Alpha Team 7

PURPLE TEAM RUN BOOK 1

Phishing | Data Exfiltration | C2 Payload

Author: Adam Baguley

Version: 2.0

Date: 20-03-2025

1. INTRODUCTION, PURPOSE & SCOPE

Introduction

This runbook outlines a coordinated exercise between the offensive (Red) and defensive (Blue) teams. The Purple Team, acting as the liaison, facilitates real-time communication, continuous feedback, and adaptive adjustments during the simulated attack. This integrated approach is designed to expose detection gaps, improve incident response capabilities, and refine threat hunting procedures.

Purpose

- Validate and improve the detection, containment, and remediation of adversarial activities.
- Test both offensive techniques (phishing, reverse shell, data exfiltration) and defensive responses.
- Ensure that cross-team collaboration yields immediate, actionable insights for continuous improvement.

Scope

- Pre-Exercise: Coordination, technical setup, and alignment of logging, SIEM (e.g., Splunk), and EDR configurations.
- In-Exercise: Execution of a detailed attack scenario with real-time monitoring, feedback, and re-execution of failed exploits.
- Post-Exercise: Comprehensive debrief, gap analysis, performance metric evaluation, and actionable recommendations.

---

2. ROLES AND RESPONSIBILITIES

Roles & Responsibilities

Adam – Red Team Operator

- Prepare scripts and executable malware.
- Execute offensive techniques (e.g., deploying reverse shells, exfiltration payloads).
- Debug and re-run exploits if needed.

Rachel – Red Team Operator & Purple Team Coordinator

- Facilitate real-time communication between teams.
- Re-execute failed exploits to validate Blue Team detection.
- Coordinate file delivery (e.g., uncompiled Python scripts) to support Blue Team analysis.
- Oversee timeline documentation and tactical adjustments.

Pavlee – Blue Team Operator

- Monitor network and endpoint logs to detect malicious activity.
- Initiate and document defensive measures and incident responses.
- Analyze evidence (e.g., SIEM/EDR logs) and contribute to post-exercise debrief.

Mariann – Blue Team Operator

- Support Pavlee in threat detection and incident response.
- Validate alerts and document response steps.
- Research and refine Splunk SPL commands and other detection rules.
- Collaborate with Rachel for correlating attack indicators.

---

3. ATTACK SCENARIO OVERVIEW

Scenario Narrative

In alignment with the Red Team Runbook, the exercise simulates the following sequence:

- **Phishing Email** A crafted email, impersonating the IT Security Department, instructs the victim to run a “mandatory security update” from a specified URL.

- **Payload Execution** The victim’s machine runs the RightPointUpdate.exe payload, which exfiltrates data (Documents and Pictures folders) to an exfiltration directory on an Ubuntu web server and initiates a reverse shell.

- **Command-and-Control(C2)** The victim’s payload continuously polls a “Commands.txt” file hosted on the simulated GitHub site. Upon detecting new commands, it executes them and writes results to “Output.txt,” thereby establishing a covert C2 channel over HTTP.

Key Technical Aspects

- **Infrastructure**
- Three VMs are used (Windows Victim, Windows Attacker, Ubuntu Web Server hosting Apache2 with WebDAV enabled).
- The Ubuntu server simulates both a GitHub private repository and an intranet page.

Communication

- The reverse shell connection is designed to mimic legitimate HTTP traffic.
- File delivery via WebDAV replicates API interactions with a private repository.
- Operational Goal:
- Demonstrate methods to achieve shell access while evading standard intrusion detection systems

Operational Goal

- Demonstrate methods to achieve shell access while evading standard intrusion detection systems.

---

4. PRE-EXERCISE COORDINATION & TECHNICAL SETUP

Infrastructure Verification Checklist:

SIEM & EDR

□ Confirm SIEM (e.g., Splunk, Elastic) is correctly set up to capture logs from mail gateways, web filters, and endpoint events.
□ Ensure EDR is configured to monitor PowerShell activity, process creation, and network anomalies.

Web Server Configuration

□ Verify Apache2 is installed, enabled, and configured to listen on both NIC IPs (192.168.1.4 and 192.168.2.4).
□ Ensure WebDAV is enabled and the exfiltration directory permissions are correctly set (using commands from Toolbox.txt).

Network Setup:

□ Validate VM IP addressing and connectivity as per the Red Team Runbook.

---

5. IN-EXERCISE MONITORING & CHECKLISTS

Real-Time Monitoring Checklist:

Attack Launch & Execution
Red Team Verification
□ Confirm dispatch of phishing emails as detailed in the Red Team Runbook.
□ Monitor the use of offensive tools (e.g., Social Engineering Toolkit) and payload execution.

Log & Alert Checks
□ Validate that SIEM captures endpoint logs.
□ Ensure alerts are triggered for suspicious subject lines, anomalous IPs, and domain lookups this may not all be possible in a simulated environment.
□ Monitor for HTTP reverse shell connections, process creation and enable relevant Windows logging as outlined in the Bluebook.

Blue Team Detection & Response
Detection Timeline
□ Record the time from phishing email dispatch to first alert (Mean Time to Detect).
□ Log response actions (e.g., blocking IPs, account resets) and record Mean Time to Respond.

Event Documentation
□ Capture detailed logs showing detection of lateral movement or command execution.
□ Verify if commands from “Commands.txt” are detected and correlate with actions on “Output.txt.”
□ Capture Windows logs that confirm commands executed by HTTP Wireshark capture and by process creation auditing with command line auditing.

Exploit Re-Execution & Feedback Loop
Re-Execution Protocol
□ Under the guidance of Rachel, re-run any failed exploits to ensure comprehensive testing.

File Delivery Verification
□ Monitor secure transfer of files (e.g., uncompiled Python scripts) from Red to Blue teams.
Real-Time Adjustments
□ Provide immediate feedback to adjust tactics if detection is delayed or overly aggressive.
□ Document all adjustments made in real time for post-exercise review.

---

6. PERFORMANCE METRICS

Key Metrics to Capture:

Mean Time to Detect (MTTD)
- Duration from phishing email sent to the first triggered alert.

Mean Time to Respond (MTTR)
- Time between alert generation and successful containment (e.g., IP blocking, process termination).

Detection Accuracy
- Ratio of false positives versus actual threats detected.

User Interaction Metrics
- Phishing link click-through rates and number of credentials submitted.

Feedback Implementation Rate
- Speed and effectiveness of in-exercise rule adjustments and tactical modifications.

---

7. REAL-TIME FEEDBACK & TACTICAL ADJUSTMENTS

Feedback Process

Observation & Communication

- The Purple Team continuously monitors the exercise and communicates in real time with both the Red and Blue teams.

Adjustment Protocol

- If any detection anomalies or delays are observed, immediate recommendations are provided (e.g., modifying SIEM rules or altering phishing content).

Documentation

- Record all tactical changes and their impact on detection and response in real time.

---

8. POST-EXERCISE ANALYSIS & REPORTING

1. **Debrief**

- Collect timelines, detection logs, and attack steps from Red Team.
- Compare with Blue Team's alerts, escalations, and containment actions.

2. **Gap Analysis**

- Identify detection blind spots (e.g certain mail attachments or newly registered domains).
- Review policy or configuration gaps in email filtering, endpoint security, or user training.

3. **Actions for Improvement**

- Update SIEM correlation rules or EDR policies.
- Provide refreshed user security awareness training.
- Enhance incident response playbooks with new detection scenarios.
- After Blue Team adjusts SIEM rules, re-send a modified phishing email to test the new detection logic.
- Validate if new network-based detections successfully block Red Team activities.
- Measure how long it takes for new detection rules to be operationalized.

Notes/Comments:

This Purple Team Playbook ensures transparency and continuous improvement by bridging Red and Blue Team efforts. Real-time feedback and collaborative adjustments allow comprehensive security assessment within the IRTx framework for both red and blue teams.