Chocolate Factory – TryHackMe Technical Report

1. Introduction

The Chocolate Factory room on TryHackMe is a Capture The Flag (CTF) challenge focused on web application exploitation, Linux privilege escalation, and post-exploitation techniques. The objective is to identify vulnerabilities, gain initial access, escalate privileges, and obtain the root flag. This lab simulates real-world misconfigurations commonly found in poorly secured systems.

Learn > Chocolate Factory

Chocolate Factory

A Charlie And The Chocolate Factory themed room, revisit Willy Wonka's chocolate factory!

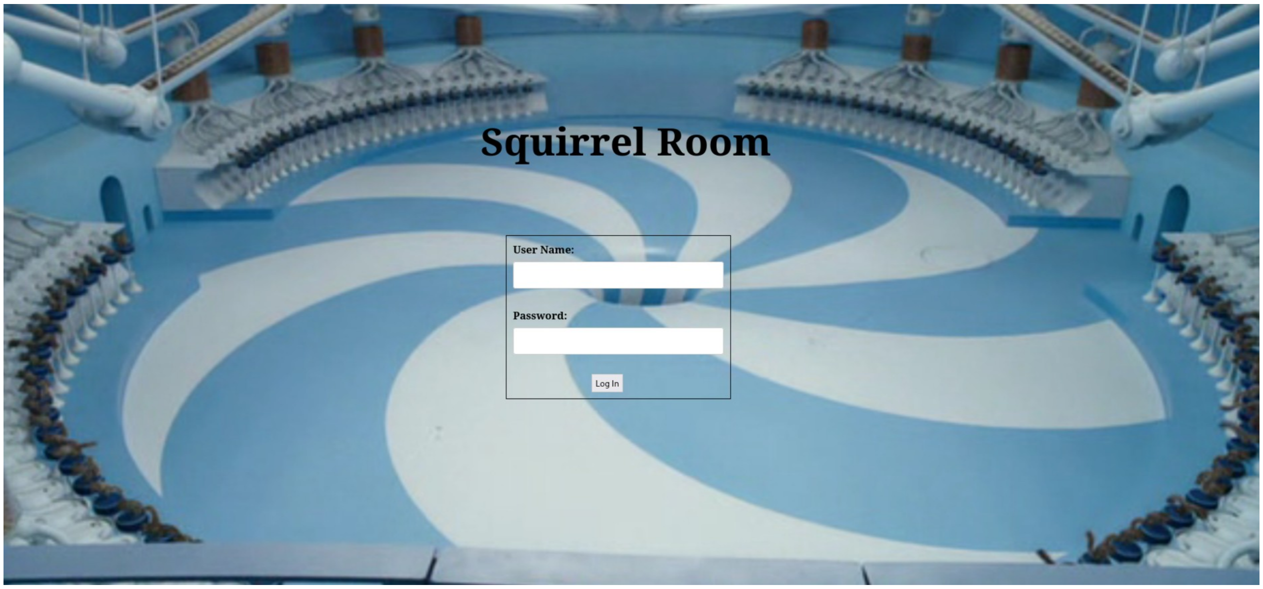
45 min 27,372

Room completed (100%)

2. Scope

The scope of this assessment is strictly limited to the TryHackMe Chocolate Factory lab environment. Activities performed include:

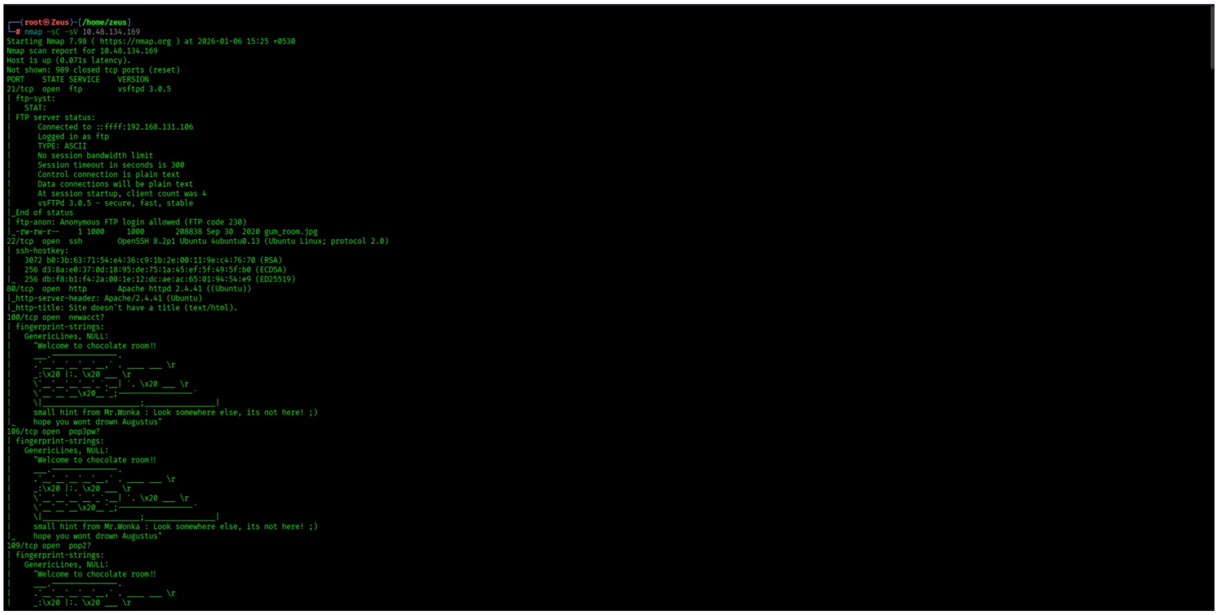
- Network and service enumeration
- Web application analysis
- Exploitation of vulnerabilities
- SSH access using discovered credentials
- Privilege escalation to root



3. Methodology

1. Reconnaissance

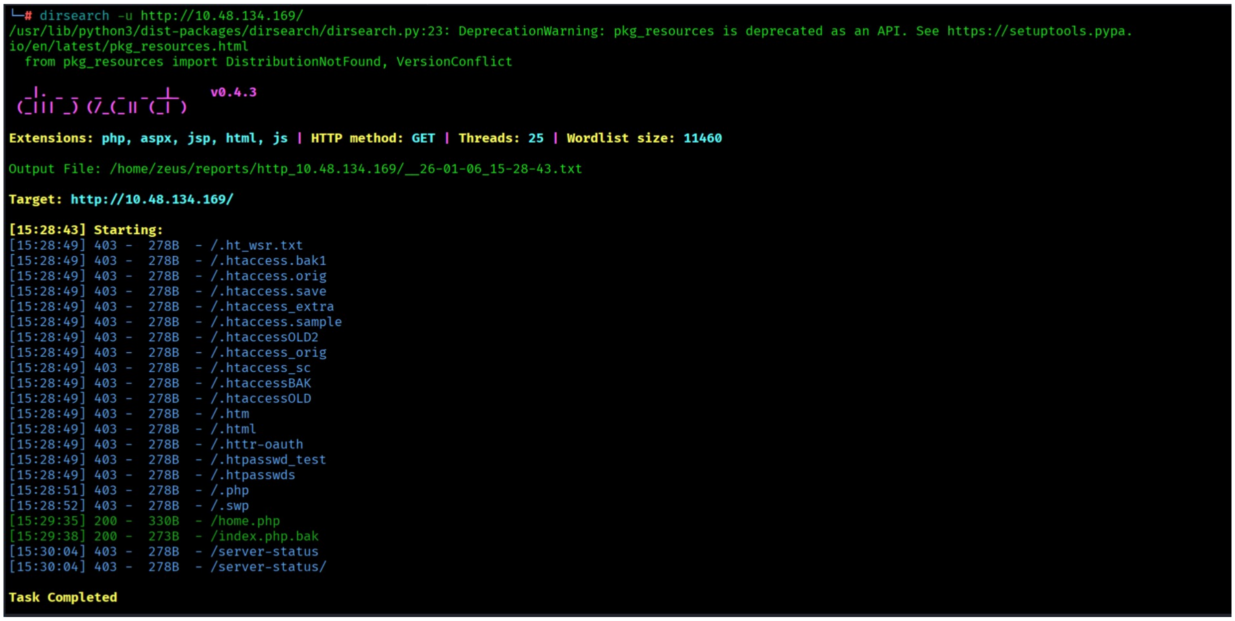
- Nmap was used to identify open ports and running services.
- HTTP services were inspected using a web browser and directory enumeration tools.



```
┌──(root㉿Zeus)-[/home/zeus]
└─# nmap -sC -sV 10.48.134.169
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-06 15:25 +0530
Nmap scan report for 10.48.134.169
Host is up (0.071s latency).
Not shown: 989 closed tcp ports (reset)
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.131.106
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-rw-r--    1 1000     1000       208838 Sep 30  2020 gum_room.jpg
22/tcp  open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b0:3b:63:71:54:e4:36:c9:1b:2e:00:11:9e:c4:76:70 (RSA)
|   256 d3:8a:e0:37:0d:18:95:de:75:1a:45:ef:5f:49:5f:b0 (ECDSA)
|_  256 db:f8:b1:f4:2a:00:1e:12:dc:ae:ac:65:01:94:54:e9 (ED25519)
80/tcp  open  http       Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
100/tcp open  newacct?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.---------------.
|     .'__'__'__'__'__,` .____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;-----------------`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
106/tcp open  pop3pw?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.---------------.
|     .'__'__'__'__'__,` .____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;-----------------`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
109/tcp open  pop2?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.---------------.
|     .'__'__'__'__'__,` .____ ___ \r
|     _:\x20 |:. \x20 ___ \r
```

2. Enumeration

- Web directories and files were enumerated to locate hidden resources.
- Source code and page content were analyzed for credentials and clues.



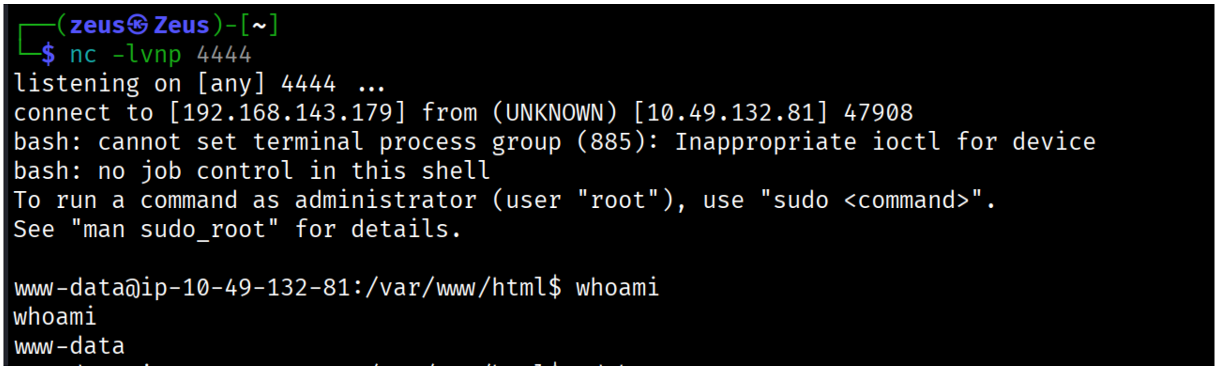
```
└─# dirsearch -u http://10.48.134.169/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.
io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/zeus/reports/http_10.48.134.169/__26-01-06_15-28-43.txt

Target: http://10.48.134.169/

[15:28:43] Starting:
[15:28:49] 403 -  278B  - /.ht_wsr.txt
[15:28:49] 403 -  278B  - /.htaccess.bak1
[15:28:49] 403 -  278B  - /.htaccess.orig
[15:28:49] 403 -  278B  - /.htaccess.save
[15:28:49] 403 -  278B  - /.htaccess_extra
[15:28:49] 403 -  278B  - /.htaccess.sample
[15:28:49] 403 -  278B  - /.htaccessOLD2
[15:28:49] 403 -  278B  - /.htaccess_orig
[15:28:49] 403 -  278B  - /.htaccess_sc
[15:28:49] 403 -  278B  - /.htaccessBAK
[15:28:49] 403 -  278B  - /.htaccessOLD
[15:28:49] 403 -  278B  - /.htm
[15:28:49] 403 -  278B  - /.html
[15:28:49] 403 -  278B  - /.httr-oauth
[15:28:49] 403 -  278B  - /.htpasswd_test
[15:28:49] 403 -  278B  - /.htpasswds
[15:28:51] 403 -  278B  - /.php
[15:28:52] 403 -  278B  - /.swp
[15:29:35] 200 -  330B  - /home.php
[15:29:38] 200 -  273B  - /index.php.bak
[15:30:04] 403 -  278B  - /server-status
[15:30:04] 403 -  278B  - /server-status/

Task Completed
```

3. Exploitation

- Insecure file exposure led to discovery of sensitive files.
- SSH private keys were obtained and used to gain shell access as a low-privileged user.

4. Privilege Escalation

- System enumeration revealed misconfigured permissions.
- Privilege escalation techniques were used to obtain root access.



```
┌──(zeus㉿Zeus)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.143.179] from (UNKNOWN) [10.49.132.81] 47908
bash: cannot set terminal process group (885): Inappropriate ioctl for device
bash: no job control in this shell
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

www-data@ip-10-49-132-81:/var/www/html$ whoami
whoami
www-data
```

4. Findings – Vulnerabilities and Difficulty

1. Open Services – Medium

   Vulnerability: Excessive network service exposure
   Method: Nmap port scanning
   Ports Identified: 22/tcp-ssh, 80/tcp-HTTP

   The system exposed multiple services to the network without proper restriction, increasing the attack surface and enabling further enumeration.

2. Weak File Permissions – Medium

   Vulnerability: Improper access control on web directories
   Method: Web directory enumeration and manual inspection
   Hidden directories and files were accessible via the web server, allowing attackers to discover sensitive information and clues required for exploitation.

3. Insecure SSH Key Storage – Medium

   Vulnerability: Incorrect Linux file permissions
   Method: Local file system enumeration
   Sensitive files were readable by unauthorized users due to misconfigured permissions, leading to information disclosure.

4. Privilege Escalation Misconfiguration – Medium

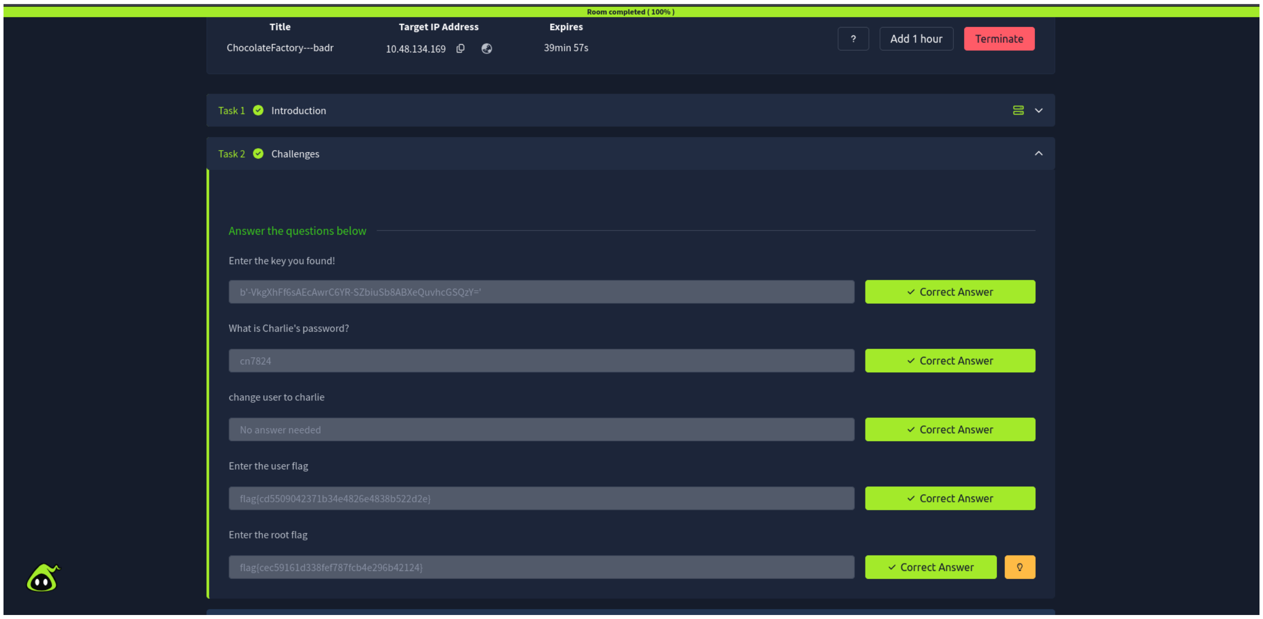
   Vulnerability: Improper credential storage
   Method: File inspection and enumeration
   SSH private keys were stored without adequate protection, allowing attackers to authenticate via SSH without passwords.

5. Recommendations

- Harden file permissions using least privilege principles.
- Remove or secure unnecessary network services.
- Protect private keys with proper access control.
- Conduct regular vulnerability scans and audits.

6. Conclusion

The Chocolate Factory lab demonstrates how common misconfigurations can lead to a complete system compromise. By following a structured penetration testing methodology, root-level access was achieved. This highlights the importance of secure configuration, monitoring, and proactive security testing.



Room completed (100%)

Title	Target IP Address	Expires
ChocolateFactory---badr	10.48.134.169	39min 57s

Task 1 ✓ Introduction

Task 2 ✓ Challenges

Answer the questions below

Enter the key you found!

b'-VkgXhFf6sAEcAwrC6YR-SZbiuSb8ABXeQuvhcGSQzY='

What is Charlie's password?

cn7824

change user to charlie

No answer needed

Enter the user flag

flag{cd5509042371b34e4826e4838b522d2e}

Enter the root flag

flag{cec59161d338fef787fcb4e296b42124}