

# Behavioral Detection of System Network Configuration Discovery, Detection Strategy DET0195

Archived: 2026-04-05 17:31:58 UTC

## AN0559

Execution of built-in tools (e.g., ipconfig, route, netsh) or PowerShell/WMI queries to enumerate IP, MAC, interface status, or routing configuration.

### Log Sources

### Mutable Elements

Field	Description
ParentProcess	Filter known/legit CLI chains (e.g., explorer.exe → cmd.exe) to reduce FP
UserContext	Target executions by non-admin or unexpected users
TimeWindow	Cluster enumeration commands within short time windows

## AN0560

Execution of `ifconfig` , `ip a` , or access to `/proc/net/` indicating collection of local interface and route configuration.

### Log Sources

### Mutable Elements

Field	Description
CommandLinePattern	Match regex for variations in enumeration syntax (e.g., <code>`ip -4 addr show`</code> )
InteractiveShellIndicator	Differentiate scripted versus interactive sessions

## AN0561

Execution of `ifconfig` , `networksetup` , or `system_profiler` to query IP/MAC/interface configuration and status.

### Log Sources

**Mutable Elements**

Field	Description
ScriptedContext	Scripted tools (e.g., bash calling `ifconfig`) vs GUI-initiated inspection
ExecutionFrequency	Enumerations executed frequently or across multiple interfaces may indicate enumeration loops

**AN0562**

Use of `esxcli network` commands (e.g., `esxcli network nic list`, `esxcli network ip interface ipv4 get`) via SSH or hostd to enumerate adapter and IP information.

**Log Sources**

**Mutable Elements**

Field	Description
SSHSessionOrigin	Detection may vary based on internal vs remote terminal usage
esxcliCommandDepth	Distinguish between benign status checks and deep enumeration chains

**AN0563**

CLI-based execution of interface and routing discovery commands (e.g., `show ip interface`, `show arp`, `show route`) over Telnet, SSH, or console.

**Log Sources**

**Mutable Elements**

Field	Description
Username	Highlight low-privileged or non-routine users performing discovery
CommandString	Allow for tuning based on command regex or frequency
TransportType	SSH vs Telnet vs Console session logging scope

---

Source: <https://attack.mitre.org/detectionstrategies/DET0195#AN0559>