Comment un Pare-feu ou un proxy de SMTP peut-il affecter des services ESMTP ?

Contenu

Question

Comment un Pare-feu ou un proxy de SMTP peut-il affecter des services ESMTP ?

Réponse

En même temps que la messagerie traitant par une appliance de sécurité du courrier électronique de Cisco (ESA), il y a un certain nombre de Pare-feu et de services proxys de SMTP disponibles qui fournissent des caractéristiques censées pour protéger des serveurs de messagerie contre l'exploit.

Certaines de ces méthodes de protection peuvent empêcher des services ESMTP tels que l'authentification de TLS et de SMTP.

Les services, tels que l'authentification de TLS et de SMTP, l'utilisation ESMTP (SMTP étendu) commandent. Afin d'accéder au positionnement de commande ESMTP, la commande EHLO doit atteindre le serveur de réception. Quelques fonctionnalités de sécurité de Pare-feu et de proxy bloqueront ou modifieront la commande EHLO en transit. Quand le périphérique de sécurité ne permet pas EHLO, aucun services ESMTP ne sera disponible. Dans ce cas, seulement les commandes de SMTP ont spécifié dans la section 4.5.1 RFC 821 sont autorisées sur un serveur de messagerie. Ceux-ci sont : HÉLICOPTÈRE, MESSAGERIE, RCPT, DONNÉES, ENSEMBLE DE RÉFÉRENCE, NOOP, et QUITTÉ. Aucune commande ESMTP n'est disponible.

Une autre fonctionnalité de sécurité utilisée par ces périphériques est modification de bannière de SMTP. Afin de masquer le type et la version du serveur de messagerie protégé, quelques périphériques obscurciront tout sauf les 220 parties de la bannière qui est exigée pour la transmission.

La bannière ressemblera souvent à :

```
220**********
```

Une partie des informations étant masquées est la publicité ESMTP dans la bannière. Quand cette publicité est retirée, un serveur de envoi ne se rendra pas compte que des commandes ESMTP soient reçues.

En résumé, les Pare-feu et les serveurs proxys de SMTP peuvent bloquer des commandes EHLO et masquer des annonces de bannière ESMTP. Quand ces mesures de sécurité sont en place, les commandes ESMTP peuvent ne pas être accessibles. Pour s'assurer que d'autres hôtes peuvent communiquer avec votre ESA utilisant ESMTP, vous pouvez devoir désactiver ces fonctionnalités de sécurité sur votre périphérique de sécurité

Informations connexes

- Test de la fonction Mailguard du pare-feu PIX Firewall
- Cisco PIX : Fonctionnalité avancée et protections d'attaque
- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems