New to Purple Team Field Manual

Your Beginner-Friendly Guide to Becoming an Effective Purple Teamer

Table of Contents

1. Introduction: What Is Purple Teaming?

Purple Teaming is the collaborative fusion of **Red Team (offense)** and **Blue Team (defense)** operations. The goal is not competition—it is **continuous improvement** of an organization's security posture.

If you are new, think of Purple Teaming as: - Learning **how attackers think** (Red) - Learning **how defenders detect & respond** (Blue) - **Bridging the two** to strengthen real-world defense

Purple Teaming = *attack* + *detect* + *improve*.

---

2. Core Skills You Will Build

Purple Teaming covers multiple technical and analytical domains:

✓ Red-Side Skills

- Adversary emulation
- MITRE ATT&CK mapping
- Exploitation fundamentals
- Post-exploitation behaviors

✓ Blue-Side Skills

- SIEM operations (Splunk, ELK)
- Log analysis
- Detection engineering
- Incident response fundamentals

✓ Purple-Side Skills

- Running collaborative exercises
- Scenario building
- Reporting improvements
- SOC + Red Team alignment

---

3. Essential Frameworks for Purple Teaming

🔹 MITRE ATT&CK

The single most important framework to understand attacker behaviors.

Link: https://attack.mitre.org

🔹 D3FEND (Defensive Techniques Framework)

MITRE’s defensive counterpart to ATT&CK.

Link: https://d3fend.mitre.org

🔹 NIST 800-53 / 800-61

- 800-53 = Security Controls
- 800-61 = Incident Response Guide

Links:

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

---

4. Purple Team Workflow (Simple Model)

1. **Choose a Threat** → Select an adversary (APT29, ransomware, insider threat).
2. **Map to MITRE ATT&CK** → Identify tactics/techniques.
3. **Build Test Scenarios** → Turn techniques into actions.
4. **Run Red Actions** → Execute attacks safely.
5. **Monitor & Detect** → Blue Team attempts detection.
6. **Document Gaps** → What worked? What failed?
7. **Improve Controls** → Tune detection, alerts, SIEM, firewall rules.

Purple Teaming is **iterative**—you repeat and refine continuously.

---

5. Tools for New Purple Teamers

🔧 Red Team Tools (Beginner-Friendly)

- **Atomic Red Team:** Small tests mapped to ATT&CK
    - https://github.com/redcanaryco/atomic-red-team

- **MITRE CALDERA:** Automated adversary emulation
  - https://caldera.mitre.org
- **AttackIQ Academy** (free training)
  - https://academy.attackiq.com

🔧 Blue Team Tools

- **Splunk Boss of the SOC (BOTS)** Resources
  - https://www.splunk.com/en_us/blog/security/splunk-bots.html
- **Wireshark** (packet analysis)
  - https://www.wireshark.org
- **Security Onion** (full SOC in a box)
  - https://securityonion.net

🔧 Purple Team Tools

- **PurpleSharp (Windows attack sim)**
  - https://github.com/mvelazc0/PurpleSharp
- **Prelude Operator (ATT&CK-driven testing)**
  - https://www.prelude.org
- **Open-source Threat Emulation Resources**
  - https://github.com/center-for-threat-informed-defense

---

6. Free Training Resources

These will help you build Purple Team competency quickly.

AttackIQ Academy (Breach & Attack Simulation)

https://academy.attackiq.com

Immersive Labs (Hands-on Labs)

https://www.immersivelabs.com

TryHackMe Purple Path

https://tryhackme.com/path/outline/purple

MITRE ATT&CK Defender (MAD) Certifications

Free or low-cost ATT&CK certifications. https://mitre-engenuity.org/mad/

Blue Team Level 1 (BTL1) Training

https://securityblue.team

7. Purple Team Scenarios You Can Start With

Below are simple, safe starter tests based on MITRE ATT&CK.

Scenario 1: PowerShell Recon (T1059.001)

- Red runs: `Get-Process`, `whoami`, `ipconfig`
- Blue checks logs, alerts, and SIEM visibility.

Scenario 2: Phishing Execution (T1566)

- Red sends safe test email
- Blue inspects logs: email gateway, SIEM alerts, user actions

Scenario 3: Credential Dump Simulation (T1003)

- Red uses Atomic Red Team test
- Blue hunts in Windows event logs

---

8. Reporting Templates (Simple Format)

Purple Team Report Template

- **Threat Scenario:**
- **MITRE Technique:**
- **Red Actions:**
- **Blue Detections:**
- **Gaps Found:**
- **Fixes Applied:**
- **Next Step:**

This keeps collaboration structured and improvement-focused.

---

9. Recommended Reading for New Purple Teamers

- **The Purple Book** (free) → https://www.thepurplebook.club
- **MITRE ATT&CK for Dummies** → Free PDFs available online
- **Blue Team Handbook: SOC, IR, Malware**
- **Red Team Development and Operations** by Joe Vest & James Tubberville

---

10. Final Advice for New Purple Teamers

- Don't try to learn **everything at once**—pick one technique and master it.
- Use **MITRE ATT&CK** as your north star.
- Practice in small, controlled environments.
- Document everything.
- Always communicate with Blue Teams.
- Purple Teaming is about **growth, not gotchas**.

Welcome to the field—your journey just began.