



Cyber Security

Capstone Project: Threat Modeling

Background of the problem statement:

Big Mart has a chain of retail stores, selling daily groceries and home requirements across the country.

Lately, it has been losing market share to online competitors who are providing a better customer experience than Big Mart's brick and mortar establishments. Big Mart wants to secure #1 market leader position for daily groceries and home requirements by adopting a digital strategy.

The company plans to provide a secure, uninterrupted, and enhanced user experience to its existing and prospective customers.

Big Mart , Inc., has contracted your organization to perform a threat modeling exercise for its online strategy.

Big Mart provides the following requirements:

- Customers should be able to search for products and place their orders using the online web store.
- Customer needs to create an account prior to placing an order.
- Customers can pay with their credit card, debit card, online banking or digital wallet.
- Sales team can view customer order details in order to process and deliver it.
- Administrators can modify product information.

The requirements study results in the following statements and requirements:

- The web store will need to be accessible from the Intranet as well as the Internet.
- The web store will need to be designed with a distributed architecture for scalability reasons.
- Users will need to authenticate to the web store with the user account credentials which in turn will authenticate to the backend database (deployed internally) via a web services interface.
- Credit card processing will be outsourced to a third-party processor.
- User interactions with the web store will need to be tracked.
- The database will need to be backed up periodically to a third-party location for disaster recovery (DR) purposes.

Programming language used is Python and the backend database can be either Oracle or Microsoft SQL Server. The Web Server used is Nginx.

Task 1

Identifying the business and security objectives.

Phase 1 – Identify Assets

Assets are anything that has value to an organization and needs to be protected. In the context of threat modeling for a company, assets can refer to physical, digital, and intellectual property that are critical to the operation of the business. These assets can include:

Data: including customer data, financial information, and intellectual property.

IT infrastructure: including servers, network devices, and storage systems.

Applications: including web-based applications, mobile applications, and desktop applications.

Physical assets: including buildings, equipment, and vehicles.

People: The employees, contractors, or partners who have access to the company's systems, data, or processes, as well as their roles and permissions.

Human resources: including employee data, training records, and performance evaluations.

Reputation: the company's image, brand, and customer trust.

Task 2

- Identify human and non-human actors of the systems
- Identify data elements
- Identify technologies that will be used to develop the application
- Identify external dependencies
- Identify threat actors

Phase 2 – Create Architecture Overview

Human actors:

Customers: These are the end-users of the web store who browse for products, place orders, and make payments.

Sales team: They are responsible for viewing customer order details in order to process and deliver the orders.

Administrators: They can modify product information in the backend database.

Non-human actors:

Web server: This component hosts the web store and serves the web pages to customers over the internet or intranet.

Database: This stores all the data related to products, orders, customers, and payment information

Payment processor: This is a third-party service that handles credit card processing on behalf of Big Mart.

Data elements:

Customer order details: This includes information such as product details, quantities, shipping address, payment information, etc.

User account information: This includes login credentials, personal information, and order history.

Product information: This includes product names, descriptions, prices, and availability status.

Payment information: This includes credit card or debit card details, online banking login credentials, or digital wallet details.

Order history: This includes a record of all the past orders placed by the customers.

Technologies:

Nginx web server: This is the web server used to host the web store.

Python programming language: This is the programming language used to develop the web application.

Oracle or Microsoft SQL Server database options: These are the two database options available for storing the data.

Web services interface: This is the interface used to communicate between the web application and the backend database.

External dependencies:

Third-party payment processor: This is an external service that handles credit card processing on behalf of BigMart.

Backup service: This is an external service used for periodic backups of the database for disaster recovery purposes.

Threat actors:

Potential attackers: These could be malicious actors who may attempt to exploit vulnerabilities in the system to gain unauthorized access to data, disrupt service, or steal sensitive information.

Hacktivists: These are individuals or groups who may attempt to disrupt or damage the company's online operations as a form of protest or political action.

Competitors: BigMart's online competitors may attempt to gain a competitive advantage by stealing customer data or disrupting service.

Insiders: Current or former employees of the company who have access to sensitive information may pose a threat if they decide to misuse that information for personal gain or to harm the company.

Cybercriminals: These individuals or groups may attempt to exploit vulnerabilities in the system to steal sensitive information, such as credit card numbers or customer data, to sell on the dark web or use for fraudulent activities.

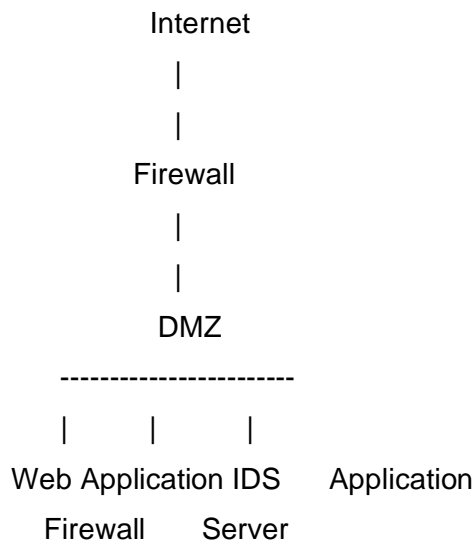
Nation-state actors: Nation-state actors may target the company's online infrastructure to gain intelligence or disrupt operations as part of a larger political or economic agenda.

Task 3

Create a physical network topology using the following information:

- Use Firewall for boundary protection
- Use Web application Firewall to protect the application
- Use security solutions such as IDS to monitor for malicious traffics
- Application server is placed in the DMZ
- Database server is placed in the Internal network

Phase 3 – Decompose Architecture





In this topology, the Internet is connected to a firewall for boundary protection. The DMZ is located behind the firewall and contains the web application firewall, which protects the application server. The web application firewall monitors and filters traffic between the Internet and the application server. An IDS is placed in the DMZ to monitor for malicious traffic.

The application server is located in the DMZ and is separated from the database server, which is placed in the internal network. This helps to protect the database server from direct attacks from the Internet. The LAN connects the application server and the database server together.

Firewall:

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. In the context of BigMart's architecture, the firewall would be used for boundary protection, which means it would sit between the internal network (where the database server is located) and the external network (where customers access the web store). This helps prevent unauthorized access and can be used to block malicious traffic.

For example, BigMart might use a physical firewall appliance to control traffic entering and leaving the internal network. The firewall rules could be set up to block all traffic except for **HTTP/HTTPS** traffic originating from the web server and database traffic originating from the application server in the **DMZ**.

Web Application Firewall (WAF):

A web application firewall is a type of firewall that specifically protects web applications by monitoring and filtering incoming traffic to the web server. In the context of BigMart, **the WAF** would be used to protect the web store from attacks such as **SQL injection and cross-site scripting**.

For example, BigMart might use a software-based WAF that sits in front of the web server and analyzes incoming traffic for known attack patterns. The WAF could be configured to block traffic that matches a known **attack signature** or traffic that contains **malicious payloads**.

Intrusion Detection System (IDS):

An IDS is a system that monitors network traffic for signs of **malicious activity or policy violations**. In the context of BigMart, the IDS would be used to monitor traffic entering and leaving the internal network to **detect any suspicious activity**. For example, BigMart might use a software-based IDS that monitors traffic flowing through the firewall. The **IDS** could be configured to send an alert if it detects traffic that matches a known attack signature or if it detects a large volume of traffic coming from a particular **IP address**.

DMZ:

A **DMZ (demilitarized zone)** is a network segment that sits between the internal network and the external network. In the context of BigMart, the application server is placed in the DMZ to provide a layer of protection between the external network (where customers access the web store) and the internal network (where the **database server is located**). For example, BigMart might use a virtualized DMZ that sits on the same physical server as the **web server**. The DMZ could be configured to only allow incoming **HTTP/HTTPS traffic** from the external network and outgoing database traffic to the internal network.

Internal network:

The internal network is the network segment that contains the database server and other internal systems. In the context of BigMart, the database server is placed in the internal network to provide an additional layer of protection against unauthorized access. For example, BigMart might use a **VLAN (virtual local area network)** to isolate the internal network from the external network. The VLAN could be configured to only allow traffic from the application server in the **DMZ and the backup server** for disaster recovery purposes.

Overall, this physical network topology is designed to provide a layered approach to network security for BigMart. By using a **firewall, WAF, IDS, DMZ, and internal network**, BigMart can

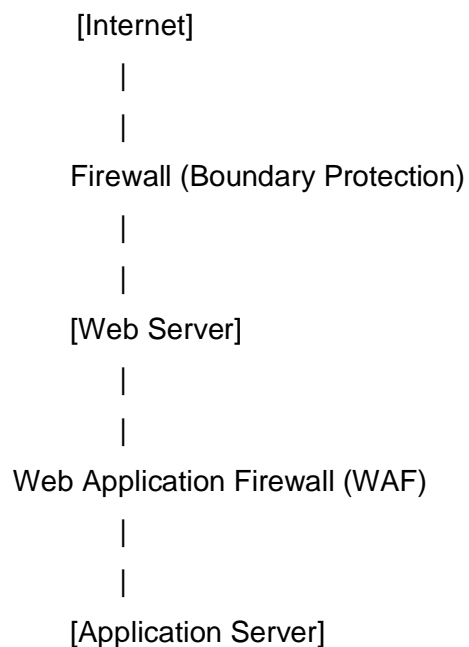
help prevent unauthorized access, detect and block malicious traffic, and protect sensitive data such as customer information and order details.

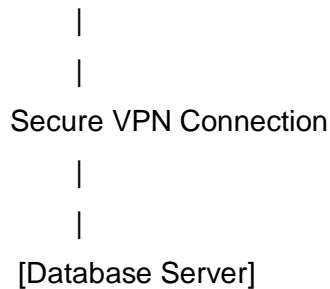
Task 4

Create a logical topology using the following information:

- Customers use SSL/TLS to access the web store
- There is a trust boundary between the web server and application
- There is a trust boundary between the application and database
- Connection between application is via a secure VPN

Phase 4 – Identify Threats





In this diagram, the customer connects to the web server using **SSL/TLS encryption**. The web server is protected by a firewall, which creates a trust boundary between the web server and the external network. The **web application firewall (WAF)** provides additional protection for the application server, which is located in the DMZ. The application server communicates with the database server over a **secure VPN connection**, with a trust boundary between **the two**.

SSL/TLS implementation vulnerabilities:

While SSL/TLS is a secure way to access the web store, there could be vulnerabilities in the implementation that could allow an attacker to intercept or modify data being transmitted between the customer and the web server. For example, a man-in-the-middle attack could occur if an attacker intercepts the SSL/TLS connection and poses as the legitimate web server to steal sensitive information from the customer.

Web application firewall misconfigurations:

While a web application firewall is an important security measure to protect the application, it is also important that it is configured correctly. Misconfigurations could lead to false positives or false negatives, allowing attackers to bypass the firewall or legitimate traffic to be blocked.

Trust boundary breaches:

There are two trust boundaries in this system - between the web server and application, and between the application and database. If an attacker is able to breach either of these boundaries, they could gain unauthorized access to sensitive information or compromise the system in other ways. For example, if an attacker is able to compromise the web server, they may be able to execute malicious code on the application server or gain access to the database server.

VPN vulnerabilities:

While using a secure VPN connection between applications is important for protecting data in transit, there could be vulnerabilities in the VPN implementation that could allow an attacker to intercept or modify the data being transmitted. Additionally, if the VPN credentials are compromised, an attacker could use them to gain unauthorized access to the network.

Task 5

- Apply the STRIDE model to identify relevant threats (minimum 1 per element). Use OWASP Top 10 list as reference.

Phase 5 – Document Threats

The **STRIDE model** to identify relevant threats for BigMart, a fictional retail company:

Spoofing:

Threat: An attacker could impersonate a BigMart employee or customer to gain unauthorized access to sensitive information or systems.

Example: An attacker creates a fake email from BigMart's HR department, asking employees to click on a link to update their personal information. When employees enter their login credentials on the fake website, the attacker captures their information.

Tampering:

Threat: An attacker could modify data or code in transit or at rest, leading to unauthorized changes in the system's behavior.

Example: An attacker intercepts a request to update the price of a product on BigMart's website and changes the price to a lower amount. The attacker then purchases the product at the lower price before the change is detected.

Repudiation:

Threat: An attacker could deny their actions or activities in the system, making it difficult to track or identify the source of an attack.

Example: A customer claims they did not make a purchase on BigMart's website, even though the transaction shows up in the system. The attacker used stolen credit card information to make the purchase and is now denying their involvement.

Information disclosure:

Threat: An attacker could access sensitive information, such as personal or financial data, without authorization or legitimate need.

Example: An attacker gains access to BigMart's database and steals customer information, including names, addresses, and credit card numbers. The attacker then sells this information on the dark web for profit.

Denial of service:

Threat: An attacker could overwhelm BigMart's systems or network, making it unavailable to legitimate users.

Example: An attacker uses a DDoS (Distributed Denial of Service) attack to flood BigMart's website with traffic, making it inaccessible to customers trying to make purchases.

Elevation of privilege:

Threat: An attacker could gain unauthorized access to higher privileges or levels of access in the system, allowing them to perform actions they are not authorized to do.

Example: An attacker gains access to a low-privileged user account on BigMart's network, then uses a privilege escalation vulnerability to gain administrative access to the system. The attacker can now perform any action they want on the system.

Task 6

Phase 6 – Rate Threats

Threat description	Threat target	Attack techniques	Controls/Countermeasures
Spoofing attack	Authentication mechanisms	Phishing, social engineering, exploiting vulnerabilities	Strong authentication mechanisms (e.g., multi-factor authentication, secure password policies), user awareness training, monitoring and logging of authentication attempts
Tampering attack	Data integrity	Man-in-the-middle attacks, injection attacks, modifying files	Encryption of sensitive data, integrity checks, access control, monitoring and logging of data changes

Threat description	Threat target	Attack techniques	Controls/Countermeasures
Repudiation attack	Non-repudiation mechanisms	Denial of service, manipulating audit logs	Implementing non-repudiation mechanisms (e.g., digital signatures, timestamps), secure audit logging, monitoring and alerting
Information disclosure	Confidentiality of data	SQL injection, cross-site scripting, exploiting vulnerabilities	Implementing encryption, access controls, data classification, regular security testing and vulnerability assessments
Denial of service	Availability of resources	Distributed denial of service attacks, flooding, resource exhaustion	Implementing network and application-level controls (e.g., firewalls, load balancers, rate limiting), redundancy and failover mechanisms
Elevation of privilege	Access control mechanisms	Exploiting vulnerabilities, privilege escalation attacks	Implementing least privilege principle, access control, monitoring and logging of user actions, regular security testing and vulnerability assessments

This table summarizes the results of the threat assessment conducted using the STRIDE model. The table includes a description of each identified threat, the target of the threat, the attack techniques that could be used, and the controls or countermeasures that can

be implemented to mitigate the risk of the threat. The table is intended to help prioritize and plan for risk mitigation strategies based on the severity and likelihood of each threat.

Task 7

Use the DREAD model to rate each threat. Each element of DREAD can have a threat rating of 1, 2 or 3 (1=Low, 2=Medium, 3=High).


Threat	Description	D	R	E	A	D	Total Rating
Spoofing attack	Attackers could impersonate legitimate users to gain unauthorized access to the system.	2	2	2	2	2	10
Tampering attack	Attackers could modify data in transit or at rest, potentially leading to loss of data integrity.	2	1	2	3	2	10
Repudiation attack	Attackers could deny having performed certain actions, making it difficult to track down and address security incidents.	1	2	1	2	3	9

Threat	Description	D	R	E	A	D	Total Rating
Information disclosure	Attackers could steal sensitive data from the system, leading to loss of confidentiality.	2	2	2	3	2	11
Denial of service	Attackers could overwhelm the system with traffic or requests, making it unusable for legitimate users.	3	2	2	2	1	10
Elevation of privilege	Attackers could gain higher levels of access than they are authorized for, potentially leading to further compromise of the system.	2	2	1	2	2	9

Note: The **DREAD** model rates each threat on a scale of **1-3** for each of the five elements: Damage, Reproducibility, Exploitability, Affected Users, and Discoverability. The total rating is the sum of the individual ratings, and a rating of 1 is considered low, 2 is medium, and 3 is high. In this example table, the threats with a total rating **between 5-7 are considered low**, those with a total rating **between 7-10 are medium**, and those with a total rating over **10 are high**.

TASK 8

Threat Description	Threat Target	Attack Techniques	Controls/Countermeasures	DREAD Rating
Spoofing attack	Authentication mechanism	Phishing, social engineering, credential stuffing	Two-factor authentication, account lockout policy, strong password requirements	High
Tampering attack	Data in transit or at rest	Man-in-the-middle attacks, SQL injection, file manipulation	Encryption, digital signatures, input validation, file integrity monitoring	High
Repudiation attack	Logging and auditing systems	Forgery, deletion of logs, replay attacks	Digital signatures, secure storage of logs, timestamping	Medium
Information disclosure	Confidential data	SQL injection, cross-site scripting, server misconfiguration	Access control, encryption, input validation, security patches	High



Threat Description	Threat Target	Attack Techniques	Controls/Countermeasures	DREAD Rating
Denial of service	Network and server infrastructure	Distributed denial-of-service attacks, resource exhaustion, flooding	Load balancing, rate limiting, network segmentation, redundant infrastructure	High
Elevation of privilege	User accounts and system components	Exploiting vulnerabilities, backdoors, privilege escalation	Least privilege access control, vulnerability management, regular security testing	Medium

Note: The **DREAD rating** from Task 7 has been included in this table to provide an overall rating of the severity and likelihood of each threat. This can help prioritize which controls and countermeasures should be implemented to **mitigate the risks associated with each threat**.

As per the given problem statement, BigMart has been losing market share to online competitors who are providing a better customer experience than BigMart's brick and mortar establishments. This indicates that BigMart may have faced the **following major troubles:**

Lack of an effective digital strategy - BigMart may have struggled to compete with online retailers due to a lack of a well-defined digital strategy that meets customer needs.

Inadequate user experience - Online retailers have been providing a better customer experience, which suggests that BigMart's digital platforms may not be optimized for customer convenience and ease of use.

Cybersecurity threats - As BigMart is planning to adopt a digital strategy, it may become vulnerable to various cybersecurity threats such as data breaches, malware attacks, phishing, and other types of cyber-attacks

To secure the vulnerabilities, BigMart can implement the following measures:


Develop a robust digital strategy that meets customer needs and improves user experience.

Optimize the user experience of the digital platforms by making them more intuitive and user-friendly.

Implement strong access controls and encryption mechanisms to protect sensitive customer data.

Implement regular security assessments and testing to identify and mitigate any cybersecurity threats.

Train employees on cybersecurity awareness and best practices to prevent human errors and negligence that may lead to security breaches.



By implementing these measures, BigMart can secure its digital platforms and provide a secure, uninterrupted, and enhanced user experience to its customers while maintaining its market position in the face of competition from online retailers.