Network Security Monitoring with Wazuh and Zeek

Overview

This project implements a **Network Security Monitoring (NSM)** solution by integrating **Zeek** with **Wazuh SIEM/XDR**. The system provides real-time visibility into network traffic and detects reconnaissance activities such as **port scanning** using centralized log analysis and correlation.

Architecture

The detection pipeline follows this flow:

1. **Traffic Monitoring** – Zeek inspects live network traffic on the endpoint
2. **Log Generation** – Zeek produces structured JSON network logs
3. **Log Ingestion** – Wazuh agent forwards Zeek logs to the Wazuh Manager
4. **Detection & Alerting** – Wazuh applies custom rules and generates alerts
5. **Threat Hunting** – Events are visualized in the Wazuh Dashboard

---

Attack Simulation

To validate detection, a controlled port scan was executed:

```
for port in {5555..5559}; do nc -zv <TARGET_IP> $port || true; done
```

This simulates network reconnaissance behavior.

```
root@ubuntu:~# for port in {5555..5559}; do nc -zv 192.168.113.129 $port || true; done
nc: connect to 192.168.113.129 port 5555 (tcp) failed: Connection refused
nc: connect to 192.168.113.129 port 5556 (tcp) failed: Connection refused
nc: connect to 192.168.113.129 port 5557 (tcp) failed: Connection refused
nc: connect to 192.168.113.129 port 5558 (tcp) failed: Connection refused
nc: connect to 192.168.113.129 port 5559 (tcp) failed: Connection refused
```

Detection Result

- Zeek detected repeated connection attempts
- Wazuh correlated the events and triggered **Rule ID 100901**
- Alerts were visible under **Threat Intelligence → Threat Hunting → Events**

	↓ timestamp	agent.name	rule.description	rule.level	rule.id
	Jan 21, 2026 @ 18:20:46.1...	ZEEK	Zeek: DNS Query revoked.grc.com attempted from source ip 192.168.113.129 source port 55973 resolved to IP(s) ["4.79.142.205"]	5	100901
	Jan 21, 2026 @ 18:20:44.1...	ZEEK	Zeek: DNS Query self-signed.badssl.com attempted from source ip 192.168.113.129 source port 55021 resolved to IP(s) ["104.154.89.105"]	5	100901
	Jan 21, 2026 @ 18:20:40.1...	ZEEK	Zeek: Client 192.168.113.129 connected to a server with self-signed certificate 104.154.89.105	8	100906
	Jan 21, 2026 @ 18:18:18.1...	ZEEK	Zeek: DNS Query wazuh.com attempted from source ip 192.168.113.129 source port 34463 resolved to IP(s) ["54.192.151.79","54.192.151.88","54.192.151.63","54...	5	100901
	Jan 21, 2026 @ 18:18:18.1...	ZEEK	Zeek: DNS Query virustotal.com attempted from source ip 192.168.113.129 source port 42740 resolved to IP(s) ["216.239.32.21","216.239.34.21","216.239.38.21","...	5	100901
	Jan 21, 2026 @ 18:17:40.1...	ZEEK	Zeek: DNS Query api.snapcraft.io attempted from source ip 192.168.113.131 source port 58310 resolved to IP(s) ["185.125.188.59","185.125.188.57","185.125.188...	5	100901
	Jan 21, 2026 @ 18:15:34.0...	ZEEK	Zeek: Network event detected	3	100100
	Jan 21, 2026 @ 18:14:26.0...	ZEEK	Zeek: Network event detected	3	100100

Key Outcomes

- Successful detection of network reconnaissance activity
- Centralized visibility of network events in a SIEM platform
- End-to-end validation from traffic capture to alert generation

---

Technologies Used

- **Wazuh** (SIEM/XDR)
- **Zeek** (Network Security Monitoring)
- **Ubuntu Linux**
- **Bash / Netcat**

Skills Demonstrated

- SIEM integration and log correlation
- Network traffic analysis
- Detection engineering
- Linux system administration