

# Recursive Enumeration of Files and Directories Across Privilege Contexts, Detection Strategy DET0370

Archived: 2026-04-05 15:01:26 UTC

## AN1040

Execution of file enumeration commands (e.g., 'dir', 'tree') from non-standard processes or unusual user contexts, followed by recursive directory traversal or access to sensitive locations.

### Log Sources

### Mutable Elements

Field	Description
CommandLineRegex	Allows tuning based on tools/scripts used for enumeration (e.g., tree, dir /s /b)
UserContext	Scoping for standard vs elevated or service accounts
TimeWindow	Defines burst activity over short periods (e.g., >50 directory queries in 30s)

## AN1041

Use of file enumeration commands (e.g., 'ls', 'find', 'locate') executed by suspicious users or scripts accessing broad file hierarchies or restricted directories.

### Log Sources

### Mutable Elements

Field	Description
FilePathDepth	Max depth of recursive access to tune noise vs anomaly
UserContext	Helpful to exclude known scripts or automation accounts

## AN1042

Execution of file or directory discovery commands (e.g., 'ls', 'find') from terminal or script-based tooling, especially outside normal user workflows.

### Log Sources

**Mutable Elements**

Field	Description
PredicateScope	Adjust macOS unified log filter to include/exclude system paths
TimeWindow	Tune based on burst access patterns

**AN1043**

Execution of esxcli commands to enumerate datastore, configuration files, or directory structures by unauthorized or remote users.

**Log Sources**

**Mutable Elements**

Field	Description
CLICommandPattern	Match on esxcli storage filesystem commands
AccessSource	Limit alerting to non-vCenter or remote IPs

**AN1044**

Execution of file discovery commands (e.g., 'dir', 'show flash', 'nvram:') from CLI interfaces, especially by unauthorized users or from abnormal source IPs.

**Log Sources**

**Mutable Elements**

Field	Description
CommandWhitelist	Filter allowed commands by account or IP
SessionOrigin	Tunable to restrict detection to remote terminal or Telnet/SSH

---

Source: <https://attack.mitre.org/detectionstrategies/DET0370#AN1042>