Pre–Pre New to Purple Team Education Pathway (Red Team Focused)

A comprehensive, beginner-safe, text-based introduction to ethical offensive security

All free resources • No videos • Foundation for Red → Purple progression

---

Table of Contents

Purpose of This Pathway

This curriculum prepares absolute beginners for safe, ethical offensive security learning **before** stepping into Purple Teaming.

By the end of this pathway, learners will: - Understand attacker concepts and terminology - Navigate Linux & Windows for offensive operations - Perform basic enumeration and recon - Understand vulnerabilities and common attack paths - Build a mindset for adversary emulation

This is the offensive equivalent to your Blue Team pre-pathway.

SECTION 1 — Offensive Security Foundations

1.1 Understanding the Red Team Mindset (Text-Based)

MITRE ATT&CK — Enterprise Matrix

https://attack.mitre.org

- Tactic flow (Initial Access → Impact)
- Technique categories
- Real-world adversary procedures

CISA Threat Actor Summaries

https://www.cisa.gov/news-events/cybersecurity-advisories

- Ransomware TTPs
- Nation-state activity overviews
- Behavior-based mapping

OWASP Top 10

https://owasp.org

- Web vulnerabilities explained in plain text
- Common exploitation patterns

Red Team Reasoning: Offensive understanding starts with how attackers move, think, and chain vulnerabilities.

SECTION 2 — Operating Systems for Attackers

2.1 Linux for Offense

Linux Journey

https://linuxjourney.com

- Shell basics
- Permissions (critical for privilege escalation)
- Processes & system navigation

OverTheWire — Bandit

https://overthewire.org/wargames/bandit

- Safe exploitation-style challenges
- Teaches command chaining, enumeration, decoding

2.2 Windows for Offense

Microsoft Learn – Windows Security Fundamentals

https://learn.microsoft.com Search: *Windows Security*

- Event logs (know what defenders see)
- Processes & services

Sysinternals Documentation

https://learn.microsoft.com/sysinternals

- Process Explorer
- Sysmon basics
- Core forensic artifacts

Red Team Reasoning: Attackers who understand Windows/Linux internals build better simulations.

SECTION 3 — Core Offensive Concepts (Text-Only)

3.1 Reconnaissance & Enumeration

HackTheBox Academy – Free Text Modules

https://academy.hackthebox.com Use free modules:

- Intro to Pentesting
- Network Enumeration
- Web Requests

TryHackMe — Free Written Rooms

https://tryhackme.com Use rooms:

- Intro to Pentesting
- Basic Pentesting
- Vulnerabilities 101

3.2 Understanding Vulnerabilities (Text-Based)

NIST National Vulnerability Database (NVD)

https://nvd.nist.gov

- CVE browsing
- CVSS scoring

Exploit Mitigations (MITRE D3FEND)

https://d3fend.mitre.org

- Understand defender countermeasures

Red Team Reasoning: Offense requires strong knowledge of how vulnerabilities work and how defenders counter them.

SECTION 4 — Beginner Offensive Techniques (Safe & Text-Based)

4.1 Basic Attack Vectors

OWASP Web Security Testing Guide (WSTG)

https://owasp.org/www-project-web-security-testing-guide/

- Input validation flaws
- Authentication issues
- Logic weaknesses

IRED.TEAM (Red Team Notes)

https://www.ired.team

- Windows internals for offense
- Command execution basics
- Privilege escalation theory

4.2 Password & Access Concepts

Red Team Password Attacks (Theory)

https://attack.mitre.org/techniques/T1110

Credential guessing

Hash attacks

OS credential access

Kerberos & AD Basics (Docs Only)

https://learn.microsoft.com Search: *Active Directory Fundamentals*

Red Team Reasoning: Even without hands-on exploitation, knowledge of attack surfaces builds offensive intuition.

SECTION 5 — Introductory Labs & Exercises (Text Only)

Project 1 — Enumeration Drill

Using only documentation and a Linux VM:

- Explore `/etc/passwd`, `/etc/shadow`
- List running processes
- Document potential weaknesses

Project 2 — Web Attack Surface Mapping

Pick any public website and document:

- Visible endpoints
- Parameters
- Cookies
- Headers

(No exploitation — only recon.)

Project 3 — MITRE Technique Breakdown

Pick one technique (e.g., T1059, T1047).

Document:

- Offense: what the attacker does
- Defense: what logs it generates
- Gaps: what might defenders miss

Project 4 — Create an Adversary Card

Using ATT&CK: - Pick an APT group

Document 3–5 techniques

Map their lifecycle

Identify their goals

SECTION 6 — Red Team Readiness Check

Before moving to the Pre–New to Purple Team Pathway, learners should be able to:

- Explain attacker tactics and techniques
- Navigate Linux comfortably
- Perform safe enumeration & recon
- Interpret Windows artifacts
- Understand basic privilege escalation concepts
- Read ATT&CK pages fluently

Completion Outcome

After completing this Red Team–focused Pre–Pre Pathway, learners will:

- Understand attacker logic & methodology
- Build safe foundational offensive skills
- Become familiar with enumeration, recon, and exploit theory
- Be ready to move into the **Pre–New to Purple Team Pathway**
- Be positioned to begin adversary emulation within the Purple Team Field Manual

This path ensures a **safe, ethical, foundational approach** to offensive security before deeper Red or Purple operations.