A Purple Team Security Assessment of a Maturity Level 1 Healthcare Provider: Detection Engineering and Validation on a Segmented Enterprise Network

Final Project Exercise Plan

Group 2

, Abdul-Ramon Adeyemi Folarin, &

, , , &

School of Information Technology Administration & Security, Seneca Polytechnic

SPR708NBB: Attack and Defense

Professor Ahmad Ghobeiti

August 12, 2026

Student Integrity Statement: I/we declare that the attached assignment is my/our own work in accordance with the Seneca Academic Policy. No part of this assignment has been copied manually or electronically from any other source (including web sites) or distributed to other students

1. Executive Summary

This document is the Exercise Plan for a Purple Team assessment of the 500.spr enterprise network, modelled as the internal infrastructure of a mid-size Ontario healthcare provider operating at Security Maturity Level 1. The exercise follows the Atomic Purple Team lifecycle and the SCYTHE Purple Team Exercise Framework. Adversary behaviour is mapped to MITRE ATT&CK version 19 and risk is framed under NIST SP 800-30.

The primary objective is to determine whether the organisation can detect and respond to a realistic intrusion ending in ransomware, and to measure the improvement achieved after targeted remediation. A single connected attack chain advances from external reconnaissance through web-application exploitation, credential access, and lateral movement to a simulated ransomware impact. Each step is jointly evaluated by offensive and defensive team members to record whether the activity was prevented, alerted, or only logged. Detection gaps drive remediation, which is then validated with a second pass of the same chain.

> **Scope reminder:** Only five machines from the 500.spr topology are in scope: extattacker, websrv-01, core-01, admin-01, and dc-dhcp-01. No activity leaves the isolated lab. The ransomware step is a simulation using file renaming only.

Table of Contents

1. Executive Summary 2
Table of Tables 4
2. Market Segment Selection and Rationale 5
2.1 Selected Segment: Healthcare 5
2.2 Current Threat Landscape 5
2.3 Active Threat Actors and TTPs 5
2.4 Regulatory Environment 5
2.5 Influence on Exercise Design 5
3. Scope 6
3.1 Systems in Scope 6
3.2 Systems Explicitly Out of Scope 6
3.3 Data and Accounts in Scope 6
4. Objectives and Goals 6
4.1 Business Objective 6
4.2 Technical Objectives 6
4.3 Success Criteria 7
5. Rules of Engagement 7
6. Stakeholders 7
7. Team Roles and Collaboration Model 8
8. Attack Plan and TTP Mapping 8
8.1 Scenario 8
8.2 Step-by-Step Chain 8
8.3 MITRE ATT&CK v19 Mapping 9
9. Identified Control Gaps and Remediation Plan 10
10. Resources and Tools 10
10.1 Offensive Tooling 10
10.2 Defensive Tooling 11
10.3 Frameworks and References 11
11. Eight-Week Exercise Schedule 11
Approval and Sign-Off 12

Table of Tables

Table 1 Systems in Scope 6
Table 2 Stakeholders 7
Table 3 Team Roles and Collaboration Model 8
Table 4 MITRE ATT&CK v19 Mapping 9
Table 5 Identified Control Gaps and Remediation Plan 10
Table 6 Offensive Tooling 10
Table 7 Defensive Tooling 11
Table 8 Eight-Week Exercise Schedule 11
Table 9 Approval and Sign-Off 12

2. Market Segment Selection and Rationale

2.1 Selected Segment: Healthcare

Healthcare was selected as the target market segment. Mid-size healthcare providers, such as regional clinic networks, are large enough to operate a domain environment, file servers, and baseline security tooling, but typically lack a dedicated security operations centre or mature incident response process. This places them squarely at Security Maturity Level 1 and makes them a realistic and highly relevant target for this exercise.

2.2 Current Threat Landscape

Healthcare is consistently the most targeted critical-infrastructure sector. Ransomware attacks on the sector rose approximately fourteen percent in the first half of 2026, averaging more than two incidents per day globally. Canada ranked among the five most affected countries. Attackers increasingly reach providers through vendors and third parties, widening the effective attack surface beyond a single organisation's perimeter.

2.3 Active Threat Actors and TTPs

The most active groups against healthcare providers in 2025 to 2026 include Qilin, LockBit, INC, and The Gentlemen. These groups follow a consistent pattern this exercise deliberately mirrors: initial access through an exposed application, credential theft, lateral movement across a flat network, and data encryption for impact. Average ransom demands in the healthcare sector reached approximately 16.9 million dollars in the first quarter of 2026.

2.4 Regulatory Environment

Ontario healthcare organisations are bound by the Personal Health Information Protection Act (PHIPA). Breach notification is required at the first reasonable opportunity, interpreted by the Information and Privacy Commissioner (IPC) as approximately seventy-two hours. Following a 2025 IPC ruling upheld on appeal, ransomware encryption alone constitutes a reportable breach even without confirmed exfiltration. The federal Personal Information Protection and Electronic Documents Act provides a further backstop. Recent amendments introduced mandatory IPC notification and the first administrative monetary penalties, up to 500,000 dollars for organisations.

2.5 Influence on Exercise Design

- Detection speed and recovery, not prevention alone, are the primary metrics because PHIPA notification is time-sensitive.
- The impact stage is included as a simulation because encryption alone triggers regulatory consequences.
- The attack chain begins at an exposed web application and file server, then moves laterally, reflecting the real compromise pattern of active threat actors in this sector.
- The four remediation targets (WAF, FIM, SIEM isolation, backup) directly address the observed attack surface of the sector.

3. Scope

3.1 Systems in Scope

Table 1 Systems in Scope

System	Role	Address
extattacker	External attacker (Kali). Executes the full Red Team chain.	172.16.22.3 / VLAN10
websrv-01	File server and first target. Docker host running Mutillidae and Samba.	172.16.22.194 / VLAN80
core-01	Core router and Suricata network IDS sensor.	Core gateway
admin-01	Wazuh SIEM (single-node Docker). Also tested as an SSH lateral-movement target.	172.16.44.66 / VLAN50
dc-dhcp-01	Domain Controller (Windows Server 2019, AD DS, DHCP). SMB lateral target.	172.16.44.130 / VLAN40

3.2 Systems Explicitly Out of Scope

- user-01: not attacked in this chain.
- websrv-02: not attacked; its ModSecurity ruleset is referenced in Remediation only.
- vpn-01: not attacked.
- Any host or network outside the isolated 500.spr lab environment.

3.3 Data and Accounts in Scope

- Domain and Samba account msingh827 and any credentials recovered during the exercise.
- VLANs 10, 80, 40, and 50 (external, web/file, network services, management).
- The Samba file share at /srv/files/home/msingh827/upload.
- The Mutillidae web application at port 8082 on websrv-01.

4. Objectives and Goals

4.1 Business Objective

Determine whether a Maturity Level 1 healthcare provider can detect and respond to a realistic intrusion ending in ransomware, and measure the improvement achieved after targeted remediation, given that PHIPA requires breach notification at the first reasonable opportunity.

4.2 Technical Objectives

1. Validate detection coverage across the full ATT&CK chain from reconnaissance through impact.
2. Identify prevention and detection gaps at each stage of the intrusion.
3. Implement and validate concrete control improvements for each identified gap.
4. Demonstrate a measurable before-and-after improvement in detection and recovery capability.

4.3 Success Criteria

- Every planned technique is executed and its prevent, alert, and log status is recorded.
- All four identified control gaps are closed and re-tested in a validation pass.
- The validation pass demonstrates that the initial exploit is blocked, file changes are detected, lateral movement to the SIEM is alerted, and the ransomware impact can be reversed from backup.

5. Rules of Engagement

- All activity is confined to the isolated 500.spr lab. No external targets and no real malware are used.
- The ransomware stage is a simulation: files are renamed or copied to a locked extension, never truly encrypted.
- The defense-impairment stage is performed, captured, and then immediately restored so monitoring is not lost for subsequent steps.
- Red documents every action with timestamps; Blue documents every alert, investigation, and response action.
- Red and Blue operate collaboratively and in real time, sharing findings at the end of each technique (purple model).
- Per-technique loop: Red executes, the team jointly records prevent / alert / log status, Blue tunes a detection, Red re-runs to confirm the fix.
- Credentials recovered during the exercise are used only against in-scope systems.
- No permanent changes are made to production configurations outside the controlled changes documented in Remediation.
- Any unexpected outage caused by exercise actions must be restored before proceeding to the next step.

6. Stakeholders

In the modelled healthcare provider the exercise informs the following roles. The student group performs the combined Red, Blue, and coordination function.

Table 2 Stakeholders

Stakeholder	Interest in the exercise
IT administrator	Owns the Domain Controller, file server, and endpoints under test.
Security engineer / SIEM operator	Owns Wazuh detection content and tuning.
Incident responder	Executes containment and recovery when a detection fires.
Privacy officer / practice leadership	Accountable for the PHIPA breach notification decision.
Purple Team (Group 2)	Runs the exercise and produces all findings and deliverables.

7. Team Roles and Collaboration Model

Table 3 Team Roles and Collaboration Model

Role	Member	Responsibility
Red Team Lead + Reporting Lead		Executes the attack chain. Maintains the timestamped attack log with every command, payload, and observed outcome. the Springer final report, the slides, and video coordination.
Blue Team Lead	Law	Monitors Wazuh and Suricata in real time. Documents every alert, investigation action, and response. Writes and tunes detection rules.
Purple Coordinator	Abdul-Ramon (Ade) Folarin	Runs the per-technique loop. Keeps Red and Blue communicating. Owns the ATT&CK v19 mapping and the detection matrix.
CTI		Owns the healthcare threat profile

Collaboration model (SCYTHE PTEF v4): for each technique, Red executes while Blue watches live. The team jointly answers whether the activity was prevented, alerted, or only logged, then Blue tunes a detection and Red re-runs the same technique to confirm the fix. All four members appear in the video recording for equal time.

8. Attack Plan and TTP Mapping

8.1 Scenario

A single connected intrusion is executed rather than several disconnected demonstrations. One chain touches more tactics and its detection gaps line up directly with the four documented weaknesses of this environment. An external attacker compromises the exposed web and file server, moves laterally to the monitoring host and the Domain Controller, and deploys a ransomware simulation against the patient-document file share. This mirrors the real pattern used by the active healthcare threat actors identified in Section 2.3.

8.2 Step-by-Step Chain

1. Recon: extattacker runs Nmap and Nikto against websrv-01 (T1595 Active Scanning).
2. Initial Access: exploit Mutillidae via command injection to write a web shell (T1190 Exploit Public-Facing Application; T1505.003 Web Shell).
3. Execution and Persistence: execute commands through the shell and establish a cron job (T1059 Command and Scripting Interpreter; T1053.003 Scheduled Task/Cron).
4. Credential Access: harvest database credentials, SSH material, and config secrets from websrv-01 (T1552.001 Credentials in Files).
5. Lateral Movement: SSH from the attacker host to admin-01, the SIEM (T1021.004 Remote Services: SSH; T1078 Valid Accounts).
6. Defense Impairment: from admin-01 attempt to stop Suricata and the Wazuh manager (T1562.001 Impair Defenses: Disable or Modify Tools). Restore immediately after capture.

7. Lateral Movement: password-spray the Domain Controller and authenticate over SMB (T1110.003 Password Spraying; T1021.002 SMB/Windows Admin Shares).
8. Impact: run the ransomware simulation against the Samba upload share (T1486 Data Encrypted for Impact, simulation only).

8.3 MITRE ATT&CK v19 Mapping

> **v19 change:** The former Defense Evasion tactic was split into Stealth and Defense Impairment in ATT&CK v19 (April 2026). Step 6 maps to the new Defense Impairment tactic, not the legacy Defense Evasion tactic.

Table 4 MITRE ATT&CK v19 Mapping

Step	Tactic (v19)	Technique	Detection opportunity
1	Reconnaissance	T1595 Active Scanning	Suricata scan signature on core-01
2	Initial Access	T1190 Exploit Public-Facing Application; T1505.003 Web Shell	WAF rule match on the payload; FIM on the web root
3	Execution / Persistence	T1059 Command and Scripting Interpreter; T1053.003 Cron	Endpoint command logging; rootcheck
4	Credential Access	T1552.001 Credentials in Files	Endpoint file-access monitoring
5	Lateral Movement	T1021.004 SSH; T1078 Valid Accounts	Wazuh sshd authentication rule on admin-01
6	Defense Impairment	T1562.001 Impair Defenses: Disable or Modify Tools	Service-stop and self-monitoring detection
7	Lateral Movement	T1110.003 Password Spraying; T1021.002 SMB Admin Shares	Windows logon events 4624/4625; Sysmon network connection
8	Impact	T1486 Data Encrypted for Impact (simulation)	Wazuh FIM mass-change rule on the share

9. Identified Control Gaps and Remediation Plan

The following four gaps are left open for the baseline pass, then closed during Remediation, and re-tested during Validation. Maturity Level 1 is demonstrated through these operational gaps, not through a simple absence of tooling.

Table 5 Identified Control Gaps and Remediation Plan

#	Gap (Maturity Level 1)	Exposed at step	Remediation plan
1	No FIM on websrv-01 covering the web root or file share	Step 2 and 8	Add syscheck directories to the Wazuh agent config on websrv-01
2	Mutillidae not behind a WAF	Step 2	Place nginx+ModSecurity reverse proxy in front of Mutillidae
3	SIEM reachable over SSH from untrusted VLANs; no self-protection alert	Step 5	Restrict SSH by source; add Wazuh rule 100200 for SIEM logins
4	No pre-incident backup or recovery process	Step 8	Create baseline backups of the web root and file share at /opt/backups

10. Resources and Tools

10.1 Offensive Tooling

Table 6 Offensive Tooling

Tool	Purpose
Kali Linux (extattacker)	Attacker platform for all Red Team steps
Nmap 7.99	Port and service enumeration (T1595)
Nikto	Web application scanning and fingerprinting (T1595)
netexec (nxc)	SMB authentication, password spraying, share enumeration (T1110.003, T1021.002)
SSH client	Lateral movement attempts to admin-01 (T1021.004)
Command injection payload (base64)	Web shell staging through Mutillidae DNS Lookup (T1190, T1505.003)
Ransomware simulation script (Assignment 2)	File renaming simulation for Impact stage (T1486)

10.2 Defensive Tooling

Table 7 Defensive Tooling

Tool	Purpose
Wazuh 4.9.2 (admin-01, Docker)	SIEM, agent management, FIM, rootcheck, custom rules
Suricata (core-01)	Network IDS, east-west traffic inspection, eve.json alerts
ModSecurity + OWASP CRS	Web application firewall protecting Mutillidae after Remediation
nftables	Host firewall restricting SSH to admin-01
Sysmon (dc-dhcp-01)	Windows endpoint telemetry: process, network, file events

10.3 Frameworks and References

- Atomic Purple Team Lifecycle, Playbook PB0170 (DefensiveOrigins, 2025)
- SCYTHE Purple Team Exercise Framework v4 (SCYTHE, 2026)
- MITRE ATT&CK Enterprise Matrix v19 (April 2026)
- NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments
- NIST Special Publication 800-61: Computer Security Incident Handling Guide
- OWASP ModSecurity Core Rule Set 3.3.5

11. Eight-Week Exercise Schedule

Table 8 Eight-Week Exercise Schedule

Week	Phase	Key activities
1	Planning	Finalise scope, roles, rules of engagement, and market segment rationale. Confirm lab access.
2	Preparation	Verify monitoring stack. Confirm Suricata and Wazuh operational. Document four baseline gaps.
3	Preparation	Deploy Wazuh agent and Sysmon on dc-dhcp-01. Confirm agent inventory. Stage attacker tooling.
4	Execution	Run Pass 1 (baseline) of the full attack chain. Document every step with evidence.
5	Detection analysis	Complete the prevent/alert/log matrix. Identify all detection gaps from Pass 1.
6	Remediation	Close the four gaps: WAF, FIM, SIEM restriction and rule, backup. Document each change.

Week	Phase	Key activities
7	Validation	Run Pass 2 with gaps closed. Capture before-and-after evidence. Complete the detection matrix.
8	Reporting	Submit Final Report (Springer PDF), Exercise Plan, Execution Logs, slides, and video.

Approval and Sign-Off

By proceeding with the exercise, all team members confirm that they have read and understood this Exercise Plan and agree to operate within the defined scope and rules of engagement.

Table 9 Approval and Sign-Off

Name	Role	Signature / Initials
	Red Team Lead + Reporting Lead	IG
Law	Blue Team Lead	SL
Abdul-Ramon Folarin	Purple Coordinator	AF
	CTI	SB