Skills Improvement Plan

## 🗓️ ****Daily Study Plan: 8 Weeks, ~2 Hrs/Day****

Each week has:

* 🧠 **Core Learning** (videos, articles, documentation)
* 🛠️ **Hands-on Practice**
* ✍  **Documentation/Reflection**
* 🧪 **Mini-projects or review**

### ✅ WEEK 1 – Python Foundations for Security

| Day | Focus | Time | Task |
| --- | --- | --- | --- |
| Mon | Python Basics | 2h | Watch first hour of [freeCodeCamp Python Course](https://www.youtube.com/watch?v=rfscVS0vtbw), follow along |
| Tue | Control Flow + Loops | 2h | Continue course, start writing basic scripts |
| Wed | Lists & Dictionaries | 2h | Parse a fake log file and print events |
| Thu | Functions & Error Handling | 2h | Build a reusable log-checking function |
| Fri | Working with Files | 2h | Write/read .log and .csv files |
| Sat | Mini Project | 2h | Build a “log monitor” script that alerts on bad login attempts |
| Sun | Optional catch-up or reflection | 1–2h | Document scripts, push to GitHub |

### ✅ WEEK 2 – AWS Cloud + Automation (Python + CLI)

| Day | Focus | Time | Task |
| --- | --- | --- | --- |
| Mon | AWS IAM, EC2, S3 basics | 2h | AWS SkillBuilder Cloud Practitioner review |
| Tue | AWS Security Services | 2h | Learn CloudTrail, Security Groups, GuardDuty |
| Wed | boto3 (Python AWS SDK) | 2h | Install boto3, list EC2s/S3s |
| Thu | Scripting audits | 2h | Script to detect public buckets or unencrypted volumes |
| Fri | Tools: Prowler or ScoutSuite | 2h | Run a scan and analyze results |
| Sat | Mini Project | 2h | Build AWS misconfig detection script |
| Sun | Optional review | 1–2h | Update GitHub, write project README |

### ✅ WEEK 3 – Splunk: Searching, Alerts, Dashboards

| Day | Focus | Time | Task |
| --- | --- | --- | --- |
| Mon | Splunk Intro + Setup | 2h | Install or access Splunk Free |
| Tue | SPL Basics | 2h | Practice searches (index=main, stats, eval) |
| Wed | Ingest Logs | 2h | Upload sample logs (syslog, auth.log, or AWS logs) |
| Thu | Alerts + Dashboards | 2h | Create alerts on failed logins or keyword matches |
| Fri | Security Content Repo | 2h | Pull a detection from [Splunk GitHub](https://github.com/splunk/security_content) |
| Sat | Mini Project | 2h | Build a mini threat detection dashboard |
| Sun | Optional: Splunk Fundamentals 1 exam | 1–2h | Take and complete the free training |

### ✅ WEEK 4 – Tenable/Nessus + Vulnerability Automation

| Day | Focus | Time | Task |
| --- | --- | --- | --- |
| Mon | Nessus Essentials Setup | 2h | Install Nessus, scan your local subnet or VM |
| Tue | Understand Plugins/CVEs | 2h | Analyze scan output, research one CVE |
| Wed | Tenable API intro | 2h | Try Tenable API calls in Postman or Python |
| Thu | Exporting Findings | 2h | Write a script to pull scan data (JSON/CSV) |
| Fri | Correlation w/ Threat Intel | 2h | Match CVEs or IPs against AbuseIPDB or Shodan |
| Sat | Mini Project | 2h | Build “Nessus Alert Summary” exporter (daily findings) |
| Sun | Reflect + push to GitHub | 1–2h | Write README, update project logs |

### ✅ WEEK 5 – CrowdStrike + Threat Hunting Concepts

| Day | Focus | Time | Task |
| --- | --- | --- | --- |
| Mon | CrowdStrike Overview | 2h | Watch Falcon UI demos + read docs |
| Tue | Detection Types | 2h | Learn how Falcon identifies threats (IOC/behavioral) |
| Wed | API Concepts | 2h | Read API docs or simulate queries with example data |
| Thu | Blue Team TTPs | 2h | MITRE ATT&CK mapping, hunting strategies |
| Fri | Splunk/Falcon Integration | 2h | Study [FDR → Splunk repo](https://github.com/CrowdStrike/FDR-splunk) |
| Sat | Mini Case Study | 2h | Analyze a public breach with CrowdStrike insights |
| Sun | Update portfolio | 1–2h | Add notes, scripts, or summaries to GitHub |

### ✅ WEEK 6 – Security Automation Projects

| Day | Focus | Time | Task |
| --- | --- | --- | --- |
| Mon | Pick Project 1 | 2h | Define: What problem does it solve? What tools? |
| Tue | Code Project 1 | 2h | Start scripting AWS, log, or vuln analysis tool |
| Wed | Polish & Test | 2h | Add error handling, logging, CLI args |
| Thu | Pick Project 2 | 2h | Example: Threat Intel → CSV tool |
| Fri | Code Project 2 | 2h | Add multithreading or multiple sources |
| Sat | Polish + README | 2h | Document clearly + screenshots |
| Sun | Reflect | 1–2h | What did you learn? Add to resume |

### ✅ WEEK 7 – Interview, Resume, Cert Prep

| Day | Focus | Time | Task |
| --- | --- | --- | --- |
| Mon | Resume Rebuild | 2h | Add projects, tools, metrics |
| Tue | LinkedIn Refresh | 2h | Update title, About section, posts |
| Wed | Interview Questions | 2h | Practice AWS/Python/Splunk scenarios |
| Thu | Mock Interview | 2h | Use ChatGPT or friend to simulate interview |
| Fri | Cert Prep (Optional) | 2h | AWS Cloud Practitioner or Splunk Core |
| Sat | Take practice tests | 2h | Time yourself, log weak areas |
| Sun | Relax + reflect | 1–2h | Prep for job hunt next week |

### ✅ WEEK 8 – Job Search + Networking Push

| Day | Focus | Time | Task |
| --- | --- | --- | --- |
| Mon | Build job tracker | 2h | Spreadsheet or Notion |
| Tue | Apply to 5+ jobs | 2h | Tailor resumes |
| Wed | Outreach | 2h | Message recruiters, post on LinkedIn |
| Thu | Interview prep | 2h | Deepen knowledge gaps |
| Fri | Apply to 5 more | 2h | Focus on growth-oriented roles |
| Sat | Rest or catch-up | Optional | Stay balanced |
| Sun | Reflect | 1–2h | Plan the next step forward |

## 🧩 Bonus Tools to Stay Organized

* ✅ [**Notion Template for Study Planning**](https://www.notion.so/) – I can create a version for you.
* ✅ **[Trello/Asana/ClickUp boards]** – Great for tracking progress visually.
* ✅ **[GitHub Projects or README Dashboard]** – List your active tools/projects + purpose.