

# Detection Strategy for Remote System Enumeration Behavior,

## Detection Strategy DET0574

Archived: 2026-04-02 11:16:30 UTC

### AN1583

Execution of network enumeration utilities (e.g., net.exe, ping.exe, tracert.exe) in short succession, often chained with lateral movement tools or system enumeration commands.

#### Log Sources

#### Mutable Elements

Field	Description
TimeWindow	Define bursty execution patterns of enumeration commands (e.g., <30s)
CommandLinePattern	Tunable per org's scripting/IT tools (e.g., exclude SCCM, PsExec)
ParentProcess	Flag suspicious process ancestry (e.g., Word.exe spawning net.exe)

### AN1584

Use of bash scripts or interactive shells to issue sequential ping, arp, or traceroute commands to map remote hosts.

#### Log Sources

#### Mutable Elements

Field	Description
TargetIPRange	Tune for sensitive internal segments or known lateral targets
ShellContext	Distinguish user-interactive enumeration vs. cronjob or baseline tooling

### AN1585

Execution of built-in or AppleScript-based system enumeration via `arp` , `netstat` , `ping` , and discovery of `/etc/hosts` contents.

#### Log Sources

#### Mutable Elements

Field	Description
ExecutionUser	Limit detection to suspicious users or automation contexts
CommandSignature	Adapt for expected enumeration tooling used in IT

### AN1586

ESXi shell or SSH access issuing `esxcli network diag ping` or viewing routing tables to identify connected hosts.

#### Log Sources

#### Mutable Elements

Field	Description
ESXCommandPattern	Match specific diag/debug commands abused for recon
RemoteUserShell	Detect unauthorized shell use or user context (e.g., root over SSH)

### AN1587

Execution of discovery commands like `show cdp neighbors` , `show arp` , and other interface-level introspection on Cisco or Juniper devices.

#### Log Sources

#### Mutable Elements

Field	Description
CommandList	Device-specific recon commands to monitor based on make/model
PrivLevel	Trigger detection for privilege escalation prior to recon commands

---

Source: <https://attack.mitre.org/detectionstrategies/DET0574#AN1587>