Active detection of vulnerable sudo versions

You might need to actively scan your Linux hosts for vulnerabilities to the Baron Samedit attack when doing the following:

- Detecting the Sudo Baron Samedit attack

Prerequisites

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

- Splunk Enterprise or Splunk Cloud Platform
- Splunk Universal Forwarder
- Technical Add-on for Samedit or Splunk Add-on for Unix and Linux
- *nix logs

Example

Your organization has unpatched Linux servers. You know those servers are vulnerable to a number of attacks, including the heap-based buffer overflow in sudo, called Baron Samedit. You want to be able to search for indications that this attack has hit your servers.

Option 1

1. Install the Technical Add-on for Samedit on a Universal Forwarder. By default, it runs once per hour.
2. Run the following search:
   - `index=<index where your *nix logs are>`
   - `sourcetype="script::samedit"

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><code>index=&lt;index where your *nix logs are&gt;</code></td>
<td>Search only the index where your *nix logs are stored.</td>
</tr>
<tr>
<td><code>sourcetype=&quot;script::samedit&quot;</code></td>
<td>Search only the execution of</td>
</tr>
</tbody>
</table>

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Result

The add-on runs various versioning commands as a scripted input, parses them to find your sudo version, and compares the version found on the system to a list of patched releases of sudo. The TA is also "Ubuntu-aware" as those systems report their version numbers differently. The key/value pair output of "samedit_status" and "finding" tells you if that particular Linux host is potentially vulnerable. This is a great way to map your patch status progress.

Option 2

1. Install the Splunk Add-on for Unix and Linux.
2. Run the following search:
   index=<index where your *nix logs are>
   sourcetype="package"

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>index=&lt;index where your *nix logs are&gt;</td>
<td>Search only the index where your *nix logs are stored.</td>
</tr>
<tr>
<td>sourcetype=&quot;script::samedit&quot;</td>
<td>Search only the packages installed on common Linux distros.</td>
</tr>
</tbody>
</table>

Result

Suppose you happen to have a vulnerability management capability (like Qualys), especially one that is doing credentialed scans of your server and workstation. You can use this search to find version numbers of sudo present and plan for mitigation. Or, if you have any attack surface management capabilities, you can determine what Unix resources are outside your firewall but on your network. RiskIQ, for example, can tell you what versions of Linux or Unix it finds, which will help you prioritize your patching once you cross-map those to versions shipped with vulnerable sudo versions. Whether you're doing internal or external scanning, you can always ingest and report on the results in Splunk and perhaps take automated action upon these results as well.