📄 Practical 6: Risk Assessment Practice Report

Objective

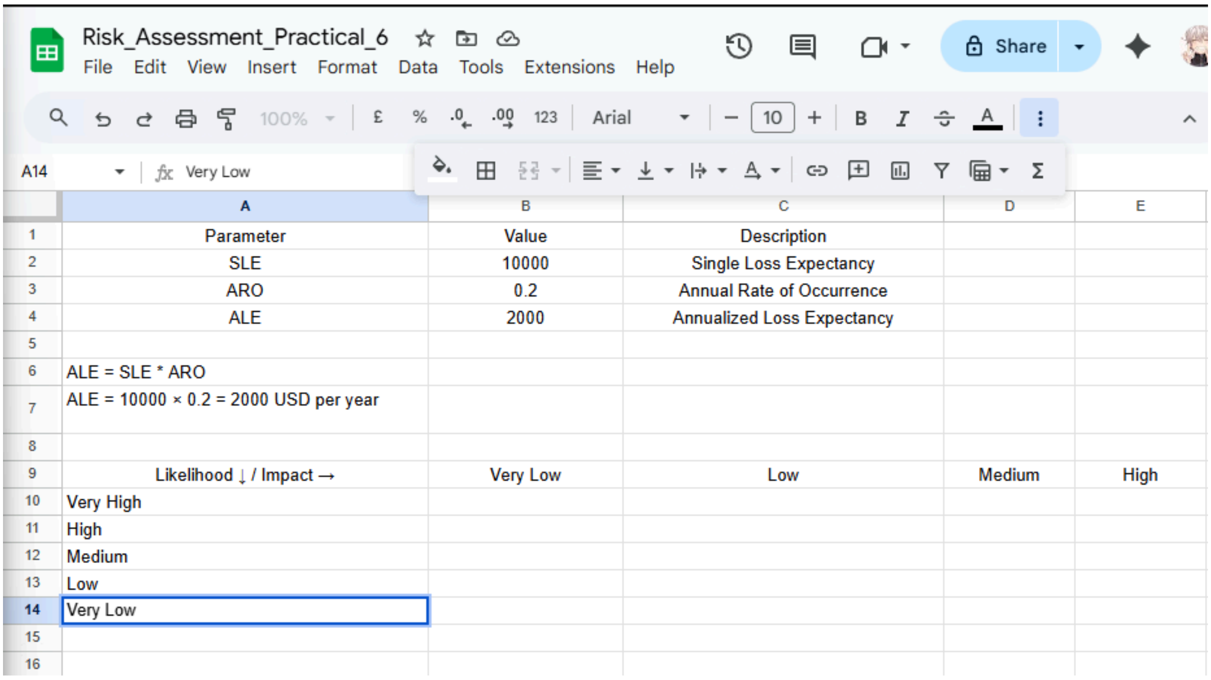
The objective of this practical was to perform a **cybersecurity risk assessment** using both **quantitative and qualitative techniques**. The task focused on calculating **Annualized Loss Expectancy (ALE)** and evaluating risk severity using a **5×5 risk matrix** for a ransomware attack scenario.

Tools Used

- **Google Sheets** – for calculations and risk visualization
- **Risk Assessment Methodology** – Quantitative (ALE) and Qualitative (Risk Matrix)

Scenario Description

A vulnerable system similar to **Metasploitable2** contains outdated and misconfigured services. An attacker exploits these vulnerabilities and deploys **ransomware**, resulting in data unavailability, potential financial loss, and operational disruption.



Risk_Assessment_Practical_6
File Edit View Insert Format Data Tools Extensions Help
Share
100%
Arial
10
A14
Very Low

	A	B	C	D	E
1	Parameter	Value	Description		
2	SLE	10000	Single Loss Expectancy		
3	ARO	0.2	Annual Rate of Occurrence		
4	ALE	2000	Annualized Loss Expectancy		
5					
6	ALE = SLE * ARO				
7	ALE = 10000 × 0.2 = 2000 USD per year				
8					
9	Likelihood ↓ / Impact →	Very Low	Low	Medium	High
10	Very High				
11	High				
12	Medium				
13	Low				
14	Very Low				
15					
16					

Quantitative Risk Assessment (ALE)

Parameters Used

- **Single Loss Expectancy (SLE):** $10,000
- **Annual Rate of Occurrence (ARO):** 0.2

ALE Calculation

The Annualized Loss Expectancy was calculated using the formula:

ALE = SLE × ARO

ALE=10,000×0.2=2,000ALE = 10,000 \times 0.2 = 2,000ALE=10,000×0.2=2,000

Result:
The organization is expected to lose **$2,000 per year** due to this risk.

Qualitative Risk Assessment (Risk Matrix)

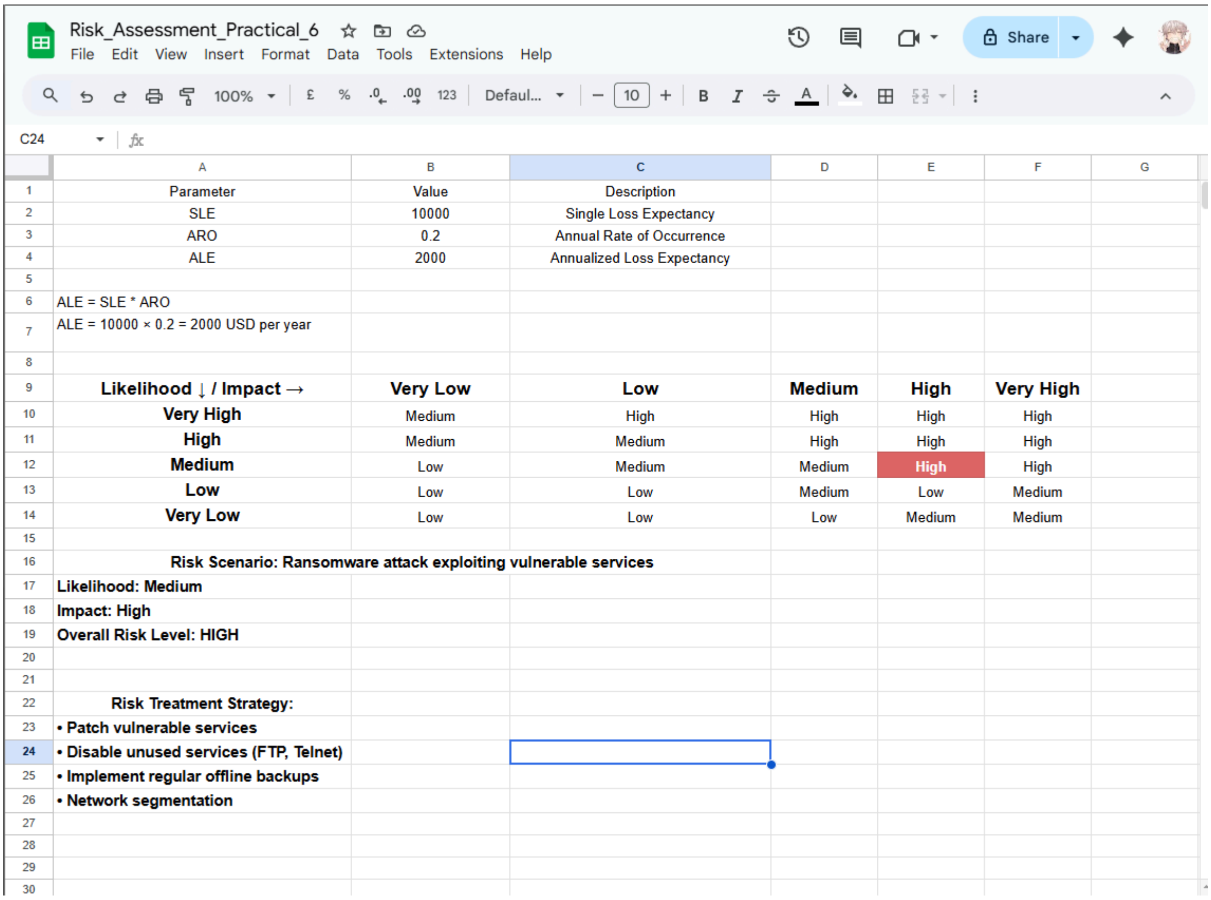
A **5×5 risk matrix** was created in Google Sheets with:

- **Likelihood levels:** Very Low to Very High
- **Impact levels:** Very Low to Very High

The ransomware scenario was evaluated with:

- **Likelihood:** Medium
- **Impact:** High

This placed the risk in the **High-risk category**, which was highlighted in the matrix.



	A	B	C	D	E	F	G
1	Parameter	Value	Description				
2	SLE	10000	Single Loss Expectancy				
3	ARO	0.2	Annual Rate of Occurrence				
4	ALE	2000	Annualized Loss Expectancy				
5							
6	ALE = SLE * ARO						
7	ALE = 10000 × 0.2 = 2000 USD per year						
8							
9	**Likelihood ↓ / Impact →**	**Very Low**	**Low**	**Medium**	**High**	**Very High**	
10	**Very High**	Medium	High	High	High	High	
11	**High**	Medium	Medium	High	High	High	
12	**Medium**	Low	Medium	Medium	**High**	High	
13	**Low**	Low	Low	Medium	Low	Medium	
14	**Very Low**	Low	Low	Low	Medium	Medium	
15							
16	**Risk Scenario: Ransomware attack exploiting vulnerable services**						
17	**Likelihood: Medium**						
18	**Impact: High**						
19	**Overall Risk Level: HIGH**						
20							
21							
22	**Risk Treatment Strategy:**						
23	**• Patch vulnerable services**						
24	**• Disable unused services (FTP, Telnet)**						
25	**• Implement regular offline backups**						
26	**• Network segmentation**						
27							
28							
29							
30							

Risk Evaluation & Treatment

Risk Level

- **Overall Risk Level: HIGH**

Recommended Risk Treatment

Risk mitigation was selected as the appropriate strategy. The following controls were proposed:

- Patch and update vulnerable services
- Disable unused services such as FTP and Telnet
- Implement regular offline backups
- Apply network segmentation to limit lateral movement

Errors and Limitations

- Risk values were based on estimates and assumptions
- Real-world impact may vary depending on organizational size
- Likelihood values may change over time with threat landscape evolution

Learning Outcomes

Through this practical, the following skills were developed:

- Understanding of quantitative and qualitative risk assessment
- Hands-on calculation of Annualized Loss Expectancy
- Creation and interpretation of a risk matrix

- Decision-making for risk treatment strategies

Conclusion

This practical successfully demonstrated how cybersecurity risks can be analyzed and prioritized using structured risk assessment methods. The ransomware scenario highlighted that even moderately likely events can result in significant annual losses, emphasizing the importance of proactive risk mitigation and security controls.