**Ubuntu Scripts for security part 1**

On my ubuntu server the first thing I did was switch to root using **su – root**. Once I was in root I then uses the nano command followed by the name of my script, in this case it’s **monitor.sh**. After the nano opens I started with **# !/bin/bash** at the very top. After I inserted an **arp-a** command allowing the script to show any local addresses my server has communicated with. Next I inserted a command that checks a user’s login. I used the command **echo “Enter UserName : ”** followed by  **read user**  & **last $user.** This command asks for an input which is a user name that has been already created on the server, I inserted root as you can see in the screenshot below.Text

Description automatically generatedCalendar

Description automatically generated

Before I create my next script, I had to install **inotify-tools** by using the command **sudo apt-get install inotify-tools**. After that was installed, I used the nano command followed by a new script name. Once the nano opened the file, I started with **#!/bin/bash** then I used **inotifywait -r -m -e modify /var/log** **| while read path \_ file; do echo $path$file modified done.**  This command will read anything that was modified under **/var/log** and echos anything back that was modified.Text

Description automatically generatedText

Description automatically generated

Next I created another script that will show any hidded files and also show any running executabels in root. First I used the nano command followed by a new script name. I then proceeded with **#!/bin/bash** at the top of my script. Next I used an **ls** command that shows any hidden files in my user root. The command that I used was **ls -dl .[^.]\* ~** to find any hidden files in the root user that im in. Next I used a **find** command to show all running executables. The command that I used was **find / -user root -perm -4000 -exec ls – ldb {} \;.** This command shows all running executables under the user root.Text

Description automatically generated

Text

Description automatically generated

Work cited

<https://lzone.de/cheat-sheet/Filesystem>

<https://pentestlab.blog/2017/09/25/suid-executables/>