如何通过思科邮件安全设备允许模拟网络钓鱼平台活动

目录

简介

本文档介绍思科邮件安全设备(ESA)上的配置步骤，以成功实现模拟网络钓鱼平台活动。

先决条件

要求

Cisco 建议您了解以下主题：

- 在ESA上创建邮件和内容过滤器。
- 主机访问表(HAT)的配置。
- 了解思科ESA的传入邮件渠道。

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

模拟网络钓鱼平台允许管理员在一个周期中运行网络钓鱼活动，以管理使用邮件系统作为社会工程攻击媒介的最大威胁之一。

问题

当ESA没有为此类模拟做好准备时，其扫描引擎停止网络钓鱼活动消息并不罕见，这会导致模拟失败或效率降低。

解决方案

> **警告**：在此配置示例中，选择*TRUSTED* 邮件流策略，以允许ESA通过更大的模拟网络钓鱼活动，而不进行任何限制。持续开展大量网络钓鱼活动可能会影响邮件处理性能。

为确保网络钓鱼活动邮件不会被ESA配置的任何安全组件阻止，需要将其置于适当位置。

1. 创建新发件人组：**GUI > Mail Policies > HAT Overview**并将其绑定到*TRUSTED* mail flow policy(或者，可以使用**GUI > Mail Policies > Mail Flow Policies下的类似选项创建新策**略)。
2. 将模拟网络钓鱼平台的发送主机或IP添加到此发件人组。如果模拟网络钓鱼平台具有大量IP，则可以添加部分主机名，或者IP范围（如果适用）。
3. 将发件人组排序到您的*阻止列*表发件人组上方，以确保其静态匹配，而不是SBRS。
4. 在GUI > Mail Policies > Mail Flow Policies > TRUSTED*(或*新创建的邮件流策略)下**禁用TRUSTED邮件流策略的所有安全功能：**

Security Features	
Spam Detection:	Use Default (On) On Off
AMP Detection	Use Default (On) On Off
Virus Protection:	Use Default (On) On Off
Sender Domain Reputation Verification:	Use Default (On) On Off
Virus Outbreak Filters:	Use Default (On) On Off
Advanced Phishing Protection:	Use Default (On) On Off
Graymail Detection:	Use Default (On) On Off
Content Filters:	Use Default (On) On Off
Message Filters:	Use Default (On) On Off

5.提**交这些更改并提交。**

之前的AsyncOS v.14

> **警告**：在此配置示例中，选择*TRUSTED* 邮件流策略，以允许ESA通过更大的模拟网络钓鱼活动，而不进行任何限制。持续开展大量网络钓鱼活动可能会影响邮件处理性能。

为确保网络钓鱼活动邮件不会被ESA配置的任何安全组件阻止，需要将其置于适当位置。

1. 创建新发件人组：**GUI > Mail Policies > HAT Overview，并**将其绑定到*TRUSTED邮*件流策略。
2. 将模拟网络钓鱼平台的发送主机或IP添加到此发件人组。如果模拟网络钓鱼平台具有大量IP，则可以添加部分主机名，或者IP范围（如果适用）。
3. 将发件人组排序到您的*阻止列*表发件人组上方，以确保其静态匹配，而不是SBRS。
4. **提交这些更改并提交。**
5. 导航至CLI并添加新的邮件过滤器、CLI **>过滤器、复**制和修改语法并添加过滤器。

6.

```
skip_engines_for_simulated_phishing:
if (sendergroup == "name_of_the_newly_created_sender_group")
{
insert-header("x-sp", "uniquevalue");
log-entry("Skipped scanning engines for simulated phishing");
skip-spamcheck();
skip-viruscheck();
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
skip-filters();
}
.
```

7. 在列表中对邮件过滤器进行向上排序，以确保邮件过滤器不会被其上方的另一个邮件过滤器跳过，该过滤器包括跳过过滤器操作。
8. 按Enter键导航回AsyncOS的主命令提示符，并发出命令“**commit**”提交更改。（请勿点击CTRL+C — 它将清除所有更改）。
9. 导航至GUI**> Mail Policies > Incoming Content Filters**
10. 创建新的传入内容过滤器，***其条件为***“其他报头”，以查找在邮件过滤器中配置的自定义报头**“x-sp”及其唯一值**，并配置操作“跳过剩余内容过滤器（最终操作）”(**Skip Remaining Content Filters [Final Action])。**
11. 将内容过滤器排序为“1”，以确保其他过滤器不会对模拟的网络钓鱼邮件采取操作。
12. 导航至**GUI > Mail Policies > Incoming Mail Policies，**并将内容过滤器分配到所需策略。
13. **提交并提交更改。**
14. 运行模拟网络钓鱼平台活动并监控mail_logs/邮件跟踪，以验证流和策略规则匹配。