Detection Strategy for Virtual Machine Discovery, Detection Strategy DET0199

Archived: 2026-04-05 18:42:36 UTC

AN0572

Monitor for execution of hypervisor management commands such as `esxcli vm process list` or `vim-cmd vmsvc/getallvms` that enumerate virtual machines. Defenders observe unexpected users issuing VM listing commands outside normal administrative workflows.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	esxi:shell	command IN ("esxcli vm process list", "vim-cmd vmsvc/getallvms")

Mutable Elements

Field	Description
ExpectedAdminUsers	List of known administrators authorized to run ESXi enumeration commands.
UnexpectedCommandPaths	Defines restricted paths or contexts where VM enumeration should not occur.

AN0573

Detects attempts to enumerate VMs via hypervisor tools like `virsh`, `VBoxManage`, or `qemu-img`. Defender correlates suspicious command invocations with parent process lineage and unexpected users.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	auditd:SYSCALL	execve: process_name IN ("virsh", "VBoxManage", "qemu-img") AND command IN ("list", "info")

Mutable Elements

Field	Description
NonRootAccounts	Monitor non-root users invoking hypervisor management utilities.
KnownAdminScripts	Whitelist of scripts expected to run VM enumeration as part of routine operations.

AN0574

Detects enumeration of VMs using PowerShell (`Get-VM`), VMware Workstation (`vmrun.exe`), or Hyper-V (`VBoxManage.exe`). Defender observes suspicious command lines executed by unexpected users or outside normal administrative sessions.

Log Sources

Mutable Elements

Field	Description
ExpectedAdminAccounts	Defines which accounts are authorized to execute VM discovery commands.
RoutineScripts	Whitelist of approved administrative scripts that legitimately invoke VM enumeration.

AN0575

Detects VM enumeration attempts using virtualization utilities such as VirtualBox (`VBoxManage`) or Parallels CLI. Defender observes abnormal invocation of VM listing commands correlated with non-admin users or unusual parent processes.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	process_name IN ("VBoxManage", "prlctl") AND command CONTAINS ("list", "show")

Mutable Elements

Field	Description
UserContext	Adjust sensitivity depending on whether the command is executed by admin or non-admin users.
ExecutionTimeWindow	Restrict alerts to unusual times when VM management is not expected.

Source: https://attack.mitre.org/detectionstrategies/DET0199