Drone Security Check Report

System Information

Username: xxx

Drone Manufacture: DJI

Drone IP: 192.168.1.6

Network Interface: wlan0

Open Ports: .!ctkframe9.!ctktextbox

Kernel Version: 5.4.0-88-generic

Security Issues

SSH Brute Force on Drone:

Founded Password:kali

Connection to SSH: ssh @192.168.1.6

SSH brute force is a method of attempting to gain unauthorized access to the drone's system by trying many passwords until the correct one is found.

Mitigation: Use strong, unique passwords, implement SSH key-based authentication, and use tools like fail2ban to block repeated failed login attempts.

Command Injection on Drone:

Command injection is an attack in which the goal is execution of arbitrary commands on the drone's operating system via a vulnerable application.

Mitigation: Validate and sanitize commands sent to the drone, implement strong authentication and authorization mechanisms, and regularly update the drone's

firmware to fix vulnerabilities.

Drone Instruction Injection:

Drone instruction injection is a type of attack where an attacker injects malicious instructions into the commands sent to the drone, potentially gaining unauthorized control.

Mitigation: Encrypt communications between the controller and the drone, implement secure authentication mechanisms, and regularly update drone firmware to patch known vulnerabilities.

ARP Spoof on Drone Network:

ARP spoofing is a technique whereby an attacker sends fake Address Resolution Protocol (ARP) messages onto the drone's local network to link the attacker?s MAC address with the IP address of the drone or controller.

Mitigation: Use ARP spoofing detection tools, implement static ARP entries, and use secure protocols like ARPSEC to prevent ARP spoofing attacks.

DoS Attack on Drone Operator:

Denial-of-Service (DoS) attacks on drone operators involve flooding the operator's communication channels with traffic, rendering them unable to control the drone effectively.

Mitigation: Use encrypted communication channels, implement DoS protection mechanisms such as rate limiting and traffic filtering, and employ intrusion detection systems to detect and respond to DoS attacks.

Drone Video Interception:

Drone video interception involves unauthorized access to the video feed

transmitted by the drone, allowing attackers to view or even manipulate the footage.Mitigation: Encrypt video transmission channels to protect the video feed from interception. Use secure communication protocols such as TLS/SSL for data transmission. Regularly update firmware to patch vulnerabilities, and ensure proper authentication mechanisms are in place for accessing the video feed.