Domande frequenti ESA: Come si esegue il test della funzione ESA Anti-Spam?

Sommario

Introduzione

In questo documento viene descritto come testare la funzione anti-spam di Cisco Email Security Appliance (ESA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ESA
- AsyncOS
- Funzione Cisco ESA Anti-Spam

Componenti usati

Le informazioni di questo documento si basano su tutte le versioni di AsyncOS.

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.

Come si esegue il test della funzione ESA Anti-Spam?

Per verificare il funzionamento della funzione ESA Anti-Spam, creare un nuovo messaggio tramite TELNET o il client di posta elettronica (Microsoft Outlook, Eudora, Thunderbird, Lotus Notes) e inserire una delle seguenti intestazioni:

- X-Advertisement: Sospetto
- X-Advertisement: Posta indesiderata
- X-Advertisement: Marketing

Èquindi possibile inviare il messaggio tramite l'ESA con la funzione Anti-Spam abilitata e monitorare i risultati.

Test protezione da posta indesiderata con TELNET

In questa sezione viene fornito un esempio che illustra come creare manualmente un messaggio di prova tramite l'utilità TELNET ampiamente disponibile.

Utilizzare le informazioni dell'esempio successivo per creare un messaggio di prova tramite TELNET. Immettere le informazioni visualizzate in **grassetto** e il server deve rispondere come indicato:

```
telnet hostname.example.com 25

220 hostname.example.com ESMTP
ehlo localhost
250-hostname.example.com
250-8BITMIME
250 SIZE 10485760
mail from:




250 sender <sender@example.com> ok
rcpt to:




250 recipient <recipient@example.com> ok
data
354 go ahead
X-Advertisement: Marketing
from: sender@example.com
to: recipient@example.com
subject: test

test
.
250 ok:  Message 120 accepted
```

Esaminare i **mail_logs** e verificare l'esito dell'analisi della posta indesiderata per accertarsi che il messaggio venga considerato come scritto. Come nell'esempio precedente, il criterio di posta in arrivo predefinito rileva che il messaggio è Marketing:

```
Thu Jun 26 22:21:56 2014 Info: New SMTP DCID 66 interface 172.11.1.111 address
 111.22.33.111 port 25
Thu Jun 26 22:21:58 2014 Info: DCID 66 TLS success protocol TLSv1 cipher
 RC4-SHA
Thu Jun 26 22:21:58 2014 Info: Delivery start DCID 66 MID 119 to RID [0]
Thu Jun 26 22:21:59 2014 Info: Message done DCID 66 MID 119 to RID [0]
Thu Jun 26 22:21:59 2014 Info: MID 119 RID [0] Response '2.0.0 s5R2LhnL014175
 Message accepted for delivery'
Thu Jun 26 22:21:59 2014 Info: Message finished MID 119 done
Thu Jun 26 22:22:04 2014 Info: DCID 66 close
Thu Jun 26 22:22:53 2014 Info: SDS_CLIENT: URL scanner enabled=0
Thu Jun 26 22:25:35 2014 Info: SLBL: Database watcher updated from snapshot
 20140627T022535-slbl.db.
Thu Jun 26 22:26:04 2014 Info: Start MID 120 ICID 426
Thu Jun 26 22:26:04 2014 Info: MID 120 ICID 426 From: <sender@example.com>
Thu Jun 26 22:26:10 2014 Info: MID 120 ICID 426 RID 0 To:
 <recipient@example.com>
Thu Jun 26 22:26:20 2014 Info: MID 120 Subject 'test'
Thu Jun 26 22:26:20 2014 Info: MID 120 ready 201 bytes from <sender@example.com>
Thu Jun 26 22:26:20 2014 Info: MID 120 matched all recipients for per-recipient
 policy DEFAULT in the inbound table
Thu Jun 26 22:26:21 2014 Info: MID 120 interim verdict using engine:
 CASE marketing
Thu Jun 26 22:26:21 2014 Info: MID 120 using engine: CASE marketing
Thu Jun 26 22:26:21 2014 Info: MID 120 interim AV verdict using Sophos CLEAN
Thu Jun 26 22:26:21 2014 Info: MID 120 antivirus negative
Thu Jun 26 22:26:21 2014 Info: Message finished MID 120 done
Thu Jun 26 22:26:21 2014 Info: MID 121 queued for delivery
Thu Jun 26 22:26:21 2014 Info: New SMTP DCID 67 interface 172.11.1.111 address
 111.22.33.111 port 25
Thu Jun 26 22:26:21 2014 Info: DCID 67 TLS success protocol TLSv1 cipher RC4-SHA
Thu Jun 26 22:26:21 2014 Info: Delivery start DCID 67 MID 121 to RID [0]
Thu Jun 26 22:26:22 2014 Info: Message done DCID 67 MID 121 to RID [0]
Thu Jun 26 22:26:22 2014 Info: MID 121 RID [0] Response '2.0.0 s5R2QQso009266
 Message accepted for delivery'
Thu Jun 26 22:26:22 2014 Info: Message finished MID 121 done
Thu Jun 26 22:26:27 2014 Info: DCID 67 close
```

Risoluzione dei problemi

Se il messaggio non viene rilevato come posta indesiderata, posta indesiderata sospetta o marketing, esaminare **Criteri posta > Criteri posta in arrivo** o **Criteri posta > Criteri posta in uscita**. Scegliere il nome del criterio o del criterio predefinito e fare clic sul collegamento ipertestuale nella colonna Protezione da posta indesiderata per verificare le impostazioni e la configurazione del criterio di protezione da posta indesiderata.

Cisco consiglia di abilitare le **impostazioni** della **posta indesiderata identificate correttamente**, le **impostazioni** della **posta indesiderata sospetta** e/o le **impostazioni** della **posta elettronica di marketing**, in base alle esigenze.