ESA DHAP功能能力提升计划

文档ID117847

已更新：钧窑25， 2014

贡献由John Yu和罗伯特Sherwin， Cisco TAC工程师。

下载 pdf文档
打印
Feedback

相关产品

- 思科内容安全管理设备
- 思科电子邮件安全工具
- 思科Web安全工具

目录

简介

本文描述如何使在思科电子邮件安全工具(ESA)的目录收获攻击预防(DHAP)功能为了防止目录收获攻击(DHAs)。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ESA
- AsyncOS

使用的组件

本文档中的信息根据AsyncOS所有版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

DHA是由垃圾邮件发送者使用为了找出有效电子邮件地址的技术。有使用为了生成地址该DHA目标的两个主要技术：

- 垃圾邮件发送者建立字母和编号的所有可能的组合列表，然后添附域名。

- 垃圾邮件发送者以结合普通的名字、姓氏和初始列表的创建使用一标准的词典攻击。

DHAP是在可以启用的思科内容安全工具的一个支持的功能，当轻量级目录访问协议(LDAP)使用时接受验证。 DHAP功能记录无效接收地址数量从一给的发送方的。

一旦发送方超过一管理员定义的阈值，发送方视为不信任，并且从该发送方的邮件阻塞没有网络设计要求(NDR)或错误代码生成。您能配置阈值根据发送方的名誉。例如，不信任或可疑发送方能有低DHAP阈值，并且委托或名声好的发送方能有高DHAP阈值。

Enable (event) DHAP

为了启用DHAP功能，请导航**邮寄策略>主机访问表(帽子)**从内容安全工具GUI和选择**邮件流量策略**。选择您希望从**策略名称**列编辑的策略。

帽子有使用为了操作在从远程主机的连接的四个基本访问规则：

- **接受**：连接接受，并且电子邮件接受由监听程序设置进一步限制。这包括接收访问表(为公共监听程序)。

- **拒绝**：连接最初接受，但是尝试连接接收4XX或5XX问候语的客户端。电子邮件没有接受。

- **TCPREFUSE** ：连接拒绝在TCP级别。

- **中继**：连接接受。接收所有收件人的由接收访问表允许和没有限制条件。域密钥签字是仅可用的在中继邮件流量策略。

在选定策略的**邮件流量限额**部分，查找和通过设置麦斯设置**目录收获攻击预防(DHAP)**配置。无效收件人每个小时。您能也选择定制麦斯。无效收件人每个小时代码和麦斯。如果如此希望，无效收件人每个小时发短信。

您必须重复此部分为了配置additonal策略的DHAP。

保证您提交并且确认在GUI上的所有变化。

Note:思科建议您使用五和十范围的一最大**无效收件人最大每个从远程主机**设置的**小时**。

Note:其他信息，参考在Cisco支持门户的**AsyncOS用户指南**。

本文档是否是有用？有 没有

感谢您的反馈。

打开支持案例（需要思科服务合同。）

相关的思科支持社区讨论

思科支持社区是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 Cisco Technical Tips Conventions 。

已更新：钧窑25， 2014
文档ID117847