Detecting usage of popular Linux post-exploitation tools

Scenario: Tools that are focused on Linux post-exploitation efforts use similar commands and many of these commands, seen in an isolated context, are not effective as single indicators of post-exploitation. Such commands are used for legitimate purposes by administrators. However, digging into the data deeper with Sysmon for Linux and looking at the different processes, services, and user-session information might indicate the use of these tools in the context of post-exploitation. Malicious actors often use these tools to search for opportunities to exploit Linux hosts. Among these tools are:

- Linpeas, used to search for possible paths to escalate privileges on Linux/Unix/MacOS hosts
- LinuxExploitSuggester, used to audit privilege escalation in Linux systems
- AutoSUID, used for harvesting of SUID executable files as a path to escalate privileges

These searches can be used as a first approach to discovering and detecting activities initiated by these tools in Linux hosts.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

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

How to use Splunk software for this use case

Depending on what information you have available, you might find it useful to identify some or all of the following:

- Linpeas for privilege escalation vulnerabilities
- LinuxExploitSuggester used to find system-specific vulnerabilities
- AutoSUID used for privilege escalation

Results

Results returned from these searches show hallmarks of checks made by these tools on Linux hosts in your environment. You should analyze these results further to identify whether they definitely show suspicious activity.
Additional resources

The content in this guide comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. In addition, these Splunk resources might help you understand and implement this use case:

• Splunk Research: Linux post-exploitation