To identify the main threats each protocol faces using the STRIDE model, we’ll assess **TLS**, **IPsec**, and **DNSSEC** against each STRIDE category to pinpoint vulnerabilities exacerbated by quantum computing capabilities.

### 1. TLS (Transport Layer Security)

TLS secures data communication but is susceptible to various quantum-based threats due to its reliance on public-key cryptography.

* **Spoofing**: An attacker could use quantum capabilities to break TLS certificates and impersonate a trusted server, tricking users into communicating with a malicious entity.
* **Tampering**: Quantum attacks on encryption keys (e.g., RSA) could allow attackers to alter data in transit without detection, compromising integrity.
* **Repudiation**: Weaknesses in digital signatures due to quantum threats mean that entities could potentially deny transactions or message exchanges if keys are compromised.
* **Information Disclosure**: By breaking TLS encryption with quantum algorithms, attackers could intercept and decrypt sensitive data, such as personal and financial information.
* **Denial of Service (DoS)**: Quantum-resistant encryption algorithms could lead to higher computational overhead, which increases susceptibility to DoS attacks due to increased processing requirements.
* **Elevation of Privilege**: By exploiting compromised credentials, attackers could escalate their access, obtaining unauthorized control over secure TLS channels.

### 2. IPsec (Internet Protocol Security)

IPsec ensures IP-level secure communications, but the use of vulnerable encryption and authentication mechanisms poses risks with the advent of quantum computing.

* **Spoofing**: Quantum-based attacks could break authentication protocols, allowing attackers to impersonate legitimate IP addresses or network entities.
* **Tampering**: By undermining encryption, attackers could modify data packets, corrupting or redirecting IP traffic undetected.
* **Repudiation**: Quantum threats to digital signature algorithms weaken IPsec’s ability to verify source authenticity, making it easier for users to deny involvement in communications.
* **Information Disclosure**: Decryption of IPsec-protected traffic due to quantum attacks could expose sensitive data, compromising user privacy and confidentiality.
* **Denial of Service (DoS)**: Resource-intensive quantum-safe algorithms could be exploited to overload IPsec-enabled devices, making them more susceptible to DoS attacks.
* **Elevation of Privilege**: By breaking authentication mechanisms, attackers could gain unauthorized access to restricted network zones or data.

### 3. DNSSEC (Domain Name System Security Extensions)

DNSSEC secures DNS by verifying authenticity, yet it is at risk due to the quantum vulnerability of its cryptographic foundations.

* **Spoofing**: An attacker could break DNSSEC’s digital signatures and impersonate legitimate DNS responses, redirecting users to malicious sites.
* **Tampering**: Quantum attacks could enable alterations to DNS records, allowing attackers to redirect users to unintended or malicious destinations.
* **Repudiation**: If DNSSEC’s signatures are compromised, DNS administrators may struggle to validate legitimate records, leading to potential denial of responsibility.
* **Information Disclosure**: Although DNSSEC does not encrypt data, any data associated with DNS queries and responses could be exposed if other security mechanisms (e.g., TLS) are broken.
* **Denial of Service (DoS)**: Quantum-resistant DNSSEC may require more resources to process, making DNS servers vulnerable to DoS attacks.
* **Elevation of Privilege**: If an attacker compromises DNSSEC, they could escalate privileges by directing traffic to control unauthorized services or intercept data.

Using the STRIDE model, these protocols exhibit significant vulnerabilities under quantum computing threats, highlighting the need for post-quantum cryptography to maintain security and trust in networked environments.