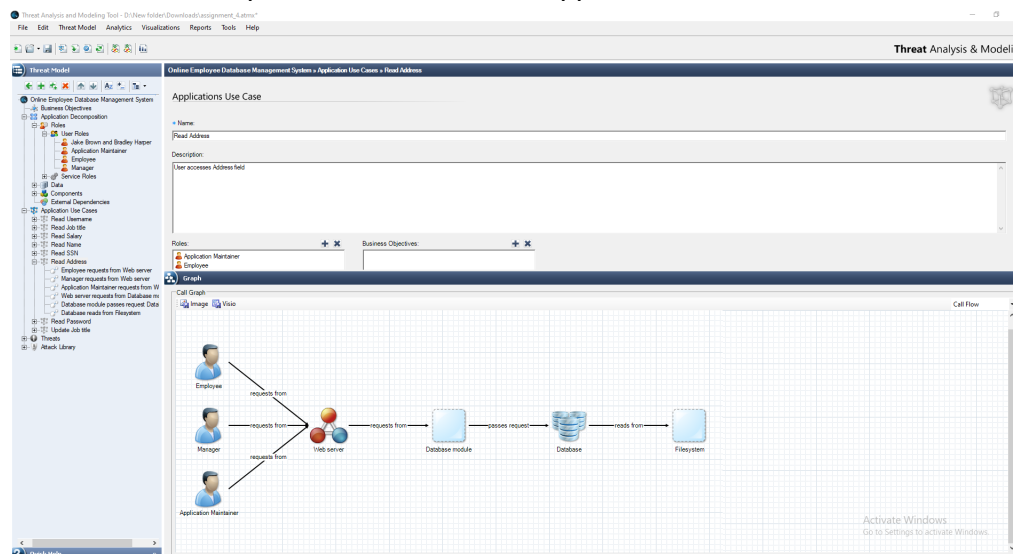


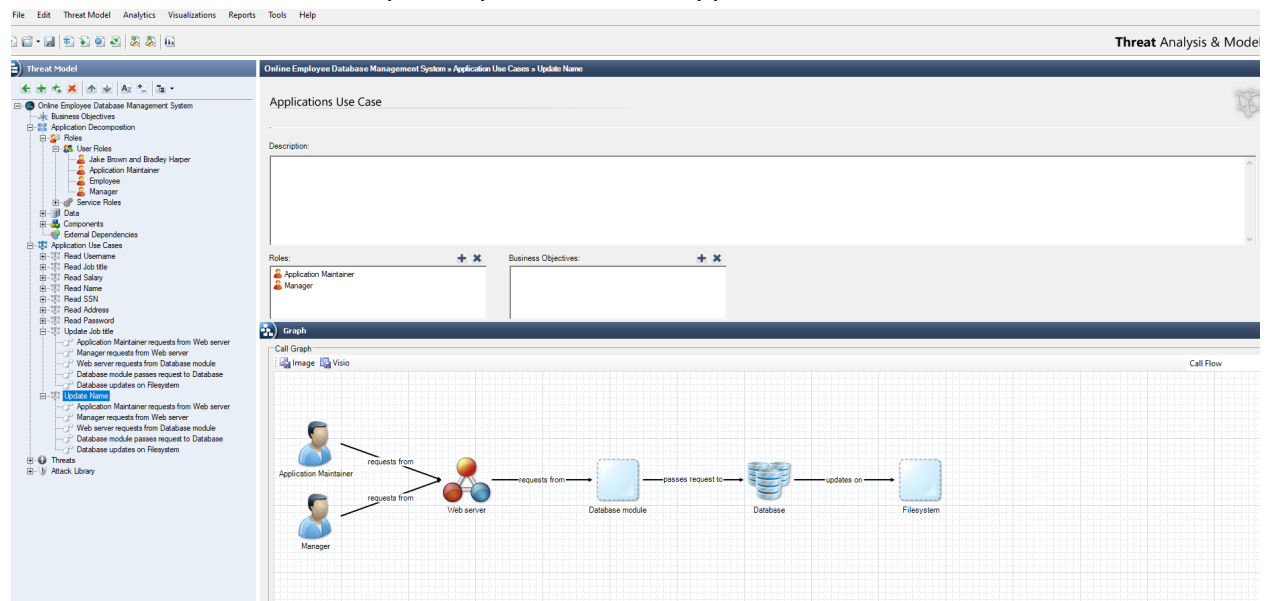
- 1 . Change name of Server Administrator to partners name: JakeBrown_BradHarper
- 2 . List the Data items: Username, Password, Job Title, Salary, Name, Social Security number, Address
- 3 . Write down the security policy of the system in the natural language
 - Application Maintainer can Create, Read, Update, or Delete any data
 - Employee can read username, job title, salary, name, social security number, and address. And can read and update password.
 - JakeBrown_BradHarper (Administrator) can Create, Read, Update, or Delete any data
 - Manager can read username, name, social security number, and address. And can read and update job title and salary.
- 4 . In the tool change the security policy where the Employee can update the Address, only if it is his/her own address.

Access Control						
	Role	Create	Read	Update	Delete	Condition
▶	Jake Brown and Bradley H	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Employee	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	If it is their own address
	Application Maintainer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Manager	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
*		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

- 5 . In the tool, complete Read Address in Application Use Cases.



6 . In the tool create and complete Update Name in Application Use cases.



7 . Add a threat in each of the threat categories.

Confidentiality:

The screenshot shows the 'Confidentiality Threat' form. The 'Name' field is 'Manager's address exposed'. The 'Description' field contains 'Attacker received manager's home address'. The 'Call' field is empty. The 'Primary Threat Factors' section has 'Unauthorized disclosure of the identity' checked. The 'Risk Measures' section shows 'Impact: Medium', 'Probability: Medium', and 'Risk Rating: 4'. The 'Risk Response' section has 'Avoid' selected. The 'Justification' field contains 'Address can be used for physical attacks or attacks on the home'. The 'Attack Countermeasures' section has 'Regulation Attack: Disable anonymous access and authenticate every principle' and 'Regulation Attack: Implement proper and effective logging' checked.

Integrity:

Online Employee Database Management System » Integrity » Integrity Threat 2

Integrity Threat

Name: Breach of Data

Description:

Call:

Primary Threat Factors

☒ Violation of access control
☐ Violation of business rule
☒ Violation of data integrity

Risk Measure

Impact: High Probability: High Risk Rating: 9

Risk Response

Risk Response: None

Justification: A data breach could lead to data being altered, damaged, stolen, sold, etc...

Attack Countermeasure

☒ Denial of Service - Use of shared resources (e.g., shared files) should be considered at design time
☒ HTTP Replay Attack - Associate state with requests & users

Availability:

Online Employee Database Management System » Availability » Ddos (denial of service)

Availability Threat

Name: Ransomware

Description: Withholding information or data until a payment is made for the information.

Call:

Primary Threat Factors

☒ Unavailability
☐ Performance degradation

Risk Measure

Impact: High Probability: Medium Risk Rating: 6

Risk Response

Risk Response: Accept

Justification: Usually cheaper to pay now and update your system to avoid future attacks

Attack Countermeasure

☒ LDAP Injection - Untreated input should be validated against an inclusion list

8 . Can you think of any other components that could have been considered but were left out of the model?

Log of changes made and/or data grabbed, add authentication as an attack type

9 . Is there anything you found interesting in using the software?

- The software was actually very easy to use and operate, even though it looked complicated and complex at first glance.
- It was a very cool and easy to understand method of the various cyber attacks as well as relations among types of users. It was very helpful to see the different methods of counterattack and response laid out as well as the probability and risk levels of the a security threat

Our team consisted of Jake Brown and Bradley Harper. Each of the members helped to contribute to the changing, creating, and updating of each task in the Modeling Tool. Jake Brown helped to create the document containing the answers to the nine questions, while assisting Bradley Harper in using the Modeling tool. Bradley Harper was tasked with manually doing the tasks in the modeling tool with assistance from Jake Brown. Bradley Harper was tasked with altering the .atmx file.