VULN SHIELDS

VULNSHIELDS CONSULTING Pvt. Ltd

HACKTHEBOX
Road map to Clear OSCP

GOVERDHAN

II

www.vulnshields.net

Disclaimer

The boxes listed below serve as a starting point to build practical skills and enhance your pentesting methodology. Please note that this list is not a substitute for the actual lab environment in the PWK/OSCP course. It is highly encouraged to go through every system in the PWK/OSCP lab environment for a better understanding and preparation for the exam.

Linux Machines

1. Lame - Difficulty: Easy

- A beginner-friendly Linux machine that focuses on basic enumeration and exploiting common vulnerabilities.
- Skills: Basic Linux enumeration, vulnerable services (Samba), privilege escalation.

2. Brainfuck - Difficulty: Easy

- A Linux machine that requires deciphering an encoded message to find the user and root flags.
- Skills: Cryptography, enumeration, web exploitation.

3. Shocker - Difficulty: Easy

- A Linux machine that targets a vulnerable CGI script to gain initial access and escalate privileges.
- Skills: Web exploitation, Bash command injection, privilege escalation.

4. Bashed - Difficulty: Easy

- A Linux machine that involves exploiting a vulnerable web application and obtaining a reverse shell.
- Skills: Web exploitation, command injection, reverse shell.

5. Nibbles - Difficulty: Easy

- A Linux machine with a web application vulnerability that can be exploited to gain initial access.
- Skills: Web exploitation, PHP deserialization, privilege escalation.

6. Beep - Difficulty: Easy

- A Linux machine that focuses on exploiting a misconfigured service to gain initial access.
- Skills: Service enumeration, file permission issues, privilege escalation.

7. Cronos - Difficulty: Easy

- A Linux machine that involves exploiting a misconfigured password policy and a vulnerable service.
- Skills: Password cracking, service enumeration, privilege escalation.

8. Nineveh - Difficulty: Easy

- A Linux machine with multiple avenues for exploitation, including a vulnerable CMS.
- Skills: Web exploitation, CMS vulnerabilities, privilege escalation.

9. Sense - Difficulty: Easy

- A Linux machine that requires finding and exploiting a remote code execution vulnerability.
- Skills: Web exploitation, command injection, reverse shell.

10. Solidstate - Difficulty: Easy

- A Linux machine that focuses on exploiting a vulnerable database and leveraging file permissions.
- Skills: Database exploitation, file permission issues, privilege escalation.

11. Node - Difficulty: Medium

- A Linux machine that involves exploiting a Node.js application to gain access and escalate privileges.
- Skills: Node.js exploitation, JavaScript deserialization, privilege escalation.

12. Valentine - Difficulty: Medium

- A Linux machine that requires exploiting a vulnerable web application to gain initial access.
- Skills: Web exploitation, PHP deserialization, privilege escalation.

13. Poison - Difficulty: Medium

- A Linux machine that involves exploiting a vulnerable CMS and leveraging misconfigured permissions.
- Skills: CMS vulnerabilities, file permission issues, privilege escalation.

14. Sunday - Difficulty: Medium

- A Linux machine that focuses on exploiting a vulnerable web application and manipulating file upload.
- Skills: Web exploitation, file upload vulnerabilities, privilege escalation.

15. Tartarsauce - Difficulty: Medium

- A Linux machine that requires exploiting a remote code execution vulnerability in a custom web application.
- Skills: Web exploitation, command injection, privilege escalation.

16. Irked - Difficulty: Medium

- A Linux machine that involves exploiting a vulnerable service and manipulating file permissions.
- Skills: Service enumeration, file permission issues, privilege escalation.

17. Friendzone - Difficulty: Medium

- A Linux machine that focuses on exploiting a vulnerable web application and leveraging misconfigurations.
- Skills: Web exploitation, misconfigurations, privilege escalation.

18. Swagshop - Difficulty: Medium

- A Linux machine that requires exploiting a vulnerable e-commerce platform and escalating privileges.
- Skills: Web exploitation, e-commerce vulnerabilities, privilege escalation.

19. Networked - Difficulty: Medium

- A Linux machine that involves exploiting a misconfigured NFS share to gain initial access.
- Skills: NFS enumeration, file permission issues, privilege escalation.

20. Jarvis - Difficulty: Medium

- A Linux machine that focuses on exploiting a vulnerable smart home automation system.
- Skills: IoT exploitation, home automation vulnerabilities, privilege escalation.

21. Mirai - Difficulty: Medium

- A Linux machine that requires exploiting IoT devices to gain initial access and escalate privileges.
- Skills: IoT exploitation, botnets, privilege escalation.

22. Popcorn - Difficulty: Medium

- A Linux machine that involves exploiting a vulnerable web application and manipulating database entries.
- Skills: Web exploitation, SQL injection, privilege escalation.

23. Haircut - Difficulty: Medium

- A Linux machine that focuses on exploiting a vulnerable web application and privilege escalation.
- Skills: Web exploitation, command injection, privilege escalation.

24. Blocky - Difficulty: Medium

- A Linux machine that requires exploiting a vulnerable Minecraft server plugin to gain access.
- Skills: Minecraft server vulnerabilities, Java deserialization, privilege escalation.

25. Frolic - Difficulty: Medium

- A Linux machine that involves exploiting a vulnerable web application and manipulating user input.
- Skills: Web exploitation, command injection, privilege escalation.

26. Postman - Difficulty: Medium

- A Linux machine that focuses on exploiting a vulnerable API to gain initial access and escalate privileges.
- Skills: API exploitation, web application vulnerabilities, privilege escalation.

27. Mango - Difficulty: Medium

- A Linux machine that requires exploiting a vulnerable CMS and leveraging insecure file uploads.
- Skills: CMS vulnerabilities, file upload vulnerabilities, privilege escalation.

28. Traverxec - Difficulty: Medium

- A Linux machine that involves exploiting a vulnerable web application and misconfigured file permissions.
- Skills: Web exploitation, file permission issues, privilege escalation.

29. OpenAdmin - Difficulty: Medium

- A Linux machine that focuses on exploiting a vulnerable web application and manipulating sudo permissions.
- Skills: Web exploitation, command injection, privilege escalation.

30. Magic - Difficulty: Medium

- A Linux machine that requires exploiting a misconfigured DNS server and manipulating zone transfers.
- Skills: DNS enumeration, zone transfer, privilege escalation.

31. Admirer - Difficulty: Medium

- A Linux machine that involves exploiting a vulnerable web application and leveraging file upload vulnerabilities.
- Skills: Web exploitation, file upload vulnerabilities, privilege escalation.

32. Blunder - Difficulty: Medium

- A Linux machine that focuses on exploiting a vulnerable content management system and misconfigurations.
- Skills: CMS vulnerabilities, misconfigurations, privilege escalation.

33. Tabby - Difficulty: Medium

- A Linux machine that requires exploiting a vulnerable web application and manipulating server-side requests.
- Skills: Web exploitation, server-side request forgery, privilege escalation.

34. Doctor - Difficulty: Medium

- A Linux machine that involves exploiting a vulnerable web application and leveraging container technology.
- Skills: Web exploitation, container vulnerabilities, privilege escalation.

35. SneakyMailer - Difficulty: Medium

- A Linux machine that focuses on exploiting a vulnerable mail server to gain initial access.
- Skills: Mail server exploitation, email spoofing, privilege escalation.

36. Passage - Difficulty: Medium

- A Linux machine that requires exploiting a vulnerable web application and manipulating user input.
- Skills: Web exploitation, command injection, privilege escalation.

37. Luanne - Difficulty: Medium

- A Linux machine that involves exploiting a vulnerable PHP application and leveraging insecure file permissions.
- Skills: Web exploitation, PHP vulnerabilities, file permission issues.

38. Time - Difficulty: Medium

- A Linux machine that focuses on exploiting a vulnerable web application and leveraging time-based attacks.
- Skills: Web exploitation, SQL injection, time-based attacks.

39. Ready - Difficulty: Medium

- A Linux machine that requires exploiting a vulnerable web application and manipulating user input.
- Skills: Web exploitation, command injection, privilege escalation.

40. Delivery - Difficulty: Medium

- A Linux machine that involves exploiting a vulnerable web application and leveraging file upload vulnerabilities.
- Skills: Web exploitation, file upload vulnerabilities, privilege escalation.

41. Ophiuchi - Difficulty: Medium

- A Linux machine that focuses on exploiting a vulnerable web application and misconfigured file permissions.
- Skills: Web exploitation, file permission issues, privilege escalation.

42. ScriptKiddie - Difficulty: Medium

- A Linux machine that requires exploiting a vulnerable web application and manipulating user input.
- Skills: Web exploitation, command injection, privilege escalation.

43. Armageddon - Difficulty: Hard

- A Linux machine that involves exploiting a vulnerable web application and leveraging memory corruption vulnerabilities.
- Skills: Web exploitation, memory corruption vulnerabilities, privilege escalation.

- **44. Knife - Difficulty: Hard**
- A Linux machine that focuses on exploiting a vulnerable web application and leveraging misconfigured permissions.
- Skills: Web exploitation, misconfigurations, privilege escalation.

45. Pit - Difficulty: Hard

- A Linux machine that requires exploiting a vulnerable web application and manipulating user input.
- Skills: Web exploitation, command injection, privilege escalation.

46. Seal - Difficulty: Hard

- A Linux machine that involves exploiting a vulnerable web application and leveraging cryptography weaknesses.
- Skills: Web exploitation, cryptography, privilege escalation.

47. Previse - Difficulty: Hard

- A Linux machine that focuses on exploiting a vulnerable web application and leveraging command injection.
- Skills: Web exploitation, command injection, privilege escalation.

48. Forge - Difficulty: Hard

- A Linux machine that requires exploiting a vulnerable web application and manipulating user input.
- Skills: Web exploitation, command injection, privilege escalation.

49. Horizontall - Difficulty: Hard

- A Linux machine that involves exploiting a vulnerable web application and leveraging container technology.
- Skills: Web exploitation, container vulnerabilities, privilege escalation.

50. Shibboleth - Difficulty: Hard

- A Linux machine that focuses on exploiting a vulnerable SAML implementation and misconfigured permissions.
- Skills: SAML exploitation, misconfigurations, privilege escalation.

51. Writer - Difficulty: Hard

- A Linux machine that requires exploiting a vulnerable web application and manipulating user input.
- Skills: Web exploitation, command injection, privilege escalation.

52. Precise - Difficulty: Hard

- A Linux machine that involves exploiting a vulnerable web application and leveraging cryptography weaknesses.
- Skills: Web exploitation, cryptography, privilege escalation.

53. Academy - Difficulty: Hard

- A Linux machine that focuses on exploiting a vulnerable web application and leveraging misconfigured permissions.
- Skills: Web exploitation, misconfigurations, privilege escalation.

54. Ellingson - Difficulty: Hard

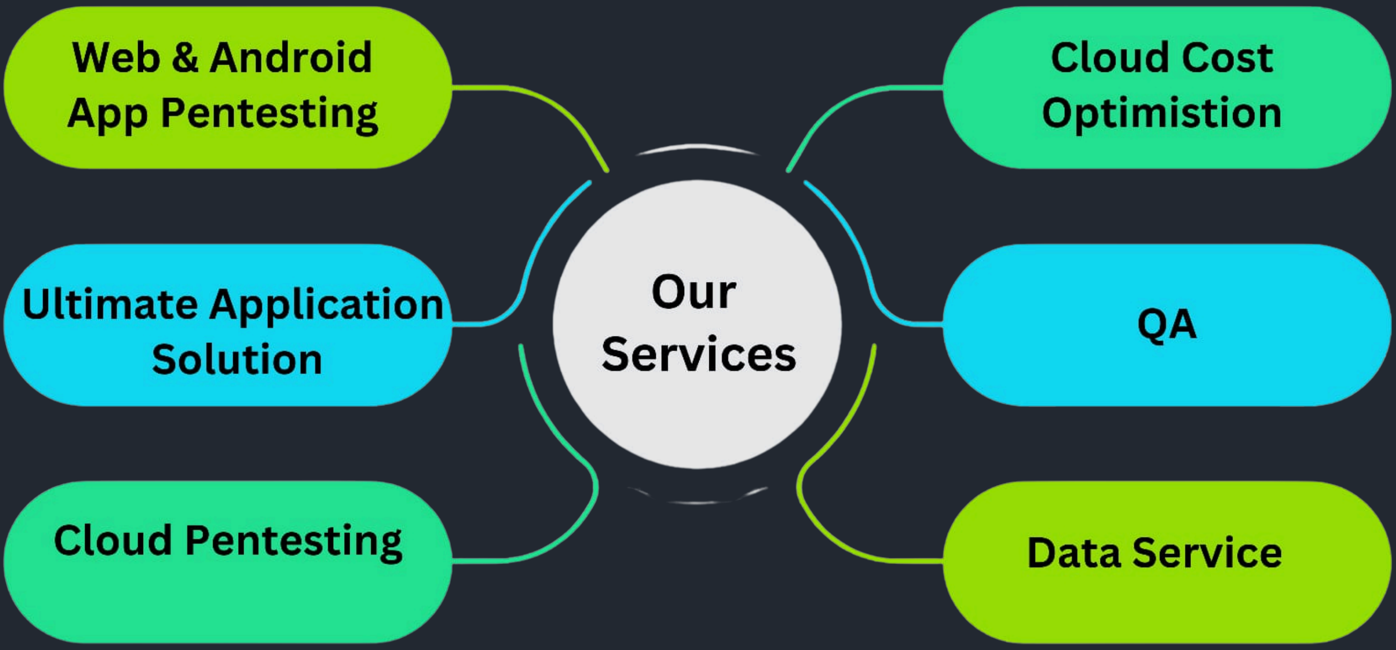
- A Linux machine that requires exploiting a vulnerable web application and manipulating user input.
- Skills: Web exploitation, command injection, privilege escalation.

55. Laboratory - Difficulty: Hard

- A Linux machine that involves exploiting a vulnerable web application and leveraging container technology.
- Skills: Web exploitation, container vulnerabilities, privilege escalation.

VULN SHIELDS

www.vulnshields.net



Our Services

Web & Android App Pentesting

Ultimate Application Solution

Cloud Pentesting

Cloud Cost Optimistion

QA

Data Service

Our Contact

☎ +91 9523917937

✉ admin@vulnshields.net

🌐 www.vulnshields.net

in linkedin.com/in/wh04m1i