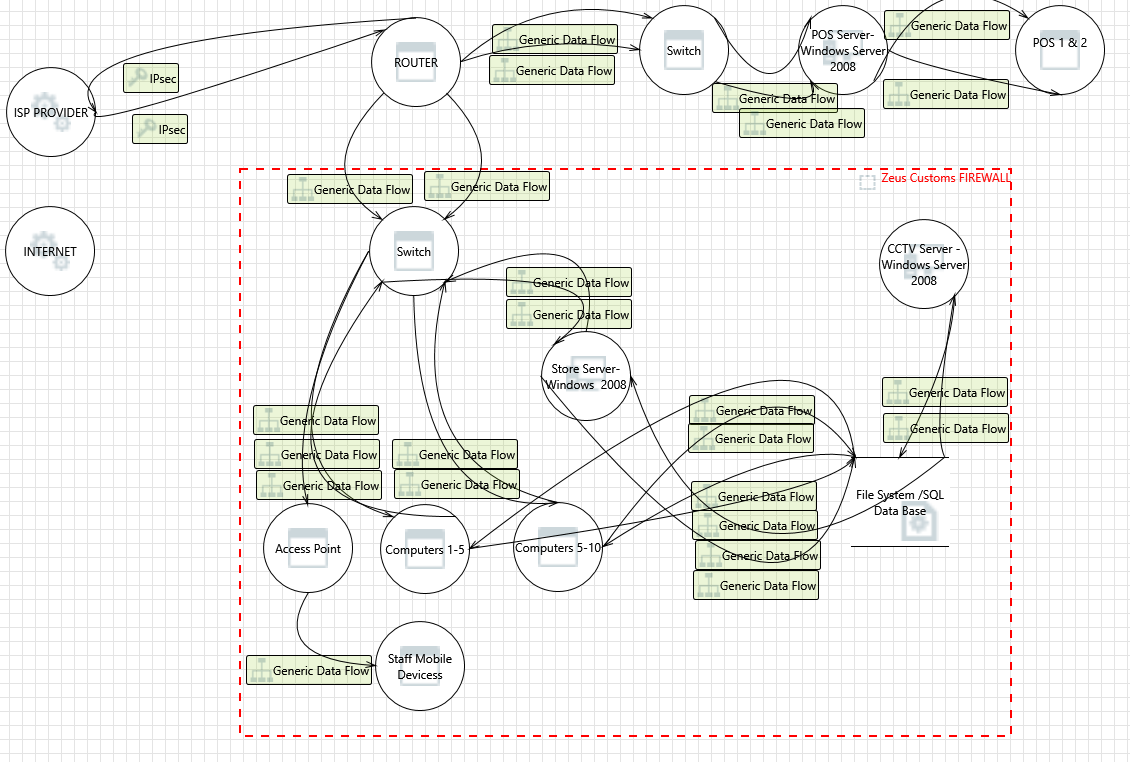
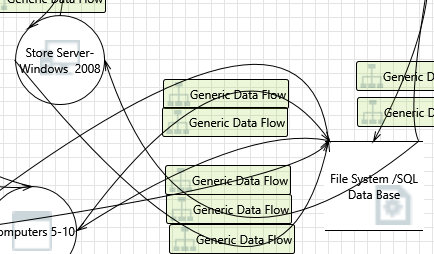
## Diagram: Diagram 1

****

### Diagram 1 Diagram Summary:

|  |  |
| --- | --- |
| Not Started | 89 |
| Not Applicable | 0 |
| Needs Investigation | 0 |
| Mitigation Implemented | 0 |
| Total | 89 |
| Total Migrated | 0 |

### Interaction: Generic Data Flow

****

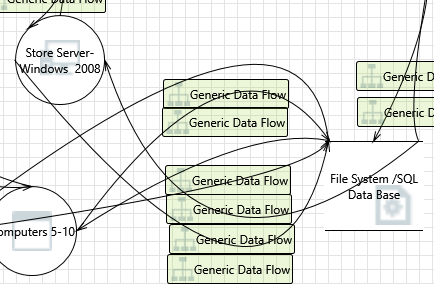
#### 1. Spoofing of Source Data Store File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | File System /SQL Data Base may be spoofed by an attacker and this may lead to incorrect data delivered to Store Server- Windows 2008. Consider using a standard authentication mechanism to identify the source data store. |
| **Justification:** | <no mitigation provided> |

#### 2. Weak Access Control for a Resource  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Improper data protection of File System /SQL Data Base can allow an attacker to read information not intended for disclosure. Review authorization settings. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 3. Spoofing of Destination Data Store File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | File System /SQL Data Base may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System /SQL Data Base. Consider using a standard authentication mechanism to identify the destination data store. |
| **Justification:** | <no mitigation provided> |

#### 4. Authorization Bypass  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Can you access File System /SQL Data Base and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface. |
| **Justification:** | <no mitigation provided> |

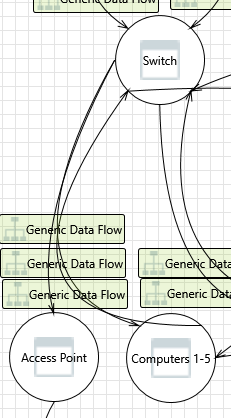
#### 5. Weak Credential Storage  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored |
| **Justification:** | <no mitigation provided> |

#### 6. Potential Excessive Resource Consumption for Store Server- Windows 2008 or File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | Does Store Server- Windows 2008 or File System /SQL Data Base take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 7. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 8. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

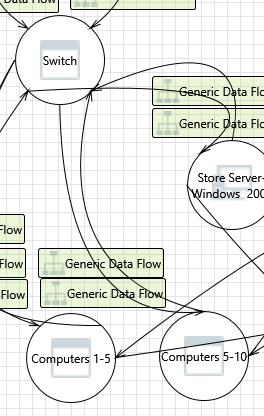
#### 9. Weak Authentication Scheme  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **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:** | <no mitigation provided> |

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

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Switch may be able to impersonate the context of Computers 1-5 in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

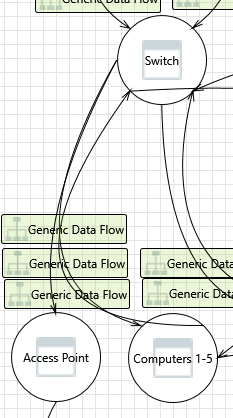
### Interaction: Generic Data Flow

****

#### 11. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Computers 5-10 may be able to impersonate the context of Switch in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

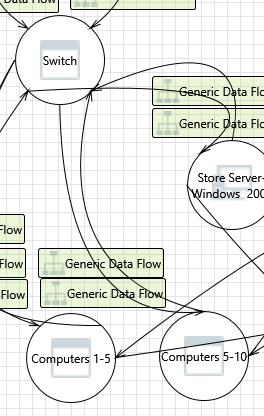
### Interaction: Generic Data Flow

****

#### 12. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Computers 1-5 may be able to impersonate the context of Switch in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 13. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 14. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

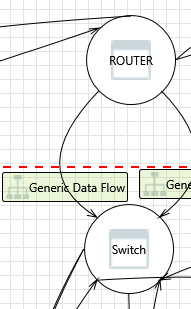
#### 15. Weak Authentication Scheme  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **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:** | <no mitigation provided> |

#### 16. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Switch may be able to impersonate the context of Computers 5-10 in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 17. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 18. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 19. Potential Data Repudiation by Switch  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Repudiation |
| **Description:** | Switch claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Justification:** | <no mitigation provided> |

#### 20. Weak Authentication Scheme  [State: Not Started]  [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:** | <no mitigation provided> |

#### 21. Potential Process Crash or Stop for Switch  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | Switch crashes, halts, stops or runs slowly; in all cases violating an availability metric. |
| **Justification:** | <no mitigation provided> |

#### 22. Data Flow Generic Data Flow Is Potentially Interrupted  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Justification:** | <no mitigation provided> |

#### 23. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Switch may be able to impersonate the context of ROUTER in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

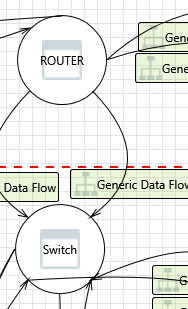
#### 24. Switch May be Subject to Elevation of Privilege Using Remote Code Execution  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | ROUTER may be able to remotely execute code for Switch. |
| **Justification:** | <no mitigation provided> |

#### 25. Elevation by Changing the Execution Flow in Switch  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | An attacker may pass data into Switch in order to change the flow of program execution within Switch to the attacker's choosing. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 26. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 27. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 28. Potential Data Repudiation by Switch  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Repudiation |
| **Description:** | Switch claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Justification:** | <no mitigation provided> |

#### 29. Weak Authentication Scheme  [State: Not Started]  [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:** | <no mitigation provided> |

#### 30. Potential Process Crash or Stop for Switch  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | Switch crashes, halts, stops or runs slowly; in all cases violating an availability metric. |
| **Justification:** | <no mitigation provided> |

#### 31. Data Flow Generic Data Flow Is Potentially Interrupted  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Justification:** | <no mitigation provided> |

#### 32. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Switch may be able to impersonate the context of ROUTER in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

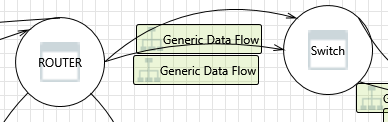
#### 33. Switch May be Subject to Elevation of Privilege Using Remote Code Execution  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | ROUTER may be able to remotely execute code for Switch. |
| **Justification:** | <no mitigation provided> |

#### 34. Elevation by Changing the Execution Flow in Switch  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | An attacker may pass data into Switch in order to change the flow of program execution within Switch to the attacker's choosing. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 35. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 36. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

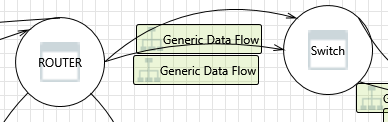
#### 37. Weak Authentication Scheme  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **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:** | <no mitigation provided> |

#### 38. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Switch may be able to impersonate the context of ROUTER in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 39. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 40. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

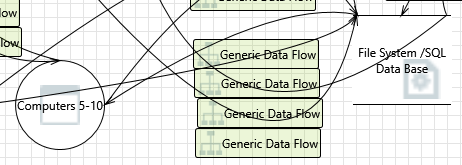
#### 41. Weak Authentication Scheme  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **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:** | <no mitigation provided> |

#### 42. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Switch may be able to impersonate the context of ROUTER in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

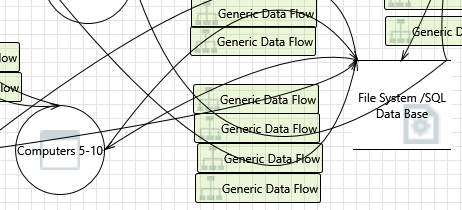
#### 43. Spoofing of Source Data Store File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | File System /SQL Data Base may be spoofed by an attacker and this may lead to incorrect data delivered to Computers 5-10. Consider using a standard authentication mechanism to identify the source data store. |
| **Justification:** | <no mitigation provided> |

#### 44. Weak Access Control for a Resource  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Improper data protection of File System /SQL Data Base can allow an attacker to read information not intended for disclosure. Review authorization settings. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 45. Spoofing of Destination Data Store File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | File System /SQL Data Base may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System /SQL Data Base. Consider using a standard authentication mechanism to identify the destination data store. |
| **Justification:** | <no mitigation provided> |

#### 46. Authorization Bypass  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Can you access File System /SQL Data Base and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface. |
| **Justification:** | <no mitigation provided> |

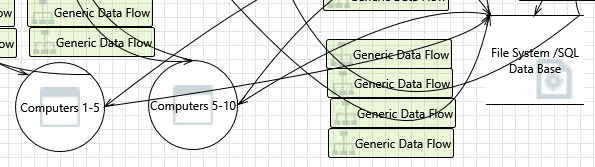
#### 47. Weak Credential Storage  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored |
| **Justification:** | <no mitigation provided> |

#### 48. Potential Excessive Resource Consumption for Computers 5-10 or File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | Does Computers 5-10 or File System /SQL Data Base take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 49. Spoofing of Destination Data Store File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | File System /SQL Data Base may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System /SQL Data Base. Consider using a standard authentication mechanism to identify the destination data store. |
| **Justification:** | <no mitigation provided> |

#### 50. Authorization Bypass  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Can you access File System /SQL Data Base and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface. |
| **Justification:** | <no mitigation provided> |

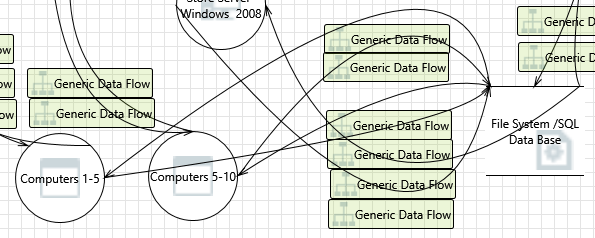
#### 51. Weak Credential Storage  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored |
| **Justification:** | <no mitigation provided> |

#### 52. Potential Excessive Resource Consumption for Computers 1-5 or File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | Does Computers 1-5 or File System /SQL Data Base take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

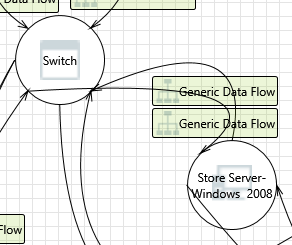
#### 53. Spoofing of Source Data Store File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | File System /SQL Data Base may be spoofed by an attacker and this may lead to incorrect data delivered to Computers 1-5. Consider using a standard authentication mechanism to identify the source data store. |
| **Justification:** | <no mitigation provided> |

#### 54. Weak Access Control for a Resource  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Improper data protection of File System /SQL Data Base can allow an attacker to read information not intended for disclosure. Review authorization settings. |
| **Justification:** | <no mitigation provided> |

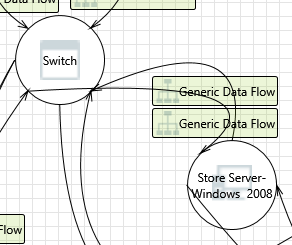
### Interaction: Generic Data Flow

****

#### 55. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Store Server- Windows 2008 may be able to impersonate the context of Switch in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 56. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 57. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

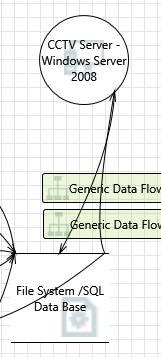
#### 58. Weak Authentication Scheme  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **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:** | <no mitigation provided> |

#### 59. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Switch may be able to impersonate the context of Store Server- Windows 2008 in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

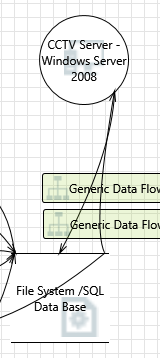
#### 60. Spoofing of Source Data Store File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | File System /SQL Data Base may be spoofed by an attacker and this may lead to incorrect data delivered to CCTV Server - Windows Server 2008. Consider using a standard authentication mechanism to identify the source data store. |
| **Justification:** | <no mitigation provided> |

#### 61. Weak Access Control for a Resource  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Improper data protection of File System /SQL Data Base can allow an attacker to read information not intended for disclosure. Review authorization settings. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 62. Spoofing of Destination Data Store File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | File System /SQL Data Base may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System /SQL Data Base. Consider using a standard authentication mechanism to identify the destination data store. |
| **Justification:** | <no mitigation provided> |

#### 63. Authorization Bypass  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Can you access File System /SQL Data Base and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface. |
| **Justification:** | <no mitigation provided> |

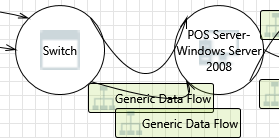
#### 64. Weak Credential Storage  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored |
| **Justification:** | <no mitigation provided> |

#### 65. Potential Excessive Resource Consumption for CCTV Server - Windows Server 2008 or File System /SQL Data Base  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | Does CCTV Server - Windows Server 2008 or File System /SQL Data Base take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout. |
| **Justification:** | <no mitigation provided> |

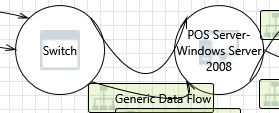
### Interaction: Generic Data Flow

****

#### 66. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | POS Server-Windows Server 2008 may be able to impersonate the context of Switch in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

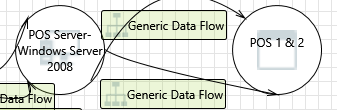
### Interaction: Generic Data Flow

****

#### 67. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | POS Server-Windows Server 2008 may be able to impersonate the context of Switch in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 68. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 69. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

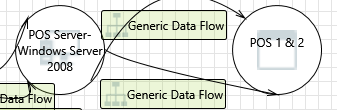
#### 70. Weak Authentication Scheme  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **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:** | <no mitigation provided> |

#### 71. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | POS 1 & 2 may be able to impersonate the context of POS Server-Windows Server 2008 in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 72. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 73. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

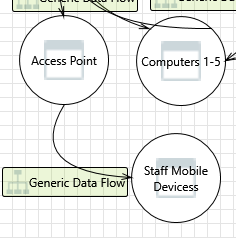
#### 74. Weak Authentication Scheme  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **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:** | <no mitigation provided> |

#### 75. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | POS 1 & 2 may be able to impersonate the context of POS Server-Windows Server 2008 in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: Generic Data Flow

****

#### 76. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Staff Mobile Devices may be able to impersonate the context of Access Point in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

#### 77. Weak Authentication Scheme  [State: Not Started]  [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:** | <no mitigation provided> |

#### 78. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

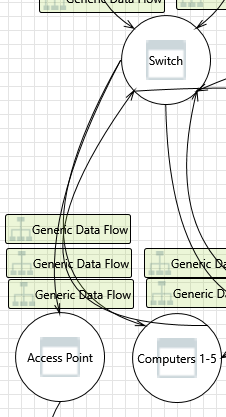
#### 79. Replay Attacks  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **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:** | <no mitigation provided> |

#### 80. Authenticated Data Flow Compromised  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | An attacker can read or modify data transmitted over an authenticated dataflow. |
| **Justification:** | <no mitigation provided> |

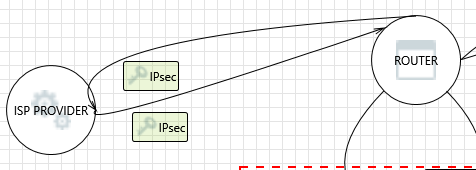
### Interaction: Generic Data Flow

****

#### 81. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Access Point may be able to impersonate the context of Switch in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: IPsec

****

#### 82. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 83. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

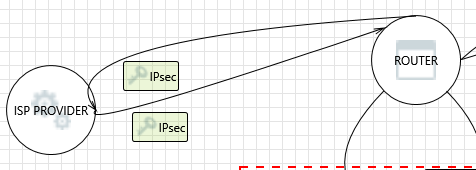
#### 84. Weak Authentication Scheme  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **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:** | <no mitigation provided> |

#### 85. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | ISP PROVIDER may be able to impersonate the context of ROUTER in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |

### Interaction: IPsec

****

#### 86. Replay Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 87. Collision Attacks  [State: Not Started]  [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:** | <no mitigation provided> |

#### 88. Weak Authentication Scheme  [State: Not Started]  [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:** | <no mitigation provided> |

#### 89. Elevation Using Impersonation  [State: Not Started]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | ROUTER may be able to impersonate the context of ISP PROVIDER in order to gain additional privilege. |
| **Justification:** | <no mitigation provided> |