目录

HOL-1942-01-NET - VMware AppDefense - 保护数据中心端点 ................................................. 2
  实验室指导 ................................................................................................................ 3
第 1 单元 - VMware AppDefense 概述（15 分钟） ............................................................. 8
  AppDefense 平台概述 ...................................................................................................... 9
  结束语 ......................................................................................................................... 13
第 2 单元 - 了解并利用 AppDefense 平台（45 分钟） ..................................................... 14
  登录实验室的“Environment & Preparing”（环境和准备）部分 .................................. 15
  了解 AppDefense Manager .................................................................................................. 18
  创建 AppDefense 安全范围 .............................................................................................. 23
  检查 AppDefense 安全范围 .............................................................................................. 30
  安全范围响应例程 .......................................................................................................... 36
  攻击应用和验证自动化响应 ............................................................................................. 44
  升级应用组件 .................................................................................................................. 63
  结束语 ......................................................................................................................... 73
HOL-1942-01-NET - VMware AppDefense - 保护数据中心端点
实验室指导

注意：本实验室只包含两个单元。预计完成时间为 45-60 分钟。

目录可以从实验室手册的右上角访问。

VMware AppDefense 是一款数据中心安全工具，能够实现应用控制、检测和响应。该工具可提供云计算工作负载保护的基本要素，例如系统完整性、应用控制和内存监控。

实验室单元列表：

- (15 分钟) - 基础 - 本单元将讲解演示平台的架构。
- (45 分钟) - 基础 - 本单元将讲解演示如何创建安全范围。然后，在制造各种攻击后，您将监控应用。最后，您将执行修复、隔离和升级操作。

实验室负责人和支持人员：

- 加拿大系统工程师 Geoff Shukin

本实验室的完成与 AppDefense 工程团队的努力是分不开的。他们给予了非常重要的支持与协助，将本实验室打造得适合 VMworld 动手实验室环境。我们要感谢以下各位：

- 技术员 Zhen Mo
- 主管工程师 Hengjun Tian
- 主管工程师 Amit Chopra
- 技术员 Alex Ma
- 主管工程师 Amol Khare

本实验室手册可以从动手实验室文档站点下载，网址为：

http://docs.hol.vmware.com

本实验室可能提供其他语言版本。要设置语言首选项并在实验室中部署本地化手册，可以在以下文档的帮助指导下完成：

主控制台的位置

1. 红框区域包含主控制台。实验室手册位于主控制台右侧的选项卡上。
2. 个别实验室可能会用到左上角独立选项卡上的其他控制台。如有需要，系统将引导您打开其他的特定控制台。
3. 实验室时间为 90 分钟，由计时器计时。实验室结果无法保存。所有操作都必须在实验室课程中完成。但是您可以单击“EXTEND”（延长）延长时间。在 VMware 活动期间，您可以将实验室时间延长两次，最多可延长 30 分钟，每单击一次可延长 15 分钟。非 VMware 活动期间，最多可将实验室时间延长至 9 小时 30 分钟。每单击一次可延长一小时。

键盘数据输入的替代方法

在本单元中，您将向主控制台中输入文本。除直接输入外，还有两种非常有用的数据输入方法，可简化输入复杂数据的过程。

单击实验室手册内容并拖放到控制台的活动窗口
您也可以单击实验室手册中的文本和命令行界面 (CLI) 命令，并将其直接拖放到主控制台中的活动窗口。

访问在线国际键盘

您还可以使用主控制台中的在线国际键盘。

1. 单击 Windows 快速启动任务栏上的键盘图标。

在活动的控制台窗口中单击一下

在本例中，您将使用在线键盘输入电子邮件地址中所使用的“@”符号。在美式键盘布局中，输入“@”符号需要按住 Shift 并按 2。

1. 在活动的控制台窗口中单击一下。
2. 单击 Shift 键。
单击 @ 键

1. 单击“@”键。
您会发现，“@”符号已在活动控制台窗口中输入。

激活提示或水印

首次启动实验室时，您可能会注意到桌面上有一个水印，提示 Windows 尚未激活。

虚拟化的一个主要优势在于，可以在任意平台上移动和运行虚拟机。本动手实验室利用了这一优势，我们可以运行多个数据中心内的实验室。但是，这些数据中心的处理器可能不同，因此会通过 Internet 触发 Microsoft 激活检查。

请放心，VMware 和这些动手实验室完全符合 Microsoft 的许可要求，您使用的实验室是一个独立的单元，不具备对 Internet 的完全访问权限，而 Windows 需要该权限才能验证激活。如果没有对 Internet 的完全访问权限，此自动化过程会失败，并且显示此水印。

这一表面问题不会影响到您的实验室。
查看屏幕右下部分

请检查是否完成实验室的所有启动例程，以及是否准备好开始。如果您看到的内容并非“Ready”（准备就绪），请等待几分钟。如果 5 分钟后，您的实验室仍未变为“Ready”（准备就绪），请寻求帮助。
第 1 单元 - VMware AppDefense 概述（15 分钟）
AppDefense 平台概述

在这一部分，您将了解有关 VMware 新推出的 AppDefense 安全平台的信息。

说明

AppDefense 是一种数据中心端点安全产品，可将威胁检测和响应嵌入应用和数据所在的虚拟化层中。AppDefense 借助 VMware vSphere® 提供了优于现有端点安全解决方案的三项关键优势：

对应用预期状态有着权威性的了解 – 知道什么是好的状态，便能检测到不好的状态。

在 vSphere hypervisor 中，AppDefense 可全面掌控数据中心端点的行为情况，并在第一时间了解所做的更改。这种切合实际情境的信息处理能力更加精确，不必再为“哪些更改合规，哪些更改的确是威胁”之类的问题猜来猜去。AppDefense 不会查看处于隔离状态的客户机工作负载，而是将工作负载作为更广泛的“安全范围”的一部分进行管理。通过这些范围，AppDefense 能够深入了解数据中心内的复杂交互行为模式，而非简单的单个虚拟机行为。

自动准确的威胁响应 – 即刻触发响应动作。当检测到威胁时，AppDefense 可以触发 vSphere 和 VMware NSX® 去编排正确的威胁响应流程，而无需手动干预。例如，AppDefense 可以自动：

- 提醒新行为
- 阻止进程通信
- 生成用于取证分析的虚拟机内存和磁盘快照
- 暂停虚拟机
- 关闭虚拟机

与攻击面隔离开来 – 借助此平台，我们可以对保护者提供保护。多数恶意软件变体在到达端点时要做第一件事是，禁用防病毒和其他基于代理的端点安全解决方案。Hypervisor 提供了一个受保护位置，让 AppDefense 可在该处运行，从而确保即使在端点受到攻击时，AppDefense 自身也能受到保护。
VMware AppDefense 平台的主要组件有：

**AppDefense Manager** 控制台是一种多租户云计算服务提供的实例，可在一个位置定义应用的预期行为和保护规则。您可以在这个位置监控配置的实施情况、安全事件以及警报。

**AppDefense** 设备是一个本地控制点，用于向管理器传入数据以及从中传出数据。它以代理身份连接 VMware 管理组件（如 vCenter），并建立指向 AppDefense Manager 的出站连接。

**AppDefense** 客户机模块部署在客户虚拟机中，现在包含最新版本的 VMTools。此模块与支持的 AppDefense 主机模块（采用 VMware 可安装捆绑包形式）一起部署在 ESXi 主机上。这两个组件协同运行，可监控和强制实现客户机行为的预期状态，并确保在 hypervisor 中将保护控制与客户机“攻击面”隔离开来。

**vCenter** 用于收集客户站点上的清单数据。此清单数据用于安全范围分配、客户机准备事宜（基于操作系统信息）以及客户机到主机的分配。AppDefense 在响应安全事件（如暂停客户机）时，也可以使用 vCenter 执行修复操作。

**NSX（可选）** 用作 AppDefense 的一个可选的附加修复通道。具体而言，在出现任何违反保护规则的行为时，都可使用 NSX 来自动或手动隔离虚拟机。

在调配时，可以选择使用 vRealize Automation/vRealize Orchestrator（可选）从应用蓝图捕获应用环境信息。
**AppDefense 功能**

AppDefense 平台提供以下功能：

- **应用控制** - 可全面查看数据中心内的工作负载及其预期状态和允许的行为，并对这些工作负载进行分组。
- **运行时异常检测与控制** - 监控操作系统、用户应用、警报和控制流程、网络以及内核事件的实时状态。
- **进程分析** - 内置的进程分析引擎可提供整体进程恶意性评分，并显示潜在可疑的具体特征。
- **经过编排的修复** - 可让用户全面了解虚拟基础架构以及客户机操作系统和应用体系，能够在出现安全事件时以更有效的方式编排具体的相关修复。

**独立的信任区域**

通过在 hypervisor 中操作，AppDefense 还可提供传统端点保护平台无法提供的保护和抽象化，从而为应用层创建最有效的最低权限模型。

在独立的“信任区域”为保护者提供保护：

- 通过在 hypervisor 中操作，AppDefense 还可提供传统端点保护平台无法提供的保护和抽象化，从而为应用层创建最有效的最低权限模型。

**内核级监控**

- 监控客户机中的每个加载/卸载事件。
- 验证已加载模块的签名，并将内存中的代码状态和磁盘状态进行比较，以防止篡改。
• 对内核代码页的所有内容进行内存跟踪，以获取有关篡改的即时通知

内存和进程监控

• 监控客户机物理/虚拟页面表映射，确保客户机操作系统的内部和外部视图一致
• 始终对 hypervisor 中的客户机进程表执行卷影复制，确保客户机的一致性

与其他端点安全产品不同，AppDefense 与攻击面隔离开，而不会牺牲提供准确安全警报所需的环境信息。此外，AppDefense 还可与 NSX 以及其他基础架构控制点配合使用，自动对检测到的威胁做出响应，从而最大限度地降低数据泄露的可能性以及对业务的影响。
结束语

恭喜您完成“第 1 单元 - VMware AppDefense 平台概述”。

继续学习下一单元：

实验室单元列表：

- (15 分钟) - 基础 - 本单元将讲解演示平台的架构。
- (45 分钟) - 基础 - 本单元将讲解演示如何创建安全范围。然后，您将在应用经历各种攻击后对其进行监控。最后，您将执行修复、隔离和升级操作。

如何结束实验室

如果您想立即结束实验室，直接单击屏幕上方的“END”（结束）按钮即可。如果不想结束，请继续学习第 2 单元。
第 2 单元 - 了解并利用 AppDefense 平台（45 分钟）
登录实验室的“Environment & Preparing”（环境和准备）部分

为了做好实验准备，我们将同时登录 vSphere 和 AppDefense Manager。

从主控制台启动 Chrome

1. 在主控制台桌面上或屏幕底部的任务栏中找到 Chrome 快捷方式。

打开 vSphere Web Client

启动 Chrome 后，系统会自动将您转到 vSphere Web Client 登录页面。使用以下凭证访问 vSphere Web Client。

1. 当系统提示输入用户名和密码时，请键入以下凭证：

<table>
<thead>
<tr>
<th>User name: <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Password: VMware1!</td>
</tr>
</tbody>
</table>

2. 单击“Login”（登录）
注意：如果几分钟之后，您的浏览器仍未进入登录页面，请直接刷新浏览器会话。

打开选项卡以显示 **AppDefense Manager**

1. 右键单击“AppDefense Manager”书签
2. 单击“Open in new tab”（在新选项卡中打开）

此操作将在 Chrome 中启动一个新选项卡以显示“AppDefense Manager”虚拟机。

3. 单击新选项卡，（未在可见区域中显示）

**注意**：根据实验室环境在开始实验之前等待的时间，系统可能会立即将您转到 AppDefense 主控制面板，如果是这样，您可以。如果系统向您展示的是主登录页面，则需要继续执行下一步骤。

登录 **AppDefense** 门户
1. 当系统提示输入用户名和密码时，请键入以下凭证：

- holuser@vmware.com
- VMware1!

2. 单击“Sign In”（登录）
了解 AppDefense Manager

在这一部分，我们将讲解演示 AppDefense Manager 以及用户界面的各个部分。

AppDefense Manager 界面

正如概述单元中所提到的，云计算管理器是一种多租户服务，可在一个位置定义应用的预期行为和保护规则。在最新版本中，此管理器在公有云中作为服务运行。客户可以使用此管理器监控配置的执行情况、安全事件以及警报。

VMware 在 AppDefense Cloud Manager 中为您建立帐户和租户后，您将收到一封关于加入该服务的电子邮件。加入该服务后，您便可以登录并连接设备以及执行其他平台配置。

但是，为了实现 VMware 动手实验室环境，此管理器将在本地实例中运行。用户 “holuser@vmware.com”已在其自己的租户下创建完成。您现在可以使用此用户的帐户登录。

在这一默认视图中，您可以看到“Protection Coverage”（保护覆盖范围）、“Security Scopes”（安全范围）、“Alarms”（警报）和“Events”（事件）。在我们探索此实验室的过程中，您会更详细地了解这些选项。

注意：视图中显示的“Provisioning Events”（调配事件）是建造此实验室时的构件，可以忽略。
查看用户设置

在 AppDefense Manager 左下角，您将在“holuser@vmware.com”用户名旁边看到一个“Setting”（设置）图标。

1. 单击 AppDefense Manager 选项卡（如果您尚未处于此页面）
2. 单击左下角“holuser@vmware.com”用户名旁边的“Setting”（设置）图标。提示：它看起来像一个小齿轮
3. 单击“Appliances”（设备）

**AppDefense Appliance (AppDefense 设备) 菜单**

AppDefense 设备是一个单独的本地控制点，用于向 AppDefense Manager 传入数据以及从中传出数据。它以代理身份连接 VMware 管理组件（如 vCenter），并建立指向 AppDefense Cloud Manager 的出站连接。

可以通过标准 .ovf 部署工作流在客户站点部署 AppDefense 设备。部署好设备后，用户将登录 AppDefense Cloud Manager 并将设备连接到其租户。此外，设备将连接到数据中心内的各种源（如 vCenter 或 NSX）。

1. 验证设备是否处于活动状态并正确连接到 vCenter 和 NSX，如上图所示。

查看“Inventory”（清单）

返回到左下角的“Settings”（设置）菜单。您将在“holuser@vmware.com”用户名旁边看到一个小齿轮图标。

1. 单击“Settings”（设置）图标
2. 单击“Inventory”（清单）
Inventory (清单)

在这个视图中，您可以在清单中提供的 ESXi 主机和虚拟机之间切换，确定其各自的模块是否已安装，操作系统版本是什么等。直接单击菜单顶部的“Hosts”（主机）或“VMs”（虚拟机）即可实现此操作。

请记住，AppDefense 监控的是客户机和主机级别的活动、损坏情况或任何其他异常行为。

Unassigned VMs (未分配的虚拟机)

返回到左下角的“Settings”（设置）菜单。您将在“holuser@vmware.com”用户名旁边看到一个小齿轮图标。

1. 单击“Settings”（设置）图标
2. 单击“Unassigned VMs”（未分配的虚拟机）

查看“Unassigned VMs”（未分配的虚拟机）

这个视图显示的是清单中当前未分配给任何安全范围的虚拟机。它还将显示这些特定虚拟机所对应的主机和客户机模块的当前运行状态。

橙色和红色区域代表处于发现模式或受保护的虚拟机。

查看“Downloads”（下载）

本实验室中使用的是 AppDefense Manager 的本地版本，该版本不支持自动下载，因此关于此步骤的图片来自基于实际生产云计算的 AppDefense Manager。您可以看到，管理门户本身就提供了所有文档、OVA 文件、VIB 和客户机模块。
创建 AppDefense 安全范围

安全范围是 AppDefense 中的基本组件，可建立应用应具备的预期状态和允许的特定行为。在这一部分，我们将为您讲解演示针对小型测试应用创建安全范围的工作流。

创建安全范围

安全范围可定义相关配置元素，以保护应用及其构成工作负载。这些配置元素构成了应用的“蓝图”或“诞生证明”。它包含描述、成员工作负载、规则和行为。

这是 AppDefense 理念的基本原则。AppDefense 专注的是应用，而不仅仅是单独的端点，因此，它能够获取更全面的关于应用预期状态的使用情景知识。

您现在可以创建一个安全范围来保护动手实验室环境中运行的抵押贷款应用示例。

在“AppDefense Manager”选项卡中，找到左侧菜单中的“Scopes”（范围）。

1. 单击“Scopes”（范围）旁边的“+”号，进入“Security Scope”（安全范围）向导。
为安全范围命名

1. 键入以下内容作为范围名称

```
HOL-App
```

2. 单击“Create”（创建）按钮

向安全范围添加服务

单击“Create”（创建）后，UI 将默认在左侧菜单中高亮显示该范围。

1. 单击 UI 左上角的“Add Service”（添加服务）按钮
创建 Web 服务

1. 键入以下内容作为服务名称
   
   Web_Tier

2. 单击向下箭头
3. 从列表中选择“Web Server”（Web 服务器）。这是一个预先填充的常用服务列表。这些条目只是描述性内容，不需要添加到安全范围中。

在“Service Description”（服务描述）中，您可以指定所选择的其他信息。这不是强制性操作，但在运维环境中指示服务的其他相关信息会非常有用。

4. 单击“Next”（下一步）
向服务添加成员

1. 选中清单中列出的 web 虚拟机旁边的复选框
2. 单击“Next”（下一步）按钮

**Allowed Behaviors** (允许的行为)

**AppDefense** 可以关联到 vRealize Automation 或 Puppet 等调配系统，定义允许的相应行为。它还可以在学习模式下运行。此运维模式允许系统根据应用在一段时间内的运行时视图填充允许的行为。

在此模式下，**AppDefense** 平台将动态地学习目标应用的行为（如端口、进程等）。在某些情况下，您可能希望明确定义允许的行为。出于本实验室的目的考虑，我们将不在此窗口中指定任何行为。
1. 单击“Finish”（完成）

创建数据库服务

现在，您将执行与上述相同的工作流来创建要在应用安全范围中使用的数据库服务。

1. 单击“Add Service”（添加服务）

指定数据库服务参数
1. 键入以下内容作为服务名称

DB_Tier

2. 单击下拉箭头
3. 选择“Other”（其他）。请记住，这是一个预先填充的常用服务列表。这些条目只是描述性内容，不需要添加到安全范围中。
4. （可选）键入一段简短说明。
5. 单击“Next”（下一步）

向数据库服务添加成员

1. 选中清单中列出的 db 虚拟机旁边的复选框
2. 单击“Next”（下一步）
完成数据库服务创建

1. 单击“Finish”（完成）
检查 AppDefense 安全范围

在这一部分，我们将修改安全范围以根据具体威胁途径更改警报操作，继续向您讲解演示 AppDefense 的使用流程。

检查安全范围设置

正如我们所讨论的，AppDefense 会创建一个允许的行为列表（如端口、进程等），以构建应用预期状态的“蓝图”或“白名单”。借助 vRealize Automation、vRealize Orchestrator、Puppet 或类似引擎等调配接口，AppDefense 可以创建此蓝图。

但是，在部署应用后，AppDefense 还可以“学习”这些行为。创建好安全范围并将其应用到某个应用后，默认模式为“Learning Mode”（学习模式），在此期间，系统会在应用运行时记录所有相关活动。

完成检查后，安全运维团队或应用所有者可以验证和/或修改这一预期活动主列表。确定最终预期状态后，系统会将安全范围置于“Protected Mode”（受保护模式）。

安全范围移至此模式后，AppDefense 将使用允许的行为列表针对工作负载强制实施正确的安全环境和状况，以防任何偏离该列表的行为。

此时请勿单击“Verify”（验证）和“Protect”（保护）。

HOL-1942-01-NET
注意：工作负载或应用的建议学习时间通常为7-14天。我们在动手实验室环境中没有那么多的时间，因此我们已自动完成服务创建过程中的大部分“允许的进程”。如果您注意到的话，这里应该有大约60个已学习的行为。

探索其中一些已学习的行为

显示的信息类型：

Path（路径）：这是从操作系统文件结构中启动进程的位置。

Hash（哈希）：这是进程中的哈希值。这是一种额外防护措施，旨在防止使用可信名称启动恶意进程的行为。

“Trust Score”（信任评分）和“Threat Score”（威胁评分）：这两个值是与Carbon Black信誉服务的后端集成基于Windows的服务提供的。该集成能够针对安全团队可能不知道的已学习行为提供相关洞察信息，这样可以针对系统在学习过程中遭到入侵的情况提供额外防护，对基于Linux的系统来说，这些评分由来自多个软件包部署站点的集成得出。在此环境中，这里的评分已预先填好以供演示。HOL环境的隔离特性使其无法产生基于实时集成的结果。

“Package”（软件包）：系统将根据与编排平台（如Puppet）的集成填充元数据。

“Outbound connection behaviors”（出站连接行为）和“Inbound connection behaviors”（入站连接行为）：这两部分提供了有关侦听和用于通信的端口和地址的信息。

1. 展开列出的任何服务旁边的“>”，即可看到关于列出的任何一种行为的一些可用详细信息。
2. 初步展开后，点击“>”即可展开CLI旁边的“Outbound connection behaviors”部分，如上图示例所示。
注意：如上一页所述，在学习模式下运行时，根据具体应用，通常建议用时为7-14天。但在此HOL环境中，我们没有这么长的时间，因此由系统自动完成了部分学习内容，并且在部分进程信息中使用了通配符。

在下一步中，您将生成一些典型流量以观察学习过程。

生成已学习的行为

1. 在浏览器中打开一个新的选项卡，请勿关闭当前选项卡。
2. 单击“Mortgage App”（抵押贷款应用）书签。此时将显示访问测试应用的登录屏幕。
3. 单击“Log In”（登录），无需提供任何凭证。
4. 刷新“Mortgage App”（抵押贷款应用）选项卡，方法是按住Ctrl键并单击“Mortgage App”（抵押贷款应用）书签两到三次，每次都点击一下“Log In”（登录）按钮以生成流量。（此时将在多个选项卡上打开应用登录页面。）此操作仅生成新学习的行为的流量，有些行为可能需要2-5分钟才能填充完。生成这些选项卡后，您随时可以将其关闭。

将“Mortgage App”（抵押贷款应用）选项卡保持在打开状态，并返回“AppDefense Manager”选项卡。
刷新 AppDefense Manager

1. 单击并返回“AppDefense Manager”选项卡。

在此环境中，从访问“Mortgage App”（抵押贷款应用）选项卡到其他行为出现在 AppDefense Manager 控制台中会存在一定延迟，但延迟应该只有几分钟。这里的要点是看到已学习行为的数量有所增加，我们创建安全范围时介绍过，自动化创建的原始数量为 60。

2. 刷新浏览器窗口中的“AppDefense Manager”选项卡。
3. 确认行为数量已在默认值 60 基础上有所增加，这体现了从执行登录操作过程中新学习的行为。 (注意：实际数量可能有所不同，具体取决于您的登录次数和环境中的延迟。)

4. 单击以突出显示“DB_Tier”。
5. 找到行为“sqlservr.exe”，然后单击“>”展开该行为。
查看已学习行为“sqlservr.exe”中的信息

1. 单击“CLI”旁边的“>”，展开有关该行为的更多信息。
2. 在“Inbound connection behaviors”（入站连接行为）下，单击“Multiple”（多个）旁边的“+”符号。

可以看到，登录抵押贷款应用的行为生成了新的活动。在“DB_Tier”中，“sqlservr.exe”进程是一项新发现的服务。在此处可以查看包括入站连接信息在内的详细信息。

确认 Python 服务在“Web_Tier”中

为了确保之后的功能可以正确展示，我们需要确认已学习 Web_Tier 上的 python 服务。
1. 单击“Web_Tier”服务。
2. 在已知行为列表中找到“python.exe”。

注意：如果 python.exe 未出现在 Web 层的行为列表中，请打开新的选项卡并生成发往抵押贷款应用的流量。

将范围改为保护模式

1. 单击浏览器顶部中间的“Verify and Protect” (验证并保护) 按钮。
2. 在显示的窗口中，单击“Verify and Protect” (验证并保护)。

将范围改为保护模式会更改 AppDefense 平台的行为。更改后，该平台将针对学习过程中发现的行为列表或“清单”评估运行时行为。

在下一部分中，您将了解 AppDefense 在保护应用时可以使用的多种响应例程。
安全范围响应例程

在本部分中，我们将了解 AppDefense 中提供的各种响应和修复例程，以及与 VMware NSX 平台的集成。

了解响应例程

安全范围进入“保护模式”后，您仍然可以查看和编辑与范围相关的服务。默认情况下，修复规则的唯一操作设为“Alert”（警示），实施设为“Automatically”（自动）。

1. 单击一次以确保突出显示“DB_Tier”服务。
2. 单击“Rules”（规则）选项卡。

可以看到，我们能够针对以下 4 种途径进行修复：

- 出站连接
- 入站连接
- 客户机操作系统完整性
- AppDefense 模块完整性

这些实施策略的默认设置均为“Alert”（警示）。在下一步中，您将更改其中一种行为，并了解 AppDefense 与 NSX 的集成。
更改规则行为

1. 还是在“DB_Tier”中，单击右上角的三个小点。
2. 单击“Edit Service”（编辑服务）。

更改规则行为（续）
1. 单击“Rules”（规则）。此时屏幕将显示以上视图。但请注意，您可能需要向下滚动才能查看所有这四种修复途径及其选项。

2. 在“Enforce Guest OS Integrity”（实施客户机操作系统完整性）下，单击“Alert”（警示）旁的箭头。

3. 选择“Quarantine”（隔离）。您会发现还有其他选项，例如“Suspend”（暂停）、“Power Off”（关闭）和“Snapshot”（快照）。

4. 单击“Automatically”（自动）旁的箭头，然后选择“Manually”（手动）。此操作将更改针对客户机操作系统完整性问题的默认行为，从而为使用 NSX 策略的虚拟机提供手动隔离选项。“Suspend”（暂停）、“Power Off”（关闭）和“Snapshot”（快照）等其他修复选项直接在 vSphere/vCenter 级别完成。

5. 单击“UPDATE”（更新）按钮。

更改需要两到三分钟才能更新完毕。现在，您可以在更新进行时查看与 NSX 集成后的安全标记。

查看 NSX 隔离策略

![vSphere Web Client 界面](image)

1. 在浏览器中单击“vSphere Web Client”选项卡以执行后续步骤。

注意：如果您已注销，可以使用以下用户名和密码重新登录 vSphere Web Client。如果未注销，则可以执行步骤 2 和 3。
2. 单击“Home”（主页）图标。
3. 单击“Networking & Security”（网络连接和安全性）。

**NSX 安全标记**

1. 单击“NSX Managers”（NSX Manager）。
1. Click “NSX Manager 192.168.110.42”.
2. Click “Manage” (管理) tab.
3. Click “Security Tags” (安全标记)。

This tag is automatically applied to the list during the installation process when the AppDefense device connects to NSX Manager.

Note: Depending on the resolution used, you may need to adjust the “Name” (名称) column width.
查看 NSX 安全策略

1. 单击“Home”（主页）按钮。
2. 单击“Networking & Security”（网络连接和安全性）菜单。
3. 单击“Service Composer”。

NSX 安全组
1. 单击“Security Groups”（安全组）。

2. 请注意，“AppDefense Quarantine”策略中没有虚拟机，该策略也是在安装过程中 AppDefense 设备与 NSX Manager 集成时自动构建的。

**NSX 安全策略**

1. 单击“Security Policies”（安全策略）选项卡，
2. 单击“AppDefense Quarantine Policy”（AppDefense 隔离策略）。

查看策略的防火墙规则
在显示的窗口中，“Firewall Rules”（防火墙规则）默认显示在“Guest Introspection Table”（客户机自检表）右边。您可能需要重新调整窗口大小或滚动浏览才能看到整套防火墙规则。您应该看到两条规则，分别用于阻止来自和访问策略安全组虚拟机的所有服务。

注意：根据使用的分辨率，您可能需要缩小 Chrome 浏览器窗口才能滚动浏览。

我们之前看到的“AppDefense”标记显示了安全组成员身份。

接下来，您将针对该应用执行一些脚本式攻击。
攻击应用和验证自动化响应

请注意，您已定义应用的预期状态，您将使用所提供的工具来攻击该应用并观察结果。

工作流简要概述

现在，您已经了解了 AppDefense 的安装以及与 NSX 和 vCenter 的集成。您还创建了安全范围，并向其中添加了 Web 和数据库服务。

此外，我们还修改了数据库服务的客户机完整性部分的规则，使其需要先进行手动交互，然后才能由 AppDefense 自动构建的 NSX 策略进行隔离。

在本实验室的最后一部分，我们将进行一次出站网络连接尝试，根据我们的安全范围，此操作将生成警报。然后我们将使用提供的一些脚本，模拟对内核级和主机级 AppDefense 模块的攻击。执行攻击后，我们将在 AppDefense Manager 中验证警报并执行虚拟机隔离。最后，我们将进行测试以确保数据库虚拟机已隔离。

登录数据库虚拟机

将已打开的浏览器窗口最小化至主控制台桌面。

1. 桌面上有两个远程桌面连接快捷方式，双击“DB_RDP.rdp”。

此时您将自动登录抵押贷款测试应用的数据库虚拟机。
访问数据库虚拟机

大约一分钟后，将弹出上面这两个窗口。将其关闭，然后执行下一步。

1. 单击“x”关闭这两个窗口。
可选操作（关闭窗口更新消息）

在某些情况下，您可能会看到关于 Windows Update 服务的弹出窗口出现（如上图所示）。只需单击“Close”（关闭）按钮将其关闭，然后继续操作即可。

启动 Firefox

1. 启动 Firefox。单元未连接到 Internet，我们只是模拟出站连接尝试。
2. 在 URL 目标窗口中键入以下网址，然后按 Enter 键。

www.google.com

等待系统显示“Server not found”（未找到服务器）。

3. 单击右上角窗口的“x”，关闭 Firefox。

启动 GIRogue 进程

GIRogue 是一个可用于在客户机和主机级别模拟各种攻击的进程。本实验室不包含有关此工具的详细信息和具体说明。我们已通过脚本编写了针对主机级别和客户机级别的两种不同攻击。但在执行攻击之前，我们需要先确保 GIRogue 进程正在运行。

1. 双击“Start GIRogue”（启动 GIRogue）快捷方式。
确认 **GIRogue** 正在运行。

单击该快捷方式后，将显示以下窗口。

1. 确认状态是否为“RUNNING”。完成确认后，即可执行内核级和主机级攻击。
2. 关闭命令提示符窗口。
执行操作系统完整性攻击

1. 双击桌面上的“OS Integrity Attack”（操作系统完整性攻击）快捷方式。
2. 确认结果是否为“SUCCESS”。
3. 关闭命令提示符窗口。

您可以自行选择执行上述操作 3-5 次。这样会在系统中生成更多警报。

执行 AppDefense 模块攻击

1. 双击桌面上的“AppDefense Module Attack”（AppDefense 模块攻击）快捷方式。
2. 验证结果是否为“SUCCESS”。
3. 关闭命令提示符窗口。

您可以自行选择执行上述操作 3-5 次。这样会在系统中生成更多警报。

返回 AppDefense Manager

1. 最小化 RDP 窗口

查看警报

在 HOL 环境内，虚拟机和 Manager 之间可能会有不同程度的延迟。警报可能需要 3-5 分钟才会出现。如果未看到文中所述的警报，您完全可以刷新 AppDefense 浏览器窗口。如有其他操作，您可能会在 Manager 中看到更多警报。此外，您看到的警报顺序也可能有所不同。

1. 单击“AppDefense Manager”选项卡。
2. （可选）如果您尚未打开“HOL-App”（动手实验室应用）范围菜单，请单击“HOL-App”（动手实验室应用）。

有几种方式可以进入服务或整个范围的警报页面。
3. 单击“DB_Tier”服务中的红色数字（数字可能有所不同，具体取决于用时和其他操作）。
您将会看到确认窗口（此处无图示）。单击“Go Ahead”（继续），继续访问 DB_Tier 服务警报。

查看警报（续）

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Scope</th>
<th>Service</th>
<th>Process</th>
<th>IP</th>
<th>Port</th>
<th>Description</th>
<th>Generated</th>
<th>Remediation status</th>
</tr>
</thead>
<tbody>
<tr>
<td>138</td>
<td>Critical</td>
<td>HOL-App</td>
<td>DB_Tier</td>
<td></td>
<td></td>
<td></td>
<td>Kernel Integrity Compromised</td>
<td>Jan 23, 2021</td>
<td>Action 1</td>
</tr>
<tr>
<td>136</td>
<td>Critical</td>
<td>HOL-App</td>
<td>DB_Tier</td>
<td></td>
<td></td>
<td></td>
<td>Kernel Integrity Compromised</td>
<td>Jan 23, 2021</td>
<td>Action 1</td>
</tr>
<tr>
<td>137</td>
<td>Critical</td>
<td>HOL-App</td>
<td>DB_Tier</td>
<td></td>
<td></td>
<td></td>
<td>Kernel Integrity Compromised</td>
<td>Jan 23, 2021</td>
<td>Action 1</td>
</tr>
<tr>
<td>135</td>
<td>Critical</td>
<td>HOL-App</td>
<td>DB_Tier</td>
<td></td>
<td></td>
<td></td>
<td>AppDefense Module tampering detected</td>
<td>Jan 23, 2021</td>
<td>Action 1</td>
</tr>
<tr>
<td>134</td>
<td>Critical</td>
<td>HOL-App</td>
<td>DB_Tier</td>
<td></td>
<td></td>
<td></td>
<td>AppDefense Module tampering detected</td>
<td>Jan 23, 2021</td>
<td>Action 1</td>
</tr>
</tbody>
</table>

警报的数量和顺序可能会有所不同。您应该至少会看到内核和 AppDefense 模块篡改警报。这是我们之前执行的 GiRogue 进程攻击的结果。

查看内核完整性警报的详细信息

在 HOL 环境内，虚拟机和 Manager 之间可能会有不同的延迟。警报可能需要 3-5 分钟才会出现。如果未看到文中所述的警报，您完全可以刷新 AppDefense 浏览器窗口。如有其他操作，您可能会在 Manager 中看到更多警报。上面列出了您要查找的关键警报。

1. 查看“Description”（描述）列和“Remediation status”（修复状态），找到“Kernel Integrity Compromised”（内核完整性已破坏）警报。
2. 请注意，此警报在“Remediation Status”（修复状态）列中没有已采取操作的相关信息。这是由于该操作在上一部分已从“Alert Automatically”（自动警示）更改为“Quarantine manually”（手动隔离）。主机完整性警报仍然采用其默认设置。
3. 单击“Description”（描述）列中的“Kernel integrity compromised”（内核完整性已破坏）。

隔离虚拟机

1. 注意警示提供的详细信息。
2. 单击“Quarantine”（隔离）按钮。
确认隔离

1. 再次单击“Quarantine”（隔离）以确认该操作。

返回“Alarms”（警报）页面

1. 单击后退箭头返回“Alarms”（警报）页面。
在 **AppDefense** 中验证隔离操作

在 **AppDefense** 的“Alarms”（警报）窗口中，找到我们已对其执行操作的“Kernel Integrity Compromised”（内核完整性已破坏）警报，您将在“Remediation status”（修复状态）中看到操作状态，它会从“Queued: Quarantine”（已排队：隔离）阶段开始。

几分钟后，此列将变为“Action taken: Quarantine”（已执行操作：隔离）。

（注意：您还可以刷新浏览器中的“AppDefense Manager”选项卡，这可能也需要一到两分钟才能显示。）

执行该操作后，我们要根据之前查看的 NSX 安全策略验证 db 虚拟机是否已真正隔离。
1. 单击“vSphere Web Client”选项卡。
2. 单击“Home”（主页）按钮。
3. 单击“Networking & Security”（网络连接和安全性）。

返回 vCenter
在 NSX 中验证隔离

1. 单击“Service Composer”。
2. 单击“Security Groups”（安全组）选项卡。
3. 单击“Virtual Machines”（虚拟机）下的数字“1”。

确认出现的窗口中的“Virtual Machines”（虚拟机）选项卡上显示了“db”。

4. 单击“X”关闭该窗口。
尝试访问抵押贷款应用

如果只隔离了 db 虚拟机，那么您应该仍能访问应用的 Web 层。

1. 在浏览器中打开新的选项卡，然后单击“Mortgage App”（抵押贷款应用）书签。
2. 单击“Log In”（登录）。
验证隔离

由于 db 虚拟机已隔离，web 虚拟机将不会收到任何响应。

几分钟后，Web 登录应该会超时，这证明 AppDefense 已调用 NSX 隔离策略。

注意：可能需要等待 3-4 分钟，应用才会超时并显示所看到的屏幕。

删除隔离
返回“vSphere Client”选项卡。在上一步中，我们确认了已通过 AppDefense 工作流对“db”虚拟机添加了安全标记，因此您现在应该位于“Service Composer”菜单中。

1. 单击“NSX Managers”(NSX Manager)。

删除隔离（续）

您将从虚拟机中删除安全标记，从而删除隔离策略。

1. 单击 NSX Manager 的 IP 地址。
2. 单击“Manage”(管理) 选项卡。
3. 单击“Security Tags”(安全标记) 按钮。
4. 选择“AppDefense.AnomalyFound”标记。
5. 单击分离安全标记图标。
删除隔离（续）

在显示的窗口中：

1. 在左侧列中，选择“db”虚拟机。
2. 单击窗口中间最上方的箭头，将 db 虚拟机移动到“Selected Objects”（选定对象）窗口中。
3. 单击“OK”（确定）。
重新测试应用功能

1. 返回浏览器选项卡，然后单击“Mortgage App”（抵押贷款应用）书签。
2. 单击“Log In”（登录）按钮。
重新测试应用功能（续）

如果应用返回账户详细信息屏幕，则表示您已从 NSX 平台成功删除隔离策略。在下一部分中，我们将了解应用组件在受保护的安全范围内升级时会发生什么情况。
升级应用组件

在本部分中，我们将了解如何在 AppDefense 平台中确认和处理应用组件的升级。

确认 Python 在 Web 层中

首先，我们来确认现有 Python 服务显示在 Web 层的允许行为列表中。

1. 返回“AppDefense Manager”选项卡。
2. 单击安全范围部分的“HOL-App”（动手实验室应用）。
3. 单击“Web_Tier”。
4. 滚动至 python.exe 进程，并将其展开以查看其特征。特别注意哈希值，记录哈希值的后 4 位，以备稍后使用。

注意：您可能会在此范围内看到新警报及其他警报，如果先前在实验室中实施了一些本地安全身份验证服务器服务 (lsass) Windows 进程和/或 RDP 会话，这种情况完全正常。尽管我们已尝试对应用中大部分干扰较大的进程使用通配符，但是鉴于我们在 HOL 环境中操作的时间较短，仍然可能有其他进程产生，正如先前在实验室中提到的那样，VMware 建议用 14-21 天来学习所有进程及其 CLI 变体。
在“web”虚拟机上验证 Python 进程

最小化浏览器，然后在主控制台虚拟机的桌面上找到 web 虚拟机的 RDP 快捷方式。

1. 双击 WEB-RDP.rdp 快捷方式，这样便会自动登录 web 虚拟机。

注意：当您登录该虚拟机时，可能会看到 Perl 和 STAF 窗口打开。请关闭或最小化这些窗口，因为本实验室不需要它们。

可选操作（关闭窗口更新消息）

在某些情况下，您可能会看到关于 Windows Update 服务的弹出窗口出现（如上图所示）。只需单击“Close”（关闭）按钮将其关闭，然后继续操作即可。
在“web”虚拟机上验证 Python 进程（续）

在 web 虚拟机任务栏中找到访问命令提示符的快捷方式。

1. 单击命令提示符快捷方式。
2. 在命令提示符窗口中插入或键入以下命令：
   
   ```bash
   python -V
   ```

确认版本为 3.5.2。这是 Web 服务器上当前运行的版本。

3. 最小化命令提示符窗口。
执行 Python 升级脚本

现在，您将使用提供的脚本升级 web 虚拟机中的 python 代码。

1. 双击桌面上的 upgrade_python 脚本。
2. 观察执行过程，停止 Web 服务，然后将其重新启动。窗口将在脚本运行后自动关闭。
验证升级

1. 将之前最小化的命令提示符窗口最大化（如果已关闭，则重新启动）。
2. 键入或插入以下命令:
   ```
   python -V
   ```
   现在，您可以看到 `python.exe` 的版本是 3.6.4。
3. 单击“-”符号，最小化 RDP 会话。
现在，您将通过访问抵押贷款应用网站，使用升级后的 python 进程生成新行为。

1. 打开一个新选项卡。
2. 单击“Mortgage App”（抵押贷款应用）书签。
3. 单击“Log In”（登录）按钮。

您可以多次执行这三个步骤，但这不是必需的。
1. 单击“AppDefense Manager”选项卡。
2. 单击“Alarms”（警报）。
3. 找到与 python.exe 升级场景相关的“info”（信息）警报。
4. 单击“Description”（描述）列中的“Upgrade scenario alarm”（升级场景警报）。

注意：由于一些因素，此警报可能需要 3-5 分钟才会显示。如果您发现这种情况，可以刷新 AppDefense 控制台页面或生成 Web 流量的更多实例。
在此页面中，您可以看到与 AppDefense 认为的升级场景有关的一些详细信息。图片中的箭头突出显示了观察到的进程哈希值。将此哈希值的后 4 位与您在本部分开始时记录的哈希值进行比较，会发现两者有所不同。这是我们有了一个新进程的主要标志之一，虽然它与原有进程很相似，功能也类似，但并不是同一进程。

AppDefense 在确定新进程是否属于升级场景时，会考虑几个因素。其中一些因素包括：

- 进程发布者和证书
- 进程名称和位置
- 通过与 Carbon Black 信誉服务的关系提供的信任和威胁分析
- 与之前进程迭代的行为对比

这样一来，我们就可以在应用的生命周期内减少“预期状态”安全模式可能产生的误报。

1. 单击右上角的“Allow Behavior”（允许的行为）。
将升级后的进程添加到应用

1. 在显示的窗口中，单击“Confirm”（确认）。

确认两种 Python 行为均显示在服务列表中

返回“HOL-App”（动手实验室应用）范围的“Web_Tier”部分，可以看到新的 python 行为已添加到该安全范围。
1. 单击左侧边栏中的“HOL-App”（动手实验室应用）。
2. 选择“Web_Tier”。
3. 滚动至 python.exe 进程，然后将其展开以查看这两个进程。

我们不会自动删除旧的进程列表。我们将其保留为历史记录，因为该范围中可能有其他虚拟机仍在使用旧版本以及旧哈希值。如果需要，可手动编辑范围。

注意：您的警报数量可能与屏幕截图中显示的不同。
结束语

在本单元中，您了解了创建安全范围、服务定义和修复策略的基本工作流，然后您模拟了对测试应用的攻击，并观察了 VMware AppDefense 如何使用 VMware NSX 安全策略隔离虚拟机。最后，您升级了一个应用组件，以了解 AppDefense 如何处理预期状态模式下的升级场景。

如果您想了解有关 VMware AppDefense 的更多信息，请查看我们的产品页面：
www.vmware.com/appdefense

您可以继续学习本实验室中以下任意一个单元。

(15 分钟) - 基础 - 本单元将讲解演示平台的架构。

(45 分钟) - 基础 - 本单元将讲解演示如何创建安全范围。然后，您将在应用经历各种攻击后监控应用的情况。最后，您将执行修复、隔离和升级操作。

有关 vSphere 安全功能的更多信息，请查看 HOL-1911-04-SDC - VMware vSphere 安全性 - 入门

如果您想下载此动手实验室或其他动手实验室的手册，请访问 http://docs.hol.vmware.com

如何结束实验室

1. 要结束实验室，请单击“END” (结束)
总结

感谢您参加 VMware 手动练习。请务必访问 http://hol.vmware.com/ 继续完成在线练习。

练习 SKU：HOL-1942-01-NET

版本：20200210-210356