**Blue Team Lab: Detecting RDP Brute Force with Winlogbeat + ELK**

**Objective:**

This lab simulated an RDP brute-force attack within a controlled internal network to demonstrate how Windows logs can be forwarded and analyzed using the ELK Stack (Elasticsearch, Logstash, Kibana). The goal was to detect the malicious activity through event code logging and analysis in Kibana.

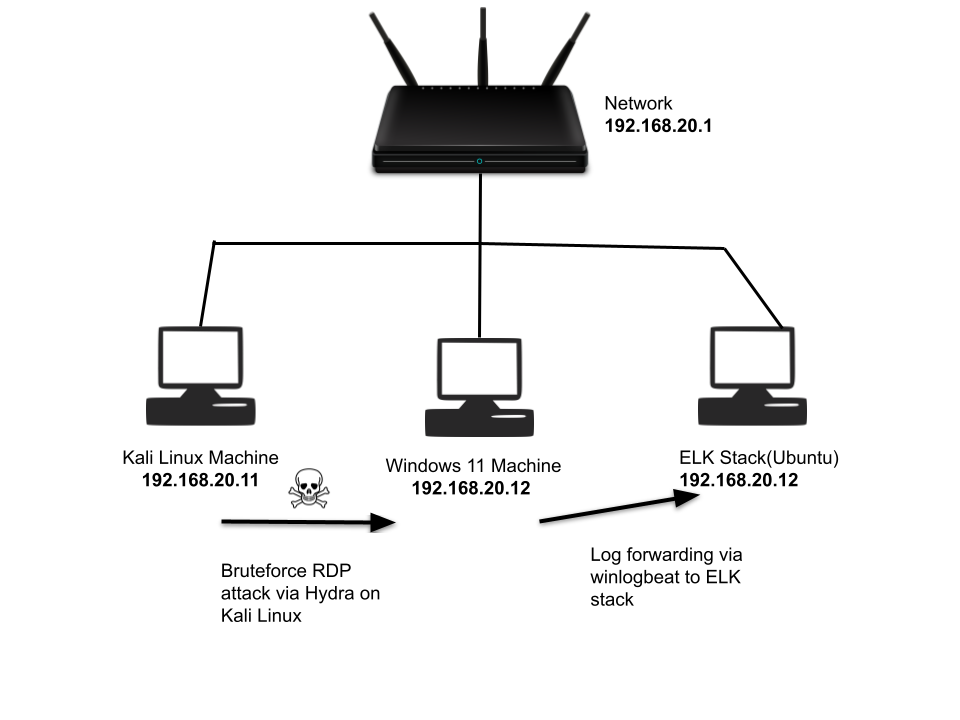
**Lab Setup:**

Kali Linux (Attacker) – 192.168.20.11

Windows 11 Pro (Target) – 192.168.20.10

Ubuntu ELK Stack (SIEM) – 192.168.20.12

All machines were connected to a virtual internal network. Winlogbeat was installed on the Windows machine to forward logs to Elasticsearch, where they were visualized in Kibana.



**Tools Used:**

Hydra – to simulate the brute-force RDP attack from Kali

Winlogbeat – to ship Windows logs to ELK

Kibana – for log visualization and event correlation

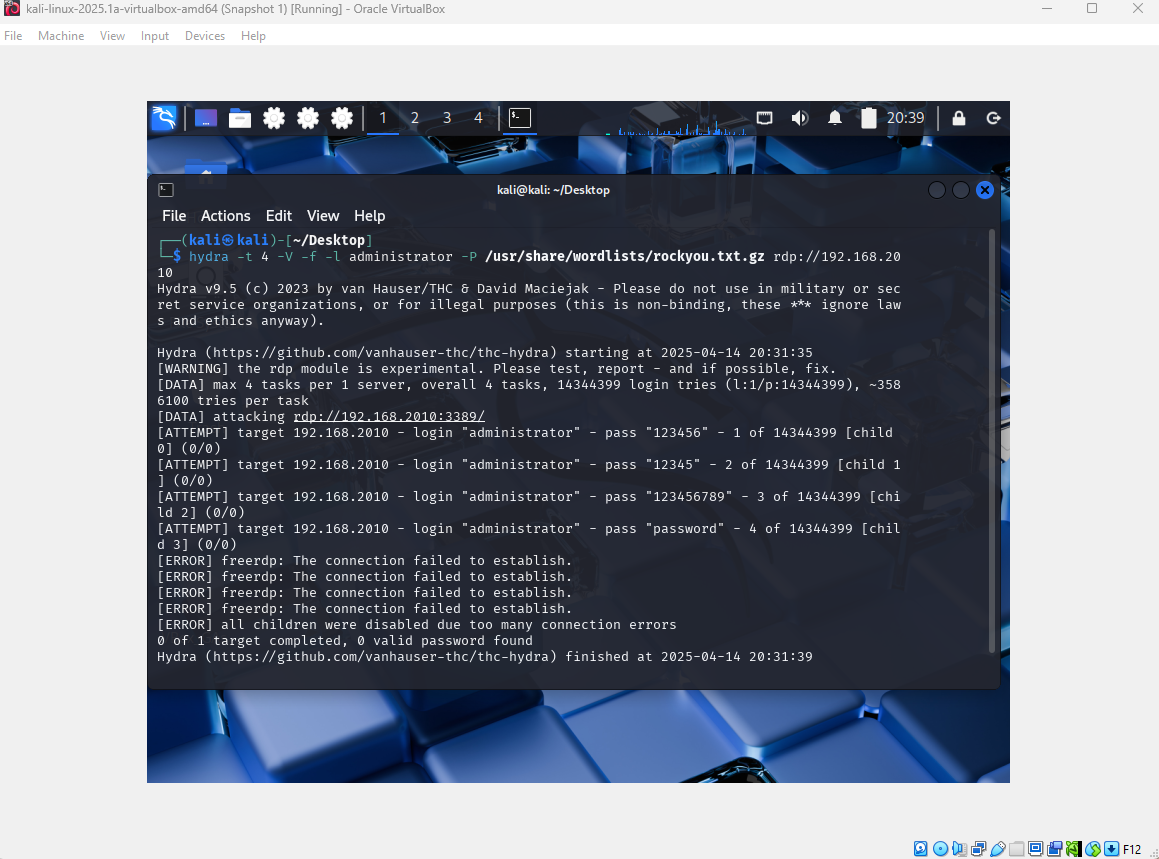
Elasticsearch + Logstash – for log storage and parsing

Attack Simulation

Using Kali, a brute-force RDP attack was launched against the Windows 11 machine:

hydra -t 4 -V -f -l Administrator -P /usr/share/wordlists/rockyou.txt rdp://192.168.20.10

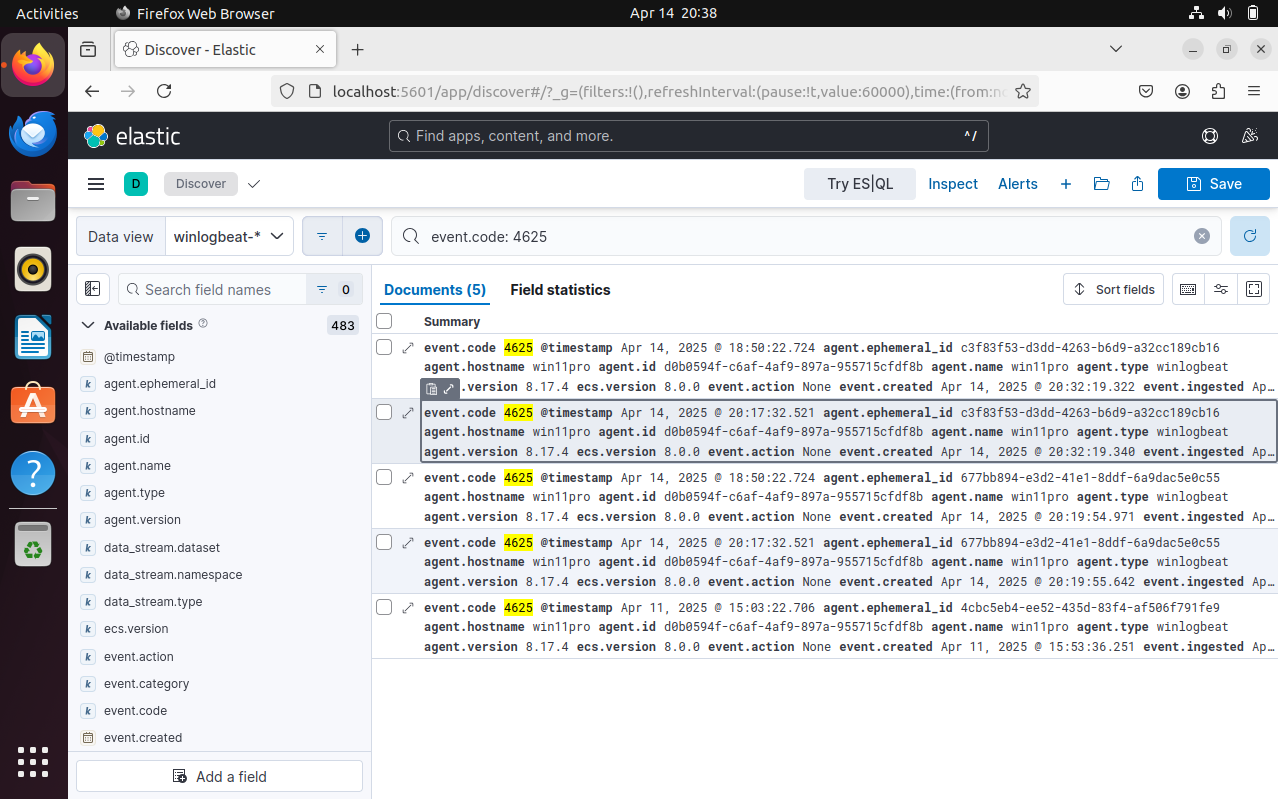
This simulated an attacker attempting multiple login combinations via RDP.



**Detection in ELK:**

On the ELK stack (Kibana), Event ID 4625 (failed login attempt) was searched using the Discover tab event.code: 4625

These logs confirmed the brute-force activity, showing multiple failed login attempts from the Kali IP.



**Outcome:**

The brute-force attack was successfully detected and logged using Winlogbeat and visualized in Kibana. This demonstrates a basic but critical use case for log correlation, alerting, and threat detection in a Blue Team environment.

**Skills Demonstrated:**

Event log forwarding (Winlogbeat → ELK)

ELK Stack deployment and configuration

Brute-force attack simulation (Hydra)

SIEM-based detection using Kibana

Windows event code analysis (Event ID 4625)