Whole Cyber “New Security Engineer: Red Team Field Guide (MSSP-Focused)”

Mapped to NICE Framework • Free & Non-Video Resources • Entry → Intermediate

INTRODUCTION This Field Guide is built for new Security Engineers entering Managed Security Service Provider (MSSP) environments where Red Team knowledge supports:

- Threat emulation
- Adversary-informed detections
- Threat hunting
- Enrichment for SOC triage
- Purple Team collaboration
- Vulnerability analysis & attack-path validation

Table of Contents

SECTION 1 — Red Team Role Orientation in an MSSP 4
How Red Team Knowledge Supports MSSP Operations 4
1.2 NICE Role Mapping: 4
SECTION 2 — Red Team Foundations (Entry Level) 5
2.1 Understanding Adversary Logic 5
SECTION 3 – OS Knowledge for Adversarial Thinking 5
3.1 Linux for Offense-Informed Defense 5
SECTION 4 — Reconnaissance & Enumeration (Safe + Theory) 5
4.1 OSINT & Pre-Attack Techniques MITRE PRE-ATT&CK (Archived Docs) 5
4.2 Safe Hands-On Recon (Non-Exploitation) 5
SECTION 5 — Vulnerability & Weakness Analysis 6
5.1 Understanding Vulnerability Mechanics 6
SECTION 6 — Adversary Tactics for MSSP Analysts 7
6.1 ATT&CK Technique Deep Dives Study and document: 7
SECTION 7 — Adversary Emulation for MSSP Environments (No malware. No unsafe techniques. Theory-Driven.) 7
7.1 MITRE ATT&CK Navigator https://mitre-attack.github.io/attack-navigator/ 7
7.2 Red → Blue → Purple Mapping Exercise Choose a technique: 7
7.3 Kill Chain Storyboarding Write a simple narrative: 7
SECTION 8 — Hands-On Red Team Exercises (Safe, Evidence-Based) 8
8.1 Enumeration Notebook 8
8.2 Web Application Mapping 8
8.3 Daily TTP Log 8
SECTION 9 — MSSP Red Team Readiness Checklist You are MSSP-ready when you can: 9
Red Team Student Guide (MSSP-Focused) 10
SECTION 1 — Course Overview 10
SECTION 2 — Required Student Materials 10
Student Workbook Requirements Students must maintain: 11
SECTION 3 — Weekly Student Guide & Assignments 11
WEEK 1 — Adversary Fundamentals for MSSPs 11
WEEK 2 — Windows & Linux for Adversarial Thinking 11

WEEK 3 — Recon & Enumeration (Safe + Theory-Driven) 12
WEEK 4 — Vulnerability & Weakness Analysis 12
WEEK 5 — Adversary Technique Mastery (ATT&CK Deep Dive) 12
WEEK 6 — Adversary Emulation for MSSP Detection Support 13
SECTION 4 — Final Assessment Students must complete: 13
FINAL CASE STUDY — Adversary Path Reconstruction 14
SECTION 5 — Completion Outcome 14
Red Team Student Workbook (MSSP Edition) 15

SECTION 1 — Red Team Role Orientation in an MSSP

How Red Team Knowledge Supports MSSP Operations

- Improve detection engineering via ATT&CK mapping
- Help SOC analysts understand attacker logic
- Enable threat hunters to follow TTP-driven searches
- Support IR with attack-path reconstruction
- Strengthen vulnerability assessments with adversary context
- Assist SecEng teams with detection tuning

1.2 NICE Role Mapping:

1 MSSP Function | Red Team Contribution | NICE Role |
2 SOC Tier 1 | Identifying attacker patterns | AN-SOC-001 |
3 SOC Tier 2 | TTP correlation, deeper log review | AN-ASA-001 |
4 Incident Response | Attack reconstruction, mapping | IR-INC-001 |
5 Threat Hunting | Hypothesis building & ATT&CK use | AN-HNT-001 |
6 Threat Intelligence | Adversary technique profiling | AN-TWA-001 |
7 Detection Engineering | Validating rules & gaps | DE-DPR-001 |
8 Vulnerability Analysis | Attack-path reasoning | AN-VRA-001 |

SECTION 2 — Red Team Foundations (Entry Level)

2.1 Understanding Adversary Logic

- MITRE ATT&CK Enterprise Matrix
  https://attack.mitre.org
- Learn each tactic (TA0001–TA0011)
- Read technique descriptions daily
- Focus on log sources and mitigations

CISA Threat Actor Reports
https://www.cisa.gov/news-events/cybersecurity-advisories

- Free intelligence on real APT behavior

OWASP Testing Guide (Text-Based)
https://owasp.org/www-project-web-security-testing-guide/

- Web attack methodologies (safe, theory-driven)

Why MSSPs need this: You cannot defend against behaviors you don't understand.

SECTION 3 – OS Knowledge for Adversarial Thinking

3.1 Linux for Offense-Informed Defense

Linux Journey https://linuxjourney.com

- File permissions → privilege escalation context
- Processes → malicious process identification
- Services → persistence points.

SECTION 4 — Reconnaissance & Enumeration (Safe + Theory)

4.1 OSINT & Pre-Attack Techniques MITRE PRE-ATT&CK (Archived Docs)

- Targeting
- Researching services
- Weakness discovery
- OWASP Recon Guidance
- Header analysis
- Directory enumeration (theoretical)

4.2 Safe Hands-On Recon (Non-Exploitation)

HackTheBox Academy

Free Text Modules Use free text-only modules:

- Intro to Pentesting
- Web Requests
- Enumeration Fundamentals

TryHackMe –

Free Text-Driven Rooms Use only:

- Intro to Pentesting
- Basic Pentesting (written walkthroughs)
- Vulnerabilities 101

Why MSSPs need this: Enumeration explains attacker entry points.

SECTION 5 — Vulnerability & Weakness Analysis

5.1 Understanding Vulnerability Mechanics

NVD — CVE Database
https://nvd.nist.gov

- Read 10 CVEs per week
- Focus on CWE categories

MITRE CWE Catalog
https://cwe.mitre.org

- Injection
- Access control failures
- Misconfigurations

OWASP Cheat Sheets
https://cheatsheetseries.owasp.org

- Input validation
- Authentication
- Secure design

Why MSSPs need this: Attackers chain weaknesses; defenders must anticipate.

SECTION 6 — Adversary Tactics for MSSP Analysts

6.1 ATT&CK Technique Deep Dives Study and document:

- T1059 Command Execution
- T1047 WMI Execution
- T1003 Credential Access
- T1021 Remote Services
- T1053 Scheduled Task persistence

SECTION 7 — Adversary Emulation for MSSP Environments (No malware. No unsafe techniques. Theory-Driven.)

7.1 MITRE ATT&CK Navigator https://mitre-attack.github.io/attack-navigator/

- Highlight top attacker techniques
- Create customer
- specific threat profiles

7.2 Red → Blue → Purple Mapping Exercise Choose a technique:

- Describe attacker action
- Identify detection log source
- Write potential SIEM correlation logic

7.3 Kill Chain Storyboarding Write a simple narrative:

- Recon
- Initial Access
- Lateral Movement
- Privilege Escalation
- Impact

Why MSSPs need this: This is how MSSPs brief customers.

SECTION 8 — Hands-On Red Team Exercises (Safe, Evidence-Based)

8.1 Enumeration Notebook

Daily exercises:

1 Observe processes
2 List network connections
3 Note suspicious patterns

8.2 Web Application Mapping

Steps:

1 List endpoints
2 Identify parameters
3 Identify server types from headers
4 (No scanning.)

8.3 Daily TTP Log

Write one technique/day: -

1 ID
2 Summary
3 Log indicators
4 Mitigations

Document:

1 Threat group name
2 Techniques used
3 Target industries

8.4 Adversary Card Creation

SECTION 9 — MSSP Red Team Readiness Checklist You are MSSP-ready when you can:

- Explain attacker TTPs clearly to SOC teammates
- Map alerts to ATT&CK techniques
- Identify attacker patterns in logs
- Understand basic recon & enumeration
- Profile a threat actor using ATT&CK
- Support IR with attack-chain reconstruction
- Help detection engineers strengthen rules
- Assist VM analysts with risk context

NICE Alignment Achieved:

- AN-HNT-001 – Threat Hunter
- AN-TWA-001 – Threat Analyst
- AN-ASA-001 – Cyber Defense Analyst
- IR-INC-001 – Incident Responder
- SP-ADV-001 – Adversary Emulation Specialist
- DE-DPR-001 – Detection Engineer

CONCLUSION

This MSSP-aligned Red Team Field Guide delivers a safe, structured pathway to:

- Understand adversary techniques
- Support SOC & IR workflows
- Strengthen detection engineering
- Enrich threat intelligence
- Build attack-path literacy
- Prepare for Purple Team operations

Red Team Student Guide (MSSP-Focused)

Student Guide • Materials • Assignments

Based on the New Security Engineer: Red Team Field Guide (MSSP Edition)

SECTION 1 — Course Overview

Course Purpose This training prepares students for entry-level Red Team–informed roles inside an MSSP, where adversary knowledge is used to:

- Strengthen detection engineering
- Support SOC Tier 1/2 analysts
- Inform threat hunting
- Enhance incident response analysis
- Provide attacker context during vulnerability reviews

SECTION 2 — Required Student Materials

Accounts / Platforms (All Free):

1 MITRE ATT&CK website
2 CISAgov advisories portal
3 OWASP Testing Guide
4 Linux Journey
5 OverTheWire Bandit
6 Microsoft Learn (Windows Security)
7 Sysinternals documentation
8 NVD & CWE databases
9 HackTheBox Academy (free text modules)
10 TryHackMe free written rooms

Recommended Tools (Free):

- VirtualBox + Ubuntu VM - Windows VM
- Notion / OneNote (for technique logs)
- ATT&CK Navigator (browser-based)

Student Workbook Requirements Students must maintain:

1 TTP Logbook (ATT&CK techniques, threat actor notes)
2 Recon Notebook (enumeration observations)
3 Adversary Profiles Binder
4 Detection Notes Binder (for Purple Team prep)

SECTION 3 — Weekly Student Guide & Assignments

A 6-week structured progression aligned to MSSP job functions.

WEEK 1 — Adversary Fundamentals for MSSPs

Learning Goals:

- Understand adversary behavior
- Learn why attackers follow specific chains
- Build a foundation in ATT&CK literacy

WEEK 2 — Windows & Linux for Adversarial Thinking

Learning Goals:

- Identify common attacker artifacts in both OS types
- Understand how processes, permissions, and logs reveal behavior

Reading Material:

- Linux Journey → Permissions & Processes sections
- OverTheWire Bandit levels 0–10
- Sysinternals documentation (Process Explorer, TCPView)
- Microsoft Learn → Windows Security Fundamentals

Assignments:

1. Document 10 Windows Event IDs relevant to attacks.

2. Complete Bandit 0–10 and write what each level taught you.

3. Use Sysinternals docs to identify:

- one suspicious process
- one persistence mechanism
- one network-based indicator

WEEK 3 — Recon & Enumeration (Safe + Theory-Driven)

Learning Goals;

- Perform safe reconnaissance activities
- Identify attacker thinking during discovery phases

Reading Material:

- OWASP Testing Guide → Discovery & Recon sections
- MITRE PRE-ATT&CK archived documentation
- HTB Academy (free): Intro to Pentesting, Web Requests

Assignments:

1. Perform a web mapping exercise (headers, cookies, visible endpoints).
2. Write a Recon Checklist of 10 steps attackers use.

Document the difference between:

1. passive recon
2. active recon
3. enumeration

WEEK 4 — Vulnerability & Weakness Analysis

Learning Goals;

- Understand how attackers chain weaknesses
- Learn CVE/CWE fundamentals

WEEK 5 — Adversary Technique Mastery (ATT&CK Deep Dive)

Learning Goals

- Build strong technique literacy
- Learn to map logs to attacker actions

Reading Material:

- 7–10 ATT&CK technique pages
- D3FEND mitigations for each
- One threat actor profile (CrowdStrike library)

Assignments

1. Create 5 technique worksheets:

a. technique ID
b. description

c. log sources
d. mitigations

2. Build a small adversary profile for one APT.

3. Explain how two techniques relate in a kill chain.

WEEK 6 — Adversary Emulation for MSSP Detection Support

Learning Goals:

- Understand how Red knowledge informs Blue actions
- Create attack-path narratives

Reading Material:

- MITRE ATT&CK Navigator
- Any CISA alert with attacker sequence

Assignments:

1. Create a kill chain storyboard:

- Recon →
- Initial Access →
- Lateral Movement →
- Impact

2. Write a detection note for a technique of your choice.

3. Write a Tier 1 SOC escalation note explaining a suspected attack.

SECTION 4 — Final Assessment Students must complete:

1. TTP Logbook (20 technique entries)
2. Adversary Profiles (3 threat actors)
3. Recon Notebook (10+ recon observations)
4. Windows Event Log Journal (10 event IDs + meanings)

FINAL CASE STUDY — Adversary Path Reconstruction

Scenario

“An MSSP customer reports multiple failed VPN logins followed by a successful login from a foreign IP. A scheduled task is created within minutes, and encoded PowerShell is executed.”

Student Tasks

1. Identify the likely attack chain used.

2. Map each action to MITRE ATT&CK.

3. Identify the log sources that validate each step.

4. Provide a risk rating.

5. Write a customer-facing summary.

6. Provide recommended immediate actions.

SECTION 5 — Completion Outcome

After completing this course, students will be prepared to support:

- SOC Tier 1 & Tier 2 analysts
- Threat Intelligence teams
- Threat Hunting teams
- Detection Engineering support roles
- MSSP Purple Team development
- Incident Response triage and enrichment

Red Team Student Workbook (MSSP Edition)

Worksheets • Drills • Recon Activities • Technique Sheets

Companion to the Red Team Student Guide (MSSP-Focused)

How to Use This Workbook This workbook is designed like an adult-learning version of a K–8 workbook, re-imagined for future Red Team–informed Security Engineers working in MSSP environments.

MODULE 1 — Adversary Fundamentals

1.1 Vocabulary Builder (Fill-in-the-Blank)

1. A _____ is a repeatable behavior an attacker uses.

2. The three stages of a TTP are: Tactic, Technique, and _____.

3. Initial Access belongs to ATT&CK tactic group “TA000__”.

4. Persistence is when attackers _____.

5. Execution events commonly appear in _____ logs.

1.2 Define These Red Team Concepts Short answers (1–2 sentences each):

Adversary_____
_____

Attack chain
_____
_____

Reconnaissance
_____
_____

Lateral movement
_____
_____

Obfuscation_____
_____

1.3 Technique Identification Drill Match the technique to its purpose:

T1059 → _____

T1003 → _____

T1047 → _____

T1021 → _____

T1053 → _____

MODULE 2 — OS Literacy for Adversary Thinking

2.1 Linux Enumeration Worksheet

Fill in the meaning: - ls -la → _____

ps aux → _____

/etc/passwd contains → _____

chmod 755 changes → _____

2.2 Linux Practical Exercise

Run each command and write what it reveals:

whoami _____

history _____

uname -a _____

2.3 Windows Process Analysis (Sysinternals Docs)

Identify:

A suspicious parent→child process chain: _____

A network-active process: _____

A persistence indicator: _____

2.4 Windows Event Log Hunt

Fill in the Event IDs:

Failed logon → Event ID _____

Process creation → Event ID _____

MODULE 3 — Recon & Enumeration (Safe)

3.1 Passive Recon Worksheet For any public website, identify:

Domain registrar:

_____

Framework or server header:
_____

Exposed directories (from page structure only):
_____

Cookies set: _____

MODULE 4 — Vulnerability & Weakness Analysis

4.1 CVE Analysis Worksheet CVE ID: _____

System Affected: _____

Attack Vector (AV): _____

CVSS Score: _____

Severity Category: _____

Summary:
_____
_____
_____

CWE Mapping: _____

4.2 CWE Deep Dive (Short Answer) Explain each: -

CWE-79 Cross-Site Scripting _____

CWE-89 SQL Injection _____

CWE-22 Path Traversal _____

4.3 OWASP Insecure Patterns Identify examples from any application:

Missing input validation _____

Weak authentication _____

Misconfiguration example _____

Installation Event ID _____

MODULE 5 — ATT&CK Technique Mastery

5.1 Technique Sheet Template

Fill one sheet per technique: - Technique ID: _____

Name: _____

Description: _____

What an attacker does: _____

Log sources that capture it: _____

Common defensive rules: _____

D3FEND mitigations: _____

(Complete 10 sheets across the module.)

5.2 Technique Sorting Exercise

Place the techniques in the right tactic category:

T1059 → _____

T1136 → _____

T1041 → _____

T1021 → _____

T1053 → _____

MODULE 6 — Threat Intelligence & Actor Profiling

6.1 Threat Actor Profile Builder Threat Group

Name: _____

Origin/Attribution: _____

Motivation: _____

Industries Targeted: _____

Known Techniques (min 3):

1. _____

2. _____

3. _____

Primary Kill Chain Flow:

_____

_____

_____

MODULE 7 — Adversary Emulation (Theory Only)

7.1 Mini Kill Chain Activity Write a simple attacker chain:

Recon → _____

Initial Access → _____

Execution → _____

Lateral Movement → _____

Persistence → _____

Impact → _____

7.2 Attack-Path Storyboard Boxes to fill:

Attacker objective: _____

Entry point: _____

Misconfiguration used: _____

Technique #1: _____

Technique #2: _____

Final goal: _____

7.3 Red → Blue Conversion Exercise Choose a technique and fill in: -

Attacker action: _____

Windows/Linux logs generated: _____

How a SOC analyst would detect it: _____

MSSP escalation text (1–2 sentences): _____

MODULE 8 — MSSP Scenario Drills

8.1 SOC Tier 1 Enrichment Worksheet

Alert: “Suspicious PowerShell command executed on host.”

Document:

What you check first:

_____

_____

Related event IDs:
_____
_____

Possible ATT&CK mapping:
_____
_____

Escalation decision:
_____
_____

8.2 Threat Hunting Hypothesis Activity

Threat Actor:
_____
_____

Technique:
_____
_____

Hypothesis: “If the attacker used this technique, we would see _____ logs.”

8.3 Detection Engineer Support Drill

Write a detection logic concept: - Technique: _____

Trigger Conditions: _____

Enrichment Data Needed: _____

Possible False Positives: _____

Recommended Customer Action: _____

FINAL EXAM — Adversary Reconstruction Case

Scenario “A foreign IP performs recon on a client-facing app, followed by authenticated login attempts and execution of encoded PowerShell. Minutes later, a scheduled task appears.”

Student Tasks

1. Reconstruct the attack chain.

_____
_____
_____
_____

2. Map each step to ATT&CK techniques.

_____
_____
_____
_____

3. Identify the log sources needed.

_____
_____
_____
_____

4. Provide a risk rating.

_____
_____
_____
_____

5. Write a Tier 2 escalation summary.

_____
_____
_____
_____

6. Provide customer remediation guidance.

_____
_____
_____
_____