UNIX ريدم ىلع بنجتلا دادعإ

المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المتطلبات</u> <u>المكونات المستخدمة</u> <u>التكوين</u> <u>التكوينات</u> <u>التحقق من الصحة</u> <u>قبل شن الهجوم</u> <u>شن الهجوم و التجنب</u> معلومات ذات صلة معلومات ذات صلة

<u>المقدمة</u>

يمكن إستخدام مدير نظام اكتشاف الاقتحام (IDS) والمستشعر من Cisco لإدارة موجه Cisco للتجنب. في هذا المستند، يتم تكوين مستشعر (sensor-2) من أجل اكتشاف الهجمات على الموجه "المنزل" ومن أجل توصيل هذه المعلومات إلى المدير "dir3". وبمجرد تكوينها، يتم تشغيل هجوم (إختبار الاتصال بحجم أكبر من 1024 بايت، وهو التوقيع 2151، وطوفان بروتوكول رسائل التحكم في الإنترنت [ICMP]، وهو التوقيع 2152) من الموجه "لموجه جهاز الاستشعار بالكشف عن الهجوم وإبلاغ ذلك إلى المدير. يتم تنزيل قائمة التحكم في الوصول (ACL) إلى الموجه التجنب حركة المرور من المهاجم. على الذي يظهر، وعلى الضحية يتم عرض قائمة التحكم في الوصول (ACL) إلى الموجه التي تم تنزيلها.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

قبل أن تحاول إجراء هذا التكوين، فتأكد من استيفاء المتطلبات التالية:

- قم بتثبيت "المستشعر" وتأكد من عمله بشكل صحيح.
- ضمنت أن ال ينشق قارن إلى المسحاج تخديد قارن خارجي.

<u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- مدير Cisco IDS 2.2.3
- مستشعر Cisco IDS 3.0.5

• موجه IOS[®] من Cisco مع 12.2.6 تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

<u>الاصطلاحات</u>

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى <u>اصطلاحات تلميحات Cisco التقنية</u>.

<u>التكوين</u>

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم <u>أداة بحث الأوامر</u> (<u>للعملاء</u> المسجلين فقط).

<u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



<u>التكوينات</u>

يستخدم هذا المستند هذه التكوينات.

- <u>ضوء الموجه</u>
- <u>منزل الموجه</u>

ضوء الموجه

```
Current configuration : 906 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
                          hostname light
                                        !
                  enable password cisco
                                       !
        username cisco password 0 cisco
                          ip subnet-zero
                                       !
                                       !
                                        !
                     ip ssh time-out 120
        ip ssh authentication-retries 3
                                       !
                          call rsvp-sync
                                       !
                                       !
                                       !
               fax interface-type modem
       mta receive maximum-recipients 0
                                        !
                      controller E1 2/0
                                       !
                                       !
                                        !
              interface FastEthernet0/0
ip address 100.100.100.2 255.255.255.0
                            duplex auto
                             speed auto
                                       !
              interface FastEthernet0/1
      ip address 1.1.1.1 255.255.255.0
                            duplex auto
                             speed auto
                                       !
                            ip classless
 ip route 0.0.0.0 0.0.0.0 100.100.100.1
                          ip http server
                     ip pim bidir-enable
                                       !
                                        !
                   dial-peer cor custom
                                       1
                                       !
                              line con 0
                             line 97 108
                              line aux 0
                            line vty 0 4
                                  login
                                       !
                                     end
                             منزل الموجه
     Current configuration : 2187 bytes
                                       !
                            version 12.2
        service timestamps debug uptime
          service timestamps log uptime
         no service password-encryption
```

```
hostname house
```

!

!

```
enable password cisco
```

```
!
                                                         !
                                                         !
                                           ip subnet-zero
                                                         !
                                                         !
                                 fax interface-type modem
                        mta receive maximum-recipients 0
                                                         !
                                                         !
                                                         !
                                                         !
                                interface FastEthernet0/0
                 ip address 100.100.100.1 255.255.255.0
After you configure shunning, IDS Sensor puts this ---!
    line in. ip access-group IDS_FastEthernet0/0_in_1 in
                                              duplex auto
                                              speed auto
                                                         !
                                interface FastEthernet0/1
                 ip address 10.64.10.45 255.255.255.224
                                             duplex auto
                                              speed auto
                                                         !
                                                         !
                                                         !
                                interface FastEthernet4/0
                                           no ip address
                                                shutdown
                                             duplex auto
                                              speed auto
                                                         !
                                             ip classless
                    ip route 0.0.0.0 0.0.0.0 10.64.10.33
            ip route 1.1.1.0 255.255.255.0 100.100.100.2
                                           ip http server
                                      ip pim bidir-enable
                                                         !
                                                         !
After you configure shunning, IDS Sensor puts these ---!
lines in. ip access-list extended IDS_FastEthernet0/0_in
                          deny ip host 100.100.100.2 any
                          permit ip host 10.64.10.49 any
                                       permit ip any any
                                                         !
                                      snmp-server manager
                                                         !
                                           call RSVP-sync
                                                         1
                                                         !
                                     mgcp profile default
                                                         !
                                     dial-peer cor custom
                                                         !
                                                         !
                                                         !
                                                         !
                                               line con 0
                                               line aux 0
                                             line vty 0 4
                                          password cisco
```

```
login
!
!
end
#house
```

<u>تكوين جهاز الاستشعار</u>

أكمل الخطوات التالية لتكوين المستشعر.

1. Telnet إلى **10.64.10.49** باسم المستخدم **الجذر** والهجوم **بكلمة المرور**.

```
2. أدخل sysconfig-sensor.
أدخل معلومات التكوين، عند طلبها، كما هو موضح في هذا المثال.
```

```
IP Address: 10.64.10.49 - 1
           IP Netmask: 255.255.254 - 2
               IP Host Name: sensor-2 - 3
        Default Route
                          10.64.10.33 - 4
                Network Access Control - 5
                              .64
                              .10
        Communications Infrastructure - 6
                        Sensor Host ID: 49
           Sensor Organization ID:
                                       900
                Sensor Host Name: sensor-2
        Sensor Organization Name:
                                    cisco
     Sensor IP Address:
                               10.64.10.49
                   IDS Manager Host ID: 50
        IDS Manager Organization ID:
                                       900
        IDS Manager Host Name:
                                      dir3
      IDS Manager Organization Name: cisco
                               10.64.21.50
IDS Manager IP Address:
```

4. عند المطالبة، قم بحفظ التكوين والسماح للمستشعر بإعادة التمهيد.

إضافة المستشعر إلى المدير

أتمت هذا steps أن يضيف المستشعر إلى المدير.

1. Telnet إلى 10.64.21.50 باسم المستخدم netrangr والهجوم بكلمة المرور.
 2. أدخل الفيديو لتشغيل برنامج OpenView من HP.
 3. في القائمة الرئيسية، حدد تأمين > تكوين.
 4. في الأداة المساعدة لإدارة ملف التكوين، حدد ملف > إضافة مضيف، ثم انقر بعد ذلك.
 5. هذا مثال على كيفية ملء المعلومات

Use this panel to specify the remote machine to which you wish to establish connectivity. If you need to add a new organization, click Create.					
Organization name	cisco —	Create			
Organization ID	900				
Host name	sensor-2į́				
Host ID	49 <u>ĭ</u>				
Host IP Address	10.64.10.49				
🗖 Secondary Dire	ctor				
🗖 IOS IDS					
🕱 Sensor / IDSM					
	هو موضح في هذا	ِ لنوع الح <i>ه</i> از، وانقر التالي ، كما	المطلوبة.لــــــــــــــــــــــــــــــــــــ		
Use this dialog H	pox to define the t	cype of machine you are	adding.		
Please remember the remote machin this Director. A by running syscon this is accomplis and modifying the	that in order for o ne must already kno For Sensors, this i ofig-sensor. For r shed by running nr(e hosts and routes	connectivity to be estab ow the IDs and IP addres is accomplished at insta remote (secondary) Direc Configure on the remote System Files accordingl	lished, s of ll time tors, machine Y+		
Initialize a newly installed Sensor					
C Connect to a previously configured Sensor					
🔘 Forward alarms	to a secondary Dir	rector			
لتضييلك كتقابياتها	احد ترازا کار سالتہ میں	الا الدقائة أم تكواكة مقافت	المثال. 7 قب تخي البحار ما م		

7. قم بتغيير السجل وإبطال الدقائق، او تركها كقيمة افتراضية إذا كانت القيم مقبولة. غيرت الشبكة قارن إسم إلى الاسم من ك sniffing قارن.في هذا المثال ستكون "iprb0." يمكن أن يكون "spwr0" أو أي شيء آخر حسب نوع المستشعر وكيفية توصيل المستشعر الخاص بك.

Use this dialog box to set the time in minutes for automatic logging and shunning, the name of the Sensor network interface performing packet capture, and the addresses and netmasks of networks protected by the Sensor.						
Number of minutes to log on an event.	15]					
Number of minutes to shun on an event. 15						
Network Interface Name						
Sensor Protected Networks Internal IP Addresses						

8. طقطقت **بعد ذلك** إلى أن هناك خيار أن يطقطق **إنجاز**.لقد أضفت المستشعر بنجاح إلى Director. من القائمة الرئيسية، يجب أن ترى -2، كما في هذا المثال.

											المتال.
Мар	Edit	View	Perfor	mance	Config	guration	Fault	Security	Tools	Options	
₩inc	low										<u>H</u> elp
⊿	@ /	1	s Se⊂ 2	Q	C) H ⁰ Hiler						
		_					_		_		
	l (h	<u> </u>			_~^/_	•				
		Y	/ ଆ							Y /	
	5	ensur-	۷.			<u>ars</u>			50	150[-5]	

<u>تكوين التجنب لموجه Cisco IOS</u>

أكمل الخطوات التالية لتكوين التجنب لموجه Cisco IOS.

- 1. في القائمة الرئيسية، حدد **تأمين > تكوين**.
- 2. في الأداة المساعدة لإدارة ملف التكوين، قم بإبراز **المستشعر-2** وانقر فوقه نقرا مزدوجا.
 - 3. فتح **إدارة الأجهزة**.
- 4. انقر فوق **أجهزة > إضافة**، وأدخل المعلومات كما هو موضح في هذا المثال. انقر فوق **موافق**" للمتابعة.تطابق كلمات مرور Telnet والتمكين ما هو في الموجه "Home".

10 044	U.S. News
IP Hodress	User Name
10.64.10.45	I
Device Type	Password
Cisco Router[Including Cat5kRSM,Cat6kMSFC] -	*****
	,
Sensor's NAT IP Address	Enable Password
I	****
Enable SSH	

5. انقر فوق **الواجهات > إضافة**، وأدخل هذه المعلومات، وانقر فوق **موافق** للمتابعة.

IP Address	PostShun ACL Name
10.64.10.45 -] 198
PreShun ACL Name	Interface Name
199 1	FastEthernet0/0
	Divertion
	in —

6. انقر فوق **تجنب > إضافة** وحدد **مستشعر-cisco.2** كخادم تجنب. قم بإغلاق إطار إدارة الأجهزة عند

	Shunning Servers	
	Sensor	Add
	sensor-2.cisco	Delete
		Modify
		-
10.64.10.254	العالي. ، وانقر فوق الشبكات المحمية . إضافة النطاق 10.64.10.1 إلى ·	الانتهاء. 7. افتح نافذة اكتشاف الاقتحام
	موضح فی هذا	في الشبكة المحمية، كما هو
-50	ource Address	

Source Address	
Enter range of IP addresses to be protected	
OEnter a network address to be protected	
Start Address:	
10.64.10.1	
End Address:	
10.64.10.254	
	المثال

- 8. انقر على **ملف تخصيص > التكوين اليدوي**.
- 9. حدد **تعديل التوقيعات > حركة مرور ICMP الكبيرة** بمعرف **2151**.
- 10. انقر فوق**َ تعديل**، وقم بتغيير **الإجراء** من لا شيء إلى **تجاهل & تسجيل الدخول**، وانقر فوق **موافق** للمتابعة.

Signature ICMP Flood	sensor-2.cisco loggerd)4	
ID 2152	dir3.cisco smid ₽	
Action Shun & Log —		

11. أختر **طوفان ICMP** بمعرف **2152**، وانقر فوق **تعديل**. قم بتغيير **الإجراء** من لا شيء إلى **تجاهل & تسجيل** الدخول، وانقر فوق **موافق**

للمتابعة.

Signa	ture		sensor-2.cisco loggerd	
Large	e ICMP traffic		3	
ID			dir3.cisco smid	
2151	[B	Í
,				
Actio	n			
	Shun & Log	-		

- 12. انقر فوق **موافق** لإغلاق نافذة اكتشاف الاقتحام.
- 13. افتح مجلد "ملفات النظام"، وافتح نافذة "ملفات النظام".تأكد من تمكين هذه

Daemons			
	▼ nr.postofficed	🗙 nr.configd	
	🕱 nr.loggerd	nr.smid	
	🗙 nr.sensord	nr.eventd	
	🕱 nr.packetd	🕱 nr.sapd	
	🕱 nr.managed	🗙 nr.fileXferd	
			الأجهزة:

14. انقر فوق **موافق** للمتابعة، أختر الإصدار الذي تم تعديله للتو، وانقر فوق **حفظ** ثم **تطبيق**.انتظر حتى يخبرك النظام بأن أداة الاستشعار قد انتهت من إعادة تشغيل الخدمات، ثم قم بإغلاق كافة النوافذ الخاصة بتكوين المدير.

		مىدىر.
Version / Item	Creation Time	Open
占 👼 Version 11	Mon Apr 22 21:04:57 EDT 2002	
- 🔤 Communications	Mon Apr 22 21:04:57 EDT 2002	View
- 🔊 Data Management	Mon Apr 22 21:04:57 EDT 2002	
- 🖳 Device Management	Mon Apr 22 21:04:57 EDT 2002	Save
- ≿o [†] Event Processing	Mon Apr 22 21:04:57 EDT 2002	
- 🖓 Intrusion Detection	Mon Apr 22 21:04:57 EDT 2002	Apply
占 🕞 System Files		
- 💷 Authorization	Mon Apr 22 21:04:57 EDT 2002	Delete
– 🍓 Daemons	Mon Apr 22 21:04:57 EDT 2002	
1		
	Close	

<u>التحقق من الصحة</u>

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** <u>أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل</u> إ<u>خراج أمر</u> ا<mark>لعرض.</mark>

- show access-list يسرد عبارات الأوامر access-list في تكوين الموجه. كما أنها تسرد عدد مرات مطابقة العنصر أثناء بحث أمر access-list.
 - ping يستخدم لتشخيص اتصال الشبكة الأساسي.

<u>قبل شن الهجوم</u>

قبل تشغيل هجوم، قم بإصدار هذه الأوامر.

house#show access-list Extended IP access list IDS_FastEthernet0/0_in_1 permit ip host 10.64.10.49 any (permit ip any any (12 matches #house

light#ping 10.64.10.45

.Type escape sequence to abort :Sending 5, 100-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms #light

```
<u>شن الهجوم و التجنب</u>
```

أطلق هجومك من الموجه "الضوء" إلى "بيت" الضحية. عندما تتأثر قائمة التحكم في الوصول (ACL)، يتم مشاهدة الملفات التي يتعذر الوصول إليها.

بمجرد اكتشاف المستشعر للهجوم، ويتم تنزيل قائمة التحكم في الوصول (ACL)، ويتم عرض هذا الإخراج على "House".

house**#show access-list** Extended IP access list IDS_FastEthernet0/0_in_0 permit ip host 10.64.10.49 any (deny ip host 100.100.2 any (459 matches permit ip any any لا تزال المناطق التي يتعذر الوصول إليها مرئية على "الضوء"، كما هو موضح في هذا المثال.

> Light**#ping 10.64.10.45** Type escape sequence to abort . Sending 5, 100-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds . U.U.U (Success rate is 0 percent (0/5 بعد 15 دقيقة، يعود "هاوس" إلى طبيعته، لأن التجنب تم ضبطه على 15 دقيقة.

> > House#**show access-list** Extended IP access list IDS_FastEthernet0/0_in_1 permit ip host 10.64.10.49 any (permit ip any any (12 matches #house

"الضوء" يمكنه إختبار "البيت".

Light#**ping 10.64.10.45**

.Type escape sequence to abort :Sending 5, 100-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

<u>معلومات ذات صلة</u>

- <u>صفحة دعم منع التسلل الآمن من Cisco</u>
- الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما