### S - Spoofing

\*\*Threat Agents:\*\*

1. External attacker

2. Internal attacker

3. Third-party vendors

4. Rogue administrators

5. Malware or compromised systems

6. Insider threat (disgruntled employees)

7. Network eavesdroppers

8. Policy violations

9. Credential theft

10. Phishing attacks

\*\*Threat Descriptions:\*\*

1. External attackers may attempt to spoof their identity to gain unauthorized access to the SFTP server.

- Likelihood: Moderate

- Impact: High

2. Internal attackers could also impersonate legitimate users to access sensitive data.

- Likelihood: Moderate

- Impact: High

3. Third-party vendors might attempt to impersonate trusted sources to inject malicious files into the system.

- Likelihood: Low

- Impact: Moderate

4. Rogue administrators could misuse their privileges to impersonate others.

- Likelihood: Low

- Impact: Moderate

5. Malware or compromised systems could spoof legitimate connections.

- Likelihood: Moderate

- Impact: Moderate

6. Insider threats might exploit their knowledge to spoof identities.

- Likelihood: Moderate

- Impact: High

7. Network eavesdroppers could attempt to intercept and manipulate traffic.

- Likelihood: Moderate

- Impact: Moderate

8. Policy violations could lead to unauthorized access.

- Likelihood: Low

- Impact: Low

9. Credential theft can result in unauthorized access.

- Likelihood: Moderate

- Impact: High

10. Phishing attacks may trick users into disclosing credentials.

- Likelihood: Moderate

- Impact: Moderate

### T - Tampering

\*\*Threat Agents:\*\*

1. External attacker

2. Internal attacker

3. Third-party vendors

4. Malware or compromised systems

5. Data interception and modification

6. Network manipulation

7. Unauthorized system changes

8. Malicious software updates

9. Misconfiguration

10. Lack of data integrity checks

\*\*Threat Descriptions:\*\*

1. External attackers may attempt to alter data during transmission or storage.

- Likelihood: Moderate

- Impact: High

2. Internal attackers could tamper with data to disrupt operations or steal sensitive information.

- Likelihood: Moderate

- Impact: High

3. Third-party vendors might send malicious files or tampered data.

- Likelihood: Low

- Impact: Moderate

4. Malware or compromised systems could introduce unauthorized changes.

- Likelihood: Moderate

- Impact: High

5. Data interception and modification during transit.

- Likelihood: Moderate

- Impact: Moderate

6. Network manipulation to tamper with data in transit.

- Likelihood: Moderate

- Impact: Moderate

7. Unauthorized system changes by administrators.

- Likelihood: Low

- Impact: Moderate

8. Malicious software updates compromising data integrity.

- Likelihood: Low

- Impact: High

9. Misconfigurations leading to vulnerabilities.

- Likelihood: Moderate

- Impact: High

10. Lack of data integrity checks allowing undetected tampering.

- Likelihood: Moderate

- Impact: High

### R - Repudiation

\*\*Threat Agents:\*\*

1. External attacker

2. Internal attacker

3. Third-party vendors

4. Rogue administrators

5. Malware or compromised systems

6. Insider threats

7. Legal disputes

8. Lack of audit logs

9. Inadequate log protection

10. Incomplete or inconsistent logging

\*\*Threat Descriptions:\*\*

1. External attackers may gain access to the server and deny their actions.

- Likelihood: Moderate

- Impact: Moderate

2. Internal attackers could manipulate logs or erase evidence of their actions.

- Likelihood: Moderate

- Impact: Moderate

3. Third-party vendors might claim that they never sent certain files.

- Likelihood: Low

- Impact: Moderate

4. Rogue administrators may deny their unauthorized activities.

- Likelihood: Low

- Impact: Moderate

5. Malware or compromised systems might alter logs.

- Likelihood: Moderate

- Impact: Moderate

6. Insider threats could exploit their knowledge to deny actions.

- Likelihood: Moderate

- Impact: Moderate

7. Legal disputes may require non-repudiation evidence.

- Likelihood: Low

- Impact: Moderate

8. Lack of audit logs may hinder investigation.

- Likelihood: Moderate

- Impact: High

9. Inadequate log protection may allow tampering.

- Likelihood: Moderate

- Impact: High

10. Incomplete or inconsistent logging may lead to disputes.

- Likelihood: Moderate

- Impact: Moderate

### I - Information Disclosure

\*\*Threat Agents:\*\*

1. External attacker

2. Internal attacker

3. Third-party vendors

4. Misconfiguration

5. Unauthorized software

6. Social engineering

7. Insider threats

8. Data leaks

9. Unencrypted backups

10. Unsanctioned devices

\*\*Threat Descriptions:\*\*

1. External attackers may attempt to intercept and access sensitive data during transmission.

- Likelihood: High

- Impact: High

2. Internal attackers could exploit vulnerabilities to access confidential information.

- Likelihood: Moderate

- Impact: High

3. Third-party vendors might send sensitive files that get exposed.

- Likelihood: Low

- Impact: Moderate

4. Misconfiguration may inadvertently expose sensitive data.

- Likelihood: Moderate

- Impact: High

5. Unauthorized software could lead to data leaks.

- Likelihood: Moderate

- Impact: Moderate

6. Social engineering attacks may trick employees into disclosing sensitive information.

- Likelihood: Moderate

- Impact: Moderate

7. Insider threats might intentionally leak sensitive data.

- Likelihood: Moderate

- Impact: High

8. Data leaks through insecure backups.

- Likelihood: Moderate

- Impact: High

9. Unsanctioned devices accessing sensitive data.

- Likelihood: Moderate

- Impact: Moderate

10. Unencrypted backups being accessed by unauthorized individuals.

- Likelihood: Moderate

- Impact: High

### D - Denial of Service

\*\*Threat Agents:\*\*

1. External attacker

2. Internal attacker

3. Third-party vendors

4. Malware or botnets

5. Natural disasters

6. Network failures

7. Power outages

8. Hardware failures

9. Software bugs

10. Resource exhaustion

\*\*Threat Descriptions:\*\*

1. External attackers may launch DDoS attacks to disrupt SFTP services.

- Likelihood: High

- Impact: High

2. Internal attackers could flood the server with requests to exhaust resources.

- Likelihood: Moderate

- Impact: High

3. Third-party vendors might unintentionally overload the server with large file transfers.

- Likelihood: Low

- Impact: Moderate

4. Malware or botnets may be used to launch coordinated DDoS attacks.

- Likelihood: Moderate

- Impact: High

5. Natural disasters, such as floods or earthquakes, could disrupt server operations.

- Likelihood: Low

- Impact: High

6. Network failures may result in service interruptions.

- Likelihood: Moderate

- Impact: High

7. Power outages may render the server inaccessible.

- Likelihood: Moderate

- Impact: High

8. Hardware failures could lead to service downtime.

- Likelihood: Moderate

- Impact: High

9. Software bugs or vulnerabilities may be exploited for DoS.

- Likelihood: Moderate

- Impact: High

10. Resource exhaustion due to inefficient resource management.

- Likelihood: Moderate

- Impact: High

### E - Elevation of Privilege

\*\*Threat Agents:\*\*

1. Internal attacker

2. Misconfiguration

3. Exploitable software vulnerabilities

4. Insufficient access controls

5. Rogue administrators

6. Social engineering

7. Unauthorized privilege escalation

8. Inadequate password policies

9. Insider threats

10. Weak encryption practices

\*\*Threat Descriptions:\*\*

1. Internal attackers may attempt to escalate their privileges to gain unauthorized access.

- Likelihood: Moderate

- Impact: High

2. Misconfigurations in the server or access controls could lead to unintended privilege escalation.

- Likelihood: Moderate

- Impact: High

3. Exploitable software vulnerabilities may be used to gain higher privileges.

- Likelihood: Moderate

- Impact: High

4. Insufficient access controls could allow unauthorized users to elevate their privileges.

- Likelihood: Moderate

- Impact: High

5. Rogue administrators might misuse their privileges.

- Likelihood: Moderate

- Impact: High

6. Social engineering attacks could trick users into granting elevated privileges.

- Likelihood: Moderate

- Impact: High

7. Unauthorized privilege escalation attempts.

- Likelihood: Moderate

- Impact: High

8. Inadequate password policies may lead to password-based privilege escalation.

- Likelihood: Moderate

- Impact: High

9. Insider threats intentionally elevating their privileges.

- Likelihood: Moderate

- Impact: High

10. Weak encryption practices leading to unauthorized data access.

- Likelihood: Moderate

- Impact: High

Certainly, I can add existing controls and recommended controls to each threat type (the 6 STRIDE letters). Here's the information for each threat type:

### S - Spoofing

\*\*Existing Controls:\*\*

1. Strong authentication mechanisms for user access.

2. Access control lists to restrict access to authorized users.

3. Secure communication channels using SSH for SFTP.

4. Firewall rules to control traffic to and from the DMZ.

5. Intrusion detection and prevention systems.

6. Regular security training and awareness programs.

7. Periodic password changes and account lockouts.

8. Email filtering to detect and prevent phishing attempts.

9. Certificate-based authentication for third-party vendors.

10. Network segmentation to isolate sensitive systems.

\*\*Recommended Controls:\*\*

1. Implement multi-factor authentication for user access.

2. Regularly audit user accounts and privileges.

3. Use digital certificates for third-party vendor authentication.

4. Employ intrusion detection systems to identify potential spoofing attempts.

5. Conduct regular security training and awareness programs for employees.

6. Periodically review and update access control policies.

7. Implement strong anti-phishing measures.

### T - Tampering

\*\*Existing Controls:\*\*

1. Data integrity checks during transmission using cryptographic hash functions.

2. File integrity monitoring tools.

3. Regular backups to recover from tampering incidents.

4. Access controls to limit system changes.

5. Network monitoring and anomaly detection.

6. Strong change management processes.

7. Patch management to address vulnerabilities.

8. Regular system audits and configuration reviews.

\*\*Recommended Controls:\*\*

1. Implement digital signatures to ensure data integrity.

2. Use intrusion detection systems to detect unauthorized data modifications.

3. Employ strict access controls to limit the number of individuals who can modify files.

4. Educate third-party vendors on secure file transfer practices.

5. Regularly update and patch systems.

6. Implement robust change management processes.

7. Configure systems securely to prevent misconfigurations.

### R - Repudiation

\*\*Existing Controls:\*\*

1. Logging and audit trails.

2. Role-based access control with restricted admin access.

3. Regular log review and analysis.

4. Legal and compliance requirements.

5. Data backup and log storage.

6. Encryption of log data.

7. Time-stamping and digital signatures on logs.

\*\*Recommended Controls:\*\*

1. Implement secure logging practices to ensure logs cannot be tampered with.

2. Use digital signatures for log entries.

3. Maintain off-site backups of logs.

4. Implement strong user authentication to prevent unauthorized access.

5. Ensure compliance with legal and regulatory requirements.

6. Regularly review and update log retention policies.

7. Train employees on the importance of accurate logs.

### I - Information Disclosure

\*\*Existing Controls:\*\*

1. Encryption for data in transit and at rest.

2. Access controls to limit access to authorized personnel.

3. Periodic vulnerability scanning and patch management.

4. Data classification and labeling.

5. Data loss prevention (DLP) solutions.

6. Security awareness training.

7. Endpoint protection and intrusion detection systems.

8. Secure data disposal practices.

9. Mobile device management (MDM) for sanctioned devices.

10. Backup encryption and access controls.

\*\*Recommended Controls:\*\*

1. Encrypt data at rest in addition to data in transit.

2. Conduct regular security assessments and penetration testing.

3. Train employees and third-party vendors on secure data handling.

4. Implement data loss prevention (DLP) solutions to monitor and prevent data leaks.

5. Develop and enforce policies for data classification and labeling.

6. Implement strong endpoint protection measures.

7. Ensure secure data disposal practices are in place.

8. Enforce mobile device management (MDM) policies.

9. Encrypt backups and restrict access.

10. Implement strict access controls for sensitive data.

I will provide the existing and recommended controls for the remaining threat types in the next response.

Certainly, here are the existing and recommended controls for the remaining threat types:

### D - Denial of Service

\*\*Existing Controls:\*\*

1. Network and application-level DDoS protection.

2. Resource monitoring and scaling.

3. Redundancy and failover mechanisms.

4. Uninterruptible power supplies (UPS).

5. Regular software updates and patch management.

6. Disaster recovery and business continuity planning.

7. Intrusion detection and prevention systems.

8. Load balancing for traffic distribution.

9. Capacity planning and resource optimization.

10. Network segmentation for isolation.

\*\*Recommended Controls:\*\*

1. Implement rate limiting and access controls to mitigate excessive requests.

2. Use load balancing to distribute traffic and reduce the impact of DoS attacks.

3. Deploy redundancy and failover mechanisms for high availability.

4. Maintain UPS and backup power sources.

5. Continuously update and patch software to address vulnerabilities.

6. Develop and test disaster recovery and business continuity plans.

7. Monitor network traffic for anomalies and use intrusion prevention systems.

8. Regularly review and optimize resource allocation.

9. Implement network segmentation to isolate critical systems from potential attacks.

### E - Elevation of Privilege

\*\*Existing Controls:\*\*

1. Least privilege principle for user accounts.

2. Regular security assessments and audits.

3. Security awareness training for employees.

4. Strong access controls and segregation of duties.

5. Vulnerability scanning and patch management.

6. Intrusion detection and prevention systems.

7. Password complexity and expiration policies.

8. Logging and monitoring of privilege changes.

9. Encryption for sensitive data.

10. Role-based access control.

\*\*Recommended Controls:\*\*

1. Continuously monitor for privilege escalation attempts.

2. Implement strict access control and auditing policies.

3. Regularly review and update server configurations.

4. Employ intrusion detection systems to detect unusual behavior.

5. Enhance user awareness and training on privilege escalation risks.

6. Promptly patch and update software to address vulnerabilities.

7. Enforce strong password policies and account lockouts.

8. Implement encryption best practices for data protection.

9. Regularly review and adjust role-based access control.

10. Conduct regular security assessments to identify and remediate privilege escalation vulnerabilities.

These controls help mitigate the risks associated with each STRIDE threat type. Remember to tailor these controls to your specific environment and regularly assess and update them to address emerging threats and vulnerabilities.