Cybersecurity Detection Lab Project Documentation

# 1. Lab Setup

The following environment was configured to simulate adversary techniques and demonstrate detection using QRadar CE and Wireshark:

- Attacker Machine: Kali Linux VM (192.168.25.200, vmnet8)  
- SIEM: QRadar CE VM (192.168.25.100, vmnet8)  
- Host/Victim: Windows machine (192.168.25.1, vmnet8)  
- Tools Installed on Windows: Wireshark, WinCollect  
- Log Sources:  
 \* WinCollect (Windows event logs forwarded to QRadar)  
 \* Rsyslog (enabled on Kali to forward logs to QRadar)

# 2. Attack Simulation 1: Nmap Scan

Objective: Simulate reconnaissance activity using Nmap from Kali against Windows host.

Steps:

1. On Kali (192.168.25.200), executed the following Nmap scan:  
 nmap -sS 192.168.25.1  
  
2. Logs generated from Windows and were forwarded to QRadar CE.  
3. A custom detection rule was created in QRadar to identify port scanning activity.  
4. Result: Offense was triggered in QRadar, confirming detection of the Nmap scan.

5. Upon detection, the source IP (192.168.25.200) was automatically added to a QRadar Reference Data Set (Blacklist).  
6. Result: QRadar generated an offense, and the malicious IP was successfully blacklisted

# 3. Attack Simulation 2: Brute Force with Hydra

Objective: Simulate brute force authentication attempts from Kali against Windows RDP service.

Steps:

1. On Kali, executed Hydra brute force against Windows RDP:  
 hydra -l administrator -P /usr/share/wordlists/rockyou.txt rdp://192.168.25.1  
  
2. Windows logs (failed logon attempts) were collected via WinCollect and forwarded to QRadar CE.  
3. A custom QRadar rule was created to detect multiple failed login attempts from the same source.

# 4. Outcomes and Learning

Through this lab, the following key learning outcomes were achieved:

- Successfully configured an environment with Kali, Windows, QRadar CE, and Wireshark.  
- Forwarded logs from multiple sources (WinCollect + Rsyslog) into QRadar.  
- Simulated reconnaissance and brute force attacks mapped to MITRE ATT&CK framework.  
- Developed custom QRadar detection rules.  
- Automated threat response by adding malicious IPs into a reference data set (blacklist).  
- Verified attacks using Wireshark packet captures.

# 5. Future Enhancements

- Add ATT&CK techniques (Nmap, Brute Force,persistence, lateral movement, exfiltration).  
- Integrate Sysmon on Windows for richer event logging.  
- Automate detection rules deployment.  
- Expand to include threat hunting dashboards.

# 6. Lab Architecture Diagram

The following diagram illustrates the overall architecture of the lab setup. It shows how the attacker (Kali Linux), victim (Windows), SIEM (QRadar CE), and Wireshark are interconnected in the same network segment (vmnet8).

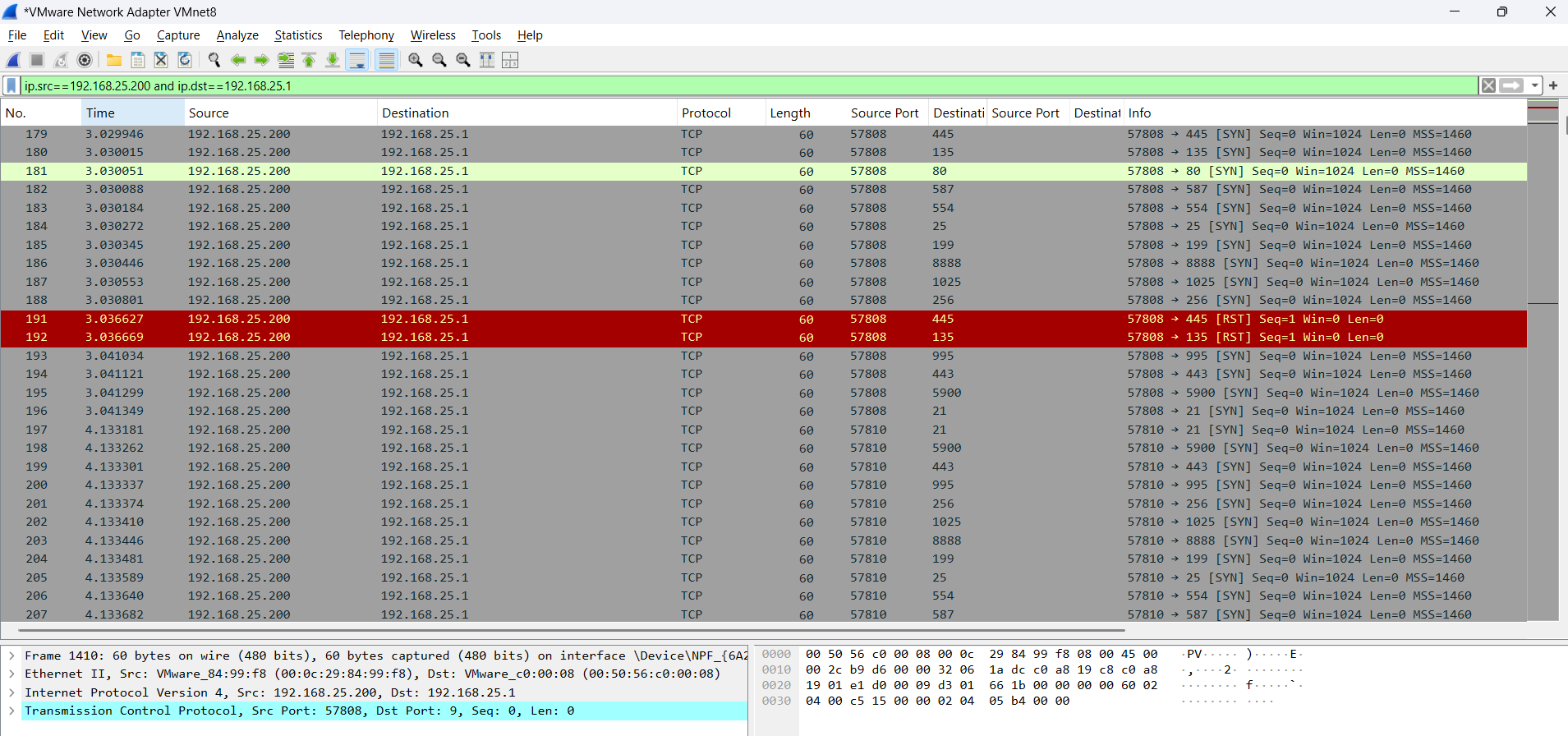
Suggested diagram (to be added manually):  
Kali (192.168.25.200) ---> Windows (192.168.25.1) ---> QRadar CE (192.168.25.100)  
 ↓  
 Wireshark Capture

# 7. Screenshots and Evidence

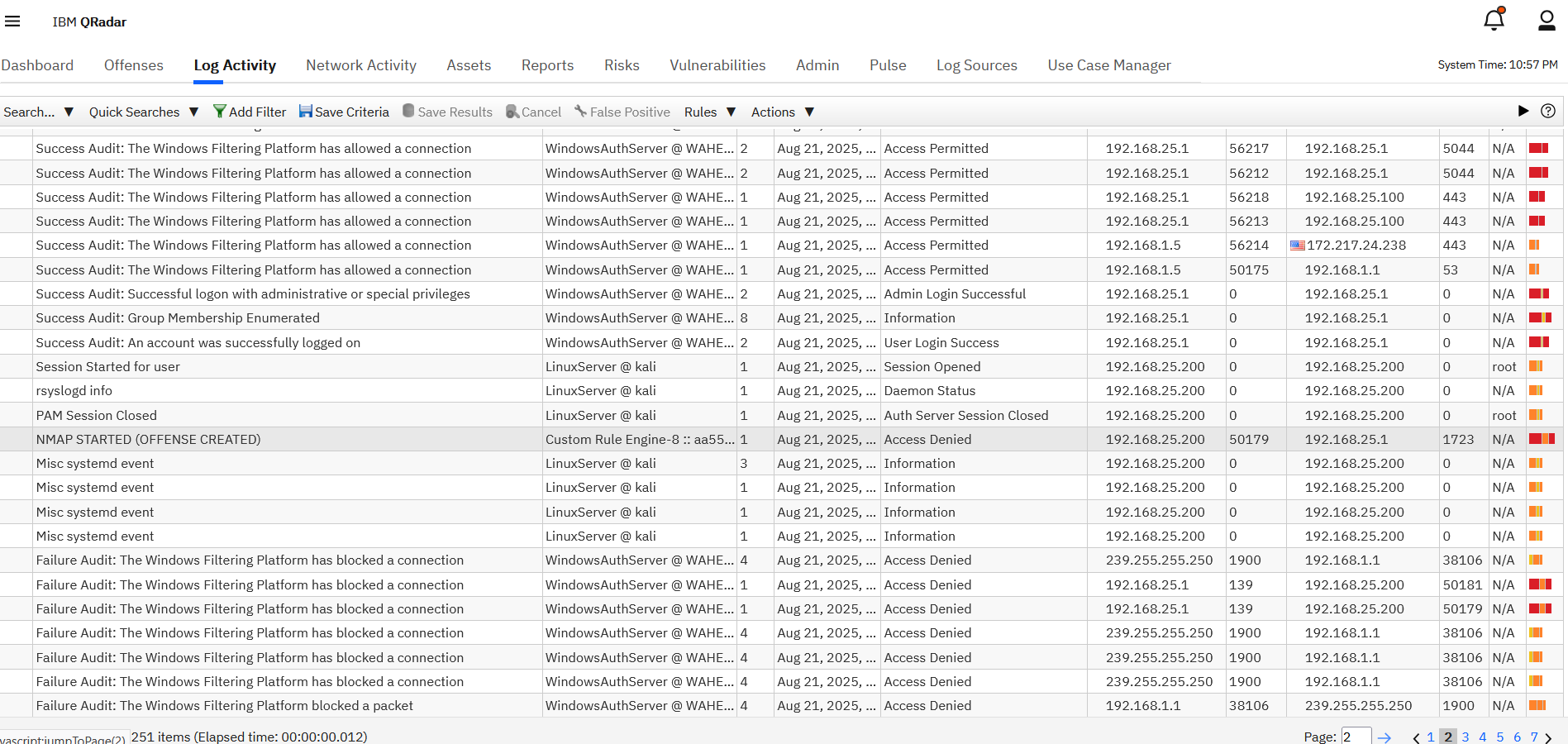
The following screenshots should be inserted here to demonstrate the evidence of attacks and detections:

- Wireshark capture of Nmap scan packets.  
- QRadar offense screen showing detection of Nmap scan.  
- QRadar reference data set showing blacklisted IP.   
- QRadar custom rule configuration screenshot.  
- QRadar offense screen showing brute force detection.

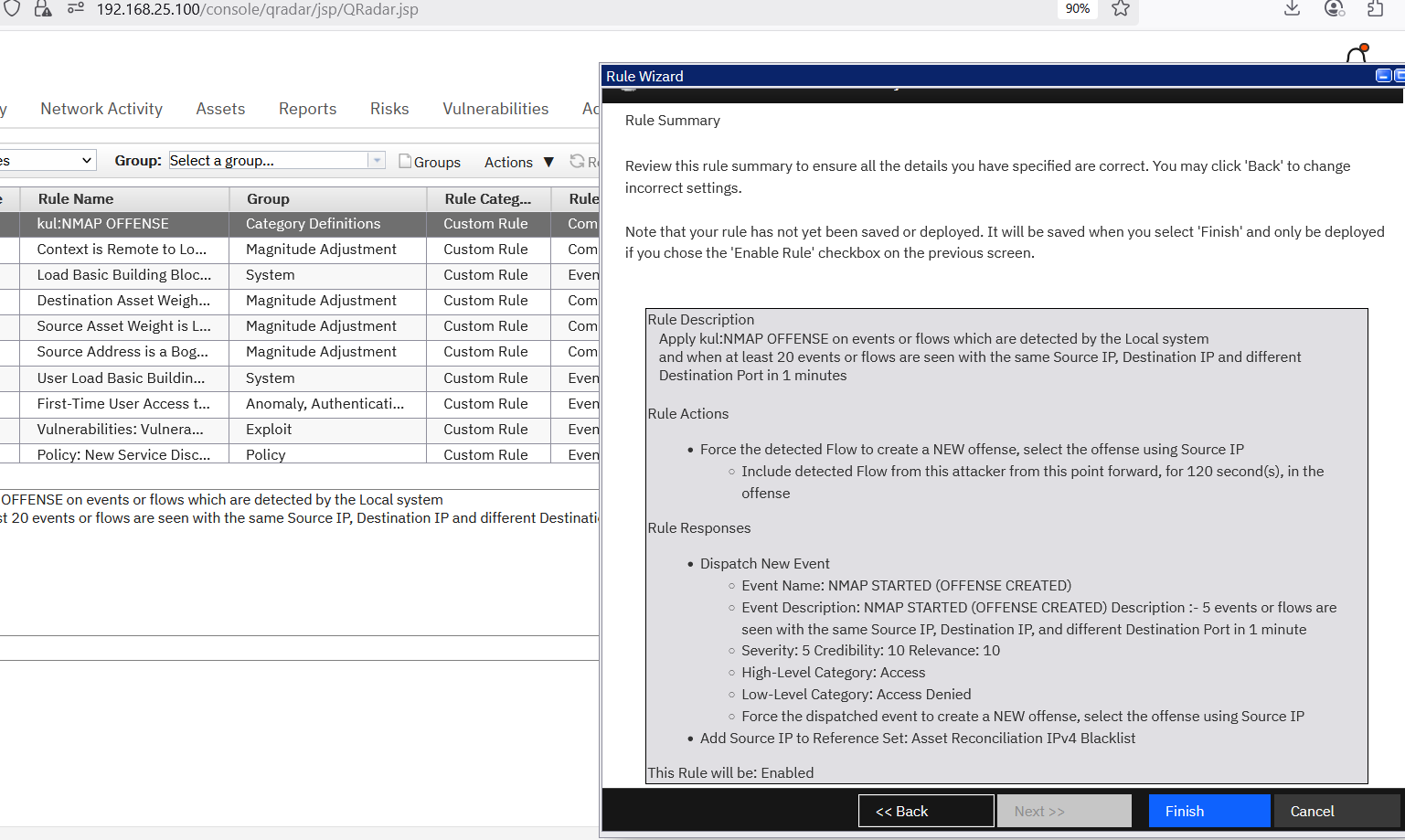
**- Wireshark capture of Nmap scan packets.**



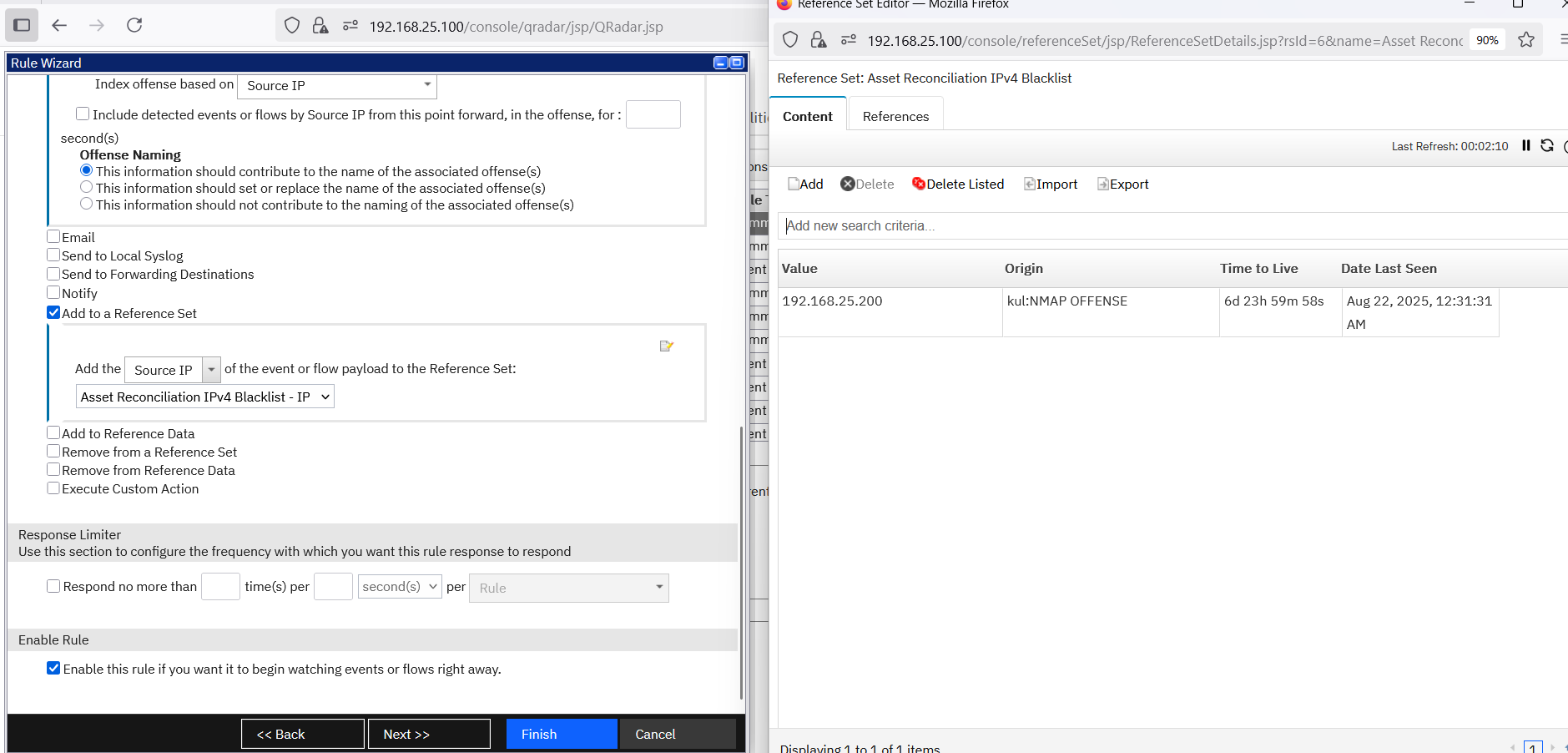
**- QRadar offense screen showing detection of Nmap scan.**

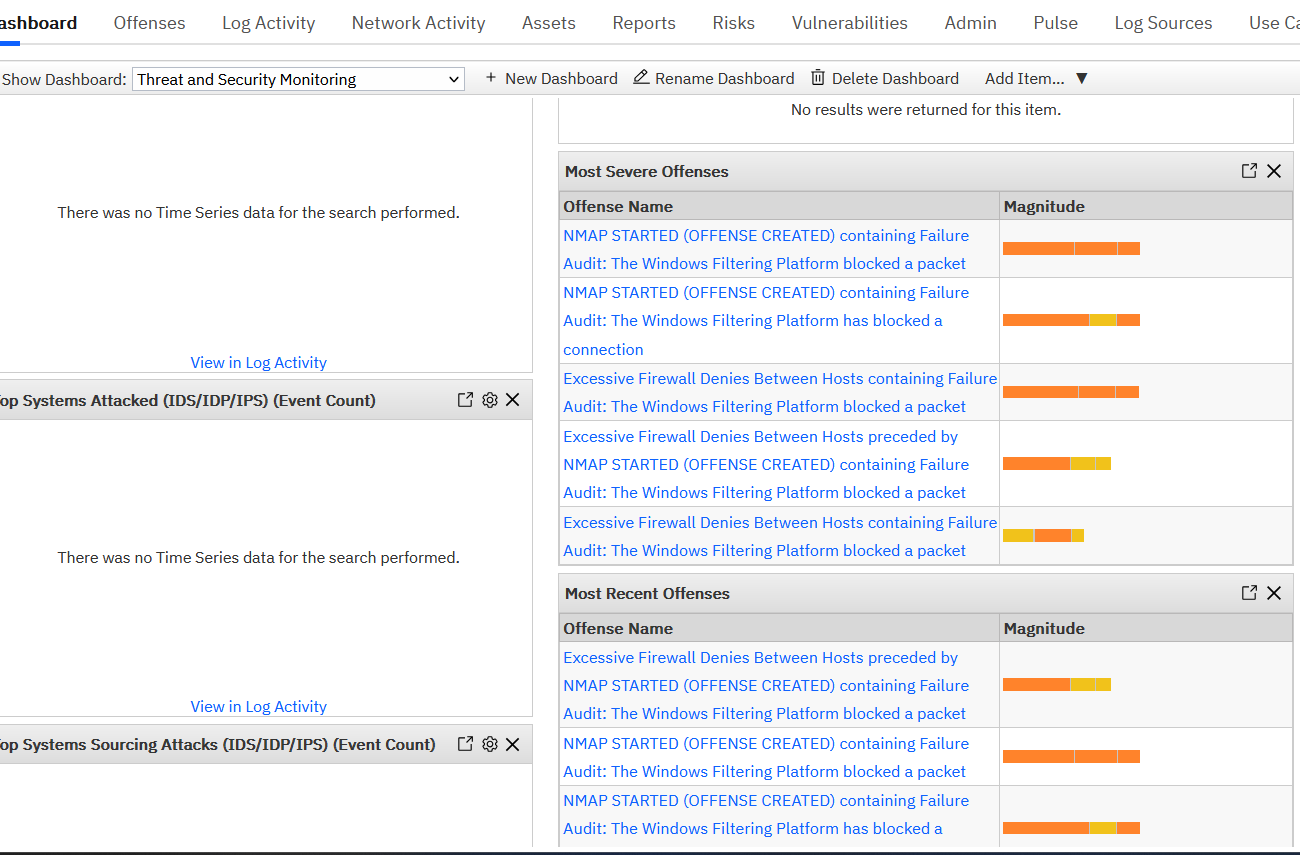


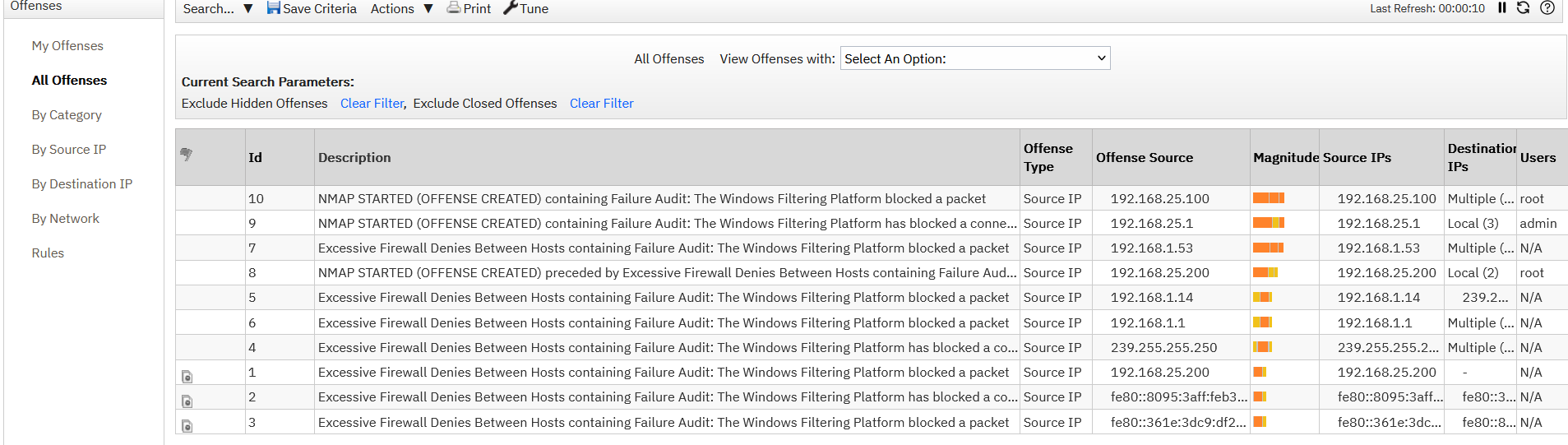
**QRadar custom rule configuration screenshot.**



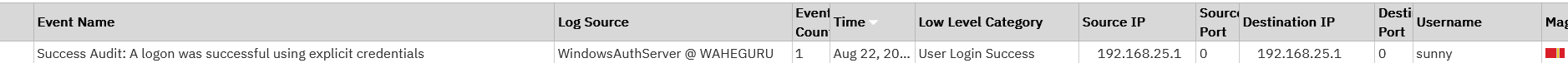
**- QRadar reference data set showing blacklisted IP.**







**- QRadar offense screen showing brute force detection.**



Brute fore initiated from Kali to Windows:-

