Almely Ramos

Scripts for Security 1

Linux Admin

11/19/19

1. **Script 1**

<https://github.com/onlybuilt4cubanliz/Linux_Admin/blob/master/script1.sh>

A screenshot of a cell phone

Description automatically generated

Above is the script (Also a link provided to my GitHub account)

Step 1: Run the script

command: ./script1.sh

**Step 2: Make sure these files have been made.**



When you run the script it will make 2 files.

The size.pid will help to see if there have been any new intrusions.

The “19-Nov.log” is a file that its name will change every time you run the script. I usually run the script every time I start the server, so it updates the date every time.

Also, the date log is where you will find the details of the intrusion.

These 2 files cannot be deleted as they update every time the script is ran and will contain previous history and information pertaining to older intrusion attempts.

1. **Script 2**

<https://github.com/onlybuilt4cubanliz/Linux_Admin/blob/master/script2.sh>

(I can’t screenshot the script, it’s too long)

**Script to detect changes in /etc**

**Step 1: Run the Script**

command: ./script2.sh

**Step 2: After you have ran the scripts, make sure these files have been made.**

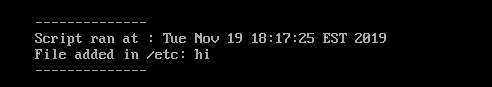
A picture containing object

Description automatically generated

Once you run the script you 2 files will have been created:

**file\_diff.report**- This is where all the changes will appear, it’s a report of all the changes that have been made in the /etc directory.

For Example:



I made a file called “hi” in /etc and once I ran the script and opened up the report it tells me when I ran the script and what has changed in that directory.

**soft.tmp**- The soft temp file its just a file listing all that is in the /etc directory after I have ran the script. It keeps a record of it just so who ever has run the script can double check if the changes that the report calls to, have actually happened.

1. **Script 3**

<https://github.com/onlybuilt4cubanliz/Linux_Admin/blob/master/script3.sh>

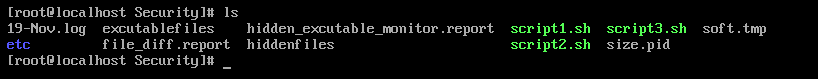
(I can’t screenshot the script, it’s too long)

**Script to monitor hidden files, executable files**

**Step 1: Run the Script**

**command: ./script3.sh**

**Step 2: Make sure that these files are created:**

****

**executablefiles – This takes record of all the executable files that are currently on the server.**

**hiddenfiles – This takes record of all the hidden files that are currently on the server.**

**hidden\_executable\_monitor\_report – This is the report that will tell you of any changes that have been made to these files, who made them, and when they were made.**

**Visual of Monitor Report**

**A screenshot of a cell phone

Description automatically generated**