Sicherheits-Analyse von Virtualisierungs-Lösungen

Studiengang: Informatik | Vertiefung: IT-Security
Betreuer: Prof. Hansjürg Wenger
Experte: Prof. Dr. Torsten Braun (Universität Bern, Institut für Informatik)

Virtuelle Systeme haben in den letzten Jahren einen gewaltigen Aufschwung erlebt und sind in vielen Unternehmen nicht mehr wegzudenken. Diese Umgebungen beinhalten meist alle, für das produktive Tagesgeschäft, erforderlichen virtuellen Server, weshalb die Sicherheit der kompletten Umgebung von grosser Bedeutung ist. Die Resultate der Arbeit zeigen, dass diverse Angriffsvektoren in zentralen Mechanismen und Features existieren, wodurch grosser Schaden angerichtet werden kann.

Zielsetzung

Das Ziel dieser Arbeit war die virtuellen Serversysteme von KVM, Microsoft und VMware genauer zu analysieren und auf Schwachstellen zu prüfen. Besonderes Augenmerk erhielten hierbei die Verwaltungstools, die Migrationstechnologie, sowie die Netzwerk- und Storage-Infrastruktur, da diese das Rückgrat einer virtuellen Umgebung bilden. Aufgrund der aus der Analyse gewonnen Erkenntnisse wurden Best-Practice Lösungen ausgearbeitet.

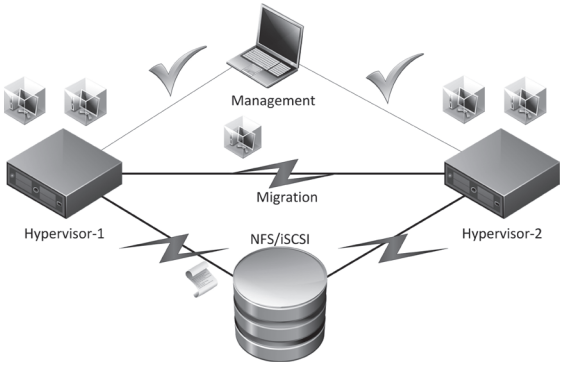
Recherche/Analyse

Alle drei Systeme verfügen über eine Vielzahl an Features, welche den Ansprüchen der meisten Unternehmen genügen. Die Verwaltungstools arbeiten mit aktuellen Verschlüsselungen, weshalb in diesem Bereich keine grossen Sicherheitslücken entdeckt werden konnten. Anders im Storage- sowie Migrationsbereich, in denen keine Verschlüsselung eingesetzt wird, wodurch eine Vielzahl von möglichen Angriffen existiert. Dadurch ist es möglich, alle Daten welche sich im Arbeitsspeicher befinden, während einer Migration auszulesen, oder zu verändern. Die selben Lücken konnten bei der Storage-Migration und im Storage-Netzwerk aufgedeckt werden. Die Manipulationen werden jedoch direkt auf der Festplatte durchgeführt, wodurch diese ebenfalls einen Neustart überleben. Durch den Austausch des gehashten Passwortes, ist es einem Angreifer möglich, sich Zugang zu jeder beliebigen virtuellen Maschine (VM) zu verschaffen. Ein tieferes Verständnis der eingesetzten Protokolle erlaubt theoretisch das Manipulieren der kompletten VM. Denkbar ist deshalb ebenfalls, das Einschleusen von Schadsoftware während einer Migration oder dem Starten des Systems.

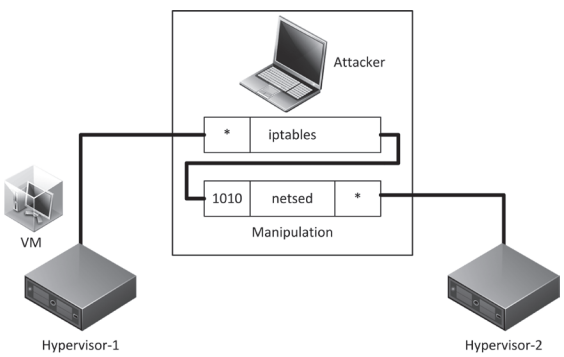
Sicherheitsempfehlungen

Die Recherchen haben gezeigt, dass alle drei Hersteller durchaus «Best Practice»-Empfehlungen anbieten. Diese beziehen sich jedoch hauptsächlich auf Performanceoptimierungen und nur in seltenen Fällen auf die Sicherheit des Systems. Zum Schutz der aufgedeckten Attacken wurde für jede Umgebung die «Best Practice»-Empfehlung des Herstellers mit Sicherheitsoptimierungen erweitert. Die evaluierten Empfehlungen eliminieren die aufgedeckten Lücken und können auf virtuelle Umgebungen angewendet werden. Durch das in dieser Arbeit aufgebaute Wissen ist es ebenfalls möglich, Sicherheitslösungen, welche die jeweilige Komplexität der geplanten Infrastruktur und die Ansprüche des Unternehmens berücksichtigen, entsprechend zu evaluieren und realisieren.

Michael Schwab
m.schwab555@gmail.com



Veranschaulichung der Sicherheitsanalysen



Schema Migrations-Angriff