hôtes surveillés qui ont les chaînes de fournisseur mappées utilisent les mappages de produit personnalisés. Pour cette raison, vous pouvez souhaiter mapper les vulnérabilités pour tous les serveurs de la cartographie du réseau avec une chaîne de fournisseur particulière au lieu de définir explicitement le fournisseur, le produit et la version du serveur.

Création de mappages de produits personnalisés

Si le système ne peut pas mapper un serveur à un fournisseur et à un produit dans la VDB, vous pouvez créer le mappage manuellement. Lorsque vous activez un mappage de produit personnalisé, le système mappe les vulnérabilités du fournisseur et du produit spécifiés à tous les serveurs de la cartographie du réseau où cette chaîne de fournisseur se trouve.

Remarque Les mappages de produits personnalisés s'appliquent à toutes les occurrences d'un protocole d'application, quelle que soit la source des données d'application (comme Nmap, la fonctionnalité d'entrée de l'hôte ou le système Firepower lui-même). Toutefois, si les mappages de vulnérabilité tiers pour les données importées à l'aide de la fonctionnalité d'entrée d'hôte sont en conflit avec les mappages que vous avez définis par le biais d'un mappage de produit personnalisé, le mappage de vulnérabilité tiers remplace le mappage de vulnérabilité de produit personnalisé et utilise les paramètres de mappage de vulnérabilité tiers lorsque cela se produit.

Vous créez des listes de mappages de produits, puis vous activez ou désactivez l'utilisation de plusieurs mappages à la fois en activant ou désactivant chaque liste. Lorsque vous spécifiez un fournisseur avec lequel effectuer le mappage, le système met à jour la liste des produits pour inclure uniquement ceux de ce fournisseur.

Après avoir créé un mappage de produit personnalisé, vous devez activer la liste de mappage de produits personnalisée. Après avoir activé une liste de mappage de produits personnalisée, le système met à jour tous les serveurs avec les occurrences des chaînes de fournisseur spécifiées. Pour les données importées par la fonction d'entrée de l'hôte, les vulnérabilités sont mises à jour, sauf si vous avez déjà explicitement défini les mappages de produits pour ce serveur.

Si, par exemple, votre entreprise modifie la bannière de vos serveurs Web Apache Tomcat pour qu'elle soit nommée `serveur Web interne`, vous pouvez mapper la chaîne de fournisseur `serveur Web interne` avec le fournisseur **Apache** et le produit **Tomcat**, puis activer la liste contenant ce mappage, tous les hôtes où un serveur étiqueté `serveur Web interne` se trouve ont des vulnérabilités pour Apache Tomcat dans la base de données.

Astuces Vous pouvez utiliser cette fonctionnalité pour mapper les vulnérabilités aux règles de prévention des intrusions locales en mappant le SID de la règle à une autre vulnérabilité.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Custom Products Mapping** (Mappage de produits personnalisé)

Étape 3 Cliquez sur **Create CustomeProduct Mapping List** (Créer une liste de mappage de produits personnalisée).

Étape 4 Saisissez un **nom de la liste de mappage de produits personnalisée**

Étape 5 Cliquez sur **Add Vendor String** (Ajouter une chaîne de fournisseurs).

Étape 6 Dans le champ **Vendor String** (Chaîne de fournisseurs), saisissez la chaîne de fournisseur qui identifie les applications qui doivent être mappées aux valeurs de fournisseur et de produit choisies.

Étape 7 Choisissez le fournisseur avec lequel vous souhaitez effectuer le mappage dans la liste déroulante **Vendor** (Fournisseur).

Étape 8 Choisissez le produit que vous souhaitez mapper dans la liste déroulante **Product** (Produit).

Étape 9 Cliquez sur **Add** (Ajouter) pour ajouter la chaîne de fournisseur mappée à la liste.

Étape 10 Si nécessaire, répétez les étapes 4 à 8 pour ajouter des mappages de chaînes de fournisseurs supplémentaires à la liste.

Étape 11 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Activez la liste de mappage de produits personnalisée Pour en savoir plus, consultez Activation et désactivation des mappages de produits personnalisés, à la page 18.

Modification des listes de mappage de produits personnalisées

Vous pouvez modifier des listes de mappage de produits personnalisés existantes en ajoutant ou en supprimant des chaînes de fournisseur ou en modifiant le nom de la liste.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Custom Products Mappings** (Mappage de produits personnalisé)

Étape 3 Cliquez sur **Edit** () à côté de la liste de mappage de produits que vous souhaitez modifier.

Si **Afficher** () apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Apportez des modifications à la liste comme décrit dans Création de mappages de produits personnalisés, à la page 17.

Étape 5 Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Activation et désactivation des mappages de produits personnalisés

Vous pouvez activer ou désactiver l'utilisation d'une liste complète de mappages de produits personnalisés à la fois. Après avoir activé une liste de mappage de produit personnalisée, chaque mappage de cette liste s'applique à toutes les applications avec la chaîne de fournisseur spécifiée, qu'il soit détecté par les périphériques gérés ou importé par la fonctionnalité d'entrée de l'hôte.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Custom Products Mappings** (Mappage de produits personnalisé)

Étape 3 Cliquez sur le curseur à côté de la liste de mappage de produit personnalisée pour l'activer ou la désactiver.

Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Analyse Nmap

Le système Firepower crée des cartes du réseau grâce à une analyse passive du trafic sur votre réseau. Les renseignements obtenus par cette analyse passive peuvent occasionnellement être incomplets, selon les conditions du système. Cependant, vous pouvez analyser activement un hôte pour obtenir des informations complètes. Par exemple, si un hôte a un serveur sur un port ouvert, mais que le serveur n'a reçu ni envoyé de trafic depuis que le système surveille votre réseau, le système n'ajoute pas d'informations sur ce serveur à la cartographie du réseau. Si vous analysez directement cet hôte à l'aide d'un analyseur actif, vous pouvez détecter la présence du serveur.

Le système Firepower s'intègre à Nmap ™, un analyseur actif à code source ouvert pour l'exploration de réseau et l'audit de sécurité.

Lorsque vous numérisez un hôte à l'aide de Nmap, le système :

- Ajoute des serveurs sur des ports ouverts non détectés précédemment à la liste de serveurs dans le profil d'hôte de cet hôte. Le profil d'hôte répertorie tous les serveurs détectés sur des ports TCP filtrés ou fermés ou sur des ports UDP dans la section des résultats d'analyse. Par défaut, Nmap analyse plus de 1660 ports TCP.

  Si le système reconnaît un serveur identifié lors d'une analyse Nmap et qu'une définition de serveur correspond, il fait correspondre les noms que Nmap utilise pour les serveurs avec les définitions de serveur Cisco correspondantes.

- Il compare les résultats de l'analyse à plus de 1 500 empreintes de systèmes d'exploitation connues pour déterminer le système d'exploitation et attribue des notes à chacun. Le système d'exploitation affecté à l'hôte l'empreinte du système d'exploitation ayant la note la plus élevée.

  Le système fait correspondre les noms de systèmes d'exploitation Nmap aux définitions de systèmes d'exploitation de Cisco.

- Il attribue des vulnérabilités à l'hôte pour les serveurs et systèmes d'exploitation ajoutés.

Remarque :

- Un hôte doit exister dans la cartographie du réseau pour que Nmap puisse ajouter ses résultats au profil d'hôte.
- Si l'hôte est supprimé de la cartographie du réseau, tous les résultats d'analyse Nmap pour cet hôte sont rejetés.

Astuces Certaines options d'analyse (comme le balayage de ports) peuvent imposer une charge importante sur les réseaux par la faible bande passante. Planifiez de telles analyses pour qu'elles s'exécutent pendant les périodes de faible utilisation du réseau.

Pour plus d'informations sur la technologie Nmap sous-jacente utilisée pour l'analyse, consultez la documentation de Nmap à l'adresse http://insecure.org/.

Options de correction de Nmap

Vous définissez les paramètres d'une analyse Nmap en créant une correction Nmap. Une correction Nmap peut être utilisée comme réponse dans une politique de corrélation, exécutée à la demande ou planifiée pour s'exécuter à une heure précise.

Notez que les données du serveur et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse de Nmap. Si vous prévoyez analyser un hôte à la recherche des données du système d'exploitation et du serveur à l'aide de Nmap, vous pouvez configurer des analyses planifiées régulièrement pour maintenir à jour les données du système d'exploitation et du serveur fournis par Nmap.

Le tableau suivant explique les options configurables dans les corrections Nmap.

Tableau 1 : Options de correction de Nmap

Option	Description	Option Nmap correspondante
Analyser quelle(s) adresse(s) de l'événement?	Lorsque vous utilisez une analyse Nmap comme réponse à une règle de corrélation, sélectionnez l'une des options suivantes pour contrôler l'adresse qui est analysée dans l'événement : celle de l'hôte source, de l'hôte de destination ou les deux : • **Analyser les adresses source et de destination** analyse les hôtes représentés par l'adresse IP source et l'adresse IP de destination dans l'événement. • **Analyser l'adresse source uniquement** analyse l'hôte représenté par l'adresse IP source de l'événement. • **Analyser l'adresse de destination seulement** analyse l'hôte représenté par l'adresse IP de destination de l'événement.	S. O.

Option	Description	Option Nmap correspondante
Types d'analyse	Sélectionnez la façon dont Nmap analyse les ports : • L'analyse **TCP Syn** se connecte rapidement à des milliers de ports sans utiliser d'établissement de liaison TCP complet. Cette option vous permet d'analyser rapidement en mode furtif les hôtes sur lesquels le compte `administrateur` dispose d'un accès brut aux paquets ou sur lesquels IPv6 n'est pas en cours d'exécution, en démarrant des connexions TCP sans les établir. Si un hôte reconnaît le paquet Syn envoyé dans une analyse Syn TCP, Nmap réinitialise la connexion. • L'analyse **TCP Connect** utilise l'appel système `connect()` pour ouvrir des connexions par l'intermédiaire du système d'exploitation sur l'hôte. Vous pouvez utiliser l'analyse TCP Connect si l'utilisateur `admin` sur le centre de gestion ou le périphérique géré ne dispose pas de privilèges bruts sur les paquets sur un hôte ou si vous analysez des réseaux IPv6. En d'autres termes, utilisez cette option dans les situations où l'analyse TCP Syn ne peut pas être utilisée. • L'analyse **TCP ACK** envoie un paquet ACK pour vérifier si les ports sont filtrés ou non. • L'analyse **TCP Window** fonctionne de la même manière que l'analyse par TCP ACK, mais peut également déterminer si un port est ouvert ou fermé. • L'analyse **TCP Maimon** identifie les systèmes dérivés de BSD à l'aide d'une sonde FIN/ACK.	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon** : `-sM`
Analyser les ports UDP	Activez pour analyser les ports UDP en plus des ports TCP. Notez que l'analyse des ports UDP peut prendre du temps, évitez donc d'utiliser cette option si vous souhaitez analyser les ports UDP rapidement.	`-sU`
Utiliser le port à partir de l'événement	Si vous prévoyez d'utiliser la correction comme réponse dans une politique de corrélation, activez cette analyse pour que la correction analyse uniquement le port spécifié dans l'événement qui déclenche la réponse de corrélation. • Sélectionnez **On** (activer) pour analyser le port lors de l'événement de corrélation, plutôt que les ports que vous avez spécifiés lors de la configuration de la correction de Nmap. Si vous analysez le port lors de l'événement de corrélation, notez que la correction analyse le port aux adresses IP que vous spécifiez lors de la configuration de la correction de Nmap. Ces ports sont également ajoutés à la cible d'analyse dynamique de la correction. • Sélectionnez **Off** (désactiver) pour analyser uniquement les ports que vous avez spécifiés dans la configuration de correction Nmap. Vous pouvez également contrôler si Nmap collecte des informations sur le système d'exploitation et le serveur. Activez l'option **Use Port from Event** (utiliser le port à partir de l'événement) pour analyser le port associé au nouveau serveur.	S. O.

Option	Description	Option Nmap correspondante
Analyse à partir du moteur de détection de rapports	Activez pour analyser un hôte à partir du périphérique , sur lequel le moteur de détection qui a signalé l'hôte se trouve. • Pour analyser à partir du périphérique qui exécute le moteur de détection de rapports, sélectionner **On** (activer). • Pour analyser à partir du périphérique configuré dans la correction, sélectionner **Off** (désactiver).	S. O.
Balayage rapide des ports	Activez pour analyser uniquement les ports TCP répertoriés dans le fichier `nmap-services` situé dans le répertoire `/var/sf/nmap/partage/nmap/nmap-services` sur le périphérique qui effectue l'analyse, en ignorant les autres paramètres de port. Notez que vous ne pouvez pas utiliser cette option avec l'option **Plages de ports et ordre de balayage**. • Pour analyser uniquement les ports répertoriés dans le fichier `nmap-services` situé dans le répertoire `/var/sf/nmap/partage/nmap/nmap-services` sur le périphérique qui effectue l'analyse, en ignorant les autres paramètres de port, sélectionnez **On** (activé). • Pour analyser tous les ports TCP, sélectionnez **Off** (désactiver).	`-F`
Plages de ports et ordre de balayage	Définissez les ports spécifiques que vous souhaitez analyser en utilisant la syntaxe de spécification de port Nmap et l'ordre dans lequel vous souhaitez les analyser. Notez que vous ne pouvez pas utiliser cette option avec l'option d' **analyse rapide de ports**.	`-p`
Sondez les ports ouverts pour obtenir des informations sur le fournisseur et la version	Activez cette option pour détecter les informations sur le fournisseur et la version du serveur. Si vous sondez les ports ouverts à la recherche d'informations sur la version et le fournisseur du serveur, Nmap obtiendra des données de serveur qu'il utilise pour identifier les serveurs. Il remplace ensuite les données de serveur Cisco pour ce serveur. • Sélectionnez **On** (activer) pour analyser les ports ouverts sur l'hôte à la recherche d'informations sur le serveur afin d'identifier les fournisseurs et les versions du serveur. • Sélectionnez **off** (désactiver) pour continuer à utiliser les informations du serveur Cisco pour l'hôte.	`-sV`
Intensité de la version de service	Sélectionnez l'intensité des sondes Nmap pour les versions de service. • Pour utiliser plus de sondes avec une précision supérieure avec une analyse plus longue, sélectionnez une valeur plus élevée. • Pour utiliser moins de sondes avec moins de précision avec une analyse plus rapide, sélectionnez une valeur inférieure.	`--version-intensity` <intensity>

Option	Description	Option Nmap correspondante
Détecter le système d'exploitation	Activez cette option pour détecter les informations sur le système d'exploitation de l'hôte. Si vous configurez la détection du système d'exploitation pour un hôte, Nmap analyse l'hôte et utilise les résultats pour créer une évaluation pour chaque système d'exploitation qui reflète la probabilité que le système d'exploitation soit en cours d'exécution sur l'hôte. • Sélectionnez **On** (activé) pour analyser l'hôte à la recherche d'informations permettant d'identifier le système d'exploitation. • Sélectionnez **Off** (désactivé) pour continuer à utiliser les informations du système d'exploitation Cisco pour l'hôte.	`-o`
Traiter tous les hôtes comme en ligne	Activez pour ignorer le processus de découverte d'hôte et exécuter une analyse de port sur chaque hôte de la plage cible. Notez que lorsque vous activez cette option, Nmap ignore les paramètres de **la méthode de découverte** de l' **hôte et de la liste de ports de découverte** de l'hôte . • Pour ignorer le processus de découverte d'hôte et exécuter une analyse de port sur chaque hôte de la plage cible, sélectionnez **On** (activer). • Pour effectuer la découverte d'hôte à l'aide des paramètres de **la méthode de découverte d'hôte** et de la **liste de ports de découverte d'hôte** et ignorer le balayage de port sur tout hôte non disponible, sélectionnez **Off** (désactiver).	`-PN`

Option	Description	Option Nmap correspondante
Méthode de découverte de l'hôte	Sélectionnez cette option pour effectuer la découverte d'hôte pour tous les hôtes de la plage cible, sur les ports répertoriés dans la liste des ports de **découverte d'hôte**, ou si aucun port n'est répertorié, sur les ports par défaut pour cette méthode de découverte d'hôte. Notez que si vous avez également activé l'option **Traiter tous les hôtes comme en ligne**, l'option **Méthode de découverte de l'hôte** n'a aucun effet et que la découverte d'hôte n'est pas effectuée. Sélectionnez la méthode à utiliser lorsque Nmap teste pour voir si un hôte est présent et disponible : • L'option **TCP SYN** envoie un paquet TCP vide avec le drapeau SYN défini et reconnaît l'hôte comme disponible si une réponse est reçue. Le protocole SYN TCP analyse le port 80 par défaut. Notez que les analyses SYN TCP sont moins susceptibles d'être bloquées par un pare-feu avec des règles de pare-feu dynamiques. • L'option **TCP ACK** envoie un paquet TCP vide avec l'indicateur ACK activé et reconnaît l'hôte comme disponible si une réponse est reçue. TCP ACK analyse également le port 80 par défaut. Notez que les analyses TCP ACK sont moins susceptibles d'être bloquées par un pare-feu avec des règles de pare-feu sans état. • L'option **UDP** envoie un paquet UDP et suppose la disponibilité de l'hôte si une réponse de port inaccessible est envoyée d'un port fermé. UDP analyse le port 40125 par défaut.	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`
Liste des ports de découverte d'hôte	Spécifiez une liste personnalisée de ports, séparés par des virgules, que vous souhaitez analyser lors de la découverte d'hôte.	liste de ports pour la méthode de découverte d'hôte
Scripts NSE par défaut	Activez pour exécuter l'ensemble par défaut de scripts Nmap pour la découverte de l'hôte et la détection des vulnérabilités et du serveur, du système d'exploitation. Reportez-vous à https://nmap.org/nsedoc/catégories/default.html pour obtenir la liste des scripts par défaut. • Pour exécuter l'ensemble de scripts Nmap par défaut, sélectionnez **On**. • Pour ignorer l'ensemble de scripts Nmap par défaut, sélectionnez **Off**.	`-sC`
Modèle de calendrier	Sélectionner le moment du processus d'analyse; Plus le nombre que vous sélectionnez est élevé, plus l'analyse est rapide et moins complète.	**0** : `T0` (paranoïaque) **1** : `T1` (sournois) **2** : `T2` (courtois) **3** : `T3` (normal) **4** : `T4` (agressif) **5** : `T5` (fou)

Lignes directrices d'analyse Nmap

Bien que l'analyse active puisse obtenir des informations précieuses, la surutilisation d'un outil tel que Nmap peut sur téléverser les ressources de votre réseau ou même faire planter des hôtes importants. Lorsque vous utilisez un analyseur actif, vous devez créer une politique d'analyse en suivant ces instructions pour vous assurer que vous analysez uniquement les hôtes et les ports que vous devez analyser.

Sélection des cibles de balayage appropriées

Lorsque vous configurez Nmap, vous pouvez créer des cibles d'analyse qui identifient les hôtes que vous souhaitez analyser. Une cible d'analyse comprend une adresse IP unique, un bloc d'CIDR ou une plage d'octets d'adresses IP, une plage d'adresses IP ou une liste d'adresses IP ou de plages à analyser, ainsi que les ports sur le ou les hôtes.

Vous pouvez définir des cibles comme suit :

- Pour les hôtes IPv6 :
  - une adresse IP exacte (par exemple, `2001:DB8:1::168:ABCD`)
- Pour les hôtes IPv4 :
  - une adresse IP exacte (par exemple, `192.168.1.101`) ou une liste d'adresses IP séparées par des virgules ou des espaces
  - un bloc d'adresse IP au moyen de la notation CIDR (par exemple, `192.168.1.0/24` analyse les 254 hôtes entre 192.168.1.1 et 192.168.1.254 compris).
  - une plage d'adresses IP utilisant des adresses par plage d'octets (par exemple, `192.168.0-255.1-254` analyse toutes les adresses de la plage 192.168.xx, sauf celles se terminant par .0 et ou .255)
  - une plage d'adresses IP utilisant la césure (par exemple, `192.168.1.1 à 192.168.1.5` analyse les six hôtes entre 192.168.1.1 et 192.168.1.5 inclusivement)
  - une liste d'adresses ou de plages séparées par des virgules ou des espaces (p. ex., `192.168.1.0/24, 194.168.1.0/24` analyse les 254 hôtes entre 192.168.1.1 et 192.168.1.254, compris et les 254 hôtes entre 194.168. 1.1 et 194.168.1.254, compris)

Les cibles d'analyse idéales pour les analyses Nmap comprennent les hôtes dont le système d'exploitation que le système n'est pas en mesure d'identifier, les hôtes dont des serveurs non identifiés ont été récemment détectés sur votre réseau. Rappelez-vous que les résultats Nmap ne peuvent pas être ajoutés à la cartographie du réseau pour les hôtes qui n'existent pas déjà dans la cartographie du réseau.

⚠

Mise en garde

- Les données du serveur et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse Nmap. Si vous prévoyez d'analyser un hôte à l'aide de Nmap, planifiez régulièrement des analyses.
- Si un hôte est supprimé de la cartographie du réseau, tous les résultats d'analyse Nmap sont rejetés.
- Assurez-vous d'avoir l'autorisation d'analyser vos cibles. Il peut être illégal d'utiliser Nmap pour analyser des hôtes qui ne vous appartiennent pas ou qui ne appartiennent pas à votre entreprise.

Sélection des ports appropriés à analyser

Pour chaque cible d'analyse que vous configurez, vous pouvez sélectionner les ports que vous souhaitez analyser. Vous pouvez désigner des numéros de port individuels, des plages de ports ou une série de numéros de port et de plages de ports pour déterminer l'ensemble exact de ports à analyser sur chaque cible.

Par défaut, Nmap analyse les ports TCP 1 à 1024. Si vous prévoyez d'utiliser la correction comme réponse dans une politique de corrélation, vous pouvez faire en sorte que la correction analyse uniquement le port spécifié dans l'événement qui déclenche la réponse de corrélation. Si vous exécutez la correction à la demande ou en tant que tâche planifiée, ou si vous n'utilisez pas le port de l'événement, vous pouvez utiliser d'autres options de port pour déterminer quels ports sont analysés. Vous pouvez choisir d'analyser uniquement les ports TCP répertoriés dans le fichier `nmap-services`, en ignorant les autres paramètres de port. Vous pouvez également analyser les ports UDP en plus des ports TCP. Notez que l'analyse des ports UDP peut prendre du temps, évitez donc d'utiliser cette option si vous souhaitez analyser rapidement. Pour sélectionner les ports ou la plage de ports à analyser, utilisez la syntaxe de spécification de port Nmap pour identifier les ports.

Définition des options de découverte de l'hôte

Vous pouvez décider si vous souhaitez effectuer une découverte d'hôte avant de lancer une analyse de port pour un hôte, ou vous pouvez supposer que tous les hôtes que vous prévoyez analyser sont en ligne. Si vous choisissez de ne pas traiter tous les hôtes comme en ligne, vous pouvez choisir la méthode de découverte d'hôte à utiliser et, si nécessaire, personnaliser la liste des ports analysés lors de la découverte d'hôte. La découverte d'hôte ne sonde pas les ports répertoriés pour le système d'exploitation ou le serveur; il utilise la réponse sur un port particulier uniquement pour déterminer si un hôte est actif et disponible. Si vous effectuez une découverte d'hôte et qu'un hôte n'est pas disponible, Nmap ne analyse pas les ports sur cet hôte.

Exemple : utilisation de Nmap pour résoudre des systèmes d'exploitation inconnus

Cet exemple décrit une configuration Nmap conçue pour résoudre les systèmes d'exploitation inconnus. Pour un aperçu complet de la configuration de Nmap, consultez Gestion de l'analyse Nmap, à la page 28.

Si le système ne peut pas déterminer le système d'exploitation sur un hôte de votre réseau, vous pouvez utiliser Nmap pour analyser activement l'hôte. Nmap utilise les informations qu'il obtient lors de l'analyse pour évaluer les systèmes d'exploitation possibles. Il utilise ensuite le système d'exploitation ayant la note la plus élevée comme identification du système d'exploitation hôte.

L'utilisation de Nmap pour défier les nouveaux hôtes des informations sur le système d'exploitation et le serveur désactive la surveillance par le système de ces données pour les hôtes analysés. Si vous utilisez Nmap pour découvrir l'hôte et le système d'exploitation du serveur pour les hôtes que le système signale comme ayant des systèmes d'exploitation inconnus, vous pourrez peut-être identifier des groupes d'hôtes similaires. Vous pouvez ensuite créer une empreinte personnalisée basée sur l'une d'entre elles pour que le système associe l'empreinte au système d'exploitation que vous connaissez sur l'hôte en fonction de l'analyse Nmap. Chaque fois que cela est possible, créez une empreinte personnalisée plutôt que de saisir des données statiques via une source tierce comme Nmap, car l'empreinte personnalisée permet au système de continuer à surveiller le système d'exploitation hôte et de le mettre à jour au besoin.

Dans cet exemple, vous devez :

1. Configurez une instance d'analyse comme décrit dans Ajout d'une instance d'analyse Nmap, à la page 29.
2. Créez une correction Nmap en utilisant les paramètres suivants :
   - Activez l' **utilisation du port de l'événement** pour analyser le port associé au nouveau serveur.
   - Activez **Detect Operating System** (détecter le système d'exploitation) pour détecter les renseignements sur le système d'exploitation de l'hôte.

- Activez **la sonde des ports ouverts pour les informations sur le fournisseur et la version** afin de détecter les informations sur le fournisseur et la version du serveur.
- Activez l'option **Traiter tous les hôtes comme en ligne**, car vous savez que l'hôte existe.

3. Créer une règle de corrélation qui se déclenche lorsque le système détecte un hôte doté d'un système d'exploitation inconnu. La règle doit se déclencher lorsqu'un **événement de découverte se produit** et **que les informations sur le système d'exploitation d'un hôte ont changé** et qu'il répond aux conditions suivantes : le **nom du système d'exploitation est inconnu**.
4. Créez une politique de corrélation qui contient la règle de corrélation.
5. Dans la politique de corrélation, ajoutez la correction Nmap que vous avez créée à l'étape 2 en tant que réponse à la règle que vous avez créée à l'étape 3.
6. Activez la politique de corrélation.
7. Purgez les hôtes sur la cartographie du réseau pour forcer le redémarrage de la découverte du réseau et recréer la cartographie du réseau.
8. Après un jour ou deux, recherchez les événements générés par la politique de corrélation. Analysez les résultats Nmap pour les systèmes d'exploitation détectés sur les hôtes pour voir s'il y a une configuration d'hôte particulière sur votre réseau que le système ne reconnaît pas.
9. Si vous trouvez des hôtes avec des systèmes d'exploitation inconnus dont les résultats Nmap sont identiques, créez une empreinte personnalisée pour l'un de ces hôtes et utilisez-la pour identifier des hôtes similaires ultérieurement.

Sujets connexes

Création d'une correction Nmap, à la page 33
Résultats de l'analyse Nmap, à la page 36
Création d'une empreinte personnalisée pour les clients, à la page 6

Exemple : utilisation de Nmap pour répondre aux nouveaux hôtes

Cet exemple décrit une configuration Nmap conçue pour répondre à de nouveaux hôtes. Pour un aperçu complet de la configuration de Nmap, consultez Gestion de l'analyse Nmap, à la page 28.

Lorsque le système détecte un nouvel hôte dans un sous-réseau où des intrusions sont probables, vous pouvez analyser cet hôte pour vous assurer de disposer de renseignements exacts sur sa vulnérabilité.

Vous pouvez y parvenir en créant et en activant une politique de corrélation qui détecte lorsqu'un nouvel hôte apparaît dans ce sous-réseau et qui lance une correction qui effectue une analyse Nmap sur l'hôte.

Pour ce faire, vous devez :

1. Configurez une instance d'analyse comme décrit dans Ajout d'une instance d'analyse Nmap, à la page 29.
2. Créez une correction Nmap en utilisant les paramètres suivants :
   - Activez l' **utilisation du port de l'événement** pour analyser le port associé au nouveau serveur.
   - Activez **Detect Operating System** (détecter le système d'exploitation) pour détecter les renseignements sur le système d'exploitation de l'hôte.
   - Activez **la sonde des ports ouverts pour les informations sur le fournisseur et la version** afin de détecter les informations sur le fournisseur et la version du serveur.

- Activez l'option **Traiter tous les hôtes comme en ligne**, car vous savez que l'hôte existe.

3. Créez une règle de corrélation qui se déclenche lorsque le système détecte un nouvel hôte sur un sous-réseau spécifique. La règle doit se déclencher lorsqu'un **événement de découverte se produit** et **qu'un nouvel hôte est détecté**.
4. Créez une politique de corrélation qui contient la règle de corrélation.
5. Dans la politique de corrélation, ajoutez la correction Nmap que vous avez créée à l'étape 2 en réponse à la règle que vous avez créée à l'étape 3.
6. Activez la politique de corrélation.
7. Lorsque vous êtes informé de la présence d'un nouvel hôte, vérifiez le profil d'hôte pour voir les résultats de l'analyse Nmap et corriger toutes les vulnérabilités qui s'appliquent à l'hôte.

Après avoir activé la politique, vous pouvez consulter régulièrement l'affichage de l'état de la correction (**Analysis (analyse)** > **Correlation** > **Status (état)**) pour vérifier quand la correction a été lancée. La cible d'analyse dynamique de la correction doit inclure les adresses IP des hôtes qu'elle a analysés suite à la détection du serveur. Vérifiez le profil d'hôte de ces hôtes pour voir s'il existe des vulnérabilités qui doivent être traitées pour l'hôte, en fonction du système d'exploitation et des serveurs détectés par Nmap.

Mise en garde Si votre réseau est volumineux ou dynamique, la détection d'un nouvel hôte peut être trop fréquente pour être détectée à l'aide d'une analyse. Pour éviter la surcharge de ressources, évitez d'utiliser les analyses Nmap comme réponse aux événements qui se produisent fréquemment. En outre, notez que l'utilisation de Nmap pour défier les nouveaux hôtes en matière d'informations sur le système d'exploitation et le serveur désactive la surveillance de ces données pour les hôtes analysés.

Sujets connexes

Création d'une correction Nmap, à la page 33

Gestion de l'analyse Nmap

Pour utiliser l'analyse Nmap, vous devez au minimum configurer une instance d'analyse Nmap et une correction Nmap. La configuration d'une cible d'analyse Nmap est facultative.

Procédure

Étape 1 Configurer l'analyse Nmap :

- Ajoutez une instance d'analyse Nmap comme décrit dans Ajout d'une instance d'analyse Nmap, à la page 29.
- Créez une correction Nmap comme décrit dans Création d'une correction Nmap, à la page 33.
- Vous pouvez également ajouter une cible d'analyse Nmap comme décrit dans Ajout d'une cible d'analyse Nmap, à la page 31.

Étape 2 Exécutez l'analyse Nmap :

- Exécutez une analyse Nmap à la demande comme décrit dans Exécution d'une analyse Nmap à la demande, à la page 35.

- Configurez des analyses Nmap automatiques comme décrit dans la section *Automatisation de l'analyse Nmap* dans le fichier Guide d'administration Cisco Secure Firewall Management Center.
- Planifiez des analyses Nmap automatiques comme décrit dans la section *Planification d'une analyse Nmap* dans le fichier Guide d'administration Cisco Secure Firewall Management Center.

Prochaine étape

- Surveiller l'analyse Nmap en cours en visualisant la tâche associée; consultez la section *Affichage des messages en lien avec les tâches* dans le Guide d'administration Cisco Secure Firewall Management Center.
- Vous pouvez également affiner l'analyse :
  - Modifiez une instance d'analyse Nmap comme décrit dans Modification d'une instance d'analyse Nmap, à la page 30.
  - Modifiez une cible d'analyse Nmap comme décrit dans Modification d'une cible d'analyse Nmap, à la page 32.
  - Modifiez une correction Nmap comme décrit dans Modification d'une correction Nmap, à la page 35.

Ajout d'une instance d'analyse Nmap

Vous pouvez configurer une instance d'analyse distincte pour chaque module Nmap que vous souhaitez utiliser pour analyser votre réseau à la recherche de vulnérabilités. Vous pouvez configurer des instances de balayage pour le module Nmap local à l'aide de Cisco Secure Firewall Management Center et pour tous les périphériques que vous souhaitez utiliser pour exécuter des analyses à distance. Les résultats de chaque analyse sont toujours stockés sur le centre de gestion où vous configurez l'analyse, même si vous exécutez l'analyse à partir d'un périphérique distant. Pour éviter l'analyse accidentelle ou malveillante d'hôtes essentiels, vous pouvez créer une liste noire pour l'instance afin d'indiquer les hôtes qui ne doivent jamais être analysés avec l'instance.

Vous ne pouvez pas ajouter une instance d'analyse avec le même nom qu'une instance d'analyse existante.

Dans un déploiement multidomaine, le système affiche les règles créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les instances d'analyse créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier des tableaux personnalisés dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Accédez à la liste des instances d'analyse Nmap en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Actions** > **Instances**.
- Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Ajouter la correction :

- Si vous avez accédé à la liste par la première méthode ci-dessus, localisez la section Add a New Instance (Ajouter une nouvelle instance), choisissez le module Nmap Remédiation (Correction Nmap) dans la liste déroulante, puis cliquez sur **Add** (Ajouter).

- Si vous avez accédé à la liste par la deuxième méthode ci-dessus, cliquez sur **Add Nmap Instance** (Ajouter une instance Nmap).

Étape 3 Saisissez un **nom d'instance**.

Étape 4 Saisissez une **description**.

Étape 5 Éventuellement, dans le champ **Hôtes exemptés**, spécifiez les hôtes ou les réseaux qui ne doivent *jamais* être analysés avec cette instance d'analyse, en utilisant la syntaxe suivante :

- Pour les hôtes IPv6, une adresse IP exacte (par exemple, `2001:DB8::fedd:eeff`)
- Pour les hôtes IPv4, une adresse IP exacte (par exemple, `192.168.1.101`) ou un bloc d'adresses IP à l'aide de la notation CIDR (par exemple, `192.168.1.0/24` analyse les 254 hôtes entre `192.168.1.1` et `192.168.1.254`, compris)
- Notez que vous ne pouvez pas utiliser un point d'exclamation (!) pour annuler une valeur d'adresse.

Remarque Si vous ciblez spécifiquement une analyse vers un hôte qui se trouve dans un réseau sur la liste noire, cette analyse ne s'exécutera pas.

Étape 6 Éventuellement, pour exécuter l'analyse à partir d'un périphérique distant au lieu de centre de gestion, spécifiez l'adresse IP ou le nom du périphérique tel qu'il apparaît dans la page Information du périphérique de l'interface Web centre de gestion, dans le champ **Remote Device Name** (nom du périphérique distant).

Étape 7 Cliquez sur **Create** (créer).
Lorsque le système a terminé de créer l'instance, il l'affiche en mode Modifier.

Étape 8 Ajoutez éventuellement une correction Nmap à l'instance. Pour ce faire, localisez la section de correction configurée de l'instance, cliquez sur **Add**(ajouter) et créez une correction comme décrit dans Création d'une correction Nmap, à la page 33.

Étape 9 Cliquez sur **Annuler** pour revenir à la liste des instances.

Remarque Si vous avez accédé à la liste des instances d'analyse Nmap via l'option **Scanners**, le système n'affiche pas l'instance que vous avez ajoutée, sauf si vous avez également ajouté une correction à l'instance. Pour afficher les instances auxquelles vous n'avez pas encore ajouté de corrections, utilisez l'option de menu **Instances** pour accéder à la liste.

Modification d'une instance d'analyse Nmap

Lorsque vous modifiez une instance d'analyse, vous pouvez afficher, ajouter et supprimer les corrections associées à l'instance. Supprimez une instance d'analyse Nmap lorsque vous ne souhaitez plus utiliser le module Nmap profilé dans l'instance. Notez que lorsque vous supprimez l'instance d'analyse, vous supprimez également toutes les corrections qui utilisent cette instance.

Dans un déploiement multidomaine, le système affiche les règles créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les instances d'analyse créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier des tableaux personnalisés dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Accédez à la liste des instances d'analyse Nmap en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Actions** > **Instances**.
- Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Cliquez sur **Afficher** ( ) à côté de l'instance que vous souhaitez modifier.

Étape 3 Modifiez les paramètres d'instance d'analyse comme décrit dans Ajout d'une instance d'analyse Nmap, à la page 29.

Étape 4 Cliquez sur **Save** (enregistrer).

Étape 5 Cliquez sur **Done (Terminé)**.

Prochaine étape

- Si vous le souhaitez, vous pouvez ajouter une nouvelle correction à l'instance d'analyse. voir Création d'une correction Nmap, à la page 33
- Vous pouvez également modifier une correction associée à l'instance; voir Modification d'une correction Nmap, à la page 35.
- Vous pouvez également supprimer une correction associée à l'instance; voir Exécution d'une analyse Nmap à la demande, à la page 35.
- Vous pouvez également supprimer l'instance d'analyse en cliquant sur **Supprimer** ( ) à côté de celle-ci.

Ajout d'une cible d'analyse Nmap

Lorsque vous configurez un module Nmap, vous pouvez créer et enregistrer des cibles d'analyse qui identifient les hôtes et les ports que vous souhaitez cibler lorsque vous effectuez une analyse à la demande ou planifiée, afin de ne pas avoir à construire une nouvelle cible d'analyse à chaque fois. Une cible d'analyse comprend une adresse IP unique ou un bloc d'adresses IP à analyser, ainsi que les ports sur l'hôte ou les hôtes. Pour les cibles Nmap, vous pouvez également utiliser les adresses par plage d'octets Nmap ou les plages d'adresses IP. Pour de plus amples renseignements sur les adresses par plage d'octets Nmap, consultez la documentation de Nmap à l'adresse http://insecure.org.

Remarque :

- La recherche de cibles d'analyse contenant un grand nombre d'hôtes peut prendre beaucoup de temps. Pour contourner le problème, analysez moins d'hôtes à la fois.
- Les données du serveur et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse Nmap. Si vous prévoyez d'analyser un hôte à l'aide de Nmap, planifiez régulièrement des analyses. Si un hôte est supprimé de la cartographie du réseau, tous les résultats d'analyse Nmap sont rejetés.
- Dans un déploiement multidomaine, le système affiche les cibles d'analyse créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les cibles d'analyse créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les cibles d'analyse dans un domaine inférieur, basculez dans ce domaine.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Dans la barre d'outils, cliquez sur **Cibles**.

Étape 3 Cliquez sur **Créer une cible d'analyse**.

Étape 4 Dans le champ **Name** (Nom), saisissez le nom que vous souhaitez utiliser pour cette cible d'analyse.

Étape 5 Dans la zone de texte **IP Range** (Plage IP), précisez l'hôte ou les hôtes que vous souhaitez analyser en utilisant la syntaxe décrite dans Lignes directrices d'analyse Nmap, à la page 25.

Remarque Si vous utilisez une virgule dans une liste d'adresses ou de plages d'adresses IP dans une cible d'analyse, la virgule est convertie en espace lorsque vous enregistrez la cible.

Étape 6 Dans le champ **Ports**, précisez les ports que vous souhaitez analyser.

Vous pouvez saisir n'importe laquelle des valeurs suivantes, en utilisant des valeurs comprises entre 1 et 65 535 :

- un numéro de port
- une liste de ports séparés par des virgules
- une plage de numéros de port séparés par un tiret
- des plages de numéros de port séparés par des tirets, séparées par des virgules

Étape 7 Cliquez sur **Save** (enregistrer).

Modification d'une cible d'analyse Nmap

Astuces Vous pouvez souhaiter modifier la cible d'analyse dynamique d'une correction si vous ne souhaitez pas utiliser la correction pour analyser une adresse IP spécifique, mais que l'adresse IP a été ajoutée à la cible parce que l'hôte a été impliqué dans une violation de politique de corrélation qui a lancé la correction.

Supprimez une cible d'analyse si vous ne souhaitez plus analyser les hôtes qui y sont répertoriés.

Dans un déploiement multidomaine, le système affiche les cibles d'analyse créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les cibles d'analyse créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les cibles d'analyse dans un domaine inférieur, basculez dans ce domaine.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Dans la barre d'outils, cliquez sur **Cibles**.

Étape 3 Cliquez sur **Edit** (✎) à côté de la cible d'analyse que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Apportez les modifications nécessaires. Pour en savoir plus, consultez Ajout d'une cible d'analyse Nmap, à la page 31.

Étape 5 Cliquez sur **Save** (enregistrer).

Étape 6 Vous pouvez également supprimer la cible de l'analyse en cliquant sur **Supprimer** ( ) à côté d'elle.

Création d'une correction Nmap

Une correction Nmap ne peut être créée qu'en l'ajoutant à une instance d'analyse Nmap existante. La correction définit les paramètres de l'analyse. Elle peut être utilisée comme réponse dans une politique de corrélation, exécutée à la demande ou exécutée comme tâche planifiée à une heure précise.

Les données du serveur et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse Nmap. Si vous prévoyez d'analyser un hôte à l'aide de Nmap, planifiez régulièrement des analyses. Si un hôte est supprimé de la cartographie du réseau, tous les résultats d'analyse Nmap sont rejetés.

Pour des informations générales sur les fonctionnalités de Nmap, consultez la documentation de Nmap à l'adresse http://insecure.org.

Dans un déploiement multidomaine, le système affiche les corrections Nmap créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les corrections Nmap créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les corrections Nmap dans un domaine inférieur, basculez dans ce domaine.

Avant de commencer

- Ajoutez une instance d'analyse Nmap comme décrit dans Ajout d'une instance d'analyse Nmap, à la page 29.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Instances**.

Étape 2 Cliquez sur **Afficher** ( ) à côté de l'instance à laquelle vous souhaitez ajouter la correction.

Étape 3 Dans la section des corrections configurées , cliquez sur **Add** (Ajouter).

Étape 4 Saisissez le **Remediation Name** (nom de correction).

Étape 5 Saisissez une **description**.

Étape 6 Si vous prévoyez utiliser cette correction en réponse à une règle de corrélation qui se déclenche lors d'une intrusion, d'un événement de connexion ou d'un événement utilisateur, configurez l'option**Analyse Quelle(s) adresse(s) de l'événement?**.

Astuces Si vous prévoyez utiliser cette correction en réponse à une règle de corrélation qui se déclenche sur un événement de découverte ou un événement d'entrée de l'hôte, par défaut la correction analyse l'adresse IP de l'hôte impliqué dans l'événement ; vous n'avez pas besoin de configurer cette option.

Remarque N'affectez **pas** de correction Nmap comme réponse à une règle de corrélation qui se déclenche lors d'une modification de profil de trafic.

Étape 7 Configurez l'option **Scan Type** (type d'analyse).

Étape 8 Éventuellement, pour analyser les ports UDP en plus des ports TCP, choisissez **On** (Activer) pour l'option **de balayage des ports UDP**.

Astuces Une analyse de ports UDP prend plus de temps qu'une analyse de ports TCP. Pour accélérer vos analyses, laissez cette option désactivée.

Étape 9 Si vous prévoyez utiliser cette correction en réponse à des violations de la politique de corrélation, configurez l'option **Use Port from Event** (utiliser le port à partir de l'événement).

Étape 10 Si vous prévoyez utiliser cette correction en réponse à des violations de la politique de corrélation et que vous souhaitez exécuter l'analyse à l'aide du périphérique exécutant le moteur de détection qui a détecté l'événement, configurez l'option **Analyse à partir du moteur de détection de rapports**.

Étape 11 Configurez l'option **d'analyse rapide des ports**.

Étape 12 Dans le champ **Plages de ports et ordre d'analyse**, saisissez les ports que vous souhaitez analyser par défaut, en utilisant la syntaxe de spécification de port de Nmap, dans l'ordre dans lequel vous souhaitez analyser ces ports.

Utilisez le format suivant :

- Spécifiez des valeurs de 1 à 65 535.
- Séparez les ports par des virgules ou des espaces.
- Utilisez un tiret pour indiquer une plage de ports.
- Lors de l'analyse des ports TCP et UDP, commencez la liste des ports TCP que vous souhaitez analyser par un T et la liste des ports UDP par un U.

Remarque L'option **Use Port from Event** (utiliser le port de l'événement) remplace ce paramètre lorsque la correction est lancée en réponse à une violation de politique de corrélation, comme décrit à l'étape 8.

Exemple :

Pour analyser les ports 53 et 111 pour le trafic UDP, puis analyser les ports 21-25 pour le trafic TCP, saisissez `U:53,111, T:21-25`.

Étape 13 Pour sonder les ports ouverts à la recherche d'informations sur le fournisseur et la version du serveur, configurez **Sonder les ports ouverts à la recherche des informations sur le fournisseur et la version**.

Étape 14 Si vous choisissez de sonder les ports ouverts, définissez le nombre de sondes utilisées en choisissant un nombre dans la liste déroulante **Service Version Intensity** (Intensité de version de service).

Étape 15 Pour analyser le système d'exploitation, configurez les paramètres **de détection du système d'exploitation**.

Étape 16 Pour déterminer s'il y a découverte d'hôte et si les analyses de ports sont exécutées uniquement sur les hôtes disponibles, configurez **Traiter tous les hôtes en ligne**.

Étape 17 Pour définir la méthode que vous souhaitez que Nmap utilise lors des tests de disponibilité de l'hôte, choisissez une méthode dans la liste déroulante **Host Discovery Method** (Méthode e découverte de l'hôte).

Étape 18 Si vous souhaitez analyser une liste personnalisée de ports lors de la découverte d'hôte, saisissez une liste de ports appropriée pour la méthode de découverte d'hôte que vous avez choisie, séparés par des virgules, dans le champ **Host Discovery Port List** 5List des ports de découverte de l'hôte).

Étape 19 Configurez l'option **Default NSE Scripts** pour contrôler s'il faut utiliser l'ensemble par défaut de scripts Nmap pour la découverte d'hôte et de serveur, le système d'exploitation et la découverte de vulnérabilité.

Astuces Consultez http://nmap.org/nsedoc/categories/default.html pour obtenir la liste des scripts par défaut.

Étape 20 Pour définir la synchronisation du processus d'analyse, choisissez un numéro de modèle de synchronisation dans la liste déroulante **Timing Template** (modèle de synchronisation).

Choisissez une valeur plus élevée pour une analyse plus rapide et moins complète et une valeur plus basse pour une analyse plus lente et plus complète.

Étape 21 Cliquez sur **Create** (créer).
Lorsque le système a terminé de créer la correction, il l'affiche en mode de modification.

Étape 22 Cliquez sur **Done** (Terminer) pour revenir à l'instance associée.

Étape 23 Cliquez sur **Cancel** (Annuler) pour revenir à la liste des instances.

Sujets connexes

Options de correction de Nmap, à la page 20

Modification d'une correction Nmap

Les modifications que vous apportez aux corrections Nmap n'affectent pas les analyses en cours. Les nouveaux paramètres prennent effet au démarrage de la prochaine analyse. Supprimez une correction Nmap si vous n'en avez plus besoin.

Dans un déploiement multidomaine, le système affiche les corrections Nmap créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les corrections Nmap créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les corrections Nmap dans un domaine inférieur, basculez dans ce domaine.

Procédure

Étape 1 Accédez à la liste des instances d'analyse Nmap en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Actions** > **Instances**.
- Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Accédez à la correction que vous souhaitez modifier :

- Si vous avez accédé à la liste par la première méthode ci-dessus, cliquez sur **Afficher** ( ) à côté de l'instance concernée, puis cliquez de nouveau à côté de la correction que vous souhaitez modifier dans la section des corrections configurées.
- Si vous avez accédé à la liste par la deuxième méthode ci-dessus, cliquez sur **Afficher** ( ) à côté de la correction que vous souhaitez modifier.

Étape 3 Apportez les modifications nécessaires, comme décrit dans Création d'une correction Nmap, à la page 33.

Étape 4 Cliquez sur **Save** (Enregistrer) si vous souhaitez enregistrer vos modifications ou sur **Done** (Terminé) si vous souhaitez quitter sans enregistrer.

Étape 5 Vous pouvez également supprimer la correction en cliquant sur **Supprimer** ( ) à côté de celle-ci.

Exécution d'une analyse Nmap à la demande

Vous pouvez lancer des analyses Nmap à la demande chaque fois que nécessaire. Vous pouvez définir la cible d'une analyse à la demande en saisissant les adresses IP et les ports que vous souhaitez analyser ou en choisissant une cible d'analyse existante.

Les données du serveur et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse Nmap. Si vous prévoyez d'analyser un hôte à l'aide de Nmap, planifiez régulièrement des analyses. Si un hôte est supprimé de la cartographie du réseau, tous les résultats d'analyse Nmap sont rejetés.

Avant de commencer

- Vous pouvez également ajouter une cible d'analyse Nmap; voir Ajout d'une cible d'analyse Nmap, à la page 31.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 À côté de la correction Nmap que vous souhaitez utiliser pour effectuer l'analyse, cliquez sur **Numérisation** ( ).

Étape 3 Éventuellement, pour analyser à l'aide d'une cible d'analyse enregistrée, choisissez une cible dans la liste déroulante **Saved Targets** (Cibles enregistrées) et cliquez sur **Load** (Téléverser).

Étape 4 Dans le champ **IP range(s)** (Plages IP), précisez l'adresse IP des hôtes que vous souhaitez analyser ou modifiez la liste téléversée.

Remarque :

- Pour les hôtes avec des adresses IPv4, vous pouvez spécifier plusieurs adresses IP séparées par des virgules ou utiliser la notation CIDR. Vous pouvez également annuler les adresses IP en les faisant précéder d'un point d'exclamation (!).
- Pour les hôtes avec des adresses IPv6, utilisez une adresse IP exacte. Les plages ne sont pas prises en charge.

Étape 5 Dans le champ **Ports**, précisez les ports que vous souhaitez analyser ou modifiez la liste téléversée.

Vous pouvez saisir un numéro de port, une liste de ports séparés par des virgules ou une plage de numéros de ports séparés par un tiret.

Étape 6 Dans un déploiement multidomaine, utilisez le champ **Domaine** pour préciser le domaine descendant dans lequel vous souhaitez effectuer l'analyse.

Étape 7 Cliquez sur **Analyser maintenant**.

Prochaine étape

- Si vous le souhaitez, vous pouvez suivre l'état de la tâche; voir *Affichage des messages de la tâche* dans la section Guide d'administration Cisco Secure Firewall Management Center.

Résultats de l'analyse Nmap

Vous pouvez surveiller les analyses Nmap en cours, importer les résultats d'analyses effectuées précédemment à l'aide du système Firepower ou des résultats obtenus à l'extérieur du système Firepower, puis afficher et analyser les résultats d'analyse.

Vous pouvez afficher les résultats d'analyse que vous créez en utilisant le module Nmap local sous forme de page rendue dans une fenêtre contextuelle. Vous pouvez également télécharger le fichier de résultats Nmap au format XML brut.

Vous pouvez également afficher les informations sur le système d'exploitation et le serveur détectés par Nmap dans les profils d'hôte et dans la cartographie du réseau. Si l'analyse d'un hôte produit des informations de serveur pour des serveurs sur des ports filtrés ou fermés, ou si une analyse collecte des informations qui ne peuvent pas être incluses dans les informations sur le système d'exploitation ou la section serveurs, le profil d'hôte inclut ces résultats dans une section de résultats d'analyse Nmap.

Affichage des résultats de l'analyse Nmap

Lorsqu'une analyse Nmap est terminée, vous pouvez afficher un tableau des résultats de l'analyse.

Vous pouvez manipuler l'affichage des résultats en fonction des informations que vous recherchez. La page qui s'affiche lorsque vous accédez aux résultats d'analyse diffère selon le flux de travail que vous utilisez. Vous pouvez utiliser le flux de travail prédéfini, qui comprend un affichage sous forme de tableau des résultats d'analyse. Vous pouvez également créer un flux de travail personnalisé qui affiche uniquement les informations correspondant à vos besoins spécifiques.

Dans un déploiement multidomaine, vous pouvez afficher les données du domaine actuel et de tous les domaines descendants. Vous ne pouvez pas afficher les données des domaines de niveau supérieur ou connexes.

Vous pouvez télécharger et afficher les résultats de Nmap à l'aide de la DTD Nmap version 1.01, disponible à l'adresse http://insecure.org.

Vous pouvez également effacer les résultats de l'analyse.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Dans la barre d'outils, cliquez sur **Résultats de l'analyse**.

Étape 3 Vous avez les choix suivants :

- Ajustez la plage temporelle comme décrit dans *Contraintes de temps de l'événement* dans Guide d'administration Cisco Secure Firewall Management Center.
- Pour utiliser un autre flux de travail, y compris un flux de travail personnalisé, cliquez sur **(changer de flux de travail)** à côté du titre du flux de travail.
- Pour afficher les résultats de l'analyse sous la forme d'une page rendue dans une fenêtre contextuelle, cliquez sur **View** (afficher) à côté de la tâche d'analyse.
- Pour enregistrer une copie du fichier de résultats de l'analyse afin de pouvoir afficher le code XML brut dans n'importe quel éditeur de texte, cliquez sur **Télécharger** à côté de la tâche d'analyse.
- Pour trier les résultats de l'analyse, cliquez sur le titre de la colonne. Cliquez à nouveau sur le titre de la colonne pour inverser l'ordre de tri.
- Pour limiter les colonnes qui s'affichent, cliquez sur **Fermer** (×) dans l'en-tête de la colonne que vous souhaitez masquer. Dans la fenêtre contextuelle qui apparaît, cliquez sur **Apply** (Appliquer).

  Astuces Pour masquer ou afficher d'autres colonnes, cochez ou décochez les cases appropriées avant de cliquer sur **Apply** (Appliquer). Pour rajouter une colonne désactivée à la vue, cliquez sur la flèche de développement afin de développer les contraintes de recherche, puis cliquez sur le nom de la colonne sous **Colonnes désactivées**.

- Pour passer à la page suivante dans le flux de travail, consultez *Utilisation des pages d'exploration avant* dans Guide d'administration Cisco Secure Firewall Management Center.
- Pour configurer les instances de balayage et la correction, cliquez sur **Analyseurs** dans la barre d'outils et consultez Gestion de l'analyse Nmap, à la page 28.
- Pour naviguer dans les pages de flux de travail et entre elles, consultez *Outils de navigation dans les pages de flux de travail* dans Guide d'administration Cisco Secure Firewall Management Center.
- Pour accéder à d'autres affichages d'événements afin d'afficher les événements associés, choisissez le nom de l'affichage d'événements que vous souhaitez voir dans la liste déroulante **Aller à**.
- Pour rechercher des résultats d'analyse, saisissez vos critères de recherche dans les champs appropriés.

Sujets connexes

Champs des résultats de l'analyse Nmap, à la page 38

Champs des résultats de l'analyse Nmap

Lorsque vous exécutez une analyse Nmap, centre de gestion collecte les résultats de l'analyse dans une base de données. Le tableau suivant décrit les champs du tableau des résultats d'analyse qui peuvent être affichés et recherchés.

Tableau 2 : Champs des résultats de l'analyse Nmap

Champ	Description
Heure de début	La date et l'heure de début de l'analyse qui a produit les résultats.
Heure de fin	La date et l'heure de fin de l'analyse qui a produit les résultats.
Cible	Adresse IP (ou nom d'hôte, si la résolution DNS est activée) de la cible de l'analyse pour l'analyse qui a produit les résultats.
Type d'analyse	Soit `Nmap`, soit le nom de l'analyseur tiers pour indiquer le type d'analyse qui a produit les résultats.
Mode de balayage	Le mode d'analyse qui a produit les résultats : • `À la demande` : résultats des analyses exécutées à la demande. • `Importé` : résultats des analyses effectuées sur un autre système et importés dans centre de gestion. • `Planifié` : résultats des analyses exécutées en tant que tâche planifiée.
Résultats	Les résultats de l'analyse.
Domaine	Domaine de la cible de l'analyse. Ce champ n'est présent que dans un déploiement multidomaine.

Importer les résultats de l'analyse Nmap

Vous pouvez importer des fichiers de résultats XML créés par une analyse Nmap effectuée à l'extérieur du système Firepower. Vous pouvez également importer des fichiers de résultats XML que vous avez

précédemment téléchargés à partir du système Firepower. Pour importer les résultats d'analyse Nmap, le fichier de résultats doit être au format XML et respecter la DTD version 1.01. Pour de plus amples renseignements sur la création de résultats Nmap et sur la DTD Nmap, consultez la documentation de Nmap à l'adresse http://insecure.org.

Un hôte doit déjà exister dans la cartographie du réseau pour que Nmap puisse ajouter ses résultats au profil d'hôte.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Dans la barre d'outils, cliquez sur **Importer les résultats**.

Étape 3 Dans un déploiement multidomaine, choisissez un domaine descendant dans la liste déroulante **Domain** (domaine) pour préciser où vous souhaitez stocker les résultats importés.

Étape 4 Cliquez sur **Parcourir** pour accéder au fichier de résultats.

Étape 5 De retour à la page Import Resolutions, cliquez sur **Import** pour importer les résultats.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.