Cyber Public School

Roadmap to Clear
OSCP

Linux Machines:

Linux Machines:

1. Lame - Difficulty: Easy
- **Description:** A beginner-friendly Linux machine that focuses on basicenumeration and exploiting common vulnerabilities.
- **Skills:** Basic Linux enumeration, vulnerable services (Samba), privilege escalation.

2. Brainfuck - Difficulty: Easy
- **Description:** A Linux machine that requires deciphering an encodedmessage to find the user and root flags.
-    **Skills:** Cryptography, enumeration, web exploitation.

3. Shocker - Difficulty: Easy
- **Description:** A Linux machine that targets a vulnerable CGI script to gaininitial access and escalate privileges.
-    **Skills:** Web exploitation, Bash command injection, privilege
     escalation.

4. Bashed - Difficulty: Easy
- **Description:** A Linux machine that involves exploiting a vulnerable webapplication and obtaining a reverse shell.
-    **Skills:** Web exploitation, command injection, reverse shell.

5. Nibbles - Difficulty: Easy
- **Description:** A Linux machine with a web application vulnerability that canbe exploited to gain initial access.
- **Skills:** Web exploitation, PHP deserialization, privilege escalation.

Linux Machines:

6. Beep - Difficulty: Easy
- **Description:** A Linux machine that focuses on exploiting a misconfiguredservice to gain initial access.
- **Skills:** Service enumeration, file permission issues, privilege escalation.

7. Cronos - Difficulty: Easy
- **Description:** A Linux machine that involves exploiting a misconfiguredpassword policy and a vulnerable service.
- **Skills:** Password cracking, service enumeration, privilege escalation.

8. Nineveh - Difficulty: Easy
- **Description:** A Linux machine with multiple avenues for exploitation,including a vulnerable CMS.
- **Skills:** Web exploitation, CMS vulnerabilities, privilege escalation.

9. Sense - Difficulty: Easy
- **Description:** A Linux machine that requires finding and exploiting a remotecode execution vulnerability.
- **Skills:** Web exploitation, command injection, reverse shell.

10. Solidstate - Difficulty: Easy
- **Description:** A Linux machine that focuses on exploiting a vulnerabledatabase and leveraging file permissions.
- **Skills:** Database exploitation, file permission issues, privilege escalation.

11. Node - Difficulty: Medium
- **Description:** A Linux machine that involves exploiting a Node.js applicationto gain access and escalate privileges.
- **Skills:** Node.js exploitation, JavaScript deserialization, privilege escalation.

12. Valentine - Difficulty: Medium
- **Description:** A Linux machine that requires exploiting a vulnerable webapplication to gain initial access.
- **Skills:** Web exploitation, PHP deserialization, privilege escalation.

13. Poison - Difficulty: Medium
- **Description:** A Linux machine that involves exploiting a vulnerable CMSand leveraging misconfigured permissions.
- **Skills:** CMS vulnerabilities, file permission issues, privilege escalation.

14. Sunday - Difficulty: Medium
- **Description:** A Linux machine that focuses on exploiting a vulnerable webapplication and manipulating file upload.
- **Skills:** Web exploitation, file upload vulnerabilities, privilege escalation.

15. Tartarsauce - Difficulty: Medium
- **Description:** A Linux machine that requires exploiting a remote codeexecution vulnerability in a custom web application.
- **Skills:** Web exploitation, command injection, privilege escalation.

Linux Machines:

16. Irked - Difficulty: Medium
- **Description:** A Linux machine that involves exploiting a vulnerable serviceand manipulating file permissions.
- **Skills:** Service enumeration, file permission issues, privilege escalation.

17. Friendzone - Difficulty: Medium
- **Description:** A Linux machine that focuses on exploiting a vulnerable webapplication and leveraging misconfigurations.
- **Skills:** Web exploitation, misconfigurations, privilege escalation.

18. Swagshop - Difficulty: Medium
- **Description:** A Linux machine that requires exploiting a vulnerablee-commerce platform and escalating privileges.
- **Skills:** Web exploitation, e-commerce vulnerabilities, privilege escalation.

19. Networked - Difficulty: Medium
- **Description:** A Linux machine that involves exploiting a misconfigured NFSshare to gain initial access.
- **Skills:** NFS enumeration, file permission issues, privilege escalation.

20. Jarvis - Difficulty: Medium
- **Description:** A Linux machine that focuses on exploiting a vulnerablesmart home automation system.
- **Skills:** IoT exploitation, home automation vulnerabilities, privilegeescalation.

Linux Machines:

21. Mirai - Difficulty: Medium
- **Description:** A Linux machine that requires exploiting IoT devices to gaininitial access and escalate privileges.
- **Skills:** IoT exploitation, botnets, privilege escalation.

22. Popcorn - Difficulty: Medium
- **Description:** A Linux machine that involves exploiting a vulnerable webapplication and manipulating database entries.
- **Skills:** Web exploitation, SQL injection, privilege escalation.

23. Haircut - Difficulty: Medium
- **Description:** A Linux machine that focuses on exploiting a vulnerable webapplication and privilege escalation.
- **Skills:** Web exploitation, command injection, privilege escalation.

24. Blocky - Difficulty: Medium
- **Description:** A Linux machine that requires exploiting a vulnerableMinecraft server plugin to gain access.
- **Skills:** Minecraft server vulnerabilities, Java deserialization, privilegeescalation.

25. Frolic - Difficulty: Medium
- **Description:** A Linux machine that involves exploiting a vulnerable webapplication and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

Linux Machines:

26. Postman - Difficulty: Medium
- **Description:** A Linux machine that focuses on exploiting a vulnerable APIto gain initial access and escalate privileges.
- **Skills:** API exploitation, web application vulnerabilities, privilege escalation.

27. Mango - Difficulty: Medium
- **Description:** A Linux machine that requires exploiting a vulnerable CMSand leveraging insecure file uploads.
- **Skills:** CMS vulnerabilities, file upload vulnerabilities, privilege escalation.

28. Traverxec - Difficulty: Medium
- **Description:** A Linux machine that involves exploiting a vulnerable webapplication and misconfigured file permissions.
- **Skills:** Web exploitation, file permission issues, privilege escalation.

29. OpenAdmin - Difficulty: Medium
- **Description:** A Linux machine that focuses on exploiting a vulnerable webapplication and manipulating sudo permissions.
- **Skills:** Web exploitation, command injection, privilege escalation.

30. Magic - Difficulty: Medium
- **Description:** A Linux machine that requires exploiting a misconfiguredDNS server and manipulating zone transfers.
- **Skills:** DNS enumeration, zone transfer, privilege escalation.

Linux Machines:

31. Admirer - Difficulty: Medium

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

32. Blunder - Difficulty: Medium

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

33. Tabby - Difficulty: Medium

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

34. Doctor - Difficulty: Medium

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

35. SneakyMailer - Difficulty: Medium

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

Linux Machines:

36. Passage - Difficulty: Medium
- **Description:** A Linux machine that requires exploiting a vulnerable webapplication and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

37. Luanne - Difficulty: Medium
- **Description:** A Linux machine that involves exploiting a vulnerable PHPapplication and leveraging insecure file permissions.
- **Skills:** Web exploitation, PHP vulnerabilities, file permission issues.

38. Time - Difficulty: Medium
- **Description:** A Linux machine that focuses on exploiting a vulnerable webapplication and leveraging time-based attacks.
- **Skills:** Web exploitation, SQL injection, time-based attacks.

39. Ready - Difficulty: Medium
- **Description:** A Linux machine that requires exploiting a vulnerable webapplication and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

40. Delivery - Difficulty: Medium
- **Description:** A Linux machine that involves exploiting a vulnerable webapplication and leveraging file upload vulnerabilities.
- **Skills:** Web exploitation, file upload vulnerabilities, privilege escalation.

Linux Machines:

41. Ophiuchi - Difficulty: Medium
- **Description:** A Linux machine that focuses on exploiting a vulnerable webapplication and misconfigured file permissions.
- **Skills:** Web exploitation, file permission issues, privilege escalation.

42. ScriptKiddie - Difficulty: Medium
- **Description:** A Linux machine that requires exploiting a vulnerable webapplication and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

43. Armageddon - Difficulty: Hard
- **Description:** A Linux machine that involves exploiting a vulnerable webapplication and leveraging memory corruption vulnerabilities.
- **Skills:** Web exploitation, memory corruption vulnerabilities, privilege escalation.

44. Knife - Difficulty: Hard
- **Description:** 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

- **Description:** 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

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

47. Previse - Difficulty: Hard

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

48. Forge - Difficulty: Hard

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

49. Horizontall - Difficulty: Hard

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

Linux Machines:

50. Shibboleth - Difficulty: Hard
- **Description:** A Linux machine that focuses on exploiting a vulnerable SAML implementation and misconfigured permissions.
- **Skills:** SAML exploitation, misconfigurations, privilege escalation.

51. Writer - Difficulty: Hard
- **Description:** 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
- **Description:** A Linux machine that involves exploiting a vulnerable webapplication and leveraging cryptography weaknesses.
- **Skills:** Web exploitation, cryptography, privilege escalation.

53. Academy - Difficulty: Hard
- **Description:** A Linux machine that focuses on exploiting a vulnerable webapplication and leveraging misconfigured permissions.
- **Skills:** Web exploitation, misconfigurations, privilege escalation.

54. Ellingson - Difficulty: Hard
- **Description:** A Linux machine that requires exploiting a vulnerable webapplication and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

Linux Machines:

55. Laboratory - Difficulty: Hard

- Description: A Linux machine that involves exploiting a vulnerable web application and leveraging container technology.

- Skills: Web exploitation, container vulnerabilities, privilege escalation.

Windows Machines:

1. Blue - Difficulty: Easy

- **Description:** A Windows machine that focuses on exploiting a vulnerable SMB service to gain initial access and escalate privileges.

- **Skills:** SMB enumeration, EternalBlue exploit, privilege escalation.

2. Devel - Difficulty: Easy

- **Description:** A Windows machine that involves exploiting a vulnerableFTP server and leveraging misconfigured permissions.

- **Skills:** FTP enumeration, file permission issues, privilege escalation.

3. Optimum - Difficulty: Easy

- **Description:** A Windows machine that requires exploiting a misconfigured service to gain initial access and escalate privileges.

- **Skills:** Service enumeration, Windows privilege escalation.

4. Bastard - Difficulty: Easy

- **Description:** A Windows machine that focuses on exploiting a vulnerable file share and manipulating file permissions.

- **Skills:** File share enumeration, file permission issues, privilege escalation.

Windows Machines:

5. Granny - Difficulty: Easy
- **Description:** A Windows machine that involves exploiting a vulnerableweb application and leveraging command injection.
- Skills: Web exploitation, command injection, privilege escalation.

6. Aragog - Difficulty: Easy
- **Description:** A Windows machine that requires exploiting a vulnerableweb application and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

7. Arctic - Difficulty: Easy
- **Description:** A Windows machine that focuses on exploiting a misconfigured Active Directory service and escalating privileges.
- **Skills:** Active Directory enumeration, Windows privilege escalation.

8. Jeeves - Difficulty: Easy
- **Description:** A Windows machine that involves exploiting a vulnerableweb application and leveraging file upload vulnerabilities.
- Skills: Web exploitation, file upload vulnerabilities, privilege escalation.

9. SwagShop - Difficulty: Easy
- **Description:** A Windows machine that requires exploiting a vulnerablee-commerce platform and escalating privileges.
- Skills: Web exploitation, e-commerce vulnerabilities, privilege escalation.

10. Bart - Difficulty: Easy
- **Description:** A Windows machine that focuses on exploiting a vulnerable backup service and manipulating file permissions.
- **Skills:** Backup service enumeration, file permission issues, privilege escalation.

11. Granny - Difficulty: Medium
- **Description:** A Windows machine that involves exploiting a vulnerable web application and leveraging command injection.
- **Skills:** Web exploitation, command injection, privilege escalation.

12. Redcross - Difficulty: Medium
- **Description:** A Windows machine that requires exploiting a vulnerable web application and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

13. BlueShadow - Difficulty: Medium
- **Description:** A Windows machine that focuses on exploiting a misconfigured Active Directory service and escalating privileges.
- **Skills:** Active Directory enumeration, Windows privilege escalation.

14. Celestial - Difficulty: Medium
- **Description:** A Windows machine that involves exploiting a vulnerable web application and leveraging file upload vulnerabilities.
- **Skills:** Web exploitation, file upload vulnerabilities, privilege escalation.

15. Nineveh - Difficulty: Medium
- **Description:** A Windows machine that requires exploiting a vulnerable web application and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

16. SolidState - Difficulty: Medium
- **Description:** A Windows machine that focuses on exploiting a vulnerable database and leveraging file permissions.
- **Skills:** Database exploitation, file permission issues, privilege escalation.

17. Bastard - Difficulty: Medium
- **Description:** A Windows machine that involves exploiting a vulnerable file share and manipulating file permissions.
- **Skills:** File share enumeration, file permission issues, privilege escalation.

18. Optimum - Difficulty: Medium
- **Description:** A Windows machine that requires exploiting a misconfigured service to gain initial access and escalate privileges.
- **Skills:** Service enumeration, Windows privilege escalation.

19. SecNotes - Difficulty: Medium
- **Description:** A Windows machine that focuses on exploiting a vulnerable note-taking application and leveraging insecure file permissions.
- **Skills:** Application exploitation, file permission issues, privilege escalation.

20. Bounty - Difficulty: Medium
- **Description:** A Windows machine that requires exploiting a vulnerable web application and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

21. Reel - Difficulty: Medium
- **Description:** A Windows machine that involves exploiting a vulnerable web application and leveraging file upload vulnerabilities.
- **Skills:** Web exploitation, file upload vulnerabilities, privilege escalation.

22. Love - Difficulty: Medium
- **Description:** A Windows machine that focuses on exploiting a misconfigured Active Directory service and escalating privileges.
- **Skills:** Active Directory enumeration, Windows privilege escalation.

23. Arkham - Difficulty: Medium
- **Description:** A Windows machine that requires exploiting a vulnerable web application and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

24. Bank - Difficulty: Medium
- **Description:** A Windows machine that involves exploiting a vulnerable banking application and leveraging insecure file permissions.
- **Skills:** Web exploitation, file permission issues, privilege escalation.

25. Ropme - Difficulty: Medium
- **Description:** A Windows machine that focuses on exploiting a vulnerable binary and leveraging Return-Oriented Programming (ROP).
- **Skills:** Binary exploitation, ROP, privilege escalation.

26. Remote - Difficulty: Medium
- **Description:** A Windows machine that requires exploiting a vulnerable web application and manipulating user input.
- Skills: Web exploitation, command injection, privilege escalation.

27. Valentine - Difficulty: Medium
- **Description:** A Windows machine that involves exploiting a vulnerable web application and leveraging misconfigured permissions.
- **Skills:** Web exploitation, misconfigurations, privilege escalation.

28. Falafel - Difficulty: Medium
- **Description:** A Windows machine that focuses on exploiting a vulnerable web application and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

29. Bastard - Difficulty: Hard
- **Description:** A Windows machine that requires exploiting a vulnerable file share and manipulating file permissions.
- **Skills:** File share enumeration, file permission issues, privilege escalation.

30. Optimum - Difficulty: Hard
- **Description:** A Windows machine that involves exploiting a misconfigured service to gain initial access and escalate privileges.
-     **Skills:** Service enumeration, Windows privilege escalation.

31. Blocky - Difficulty: Hard
- **Description:** A Windows machine that focuses on exploiting a vulnerable Minecraft server plugin to gain access.
-     **Skills:** Minecraft server vulnerabilities, Java deserialization, privilege escalation.

32. Granny - Difficulty: Hard
- **Description:** A Windows machine that involves exploiting a vulnerable web application and leveraging command injection.
-     **Skills:** Web exploitation, command injection, privilege escalation.

33. Celestial - Difficulty: Hard
- **Description:** A Windows machine that requires exploiting a vulnerable web application and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

34. Sizzle - Difficulty: Hard
- **Description:** A Windows machine that focuses on exploiting a vulnerable web application and leveraging file upload vulnerabilities.
- **Skills:** Web exploitation, file upload vulnerabilities, privilege escalation.

35. Blocky - Difficulty: Hard
- **Description:** A Windows machine that involves exploiting a vulnerable Minecraft server plugin to gain access.
- **Skills:** Minecraft server vulnerabilities, Java deserialization, privilege escalation.

36. Bounty - Difficulty: Hard
- **Description:** A Windows machine that requires exploiting a vulnerable web application and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

37. Traverxec - Difficulty: Hard
- **Description:** A Windows machine that focuses on exploiting a vulnerable content management system and misconfigurations.
- **Skills:** CMS vulnerabilities, misconfigurations, privilege escalation.

Windows Machines:

38. Doctor - Difficulty: Hard
- **Description:** A Windows machine that requires exploiting a vulnerable web application and manipulating user input.
- **Skills:** Web exploitation, command injection, privilege escalation.

39. Bastion - Difficulty: Hard
- **Description:** A Windows machine that involves exploiting a vulnerable web application and leveraging file upload vulnerabilities.
- **Skills:** Web exploitation, file upload vulnerabilities, privilege escalation.

40. Forest - Difficulty: Hard
- **Description:** A Windows machine that focuses on exploiting a misconfigured Active Directory service and escalating privileges.
- **Skills:** Active Directory enumeration, Windows privilege escalation.

Miscellaneous Machines:

Miscellaneous Machines:

1. Jeeves [Windows] -
Difficulty: Easy

2. Bart [Windows]
Difficulty: Easy

3. Tally [Windows]
Difficulty: Easy

4. Kotarak [Linux]
Difficulty: Easy

5. Falafel [Linux]
Difficulty: Easy

6. Devops [Linux]
Difficulty: Easy

7. Hawk [Linux]
Difficulty: Easy

8. Netmon [Windows]
Difficulty: Medium

9. Lightweight [Linux]
Difficulty: Medium

Miscellaneous Machines:

10. La Casa De Papel [Linux]
Difficulty: Medium

11. Jail [Linux]
Difficulty: Medium

12. Safe [Linux]
Difficulty: Medium

13. Bitlab [Linux]
Difficulty: Medium

14. Sizzle [Windows]
Difficulty: Medium

15. Sniper [Windows]
Difficulty: Medium

16. Control [Windows]
Difficulty: Medium

17. October [Linux]
Difficulty: Medium

18. Mango [Linux]
Difficulty: Medium

19. Nest [Windows]
Difficulty: Medium

Miscellaneous Machines:

20. Book [Linux]
Difficulty: Medium

21. Sauna [Windows]
Difficulty: Medium

22. Cascade [Windows]
- Difficulty: Medium

23. Querier [Windows]
Difficulty: Medium

24. Quick [Linux]
Difficulty: Medium

25. BlackField [Windows]
Difficulty: Medium

26. APT [Windows]
Difficulty: Medium

27. Atom [Windows]
Difficulty: Medium

28. BreadCrumbs [Windows]
Difficulty: Medium

29. Monitors [Linux]
Difficulty: Medium

Miscellaneous Machines:

30. Dynstr [Linux]
Difficulty: Medium

31. PivotAPI [Windows]
Difficulty: Medium

32. Pikaboo [Linux]
Difficulty: Medium

33. Monteverde [Windows]
Difficulty: Medium

34. Writer [Linux]
Difficulty: Medium

35. Forge [Linux]
Difficulty: Medium

36. Stacked [Linux]
Difficulty: Medium

37. Backdoor [Linux]
Difficulty: Hard

38. Search [Windows]
Difficulty: Hard

39. Undetected [Linux] (More like an IR box)
Difficulty: Hard

Active Directory Machines:

1. Forest
Difficulty: Medium

2. Sunna
Difficulty: Medium

3. Monteverde
Difficulty: Hard

4. Sizzle
Difficulty: Medium

5. Fuse
Difficulty: Hard

https://cyberpublicschool.com/