Table of Contents

HOL-1842-01-NET - VMware AppDefense - Secure Datacenter Endpoints ...................2
Lab Guidance .............................................................................................................3
Module 1 - Overview of VMware AppDefense (15 Minutes).......................................9
  AppDefense Platform Overview ...........................................................................10
  Conclusion.............................................................................................................14
Module 2 - Exploring & Utilizing the AppDefense Platform (45 Minutes)....................15
  Logging in to the Environment & Preparing for the Lab ........................................16
  Exploring the AppDefense Manager .................................................................19
  Create an AppDefense Security Scope ...............................................................24
  Examining the AppDefense Security Scope .........................................................31
  Security Scope Response Routines .......................................................................38
  Attacking the Application & Validating the Automated Response ......................46
  Upgrading Application Components ..................................................................66
  Conclusion.............................................................................................................76
HOL-1842-01-NET - VMware AppDefense - Secure Datacenter Endpoints
Lab Guidance

Note: There are only two modules in this lab. The expected time of completion is 45-60 minutes.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

VMware AppDefense is a datacenter security tool that enables Application Control, Detection, and Response. It is meant to provide foundational elements of Cloud Workload Protection, such as System Integrity, App Control, and Memory Monitoring.

Lab Module List:

- **Module 1 - Overview of VMware AppDefense** (15 minutes) - Basic - This module will walk through the structure of the platform.
- **Module 2 - Exploring and Utilizing the AppDefense Platform** (45 minutes) - Basic - This module will walk through the creation of a security scope. Secondly, you will monitor the application after various attacks have been made. Finally, you will perform remediation, quarantine, and upgrade actions.

Lab Captains & Support:

- **Geoff Shukin, Systems Engineer, Canada**

This lab would not have been possible without the dedication of the AppDefense engineering team. Their support and assistance to make this something suitable for the VMworld HOL environment was instrumental. We would like to thank the following:

- Zhen Mo, Member of Technical Staff
- HengJun Tian, Staff Engineer
- Amit Chopra, Staff Engineer
- Alex Ma, Member of Technical Staff
- Amol Khare, Staff Engineer

This lab manual can be downloaded from the Hands-on Labs Document site found here:

http://docs.hol.vmware.com

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.

2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.

3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the EXTEND to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.
Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.
Click once in active console window

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the Shift key.

Click on the @ key

1. Click on the "@" key.

Notice the @ sign entered in the active console window.
Look at the lower right portion of the screen

Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.

**Activation Prompt or Watermark**

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.
This cosmetic issue has no effect on your lab.
Module 1- Overview of VMware AppDefense (15 Minutes)
AppDefense Platform Overview

In this section, you will read about VMware's new AppDefense security platform.

Description

AppDefense is a data center endpoint security product that embeds threat detection and response into the virtualization layer on which applications and data live. Leveraging VMware vSphere®, AppDefense delivers three key advantages over existing endpoint security solutions:

Authoritative knowledge of application intended state  When you know what’s good, you can detect what’s bad.

From inside the vSphere hypervisor, AppDefense has an authoritative understanding of how data center endpoints are meant to behave and is the first to know when changes are made. This contextual intelligence removes the guesswork involved in determining which changes are legitimate and which are real threats. AppDefense does not look at a guest workload in isolation. Instead, it manages workloads as part of broader “Security Scopes”. These scopes allow AppDefense to have a deeper understanding of complex interactive behaviour patterns in the data center as opposed to simply individual machine behaviour.

Automated, precise threat response  The right response at the right time. When a threat is detected, AppDefense can trigger vSphere and VMware NSX® to orchestrate the correct response to the threat, without the need for manual intervention. For example, AppDefense can automatically:

- Block process communication
- Snapshot an endpoint for forensic analysis
- Suspend an endpoint
- Shut down an endpoint

Isolation from the attack surface  The platform allows us to protect the protector. The first thing that most malware variants do when they reach an endpoint is disable antivirus and other agent-based endpoint security solutions. The hypervisor provides a protected location from which AppDefense can operate, ensuring that even if an endpoint is compromised, AppDefense itself is protected.
The primary components of the VMware AppDefense platform are:

**The AppDefense Manager console** is a multi-tenant cloud service provided instance to define the intended behaviour and protection rules of your applications in one place. You can monitor the enforcement of configuration, security events and alarms from here.

**The AppDefense Appliance** is an on-premises based control point for ingress and egress of data from and to the Manager. It brokers connections to the VMware management components (e.g. vCenter) and makes outbound connections to the AppDefense Manager.

**The AppDefense Guest module** deployed in the customer VM, along with supporting **AppDefense Host Modules** (in the form of VMware Installable Bundles) deployed on the ESX host. These two components work in concert to monitor and enforce the intended state of the guest behaviour as well as ensure that the protection controls are isolated in the hypervisor away from the guest "attack surface".

**vCenter** is used to gather inventory data on the customer’s site. This inventory data is used for security scope assignment, guest readiness (based on OS information) and guest to host assignment. AppDefense can also use vCenter to perform remediation actions in response to security events, such as suspending a guest.
**NSX (Optional)** is used as an additional, optional remediation channel for AppDefense. Specifically, NSX can be used to automatically or manually quarantine the machine(s) if any of the protection rules are violated.

**vRealize Automation/vRealize Orchestrator (Optional)** can be optionally used to capture application context at provisioning time from the Application blueprint.

## AppDefense Capabilities

The AppDefense platform provides:

- **Application Control** -- Comprehensive viewing and grouping of workloads in the datacenter, their intended state, and allowed behaviour
- **Run-Time Anomaly Detection & Control** -- Monitor the real time state of the OS and user application, alert and control process, network and kernel events
- **Process Analysis** -- The built-in process analysis engine gives overall process maliciousness rating as well as specific traits that are potentially suspicious
- **Orchestrated Remediation** -- Full visibility into the virtual infrastructure, as well as the guest OS and application stack provides a more effective way to orchestrate specific and relevant remediations during a security incident.

## The Separate Zone of Trust

1. Attacker compromises an app
2. AppDefense is protected from the attack surface
AppDefense's operation from within the hypervisor also provides protection and abstraction not available with traditional end-point protection platforms creating the most effective least-privilege model for the application layer.

**Protection of the Protector in a Separate "Trust Zone"**

- Full code and data protection on the VMware kernel module early during boot sequence
- Monitoring of pre-loaded drivers and code pages that are inserted by the OS prior to the module starting in the guest OS

**Kernel Level Monitoring**

- Monitor every load/unload event in the guest
- Verify signatures of loaded modules and compare code state in memory to disk state to prevent tampering
- Place a memory trace on every bit of kernel code pages for instant notification of tampering

**Memory and Process Monitoring**

- Monitor guest physical/virtual page table mapping to ensure a consistent view from both inside and outside the guest OS
- Keep a shadow copy of the guest process tables in the hypervisor to ensure guest consistency

Unlike other endpoint security products, AppDefense is isolated from the attack surface without sacrificing the context necessary to provide accurate security alerts. Furthermore, AppDefense works with NSX and other infrastructure control points to automate the response to detected threats, minimizing the potential for data exfiltration and the impact to the business.
Conclusion

Congratulations on completing Module 1 -- An overview of the VMware App Defense Platform.

Proceed to the next module:

Lab Module List:

- **Module 1 - Overview of VMware App Defense** (15 minutes) - Basic - This module will walk you through the structure of the platform.
- **Module 2 - Exploring & Utilizing the AppDefense Platform** (45 minutes) - Basic - This module will walk you through the creation of a security scope. Secondly, you will monitor the application after various attacks have been made. Finally, you will perform remediation, quarantine and upgrade actions.

How to End Your Lab

If you would like to end the lab now, you can simply click the "End" button in the upper part of your screen. Otherwise, please proceed to Module 2.
Module 2 - Exploring & Utilizing the AppDefense Platform (45 Minutes)
Logging in to the Environment & Preparing for the Lab

We will log in to both vSphere and the AppDefense Manager in preparation for the lab.

Launch Chrome from Main Console

1. Find the shortcut to Chrome on the Main Console Desktop or in the TaskBar at the bottom of the screen.

Open the vSphere Web Client

Launching Chrome should take you automatically to the vSphere Web Client login page. Use the following credentials to access the web client.

1. When prompted, **TYPE** the following credentials for user and password:

   - **User name:** administrator@vsphere.local
   - **Password:** VMware1!
2. **CLICK** Login

NOTE: If after a few minutes, your browser still does not take you to the login page, simply refresh the browser session.

**Open Tab to the AppDefense Manager**

1. **RIGHT-CLICK** on the bookmark "AppDefense Manager"
2. **CLICK** on the "Open in new tab"

This action will result in a new tab launched in Chrome to the "AppDefense Manager" VM.

3. **CLICK** On the new tab. (not shown in the visual)

**Note:** Depending on how long the Lab Environment has been waiting prior to beginning the lab, you may be taken immediately to the main AppDefense dashboard, if that is the case, you can [skip to this step](#). If you are presented with a main logon page, then proceed to the next step.
Log in to the AppDefense Portal

1. When prompted, **TYPE** the following credentials for user and password:

   - holuser@vmware.com
   - VMware1!

2. **CLICK** Sign In
Exploring the AppDefense Manager

In this section, we will walk through the AppDefense Manager and the various sections of the User Interface.

The AppDefense Manager Interface

As was mentioned in the overview module, the cloud manager is a multi-tenant service that defines the intended behaviour and protection rules of your applications in one place. In the current version, this manager runs in the public cloud as a service. This is where customers will monitor the enforcement of configuration, security events, and alarms.

After VMware establishes your account and tenant in the AppDefense Cloud Manager, you will receive an email to join the service. Once you have joined the service, you can log in and connect appliances, as well as perform other platform configurations.

For the purpose of the VMware Hands-on-Labs environment, however, this manager is running in a local instance. The user "holuser@vmware.com" has been created under its own tenant. You are currently logged in under this user's account.

In this default view, you can see Protection Coverage, Security Scopes, Alarms and Events. You will explore these in more detail as we proceed through the lab.

Note: The Provisioning Events shown are artifacts from the construction of this lab. You can disregard them.
Viewing the User Settings

On the Manager in the bottom left corner, you will see a settings icon next to the name "holuser@vmware.com".

1. **CLICK** on the **AppDefense Manager** tab (if you are not already there)
2. **CLICK** on the "setting" icon in the bottom left corner next to the username 'holuser@vmware.com'. Hint: It looks like a small gear
3. **CLICK** on Appliances

**AppDefense Appliance Menu**

The AppDefense appliance is a single, on-premises control point for ingress and egress of data to and from the AppDefense manager. It brokers connections to the VMware management components (like vCenter) and makes outbound connections to the AppDefense Cloud Manager.

The AppDefense appliance is deployed at the customer site through a standard .ovf deployment workflow. Once the appliance is deployed, the user will log into the AppDefense Cloud Manager and connect the appliance to their tenant. In addition, the appliance will be connected to various sources in the datacenter (e.g. vCenter or NSX).

1. **VALIDATE** that the appliance is active and properly connected to vCenter and NSX as depicted in the image above.

**Viewing the Inventory**

Return to the settings menu in the lower left hand corner. You will see a little gear icon next to the name "holuser@vmware.com".
1. CLICK on the setting icon
2. CLICK on Inventory

The Inventory

In this view, you can toggle between the ESXi hosts and the VMs that are available within the inventory and determine whether or not their respective modules are installed, OS versions, etc. This is accomplished by simply clicking on the "Hosts" or "VMs" tab at the top of the menu.

Remember that AppDefense is watching at the guest and host level for activity, corruption or any other anomalous behaviour.

Unassigned VMs
Return to the settings menu in the lower left hand corner. You will see a little gear icon next to the name "holuser@vmware.com".

1. **CLICK** on the "setting" icon
2. **CLICK** on Unassigned VMs

### Viewing Unassigned VMs

![Unassigned VMs screenshot]

This view shows the virtual machines in the inventory that have not been currently assigned to any security scopes. It will also show the current operational status of the host and guest modules for those particular virtual machines.

The orange and red areas represent VMs that are either in discovery mode or under protection.

### Viewing Downloads

![Downloads screenshot]

The On-Prem build of the AppDefense Manager used in this lab does not support automatic downloads, so the image on this step is from the actual production cloud based AppDefense Manager. You can see that all documentation, ova files, VIBs and guest modules are available in the management portal itself.
Create an AppDefense Security Scope

A Security Scope in AppDefense is the foundational component that establishes what the intended state and specific allowed behaviors of an application should be. In this section, you will walk through the workflow of creating a security scope against a small test application.

Creating a Security Scope

A Security Scope defines the relevant configuration elements to protect an application and its constituent workloads. These configuration elements constitute a "blueprint" or "birth certificate" for the application. It contains a description, member workloads, rules and behaviors.

This is fundamental to the AppDefense philosophy. By focusing on applications as opposed to just individual endpoints, AppDefense derives a greater contextual knowledge of the intended state of the application.

You will now create a security scope to protect the sample mortgage app running in the HOL environment.

In the AppDefense Manager tab, locate the "Scopes" section in the left hand menu.

1. CLICK the "+" sign next to Scopes to enter the Security Scope wizard.
Name the Security Scope

1. TYPE the following for the name of the Scope

HOL-App

2. CLICK the Create button

Add Services to the Security Scope

After you click create, the UI will default to that scope highlighted in the left hand menu.

1. CLICK the Add Service button in the top left-center of the UI
Create the Web Service

1. TYPE the following for the name of the service

   Web_Tier

2. CLICK the down arrow and
3. SELECT Web Server from the list. This is a pre-populated list of common services. These entries are only descriptive and not required to complete the security scope.

   In the Service Description, you can specify other information of your choosing. This is not mandatory, but can be useful in operational environments to denote additional relevant information on the service.

4. CLICK Next
Add Members to the Service

1. SELECT the check box next to the web virtual machine listed in the inventory
2. CLICK the Next button

Allowed Behaviors

AppDefense can tie into provisioning systems such as vRealize Automation or Puppet to define appropriate and allowed behaviors. It can also function in learning mode. This mode of operation allows the system to populate allowed behaviour based on a runtime view of the application over a period of time.

In this mode, the AppDefense platform will dynamically learn behaviors (e.g. ports, processes, etc.) of the targeted application. There may be some cases where you will
want to specifically define allowed behaviours. For the purposes of this lab, we will not specify any behaviors in this window.

1. CLICK **Finish**

**Create the DB Service**

You will now execute the same workflow to create the DB service for use in the application's security scope.

1. CLICK on **Add Service**
Specify DB Service Parameters

1. TYPE the following for the Service Name

   **DB_Tier**

2. CLICK on the drop-down arrow and

3. SELECT Other. Remember that this is a pre-populated list of common services. These entries are only descriptive and not required to complete the security scope.

4. (Optional) TYPE a brief description

5. CLICK **Next**
Add Members to the DB Service

1. SELECT the checkbox next to the db virtual machine listed in the inventory
2. CLICK Next

Finish the DB Service Creation

1. CLICK Finish
Examining the AppDefense Security Scope

This section continues to walk through the basic workflow of using AppDefense by modifying the security scope to change the alerting actions based on specific threat vectors.

Examine your Security Scope Settings

As we have discussed, AppDefense creates a list of allowed behaviors (e.g. ports, processes, etc.) to build a "blueprint" or "whitelist" of the intended state of the application. AppDefense can create this blueprint with assistance from provisioning interfaces such as vRealize Automation, vRealize Orchestrator, Puppet, or similar engines.

However, when the application is already deployed, AppDefense can also "learn" these behaviors. After a Security Scope is created and applied to an application, it defaults to "Learning Mode". During this time, all relevant activity is recorded as the application is functioning.

Once reviewed, this master list of intended activity can be validated and/or modified by a security operations team or application owner. After the final intended state is determined, the security scope is placed into "protected mode".
Once the scope is moved into this mode, AppDefense will use the allowed behavior list to enforce the correct security context and posture for the workload against any deviation from that list.

**DO NOT CLICK VERIFY AND PROTECT AT THIS TIME.**

- NOTE: Normally, the learning period for a workload or application is a recommended 7-14 days. Since we do not have that timeframe from within the HOL lab environment, we have automated most of the "allowed processes" into the creation of the service. If you notice, there should be roughly 60 learned behaviors.

**Explore Some of the Learned Behaviors**

1. You can see some of the available detail on any one of the Behaviors listed by expanding the "->" next to any of the services listed.
2. Once the initial expansion is made, you can expand the section next to CLI by clicking the "->" as is shown by the example in the image above.

The types of information displayed:

**Path:** This is the location where the process was launched from within the OS file structure.

**Hash:** This is a hash value on the process. This is an extra protection in case a rogue process using a trusted name were to be launched.
Trust Score and Threat Score: These two values are provided by a backend integration with a Carbon Black reputation service for Windows based services. This integration provides insight into Behaviors that are learned which may not be known by the security team. This provides extra protection against the question "What happens if my system is already compromised during the learning process?" For Linux based systems, these scores are derived by integration from various package deployment sites. In this environment, the scores here have been pre-populated for illustration. The isolated nature of the HOL environment prevents live integration based results.

Package: Metadata would be populated based on integration with orchestration platforms such as Puppet.

Outbound and Inbound Connections: These sections provide information on what ports and addresses are being listened to and communicated across.

Note: As was stated in the previous page, when operating in learning mode, the typical time recommended is between 7-14 days depending on the application. We do not have that long in this HOL environment, so we have automated some of the learning as well as wildcarded some of the process information.

In the next step, you will generate some typical traffic to observe the learning process.
Generate Learned Behaviors

1. Open a New Tab in the browser, **DO NOT CLOSE** the current ones.
2. CLICK the **Mortgage App** bookmark. This will result in the login screen to the test application.
3. CLICK **Log In**--there are no credentials required.
4. REFRESH the "Mortgage App" by holding the control key and CLICKING on the **Mortgage App bookmark** two or three times and hitting the Log In button each time to generate traffic. (This will open the app login in multiple tabs. This action is simply generating traffic of new learned Behavior. It could take 2-5 minutes for some Behaviors to populate. You can feel free to close these tabs after generating them.

Leave the Mortgage App tab open, and return to the AppDefense Manager tab.
1. CLICK and return to the AppDefense Manager tab.

There will be some delay in the environment between the time the Mortgage App is accessed and the additional Behaviors show up in the AppDefense manager console. This should only be a few minutes. The important element here is to see the number of learned Behaviors increment from the original 60 that were created by our automation that was described when we created the security scope.

2. REFRESH the browser window on the AppDefense Manager tab.
3. VERIFY the number of Behaviors has increased from the default 60 to reflect the newly learned Behavior from executing the login operation. (NOTE: Your numbers may be different based upon the number of times you logged in and the delay in the environment)
4. CLICK to highlight the DB_Tier
5. LOCATE the Behavior "sqlservr.exe" and CLICK on the "->" to expand that behavior.
View the Information in the Learned Behavior "sqlservr.exe"

1. CLICK the ">" next CLI to expand more information about the Behavior
2. CLICK the "+" sign next to the word Multiple under Inbound Connection Behaviors

As you can see, the act of logging into the Mortgage application generated new activity. On the DB_Tier, one of the new services discovered was the sqlservr.exe process. The details including inbound connection information can be viewed here.

Verify that Python Service is in the Web_Tier
To insure that a later capability is demonstrated correctly, we need to verify that the python service on the Web_Tier has been learned.

1. CLICK on the Web_Tier Service.
2. Locate "python.exe" in the list of known Behaviors.

Note: If the python.exe does not show up in the Web Tier list of Behaviors, open up new tabs and generate traffic to the Mortgage App.

**Move Scope to Protect Mode**

1. CLICK the **Verify and Protect** button at the top center of the browser
2. In the resulting window, CLICK **Verify and Protect**

Putting the Scope into Protect mode changes the Behavior of the AppDefense platform. The platform will now evaluate runtime behaviors against the list or "manifest" of Behaviors that was discovered during the learning process.

In the next section, you will examine the various response routines that AppDefense can use when protecting applications.
Security Scope Response Routines

In this section, we will explore the various response and remediation routines that are available in AppDefense as well as the integration with VMware's NSX platform.

Explore Response Routines

Once the Security Scope is in "Protect Mode", you can still review and edit services associated with the scope. By default, the only actions for the Remediation Rules are set to "Alert" and the enforcement is "Automatically".

1. CLICK once to make sure the DB_Tier service is highlighted
2. CLICK on the Rules tab

As you can see, there are 4 vectors that we can remediate against:

- Outbound Connections
- Inbound Connections
- Guest OS Integrity
- AppDefense Module Integrity

The default setting for these enforcement policies is set to Alert. In the next step, you will change one of those behaviours and we will examine the AppDefense integration with NSX.
Change Rule Behavior

1. While still on the DB_Tier, CLICK the three little dots in the upper right hand corner
2. CLICK Edit Service

Change Rule Behavior (cont.)
1. **CLICK Rules**

The screen will launch with the view above. However, you may need to scroll down some to see all four of the remediation vectors and their options.

2. Under Enforce Guest OS Integrity, CLICK the arrow next to Alert.
3. SELECT **Quarantine**. You will notice there are other choices such as Suspend, Power Off and Snapshot.
4. CLICK the arrow next to Automatically, and SELECT **Manually**

This will change the default behavior for Guest OS integrity issues to provide a manual quarantine option for the VM using an NSX policy. The other remediation actions (e.g. Suspend, Power Off, & Snapshot) are done directly at the vSphere/vCenter level.

5. CLICK the "UPDATE" button.

It will take two to three minutes for the change to be completely updated. Now, you will look at the NSX integration with security tags while the update is occurring.

**Examine the NSX Quarantine Policy**

1. CLICK on the **vSphere Web Client Tab** on your browser to perform the next steps.
Note: If you have been logged out, you can log back into the vSphere Web Client with the following username and password. If not, you can proceed to Step 2 and 3.

administrator@vsphere.local
VMware1!

2. CLICK on the Home icon
3. CLICK on Networking & Security

NSX Security Tags

1. CLICK on NSX Managers
1. CLICK on the **NSX Manager 192.168.110.42**
2. CLICK on the **Manage** Tab
3. CLICK on **Security Tags**
4. LOCATE the Security Tag "**AppDefense.AnomalyFound**"

This tag is automatically applied to the list when the AppDefense Appliance is connected to the NSX Manager during installation.

**NOTE:** Depending on resolution, you may need to re-size the Name column width.
Examine NSX Security Policy

1. CLICK the **Home Button**
2. CLICK **Networking & Security** Menu
3. CLICK **Service Composer**

### NSX Security Groups

- Security Groups
  - Synchronization Status:
    - There are no synchronization errors or warnings.
  - Firewall Publish Status:
    - Last publish operation succeeded 1/22/20
1. CLICK on Security Groups.

2. NOTICE that there are no VMs in the "AppDefense Quarantine" Policy--This policy was also automatically built when the AppDefense Appliance was integrated with the NSX manager during installation.

NSX Security Policy

[Image of NSX Security Policy interface]

1. CLICK on the Security Policies Tab
2. CLICK on AppDefense Quarantine Policy

Examine Firewall Rules for the Policy

[Image of Firewall Rules interface]

In the resulting window, the default location of the Firewall Rules are right of the Guest Introspection Table. You may need to resize the window or navigate over to see the
entire set of Firewall Rules. Once there, you should see two rules that block all services from and to the Policy Security Group VMs.

Note: Depending on your resolution, you may need to zoom out on the Chrome browser window to be able to scroll over.

The Security Group membership is based on the presence of the "AppDefense" tag that we saw earlier.

Next, you will perform some scripted attacks against the application.
Attacking the Application & Validating the Automated Response

Now that you have defined what the intended state of your application should be, you will use tools provided to attack the application and observe the results.

Brief Workflow Overview

At this point, you have reviewed the installation of AppDefense and its integration with NSX and vCenter. You have created a security scope and added the web and db services to it.

In addition, we have modified rules of the Guest Integrity section of the DB service so that it would require a manual interaction prior to being quarantined by an NSX policy that was automatically built by AppDefense.

In this final section of the lab, we will generate an outbound network connection attempt which will generate an alarm against our security scope. Then we will be using some provided scripts to simulate attacks on the kernel and host level AppDefense modules. Once the attacks are executed, we will validate the alarms in AppDefense Manager and perform a quarantine of the VM. Finally, we will test to ensure the DB VM is isolated.

Log on to the DB VM

Minimize the browser window you have open to return to the Main Console desktop.

1. On the Desktop, there are two remote desktop connection shortcuts. Double-click on `DB_RDP.rdp`
This will automatically log you into the DB VM of the Mortgage Test application

**Accessing the DB virtual machine**

![Image of virtual machine with buttons highlighted]

After a minute or so, these two windows will pop-up. You close them and proceed to the next step.

1. CLICK on the "x" to close these two windows.
Optional (Dismiss Windows Update Messages)

You may at some point see a pop-up window appear regarding Windows Update Service like the visual above. Simply dismiss by clicking on the "Close" button and proceed.

Launch Firefox
1. **LAUNCH Firefox.** The pod is not connected to the Internet, we are just simulating an outbound connection attempt.

2. **TYPE** the following in the URL destination window and press enter.

   ```
   www.google.com
   ```

   Wait until you see "Server not found."

3. **CLOSE Firefox** by clicking on the "x" in the upper right hand window

### Start the GIRogue Process

GIRogue is a process that can be used to simulate different attacks at both the Guest and Host level. The details and specifics of this tool are beyond the scope of this lab. We have scripted two different attacks against the Host and Guest level. However, before we can execute the attacks, we need to ensure that the GIRogue process is running.

1. **DOUBLE CLICK** on the **Start GIRogue** shortcut.
Validate GI Rogue is running

Once you have clicked the shortcut, the resulting window will appear.

1. **Verify that the State is "RUNNING"**. Once you have validated this, proceed to the executing the Kernel and Host level attacks.
2. **CLOSE the CMD window**
Execute the OS Integrity Attack

1. DOUBLE-CLICK on the **OS Integrity Attack** shortcut on the Desktop
2. VERIFY the Result was **SUCCESS**
3. CLOSE the **CMD** window

You can feel free to execute this 3-5 times. This will generate more alarms in the system.

Execute the AppDefense Module Attack
1. DOUBLE-CLICK on the **AppDefense Module Attack** shortcut on the Desktop  
2. VERIFY the Result was **SUCCESS**  
3. CLOSE the **CMD** window

You can feel free to execute this 3-5 times. This will generate more alarms in the system.

**Return to the AppDefense Manager**

![Image of AppDefense Manager tab]

1. Minimize the **RDP Window**

**Check Alarms**

![Image of AppDefense Manager window with Alarms]

Within the HOL environment, there may be varying degrees of delay between the VMs and the Manager. It may take 3-5 minutes for the alarms to show up. Refreshing the AppDefense browser window is perfectly acceptable until you see the alarms depicted. Depending on other actions, you may see more alarms in the manager. You may also see alarms in a different order.

1. CLICK on the **AppDefense Manager** tab
2. (Optional) If you are not already on the HOL-App Scopes menu, the CLICK on the HOL-App.

There are several ways to get to the alarms page for a service, or complete scope.

3. CLICK on the red number in the DB_Tier Service (your number may be different depending on timing and other actions).

You will get a confirmation window (not pictured here). CLICK on "Go Ahead" to proceed to the DB_Tier service alarms.

Check Alarms (cont.)

The number and order of your alarms may vary. You should see at a minimum both kernel and AppDefense Module Tampering alarms. These are the result of the GIRogue process attacks we executed previously.

Examine Kernel Integrity Alarm Detail

Within the HOL environment, there may be varying degrees of delay between the VMs and the Manager. It may take 3-5 minutes for the alarms to show up. Refreshing the
AppDefense browser window is perfectly acceptable until you see the alarms depicted. Depending on other actions, you may see more alarms in the manager. The key alarms you are looking for are listed above.

1. **Examine the Description column** "Remediation status" and locate a "Kernel Integrity Compromised" alarm.
2. Notice how this alarm does not have anything in terms of an action taken in the Remediation Status column. This is due to the fact that the action was changed from "Alert Automatically" to "Quarantine manually" in previous section. The Host Integrity alarm is still at its default setting.
3. CLICK on the **Kernel integrity compromised** in the Description column

**Quarantine the VM**

![Quarantine VM Dialogue Box]

1. NOTICE the detail provided by the alert
2. CLICK the **Quarantine** button
Confirm the Quarantine

1. CLICK Quarantine again to confirm the action.

Go Back to Alarms

1. CLICK on the Back Arrow to return to Alarms
Verify Quarantine Action in AppDefense

In the AppDefense Alarms window, find the **Kernel Integrity Compromised** alarm that we acted upon. You will see in the "Remediation Action" a status of the action. It will start in the **Queued: Quarantine** phase.

After a few minutes, the column should change to **Action taken: Quarantine**.

(Note: you can also refresh the AppDefense manager tab in the browser--it still may take a minute or two to show up)

Once that action has been taken, we will verify that the DB virtual machine is indeed isolated based on the NSX security policy we examined earlier.
Return to vCenter

1. CLICK on the **vSphere Web Client tab**
2. CLICK on the **Home Button**
3. CLICK on **Networking & Security**
Verify the Quarantine in NSX

1. CLICK on Service Composer
2. CLICK on Security Groups Tab
3. CLICK on the number "1" under the Virtual Machines

VERIFY the "db" is present on the Virtual Machines tab in the resulting window

4. CLICK the X to close the window
Attempt to Access the Mortgage App

Given that only the db virtual machine is isolated, you should be able to still access the web tier of the application.

1. Open a new tab in the browser and CLICK on the Mortgage App bookmark
2. CLICK Log In
Validate the Quarantine

Since the DB virtual machine is isolated, the web virtual machine will not receive any response.

After a few minutes the web login should time out proving that AppDefense has invoked an NSX Quarantine policy.

NOTE: The application could take as long as 3-4 minutes prior to timing out and displaying the screen you see.
Remove Quarantine

Return to the vSphere Client Tab. You should be on the Service Composer Menu from the previous step when we verified the security tag was added to the "db" VM through the AppDefense workflow.

1. CLICK on **NSX Managers**
You will remove the Security Tag from the VM and thus remove the quarantine policy.

1. CLICK on the **IP Address** of the NSX Manager
2. CLICK on the **Manage** tab
3. CLICK on the **Security Tags** button
4. SELECT the **AppDefense.AnomalyFound** Tag
5. CLICK on the "**Detach Security Tag Icon**"
Remove Quarantine (cont.)

In the resulting window:

1. SELECT the db VM in the Left-Hand Column
2. CLICK the **top arrow in the middle of the window** to move the db VM to the "Selected Object Window"
3. CLICK OK
Re-Test the Application Function

1. RETURN to a browser tab and CLICK on the "Mortgage App" bookmark
2. CLICK on the Log In button
Re-Test the Application Function (cont.)

If the application returns the account detail screen, then you have successfully removed the quarantine policy from the NSX platform. In the next section, we will examine what happens when application components are upgraded when in a protected Security Scope.
Upgrading Application Components

In this section, we will examine how upgrades of application components are identified and processed with the AppDefense platform.

Verify Python in the Web Tier

First, let’s verify that we see the existing Python service in the Web Tier's list of allowed behaviors.

1. Return to the AppDefense Manager tab
2. CLICK on HOL-App in the Security Scopes section
3. Click on the Web_Tier
4. SCROLL and expand the python.exe process to see it's characteristics. Pay special attention to the hash value. Make a note of the last 4 digits of the hash value for later.

NOTE: You may see new and other alarms in the scope. This is perfectly normal with some of the lsass windows processes and/or RDP sessions that were conducted earlier in the lab. While we attempted to wildcard most of the noisier processes in the application, there are still others that will spawn given the short time frame we are dealing with in the HOL environments. As was mentioned earlier in the lab, VMware recommends 14-21 days to learn all processes and their CLI variants.
Verify Python Process on the "web" VM

Minimize the browser and locate the RDP short-cut to the Web VM on the desktop of the Main Console VM.

1. DOUBLE-CLICK the WEB-RDP.rdp shortcut. This will auto-login to the web VM.

NOTE: When you log in to the VM, you may see a perl and STAF window launch. Just close or minimize these windows as they are not needed for the lab.

Optional (Dismiss Windows Update Messages)

You may at some point see a pop-up window appear regarding Windows Update Service like the visual above. Simply dismiss by clicking on the "Close" button. and proceed.
Verify Python Process on the "web" VM (cont.)

Locate the shortcut to the CMD prompt on the web VM taskbar.

1. CLICK on the CMD shortcut
2. INSERT or TYPE the following command into the cmd window

```
python -V
```

Verify that the version is 3.5.2. This is the current running version on the web server.

3. MINIMIZE the **CMD** Window
You will now upgrade the python code on the web vm using a script provided.

1. DOUBLE-CLICK on the upgrade_python script on the desktop
2. OBSERVE the execution stop the web service and then restart it. The window will auto close after the script runs.
Verify the Upgrade

1. MAXIMIZE the CMD prompt (or re-launch it if you closed it) that you previously had minimized.
2. TYPE or INSERT the following command:

```
python -V
```

You can now see that the version of python.exe is 3.6.4.

3. MINIMIZE the RDP Session by CLICKING on the "_" symbol
Return to the Chrome Browser

Now you will generate new behaviour using the upgraded python process by visiting our Mortgage App website.

1. OPEN a **New Tab**
2. CLICK on the **Mortgage App bookmark**
3. CLICK on the **Log In** button

You may want to perform these three steps a couple of times, but it is not required.
1. **CLICK** on the AppDefense Manager Tab
2. **CLICK** on Alarms
3. **LOCATE** an "info" alarm that is related to an upgrade scenario for python.exe
4. **CLICK** on the "Upgrade scenario alarm" in the Description column

NOTE: Depending on some factors, it could take as long as 3-5 minutes before this alarm shows. If you find that to be the case, you can refresh the AppDefense console page and/or generate more instances of the web traffic.
In this page, you can see some of the details associated with what AppDefense believes to be an upgrade scenario. The arrow in the graphic highlights the process hash that was observed. Compare the last 4 digits of this hash to the one you noted at the beginning of this section and you will that they are different. This is one of the key indicators that we have a new process albeit similar and performing similar functionality.

When AppDefense is determining whether a new process is an upgrade scenario, we look at several factors. Some of these factors are:

- Process Publisher and Certificate
- Process Name and Location
- Trust and Threat Analysis provided through relationship with Carbon Black reputation service
- Behaviour comparison to previous process iteration
This allows us to reduce potential false positives of an "intended state" security model through the lifecycle of the application.

1. CLICK **Allow Behavior** in the upper right-hand corner

**Add Upgraded Process to the Application**

![Confirm Allow Behavior dialog box]

1. CLICK **Confirm** in the Resulting Window
Verify both Python Behaviours are Present in the Service List

Return to the Web_Tier of the HOL-App Scope and see the new python behaviour added to the Security Scope.

1. CLICK on HOL-App in the left-hand sidebar
2. SELECT the Web_Tier
3. SCROLL and then EXPAND the python.exe processes to see both.

We do not automatically remove the old process list. We keep it for history and because there could be other VMs in the scope that still are using the older version with the older hash. The scope can be manually edited if needed.

NOTE: Your alarm numbers may vary than what is shown on the screen shot.
Conclusion

In this module, you went through the basic workflow of creating security scopes, service definitions and remediation policies. You then simulated an attack on a test application and observed VMware AppDefense quarantine the virtual machine using VMware NSX security policies. Finally, you upgraded a application component to see how AppDefense deals with upgrade scenarios in an intended state model.

If you would like more information on VMware's AppDefense, please check out our products page at: www.vmware.com/appdefense

You can proceed to any module in the lab below.

**Module 1 - Overview of VMware App Defense** (15 minutes) - Basic - This module will walk you through the structure of the platform.

**Module 2- Exploring and Using the AppDefense Platform** (45 minutes) - Basic - This module will walk you through the creation of a security scope. Secondly, you will monitor the application after various attacks have been made. Finally, you will perform remediation, quarantine, and upgrade actions.

For more information on vSphere Security features, please check out the **HOL-1811-01-SDC - vSphere v6.5 - What's New?**

If you want to download the manual for this or any other Hands on Lab, please visit http://docs.hol.vmware.com

**How to End your Lab**

1. To end your lab, Click the END
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1842-01-NET

Version: 20180408-193059