In chaos engineering, "DNS spoofing" refers to the deliberate manipulation of Domain Name System (DNS) responses to redirect traffic to unintended or malicious destinations. This technique involves falsifying DNS responses to map domain names to incorrect or unauthorized IP addresses.

Here's how DNS spoofing works:

1. When a client application sends a DNS query to resolve a domain name (e.g., www.example.com), it typically sends the request to a DNS resolver.

2. The DNS resolver then forwards the query to DNS servers responsible for the domain.

3. The authoritative DNS servers respond with the correct IP address associated with the domain name.

4. The DNS resolver then returns the IP address to the client application, allowing it to connect to the desired server.

In DNS spoofing, an attacker or chaos engineer intercepts DNS queries and sends false DNS responses to the client. These falsified responses contain incorrect IP addresses, leading the client to connect to unintended or malicious servers.

In the context of chaos engineering, DNS spoofing can be used to simulate scenarios where DNS resolution is compromised. By redirecting traffic to unexpected destinations, engineers can assess how the system reacts to such disruptions and whether it can maintain functionality and security. They may evaluate whether the system's error handling mechanisms, DNS caching strategies, or security controls are effective in detecting and mitigating DNS spoofing attacks.

Overall, DNS spoofing experiments help identify vulnerabilities in the system's DNS infrastructure and validate the effectiveness of mitigation strategies. This allows engineers to strengthen the system's resilience to DNS-related threats and ensure reliable operation in real-world scenarios.

**ping <target-hostname>** command.

|  |  |  |
| --- | --- | --- |
| **Variables** | **Description** | **Notes** |
| TARGET\_CONTAINER | Name of container which is subjected to dns spoof | None |
| TOTAL\_CHAOS\_DURATION | The time duration for chaos insertion (seconds) | Default (60s) |
| SPOOF\_MAP | Map of the target hostnames eg. '{"abc.com":"spoofabc.com"}' where key is the hostname that needs to be spoofed and value is the hostname where it will be spoofed/redirected to. | If not provided, no hostnames/domains will be spoofed |
| PODS\_AFFECTED\_PERC | The Percentage of total pods to target | Defaults to 0 (corresponds to 1 replica), provide numeric value only |
| CONTAINER\_RUNTIME | container runtime interface for the cluster | Defaults to containerd, supported values: docker |
| SOCKET\_PATH | Path of the docker socket file | Defaults to /run/containerd/containerd.sock |
| LIB | The chaos lib used to inject the chaos | Default value: litmus, supported values: litmus |
| LIB\_IMAGE | Image used to run the netem command | Defaults to litmuschaos/go-runner:latest |
| RAMP\_TIME | Period to wait before and after injection of chaos in sec |  |
| SEQUENCE | It defines sequence of chaos execution for multiple target pods | Default value: parallel. Supported: serial, parallel |