ファイアウォールまたは SMTP プロキシは ESMTP サービスにどのような影響を与える可能性がありますか。

目次

質問

ファイアウォールまたは SMTP プロキシは ESMTP サービスにどのような影響を与える可能性がありますか。

回答

Cisco E メール セキュリティ アプライアンス (ESA) を通って処理するメールと共にいくつかのファイアウォールおよび利用可能なエクスプロイトからメール サーバを保護するために意味される機能を提供する SMTP プロキシサービスがあります。

いくつかの保護のこれらの方式は TLS および SMTP 認証のような ESMTP サービスを妨害できます。

サービスは、TLS および SMTP 認証のような、使用 ESMTP （ 拡張 SMTP) 命じます。 ESMTP コマンド セットにアクセスするために、EHLO コマンドは受信サーバに達する必要があります。 いくつかのファイアウォールおよびプロキシ セキュリティ機能は送信中に EHLO コマンドをブロックするか、または修正します。 安全 装置が EHLO を可能にしない場合、ESMTP サービスは利用できません。 この場合、RFC 821 セクション 4.5.1 で規定 される SMTP コマンドだけメール・サーバで許可されます。 これらを次に示します。 ヘリコプター、メール、RCPT、DATA、RSET、NOOP、およびやめられる。 ESMTP コマンドは利用できません。

これらのデバイスによって使用されるもう一つのセキュリティ機能は SMTP バナー修正です。 保護されたメール・サーバの種類およびバージョンを隠すために、いくつかのデバイスはすべて通信に必要となるバナーの 220 部分を覆いますが。

バナーは頻繁に類似したのにようです:

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

隠されている情報の一部分はバナーの ESMTP アドバタイズメントです。 このアドバタイズメントが取除かれる場合、送信サーバは ESMTP コマンドが許可されることわかっていません。

要約すると、ファイアウォールおよび SMTP プロキシ・ サーバは EHLO コマンドをブロックし、ESMTP バナー アドバタイズメントを隠すかもしれません。 これらのセキュリティ対策が時、ESMTP コマンドはアクセス可能ではないかもしれません。 他のホストが ESMTP を使用して ESA と通信できるようにするために安全 装置のこれらのセキュリティ機能を無効に する必要がある場合もあります

関連情報

- PIXファイアウォール メールガード機能のテスト
- Cisco PIX: 進んだ機能および不正侵入ガード
- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems