SPRING 15

EJERCICIO 1 – UNIDAD 1

CRONNTAB

METODOS WILDCVARDS Y FILE OVERWRITE

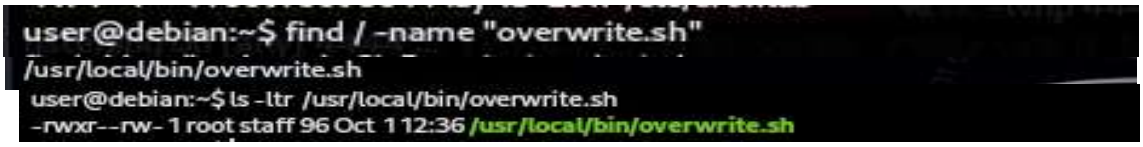
En este ejercicio se trabajará la escalada de privilegios de las siguientes formas, debiendo explicar con capturas y texto el procedimiento seguido para cada una de ellas:

- En ambos ejercicios nos conectamos a la Maquina Debian 6 con IP 10.0.2.28, la cual, ya ha sido comprometida anteriormente y ahora vamos a escalar privilegios a través de SSH en el sistema:

1. Elevación de privilegios *mediante* ***Cron – File Overwrite:***

   - Se procede a ver el servicio Crontab, presentando permisos de lectura para todos, por lo que no se puede crear una nueva tarea con el usuario actual, debiendo explotar alguno de los presentes.

   - Se realiza la búsqueda de la ruta del archivo overwrite.sh, siendo la misma */usr/local/bin/overwrite.sh*:

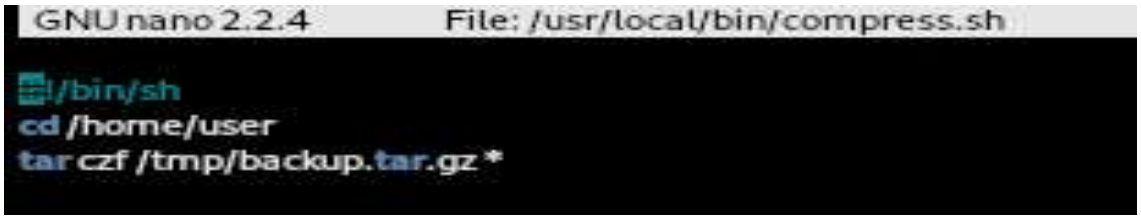


   - se modifica con nano el archivo overwrite.sh, añadiendo al archivo /bin/Bash el permiso Bit SUID (s), consiguiendo elevación de privilegios a root:

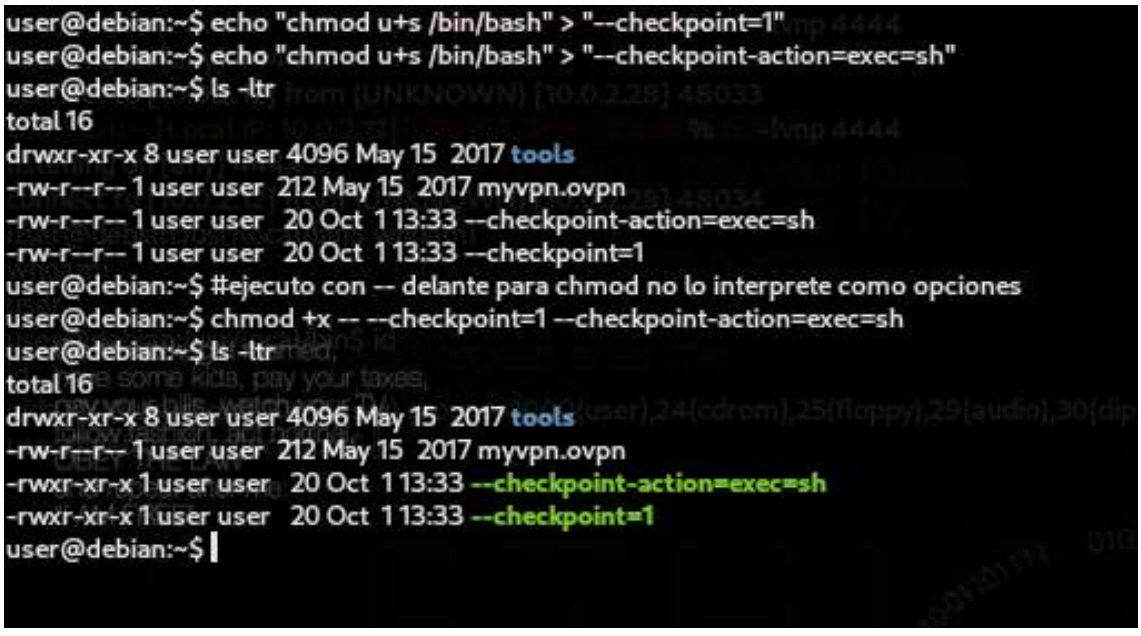
2. Elevación de privilegios a través los ***wildcards*** del archivo ***Cron***:

- En el Cron se pueden usar comodines (wildcards) para la ejecución periódica de tareas, pero si no son configurados adecuadamente puede permitir que personas sin autorización escalen privilegios a través de ellos, ejecutando código malicioso.

- Como anteriormente observamos solo había 2 archivos que se podían modificar en el Crontab, ya que este último tenía solo permisos de lectura y no permitía crear nuevas tareas, asi que para este caso usaremos el archivo *"/usr/local/bin/compress.sh"*
- Este archivo por su contenido, se utiliza para hacer una copia comprimida (tar.gz) de los archivos del directorio *"/home/user*" almacenándose en "*/tmp/backup.tar.gz*".
- El comando de compresión *tar* tiene una vulnerabilidad en los puntos de control o *checkpoints,* que puede ser explotada a través de los wildcards o comodines, si el administrador no tiene cuidado en cómo se manejan.



- Para su explotación accedemos al directorio */home/user*, donde creamos dos archivos, llamados *"- - checkpoints=1*" y *"- -* "*checkpoint-action=exec=sh*" y le añadimos con chmod permisos de ejecución, que el archivo "compress" hace una copia comprimida de este directorio como hemos dicho anteriormente.



- Ahora cuando se ejecute el archivo “compress” como tarea programada (cada minuto) en Crontab, haciendo que el comando *tar*, al ver el archivo *“- -checkpoint=1”* haga una pausa tras realizar la primera tarea, momento que entra en ejecución el segundo archivo *“--checkpoint-action=exec=sh”* , el cual esta configurado para ejecutarse cuando se encuentre un checkpoint dentro de *tar* , ejecutando un shell.