Exploitation of Remote Services – multi-platform lateral movement detection, Detection Strategy DET0118

Archived: 2026-04-05 16:47:07 UTC

AN0327

Correlates inbound network access to remote service ports (e.g., SMB/RPC 445/135, RDP 3389, WinRM 5985/5986) with near-time instability in the target service (crash, abnormal restart), suspicious child process creation under the service, and post-access lateral-movement behaviors. The chain indicates likely exploitation rather than normal administration.

Log Sources

Mutable Elements

Field	Description
ServicePortSet	List of monitored service ports (default: 445,135,3389,5985,5986,1433,3306).
TimeWindow	Correlation window between inbound access and crash/child-process (default: 10 minutes).
AllowedAdminCIDRs	Known management networks to suppress benign admin traffic.
MinConnErrorRate	Percent of failed/aborted connections to treat as anomalous (default: 30%).

AN0328

Links inbound network access to SSHD/SMB/NFS/Databases or custom daemons with subsequent daemon crash/restart, core dump, or spawning of shells/reverse shells from the service context, indicating remote exploitation.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	linux:syslog	kernel|systemd messages indicating 'segmentation fault'|'core dumped'|'service terminated unexpectedly' for sshd, smbd, vsftpd, mysqld, httpd, etc.

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve of /bin/sh,/bin/bash,/usr/bin/curl,/usr/bin/python by service accounts (e.g., apache, mysql, nobody) immediately after inbound network activity.
Network Traffic Content (DC0085)	NSM:Flow	Inbound connections to monitored service ports from external or unusual internal sources; rapid follow-on lateral connections from the same host.

Mutable Elements

Field	Description
ServiceNames	Linux daemons to watch (sshd, smbd, nfsd, httpd/nginx, mysqld, postgres, redis).
CoreDumpPaths	Paths indicating crash artifacts (/var/crash, /var/lib/systemd/coredump).
ShellSpawnAllowlist	Paths/users allowed to spawn shells from services (default: empty).
TimeWindow	Correlation window (default 10m).

AN0329

Detects exploitation targeting ESXi/vCenter by correlating attempts to reach known exploitable endpoints (OpenSLP 427, CIM 5989, Hostd/Vpxa HTTPS 443, ESXi SOAP) with vmkernel/hostd crashes, unexpected hostd/vpxa restarts, or new reverse/outbound connections from ESXi host/vCenter to internal assets.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	esxi:hostd	Keywords: 'Backtrace','Signal 11','PANIC','hostd restarted','assert' or 'Service terminated unexpectedly' in /var/log/hostd.log, /var/log/vmkernel.log, /var/log/syslog.log.
Network Traffic Content (DC0085)	NSM:Flow	Inbound to tcp/427 (OpenSLP), tcp/443 (vSphere APIs), tcp/902, tcp/5989 followed by new unexpected outbound sessions from the ESXi/vCenter host.

Mutable Elements

Field	Description
ESXiServicePorts	427, 443, 902, 5989; modify per version/hardening.
MgmtCIDRs	Legit management networks for vCenter/ESXi.
RestartKeywords	Crash/restart patterns to match in logs.

AN0330

Ties inbound access to exposed services (ARD/VNC 5900, SSH 22, ScreenSharing, web services) with process crashes in unified logs and abnormal child processes spawned under those services (e.g., bash, curl) to indicate exploitation.

Log Sources

Mutable Elements

Field	Description
ServicePortSet	22, 5900, 8080/8443 by default.
AllowedAdmins	MDM/jump-host IPs allowed to manage endpoints.
TimeWindow	Default: 10 minutes.

Source: https://attack.mitre.org/detectionstrategies/DET0118#AN0327