Incident Detection & Response Report

# 1. Executive Summary

This report documents the detection and response activities conducted in a controlled cybersecurity lab environment. The objective was to simulate adversary techniques and validate detection using QRadar CE, with supporting evidence captured via Wireshark.

# 2. Incident Details

Date of Simulation: [Insert Date]  
Detected by: QRadar CE (Community Edition)  
Source System: Kali Linux (192.168.25.200)  
Target System: Windows Host (192.168.25.1)  
SIEM: QRadar CE (192.168.25.100)

# 3. Attack Simulation 1: Network Scanning

Description:

An Nmap SYN scan was executed from Kali Linux to enumerate open ports and services running on the Windows host. The scan used verbose and timing options to accelerate discovery.

Command Executed:  
nmap -sS -vv -T4 192.168.25.1

Detection:

- QRadar CE received logs from Windows via WinCollect.  
- Custom rule triggered upon detecting multiple connection attempts.

# 4. Attack Simulation 2: Brute Force

Description:

A brute force attack was launched using Hydra against the Windows ssh service. The attacker attempted multiple login combinations using a common password list.

Command Executed:  
hydra -l sunny -P /usr/share/wordlists/rockyou.txt ssh://192.168.25.1

Detection:

- Windows event logs (failed login attempts, Event ID 4625) were forwarded via WinCollect.  
- QRadar custom rule detected repeated failed logins.  
- Offense generated in QRadar, attacker IP blacklisted (Reference Data Set).

# 5. Attack Simulation 3: Valid Accounts

Description:

After brute force attempts, a valid account was compromised. The attacker successfully logged into the Windows host using discovered credentials.

Steps:

1. Created test account on Windows: net user attacker Passw0rd! /add  
2. Hydra used to crack credentials from wordlist.  
3. Successful login via SSH using hydra from Kali.

Detection:

- Event ID 4624 (Successful Logon) observed following failed attempts (4625).  
- QRadar rule correlated failed and successful logon events.

# 6. Conclusion

The lab successfully simulated multiple adversary. QRadar CE was able to detect reconnaissance brute force and valid account compromise The detection pipeline validated that log sources (WinCollect, Rsyslog) were functioning, and custom correlation rules in QRadar provided actionable alerts for SOC-style monitoring.