Buscando accesos raros a una cuenta de correo en los logs de cPanel

Introducción

Algunas veces se hace necesario revisar los logs para investigar problemas reportados en tickets de "no me llegan los correos".

Muchas veces son filtros de correo mal implementados, pero otras veces son signos de que la cuenta está hackeada.

Una cosa que no entienden los usuarios es que un exploit que permita acceso al atacante para inyectar un mini shell o una utilidad de administración de archivos, le da al atacante acceso a ciertas cosas de su cuenta.

Asi que haremos uso intensio de `grep,` awk`y otros comandos de shell.

Busqueda de accesos en el correo

```
{ grep -Ei "login:" /var/log/maillog | awk '{print $1 " " $2 " " $3 " " $10 " " $8 }' | sed 's/rip=//g;s/,//g' && grep -Ei "\[webmaild\]" /usr/local/cpanel/logs/session_log* | awk '{print $1 " " $2 " " $6 " " $8}' | cut -d"[" -f 2 | sort | uniq && grep -Ei "\[webmaild\]" /usr/local/cpanel/logs/login_log* | awk '{print $1 " " $2 " " $6 " " $8}' | cut -d"[" -f 2 | sort | uniq; }



2024-07-02 21:21:44 213.194.xxx.220 paqui@dfsdfsdfsdf.com
2024-07-02 21:57:51 213.194.xxx.220 info@sdfsdfsdfsdf.com
2024-07-02 22:49:56 216.147.xxx.79 reservas@sdfsefsfdd.com
2024-07-02 23:21:27 213.194.xxx.220 info@sdfsdfsdf.com
2024-07-03 03:07:18 35.173.xxx.157 ignacio@sdfsdfsdf.es
2024-07-03 05:50:35 80.30.xxx.100 educacion@sdfsdfs.sdfsdfsdfss.org
```

Version por cuenta especifica

```
cuenta="usuario@dominio.com"

{
  grep -Ei "login:" /var/log/maillog | grep "$cuenta" | awk '{print $1 " " $2 " " $3 " " $10 "
" $8}' | sed 's/rip=//g;s/,//g'
  grep -Ei "\[webmaild\]" /usr/local/cpanel/logs/session_log* | grep "$cuenta" | awk '{print
$1 " " $2 " " $6 " " $8}' | cut -d"[" -f 2 | sort | uniq
  grep -Ei "\[webmaild\]" /usr/local/cpanel/logs/login_log* | grep "$cuenta" | awk '{print $1
" " $2 " " $6 " " $8}' | cut -d"[" -f 2 | sort | uniq
}

2024-06-26 08:51:11 213.194.xxx.220 usuario@dominio.com
2024-07-01 22:39:16 213.194.xxx.220 usuario@dominio.com
2024-07-02 12:06:21 31.221.xxx.87 usuario@dominio.com
2024-07-02 14:08:57 213.194.xxx.220 usuario@dominio.com
2024-07-02 14:17:08 213.194.xxx.220 usuario@dominio.com
```

Agradecimientos

A Ehsan Dowlatshah en How To List Email Login History? por la idea.

Aviso

Revision #1
Created 2024-07-03 07:28:39 UTC by Abkrim
Updated 2024-07-03 07:41:14 UTC by Abkrim