Report 1:

***Executive summary/abstract:***

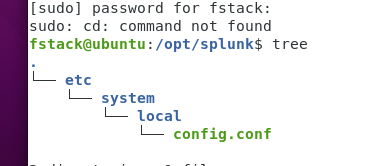
The automation and "A" portion of the CIA triad in computing makes it a glorious opportunity for those looking to disrupt daily processes of clients, owners, users, hosts, and everything in between. There is no simple resolution for the internal threat created by our need to have systems up and able to use at anyone's fingertips. The report highlights ways to use scripting, MD5/Sha256, and using the commands to create inventive and clever ways to audit your own system internally, as well as some of the pitfalls that system admins can fall into in trying to create autonomy.

Intro

In the cybersecurity realm there is a large issue within the automation processes. Meaning if the wrong person can get into the system and everyday processes, then what can ensue is a total lack of dysfunction. In our task to correct these "config" we clearly saw that someone may have done the same to our configuration file. The biggest takeaway as well seems to be that automation is our best friend but also our worst enemy, in reality it's one of our biggest internal threats. Additionally, with how Splunk treats the ability to process data it also charges for the amount of data that is being used, which in turn can be more costly to us as a company going forward. The solution to the script file that has been modified entails several processes which will be expounded upon later, the initial step toward a more secure group of computing is setting up adequate permissions for groups.

Body

In our systems of computing, we value Confidentiality, Integrity, and most of all availability, for us to be able to have a system be always running, there will be gaps, and opportunities. In our case figure 1 shows how easy it can be to mess with the automated processes within our systems. Constant need for availability creates a constant stress on systems to be up, which in turn creates a dire need to create backups, patches, updates and constant software trails and audits.



Important configuration file shouldn’t have loose permissions and be accessible easily figure 2 shows the permissions on our file:



Showing that the file was clearly accessible to everyone without any form of authentication, two or three factor authentication must be enacted within the process when looking to be allowed into the permissions of any DAILY process. Audits of these processes should and will be a KEY dire needed for systems, and gap analysis needs to be quarterly.

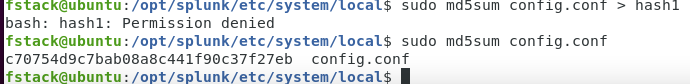
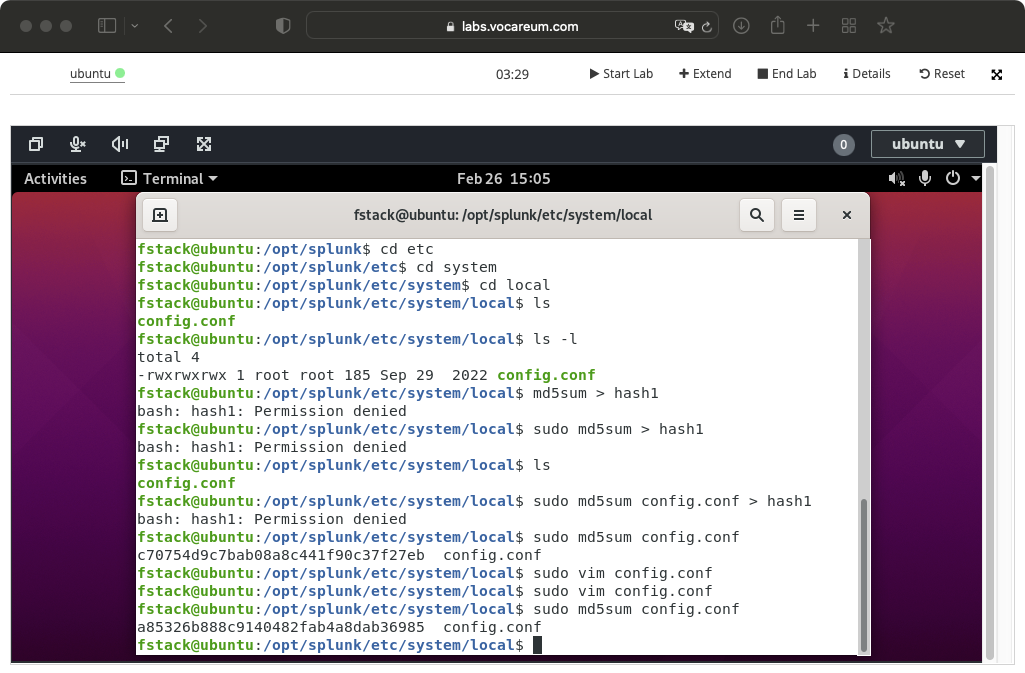


Figure 3 above displays the need for a constant outflow of automated security scripts. MD5 redirect files will allow users and clients of our services to consistently see edits to files, scripts, and a multitude of accessibility components. Any small change to a file is immediately seen, although we suggest

Sha256-md5 trails are a good basis for any security audit trail. Figure 4 below shows how fast and immediate any change to file can be seen after our edit of the script.



***Conclusion***

In summation there are various recommendations that can be easily applied in order to create a safer computing environment in your business. Each of following are mainly due to the constant stress the availability is creating within systems:

1. Permissions on all files that have to do with configurations
2. Groups that are created for specific access to specific work need/function files.
3. Two factor authentication, maybe even three, where access to the company sso and vpn is needed to even access such processes.
4. Least privilege.
5. Automated scripts of MD5 and Sha256 on important configs, logs, and processes.

All can be done in a manner that can sure up the system but also create countless opportunities for honeypots as well. Once given the green light for these processes the initial step is running a gap analysis in order to get a larger overview of systems, then begin changes for a better and safer computing landscape.