Hoe kan een firewall of een MTP-proxy de ESMTP-diensten beïnvloeden?

Inhoud

vraag

Hoe kan een firewall of een MTP-proxy de ESMTP-diensten beïnvloeden?

Antwoord

In combinatie met mailverwerking door een Cisco Email Security Appliance (ESA) zijn er een aantal firewalls en MTP-proxyservices beschikbaar die functies bieden die bedoeld zijn om mailservers te beschermen tegen exploitatie.

Sommige van deze beschermingsmethoden kunnen de ESMTP-diensten, zoals TLS- en MTP-verificatie, belemmeren.

De services, zoals TLS en TCP-verificatie, gebruiken ESMTP (Extended MTP)-opdrachten. Om toegang te krijgen tot de ESMTP-opdrachtset moet de EHLO-opdracht de ontvangende server bereiken. Sommige firewall- en proxy-beveiligingsfuncties zullen de EHLO-opdracht tijdens het transport blokkeren of wijzigen. Wanneer het veiligheidsapparaat EHLO niet toelaat, zijn er geen ESMTP-services beschikbaar. In dit geval, zijn alleen de opdrachten die in RFC 821, sectie 4.5.1, zijn gespecificeerd op een mailserver toegestaan. Dit zijn: HELO, MAIL, RCPT, DATA, RSET, NOOP en QUIT. Er zijn geen ESMTP-opdrachten beschikbaar.

Een andere beveiligingsfunctie die door deze apparaten wordt gebruikt, is het wijzigen van een mtp-banner. Om het type en de versie van de beschermde mailserver te verbergen, zullen sommige apparaten alle behalve het 220 gedeelte van de banner aan het oog onttrekken die voor de communicatie vereist is.

Het spandoek lijkt vaak op:

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

Een deel van de informatie die wordt verborgen is de ESMTP-advertentie in de banner. Wanneer deze advertentie wordt verwijderd, is een verzendserver zich er niet van bewust dat ESMTP-opdrachten zijn geaccepteerd.

Samengevat kunnen firewalls en MTP-proxyservers EHLO-opdrachten blokkeren en ESMTP-

banneradvertenties verbergen. Wanneer deze beveiligingsmaatregelen van kracht zijn, zijn ESMTP-opdrachten mogelijk niet toegankelijk. Om er zeker van te zijn dat andere hosts met uw ESA kunnen communiceren via ESMTP, moet u deze beveiligingsfuncties mogelijk op uw beveiligingsapparaat uitschakelen

Gerelateerde informatie

- De functie PIX-firewall-mailbeveiliging testen
- Cisco PIX: Geavanceerde functies en aanvallen
- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems