# Blue Team Scenario Report

**Project Title: Blue Team Defense – Network and Host Forensics  
Date: 02/23/25  
Author: Nauman Munir, Omar Hassan, Asma Jamal**

## 1. Introduction

**This report documents the defensive measures and forensic investigations performed on a Windows 10 virtual machine. The Blue Team tasks included capturing and analyzing network traffic, vulnerability scanning, crafting detection rules, and performing disk and memory forensics. Additionally, a bonus analysis using Ghidra was conducted to extract malicious strings from a malware sample.**

## 2. Scenario Steps

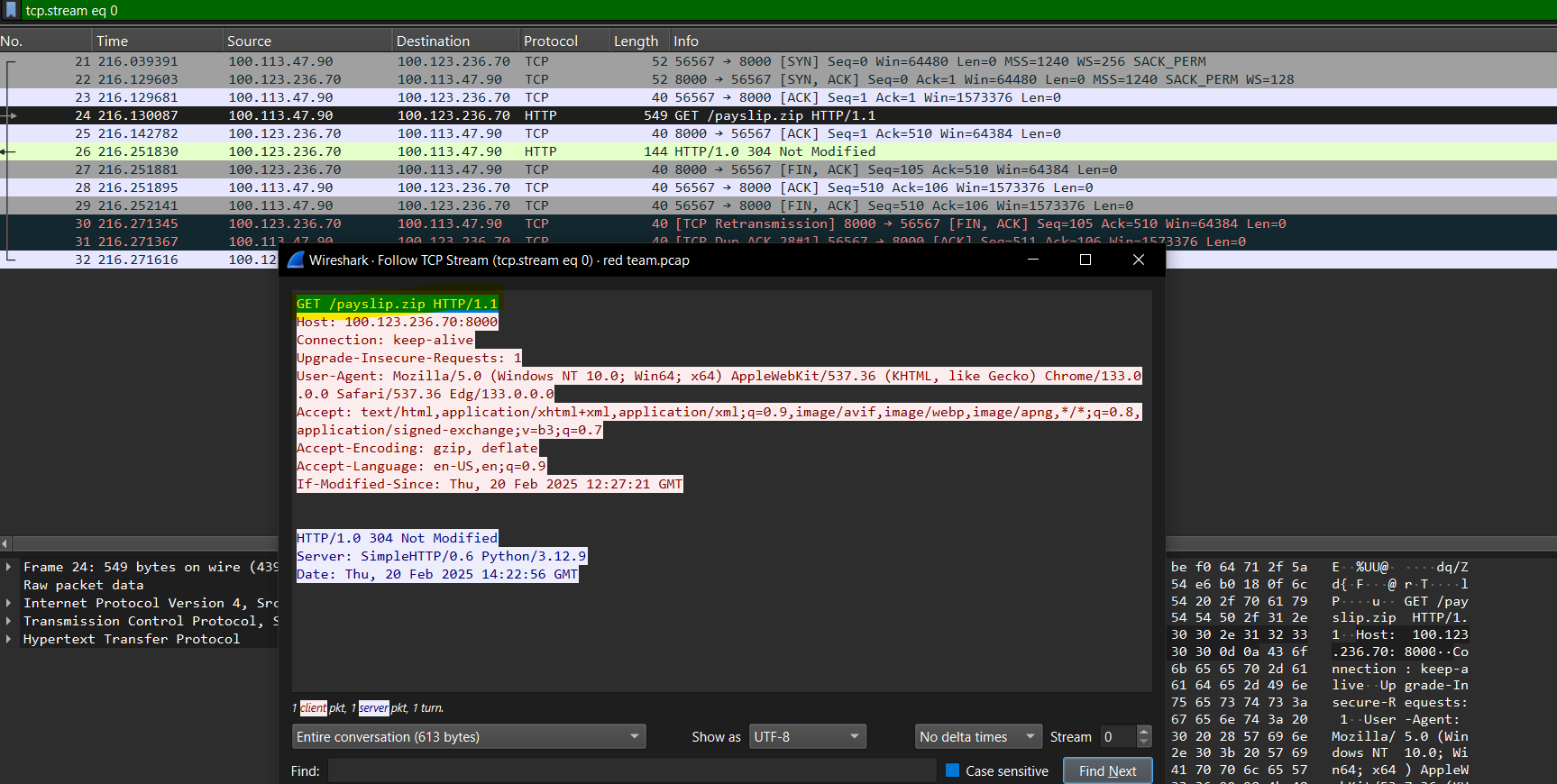
**Step 1: Recording & Saving Network Packets (10%)**

**Objective:  
Capture and store network traffic for detailed analysis to identify potential malicious activities before any C2 malware is delivered.**

**Environment:  
Windows 10 Virtual Machine**

**Procedure:**

* **Initiated packet capture with Wireshark on the target network.**
* **Continuously recorded traffic until the red team operations were completed.**
* **Saved the complete traffic data as a PCAP file.**

**Evidence:****

## Step 2: Investigate the PCAP (10%)

**Objective:  
Analyze the captured PCAP to identify reconnaissance and reverse shell packets.**

**Environment:  
Windows 10 Virtual Machine**

**Procedure:**

* **Loaded the saved PCAP file in Wireshark.**
* **Applied filters to isolate packets related to reconnaissance (e.g., excessive SYN packets) and reverse shell communications.**
* **Documented unusual patterns indicative of unauthorized activity.**

**Evidence:**

* ***Screenshot:* Filtered results showing SYN packets and reverse shell traffic.**

**Step 3: Perform Network Vulnerability Scanning (10%)**

**Objective:  
Identify vulnerabilities in the network that could be exploited by attackers.**

**Environment:  
Windows 10 Virtual Machine**

**Procedure:**

* **Used Nessus Professional to perform a deep scan of the network.**
* **Configured the scanner to check for outdated systems, misconfigurations, and open ports.**
* **Reviewed the scan report to correlate vulnerabilities with observed reconnaissance activities.**

**Evidence:**

* ***Attachment:* PDF Nessus scan report.**

## Step 4: Craft Detection Rules Using IPS (20%)

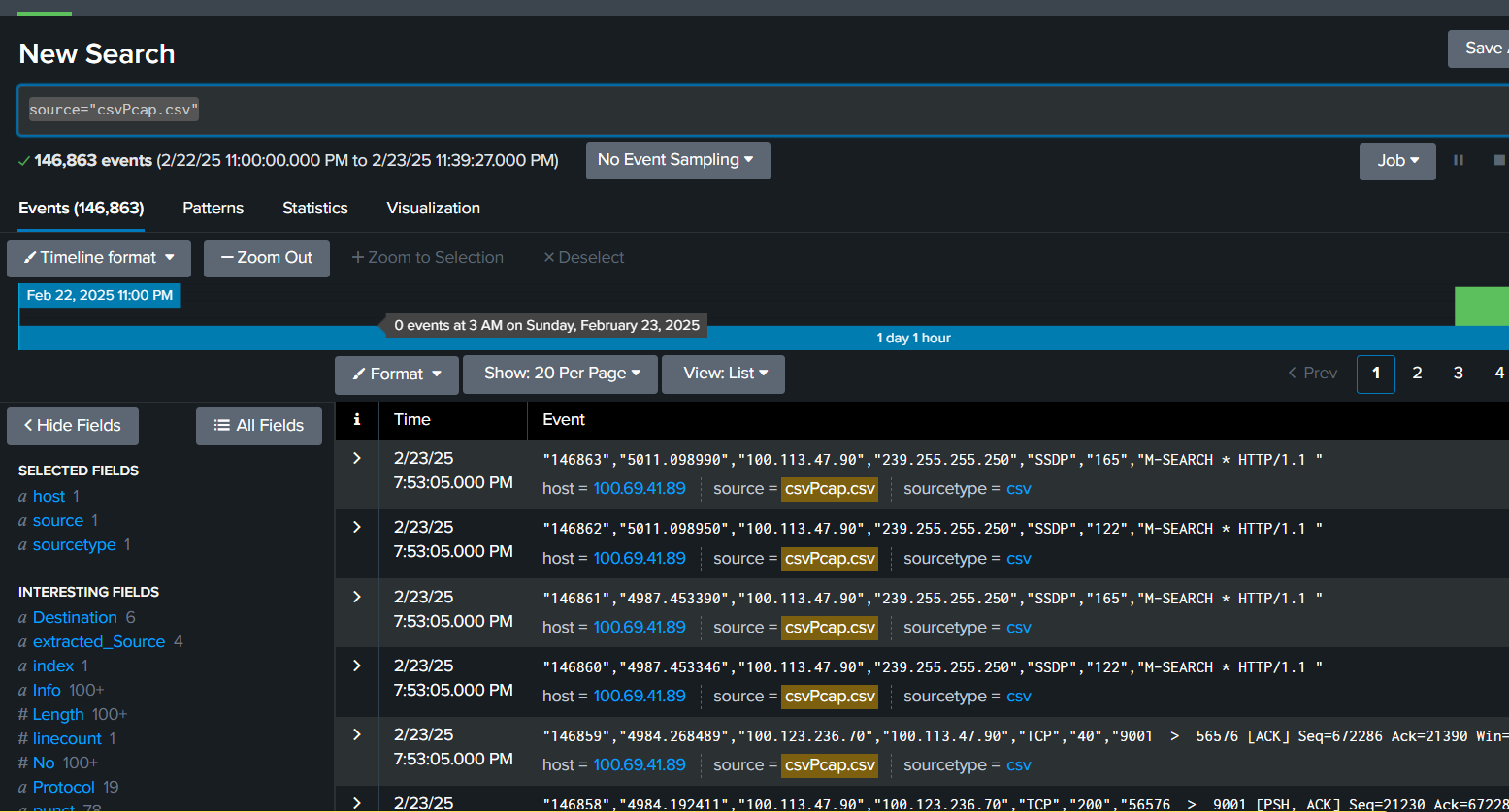
**Objective:  
Develop and implement detection rules to block malicious network activities.**

**Environment:  
Windows 10 Virtual Machine**

**Procedure:**

* **Imported the PCAP file into Suricata.**
* **Applied default IPS rules and then developed custom rules to identify reverse shell and reconnaissance signatures.**
* **Forwarded alerts from Suricata to Splunk for centralized monitoring.**

**Evidence:**

****

## Step 5: Investigate the PCAP with a SIEM Solution (20%)

**Objective:  
Correlate network traffic with system logs to confirm and detail suspicious activities.**

**Environment:  
Windows 10 Virtual Machine**

**Procedure:**

* **Converted PCAP data to CSV format and ingested it into Splunk.**
* **Imported additional logs (e.g., DNS, Windows logs) into Splunk.**
* **Built dashboards to identify unusual DNS requests, port scans, and outbound connections.**
* **Correlated network anomalies with host-based events.**

**Evidence:**

