تعيين الأهداف – إرشادات خاصة بنظام المراقبة n-ORM

المحتويات

1 مقدمة..... 1
2 تنسيق الملف..... 1
3 تحديث الملف..... 1
3.1 التحديث التلقائي..... 1
3.2 تحديد الهدف 1
3.3 تحديد الفئة 1
3.4 تحرير التعارضات..... 1

1 مقدمة

توضح هذه الوثيقة استخدام ملف التعيينات في النظام. تم إعطاء مثال في الشكل رقم 1. يستخدم ملف التعيينات للتعيين بين تصنيف snort للتهديد والمتطلبات الخاصة بملف nORM XML.

2 تنسيق الملف

هذا الملف عبارة عن ملف CSV بسيط بسطر واحد لكل تهديد. يحتوي كل سطر على خمس قيم:

معرف الأمان SID – رقم التعريف الوحيد الذي تم تعيينه لهذا التهديد بواسطة نظام IDS/IPS الخارجي

تنبيه – يعد هذا اسم التهديد الذي يتم توفيره أيضًا بواسطة نظام كشف التسلل/منع التسلل الخارجي، ولكن يمكن تغييره بواسطة المسؤول.

هدف – الهدف كما هو مطلوب بواسطة علامة تهديد nORM ويتم توفيره يدويًا بواسطة المسؤول. القيمة الافتراضية "Unknown".

فئة – هو حقل الفئة كما هو مطلوب بواسطة علامة تهديد nORM، ويتم توفيره أيضًا بواسطة المسؤول. القيمة الافتراضية "Indiscriminate".

الخطورة – هي SeverityScore التي يتم وضعها كما هو مطلوب بواسطة علامة تهديد nORM. يتم حساب القيمة الافتراضية تلقائيًا من قيمة الأفضلية لنظام كشف التسلل/منع التسلل.

يُعتبر التعيين من نظام كشف التسلل/منع التسلل الخارجي إلى nORM هو:

$1 \rightarrow 10;\ 2 \rightarrow 7;\ 3 \rightarrow !\ 4;\ 4 \rightarrow 1.$

3 تحديث الملف

3.1 تحديث تلقائي

عندما يكتشف النظام تهديدًا جديدًا غير موجود في ملف التعيين، يتم إضافة سطر جديد تلقائيًا مع القيم الافتراضية التي تم ذكرها أعلاه. والغرض من ذلك هو أن مسؤول النظام سيقوم بالتحقق من القيم المفقودة بشكل دوري وملئها. ينبغي تحديد هذا باعتباره جزءًا من عمل مسؤول النظام.

3.2 تحديد الهدف

لتحديد الهدف من التهديد يجب إجراء فحص يدوي لقواعد نظام كشف التسلل/منع التسلل الخارجي الموجودة قيد الاستخدام. لذلك من المهم البدء بمجموعة من القواعد جيدة التوثيق.

تتوفر هذه المجموعات على http://www.snort.org/vrt/ على سبيل المثال قواعد Source_re VRT certi_ed.

سيستخدم هذا المستند "القواعد الخاصة بـ Snort v2.4" باعتبارها أمثلة. يسمى ملف القواعد snortrules-pr-2.4.tar.gz.

عند إفراغ هذه المحتويات نحصل على اثنين من الدلائل؛ قواعد ومستندات. يحتوي دليل المستندات على توقيعات دلائل إضافية. يوجد هنا ملف مطابق لكل معرف أمان SID. يظهر ملف المستند 2924.txt في الشكل 2. في هذه الحالة يكون القسم المناسب هو "الأنظمة المتأثرة"، بالرغم من أن قسم "الموجز" سيعطي معلومات كافية في معظم الحالات. وفي هذه الحالة، نظرًا لأن "كل الأنظمة التي تشارك الموارد التي تستخدم SMB" تكون متأثرة، يتم استخدام قيمة لـ SMB. يلزم الاتفاق على القيم الدقيقة بين نظام الالتقاط وn-ORM.

3.3 تحديد الفئة

ستكون كافة التهديدات غير مميزة. الفرق هو أن هذا الهجوم (الموجه) المميز سيتم توجيهه عند نقطة ما بواسطة إنسان يستهدف جهازًا معينًا، بخلاف الفيروسات التي تنتشر ذاتيًا. من الصعب تحديد هذا من مُعرف التهديد ببساطة.

3.4 تحرير التعارضات

يتم مراجعة وتحديث ملف التعيين بشكل افتراضي بواسطة النظام مرة كل أسبوع عند منتصف الليل صباح يوم الاثنين. سيتم إكمال أي تحديثات في أجزاء من الثانية. ولكن، لا ينبغي على مسؤول النظام تحرير الملف في هذا الوقت، أو بطريقة أكثر دلالة ترك جلسة عمل التحرير مفتوحة في هذا الوقت.

```
# SID,Alert,Target,Category,Severity
2050,MS-SQL version overflow attempt,SQLServer,Indiscriminate,1
2003,MS-SQL Worm propagation attempt,Unknown,Indiscriminate,7
2466,NETBIOS SMB-DS IPC$ unicode share access,Unknown,Indiscriminate,4
2924,NETBIOS SMB-DS repeated logon failure,Unknown,Indiscriminate,10
2404,NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt
,Unknown,Indiscriminate,10
1113,WEB-MISC http directory traversal,Unknown,Indiscriminate,7
2570,WEB-MISC Invalid HTTP Version String,Unknown,Indiscriminate,7
1852,WEB-MISC robots.txt access,Unknown,Indiscriminate,7
1002,WEB-IIS cmd.exe access,Unknown,Indiscriminate,10
1408,DOS MSDTC attempt,Unknown,Indiscriminate,7
472,ICMP redirect host,Unknown,Indiscriminate,7
1918,SCAN SolarWinds IP scan attempt,Unknown,Indiscriminate,4
2417,FTP format string attempt,Unknown,Indiscriminate,4
579,RPC portmap mountd request UDP,Unknown,Indiscriminate,7
```

الشكل 1: مثال على ملف تعيينات

القاعدة:
--
معرف الأمان:
2924
--
موجز:
تم إنشاء هذا الحدث عندما تم إجراء محاولات متكررة فاشلة للوصل إلى مساحة مشتركة على شبكة SMB.
--
التأثير:
غير معروف. احتمال كشف للمعلومات وفقد البيانات.
--
معلومات مفصلة:
يشير هذا الحدث إلى أنه تم إجراء محاولات متعددة فاشلة للوصل إلى مساحة مشتركة على شبكة SMB. قد يشير ذلك إلى جهود محددة تم اتخاذها بواسطة مستخدم غير معتمد للوصل إلى معلومات وبيانات على مساحة مشتركة على الشبكة.
--
الأنظمة المتأثرة:
كافة الأنظمة المشاركة لموارد تستخدم SMB
--
سيناريوهات الهجوم:
بإمكان المتسللين إجراء محاولات متكررة للوصول إلى المساحات المشتركة على الشبكة في محاولة للحصول على المعلومات.
--
سهولة الهجوم:
بسيط. لا يلزم استخدام برنامج معطل للأمان.
--
نتائج إيجابية كاذبة:
غير معروف
--
نتائج سلبية كاذبة:
غير معروف
--
الإجراء التصحيحي:
قم بتطبيق تحكم صارم في الوصول إلى كافة موارد الشبكات.
--

الشكل 2: وثائق SNORT الخاصة بالقاعدة 2924 من snort لـ SNORT 2.4