**🔒 Cyber Recon Tool :-**

**📌 What is this tool?**

The Cyber Recon Tool is a simple, beginner-friendly application that helps you gather useful information about websites and servers.  
It comes with an easy-to-use interface (no command line needed!) and is designed mainly for students, researchers, and ethical security testers.

Think of it as your digital magnifying glass — it gives you a clear picture of what’s running behind a website.

**🛠️ What can it do?**

**With just one click, the tool can:  
✅ Find the domain’s IP address  
✅ Run a DNS check (nslookup)  
✅ Pull WHOIS details (registrar info, expiry dates, etc.)  
✅ Look at the site’s SSL certificate  
✅ Scan common open ports (like FTP, SSH, HTTP, HTTPS, MySQL)  
✅ Collect HTTP headers  
✅ Detect technologies (like Apache, PHP, WordPress, etc.)  
✅ Grab banners from services (server greetings/version info)  
✅ Save everything into a PDF report  
✅ Send the report to your email**

**🚀 How to use it:-**

1. **Start the app**
   * Run CyberRecon.exe.
   * The main window will appear.
2. **Enter a target**
   * Type a website (e.g., amazon.in).
   * Click Run Recon.
3. **View results**
   * Results will show in the output box.
   * A neat PDF report is also saved in the reports folder.
4. **Send report by email :-**
   * Click Send Email Report.
   * **Enter:**
     + Your Gmail address
     + A Gmail App Password (explained below)
     + Recipient’s email
   * **The PDF report will be sent automatically.**
5. **Project info**
   * Click Project Info to read the included Project\_Info.pdf document.

**📄 What’s inside the report?**

**Each PDF gives you:**

* Target & Timestamp → Which domain was scanned and when.
* IP Address → The site’s IP address.
* nslookup Output → DNS resolution details.
* WHOIS Info → Who owns the domain, registrar, expiry, etc.
* SSL Certificate → Security certificate details, valid dates, and linked domains.
* Open Ports → Services found open (e.g., FTP, SSH, HTTP).
* HTTP Headers → Info shared by the web server.
* Technology Fingerprints → Guesses of the tech used (e.g., Apache, PHP, WordPress).
* Banner Grab → Raw greetings or version info from services.
* PDF Saved & Email Sent → Confirmation messages.

**📧 Sending reports via Gmail**

Google no longer allows normal passwords for apps like this. Instead, you need a special App Password.

**How to get one:**

1. **Log into your Gmail.**
2. **Go to Google Account → Security Settings.**
3. **Turn on 2-Step Verification.**
4. **Once that’s done, go to App Passwords.**
5. **Choose:**
   * **App → “Mail”**
   * **Device → “Other” → type CyberRecon**
6. **Click Generate.**
7. **Copy the 16-character password (example: abcd efgh ijkl mnop).**
8. **Paste it into the tool’s “App Password” field.**

**⚠️ Don’t use your normal Gmail password.  
⚠️ Keep your App Password safe — you can delete it anytime in your Google account.**

**📂 Files included**

* CyberRecon.exe → Main application
* bg.jpg → GUI background image
* Project\_Info.pdf → Documentation about the project
* README.md → This guide
* reports/ → Folder where reports are saved

**⚠️ Important note**

This tool is for learning and ethical security testing only.  
Never scan websites or servers that you don’t own or don’t have permission to test.  
The author is not responsible for misuse