**Problem statement   
Task: Malware Injection  
  
Description: Simulate malware running within a pod or node.  
Network type: PodChaos (malware simulation)  
  
  
Path to Shell script**  
cd /root/kalyani  
cat malware.sh  
  
**To apply the experiment**  
./malware.sh  
  
\* k9s  
\* Go to existing pod   
\* check cd /tmp   
\* ls   
We can see the malware.txt

Not able to create with yaml. Because it creating new pods every time.   
  
  
**Different ways to eradicate  
  
1.** Implement Pod Security Policies (PSPs) or Pod Security Admission (PSA)  
**Objective**: Restrict pod privileges to prevent unauthorized file modifications.  
  
**2.** Use Kubernetes Network Policies  
**Objective**: Block unauthorized network access to your PostgreSQL pod.

**3.** Restrict Volume Mounts and File Access

**Objective:** Ensure malware.txt cannot be written to disk.

**4.** Enable SELinux or AppArmor

**Objective:** Enforce security rules at the operating system level.  
  
**5.** Monitor File Integrity

**Objective:** Detect unauthorized file creation (malware.txt).

**6.** Use Admission Controllers (Kyverno or OPA Gatekeeper)

**Objective:** Block pods with insecure configurations.

**7.** Scan Containers for Vulnerabilities

**Objective:** Ensure images are secure.

**8.** Enforce Least Privilege Principle

**Objective:** Run containers as non-root users.