CyberSwarm CLI - Quick Start Guide

Get up and running with CyberSwarm CLI in 5 minutes!

🚀 Quick Setup

Step 1: Get Your Gemini API Key

1. Visit https://makersuite.google.com/app/apikey
2. Sign in with your Google account
3. Click “Create API Key”
4. Copy your API key

Step 2: Configure CyberSwarm

Edit the `.env` file and add your API key:

```
nano .env
```

Replace `YOUR_GEMINI_API_KEY_HERE` with your actual API key:

```
GEMINI_API_KEY=AIzaSyC...your_actual_key_here...
```

Save and exit (Ctrl+X, Y, Enter)

Step 3: Install Dependencies (if not done)

```
npm install
```

Step 4: Build the Application (if not done)

```
npm run build
```

Step 5: Validate Configuration

```
npm run cyberswarm -- validate
```

You should see:

```
✓ Configuration is valid
✓ Gemini API key is set
```

🎯 Run Your First Simulation

Quick 30-Second Test

```
npm run cyberswarm -- start --target 192.168.1.0/24 --duration 30
```

Using a Pre-configured Scenario

```
npm run cyberswarm -- start --scenario basic-scan
```

What You'll See

The simulation will display:
- 🤖 **Agent Status**: All 5 agents and their current state
- 📊 **Recent Events**: Security events as they happen
- 📝 **Active Tasks**: What each agent is working on
- 🧠 **Chain of Thought**: AI reasoning for decisions

Press `Ctrl+C` to stop the simulation at any time.

📋 Available Commands

List Scenarios

```
npm run cyberswarm -- scenarios
```

Run Specific Scenario

```
npm run cyberswarm -- start --scenario full-pentest
```

Custom Duration

```
npm run cyberswarm -- start --duration 120  # 2 minutes
```

Save Results

```
npm run cyberswarm -- start --output ./my-results.json
```

Generate Report

```
npm run cyberswarm -- report -i ./my-results.json -o ./my-report.md
```

🎭 Try These Scenarios

1. Quick Network Discovery (30 seconds)

```
npm run cyberswarm -- start --scenario basic-scan --duration 30
```

2. Full Security Assessment (5 minutes)

```
npm run cyberswarm -- start --scenario full-pentest --duration 300
```

3. Defensive Operations (2 minutes)

```
npm run cyberswarm -- start --scenario defensive-only --duration 120
```

📊 Understanding the Output

Agent Types

- **Discovery Agent**: Finds targets and scans networks
- **Vulnerability Scanner**: Identifies security weaknesses
- **Patch Management**: Applies defensive measures
- **Network Monitor**: Detects intrusions
- **Strategy Adaptation**: Adapts attack tactics

Event Severity

- 🔴 **Critical**: Requires immediate attention
- 🟡 **High**: Important security findings
- 🔵 **Medium**: Notable events
- ⚪ **Low**: Informational

Agent Status

- 🟢 **IDLE**: Available for tasks
- 🟡 **BUSY**: Currently executing a task
- 🔴 **ERROR**: Encountered an error
- ⚪ **OFFLINE**: Not active

📁 Finding Your Results

After a simulation:
- **Logs**: `output/logs/simulation-*.json`
- **Reports**: `output/reports/report-*.md`
- **Exports**: `output/exports/simulation-*.json`

🔧 Common Issues

“GEMINI_API_KEY is required”

✅ Make sure you’ve set your API key in `.env`

Module Errors

✅ Run `npm run build` to compile TypeScript

Permission Errors

✅ Make sure you have write access to the `output/` directory

🎓 Next Steps

1. **Read the Full README**: Check `README.md` for detailed documentation
2. **Explore Scenarios**: Modify scenarios in `config/scenarios/`
3. **Check the CVE Database**: View `knowledge/cve-database.json`
4. **Analyze Reports**: Open generated markdown reports

💡 Tips

- Start with shorter durations (30-60 seconds) to understand the flow
- Use `--output` to save results for later analysis
- Check the logs directory for detailed information
- Each agent uses Gemini AI for intelligent decision-making

⚡ Quick Examples

Example 1: Quick Test

```
npm run cyberswarm -- start -t 10.0.0.0/24 -d 30
```

Example 2: Save Results

```
npm run cyberswarm -- start -s basic-scan -o ./test-$(date +%Y%m%d).json
```

Example 3: Full Workflow

```
# Run simulation
npm run cyberswarm -- start -s full-pentest -d 120 -o ./pentest.json

# Generate report
npm run cyberswarm -- report -i ./pentest.json -o ./pentest-report.md

# View report
cat ./pentest-report.md
```

🎉 You're Ready!

You now have a working multi-agent cybersecurity simulation platform powered by Google Gemini AI!

For more information, see:
- `README.md` - Full documentation
- `config/scenarios/` - Scenario configurations
- `knowledge/` - CVE database and threat intelligence

Happy Simulating! 🔒🚀