معلمات توقيع معرفات وحدة تحكم الشبكة المحلية اللاسلكية

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
محددات معرفات وحدات التحكم
التواقيع القياسية الخاصة بوحدة التحكم IDS
رسائل IDS
معلومات ذات صلة

المقدمة

يصف هذا المستند كيفية تكوين توقيعات نظام اكتشاف الاقتحام (IDS) في برنامج وحدة تحكم الشبكة المحلية اللاسلكية (WLAN) من Cisco الإصدار 3.2 والإصدارات الأقدم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN) الإصدار 3.2 والإصدارات الأحدث.

الاصطلاحات

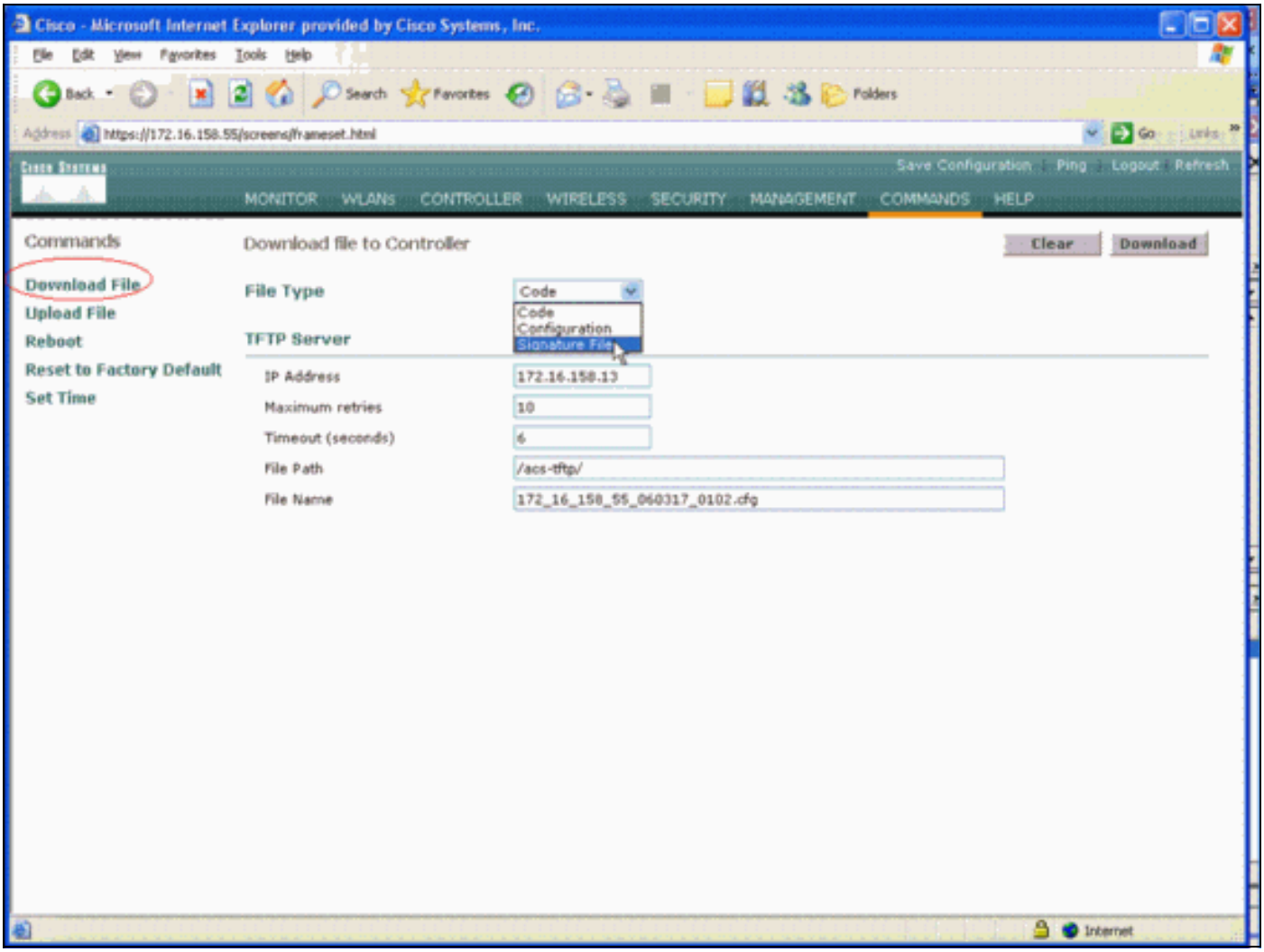
راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يمكنك تحميل ملف توقيع IDS لتحرير التوقيع (أو لمراجعة الوثائق). أختر **أوامر > تحميل ملف > ملف توقيع**. لتنزيل ملف توقيع IDS معدل، أختر **أوامر > تنزيل ملف > ملف توقيع**. بعد تنزيل ملف توقيع إلى وحدة التحكم، يتم تحديث جميع نقاط الوصول (APs) المتصلة بوحدة التحكم في الوقت الفعلي باستخدام معلمات التوقيع التي تم تحريرها

حديثا.

يوضح هذا الإطار كيفية تنزيل ملف التوقيع:



يوثق ملف توقيع IDS تسع معلمات لكل توقيع IDS. يمكنك تعديل معلمات التوقيع هذه وكتابة توقيعات مخصصة جديدة. راجع التنسيق الذي يوفره قسم معلمات معرفات وحدات التحكم في هذا المستند.

محددات معرفات وحدات التحكم

يجب *أن* يكون لكل التوقيعات هذا التنسيق:

```
= Name = <str>, Ver = <int>, Preced = <int>, FrmType = <frmType-type>, Pattern
,<pattern-format>, Freq = <int>, Interval = <int>, Quiet = <int>, Action = <action-val>
<Desc = <str
```

الحد الأقصى لطول السطر هو 1000 حرف. لا يتم تحليل الخطوط التي تكون أطول من 1000 بشكل صحيح.

كل الأسطر التي تبدأ ب # في ملف IDS نصي تعتبر تعليقات ويتم تخطيها. كما يتم تخطي كافة الخطوط الفارغة، والتي هي عبارة عن خطوط تحتوي على مسافة بيضاء فقط أو سطر جديد. يجب *أن* يحتوي السطر غير الفارغ الأول غير المعلق على الكلمة الأساسية . إذا كان الملف ملف توقيع تم توفيره من Cisco، فيجب ألا تقوم بتغيير قيمة . تستخدم Cisco هذه القيمة لإدارة إصدارات ملف التوقيع. إذا كان الملف يحتوي على توقيعات تم إنشاؤها من قبل المستخدم النهائي، فإن قيمة يجب أن تكون (=).

معلمات توقيع IDS التسعة التي يمكنك تعديلها هي:

- = اسم التوقيع. هذه سلسلة فريدة تعرف التوقيع. الحد الأقصى لطول الاسم هو 20 حرفا.
- = أسبقية التوقيع. هذا معرف فريد يشير إلى أسبقية التوقيع بين كل التوقيعات المعرفة في ملف التوقيع. يجب أن يكون هناك رمز مميز لكل توقيع.
- **FrmType** = نوع الإطار. يمكن أن تأخذ هذه المعلمة قيما من القائمة <frmType-val>. يجب أن يكون هناك رمز مميز FrmType واحد لكل توقيع. يمكن أن يكون <frmType-val>أحد الكلمتين الأساسيتين التاليتين فقط:mgmtيشير <frmType-val>إلى ما إذا كان هذا التوقيع يكتشف البيانات أو إطارات الإدارة.
- = نمط التوقيع. يتم إستخدام قيمة الرمز المميز لاكتشاف الحزم التي تطابق التوقيع. يجب *أن* يكون هناك رمز مميز واحد على الأقل لكل توقيع. يمكن أن يكون هناك ما يصل إلى خمسة من تلك الرموز لكل توقيع. إذا كان التوقيع به أكثر من واحد من تلك الرموز، يجب أن تطابق الحزمة قيم كل العلامات المميزة لكي تتطابق الحزمة مع التوقيع.عندما تتلقى نقطة الوصول حزمة، فإن نقطة الوصول تأخذ تدفق البايت الذي يبدأ من <offset>، وتقوم بمقارنة النتيجة ب <mask>، وتقارن النتيجة ب <pattern>. إذا عثرت نقطة الوصول على تطابق، فإن نقطة الوصول تعتبر الحزمة تطابق مع التوقيع. يمكن أن يسبق <pattern-format>عامل تشغيل الإلغاء !". في تلك الحالة، كل ربط أن يفشل ال تطابق عملية أن هذا قسم يصف يكون اعتبرت مطابقة مع التوقيع.
- **FREQ** = تكرار مطابقة الحزمة في الحزم/الفاصل الزمني. تشير قيمة هذا الرمز المميز إلى عدد الحزم لكل فترة قياس يجب أن تطابق هذا التوقيع قبل تنفيذ التوقيع. تشير القيمة 0 إلى أن التوقيع يتم إتخاذه في كل مرة تطابق فيها الحزمة التوقيع. الحد الأقصى لقيمة هذا الرمز المميز هو 65،535. يجب أن يكون هناك رمز مميز Freq لكل توقيع.
- = الفاصل الزمني للقياس بالثواني. تشير قيمة هذا الرمز المميز إلى الفترة الزمنية التي يحددها الحد (أي Freq). القيمة الافتراضية لهذا الرمز المميز هي 1 ثانية. الحد الأقصى لقيمة هذا الرمز المميز هو 3600.
- = وقت الهدوء بالثواني. تشير قيمة هذا الرمز المميز إلى مقدار الوقت الذي يجب أن يمر خلاله لا تستلم نقطة الوصول الحزم التي تطابق التوقيع قبل أن تحدد نقطة الوصول أن الهجوم الذي يشير إليه التوقيع قد تم إيقافه. إذا كانت قيمة الرمز المميز Freq هي 0، فسيتم تجاهل هذا الرمز المميز. يجب *أن* يكون هناك رمز مميز لكل توقيع.
- = إجراء التوقيع. هذا يشير إلى ما يجب أن تقوم به نقطة الوصول إذا طابقت الحزمة التوقيع. يمكن أن تأخذ هذه المعلمة قيما من القائمة <action-val>. يجب أن يكون هناك رمز مميز واحد لكل توقيع. يمكن أن يكون <action-val>أحد الكلمتين الأساسيتين التاليتين فقط:none = عدم القيام بأي شيء. = تقرير عن مطابقة المحول.
- **DESC** = وصف التوقيع. هذه سلسلة تصف الغرض من التوقيع. عندما يتم الإبلاغ عن تطابق توقيع في مصيدة بروتوكول إدارة الشبكة البسيط (SNMP)، يتم توفير هذه السلسلة للمصيدة. الحد الأقصى لطول الوصف هو 100 حرف. يجب أن يكون هناك رمز مميز Desc لكل توقيع.

التواقيع القياسية الخاصة بوحدة التحكم IDS

يتم شحن توقيعات IDS هذه مع وحدة التحكم ك "توقيعات IDS القياسية". يمكنك تعديل كل معلمات التوقيع هذه، كما يصف قسم معلمات معرفات وحدات التحكم.

```
Revision = 1.000
,Name = "Bcast deauth", Ver = 0, Preced= 1, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF
        Pattern = 4:0x01:0x01, Freq=30, Quiet = 300, Action = report, Desc="Broadcast
                                                        "Deauthentication Frame

                = Name = "NULL probe resp 1", Ver = 0, Preced = 2, FrmType = mgmt, Pattern
= 0:0x0050:0x03FF, Pattern = 36:0x0000:0xFFFF, Freq=1, Quiet = 300, Action = report, Desc
                                                "NULL Probe Response - Zero length SSID element"

                = Name = "NULL probe resp 2", Ver = 0, Preced = 3, FrmType = mgmt, Pattern
= 0:0x0050:0x03FF, Pattern = !36:0x00:0xFF, Freq=1, Quiet = 300, Action = report, Desc
                                                "NULL Probe Response - No SSID element"

,Name = "Assoc flood", Ver = 0, Preced= 4, FrmType = mgmt, Pattern = 0:0x0000:0x03FF
```

```
"Freq=50, Quiet = 600, Action = report, Desc="Association Request flood

,Name = "Auth Flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0: 0x00b0: 0x03FF
"Freq=50, Quiet = 600, Action = report, Desc="Authentication Request flood

,Name = "Reassoc flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0:0x0020:0x03FF
"Freq=50, Quiet = 600, Action = report, Desc="Reassociation Request flood

= Name = "Broadcast Probe flood", Ver = 0, Preced= 6, FrmType = mgmt, Pattern
,0:0x0040:0x03FF, Pattern = 4:0x01:0x01, Pattern = 24:0x0000:0xFFFF, Freq=50, Quiet = 600
"Action = report, Desc="Broadcast Probe Request flood

,Name = "Disassoc flood", Ver = 0, Preced= 7, FrmType = mgmt, Pattern = 0:0x00A0:0x03FF
"Freq=50, Quiet = 600, Action = report, Desc="Disassociation flood

,Name = "Deauth flood", Ver = 0, Preced= 8, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF
"Freq=50, Quiet = 600, Action = report, Desc="Deauthentication flood

,Name = "Res mgmt 6 & 7", Ver = 0, Preced= 9, FrmType = mgmt, Pattern = 0:0x0060:0x03EF
"Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types 6 and 7

,Name = "Res mgmt D", Ver = 0, Preced= 10, FrmType = mgmt, Pattern = 0:0x00D0:0x03FF
"Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-type D

,Name = "Res mgmt E & F", Ver = 0, Preced= 11, FrmType = mgmt, Pattern = 0:0x00E0:0x03EF
"Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types E and F

,Name = "EAPOL flood", Ver = 0, Preced= 12, FrmType = data, Pattern = 0:0x0108:0x03FF
Pattern = 30:0x888E:0xFFFF, Freq=50, Quiet = 300, Action = report, Desc="EAPOL Flood
"Attack

= Name = "NetStumbler 3.2.0", Ver = 0, Preced= 13, FrmType = data, Pattern
= 0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern
"36:0x466c7572:0xFFFFFFFF, Freq = 1, Quiet = 300, Action = report, Desc="NetStumbler 3.2.0

= Name = "NetStumbler 3.2.3", Ver = 0, Preced= 14, FrmType = data, Pattern
= 0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern
"36:0x416C6C20:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.2.3

= Name = "NetStumbler 3.3.0", Ver = 0, Preced= 15, FrmType = data, Pattern
= 0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern
"36:0x20202020:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.3.0

= Name = "NetStumbler generic", Ver = 0, Preced= 16, FrmType = data, Pattern
,0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Freq = 1
"Quiet = 600, Action = report, Desc="NetStumbler

,Name = "Wellenreiter", Ver = 0, Preced= 17, FrmType = mgmt, Pattern = 0:0x0040:0x03FF
:Pattern = 24:0x001d746869735f69735f757365645f666f725f77656c6c656e726569
,0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff, Freq = 1, Quiet = 600
"Action = report, Desc="Wellenreiter
```

رسائل IDS

باستخدام وحدة تحكم الشبكة المحلية اللاسلكية الإصدار 4.0، قد تحصل على رسالة IDS هذه.

```
,Big NAV Dos attack from AP with Base Radio MAC 00:0f:23:xx:xx:xx
Slot ID 0 and Source MAC 00:00:00:00:00:00
```

تشير رسالة IDS هذه إلى أن حقل متجه تخصيص الشبكة 802.11 (NAV) في إطار 802.11 اللاسلكي كبير جدا وقد تكون الشبكة اللاسلكية تحت هجوم رفض الخدمة (أو هناك عميل يسيء التصرف).

بعد إستلام رسالة IDS هذه، تتمثل الخطوة التالية في تعقب العميل المسيء. يجب عليك تحديد موقع العميل بناء على قوة الإشارة الخاصة به باستخدام sniffer لاسلكي في المنطقة المحيطة بنقطة الوصول أو إستخدام خادم الموقع لتحديد موقعه.

حقل NAV هو الآلية الظاهرية لاستشعار الناقل المستخدمة للحد من التصادمات بين المحطات الطرفية المخفية (العملاء اللاسلكيون الحاليون لا يمكن للعميل اللاسلكي اكتشافهم عندما يبث) في عمليات إرسال 802.11. تتسبب المحطات الطرفية المخفية في حدوث مشاكل لأن نقطة الوصول قد تستلم حزم من عميلين يمكنهما الإرسال إلى نقطة الوصول ولكنهما لا يستقبلان رسائل بعضهما البعض. عندما يبث هؤلاء العملاء في نفس الوقت، تتصادم حزماتهم عند نقطة الوصول فينتج عن ذلك عدم إستلام نقطة الوصول للحزمة بشكل واضح.

كلما رغب عميل لاسلكي في إرسال حزمة بيانات إلى نقطة الوصول، فإنه يرسل في الواقع تسلسلا من أربع حزم يسمى تسلسل حزمة RTS-CTS-DATA-ACK. يحمل كل إطار من الإطارات الأربعة 802.11 حقل NAV يشير إلى عدد الميكروثوان التي يتم حجز القناة لها بواسطة عميل لاسلكي. أثناء مصافحة RTS/CTS بين العميل اللاسلكي ونقطة الوصول، يرسل العميل اللاسلكي إطار RTS صغيرا يتضمن فاصل NAV كبيرا بما يكفي لإكمال التسلسل بالكامل. وهذا يشمل إطار CTS وإطار البيانات وإطار الإقرار اللاحق من نقطة الوصول.

عندما يرسل العميل اللاسلكي حزمة RTS الخاصة به باستخدام مجموعة NAV، فإنه يتم إستخدام القيمة المرسلة لتعيين وحدات توقيت NAV على جميع العملاء اللاسلكيين الآخرين المرتبطين بنقطة الوصول. ترد نقطة الوصول على حزمة RTS من العميل مع حزمة CTS تحتوي على قيمة NAV جديدة تم تحديثها لحساب الوقت المنقضي بالفعل أثناء تسلسل الحزمة. بعد إرسال حزمة CTS، يكون كل عميل لاسلكي يمكن أن يستلم من نقطة الوصول قد قام بتحديث وحدة توقيت NAV الخاصة به وتأجيل جميع عمليات الإرسال إلى أن يصل جهاز توقيت NAV الخاص به إلى 0. مما يبقي القناة حرة للعميل اللاسلكي ليكمل عملية إرسال الحزمة إلى نقطة الوصول.

وقد يستغل المهاجم هذه الآلية الافتراضية لاستشعار الناقل من خلال التأكيد على قضاء وقت طويل في حقل NAV. وهذا يمنع العملاء الآخرين من إرسال الحزم. الحد الأقصى لقيمة NAV هو 32767، أو حوالي 32 مللي ثانية على شبكات 802.11b. لذلك نظريا يحتاج المهاجم فقط أن يبث ما يقرب من 30 حزمة في الثانية ليمشط كل الوصول إلى القناة.

معلومات ذات صلة

- سلسلة وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية 4400 من Cisco
- سلسلة وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية 4100 من Cisco
- سلسلة وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية 2000 من Cisco
- محركات توقيع نظام اكتشاف الاقتحام Cisco Intrusion Detection System Signature Engines، الإصدار 3.1
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).