Intégration de pxGrid de version 1.3 ISE avec l'application de pxLog IPS

Contenu

Introduction

La version 1.3 du Cisco Identity Services Engine (ISE) prend en charge un nouveau pxGrid appelé par API. Ces protocole qui prend en charge l'authentification, cryptage, et privilèges modernes et flexibles (groupes) tient compte de l'intégration facile avec d'autres solutions de sécurité. Ce document décrit l'utilisation de l'application de pxLog qui a été écrite comme validation de principe. le pxLog peut recevoir des messages de Syslog du Système de prévention d'intrusion (IPS) et envoyer des messages de pxGrid à l'ISE afin de mettre en quarantaine l'attaquant. En conséquence, modification de RAYON d'utilisations ISE de l'autorisation (CoA) afin de changer l'état d'autorisation du point final qui limite l'accès au réseau. Toute la ceci arrive d'une manière transparente à l'utilisateur final.

Pour cet exemple, Snort a été utilisé comme IPS, mais n'importe quelle autre solution pourrait être utilisée. En fait ce ne doit pas être un IPS. Tout ce qui est exigé est d'envoyer le message de Syslog au pxLog avec l'adresse IP de l'attaquant. Ceci crée une possibilité pour l'intégration d'un grand nombre de solutions.

Ce document présente également comment dépanner et tester des solutions de pxGrid, avec les problèmes et les limites typiques.

Déni de responsabilité : L'application de pxLog n'est pas prise en charge par Cisco. Cet article a été écrit comme validation de principe. L'objectif principal était de l'utiliser pendant betatesting de l'implémentation de pxGrid sur l'ISE.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez l'expérience avec la configuration de Cisco ISE et la connaissance de base de ces thèmes :

- Déploiements ISE et configuration d'autorisation
- Configuration CLI des commutateurs Cisco Catalyst

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7
- Logiciel de commutateur de gamme de Cisco Catalyst 3750X, versions 15.0 et ultérieures
- Logiciel de Cisco ISE, versions 1.3 et ultérieures
- Sécurité mobile de Cisco AnyConnect avec l'Access Manager de réseau (NAM), version 3.1 et ultérieures
- Version 2.9.6 de Snort avec par acquisition de données (DAQ)
- application de pxLog installée sur le Tomcat 7 avec la version 5 de MySQL

Schéma de réseau et circulation

Voici la circulation, comme illustré dans le schéma de réseau :

1. Un utilisateur de Microsoft Windows 7 se connecte au commutateur et exécute l'authentification de 802.1x.

2. Le commutateur utilise l'ISE en tant que serveur d'Authentification, autorisation et comptabilité (AAA). La règle d'autorisation d'**accès complet de dot1x** est appariée et le plein accès au réseau est accordé (DACL : PERMIT_ALL).

3. Les essais d'utilisateur à connecter au réseau de confiance et viole la règle de renifler.

4. En conséquence, reniflez envoie une alerte à l'application de pxLog (par l'intermédiaire du Syslog).

5. L'application de pxLog exécute la vérification contre sa base de données locale. Il est configuré afin d'attraper des messages de Syslog envoyés par Snort et extraire l'adresse IP de l'attaquant. Alors il emploie le pxGrid pour envoyer une demande vers l'ISE afin de mettre en quarantaine l'adresse IP d'attaquant (l'ISE est un contrôleur de pxGrid).

6. L'ISE réévalue sa stratégie d'autorisation. Puisque le point final est mis en quarantaine, la **session :** La condition de **quarantaine d'ÉGAUX d'EPSStatus** est remplie et un profil différent d'autorisation est apparié (**quarantaine de dot1x**). L'ISE envoie un CoA se termine au commutateur afin de terminer la session. Ceci déclenche la ré-authentification et un nouvel ACL téléchargeable (DACL) (PERMIT_ICMP) est appliqué, qui fournit l'accès au réseau limité à l'utilisateur final.

7. Àce stade, l'administrateur pourrait décider à l'unquarantine le point final. Ceci peut être réalisé par l'intermédiaire du GUI du pxLog. De nouveau, le message de pxGrid vers l'ISE est envoyé.

8. L'ISE exécute une exécution semblable comme dans l'étape 6. Cette fois, le point final n'est plus mis en quarantaine et l'accès complet est fourni.

pxLog

Architecture

La solution est d'installer un ensemble d'applications sur une machine Linux :

1. L'application de pxLog écrite à Javas et déployée sur le serveur de Tomcat. Cette application se compose :

   Servlet ce requêtes Web de processus - Ceci est utilisé afin d'accéder au panneau administratif par l'intermédiaire du navigateur Web.

   Module d'autorité - Filetez qui est commencé ainsi que le servlet. L'autorité lit des messages de Syslog à partir du fichier (optimisé), traite ces messages selon les règles configurées, et exécute des actions (comme la quarantaine par l'intermédiaire du pxGrid).

2. La base de données mysql qui contient la configuration pour le pxLog (des règles et des logs).

3. Le serveur de Syslog qui reçoit des messages de Syslog des systèmes externes et les écrit à un fichier.

Installation

L'application de pxLog utilise ces bibliothèques :

- jQuery (pour le support d'AJAX)
- JavaServer pagine la bibliothèque standard de balise (JSTL) (le modèle modèle de contrôleur de vue (MVC), des données est séparé de la logique : Le code de la page de JavaServer (JSP) n'est utilisé pour rendre seulement, aucun code HTML dans des classes de Javas)
- Log4j comme sous-système se connectant
- Connecteur de MySQL
- displaytag pour rendre/triant des tables
- pxGrid API par Cisco (en cours alpha 147 de version)

Toutes ces bibliothèques sont déjà dans le répertoire de bibliothèque du projet tellement là ne sont aucun besoin de télécharger plus de fichiers d'archives de Javas (POT).

Afin d'installer l'application :

1. Éclatez le répertoire entier au répertoire de Tomcat Webapp.

2. Éditez le **fichier WEB-INF/web.xml**. La seule modification exigée est la serveripvariable, qui devrait indiquer l'ISE. Également Javas délivrent un certificat KeyStores (un pour fait confiance et un pour l'identité) pourraient être générées (au lieu du par défaut). Ceci est utilisé par le pxGrid API qui utilise la session de Secure Sockets Layer (SSL) avec les les deux les Certificats de client et serveur. Les deux côtés de la nécessité de transmission de présenter avec le certificat et de devoir se faire confiance. Référez-vous au pour en savoir plus de section de conditions requises de Protocol de pxGrid.

3. Assurez-vous que l'adresse Internet ISE est résolue correctement sur le pxLog (référez-vous

à l'enregistrement dans le Domain Name Server (DN) ou l'**entrée de /etc/hosts**). Référez-vous au pour en savoir plus de section de conditions requises de Protocol de pxGrid.

4. Configurez la base de données mysql avec le **script mysql/init.sql**. Des qualifications peuvent être changées mais devraient être reflétées dans le **fichier WEB-INF/web.xml.**

Reniflez

Cet article ne se concentre sur aucune particularité IPS, qui est pourquoi seulement une brève explication est fournie.

Snort est configuré comme en ligne avec le support DAQ. Le trafic est réorienté avec des iptables :

```
iptables -I FORWARD -j ACCEPT
iptables -I FORWARD -j NFQUEUE --queue-num 1
```

Puis, après inspection, il est injecté et expédié selon des règles iptable par défaut.

Quelque la coutume reniflent des règles ont été configurées (le fichier de **/etc/snort/rules/test.rules** est inclus en configuration globale).

```
alert icmp any any -> any any (itype:8; dsize:666<>686; sid:100122)
alert icmp any any -> any any (itype:8; ttl: 6; sid:100124)
```

Reniflez envoie un message de Syslog quand le Time to Live (TTL) du paquet est égal à 6 ou la taille de la charge utile est entre 666 et 686. Le trafic n'est pas bloqué par Snort.

Également des seuils devraient être installés pour s'assurer que les alertes ne sont pas déclenchées trop souvent (**/etc/snort/threshold.conf**) :

```
event_filter gen_id 1, sig_id 100122, type limit, track by_src, count 1, seconds 60
event_filter gen_id 1, sig_id 100124, type limit, track by_src, count 1, seconds 60
```

Puis les points de serveur de Syslog à l'ordinateur de pxLog (**/etc/snort/snort.conf**) :

```
output alert_syslog: host=10.222.0.61:514, LOG_AUTH LOG_ALER
```

Pour quelques versions Snort, il y a des bogues liées à la configuration de Syslog, et alors on pourrait utiliser les valeurs par défaut qui indiquent le localhost et le Syslog-NG pourrait être configuré afin d'expédier les messages spécifiques à l'hôte de pxLog.

ISE

Configuration

Person et certificat

1. Activez le rôle de pxGrid, qui est désactivé sur l'ISE par défaut, sous la **gestion > le déploiement** :

2. Vérifiez si les Certificats sont utilisés pour le pxGrid sous la **gestion > les Certificats > les Certificats de système** :

Service de protection de point final (ENV)

L'ENV devrait être activée (désactivé par défaut) de la **gestion > des configurations** :

Ceci te permet pour utiliser la fonctionnalité de quarantaine/unquarantine.

Règles d'autorisation

La première règle est produite seulement quand le point final est mis en quarantaine. L'accès alors limité est dynamiquement imposé par le CoA de RAYON. Le commutateur doit également être ajouté aux périphériques de réseau avec le secret partagé correct.

Dépannez

L'état de pxGrid peut être vérifié avec le CLI :

```
lise/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          6717
Database Server                        running          51 PROCESSES
Application Server                     running          9486
Profiler Database                      running          7804
AD Connector                           running          10058
M&T Session Database                   running          7718
M&T Log Collector                      running          9752
M&T Log Processor                      running          9712
Certificate Authority Service          running          9663
pxGrid Infrastructure Service          running          14979
pxGrid Publisher Subscriber Service    running          15281
pxGrid Connection Manager              running          15248
pxGrid Controller                      running          15089
Identity Mapping Service               running          9962
```

Il y a également distinct met au point pour le pxGrid (**gestion > se connectant > configuration > pxGrid de log de debug**). Des fichiers de debug sont enregistrés dans le répertoire de pxGrid. Les données les plus importantes sont dans le **pxgrid/pxgrid-jabberd.log et le** pxgrid/pxgrid-controller.log**.**

Test

Step1. Inscription au pxGrid

L'application de pxLog est automatiquement déployée quand des débuts de Tomcat.

1. Afin d'utiliser le pxGrid, enregistrez deux utilisateurs dans l'ISE (un avec l'accès de session, et un avec la quarantaine). Ceci peut être terminé des **utilisateurs d'exécutions > de registre de Pxgrid** :

   L'enregistrement commence automatiquement :

2. Àce stade, il est nécessaire d'approuver des utilisateurs enregistrés sur l'ISE (l'approbation automatique est désactivée par défaut) :

   Après l'approbation, le pxLog informe automatiquement l'administrateur (par l'intermédiaire d'un appel d'AJAX) :

   ISE affiche l'état pour ces deux utilisateurs en tant qu'en ligne ou off-line (pas en attendant plus).

Step2. le pxLog ordonne la configuration

le pxLog doit traiter des messages de Syslog et exécuter des actions basées sur lui. Afin d'ajouter une nouvelle règle, choisie **gérez les règles** :

Maintenant le module d'autorité recherche cette expression régulière (RegExp) dans le message de Syslog : « reniflez [». Si trouvé, il recherche toutes les adresses IP et sélectionne celui avant dernières. Ceci apparie la plupart des solutions de sécurité. Référez-vous au pour en savoir plus de section de Syslog. Cette adresse IP (attaquant) est mise en quarantaine par l'intermédiaire du pxGrid. Également une règle plus granulaire pourrait être utilisée (par exemple, elle pourrait inclure le nombre de signature).

Step3. Première session de dot1x

La station de Microsoft Windows 7 initie une session de câble de dot1x. Cisco Anyconnect NAM a été utilisé en tant que suppliant. La méthode de l'EAP Protocol-protégée par authentification extensible (EAP-PEAP) est configurée.

Le profil d'autorisation d'**accès complet de dot1x** ISE est sélectionné. Le commutateur télécharge la liste d'accès afin d'accorder l'accès complet :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
```

```
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ALL-53fc9dbe
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E6BAB267CF
     Acct Session ID:  0x00003A70
              Handle:  0xA100080E

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
    permit ip any any
```

Step4. Le PC de Microsoft Windows envoie le paquet qui déclenche l'alarme

Ceci affiche ce qui se produit si vous envoyez d'un paquet de Microsoft Windows avec TTL = 7 :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ALL-53fc9dbe
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E6BAB267CF
     Acct Session ID:  0x00003A70
              Handle:  0xA100080E

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
    permit ip any any
```

Que la valeur est décrémentée sur Snort dans la chaîne d'expédition et une alarme est augmenté. En conséquence, un message de Syslog vers le pxLog est envoyé :

```
Sep  6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 ->
10.222.0.61
```

Step5. pxLog

Le pxLog reçoit le message de Syslog, traite lui, et des demandes mettre en quarantaine cette adresse IP. Ceci peut être confirmé si vous vérifiez les logs :

Step6. Quarantaine ISE

Les états ISE que l'adresse IP a été mise en quarantaine :

En conséquence, il passe en revue la stratégie d'autorisation, choisit la quarantaine, et envoie le CoA de RAYON afin de mettre à jour l'état d'autorisation sur le commutateur pour ce point final spécifique.

C'est le CoA terminent le message qui force le suppliant pour initier une nouvelle session et pour obtenir l'accès limité (Permit_ICMP) :

Le résultat peut être confirmé sur le commutateur (accès limité pour le point final) :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

Step7. pxLog Unquarantine

Àce stade, l'administrateur décide à l'unquarantine qui point final :

La même exécution peut être exécutée directement de l'ISE :

Step8. ISE Unquarantine

L'ISE de nouveau passe en revue les règles et met à jour l'état d'autorisation sur le commutateur (on accorde le plein accès au réseau) :

L'état confirme :

fonctionnalité de pxLog

L'application de pxLog a été écrite afin d'expliquer la fonctionnalité du pxGrid API. Il vous permet à :

- Enregistrez la session et les utilisateurs ENV sur l'ISE
- Téléchargez les informations sur toutes les sessions actives sur l'ISE
- Téléchargez les informations sur une session active spécifique sur l'ISE (par l'adresse IP)
- Téléchargez les informations sur un utilisateur actif spécifique sur l'ISE (par le nom d'utilisateur)
- Affichez les informations sur tous les profils (le profileur)
- Affichez les informations sur les balises de groupe de sécurité de TrustSec (SGTs) définies sur l'ISE
- Version de contrôle (capacités de pxGrid)
- Quarantaine basée sur l'IP ou l'adresse MAC
- Unquarantine a basé sur l'IP ou l'adresse MAC

Plus de fonctionnalité est prévue à l'avenir.

Voici quelques captures d'écran d'exemple de pxLog :

conditions requises de Protocol de pxGrid

Groupes

Le client (utilisateur) peut être un membre d'un groupe à la fois. Les deux groupes les plus utilisés généralement sont :

- Session - Utilisé afin de parcourir/informations de téléchargement sur des sessions/profils/SGTs
- ENV - Utilisé afin d'exécuter la quarantaine

Certificats et Javas KeyStore

Comme mentionné précédemment, le contrôleur de les deux applications cliente, de pxLog et de pxGrid (ISE), doit avoir des Certificats configurés afin de communiquer. L'application de pxLog maintient ceux dans les fichiers de KeyStore de Javas :

- **mémoire/client.jks -** Inclut le client et les Certificats d'Autorité de certification (CA)
- **mémoire/root.jks -** Inclut la chaîne ISE : Identité du noeud de surveillance et de dépannage (MNT) et le certificat de CA

Des fichiers sont protégés par mot de passe (par défaut : cisco123). L'emplacement de fichier et les mots de passe peuvent être changés dans **WEB-INF/web.xml.**

Voici les étapes pour générer nouvelle Java KeyStore :

1. Afin de créer un keystore de racine (faite confiance), importez le certificat de CA (**cert-ca.der devrait** être dans le format DER) :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

2. Quand vous créez un nouveau keystore, choisissez un mot de passe, qui est utilisé plus tard afin d'accéder au keystore.

3. Importez le certificat d'identité MNT au keystore de racine (**cert-mnt.der est le** certificat d'identité pris d'ISE et devrait être dans le format DER) :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
```

```
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

4. Afin de créer le keystore de client, importez le certificat de CA :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

5. Créez une clé privée dans le keystore de client :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

6. Générez une demande de signature de certificat (CSR) dans le keystore de client :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

7. Signez le cert-client.csr et importez le certificat client signé :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

8. Vérifiez que les deux keystores contiennent les Certificats corrects :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

Attention : Quand le noeud ISE 1.3 est mis, il y a à jour une option de garder le certificat d'identité, mais la signature CA est enlevée. En conséquence, l'ISE mis à jour utilise un nouveau certificat mais ne relie jamais le certificat de CA dans le message SSL/ServerHello. Ceci déclenche la panne sur le client qui compte (selon le RFC) voir une pleine chaîne.

Adresse Internet

Le pxGrid API pour plusieurs fonctions (comme le téléchargement de session) exécute la validation supplémentaire. Le client entre en contact avec l'ISE et reçoit l'adresse Internet ISE, qui est définie par la commande d'adresse Internet dans le CLI. Puis, les essais de client pour exécuter la résolution de DN pour cette adresse Internet et essais d'entrer en contact avec et chercher des données de cette adresse IP. Si la résolution de DN pour l'adresse Internet ISE échoue, le client n'essaye pas de n'obtenir aucune donnée.

Attention : Notez que seulement l'adresse Internet est utilisé pour cette résolution, qui est **lise** dans ce scénario, pas le nom de domaine complet (FQDN), qui est **lise.example.com** dans ce scénario.

Note pour des développeurs

Cisco édite et prend en charge le pxGrid API. Il y a un module nommé comme ceci :

pxgrid-sdk-1.0.0-167

Àl'intérieur de lui y a :

- fichiers jar de pxGrid avec les classes, qui peuvent être facilement décodées aux fichiers de

Javas pour vérifier le code
- Javas KeyStores d'échantillon avec des Certificats
- Exemples de script qui utilisent les classess de Javas d'échantillon qui utilisent le pxGrid

Syslog

Voici la liste de solutions de sécurité qui envoient des messages de Syslog avec l'adresse IP d'attaquant. Ceux-ci peuvent être facilement intégrés avec le pxLog tant que vous utilisez la règle correcte de RegExp dans la configuration.

Reniflez

Reniflez envoie des alertes de Syslog dans ce format :

```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

3750#show ip access-lists interface g0/17
     permit icmp any any
```

Voici un exemple :

```
snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61
```

L'adresse IP d'attaquant est toujours la deuxième avant dernière (destination). Il est simple de construire un RegExp granulaire pour une signature spécifique et d'extraire l'adresse IP d'attaquant. Voici un exemple RegExp pour la signature 100124 et le Protocole ICMP (Internet Control Message Protocol) de message :

```
snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61
```

Inspection de l'appliance de sécurité adaptable Cisco (ASA)

Quand l'ASA est configurée pour l'inspection de HTTP (exemple), le message correspondant de Syslog ressemble à ceci :

```
Mar 12 2014 14:36:20: %ASA-5-415006: HTTP - matched Class 23:
        MS13-025_class in policy-map MS_Mar_2013_policy, URI matched -
        Dropping connection from inside:192.168.60.88/2135 to
        outside:192.0.2.63/80
```

De nouveau un RegExp granulaire a pu être utilisé afin de filtrer ces messages et extraire l'adresse IP d'attaquant, le deuxième avant dernière.

Systèmes de prévention des intrusions de nouvelle génération de Cisco Sourcefire (NGIPS)

Voici un message d'exemple envoyé par le capteur de Sourcefire :

```
Jan 28 19:46:19 IDS01 SFIMS: [CA IDS][Policy1][119:15:1] http_inspect: OVERSIZE
REQUEST-URI DIRECTORY [Classification: Potentially Bad Traffic] [Priority: 2]
{TCP} 10.12.253.47:55504 -> 10.15.224.60:80
```

Tellement de nouveau, il est simple d'extraire l'adresse IP d'attaquant parce que la même logique s'applique. Également le nom de stratégie et la signature est fourni, ainsi la règle de pxLog peut être granulaire.

Genévrier NetScreen

Voici un message d'exemple envoyé par la détection d'intrusion de genévrier et la prévention plus anciennes (IDP) :

```
dayId="20061012" recordId="0" timeRecv="2006/10/12
21:52:21" timeGen="2006/10/12 21:52:21" domain="" devDomVer2="0"
device_ip="10.209.83.4" cat="Predefined" attack="TROJAN:SUBSEVEN:SCAN"
srcZn="NULL" srcIntf="NULL" srcAddr="192.168.170.20" srcPort="63396"
natSrcAddr="NULL" natSrcPort="0" dstZn="NULL" dstIntf="NULL"
dstAddr="192.168.170.10" dstPort="27374" natDstAddr="NULL" natDstPort="0"
protocol="TCP" ruleDomain="" ruleVer="5" policy="Policy2" rulebase="IDS"
ruleNo="4" action="NONE" severity="LOW" alert="no" elaspedTime="0" inbytes="0"
outbytes="0" totBytes="0" inPak="0" outPak="0" totPak="0" repCount="0"
packetData="no" varEnum="31" misc="<017>'interface=eth2" user="NULL"
app="NULL" uri="NULL"
```

L'adresse IP de l'attaquant peut être extraite de la même manière.

Genévrier JunOS

JunOS est semblable :

```
Jul 16 10:09:39 JuniperJunOS: asp[8265]:
ASP_IDS_TCP_SYN_ATTACK: asp 3: proto 6 (TCP),
ge-0/0/1.0 10.60.0.123:2280 -> 192.168.1.12:80, TCP
SYN flood attack
```

Iptables de Linux

Voici quelques iptables de Linux d'exemple.

```
Jun 15 23:37:33 netfilter kernel: Inbound IN=lo OUT=
MAC=00:13:d3:38:b6:e4:00:01:5c:22:9b:c2:08:00 src=10.0.0.1 DST=10.0.0.100 LEN=60
```

```
TOS=0x10 PREC=0x00 TTL=64 ID=47312 DF PROTO=TCP SPT=40945 DPT=3003 WINDOW=32767
RES=0x00 SYN URGP=0
```

Vous pouvez envoyer les informations de Syslog pour n'importe quel type de paquet avec la fonctionnalité avancée fournie par les modules iptable comme la connexion dépistant, des xtables, des rpfilters, filtrage, et ainsi de suite.

FreeBSD IPFirewall (IPFW)

Voici un message d'exemple pour IPFW bloquant des fragments :

```
Sep  7 15:03:14 delta ipfw: 11400 Deny UDP 10.61.216.50 10.81.199.2 in via fxp0
(frag 52639:519@1480)
```

Préparation VPN et manipulation CoA

L'ISE peut identifier le type de sessions en termes de manipulation CoA.

- Pour un contournement de câble de l'authentification 802.1x/MAC (MAB), l'ISE envoie le CoA authentifie à nouveau, qui déclenche une deuxième authentification.
- Pour une radio 802.1x/MAB, l'ISE envoie le CoA se termine, qui déclenche une deuxième authentification.
- Pour une ASA VPN, l'ISE envoie un CoA avec un nouveau DACL relié (aucune deuxième authentification).

Le module ENV est simple. Quand il exécute une quarantaine, il envoie toujours un CoA terminent le paquet. Pour sessions de câble/Sans fil, ce n'est pas un problème (tous les suppliants de 802.1x peuvent initier d'une manière transparente une deuxième session d'EAP). Mais quand l'ASA reçoit le CoA terminez, il relâche la session VPN et l'utilisateur final est présenté avec ceci :

Il y a deux solutions possibles pour forcer l'AnyConnect VPN pour rebrancher automatiquement (configuré dans le profil XML) :

- Autoreconnect, qui fonctionne seulement quand vous perdez la connexion avec la passerelle VPN, pas pour l'arrêt administratif
- Illimité, qui fonctionne et des forces AnyConnect pour rétablir automatiquement la session

Même lorsque la nouvelle session est établie, l'ASA choisit le nouvel audit-session-id. Du point de vue ISE, c'est une nouvelle session et il n'y a aucune occasion de rencontrer la règle de quarantaine. Également pour les VPN, il n'est pas possible d'utiliser l'adresse MAC du point final comme identité, par opposition à dot1x de câble/Sans fil.

La solution est de forcer l'ENV pour se comporter comme l'ISE et pour envoyer le type approprié de CoA basé sur la session. Cette fonctionnalité sera introduite dans la version 1.3.1 ISE.

Partenaires et solutions de pxGrid

Voici une liste de Partenaires et de solutions de pxGrid :

- LogRhythm (les informations relatives à la sécurité et gestion d'événement (SIEM)) - Prend en charge le transfert figurative d'état (REPOS) API
- Splunk (SIEM) - Prend en charge le REPOS API
- HP Arcsight (SIEM) - Prend en charge le REPOS API
- Sentinelle NetIQ (SIEM) - Plans pour prendre en charge le pxGrid
- Lancope StealthWatch (SIEM) - Plans pour prendre en charge le pxGrid
- Cisco Sourcefire - Plans pour prendre en charge le pxGrid 1HCY15
- Appliance de sécurité Web de Cisco (WSA) - Plans pour prendre en charge le pxGrid en avril 2014

Voici d'autres Partenaires et solutions :

- Défendable (estimation de vulnérabilité)
- Emulex (capture et médecines légales de paquet)
- Réseaux de Bayshore (prévention de perte de données (DLP) et Internet de stratégie de choses (IoT))
- Identité de ping (l'identité et la Gestion d'Access (JE SUIS) /Single se connectent (SSO))
- Qradar (SIEM)
- LogLogic (SIEM)
- Symantec (Gestion de périphérique mobile d'amd SIEM (MDM))

Référez-vous au catalogue de solutions de marché pour la liste complète de solutions de sécurité.

ISE API : REPOS contre EREST contre le pxGrid

Il y a trois types d'API disponibles sur la version 1.3 ISE.

Voici une comparaison :

	REPOS	**Reposant externe**	**pxGrid**
Authentification client	nom d'utilisateur + mot de passe (HTTP de base authentique)	nom d'utilisateur + mot de passe (HTTP de base authentique)	certificat
Séparation de privilège	non	limité (admin ERS)	oui (grou
Accéder à	MNT	MNT	MNT
Transport	tcp/443 (HTTPS)	tcp/9060 (HTTPS)	tcp/5222 (XMPP)
Méthode de HTTP	OBTENEZ	GET/POST/PUT	GET/PO
Activé par défaut	oui	non	non
Nombre d'exécutions	peu	beaucoup	peu
Le CoA se terminent	pris en charge	non	pris en c
Le CoA authentifient à nouveau	pris en charge	non	pris en c *
Exécutions d'utilisateur	non	oui	non
Exécutions de point final	non	oui	non
Exécutions de groupe d'identité de point final	non	oui	non
Quarantaine (IP, MAC)	non	non	oui
UnQuarantine (IP, MAC)	non	non	oui
PortBounce/arrêt	non	non	oui

Exécutions d'utilisateur d'invité	non	oui	non
Exécutions de portail d'invité	non	oui	non
Exécutions de périphérique de réseau	non	oui	non
Exécutions de groupe de périphériques réseau	non	oui	non

* Les utilisations de quarantaine ont unifié le support CoA de la version 1.3.1 ISE.

Téléchargements

le pxLog peut être téléchargé de Sourceforge.

Le kit de développement logiciel (SDK) est déjà inclus. Pour la dernière documentation SDK et API pour le pxGrid, contactez votre partenaire ou l'équipe de compte Cisco.

Informations connexes

- REPOS API de Cisco ISE 1.2
- Cisco ISE 1.2 API reposant externe
- Guide d'administrateurs de Cisco ISE 1.3
- Support et documentation techniques - Cisco Systems