Linpeas checks for privilege escalation vulnerabilities

You might need to detect use of the Linpeas tool on your Linux endpoints when doing the following:

- Detecting usage of popular Linux post-exploitation tools

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- People: Security analyst or threat hunter
- Technologies: Splunk Cloud Platform or Splunk Enterprise
- Add-on: Add-on for Linux Sysmon
- Data: Sysmon for Linux

Example

Linpeas is a popular tool used to search for possible paths to escalate privileges on Linux, Unix, and MacOS hosts. It provides users with possible exploits available for the target host based on system, service, and library information, as well as version levels. Tools like Linpeas frequently use the strings and grep system utilities to extensively and recursively check for important system files such as /etc/shadow and /etc/passwd or directories such as /usr/bin or /tmp.

You can use this search to identify some common hallmarks of Linpeas checks on hosts in your environment.

To optimize the search shown below, you should specify an index and a time range.

Run the following search:

```
sourcetype="sysmon_linux" CommandLine!=null parent_process_exec=sudo OR parent_process_exec=bash OR CommandLine="cve-list" | stats count BY Computer CommandLine user process_path
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.
<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=“sysmon_linux” CommandLine!=null</td>
<td>Search the sysmon_linux sourcetype for parent processes and command lines associated with Linpeas usage.</td>
</tr>
<tr>
<td>parent_process_exec=sudo OR parent_process_exec=bash OR CommandLine=“cve-list”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>stats count BY Computer CommandLine user process_path</td>
</tr>
</tbody>
</table>

**Result**

Linpeas is a verbose tool and positive results from this search should show extensive use of the grep utility that it uses to perform its checks.