■ Home Lab Project #2 – RDP Brute Force Simulation

■ Objective

Simulate a brute-force attack against RDP from Kali Linux, then review indicators of compromise (IOCs) using Wireshark and Event Viewer.

■ Lab Setup

- Windows VM: RDP Enabled

- Kali VM: Used Hydra for attack simulation

■ Step-by-Step Walkthrough

Step 1 – Enable RDP on Windows
Settings → System → Remote Desktop → Enable Remote Desktop

Step 2 – Verify RDP Service

```
netstat -an | find ":3389"
```

Step 3 – Capture RDP Traffic with Wireshark
Started capture on TCP/3389

Step 4 – Launch Hydra Brute Force from Kali

```
hydra -l <username> -P <wordlist> rdp://<WINDOWS_IP>
```

Step 5 – Analyze Logs and Traffic
Wireshark: Observed repeated RDP connection attempts
Event Viewer: Looked for Event ID 4625 (failed logon attempts)

■ Key Findings

■ Hydra generated multiple failed RDP logon attempts

■ Windows logs recorded source IP, username, and failure reason

■ Wireshark clearly displayed RDP connection attempts

■ Lessons Learned

- Brute-force attacks are noisy and easily detectable with proper logging.

- Event ID 4625 is key for detecting RDP attacks.

- Correlating network and log data helps create effective detection rules.

■ Detection & Prevention

■ Detection: Create SIEM rules to alert on multiple Event ID 4625 within a short time window.

■ Prevention: Enable account lockout policies, restrict RDP to specific IP ranges or VPN, use strong passwords, and implement rate limiting (e.g., Fail2ban).