Configurazione della reimpostazione TCP IPS con l'IME

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Configurazioni Avvia la configurazione del sensore Aggiungere il sensore all'IME Configurare il ripristino TCP per il router Cisco IOS Verifica Avvia l'attacco e reimposta TCP Risoluzione dei problemi Suggerimenti Informazioni correlate

Introduzione

In questo documento viene descritta la configurazione del ripristino TCP IPS (Intrusion Prevention System) tramite l'IME (IPS Manager Express). I sensori IME e IPS vengono utilizzati per gestire un router Cisco per il reset TCP. Quando si esamina la configurazione, tenere presente quanto segue:

- Installare il sensore e accertarsi che funzioni correttamente.
- Estendere l'interfaccia di sniffing al router esterno all'interfaccia.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco IPS Manager Express 7.0
- Sensore Cisco IPS 7.0(0.88)E3
- Router Cisco IOS® con software Cisco IOS versione 12.4

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

Configurazione

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Configurazioni

Nel documento vengono usate le configurazioni mostrate di seguito.

- Luce router
- Router House

Luce router

Current configuration : 906 bytes

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname light
!
enable password cisco
1
username cisco password 0 cisco
ip subnet-zero
!
1
1
ip ssh time-out 120
ip ssh authentication-retries 3
!
call rsvp-sync
!
1
!
fax interface-type modem
mta receive maximum-recipients 0
1
controller E1 2/0
!
!
!
interface FastEthernet0/0
 ip address 10.100.100.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
1
interface BRI4/0
no ip address
shutdown
1
interface BRI4/1
no ip address
shutdown
!
interface BRI4/2
no ip address
shutdown
!
interface BRI4/3
no ip address
shutdown
1
ip classless
ip route 0.0.0.0 0.0.0.0 10.100.100.1
ip http server
ip pim bidir-enable
!
1
dial-peer cor custom
!
1
line con 0
```

```
line 97 108
line aux 0
line vty 0 4
login
!
end
Router House
Current configuration : 939 bytes
1
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
1
logging queue-limit 100
enable password cisco
1
ip subnet-zero
1
!
no ip cef
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!
interface FastEthernet0/0
 ip address 10.66.79.210 255.255.255.224
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 10.100.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface ATM1/0
no ip address
shutdown
no atm ilmi-keepalive
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.193
ip route 1.1.1.0 255.255.255.0 10.100.100.2
no ip http server
no ip http secure-server
!
!
1
1
call rsvp-sync
!
```

```
mgcp profile default
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
password cisco
login
line vty 5 15
login
!
!
end
```

Avvia la configurazione del sensore

Completare questa procedura per avviare la configurazione del sensore.

- 1. Se è la prima volta che si accede al sensore, è necessario immettere **cisco** come nome utente e **cisco** come password.
- 2. Quando il sistema chiede di cambiare la password.**Nota:** Cisco123 è una parola del dizionario e non è consentita nel sistema.
- 3. Digitare **setup** e completare il prompt di sistema per impostare i parametri di base per i sensori.
- 4. Immettere le informazioni seguenti: sensor5#**setup**

--- System Configuration Dialog ---

!--- At any point you may enter a question mark '?' for help. *!--- Use ctrl-c* to abort the configuration dialog at any prompt. *!--- Default settings are in square brackets '[]'.*

```
Current Configuration:
```

```
networkParams
ipAddress 10.66.79.195
netmask 255.255.255.224
defaultGateway 10.66.79.193
hostname Corp-IPS
telnetOption enabled
!--- Permit the IP address of workstation or network with IME accessList ipAddress
10.66.79.0 netmask 255.255.255.0
exit
timeParams
summerTimeParams
active-selection none
exit
exit
service webServer
general
ports 443
exit
exit
```

5. Salvare la configurazione. Il salvataggio della configurazione da parte del sensore può

richiedere alcuni minuti.

- [0] Go to the command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration and exit setup.

Enter your selection[2]: 2

Aggiungere il sensore all'IME

Completare questa procedura per aggiungere il sensore all'IME:

- 1. Accedere al PC Windows in cui è installato IPS Manager Express e aprire IPS Manager Express.
- 2. Scegliete Home > Aggiungi

Home 🔀 Configuration 🌆	Event Monitoring 🚮 Reports	💡 Help
Devices 🗗 🖓	Home > Devices > Devi	ce List
💒 Device List	Add 🗹 Edit 📋 Delete	🕨 🕨 Start 👻 📕 Stop 👻 🇞 Status
	Time Device Name	IP Address Device Type Event S
	😨 Edit Device	
	Sensor Name:	Corp-IPS
	Sensor IP Address:	10.66.79.195
	User Name:	cisco
	Password:	•••••
	Web Server Port:	443
	Communication protocol -	
	💿 Use encrypted conner	ction (https)
	O Use non-encrypted co	onnection (http)
	Event Start Time (UTC) -	
	Most Recent Alerts	
	Start Date (YYYY:MM)	DD):::
	Start Time (HH:MM:SS);
	Exclude alerts of the follo	wing severity level(s)
	Informational Lo	w 🔄 Medium 🔄 High

- 3. Digitare queste informazioni e fare clic su **OK** per completare la configurazione.
- 4. Scegliere **Devices > Corp-IPS** per verificare lo stato del sensore, quindi fare clic con il pulsante destro del mouse per scegliere **Device Status** (Stato dispositivo).Verificare che la

sottoscrizione Sia stata aperta

correttamente.

😨 Device Status	- Corp-IPS	X
Connection Status: Sensor Version:	Subscription successfully opened.	
Cisco Intrusion Pre Host: Realm Keys & k Signature Definition Signature Update Virus Update Component Statistic	vention System, Version 7.0(0.88)E3 ev1.0 vi e S310.0 2007-12-05 VI.2 2005-11-24 is Information: (Press CTRL+F to start searching.)	
AnalysisEngir ReceiverSt TotalPacke Transmitte Transmit DeniedP ResetPa FRU Fra currentf	eStatistics Analysis Engine Statistics ate Receiver Statistics dets Total number of packets processed since reset = 0 rstats Transmitter Statistics ttedPackets Total number of packets transmitted = 0 ackets Total number of packets denied = 0 ackets Total number of packets reset = 0 gnent Reassembly Unit Statistics ragmentsHeld Number of fragments currently n FRU = 0	
Current StreamRea embryor establist dosingS ourrents Current SignatureD Total UDPAoB AxBx SigEvents TotalEve ActionsExe produce	PartialDatagrams Number of datagrams currently in FRU = 0 assemblyUnit TCP Stream Reassembly Unit Statistics in:Streams TCP streams currently in the embryonic state = 0 medStreams TCP streams currently in the dosing state = 0 Streams TCP streams currently in the system = 0 QueuedPackets TCP Packets currently queued for reassembly = VEStats The Signature Database Statistics. Total nodes active = 0 b TCP nodes keyed on both IP addresses and both ports = 0 b UDP nodes keyed on both IP addresses and both ports = 0 Statistics for Signature Events ents Number of SigEvents since reset = 0 sourced Statistics for Actions executed on a SigEvent Alert Number of Alerts written to the IdsEventStore = 0 Stats Insection Stats	Press CTRL+F to start searching. Press up/down an next or previous matching word.
NE al te	Refresh Close	

Configurare il ripristino TCP per il router Cisco IOS

Completare questa procedura per configurare il ripristino TCP per il router Cisco IOS:

- 1. Dal PC IME, aprire il browser Web e visitare il sito https://10.66.79.195.
- 2. Fare clic su OK per accettare il certificato HTTPS scaricato dal sensore.
- Nella finestra di accesso, immettere cisco come nome utente e 123cisco123 come password.Viene visualizzata la seguente interfaccia di gestione IME:

Home 🗞 Configuration 🌆 Ev	ent Monitorin	ig 🚮 Reports 🤗 He	lp				
Configuration > Corp-IPS > Policies	s > Signatu	re Definitions > sig0 > /	Active Sigr	atures			
Corp-IPS							
IPS Policies Signature Definitions	C Edit	Actions 🕒 Enable Ø Dis	sable 📀 R	estore Default	Show	Events +	1 1 M
Active Signatures	Filter: 5	ig ID 📉					
Adware/Spyware	ID A	Name	Fnabled	Severity	Fidelity	Base	Signatu
- 😭 Attack	10	ivanie	Endered	Devenity	Rating	RR	Alert an
DDoS	1000/0	IP options-Bad Option		🦺 Infor	75	18	Alert
Dos Secol	1004/0	IP options-Loose Sour		High	100	100	Alert
	1006/0	IP options-Strict Sourc	~	High	100	100	Alert
S Instant Messaging	1007/0	IPv6 over IPv4		L Infor	100	25	Alert
L2/L3/L4 Protocol	1101/0	Unknown IP Protocol	¥	👗 Infor	75	18	Alert
	1102/0	Impossible IP Packet		High	100	100	Alert
S OS	1104/0	IP Localhost Source S	V	High	100	100	Alert
Other Services	1107/0	RFC 1918 Addresses		🔥 Infor	100	25	Alert
P2P	1108/0	IP Packet with Proto 11	 Image: A start of the start of	High	100	100	Alert
Reconnaissance	1109/0	Cisco IOS Interface DoS		O Medium	75	56	Alert
Releases	1109/1	Cisco IOS Interface DoS		Medium	75	56	Alert
Web Server	1109/2	Cisco IO5 Interface Do5		Medium	75	56	Alert
All Signatures	1109/3	Cisco IOS Interface DoS		😑 Medium	75	56	Alert
Event Action Rules	1200/0	IP Fragmentation Buff		i Infor	100	25	Alert
Tules0	1201/0	IP Fragment Overlap		i Infor	100	25	Alert
😑 🔂 Anomaly Detections	1202/0	IP Fragment Overrun	 Image: A start of the start of	High	100	100	Alert
ot - 10	i toooto	10.5	E.2.		100	100	1000

- 4. Nella scheda Configurazione fare clic su Firme attive.
- 5. Fare quindi clic su **Firma**

Configuration > Corp-IPS > Policie	s > Signature Definitions > sig0	> Act		Refresh
Corp-IPS	Image: Contract of the second seco	Disab	lelp Filter (Cear)	Q Signature Wizard
🔀 DoS	1004/0 IP optione-Loose Sour	1	(1— —)	

6. Nella procedura guidata scegliere Sì e Stringa TCP come motore firma. Fare clic su Next (Avanti).

Custom Signature Wi	zard
N Constants	Welcome
	Welcome to the Custom Signature Wizard. This wizard will guide you through the pro- a custom signature.
	Do you know which Signature Engine you want to use for the custom signature?
nda hda hD h h h h h h h h h h h h h h h h h h	O No

 Èpossibile lasciare queste informazioni predefinite oppure immettere il proprio Signature ID, il nome della firma e le note utente. Fare clic su Next (Avanti).

😨 Custom Signature Wiz	ard		X
N The state of the state	Signature Identific	ation 👘	
	Signature identificatio signature behavior. Yo default values, but ea	n parameters identify and describe the signature, but do not affect the ou must specify a Signature ID and SubSignature ID. You can override the ach required value must be unique (not used by another signature).	
	Signature ID:	60000	
m H S S S S S S S S S S S S S S S S S S	SubSignature ID:	0	
al long	Signature Name:	String.tcp	
<i>HHHHH</i>	Alert Notes:	My Sig Info	
	User Comments:	Sig Comment	

8. Scegliere Azione evento, quindi Genera avviso e Reimposta connessione TCP. Per continuare, fare clic su OK e quindi su

Α	//	/8	ar	1	i

A COMPANY AND A STATE	Engine Specific Parameter	15
	Engine-specific parameters de to fire. You can set the follow	termine what the signature looks for and what causes the signature ing String TCP engine parameters used for this signature.
	Name	Value
	Event Action	Select item(s)
Email FTP VolP Web Pages	 Strip Telnet Options Specify Min Match Length Regex String Service Ports Direction Specify Exact Match Offs Specify Max Match O Specify Min Match Of Specify Min Match O Swap Attacker Victim 	Deny Attacker Inline Deny Attacker Service Pair Inline Deny Attacker Victim Pair Inline Deny Attacker Victim Pair Inline Deny Connection Inline Deny Packet Inline Log Attacker Packets Log Pair Packets Log Pair Packets Select None Produce Alert Produce Verbose Alert Request Block Connection Request Block Host Repuest SNMP Iran ✓ Reset TCP Connection OK Cancel
	Parameter uses the D	efault Value. Click the value field to edit the value. r-Defined Value. Click the icon to restore the default value.

9. Immettere un'espressione regolare. Nell'esempio viene utilizzato testattack. Immettere 23 per le porte di servizio, scegliere **Da servire** per la direzione e fare clic su **Avanti** per continuare.

A DESCRIPTION OF	Engine Specific Parameters		
	Engine-specific parameters determine what to fire. You can set the following String TO	It the signature looks for and what causes the signature IP engine parameters used for this signature.	
	Name	Value	
		Produce Alert Reset TCP Connection	
	Strip Telnet Options	No	
	Specify Min Match Length	No	
	Regex String	testattack	
E O DE	-Service Ports	23	
1711171	Direction	To Service	
HHHHH	Specify Exact Match Offset	No	
		No	
	Specify Min Match Offset	No	
	Swap Attacker Victim	No	

10. Èpossibile lasciare queste informazioni come predefinite. Fare clic su **Next** <u>(Avanti)</u>.

😨 Custom Signature Wi	zard	×
A Destruction	Alert Response	
	You can assign the following values to this signature that reflect both your confidence in of the signature and the severity of the attack it represents. The Signature Fidelity Rati number from 0 to 100, with 100 reflecting the most confidence in this signature. This nu to help calculate the Risk Rating, which helps determine what actions result from the firm signature.	the fidelity ng is any mber is used ng of this
THE SECOND	Signature Fidelity Rating: 75	
Doom Page 1	Severity of the Alert: High	

11. Per completare la procedura guidata, fare clic su **Fine**.



 Scegliere Configurazione > sig0 > Firme attive per individuare la nuova firma creata con il Signature ID o il Nome del Signature. Per visualizzare la firma, fare clic su Modifica.

Name	Value	
-Signature Definition		
Signature ID	60000	
SubSignature ID	0	
🗹 Alert Severity	Medium	
😿 Sig Fidelity Rating	75	
🖬 Promiscuous Delta	0	
Sig Description		
🐨 Signature Name	string.tcp	
🐨 Alert Notes	My Sig Info	
😿 User Comments	Sig Comment	
🗔 Alert Traits	0	
Release	custom	
Engine	String TCP	
😿 Event Action	Produce Alert Reset TCP Connection	
🗔 Strip Telnet Options	No	
Specify Min Match Length	No	
Regex String	testattack	
Service Ports	23	
Tirection	To Service	
Specify Exact Match Offset	No	
Specify Max Match Offset	No	
Specify Min Match Offset	No	
Swap Attacker Victim	No	
de France Concellen	-	
□ Parameter uses the Default Value. Click the value ✓ Parameter uses a User-Defined Value. Click the ic	field to edit the value. on to restore the default value.	
ОК	Cancel Help	

13. Per applicare la firma al sensore, fare clic su **OK** dopo aver confermato e fare clic sul pulsante **Apply** (Applica).

Verifica

Avvia l'attacco e reimposta TCP

Completare questi passaggi per avviare l'attacco e il Reset TCP:

- 1. Prima di lanciare l'attacco, andare all'**IME**, scegliere **Monitoraggio eventi > Vista attacchi** scartati e scegliere il sensore sulla destra.
- 2. Dalla spia del router, passare da Telnet a Router House e iniziare il test di attacco.Premere <space> o <enter> per ripristinare la sessione Telnet. light#telnet 10.100.100.1

```
User Access Verification

Password:

house>en

Password:

house#testattack

[Connection to 10.100.100.1 closed by foreign host]

!--- Telnet session has been reset due to the !--- signature "String.tcp" triggered.
```

3. Dal Dashboard del Visualizzatore eventi IPS, l'Allarme rosso viene visualizzato una volta avviato

l'attacco

allac				
Date		Time	Sig. Name	Sig. ID
}- De∖	/ice: Corp-IPS (188 items)		
ė.	Severity: high	(188 items)		
(-10/23/2009	09:59:13	String.tcp	60000/0
	-10/23/2009	09:59:02	ZOTOB Worm Activity	5570/0
	-10/23/2009	09:58:57	Anig Worm File Tran	5599/0
	-10/23/2009	09:59:00	Anig Worm File Tran	5599/0
	-10/23/2009	09:58:58	Anig Worm File Tran	5599/0
	-10/23/2009	09:59:17	Nachi Worm ICMP E	2158/0

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Suggerimenti

Suggerimenti per la risoluzione dei problemi:

 Lo shun esce dalla porta di comando e di controllo per riprogrammare gli elenchi di controllo di accesso (ACL) del router. I Reset TCP vengono inviati dall'interfaccia di sniffing del sensore. Quando si imposta lo span nello switch, usare il comando set span <src_mod/src_port><dest_mod/dest_port> con entrambi i pacchetti in arrivo abilitati, come mostrato di seguito.

```
banana (enable) set span 2/12 3/6 both inpkts enable
Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12
Incoming Packets enabled. Learning enabled. Multicast enabled.
banana (enable)
banana (enable)
banana (enable) show span
Destination
              : Port 3/6
!--- connect to sniffing interface of the sensor
Admin Source : Port 2/12
!--- connect to FastEthernet0/0 of Router House
Oper Source : Port 2/12
Direction
              : transmit/receive
Incoming Packets: enabled
Multicast
               : enabled
```

 Se il Reset TCP funziona, verificare se l'allarme viene attivato per il tipo di azione Reset TCP. Se viene visualizzato l'avviso, verificare che il tipo di firma sia impostato su TCP reset.Effettuare l'accesso utilizzando l'account del servizio su per eseguire la radice ed eseguire questo comando. Questo comando presuppone che l'interfaccia di rilevamento sia impostata su eth0.

[root@sensor1 root]#tcpdump -i eth0 -n

Nota: un centinaio di reimpostazioni tcp vengono inviate alla vittima/al destinatario, quindi un centinaio vengono inviate all'aggressore/al cliente.Questo è l'output di esempio:

```
03:06:00.598777 64.104.209.205.1409 >
10.66.79.38.telnet: R 107:107(0) ack 72 win 0
03:06:00.598794 64.104.209.205.1409 >
10.66.79.38.telnet: R 108:108(0) ack 72 win 0
```

03:06:00.599360 10.66.79.38.telnet >
64.104.209.205.1409: R 72:72(0) ack 46 win 0
03:06:00.599377 10.66.79.38.telnet >
64.104.209.205.1409: R 73:73(0) ack 46 win 0

Informazioni correlate

- Pagina di supporto per Cisco Secure Intrusion Prevention
- Documentazione per Cisco Secure Intrusion Prevention System
- Documentazione e supporto tecnico Cisco Systems