SERVICE DESCRIPTION

SpiderLabs: Virtualization Technology Assessments

Service Description

Virtualization is a software implementation of a machine (computer) that executes programs like a real machine.

Virtualization can be performed across server and desktop environments. Common examples include VMware ESX, vSphere, Hyper-V, Citrix, Solaris Zones, HPUX Virtualization, and AIX LPARs.

What is Virtualization Testing?

Virtualization has recently become one of the most rapidly and widely deployed IT initiatives, used by small businesses, and large corporate or Government departments alike.

Scope and Project Phases

This security test actively validates the adherence to security policy and lists specific remediation items for each problem identified. The test is typically conducted as outlined in the Overview section (see next page) but is tailored to specific requirements.

Virtualization software (such as VMWare ESX) is a powerful tool for developers and system administrators. It allows one physical machine to run two or more operating systems simultaneously. Advanced virtualized environments include the ability to designate multiple virtual machines as a team, which administrators can then power on and off, suspend, and resume as a single object, making it particularly useful for testing client-server environments.

While they provide many improvements for system administrators, virtualization management layers represent a new type of privileged software that can be attacked, potentially granting a high level of access to the attacker.

Overview

We will perform a review of the virtualized environment and the management of that environment for problems including:

- Network topology: a virtual server should not form or contain a boundary between IT services at different levels of privilege or those that handle data with different protective markings.
- Secure management of the environment and hypervisor.
- Operating system patch level.
- Running services.
- Third-party software patch levels.
- User authentication and authorization for management – use of encryption.
- Service binary permissions.
- User account and security policy checks.
- Network shares and permissions.
- Routing table and available network interfaces.
- Network accessible services.
- Logging.
- Vulnerabilities in the hypervisor platform and base operating system.

Deliverables and Outputs

Following the conclusion of the engagement, findings will be made available via the Trustwave SpiderLabs PenTest Manager. The deliverables will be both strategic and tactical in nature, presented in a drill down format that will be highly accessible to both management and operational staff. Each finding will have a risk scoring associated with it as well as contain detailed technical information pertaining to the nature of the finding. Each finding will also be presented with clear guidance on how to remediate the issue.