PRE–NEW TO PURPLE TEAM EDUCATION PATHWAY (TEXT-ONLY EDITION)

Zero-cost. No videos. Beginner-safe. Purple Team–Ready.

Table of Contents

1

Stage 0 — Cyber & Security Foundations (Text-Based)

Goal: Build basic understanding of cybersecurity concepts, vocabulary, threats, and operations.

1. Cisco – Introduction to Cybersecurity (FREE)

https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=en-US

- Threat types
- Cyber hygiene
- Security concepts
- Fully text-based quizzes and modules

2. IBM SkillsBuild – Cybersecurity Fundamentals (FREE)

https://skillsbuild.org

- Security principles
- Threat behaviors
- SOC basics
- All delivered via text lessons and labs

3. Fortinet FCA & FCN (FREE)

https://training.fortinet.com

- Threat landscape
- Security basics
- Foundational terminology

Stage 1 — Networking Foundations (Text-Only)

Goal: Understand IPs, ports, packets, routing, and network behaviors.

1. Cisco Networking Essentials (FREE)

https://www.netacad.com/courses/networking-essentials?courseLang=en-US

- Subnetting
- Routing
- Switching
- Protocols
- Packet Tracer text labs

2. Microsoft Learn – Networking Fundamentals (FREE)

https://learn.microsoft.com

Search: “Networking Fundamentals”

- OSI model
- IPv4/IPv6
- Network security basics

3. Subnetting Practice (Interactive Text-Based)

https://subnettingpractice.com

- Auto-generated practice
- No videos or lectures

Stage 2 — Operating System Fundamentals (Text-Based)

Goal: Get comfortable with Linux + Windows—the systems attackers and defenders interact with.

1. Linux Journey (FREE)

https://linuxjourney.com

- CLI basics
- File systems
- Permissions

2. OverTheWire Wargames (FREE)

https://overthewire.org/wargames

Start: **Bandit**

- Linux basics through puzzles

3. Microsoft Learn – Windows Security Fundamentals

https://learn.microsoft.com

Search: “Windows Security”

- Logs
- Windows Event Viewer
- Local security

Stage 3 — Log Analysis & SIEM Fundamentals

Goal: Understand how defenders detect attacks.

1. Splunk Work+ (FREE)

https://workplus.splunk.com
- Search commands
- Log parsing
- Investigations

2. Elastic SIEM Documentation

https://www.elastic.co/guide
Search: “Elastic Security”
- Detection rules
- Alerts
- Response

3. MITRE D3FEND

https://d3fend.mitre.org
- Defensive techniques
- Countermeasures

Stage 4 — Offensive Basics (Text-Only)

Goal: Learn attacker behavior safely before Purple Teaming.

1. HackTheBox Academy – Free Text Modules

https://academy.hackthebox.com
Free modules:
- Intro to Networking
- Intro to Pentesting
- Web Requests

2. TryHackMe (Text-Driven Free Rooms)

https://tryhackme.com
Rooms to use:
- Intro to Cybersecurity

- Intro to Pentesting
- Basic Malware Analysis

3. MITRE ATT&CK (Enterprise Matrix)

https://attack.mitre.org
- Techniques
- Tactics
- Real threat mappings

Stage 5 — Threat Intelligence Foundations

Goal: Learn real adversary behavior and map it to MITRE ATT&CK.

1. CISA Cybersecurity Advisories (FREE)

https://www.cisa.gov/news-events/cybersecurity-advisories
- Real-world threats
- Alerts
- TTPs

2. CrowdStrike Adversary Library

https://www.crowdstrike.com/adversaries
- Threat groups
- Known TTPs

3. Recorded Future Free TI Resources

https://www.recordedfuture.com
Search: “Threat Intelligence Resources”

Stage 6 — Hands-On Purple Preparation (Text-Based Projects)

Goal: Build foundational detection + attack simulation skills.

Project 1 — Build a Mini Detection Lab

Tools: VirtualBox, Security Onion, Windows VM
Practice:
- Capture logs

- Analyze Windows events
- Identify suspicious processes

Project 2 — Atomic Red Team Test (Text-Based)

https://github.com/redcanaryco/atomic-red-team
- Run one atomic test
- Observe logs
- Write detection notes

Project 3 — Detection Notebook

Document findings:
- PowerShell commands
- Failed logins
- Process creation
- Network connections

Project 4 — MITRE Technique Mapping

Pick a technique (e.g., T1059). Document:
- What it does
- Logs produced
- How to detect it

Stage 7 — Graduation: Ready for the Purple Team Manual

After completing Stages 0–6, the learner is fully prepared to begin: - ATT&CK-driven testing
- Purple Team scenarios
- Gap analysis
- Detection engineering
- Threat emulation workflows

This ensures confidence and capability before entering the full “New to Purple Team Field Manual.”