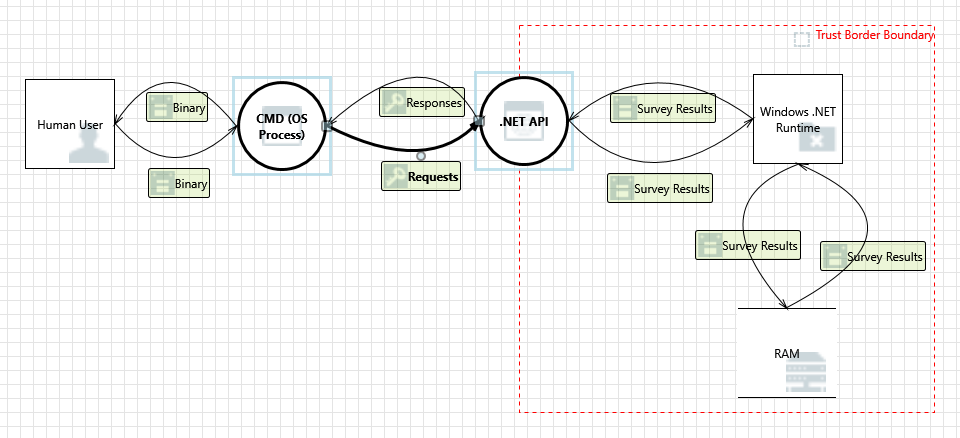
# Threat Modeling Report

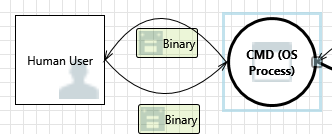
### Threat Model Summary:

|  |  |
| --- | --- |
| Not Started | 0 |
| Not Applicable | 2 |
| Needs Investigation | 0 |
| Mitigation Implemented | 13 |
| Total | 15 |
| Total Migrated | 0 |

## Diagram: Diagram 1



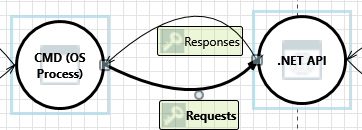
### Interaction: Binary



#### 1. Elevation Using Impersonation  [State: Not Applicable]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | CMD (OS Process) may be able to impersonate the context of Human User in order to gain additional privilege. |
| **Justification:** | La sécurité de la console du client ne compromet pas le côté du serveur, où sont stocké les données. Aucune donnée importante n’est contenue du côté client. On ne compromet pas le client, bien que l’obfuscation de l’application cliente rend la vie plus dur aux attaquants. |

### Interaction: Requests



#### 2. Elevation Using Impersonation  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | .NET API may be able to impersonate the context of CMD (OS Process) in order to gain additional privilege. |
| **Justification:** | Un système authentification par clé d’API et par mot de passe est en place. Ainsi, si l’API .NET essaie d’imiter la console du client, elle doit tout de même avoir possession de la clé d’API et d’avoir le userID afin de changer les réponses du client associé à cet userID. |

#### 3. JavaScript Object Notation Processing  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | If a dataflow contains JSON, JSON processing and hijacking threats may be exploited. |
| **Justification:** | Les objets JSONs sont vérifiés du côté serveur ainsi que tous les attributs du JSONs sont validé afin qu’ils aient un sens à la réponse attendue. |

#### 4. Replay Attacks  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity. |
| **Justification:** | Cette faille est gérée avec TLS1.2 |

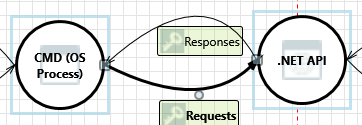
#### 5. Collision Attacks  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases. |
| **Justification:** | Utilisation de TLS1.2 |

#### 6. Weak Authentication Scheme  [State: Mitigation Implemented (Need better password encryption)]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme. |
| **Justification:** | Nous avons implémenté un système de clé API, ainsi que d’authentification par nom d’utilisateur - mot de passe. Nous acceptions seulement TLS1.2 et l’authentification par dégradation n’est pas possible. Cependant, dans le cas présent le mot de passe est hasher en Base64 dans le système de stockage. Il est évident que ce dernier devra être encrypter avec un algorithme beaucoup plus sécuritaire dans le futur (SHA-512). Cependant, puisque la communication est HTTPS, un attaquant ne verra pas le mot de passe en clair dans les paquets. |

### Interaction: Responses



#### 7. Collision Attacks  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases. |
| **Justification:** | Utilisation du protocole TLS1.2 |

#### 8. Replay Attacks  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity. |
| **Justification:** | Utilisation du protocole TLS1.2 |

#### 9. JavaScript Object Notation Processing  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | If a dataflow contains JSON, JSON processing and hijacking threats may be exploited. |
| **Justification:** | Les objets JSONs sont traités par le serveur avant d’être envoyés et les informations sont limités. |

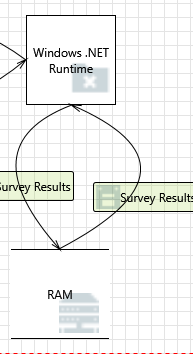
#### 10. Elevation Using Impersonation  [State: Not Applicable]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | CMD (OS Process) may be able to impersonate the context of .NET API in order to gain additional privilege. |
| **Justification:** | La sécurité de la console du client n’impacte pas directement le serveur, où sont stocké les données. On ne compromet pas le client, bien que l’obfuscation de l’application cliente rend la vie plus dur aux attaquants. |

#### 11. Weak Authentication Scheme  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme. |
| **Justification:** | Nous avons implémenté un système de clé d’API ainsi que de mot de passe. Nous devons sécuriser le stockage de ses données sensibles. |

### Interaction: Survey Results



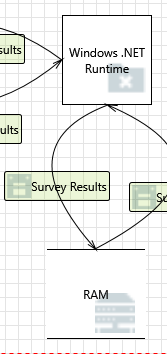
#### 12. Weak Access Control for a Resource  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Improper data protection of RAM can allow an attacker to read information not intended for disclosure. Review authorization settings. |
| **Justification:** | Cette partie se trouve dans notre barrière de confiance, mais en effet, si notre serveur est compromis, les données de la RAM le seront aussi. L’implémentation d’une base de donnée communiquant uniquement avec le serveur de façon sécurisé ajouterait une barrière de sécurité et un étape additionnel pour les attaquants. Cependant, sous Windows pour accéder à la RAM il faut un accès au niveau du Kernel, donc si simplement un service est compromis, les données de la RAM ne sont pas forcément compromises. |

#### 13. Spoofing of Source Data Store RAM  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | RAM may be spoofed by an attacker and this may lead to incorrect data delivered to Windows .NET Runtime. Consider using a standard authentication mechanism to identify the source data store. |
| **Justification:** | Cette partie se trouve dans notre zone de confiance et il est dur d’imaginer quelqu’un qui serait en mesure de spoofer la RAM. Si elle a accès au serveur avec des privilèges élevés, les données seront compromises. |

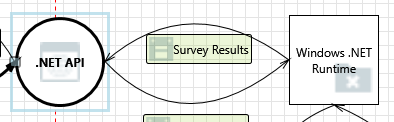
### Interaction: Survey Results



#### 14. Spoofing of Destination Data Store RAM  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | RAM may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of RAM. Consider using a standard authentication mechanism to identify the destination data store. |
| **Justification:** | Cette partie se trouve dans notre zone de confiance. |

### Interaction: Survey Results



#### 15. Elevation Using Impersonation  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | .NET API may be able to impersonate the context of Windows .NET Runtime in order to gain additional privilege. |
| **Justification:** | Cette partie ce trouve dans notre zone de confiance. |