vSphere8 Automated Scripts White Paper

Date: May 2, 2025

Title: **Utilizing bash and powershell scripting to automate the vSphere suite of STIG checklists**

Products (STIGs) affected:

- VMware vSphere 8.0 ESXi Security Technical Implementation Guide
- VMware vSphere 8.0 Virtual Machine Security Technical Implementation
- VMware vSphere 8.0 VAMI Security Technical Implementation Guide
- VMware vSphere 8.0 vCenter Appliance ESX Agent Manager (EAM) Security Technical Implementation Guide
- VMware vSphere 8.0 vCenter Appliance Envoy Security Technical Implementation Guide
- VMware vSphere 8.0 vCenter Appliance Lookup Service Security Technical Implementation Guide
- VMware vSphere 8.0 vCenter Appliance Perfcharts Security Technical Implementation Guide
- VMware vSphere 8.0 vCenter Appliance Photon OS 4.0 Security Technical Implementation Guide
- VMware vSphere 8.0 vCenter Appliance PostgreSQL Security Technical Implementation Guide
- VMware vSphere 8.0 vCenter Appliance Secure Token Service (STS) Security Technical Implementation Guide
- VMware vSphere 8.0 vCenter Appliance User Interface (UI) Security Technical Implementation Guide
- VMware vSphere 8.0 vCenter Appliance Management Interface (VAMI) Security Technical Implementation Guide
- VMware vSphere 8.0 Virtual Machine Security Technical Implementation Guide

Products Created:

- esxi8.ps1
- VMs8.ps1
- vSphere8.sh

Summary:

This executive summary provides an overview of the workflow improvements these developed scripts will have for the Unix team as well as a brief introduction to how these scripts function. The scripts were created to address inefficiencies caused by manually checking each check, creating consistency between reviewers and providing the ability to inspect a larger scope of a site's virtual infrastructure, thus providing a better auditing product.

The challenge with the vSphere checklists published by DISA is volume and scalability in enterprise environments. Across the standard checklist there are approximately four-hundred and eighty-six checks that need to be performed across three different node types. However, this approximation assumes only checking one vCenter, one ESXi host and one individual virtual machine for the entirety of said checklist. To provide context, in enterprise environments it's not uncommon to see clustering allowing for multiple vCenter managers; enterprise sites should always have multiple ESXi hosts running which could then range from a handful of ESXi hosts to potentially hundreds. Lastly it's not uncommon to see over one hundred plus virtual machines deployed at any given site per ESXi host. The end result means that any given site could potentially have thousands of manual checks required for this one technology for this individual enclave (ie. NIPR/SIPR). It goes without saying, that performing a large amount of manual checks can sometimes lead to mistakes being made, interpretations differing between reviews and a shortage of time leading to less infrastructure being reviewed.

This leads to the development of three scripts each deployed per node type. These scripts were written utilizing the same vSphere checklists in order to provide the same results as if they were done manually. These scripts' primary function is to take the work out of manually typing the conditional check onto the interrogated node; then check the desired state based on that same check against the desired output to provide a result. In simpler terms, the script runs the command defined in the individual check to determine compliance and then takes the desired output from that same check; it then compares the result and provides a finding. Output is then printed on the screen indicating whether the desired output matches that of the checklist. Notifications are provided letting both the site and reviewer know which output pertains to which check and if any additional information is needed before providing an evaluation.

This process is done for approximately ninety-five percent of the total combined checklist checks and is broken up to fit the goals of the reviewer. So, if a reviewer needed to review a single vCenter appliance, three ESXi hosts and twenty virtual machines they would have the capability to do so in an efficient manner under reasonable time constraints. This process dramatically reduces the time needed to conduct the reviews, it provides consistency in the way in which we operate and ensures less mistakes are made when reviewing desired output states.

For a more technical overview of how these scripts operate, there will be provided technical documentation that will describe these processes in more detail.