Security Check Report

System Information

Username: xxx

Drone Manufacture: DJI

Drone IP: 192.168.1.6

Network Interface: wlan0

Open Ports: [(21, 'ftp'), (22, 'ssh')]

Kernel Version: 6.8.9-arch1-1 #1 SMP PREEMPT_DYNAMIC Thu, 02 May 2024 17:49:46 +

Security Issues

SSH Brute Force:

SSH brute force is a method of attempting to gain unauthorized access to a 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.

FTP NullSession:

FTP null session is a type of security vulnerability where an attacker can access an FTP server without authentication.

Mitigation: Disable anonymous FTP access, restrict access to authorized users only, and use secure FTP protocols such as SFTP or FTPS.

Command Injection:

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application.
Mitigation: Validate and sanitize user input, use parameterized queries in databases, and employ web application firewalls (WAFs) to detect and block command injection attacks.

Drone Instruction Injection:
Drone instruction injection is a type of attack where an attacker injects malicious instructions into the commands sent to a 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:
ARP spoofing is a technique whereby an attacker sends fake Address Resolution Protocol (ARP) messages onto a local area network in order to link the attacker?s MAC address with the IP address of a legitimate member of the network.
Mitigation: Use ARP spoofing detection tools, implement static ARP entries, and use secure protocols like ARPSEC to prevent ARP spoofing attacks.

DoS 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.