# Progeta Technologies: Comprehensive Module Catalog

## Part 1: Technical Skill Modules (1–54)

### Category: Foundations & Operations

**1. Cybersecurity Fundamentals**

* **Goal:** Establish the foundational "Security Mindset" and understand the physics of data.
* **I. Core Concepts & Theory:** Data Physics (Rest/Transit/Use), Binary & Hexadecimal basics. The CIA Triad, AAA Framework, and Defense in Depth. The Risk Equation (Risk = Threat × Vulnerability). Zero Trust principles.
* **II. Tools & Tech Stack:** **VMware Workstation/VirtualBox** (Labs), **HashCalc** (Integrity), **VeraCrypt** (Encryption), **KeePassXC** (Identity).
* **III. Skills Gained:** Ability to set up a safe virtual lab. Understanding how to secure files via encryption/hashing. Articulating Risk vs. Threat.

**2. Linux Operations & Command Line**

* **Goal:** Master the OS of the internet (Linux) and move from GUI to CLI.
* **I. Core Concepts & Theory:** Kernel basics. File System Hierarchy (/root, /etc, /var). Permissions Model (Chmod/Chown). Package Management concepts.
* **II. Tools & Tech Stack:** **Kali Linux** & **Ubuntu**. **Bash** & **Zsh** (Shells). **Vim/Nano** (Editors). Core commands (grep, ssh, systemctl).
* **III. Skills Gained:** Navigation via CLI. User and permission management. Secure remote server connection via SSH.

**3. Computer Networking & TCP/IP**

* **Goal:** Understand how data moves across the internet to identify anomalies.
* **I. Core Concepts & Theory:** OSI Model vs. TCP/IP Model. IPv4/IPv6 Addressing & Subnetting. DNS resolution. The Three-Way Handshake. Common Ports (21, 22, 80, 443).
* **II. Tools & Tech Stack:** **Packet Tracer** (Simulation), **Ping**, **Traceroute**, **Netstat**, **Ncat**.
* **III. Skills Gained:** Troubleshooting connectivity issues. Reading network maps. Understanding how protocols handshake.

**4. Virtualization & Lab Setup**

* **Goal:** Build the infrastructure required to hack safely.
* **I. Core Concepts & Theory:** Type 1 vs. Type 2 Hypervisors. NAT vs. Bridged Networking. Snapshots and State Management. Sandbox isolation security.
* **II. Tools & Tech Stack:** **VMware Workstation**, **Oracle VirtualBox**, **Vagrant** (Basics).
* **III. Skills Gained:** Deploying Windows/Linux VMs. Configuring isolated virtual networks. Managing machine snapshots for recovery.

**5. Network Traffic Analysis**

* **Goal:** Develop the "Blue Team eye" to spot malicious patterns on the wire.
* **I. Core Concepts & Theory:** Deep Packet Inspection (DPI). Flow analysis. Identifying protocol anomalies. Baseline traffic vs. Malicious spikes.
* **II. Tools & Tech Stack:** **Wireshark**, **TCPDump**, **Zeek (Bro)**, **Brim**.
* **III. Skills Gained:** Capturing live traffic. Filtering noise from data. Identifying clear-text credential leaks.

**6. Packet Sniffing & Wireshark Mastery**

* **Goal:** Advanced usage of the world's primary network analysis tool.
* **I. Core Concepts & Theory:** Promiscuous Mode. Display Filters logic. TCP Stream reassembly. Extracting objects (files/images) from PCAP data.
* **II. Tools & Tech Stack:** **Wireshark** (Advanced), **TShark** (CLI), **NetworkMiner**.
* **III. Skills Gained:** Reconstructing files from captured traffic. Decrypting SSL traffic (with keys). Debugging complex network latency.

**7. SIEM Architecture & Deployment**

* **Goal:** Centralize security monitoring and visualize enterprise threats.
* **I. Core Concepts & Theory:** Log Aggregation. Normalization. Correlation Rules logic. Dashboarding. Alert Fatigue management.
* **II. Tools & Tech Stack:** **Splunk** (Free/Enterprise), **Wazuh** (Open Source), **ELK Stack** (Elasticsearch, Logstash, Kibana).
* **III. Skills Gained:** Ingesting logs from various sources. Writing basic correlation queries. Creating threat dashboards.

**8. Log Analysis & Management**

* **Goal:** The art of reading the "Black Box" of systems.
* **I. Core Concepts & Theory:** Windows Event IDs (Logon/Logoff/Failures). Linux Syslog hierarchy. Web Server Logs (Apache/IIS). Firewall Allow/Deny patterns.
* **II. Tools & Tech Stack:** **Splunk SPL**, **Grep/Awk** (Manual analysis), **Sysmon**.
* **III. Skills Gained:** Identifying Brute Force attacks in text logs. Tracking user activity across systems. Spotting persistence mechanisms.

**9. Incident Response Lifecycle**

* **Goal:** Structure the chaos of a cyberattack into a repeatable process.
* **I. Core Concepts & Theory:** NIST SP 800-61 (Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned). Triage levels (P1-P4).
* **II. Tools & Tech Stack:** **TheHive** (Case Management), **Cortex XSOAR** (Concepts), Ticket Systems (Jira).
* **III. Skills Gained:** Managing a security incident from start to finish. Documentation during crisis. Post-incident reporting.

**10. Playbook Design & Automation**

* **Goal:** Automate repetitive SOC tasks to focus on complex threats.
* **I. Core Concepts & Theory:** SOAR (Security Orchestration, Automation, and Response). Logic flows (If/Then). Standard Operating Procedures (SOPs).
* **II. Tools & Tech Stack:** **Shuffle** (Open Source SOAR), **Draw.io** (Flowcharts), **Ansible** (Basics).
* **III. Skills Gained:** Designing workflows for Phishing/Malware triage. Reducing Mean Time to Respond (MTTR).

**11. Endpoint Detection & Response (EDR)**

* **Goal:** Move beyond Antivirus to behavioral monitoring.
* **I. Core Concepts & Theory:** Signature-based vs. Behavioral detection. Host isolation. Telemetry data. Threat Hunting on the endpoint.
* **II. Tools & Tech Stack:** **CrowdStrike Falcon** (Concepts), **Wazuh Agent**, **Sysmon**, **Velociraptor**.
* **III. Skills Gained:** Deploying agents. Querying endpoint data for IOCs. Remotely isolating infected machines.

**12. Digital Forensics**

* **Goal:** Post-mortem analysis of systems to solve digital crimes.
* **I. Core Concepts & Theory:** Locard’s Exchange Principle. Order of Volatility. Deadbox vs. Live forensics. File Carving.
* **II. Tools & Tech Stack:** **Autopsy**, **FTK Imager**, **Volatility** (RAM Analysis), **Registry Viewer**.
* **III. Skills Gained:** Creating forensic images. Recovering deleted files. Analyzing Windows Registry for evidence.

**13. Evidence Handling & Chain of Custody**

* **Goal:** Ensure forensic findings hold up in a court of law.
* **I. Core Concepts & Theory:** Legal Admissibility. Integrity Hashing. Secure Storage. Documentation standards.
* **II. Tools & Tech Stack:** Hardware Write Blockers (Concepts), CoC Forms, Hashing Tools.
* **III. Skills Gained:** Proper seizure of digital devices. Maintaining a tamper-proof evidence log.

### Category: Offensive Security

**14. OSINT (Open Source Intelligence)**

* **Goal:** Gather intelligence from public sources before touching the target.
* **I. Core Concepts & Theory:** Passive vs. Active Recon. The OSINT Framework. Pivot points (Email -> Phone -> Location).
* **II. Tools & Tech Stack:** **Maltego**, **Shodan**, **Google Dorks**, **theHarvester**, **Wayback Machine**.
* **III. Skills Gained:** Building a profile on a target organization or individual. finding exposed assets.

**15. Digital Footprinting & Reconnaissance**

* **Goal:** Map the technical attack surface of an organization.
* **I. Core Concepts & Theory:** DNS Enumeration. Subdomain takeover concepts. Tech Stack identification. Email harvesting.
* **II. Tools & Tech Stack:** **Recon-ng**, **SpiderFoot**, **BuiltWith**, **DNSRecon**, **Amass**.
* **III. Skills Gained:** Mapping network ranges. Identifying used technologies (CMS/Frameworks).

**16. Dark Web Operations**

* **Goal:** Navigate the hidden web safely for intelligence gathering.
* **I. Core Concepts & Theory:** Onion Routing. Tor Network architecture. I2P. Cryptocurrency tracking. Threat Actor forums.
* **II. Tools & Tech Stack:** **Tor Browser**, **Tails OS**, **Kleopatra** (PGP).
* **III. Skills Gained:** Accessing .onion sites safely. Communicating via PGP encryption. Monitoring leak sites.

**17. Operational Security (OpSec) & Anonymity**

* **Goal:** Protect the researcher's identity during operations.
* **I. Core Concepts & Theory:** Attribution avoidance. Fingerprinting. Persona management. VPN vs. Proxy chains.
* **II. Tools & Tech Stack:** **ProtonVPN**, **Proxychains**, **User-Agent Switcher**, **Virtual Machines**.
* **III. Skills Gained:** Masking digital identity. Safe browsing habits. Preventing IP leaks.

**18. Network Scanning (Nmap/Masscan)**

* **Goal:** Active discovery of hosts and services.
* **I. Core Concepts & Theory:** TCP Connect vs. SYN Scan. UDP Scanning. Service Versioning. OS Fingerprinting logic.
* **II. Tools & Tech Stack:** **Nmap** (The Standard), **Masscan** (High speed), **Zenmap**.
* **III. Skills Gained:** Identifying live hosts. Mapping open ports and running services. Scripted scanning (NSE).

**19. Vulnerability Assessment**

* **Goal:** Identify known security flaws using automated tools.
* **I. Core Concepts & Theory:** CVEs (Common Vulnerabilities and Exposures). CVSS Scoring. False Positive verification. Authenticated vs. Unauthenticated scans.
* **II. Tools & Tech Stack:** **Nessus Essentials**, **OpenVAS**, **Greenbone**.
* **III. Skills Gained:** Configuring scan policies. Interpreting vulnerability reports. Prioritizing remediation.

**20. Web Application Security (OWASP Top 10)**

* **Goal:** Understand the most common flaws in modern web apps.
* **I. Core Concepts & Theory:** SQL Injection (SQLi). Cross-Site Scripting (XSS). IDOR. Broken Authentication. SSRF.
* **II. Tools & Tech Stack:** **OWASP Juice Shop** (Target), **DVWA**, **Browser DevTools**.
* **III. Skills Gained:** Identifying injection points. Understanding client-side vs. server-side attacks.

**21. Burp Suite Professional**

* **Goal:** Mastery of the industry-standard web hacking tool.
* **I. Core Concepts & Theory:** Intercepting Proxies. Request/Response manipulation. Fuzzing logic. Session handling.
* **II. Tools & Tech Stack:** **Burp Suite** (Proxy, Repeater, Intruder, Decoder), **FoxyProxy**.
* **III. Skills Gained:** Man-in-the-Middle of web traffic. Brute-forcing login forms. Automating payloads.

**22. System Hacking & Exploitation**

* **Goal:** Gaining access to a system using exploits.
* **I. Core Concepts & Theory:** Buffer Overflows (Intro). Shells (Bind vs. Reverse). Staged vs. Non-staged payloads.
* **II. Tools & Tech Stack:** **Metasploit Framework**, **Netcat**, **Exploit-DB**, **Searchsploit**.
* **III. Skills Gained:** Exploiting unpatched services. Generating payloads. Catching reverse shells.

**23. Privilege Escalation (Linux/Windows)**

* **Goal:** Moving from low-level user to Admin/Root.
* **I. Core Concepts & Theory:** Kernel Exploits. Sudo rights abuse. SUID binaries. Unquoted Service Paths. Token manipulation.
* **II. Tools & Tech Stack:** **LinPEAS**, **WinPEAS**, **GTFOBins**, **Mimikatz**.
* **III. Skills Gained:** Enumerating local system weakness. Elevating privileges to gain full control.

**24. Lateral Movement Techniques**

* **Goal:** Moving through a network after initial compromise.
* **I. Core Concepts & Theory:** Pivoting. Port Forwarding. Pass-the-Hash. SSH Tunneling. Living off the Land.
* **II. Tools & Tech Stack:** **Proxychains**, **PsExec**, **Impacket**, **Sshuttle**.
* **III. Skills Gained:** Routing traffic through compromised hosts. Accessing internal subnets.

**25. Active Directory Attacks**

* **Goal:** Compromising Windows Enterprise Networks.
* **I. Core Concepts & Theory:** Domain Controllers. Kerberos Authentication. NTLM. Group Policy. Tickets (TGT/TGS).
* **II. Tools & Tech Stack:** **BloodHound**, **PowerView**, **Rubeus**, **Responder**.
* **III. Skills Gained:** Mapping trust relationships. Kerberoasting. LLMNR Poisoning. Domain Admin compromise.

**26. Social Engineering Tactics**

* **Goal:** Hacking the human element.
* **I. Core Concepts & Theory:** Phishing. Vishing. Pretexting. Influence principles (Urgency, Authority). Physical security breaches.
* **II. Tools & Tech Stack:** **GoPhish**, **Social Engineering Toolkit (SET)**, **SpoofCard**.
* **III. Skills Gained:** Crafting convincing phishing campaigns. Cloning login pages. Awareness training.

**27. Malware Analysis Fundamentals**

* **Goal:** Safely dissecting malicious software to understand its behavior.
* **I. Core Concepts & Theory:** Static vs. Dynamic Analysis. Sandboxing. Packing/Obfuscation. Ransomware behavior.
* **II. Tools & Tech Stack:** **Cuckoo Sandbox**, **VirusTotal**, **PEStudio**, **Ghidra** (Basics).
* **III. Skills Gained:** Identifying malicious signatures. Running malware in safe environments. Extracting C2 domains.

**28. Indicators of Compromise (IoC) Discovery**

* **Goal:** Creating detection rules based on attack evidence.
* **I. Core Concepts & Theory:** The Pyramid of Pain. Types of IoCs (Hash, IP, Domain, TTPs). Pattern matching.
* **II. Tools & Tech Stack:** **YARA**, **Loki**, **IOC Editor**.
* **III. Skills Gained:** Writing YARA rules. Scanning systems for specific threat signatures.

### Category: DevSecOps & Code

**29. Python for Cybersecurity**

* **Goal:** Automating security tasks with custom code.
* **I. Core Concepts & Theory:** Syntax (Variables, Loops, Functions). Socket programming. HTTP Requests. Library usage.
* **II. Tools & Tech Stack:** **Python 3**, **Scapy**, **Requests**, **BeautifulSoup**.
* **III. Skills Gained:** Writing port scanners. Automating web requests. Parsing log files programmatically.

**30. Bash Scripting & Linux Automation**

* **Goal:** Leveraging the shell for speed and efficiency.
* **I. Core Concepts & Theory:** Shebang. Variables. Conditional Logic. Cron Jobs. Pipes and Redirection.
* **II. Tools & Tech Stack:** **Bash**, **Cron**, **Grep/Sed/Awk**.
* **III. Skills Gained:** Writing wrapper scripts. Automating recon tasks. Scheduling system audits.

**31. Secure Coding Practices**

* **Goal:** Writing code that is resistant to attack.
* **I. Core Concepts & Theory:** Input Validation. Output Encoding. Least Privilege. Error Handling. Parameterized Queries.
* **II. Tools & Tech Stack:** **OWASP Secure Coding Guidelines**, **SonarQube** (Concepts).
* **III. Skills Gained:** Fixing SQLi and XSS in code. Implementing secure authentication logic.

**32. Code Review & Static Analysis (SAST)**

* **Goal:** Finding bugs in code before it compiles.
* **I. Core Concepts & Theory:** SAST vs DAST. False Positive reduction. Secrets detection (Hardcoded keys).
* **II. Tools & Tech Stack:** **SonarQube**, **Snyk**, **Bandit**, **TruffleHog**.
* **III. Skills Gained:** Auditing codebases. Configuring automated scanning rules. Identifying logic bombs.

**33. Cloud Computing Fundamentals**

* **Goal:** Understanding the environment of modern infrastructure.
* **I. Core Concepts & Theory:** IaaS/PaaS/SaaS. Shared Responsibility Model. Regions & Availability Zones. VPCs.
* **II. Tools & Tech Stack:** **AWS Console** (Free Tier), **Azure Portal**.
* **III. Skills Gained:** Navigating cloud dashboards. Understanding cloud billing and resource management.

**34. Cloud Infrastructure Security (AWS/Azure)**

* **Goal:** Hardening cloud environments against misconfiguration.
* **I. Core Concepts & Theory:** IAM Roles & Policies. Security Groups. S3 Bucket permissions. Cloud Logging (CloudTrail).
* **II. Tools & Tech Stack:** **AWS IAM**, **AWS Inspector**, **ScoutSuite**, **Prowler**.
* **III. Skills Gained:** Auditing cloud accounts. Locking down public storage. Managing cloud identities.

**35. Container Security (Docker)**

* **Goal:** Securing microservices and containerized apps.
* **I. Core Concepts & Theory:** Container Isolation. Dockerfile security best practices. Distroless images. Registry trust.
* **II. Tools & Tech Stack:** **Docker**, **Docker Bench**, **Trivy**, **Clair**.
* **III. Skills Gained:** Scanning images for vulnerabilities. Writing secure Dockerfiles. Limiting container privileges.

**36. Kubernetes Security & Orchestration**

* **Goal:** Securing container orchestration at scale.
* **I. Core Concepts & Theory:** Pod Security. RBAC in K8s. Network Policies. Secrets Management. API Server security.
* **II. Tools & Tech Stack:** **Kubernetes (Minikube)**, **Kube-hunter**, **OPA (Open Policy Agent)**.
* **III. Skills Gained:** Auditing K8s clusters. Implementing network segmentation between pods.

**37. CI/CD Pipeline Security**

* **Goal:** Integrating security into the DevOps lifecycle (Shift Left).
* **I. Core Concepts & Theory:** The DevOps Loop. Automated Security Gates. Supply Chain Security. Artifact integrity.
* **II. Tools & Tech Stack:** **Jenkins**, **GitLab CI**, **OWASP Dependency Check**.
* **III. Skills Gained:** Building secure pipelines. Automating vulnerability scans on commit.

**38. API Security Testing**

* **Goal:** Securing the connective tissue of modern apps.
* **I. Core Concepts & Theory:** REST vs GraphQL. OWASP API Top 10. BOLA/IDOR. Rate Limiting. JWT Attacks.
* **II. Tools & Tech Stack:** **Postman**, **Burp Suite**, **KiteRunner**.
* **III. Skills Gained:** Testing API endpoints. Manipulating JSON tokens. Identifying logic flaws in APIs.

### Category: GRC & Strategy

**39. ISO 27001 Standards & Implementation**

* **Goal:** Understanding the global gold standard for InfoSec.
* **I. Core Concepts & Theory:** ISMS (Information Security Management System). PDCA Cycle. Annex A Controls. Policy writing.
* **II. Tools & Tech Stack:** **Documentation Templates**, **Compliance Tools**.
* **III. Skills Gained:** Drafting security policies. Preparing for external certification audits.

**40. NIST Cybersecurity Framework**

* **Goal:** Adopting the US standard for critical infrastructure protection.
* **I. Core Concepts & Theory:** The 5 Functions (Identify, Protect, Detect, Respond, Recover). NIST SP 800-53. Tier levels.
* **II. Tools & Tech Stack:** **NIST CSF Excel Tool**, **DHS CSET**.
* **III. Skills Gained:** Mapping controls to risks. Performing a gap analysis against NIST.

**41. Risk Management Strategies**

* **Goal:** Quantifying uncertainty and loss.
* **I. Core Concepts & Theory:** Risk Appetite vs. Tolerance. Qualitative vs. Quantitative Analysis. SLE/ALE. Risk Registers.
* **II. Tools & Tech Stack:** **Risk Heat Maps**, **Excel**.
* **III. Skills Gained:** Calculating financial risk. Prioritizing security investments based on ROI.

**42. Compliance Frameworks (GDPR/HIPAA/PCI-DSS)**

* **Goal:** Navigating the legal landscape of data protection.
* **I. Core Concepts & Theory:** Data Sovereignty. PII & PHI. Merchant Levels (PCI). Data Subject Rights.
* **II. Tools & Tech Stack:** **OneTrust** (Concepts), **Audit Checklists**.
* **III. Skills Gained:** Identifying regulated data. Ensuring systems meet legal privacy standards.

**43. Internal Auditing Procedures**

* **Goal:** Verifying that controls are actually working.
* **I. Core Concepts & Theory:** Audit Scope. Evidence Collection. Sampling. Reporting findings. Independence.
* **II. Tools & Tech Stack:** **AuditScripts**, **Evidence Repositories**.
* **III. Skills Gained:** Conducting stakeholder interviews. verifying technical controls. Writing audit reports.

**44. Third-Party Risk Management (TPRM)**

* **Goal:** Managing the risk of vendors and supply chains.
* **I. Core Concepts & Theory:** Vendor Due Diligence. SIG/CAIQ Questionnaires. SLAs. Right to Audit clauses.
* **II. Tools & Tech Stack:** **Vendor Assessment Templates**.
* **III. Skills Gained:** Evaluating vendor security posture. Negotiating security clauses in contracts.

**45. Cyber Warfare Tactics**

* **Goal:** Understanding the strategic landscape of nation-state conflict.
* **I. Core Concepts & Theory:** APTs (Advanced Persistent Threats). Critical Infrastructure targets. Disinformation. Cyber Espionage.
* **II. Tools & Tech Stack:** **MITRE ATT&CK Framework**.
* **III. Skills Gained:** Profiling nation-state actors. Understanding strategic cyber capabilities.

**46. Geopolitical Risk Analysis**

* **Goal:** analyzing how global events impact cyber threat levels.
* **I. Core Concepts & Theory:** Regional threat actors (Russia, China, etc.). Attribution problems. Sanctions and cyber response.
* **II. Tools & Tech Stack:** **Feedly** (Intel Aggregation), **Recorded Future** (Concepts).
* **III. Skills Gained:** Producing strategic threat briefings. Anticipating attacks based on world news.

### Category: Future Tech & AI

**47. AI for Defense (SOC Automation)**

* **Goal:** Leveraging AI to fight scale with scale.
* **I. Core Concepts & Theory:** Anomaly Detection. UEBA (User Entity Behavior Analytics). Supervised vs. Unsupervised Learning.
* **II. Tools & Tech Stack:** **Darktrace** (Concepts), **Splunk ML Toolkit**.
* **III. Skills Gained:** Configuring AI-driven alerts. Reducing false positives using ML.

**48. Adversarial AI (Attacking Models)**

* **Goal:** Understanding how to trick Artificial Intelligence.
* **I. Core Concepts & Theory:** Data Poisoning. Model Inversion. Evasion Attacks. Black Box vs White Box attacks.
* **II. Tools & Tech Stack:** **Adversarial Robustness Toolbox (ART)**, **Counterfit**.
* **III. Skills Gained:** Testing AI models for robustness. Understanding model vulnerabilities.

**49. LLM Security (Prompt Injection Defense)**

* **Goal:** Securing the new wave of Generative AI applications.
* **I. Core Concepts & Theory:** Prompt Injection (Jailbreaking). Data Leakage. OWASP Top 10 for LLMs.
* **II. Tools & Tech Stack:** **Garak**, **LangChain Security**.
* **III. Skills Gained:** Auditing LLM prompts. Preventing sensitive data exfiltration via AI.

**50. Quantum Cryptography Basics (Bonus)**

* **Goal:** Preparing for the "Q-Day" apocalypse.
* **I. Core Concepts & Theory:** Qubits. Shor’s Algorithm. Post-Quantum Cryptography (PQC). QKD.
* **II. Tools & Tech Stack:** **Qiskit** (IBM), **OpenQuantumSafe**.
* **III. Skills Gained:** Understanding the threat to RSA/ECC. Identifying crypto-agility needs.

**51. Blockchain Security (Bonus)**

* **Goal:** Securing Web3 and distributed ledgers.
* **I. Core Concepts & Theory:** Consensus (PoW/PoS). 51% Attacks. Private Keys/Wallets.
* **II. Tools & Tech Stack:** **MetaMask**, **Etherscan**, **Geth**.
* **III. Skills Gained:** analyzing blockchain transactions. Securing digital wallets.

**52. Smart Contract Auditing (Bonus)**

* **Goal:** Finding money-losing bugs in decentralized code.
* **I. Core Concepts & Theory:** Reentrancy Attacks. Integer Overflows. Flash Loans. Gas Optimization.
* **II. Tools & Tech Stack:** **Remix IDE**, **Slither**, **MythX**.
* **III. Skills Gained:** Auditing Solidity code. Identifying logic flaws in contracts.

**53. IoT Security Fundamentals (Bonus)**

* **Goal:** Securing the Internet of Things.
* **I. Core Concepts & Theory:** Edge Computing. MQTT/CoAP. Firmware security. Botnets (Mirai).
* **II. Tools & Tech Stack:** **Binwalk**, **Shodan**, **Wireshark**.
* **III. Skills Gained:** Extracting firmware. analyzing IoT network traffic.

**54. OT & SCADA Security (Bonus)**

* **Goal:** Protecting industrial control systems.
* **I. Core Concepts & Theory:** Purdue Model. PLCs & HMIs. Air Gapping. Modbus/DNP3.
* **II. Tools & Tech Stack:** **ScadaBR**, **GRFICS**.
* **III. Skills Gained:** Understanding industrial protocols. Recognizing safety system risks.

## Part 2: Soft Skill Modules (1–36)

### Category: Career & Branding

**1. Resume Building & Optimization**

* **Goal:** Creating a CV that passes the robots (ATS) and impresses humans.
* **I. Core Concepts & Theory:** ATS Logic. Keyword optimization. Action Verbs. Result-oriented bullets.
* **II. Tools & Tech Stack:** **Canva**, **Jobscan**, **LaTeX**.
* **III. Skills Gained:** Writing an ATS-compliant resume. Structuring technical experience effectively.

**2. Interview Preparation & Mock Sessions**

* **Goal:** Mastering the art of the interview.
* **I. Core Concepts & Theory:** STAR Method (Behavioral). Whiteboard coding logic. Salary negotiation basics.
* **II. Tools & Tech Stack:** **Pramp**, **Glassdoor**, **Voice Recorder**.
* **III. Skills Gained:** Answering "Tell me about yourself" confidently. Handling technical grilling.

**3. Personal Branding Strategy**

* **Goal:** Establishing a professional reputation in the industry.
* **I. Core Concepts & Theory:** Niche definition. Content strategy. Authority building. Consistency.
* **II. Tools & Tech Stack:** **Medium**, **Twitter/X**, **Personal Blog**.
* **III. Skills Gained:** creating technical content. Building an audience.

**4. LinkedIn Growth & Optimization**

* **Goal:** Turning a profile into an inbound lead generator.
* **I. Core Concepts & Theory:** SEO for Profiles. Headline engineering. Social Selling Index (SSI).
* **II. Tools & Tech Stack:** **LinkedIn Analytics**.
* **III. Skills Gained:** Creating an "All-Star" profile. Networking with recruiters.

**5. Portfolio Development**

* **Goal:** Proving skills through tangible work.
* **I. Core Concepts & Theory:** Documentation standards. GitHub structure. CTF Write-ups.
* **II. Tools & Tech Stack:** **GitHub**, **GitBook**, **WordPress**.
* **III. Skills Gained:** Showcasing code and projects. Writing technical guides.

**6. Professional Networking Strategies**

* **Goal:** Accessing the hidden job market.
* **I. Core Concepts & Theory:** Weak Ties theory. Informational Interviews. Cold outreach etiquette.
* **II. Tools & Tech Stack:** **Hunter.io**, **LinkedIn Sales Nav**.
* **III. Skills Gained:** expanding professional network. Getting referrals.

### Category: Communication

**7. Public Speaking**

* **Goal:** Delivering technical ideas with confidence.
* **I. Core Concepts & Theory:** Body language. Voice modulation. Story arcs. Handling Q&A.
* **II. Tools & Tech Stack:** **TED Talks**, **Toastmasters**.
* **III. Skills Gained:** Overcoming stage fright. Presenting to groups.

**8. Presentation Design**

* **Goal:** Creating slides that inform, not bore.
* **I. Core Concepts & Theory:** Visual Hierarchy. Data Viz best practices. "Death by PowerPoint" avoidance.
* **II. Tools & Tech Stack:** **PowerPoint**, **Canva**, **Prezi**.
* **III. Skills Gained:** Designing clean, professional decks. Summarizing complex data.

**9. Storytelling with Data (Bonus)**

* **Goal:** Making numbers emotional and memorable.
* **I. Core Concepts & Theory:** Narrative structure. Choosing correct charts. Guiding attention.
* **II. Tools & Tech Stack:** **Tableau Public**, **Google Data Studio**.
* **III. Skills Gained:** Creating compelling data narratives.

**10. Technical Writing**

* **Goal:** Writing clear, usable documentation.
* **I. Core Concepts & Theory:** Audience analysis. SOP structure. Conciseness. API Docs.
* **II. Tools & Tech Stack:** **Markdown**, **Confluence**, **Word**.
* **III. Skills Gained:** Writing Standard Operating Procedures. Documenting code.

**11. Report Writing for Executives**

* **Goal:** Translating tech risk into business language.
* **I. Core Concepts & Theory:** BLUF (Bottom Line Up Front). Executive Summaries. Risk Impact Matrices.
* **II. Tools & Tech Stack:** **Report Templates**.
* **III. Skills Gained:** Writing pentest executive summaries. Justifying budgets.

**12. Email Etiquette & Corporate Messaging (Bonus)**

* **Goal:** Professional written communication.
* **I. Core Concepts & Theory:** Tone. Clarity. Call to Action. Reply All etiquette.
* **II. Tools & Tech Stack:** **Grammarly**.
* **III. Skills Gained:** Writing effective business emails.

**13. Cross-Cultural Communication (Bonus)**

* **Goal:** Working effectively in global teams.
* **I. Core Concepts & Theory:** High vs. Low Context. Feedback styles. Time perception.
* **II. Tools & Tech Stack:** **The Culture Map**.
* **III. Skills Gained:** Navigating cultural differences in remote teams.

**14. Negotiation Skills**

* **Goal:** Getting what you want without burning bridges.
* **I. Core Concepts & Theory:** BATNA. Win-Win strategies. Anchoring.
* **II. Tools & Tech Stack:** **Levels.fyi** (Salary data).
* **III. Skills Gained:** Negotiating salaries. Securing budget approvals.

**15. Persuasion & Influence**

* **Goal:** Influencing without authority.
* **I. Core Concepts & Theory:** Cialdini’s 6 Principles. Stakeholder Management.
* **II. Tools & Tech Stack:** **Stakeholder Maps**.
* **III. Skills Gained:** Getting buy-in for security initiatives.

### Category: Cognitive & Decisions

**16. Critical Thinking**

* **Goal:** Analyzing information objectively.
* **I. Core Concepts & Theory:** First Principles. Socratic Method. Correlation vs. Causation.
* **II. Tools & Tech Stack:** **Mind Mapping**.
* **III. Skills Gained:** Questioning assumptions. Validating evidence.

**17. Analytical Problem Solving**

* **Goal:** Systematically solving complex issues.
* **I. Core Concepts & Theory:** Root Cause Analysis. 5 Whys. Fishbone Diagrams.
* **II. Tools & Tech Stack:** **SWOT Analysis**.
* **III. Skills Gained:** Debugging complex failures. finding root causes.

**18. Strategic Decision Making**

* **Goal:** Making choices under uncertainty.
* **I. Core Concepts & Theory:** OODA Loop. Decision Trees. Risk-based choices.
* **II. Tools & Tech Stack:** **Decision Matrices**.
* **III. Skills Gained:** Making fast, accurate decisions in a crisis.

**19. Cognitive Biases & Fallacies**

* **Goal:** Identifying flaws in reasoning.
* **I. Core Concepts & Theory:** Confirmation Bias. Sunk Cost. Availability Heuristic. Dunning-Kruger.
* **II. Tools & Tech Stack:** **Bias Cheat Sheets**.
* **III. Skills Gained:** Avoiding mental traps during investigations.

**20. Systems Thinking**

* **Goal:** Seeing the big picture.
* **I. Core Concepts & Theory:** Feedback loops. Second-order effects. Holistic views.
* **II. Tools & Tech Stack:** **Causal Loop Diagrams**.
* **III. Skills Gained:** Understanding how changes affect the whole ecosystem.

**21. Creative Innovation**

* **Goal:** Solving problems in novel ways.
* **I. Core Concepts & Theory:** Lateral Thinking. SCAMPER. Divergent thinking.
* **II. Tools & Tech Stack:** **Whiteboarding**.
* **III. Skills Gained:** Bypassing security controls creatively.

### Category: Management & Business

**22. Time Management & Productivity**

* **Goal:** Maximizing output and focus.
* **I. Core Concepts & Theory:** Pomodoro. Eisenhower Matrix. Deep Work.
* **II. Tools & Tech Stack:** **Trello/Notion**, **Focus Timers**.
* **III. Skills Gained:** Prioritizing tasks. Managing interruptions.

**23. Agile Methodologies**

* **Goal:** Working at the speed of modern dev.
* **I. Core Concepts & Theory:** Scrum. Kanban. Sprints. User Stories.
* **II. Tools & Tech Stack:** **Jira**, **Kanban Boards**.
* **III. Skills Gained:** Participating in stand-ups. Working in sprints.

**24. Project Management Basics**

* **Goal:** Delivering projects on time and budget.
* **I. Core Concepts & Theory:** Scope. Timeline. Critical Path. Gantt Charts.
* **II. Tools & Tech Stack:** **Asana**, **MS Project**.
* **III. Skills Gained:** Managing security projects. Tracking progress.

**25. Business Acumen for Tech Pros**

* **Goal:** Understanding the business engine.
* **I. Core Concepts & Theory:** ROI. EBITDA. Profit & Loss. Strategic alignment.
* **II. Tools & Tech Stack:** **Annual Reports**.
* **III. Skills Gained:** Speaking the language of business.

**26. Financial Literacy**

* **Goal:** Managing money and budgets.
* **I. Core Concepts & Theory:** CAPEX vs OPEX. ROSI (Return on Security Investment).
* **II. Tools & Tech Stack:** **Budget Templates**.
* **III. Skills Gained:** Creating security budgets. Calculating ROI.

**27. Change Management**

* **Goal:** Guiding organizations through transition.
* **I. Core Concepts & Theory:** ADKAR Model. Resistance management. Communication planning.
* **II. Tools & Tech Stack:** **Impact Assessments**.
* **III. Skills Gained:** Implementing new policies smoothly.

**28. Crisis Management**

* **Goal:** Leading through disaster.
* **I. Core Concepts & Theory:** Incident Command System (ICS). Reputation management.
* **II. Tools & Tech Stack:** **Tabletop Exercises**.
* **III. Skills Gained:** Managing communication during a breach.

### Category: EQ & Leadership

**29. Emotional Intelligence (EQ) (Bonus)**

* **Goal:** Managing self and others emotionally.
* **I. Core Concepts & Theory:** Self-Awareness. Self-Regulation. Empathy. Social Skills.
* **II. Tools & Tech Stack:** **EQ Assessments**.
* **III. Skills Gained:** Handling high-stress emotions.

**30. Empathy in the Workplace (Bonus)**

* **Goal:** Understanding user and team needs.
* **I. Core Concepts & Theory:** Cognitive vs Emotional Empathy. Psychological Safety.
* **II. Tools & Tech Stack:** **Empathy Maps**.
* **III. Skills Gained:** Building trust with teams.

**31. Conflict Resolution**

* **Goal:** Resolving disputes constructively.
* **I. Core Concepts & Theory:** Active Listening. De-escalation. Mediation.
* **II. Tools & Tech Stack:** **TKI Model**.
* **III. Skills Gained:** Mediating team conflicts.

**32. Team Collaboration Dynamics**

* **Goal:** Working well with others.
* **I. Core Concepts & Theory:** Psychological Safety. Remote etiquette.
* **II. Tools & Tech Stack:** **Slack/Teams**.
* **III. Skills Gained:** Collaborating cross-functionally.

**33. Stress Management & Resilience**

* **Goal:** Preventing burnout.
* **I. Core Concepts & Theory:** Burnout recognition. Detachment. Boundaries.
* **II. Tools & Tech Stack:** **Mindfulness apps**.
* **III. Skills Gained:** Maintaining mental health in Ops.

**34. Leadership Fundamentals**

* **Goal:** Inspiring and guiding others.
* **I. Core Concepts & Theory:** Servant Leadership. Delegation. Feedback loops.
* **II. Tools & Tech Stack:** **360 Feedback**.
* **III. Skills Gained:** Leading small teams.

**35. Mentorship Skills (Bonus)**

* **Goal:** Growing the next generation.
* **I. Core Concepts & Theory:** Mentor-Mentee lifecycle. Socratic questioning.
* **II. Tools & Tech Stack:** **GROW Model**.
* **III. Skills Gained:** Mentoring juniors effectively.

**36. Workplace Ethics & Integrity**

* **Goal:** Maintaining professional standards.
* **I. Core Concepts & Theory:** Code of Conduct. Whistleblowing. Grey areas.
* **II. Tools & Tech Stack:** **Case Studies**.
* **III. Skills Gained:** Navigating ethical dilemmas.