Drone Security Scoring System

Bruno José do Campo Branco

Thesis to obtain the Master of Science Degree in

Military Electrical Engineering

Supervisor(s): Prof. José Silvestre Serra Silva
Prof. Miguel Nuno Dias Alves Pupo Correia

December 2024

Declaration

I declare that this document is an original work of my own authorship and that it fulfills all the requirements of the Code of Conduct and Good Practices of the Universidade de Lisboa.

Acknowledgments

The success of this work was achieved thanks to the ongoing guidance and support of my advisors, Professor José Silva and Professor Miguel Correia. I am grateful for their full availability throughout the development of this work, as well as their motivation and all the knowledge shared, that were essential for the success of this work. I want to thank all my course comrades for their support, especially Second Lieutenant Tm Younes Zidane for providing me with data to support my work. I would also like to thank my friend, Fabio Gomes, who was always available and prepared to help. Finally, my family, who have undoubtedly been a source of inspiration throughout my work, as they have always motivated me to achieve a better version of myself, essential for this work's success.

Resumo

Os veículos aéreos não tripulados (UAV), acrónimo utilizado na tradução para a língua inglesa, têm vindo a assumir um aumento de importância em vários sectores, desde aplicações comerciais a operações militares. No entanto, com o aumento da sua utilização, as vulnerabilidades de cibersegurança em drones estão a tornar-se cada vez mais uma preocupação significativa. Os drones são suscetíveis à uma variedade de ciberataques, incluindo ataques que visam os seus canais de comunicação e sistemas, o que podem originar numa perda do controlo do drone ou um acesso não autorizado ao sistema do mesmo.

Esta dissertação propõe um novo método de classificação para avaliar o nível de segurança dos drones. O Sistema de Classificação de Segurança de Drones (D3S) é um método de avaliação de segurança que analisa os aspetos de segurança dos diversos componentes de um modelo de drone. Este sistema fornece uma classificação global de segurança, através da avaliação de métricas como os protocolos de comunicação, vulnerabilidades de software e a eficácia de mecanismos de segurança concebidos para a defesa contra ciberataques.

Para suportar o D3S e identificar potenciais vulnerabilidades nos drones foram realizados testes de penetração. A primeira fase dos testes de penetração foi a Recolha de Informação, que envolveu uma análise profunda dos protocolos de comunicação e a identificação de portas abertas no software do drone. Na segunda fase, a Exploração, foram executados ciberataques, como ataques de desautenticação, inundação e de repetição, com o objetivo de obter controlo total do UAV. Para comprovar o método D3S, foi utilizado oito modelos diferentes de drones, revelando importantes aspetos no desempenho de segurança e nas respostas dos seus sistemas. Os testes destacaram fatores como a não utilização de comunicações Wi-Fi, o que impediu a realização de ciberataques, e uma ligação direta entre o preço do UAV e as suas funcionalidades de segurança.

Palavras-chave: Veículo Aéreo não Tripulado, Cibersegurança, Ciberataque, Segurança

Abstract

Unmanned Aerial Vehicles (UAVs) have become increasingly important across various sectors, from commercial applications to military operations. However, with the increase in usage, drones' cybersecurity vulnerabilities have also emerged as a significant concern. Drones are susceptible to a range of cyber-attacks, including attacks that target their communication channels and control systems, which can result in loss of control or unauthorised access.

This thesis explores the security level of drones through a classification method. The Drone Security Scoring System (D3S) is a security assessment method that analyzes the security aspects of the diverse components within a UAV model. It provides an overall security rating by evaluation metrics, such as communication protocols, software vulnerabilities, and the effectiveness of security mechanisms designed to defend against cyber-attacks.

Penetration tests were carried out to support D3S and observe potential vulnerabilities in drones. The first phase of the penetration testing was Information Gathering, which involved a thorough analysis of the communication protocols and the identification of open ports within the drone's software. In the second phase, Exploitation, specific cyber-attacks such as deauthentication, flooding, and replay attacks were executed in an effort to take full control of the UAV. Eight different UAV models were tested using the D3S method, revealing notable variations in their security performance and system responses. The tests conducted highlighted factors such as the absence of Wi-Fi communication in certain drones, which prevented some attacks, and a direct link between the price of the UAV and its security features.

Keywords: Unmanned Aerial Vehicle, Cybersecurity, cyber-attacks, Security

Contents

List of Figures

List of Tables

Glossary

ACCESS	Advanced Communication Control Elevated Spread Spectrum
AES	Advanced Encryption Standard
AFHDS	Automatic Frequency Hopping Digital System
ARP	Address Resolution Protocol
BLOS	Beyond Line-of-Sight
BSSID	Basic Service Set Identifier
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
D3S	Drone Security Scoring System
DDoS	Distributed Denial of Service
DFD	Data Flow Diagram
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DREAD	Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability
DSM	Digital Signal Modulation
DSSS	Direct-Sequence Spread Spectrum
FASST	Futaba Advanced Spread Spectrum Technology
FHSS	Frequency-Hopping Spread Spectrum
FTP	File Transfer Protocol
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
ISAAF	Information Systems Security Assessment Framework
LOIC	Low Orbit Ion Cannon
LOS	Line-of-Sight
MAC	Media Access Control
MAVLink	Micro Air Vehicle Link

MitM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
OFDM	Orthogonal Frequency-Division Multiplexing
OSINT	*Open Source Intelligence*
OSSTMM	Open Source Security Testing Methodology Manual
PTES	Penetration Testing Execution Standard
RC	Rivest Cipher
RF	Radio Frequency
RTSP	Real Time Streaming Protocol
SAE	Simultaneous Authentication of Equals
SDR	Software Defined Radio
SSH	Secure Shell
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilige
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

Chapter 1

Introduction

This chapter presents a brief description of the importance of security in UAVs, the proposed objectives, and the key results achieved.

1.1 Motivation and Challenges

UAVs, also known as drones, were initially developed to be used in military operations and provide an advantage in the fields of strategy and tactics [1]. Their use in military operations is considered to be a revolutionary factor in conventional warfare, as in the use of large UAVs in counterterrorism operations in Afghanistan, Iraq, Pakistan, Somalia, and Syria [2].

Over the last two decades, drones have increasingly been considered a tool of war. In 2020, drones were used in the Nagorno-Karabkh war by Azerbaijan forces that decimated the Armenian army, including air defenses, combat vehicles, and other equipment. This conflict was considered one of the first in which the use of UAVs provided a devastating advantage [3]. However, terrorist organizations have also begun to carry out attacks with UAVs. In 2021, terrorists placed explosive devices on drones to attack a military building in India. Another example was in Turkey, where an organization used drones on a large scale to attack several buildings [4]. The war in Ukraine was also a landmark war in which drones were used, but the use of large drones was not effective because neither side controlled the airspace and were more susceptible to being destroyed. Thus, small UAVs operated by ground forces were used in low airspace, providing enormous advantages in surveillance of opposing forces, guiding forces, and being used as a weapon. This war between Russia and Ukraine has changed the image of small UAVs around the world [2].

Many drones have serious design flaws, and most do not encrypt communications [5]. These security flaws, also known as vulnerabilities, can allow the success of cyber-attacks on the UAV system [6]. These cyber-attacks can be used to achieve various objectives, such as disconnecting the UAV from the mobile device using the aircrack-ng tool [1] or overloading the UAV's system so that the user loses control of it, thus performing a Denial of Service (DoS) Flooding attack. Another possibility is to monitor communications, which corresponds to a Man-in-the-Middle (MitM) attack, to observe and cap-

ture possible critical data, using various tools such as arpspoof and ettercap [7]. On the other hand, it may be possible to fully control the UAV by injecting packets into it and by analyzing the communication protocol beforehand [8]. Alternatively, it may be possible to explore open ports, such as the telnet port, to gain access to the drone's system, observe critical information such as flight commands, and then take control [9]. These attacks can lead to various impacts, such as total control of the UAV by the attacker and the integrity of content, videos and images [10].

Commercial drones have been a constantly evolving technology used in everyday applications, such as real-time tracking, wireless coverage, search and rescue, delivery of goods, security, and surveillance [11] [12]. Building or acquiring a UAV is quite simple, leading to its widespread accessibility and ease of use [4], which has contributed to the increasing misuse by criminals [5]. The biggest threat from small UAV is their use in direct physical attacks on people, property, and infrastructure, as they may carry explosives, radioactive materials, or weapons [6]. A specific case of the malicious use of drones is the collection of data. The following examples describe real life scenarios where a drone can be used to obtain information with malicious intent [13]:

- The use of malicious software on the drone to track specific individuals via Wi-Fi communications of mobile devices in real-time. This software consists of impersonating the network to which the device is connected and forcing it to connect to the drone's network in order to obtain all the device's information and track it.
- Use the drone to scan the surrounding network and find domestic Wi-Fi networks to connect to the computers of that network eventually. Then, obtain remote access to the devices on that same network.
- The use of UAVs to communicate with smart devices. Using the Global Positioning System (GPS) model fitted to the drone to find the locations of the several pieces of equipment in a given area. This collection influences the privacy that individuals have in their homes.

For the execution of attacks, penetration testing methodologies can be used, as it involves identifying vulnerabilities in a system, following established phases [14] [15]. Many penetration methodologies, including Penetration Testing Execution Standard (PTES), employ different methods like Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilige (STRIDE) to search and identify vulnerabilities [1].

1.2 Objectives and Key Results

This thesis proposes a new method, the Drone Security Scoring System (D3S), to evaluate and assign a score to the security of a certain UAV model. Moreover, the D3S assessment is based on the execution of penetration tests against a set of commercial UAVs.

A classification security method for UAVs is proposed, combining the evaluation of drone communications and the results of different cyber-attacks. This method comprises groups of metrics, each with

a classification to obtain a final score for the UAV's security. The groups of metrics used are communications protocols for control and video transmission, software aspects, UAV characteristics, and the results of cyber-attacks. The development of this method was based mainly on security aspects, namely communications, as these can contain sensitive data during the establishment of the UAV connection and even during the flight, such as flight commands and access credentials, among others. This method has been designed for multiple purposes, such as checking the security of a drone, making comparisons between different drones, and also for defence since knowing the level of security the UAV has, which can be crucial for neutralizing it if used maliciously.

An important aspect of this work was the execution of cyber-attacks. These attacks were conducted to assess and justify the levels of security in UAVs against potential threats and to reveal any vulnerabilities they may possess. Also, information gathering was performed for an in-depth study before the execution of attacks. The main focus of the cyber-attacks chosen was on the drone's communications, to intercept and disable the drone's system, and finally, to gain complete control of the drone. An essential feature of this work is the use of eight UAVs of different brands and models to provide greater diversity in the implementation of D3S and observe any differences in responses to cyber-attacks.

To summarise, this work can be divided into two main phases. The first was the design of D3S, a method for evaluating a drone's security using multiple metrics. The second phase involved conducting cyber-attacks to stop the drone's user from having control and then gaining control of the drone.

1.3 Thesis Outline

This thesis is divided into five chapters. Chapter 2 presents the background and related work as a support to understand all the work developed. Chapter 3 presents the D3S method, as well as its development and the different metrics groups. Chapter 4 presents the experimental results obtained on the UAVs under study and the use of the method created. Finally, the Chapter 5 presents the conclusions reached, along with the proposed future work.

1.4 Scientific Contributions

The work developed in this thesis resulted in numerous publications, represented as follows:

1. B.Branco, J.Silva, M.Correia. Cyber-Attacks on Commercial Drones: A Review. *IEEE Access*, pages 12, 2024.

2. B.Branco, J.Silva, M.Correia. D3S: Drone Security Scoring System. *Information*, vol. 15, pp. 811, 2024. Publication date: 17 December 2024, DOI: https://doi.org/10.3390/info15120811 (ISSN: 2078-2489; JCR 2023 Impact Factor: 2.4; SCImago SJR 2023: Q2 Information Systems)

3. B.Branco, J.Silva, M.Correia. The Impact of Signal Inhibition on UAVs: DoS Attacks. *30th Portuguese Conference on Pattern Recognition (RECPAD)*, Covilhã, Portugal, October 2024.

4. B.Branco, J.Silva, M.Correia. New Drone Security Scoring System to Evaluate Drone Vulnerabilities. Submitted to *VI Encontro Anual da Investigação e Desenvolvimento em Ciências Militares (VI Annual Meeting on Research and Development in Military Sciences)*, Lisbon Portugal, November 2024.

5. B.Branco, J.Silva, M.Correia. Sistema de Classificação de Segurança em Drones. *IX Jornadas das Engenharias da Academia Militar, JEAM-IX (Military Academy's Engineering Symposium)*, Lisbon, Portugal, 2024.

Chapter 2

Background and Related Work

This chapter introduces theoretical concepts used in the following chapters and presents the work of other authors. The first part provides a description of the components and communication systems of an UAV. Next, there is a discussion on various penetration testing methodologies, along with the tools and cyber-attacks employed. Following that, a review of different cyber-attacks performed in other research papers is presented. An analysis of the Common Vulnerability Scoring System (CVSS) is also included. Finally, a summary of the entire chapter is provided.

2.1 Unmanned Aerial Vehicle

A modern UAV is an automated or remotely controlled flying vehicle with communication capabilities and a set of sensor systems and actuators [1].

There are currently several ways of classifying UAVs. One possible way is by weight, type of wing and rotors, altitude and range, and application [16], as is illustrated in Table 2.1. Another form of classification relates to command and control, that can be divided into the following categories [17]:

- **Remote pilot control**: all decisions sent to the drone are made by a human operator via a mobile device.
- **Supervised Control**: UAV has processes that are autonomous from the remote commands, although it is possible that the operator may intervene.
- **Autonomous Control**: the drone contains all the necessary components for autonomous operation.

An UAV is part of a system called Unmanned Aerial System (UAS). The central element of this system is the UAV, and the other elements are designed to support its service [18]. The elements of an UAS are: human element; command and control; UAV; communication data link; payload; launch and collection element. The command and control element can be divided into two distinct parts: the autopilot and the control station. An UAV in the autopilot system has a set of pre-programmed

Table 2.1: Classification of UAVs based on Weight, Wing and Rotor, Altitude and Range, and Application, adapted from [16].

Weight	Wing and Rotor	Altitude and Range		Application
Nano under 250g	Single Rotor	Hand Held	Altitude: <600m Range: <2 km	Personal
Micro 0.25kg to 2kg	Fixed Wing Rotor	Close	Altitude: <1500m Range: <10 km	Commercial
Small 2kg to 25kg	Tricopter	NATO	Altitude: <3000 m Range: <50 km	Government and Law enforcement
Medium 25kg to 150kg kg	Quadcopter	Tactical	Altitude: <5500m Range: <160 km	Military
Large more than 150kg	Hexacopter	Medium Altitude Long Endurance	Altitude: <9100m Range: <200 km	

instructions, giving it full control and requiring no human intervention [19]. On the other hand, the control station is an installation on the ground where human operators have the ability to control and monitor the drones during operations via a wireless connection to send commands and receive data in real-time. For a small drone, the control station is equivalent to a handheld transmitter or a remote controller [13]. The communication data link element consists of data received and transmitted by the control station and the UAV. However, there can be separate data links for different systems, as described in Subsection 2.1.2. The payload is related to the purpose of the UAV's operation, which corresponds to cameras, sensors, radars, and other diverse equipment. These objects can be used for weapons delivery, surveillance, communications, aerial detection, and many other applications [19].

2.1.1 Components

The main components of a UAV are the propellers, motors, sensors, speed controllers, flight controller, receiver, and battery. Additionally, the UAV communicates with external components, as the remote controller and Global Navigation Satellite System (GNSS), as shown in Figure 2.1.

From a hardware perspective, the flight controller is an essential component of the UAV [20]. The flight controller is the UAV's central processing unit that has the ability to interpret the high-level commands received [21]. These commands are first interpreted by the receiver via transmission protocols (TX), which are then converted into electrical signals and transmitted by receiver protocols (RX) [16]. The most common sensors are the inertial measurement unit, the main component of inertial navigation systems, and drone manoeuvers, which consist of a combination of accelerometers and gyroscopes to obtain a level of accuracy in the altitude, course, inclination of the drone and magnetometers, to measure the heading, force, and magnetic field [22].

The software can be divided into the following layers: Firmware, Middleware, and Operating System. The firmware is the lowest layer and gives instructions to the flight controller's processor. Middleware manages communication between subsystems, coordinating navigation, telecommunication services,

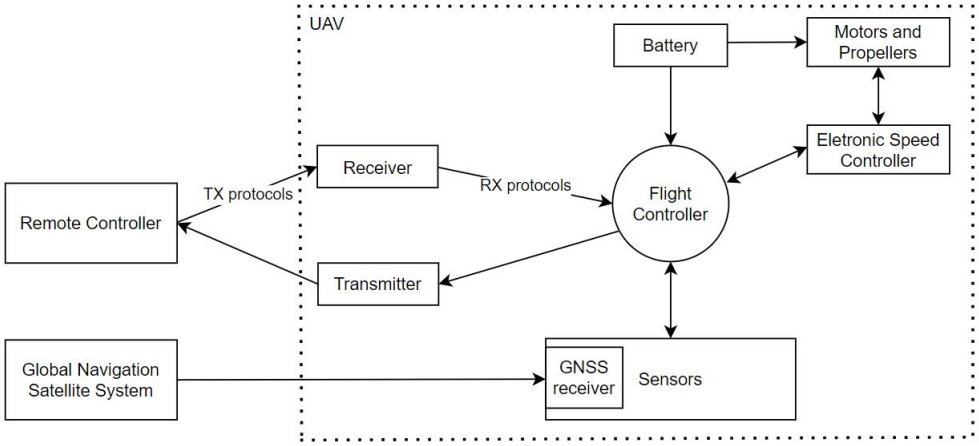


Figure 2.1: UAV Components, adapted from [16].

and propulsion control to ensure integrated system functionality. Finally, the operating system processes data in real-time, handling higher-level tasks, such as flight plans and video transmission [23].

2.1.2 Communications

The data link element of the drone's communication consists of data being received and transmitted by the control station and the drone itself. Data link communications can be divided into [19]:

- **Line-of-Sight (LOS)**: Communications related to direct radio waves. The distance of this type of communication depends on the power of the transmitter, receiver and possible obstacles. The use of a directional antenna can improve the signal strength and consequently adjust its position relative to the drone. If an antenna is used in the UAV, the signal strength is higher.

- **Beyond Line-of-Sight (BLOS)**: When direct communication between the operator and the UAV is not possible due to distance or obstacles, communication technologies like 2G, 3G, 4G, and 5G are employed in drones.

The most popular line-of-sight frequencies for small drones are 915 MHz, 2.45 GHz, and 5.8 GHz. However, a UAV can use different frequency bands for video transmission and others for command and control [19]. There are numerous communication protocols used by the UAV and remote controller. These protocols are characterized by data packets, encryption, and modulation [24].

Concerning modulations, Orthogonal Frequency-Division Multiplexing (OFDM) is one of the most common modulations used in UAVs communications protocols, which consists of using subcarries on a channel. Each subcarrier has an independent modulation scheme and, consequently, the data it carries. In turn, they are transformed into OFDM symbols, and after being concatenated, form an OFDM pulse [25]. Another modulation is Direct-Sequence Spread Spectrum (DSSS), where the message is spread over a wideband modulation code. In addition, it also uses phase shift keying, in which each bit of data is expressed in the phases of the signal wave [16]. Frequency-Hopping Spread Spectrum (FHSS) is a

modulation with a fast frequency change mechanism. This mechanism changes frequencies according to a pseudo-established sequence [25].

There are other protocols that use wireless technologies, such as Institute of Electrical and Electronics Engineers (IEEE) 802.11, which is used to create Wireless Local Area Network (WLAN)s. In these networks, there are risks in data transmission, which has led to the creation of security protocols such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 and WPA3. The WEP protocol uses the Rivest Cipher (RC) 4 encryption with a 64-bit key, 40-bit private key, and a 24-bit initial vector, but became obsolete in 2004 [26]. WEP was replaced by WPA protocol, which uses a pre-shared key, sometimes designated informally as the Wi-Fi password, to generate the keys used to protect the communication [7]. WPA was followed by WPA2, which is still widely used, but the current standard is WPA3. An important difference from the WPA2 protocol is the encryption method, which uses the Cipher Block Chaining Message Authentication Code. On the other hand, WPA3 uses the Simultaneous Authentication of Equals (SAE) protocol to perform authentication, substituting the use of the pre-shared key [26].

In addition to the IEEE 802.11 protocol, there are other protocols used in drones:

- **Micro Air Vehicle Link (MAVLink)**: Protocol used to transmit telemetry and control data in drones [25]. It has two versions, the first with an 8-byte header and packet loss detection and the second with a 14-byte header and some security mechanisms [27].

- **OcuSync**: Developed by DJI, and its main purpose is to provide security features to the UAV. It has mechanisms for protection against various cyber-attacks [28].

- **Lightbridge**: Protocol that uses FHSS and DSSS modulation. It has various video and output formats and can be used by remote controllers and mobile devices [29].

- **Futaba Advanced Spread Spectrum Technology (FASST)**: Protocol created by Futaba, used in the 2.4 GHz band with FHSS and DSSS modulation. It offers multiple channel selection modes and supports configurations of 7, 8, or 14 channels. [25].

- **Digital Signal Modulation (DSM)**: DSM2 operates in the 2.4 GHz band and uses DSSS modulation. It incorporates DuaLink technology, which operates on two channels. On the other hand, DSMX combines FHSS and DSSS modulation and a unique frequency hopping mechanism [25].

- **Advanced Communication Control Elevated Spread Spectrum (ACCESS)**: Has a capacity of 24 channels, an automatic binding mechanism, a spectrum analyzer to observe signal strength, noise, and surrounding frequencies, and an advanced encryption algorithm [30].

- **Automatic Frequency Hopping Digital System (AFHDS)**: Has several versions, the most recent being AFHDS3, which have bidirectional data transmission, providing greater security and stability. It has an automatic frequency hopping mechanism and an authentication mechanism [31].

2.2 Penetration Testing Methodologies

Penetration testing involves performing attacks on a system, network, or application to identify vulnerabilities that could be exploited by malicious actors [14]. Simultaneously, mechanisms must be implemented to validate and authenticate the entity of the pentester, ensuring it is identified as a legitimate user rather than an attacker by the system's security measures [32]. Penetration testing aims to discover vulnerabilities in different systems, such as web applications, social engineering, and wireless network infrastructures [15].

There are currently standards and methodologies for penetration testing, with the aim of providing different possible phases for carrying them out [33] [34], such as: Information Systems Security Assessment Framework (ISAAF) [35]; Zero Entry Hacking [1]; Open Source Security Testing Methodology Manual (OSSTMM) [36]; PTES [37]; National Institute of Standards and Technology (NIST) SP 800-15 [32]; Cyber Kill Chain [38].

The PTES and NIST SP 800-15 standards will be presented in more detail, as the PTES methodology involves a comprehensive process, from initial communication and threat modeling to vulnerability research, exploitation, and post-exploitation [37], and the NIST SP 800-15 provides a general penetration testing program and an overview of the essential elements, benefits and limitations [32]. OSSTMM presents an overview of penetration testing and three classes of attacks, which are: Communications, Spectrum and Physical Security. The ISAAF standard aims to evaluate application, system and network controls and consists of three phases: planning, access and reporting [33].

The Cyber Kill Chain is a methodology that aims to identify, prevent and describe a cyber-attack, and has the following phases: reconnaissance; weaponization; delivery; exploitation; installation; command and control; actions and objectives. The first phase is reconnaissance, which aims to gather information and possible vulnerabilities about the target. Arming corresponds to the action of establishing remote access to the target, so that in the delivery phase, the attack weapon is transmitted to the target. Subsequently, the attack is carried out, which replicates the exploitation phase. After carrying out the attack, it is necessary to maintain access to the target, the installation phase, and establish an access channel to the target, the command and control phase. Finally, the actions and objectives are designed to carry out measures to achieve the other objectives initially proposed [39] [40] [41].

Zero Entry Hacking consists of the following phases: reconnaissance; scanning; exploitation; maintaining access. This methodology is different because it has a cycle around the four phases mentioned and is implemented per attack vector. Thus, when it is not possible to exploit a particular attack vector, a reconnaissance of a different vector is carried out, which represents a new cycle. Scanning consists of exploiting the different vulnerabilities found in the reconnaissance phase [1] [42].

2.2.1 PTES and NIST SP 800-15

The PTES standard was created in 2010 by experts from various specific fields [33]. It aims to provide a baseline for penetration testing, and is divided into seven main sections [37]:

- **Pre-engagement interactions**:This phase is related to preparing for a penetration test in advance, i.e. asking general questions to define the purpose of the penetration test in the best possible way.
- **Information Gathering**: It consists of drawing up a document with the entire process and objectives for producing a strategic plan of attack on a target. The collection can be divided into three levels of maturity related to time, effort and access to information. The first level corresponds to basic information gathering with automated tools. Level two has a manual analysis in line with level one. Finally, level three consists of a more advanced collection with all the information gathered from the previous levels. To manage the collection of information, an *Open Source Intelligence* (OSINT) can be used, which has the search, selection and acquisition of public information. One advantage of its use is the wide use of information that is placed by companies or entities at the public level.
- **Threat Model**: It defines a threat modeling approach so that a penetration test can be performed as correctly as possible. It consists of identifying the threats and then listing them. This phase is considered critical to the success of a penetration test, due to the prioritization of all potential threats.
- **Vulnerability Analysis**: Vulnerability analysis involves discovering system and application flaws. The depth and amplitude are two factors that must be carried out in accordance with the intended objective.
- **Exploitation**: The main objective of this phase is to establish access to a system, bypassing security restrictions. If the vulnerability analysis phase is successful, this phase will correspond to the realization of an attack vector with high precision on a specific target, enabling greater impact and a high probability of success.
- **Post Exploitation**: The post exploitation phase consists of continuous monitoring of a compromised system and checking its relevance in terms of the data it contains and its usefulness. Various methods can be used in this phase with the aim of identifying and accessing new information, which in turn can provide a higher degree of access to other devices or systems.
- **Report**: All threats, vulnerabilities and actions taken in each phase are properly documented.

The NIST SP 800-15 standard consists of four phases, which can be identified in Figure 2.2 [32].

The first phase of this methodology corresponds to Planning, where the objectives are defined. The discovery phase is divided into two parts: information gathering and vulnerability analysis. Information gathering involves identifying ports, network services, applications and services in order to identify possible entries into the system. On the other hand, vulnerability analysis consists of comparing the analysis carried out on services, applications and operating systems with vulnerability databases to identify them. The next phase of the methodology, known as the attack phase, is a core component of any penetration test and involves exploiting identified vulnerabilities. If the attack is successful, the

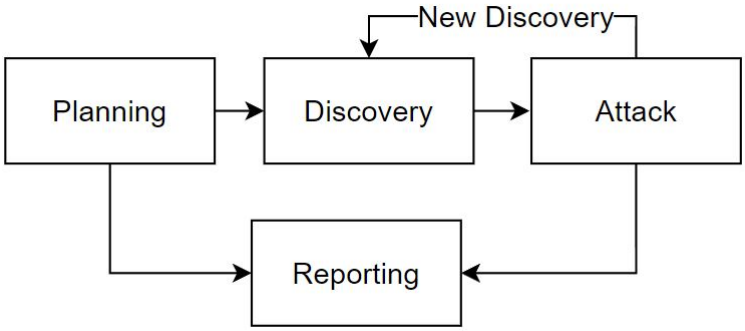


Figure 2.2: NIST SP 800-15 penetration testing methodology, adapted from [32].

vulnerability is verified, which in turn can grant the attacker a level of access to the system. This access may correspond to the maximum level or a level that provides new information about the system, which may be important for achieving a higher level of access. However, an attack may be deemed ineffective, which leads to the discovery of new vulnerability phase. The explanation of the attack phase can be seen in Figure 2.3.

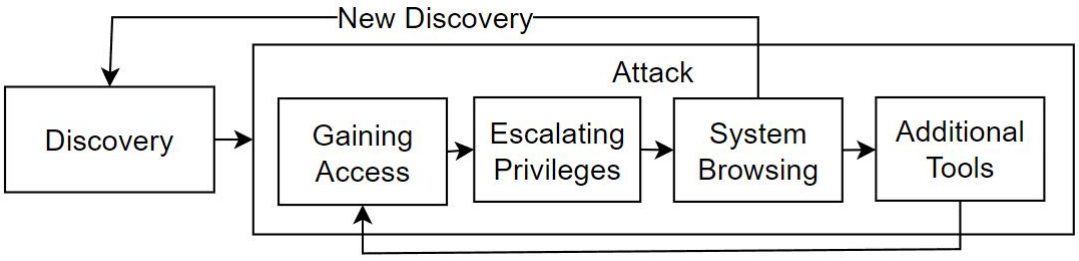


Figure 2.3: Attack phase of the NIST SP 800-15, adapted from [32].

Finally, the reporting phase takes place at the same time as the other phases. It consists of periodic reports and records throughout the course of the attacks and, at the end, all the vulnerabilities found are identified and, consequently, each one is classified [32].

2.2.2 Penetration Testing Models

Throughout the various phases of penetration testing, models such as STRIDE, Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability (DREAD), and CVSS are employed to assist in supporting the different phases of a methodology. The CVSS model will be explained in more depth in Section 2.4 as it is a fundamental element in the development of the drone evaluation model presented in Chapter 3.

Microsoft has developed a threat modeling methodology that contains four stages. The first stage is the diagram, which consists of creating an Data Flow Diagram (DFD) using the information collected from a system [43]. The identification stage aims to identify threats using the STRIDE model. Mitigation consists of deciding which procedure to adopt for each threat. The validation stage aims to verify the entire process performed in the previous phases.

Table 2.2: Threat and property definitions in the STRIDE method, adapted from [44].

Threat	Violated Property	Threat Definition
Spoofing	Authentication	Pretending to be someone other than yourself
Tampering	Integrity	Changing data or components in the system
Repudiation	No Repudiation	Not claiming responsibility for an action
Information disclosure	Confidentiality	Transmitting information to unauthorised people
Deinal of service	Availability	Exhaustion of the resources needed for the service
Elevation of privilige	Authorization	A person carries out actions that they are not authorized to do

The STRIDE method is based on the six main threat categories [43], which can be applied to each element or interaction of the DFD [1]. Table 2.2 presents the threats along with their definitions and the properties that are being violated for each threat. [45].

Table 2.3: Description of the DREAD method questions, adapted from [44].

Name	Question
Damage potential	What damage can it cause to the system?
Reproducibility	Is it easy to reproduce?
Exploitability	How much experience and effort does it take to carry out the attack?
Affected Users	How many users will be affected?
Discoverability	Is it easy to discover this vulnerability?

To assess the risk classification of a threat, Microsoft developed the DREAD method. Its function is to determine the value and impact of an identified threat using a classification method [46]. As is illustrated in the Table 2.3, where each letter corresponds to a question, which in turn is assigned a score, as can be seen in Appendix A [44].

2.2.3 Cyber-Attacks

This subsection will present numerous cyber-attacks that can be carried out either by malicious attackers or by a pentester:

- **DoS:** There are different types of DoS attacks, such as deauthentication attacks or flooding attacks. A deauthentication attack involves sending packets to break the connection between connected devices, such as the connection between the drone and the controller or a mobile device. On the other hand, a flooding attack overloads a device or communication channel with packets [9]. When this type of attack is performed by multiple devices on a target at the same time, it is considered a Distributed Denial of Service (DDoS) attack [47].

- **Dictionary Password Attack:** consists of cracking a password by making a sequence of attempts through a list of many words, symbols, numbers and passwords found in other attacks [47].

- **Brute Force:** consists of cracking a password by making several random attempts at possible passwords in the hope of hitting the right one [47].
- **Unauthorised Access:** The aim of this attack is to get inside the target system without authorization and thus be able to observe and use sensitive data and resources [48].
- **Jamming:** A jamming attack consists of transmitting electromagnetic signals identical to the communications frequency of the target device to disable the communications [49].
- **Script Injection:** This attack consists of injecting malicious code into the target operating system, with the aim of altering and/or damaging some feature of the device [48].
- **Shell Injection:** Inserts code into the shell of the target operating system, which in turn will enable the attacker to execute numerous commands in the shell [48].
- **Remote Command Executed:** The attacker can execute malicious commands on the target device to gain unauthorised access or steal or destroy resources [48].
- **Replay Attack:** It consists of using valid data captured in messages and, in turn, re-transmitting or altering them to the same target [47].
- **MitM:** Affecting availability, integrity, and/or confidentiality, these attacks can be passive or active. In a passive attack, no modifications are made to the communications, with the aim being only to capture sensitive information between devices, such as the traffic analysis MitM. In contrast, an active attack involves the attacker intercepting and modifying communications, such as Spoofing and Evil Twin [50][51].
  - **Traffic Analysis:** These attack consist of collecting information, such as the Media Access Control (MAC) address, encryption, and authentication protocols [47].
  - **Spoofing:** In a Spoofing attack, packets are used to impersonate legitimate device ny using identifiers such as IP or MAC addresses [9]. Another variant of this attack is Address Resolution Protocol (ARP) Spoofing, which exploits the ARP cache to associate the drone's IP address with the attacker's device via a fake ARP request. After the success of an ARP spoofing is possible to insert a fake MAC address device into the ARP cache, turning the attack into an ARP Poisoning attack [52].
  - **Evil Twin:** Involves setting up a fake access point that pretends to be a legitimate network. During the authentication process, this fake access point captures the 4-way handshake, allowing all communications between devices to pass through the fake access point [51].

2.2.4 Attack Tools

In the different phases of a penetration testing methodology, specific tools can be used for each phase. Below is a comprehensive list of tools available for conducting penetration tests [53]:

- **Wireshark:** Open source tool used to analyze network traffic packets [15]. It can read data from several protocols, such as Wi-Fi (IEEE 802.11 standard), Bluetooth, and others. It also decodes numerous protocols, like WEP, WPA e WPA2 [54].
- **Aircrack-ng:** Tool that can be divided into four categories: capture, attack, test, and cracking. It has the ability to capture packets, export and process data, carry out deauthentication attacks, replay attacks, injection attacks, and fake access points [55].
- **Hping3:** Network tool that sends Internet Control Message Protocol (ICMP)/User Datagram Protocol (UDP)/Transmission Control Protocol (TCP) packets with multiple peculiarities, namely by adjusting the size of the headers or the body of the packets. It is used to test firewalls, carry out DoS attacks, traceroute, and fingerprinting remote operating systems [56].
- **Low Orbit Ion Cannon (LOIC):** An open source tool for executing DoS attacks with different methods, including Slow LOIC, TCP, UDP, Hypertext Transfer Protocol (HTTP) and ICMP [57].
- **Netwox:** An open source tool for testing networks, which in turn has a command for executing DoS [57]. It uses the Netwib library, which has network functionalities for many protocols, such as TCP, UDP and ICMP. It also has the ability to encode and decode packets, launch spoofing attacks, and create clients and servers [58].
- **Hydra:** Login cracking tool that supports numerous protocols, which aims to gain unauthorised access to a system remotely [56].
- **Hashcat:** A tool that has a vast number of attacks, such as Brute Force, Dictionary, Deauthentication, Fingerprint attacks, and has more than three hundred hashing algorithms [56].
- **Ettercap:** It has several features such as analyzing hosts and networks, decrypting communication protocols, data injection, and several sniffing modes. It also has a graphical interface in addition to the command line interface [56].
- **Nmap and Nessus:** Open source network scanning tools offer diverse methods for gathering information about the system under study.. These tools can identify open ports, operating systems, vulnerabilities, and the network topology used on the system [15] [59].
- **Metasploit:** A tool capable of performing attacks and analysis to a target. It is considered a very important tool because it is extensible with exploits and has the ability to perform scanning services up to exploiting and extraction. The numerous tasks and commands are selected via a command line. [53] [54].

2.3 Cyber-Attacks on UAVs

This section provides a summary of attacks reported on UAVs and WLANs, with a more in-depth analysis of UAV targets. Initially, only a search for drone attacks was considered, however, papers

reporting attacks on WLANs were also considered since drones use wireless communication protocols in most cases.

Table 2.4 outlines the UAVs studied, detailing the specific attacks performed on each. The table includes a column with the commercial price of each drone, as this may express its sophistication and its level of security. However, the table does not show a strong correlation between price and attacks reported. For a rigorous assessment, all attacks would need to be performed on each drone under identical conditions. Figure 2.4 illustrates the distribution of the number of cyber-attacks across the different UAVs.

Table 2.4: Cyber-Attacks used in the UAVs of the selected papers.

Brand	Model	Price(€)	DoS	MitM	Password and Protocols Crack	Unauthorised Access	Command and Code Injection	Jamming
Parrot	AR	]0 ; 100] (discontinued)	✓	✓		✓		✓
ElectroFun	Cheerson CX-10W	[100; 200] (discontinued)	✓	✓		✓		
Bitcraze	Crazyflie 2.1	[150;250[						✓
DJI	Tello	[150;250[	✓	✓	✓		✓	
Parrot	Anafi	[300-400] (discontinued)	✓	✓				
3DR	Solo	[500-1000] (discontinued)	✓					
3DR	X8+	[2000-2500] (discontinued)	✓				✓	
DJI	Phantom 3	[500-1000]						✓
DJI	Phantom 4 PRO	[1000-1500]						✓

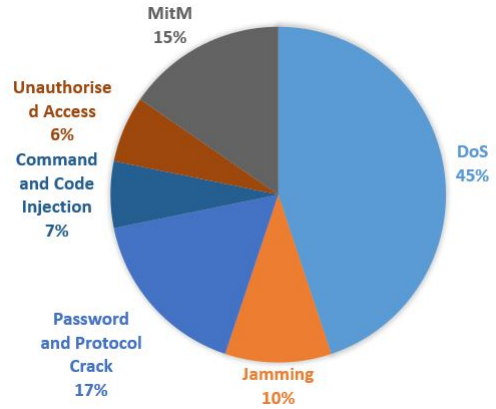


Figure 2.4: Graph with the distribution of the number of cyber-attacks

2.3.1 Denial of Service

A DoS attack makes a system unavailable for a period of time [57]. The DoS attacks reported against drones occurred at the network layer. These attacks involved obtaining the MAC and IP addresses of the drone or WLAN device.

Table 2.5: DoS Attacks on UAV

Author	Drone	Type of Attack	Tool	Target	Comments
Bertoli [60]	Parrot AR	deauthentication	Aircrack-ng	Drone and remote controller	Successful
		UDP flood	Hping3	Navigation data on port 5554	Successful
		TCP flood	Hping3	Video streaming on port 5555	Successful
Kadripathi [61]	Rogue	deauthentication	Aircrack-ng	Drone and remote controller	Successful
Feng [57]	Parrot Anafi	deauthentication	Aircrack-ng	Drone, remote controller and mobile device	Unsuccessful attack on controller
		TCP flood	Hping3	Web server on port 80	Successful
				Video streaming on port 554	Some frames were lost
			LOIC	Web server on port 80	Unsuccessful attack
				Video streaming on port 554	Successful
			Netwox	Web server on port 80	Slowing down on the web server
				Video streaming on port 554	Some frames were lost
		Slowloris (HTTP flood)	LOIC	Web server on port 80	Successful
				Video streaming on port 554	Successful
Malimban [38]	DJI Tello	deauthentication	Aircrack-ng	Drone and mobile device	Successful
Westerlundr [9]	Parrot AR Cheerson CX-10W	deauthentication	Aircrack-ng	Drone and remote controller	Successful
Vasconcelos [62]	Parrot AR 3DR Solo	TCP flood	LOIC	FTP, Telnet and video steaming ports	Successful
			Netwox	FTP, Telnet and video steaming ports	Successful
		ICMP flood	Hping3	Drone	Successful
Gran [1]	Parrot Anafi	deauthentication	Aircrack-ng	Drone and remote controller and mobile device	Unsuccessful attack on controller
Rubbestad [7]	DJI Tello	TCP flood	Hping3	Video streaming on port 9999	Successful
Intwala [63]	DJI Tello	deauthentication	Aircrack-ng	Drone and remote controller	Successful
Astaburuaga [64]	Parrot AR	deauthentication	Aircrack-ng	Drone and remote controller	Successful
Kwon [8]	3DR X8+	ICMP flood	Hping3	Drone	Successful

Several DoS attacks against drones have been demonstrated in the literature (Table 2.5). The most commonly used type of DoS was deauthentication using the aircrack-ng tool, followed by variants of flooding attacks. These variants consist of the packet protocol used in the attack, such as TCP, UDP, ICMP, and HTTP. Aircrack-ng sub-tools were used to carry out the deauthentication attack: airodump-ng, to capture the drone's MAC address and controller; aireplay-ng, to perform the attack.

According to Gran and Mickols [1], when the drone was connected to the mobile phone the deauthentication attack was carried out successfully. However, when the controller was used, the attack was not effective. The same thing happened in the work of Feng and Tornert [57], the remote controller used the IEEE 802.11w communication protocol, which has mechanisms against this type of attack, such as the management frame protection. Another mechanism against this attack is to change frequency channels when detecting communication interruption, as demonstrated by Intwala *et al.* [63] when evaluating the packet transmission rate with the success of several repeated attacks in the DJI Tello Drone. Executing a deauthentication attack can have several effects on the drone, such as simply losing the connection and continuing to fly without receiving new commands or stopping flying. These two situations were reported by Westerlund and Asif [9].

Regarding flooding attacks, different scenarios occurred in the work of Rubbestad and Söderqvist [7], such as video transmission interruption and drone control stopped. On the other hand, when Feng

and Tornert [57] carried out a flooding attack with the LOIC and Netwox tool on the drone's web server, it was ineffective, but the video transmission was stopped. However, this was not the case when using the Hping3 tool to carry out the Slowloris attack. Vasconcelos *et al.* [62] tested also this type of attack on two drones and observed that the connection between the controllers and the drones was affected, one more than the other, because one of the drones had a more robust processor.

The impact of flooding attacks can be explained by a variety of reasons, such as the implementation of protection mechanisms against these types of attacks, the construction of drone components strong enough to operate when under attack, and the operation characteristics of the various tools. To analyze the impact of each tool, a comparison of the packets between the drone and the remote controller was performed on Bertoli *et al.* [60], and a comparison of the latency rates on Vasconcelos *et al.* [62].

Bertoli *et al.* [60] studied the number of packets transmitted between the drone and the controller over a period of time in the following situations:

- No attack: 459,839 packets
- Deauthentication: 8,576 packets
- TCP flood: 403 packets
- UDP flood: 5,493 packets

From the values shown, the TCP flood attack had a greater impact than the other attacks, because the number of packets received by the UAV has drastically reduced. However, the discrepancy between the UDP flood and TCP flood attack, when using the same tool, did not influence the overall success of the attack.

The study of the latency rate on Vasconcelos *et al.* [62] showed that the Hping3 tool produced the highest value on the Parrot AR drone. On the other hand, the Netwox tool had the highest value on the 3DR Solo drone. Thus, the tools produce varying effects, which also depend on the drone's specific components. Concerning the papers targeting WLAN devices, most of them used aircrak-ng to carry out deauthentication attacks [51, 65–73]. In contrast, [74] used Nessus, while [75] relied on Wi-Fi Pumpkin. Additionally, some papers did not specify the tool used [52, 76–82].

The defense against deauthentication attacks is the use of protected management frames that are in the IEEE 802.11w communication protocols, as noted in [1]. In other words, the use of an encryption pairing mechanism between devices, which provide security for the connection and disconnection. Regarding flooding attacks, this requires a robust processing system capable of managing a large number of packets, or a system configured to reject packets that do not align with specified parameters established between the UAV and the controller.

2.3.2 Password and Protocol Crack

Table 2.6 shows the tools and the objectives (protocols or passwords) in the papers that perform this type of cyber-attack.

Table 2.6: Password and Protocols Crack

Target	Author	Objective	Tool
DJI Tello Drone	Rubbestad [7]	WPA2	Aircrak-ng
	Intwala [63]	Password	-
Wireless Network Device	Kissi [83]	WEP	Aircrak-ng
	Alhamry [66]	WPA/WPA2	Aircrak-ng
	Patel [67]		
	Pimple [69]		
	Kissi [83]		
	Fikriyadi [71]		
	Astrida [72]		
	Koutras [84]		
	Koutras [84]	WPS	Aircrak-ng
	Bakry [85]	Password	Nmap
			Hydra
	Carranza [86]	WPS	Reaver
	Syed [87]	Password	Hydra
	Gustafsson [88]	Password	Hashcat

Rubbestad and Soderqvist's work [7], which used the aircrack-ng tool in a deauthentication attack, successfully captured the WPA handshake. It was possible to crack the encryption key with the captured key, with a password dictionary. Another goal in these attacks is to discover the device's password. In the study by Intwala *et al* [63], password cracking was attempted on several passwords for the DJI Tello drone, although the tool used was not specified, and the time that would take to crack the password was studied:

- `1234567890`: 1-5 seconds
- `Abc12345`: 30 seconds
- `Abcd12345678`: 1 minute
- `abcdefgh`: 1 minute
- `Abcd#789$`: 15 minutes

The attack executed by Syed *et al.* [87] consisted of using the crack.txt dictionary with the hashcat and Hydra tool. The same procedure was performed by Gustafsson and Kvist [88] with the following dictionaries: rockyou.txt, crackstation.txt, and crackstation-human-only.txt.

The success of this type of attack depends on some variables, such as the computing power of the devices executing the attacks, the protocols being used, the dictionaries with multiple passwords, and the password that the device or drone has. To defend against this type of attack, it is essential to use

protocols with strong security and encryption features. One effective option is the WPA3 protocol, which incorporates SAE encryption, as research has shown, the WPA and WPA2 protocols are no longer effective in defending against these attacks. Passwords are also a crucial factor and are considered to be the main factor in the success or failure of these attacks, so the mixture of alphabetical, numerical, and special characters drastically increases the time it takes to find the password.

2.3.3 Man in the Middle

This attack topology is not seen in the same way by Westerlund and Asif [9], as it characterizes Spoofing and MitM as separate attacks. This poses a certain difficulty when analyzing the numerous papers, as many authors perform a spoofing attack and do not mention that they are actually carrying out a MitM attack. Table 2.7 represents some types of MitM attacks, a tool not identified in the table is Wireshark because almost all of the papers use it.

Biondi *et al.* used Wireshark and the H264 extractor to interpret and reconstruct the cameras under study video session [74]. The same can also be applied to drones since almost all drones have a camera.

Table 2.7: Types of MitM Attacks

Type of Attack	Author	Target	Tool
MAC Spoofing	Karmakar [89]	Drone	Oden
	Westerlundr [9]	Drone	Python Script
ARP Spoofing ARP Poisoning	Gran [1]	Drone	Ettercap
	Buckle [51] Gustafsson [88] Fikriyadi [71] Alhamry [66]	WLAN	Ettercap
	Bakry [85]	WLAN	Bettercap Xerosploit
	Syed [87]	WLAN	MITMF
Evil Twin	Shrivastava [90]	WLAN	Raspberry Pi 3
	Patel [67]	WLAN	Automatic Script

Karmakar *et al.* [89] executed a MAC Spoofing attack, using Wireshark to capture the MAC address and the Oden tool to change the MAC address in the firmware, which made it possible to control the drone. The same topology was employed by Westerlund and Asif [9], but opted to create a script to replay captured drone controls instead of using the Oden tool.

Rubbestad and Söderqvist [7] and Gran and Mickols [1] executed this procedure with the Arpspoof and Ettercap tools, respectively. About WLAN devices, Alhamry and Alomary [66] also carried out ARP Spoofing using Ettercap, which made it possible for all communications to pass through the attacker's machine, thus observing types of sensitive information. The same attack with the same tool was exe-

cuted by Buckle [51], Gustafsson and Kvist [88] and Fikriyadi [71]. It was conducted by Bakry *et al.* [85] the same procedure using a Raspberry Pi with the Bettercap and Xerosploit tools. Another tool to carry out this attack is MITMF [87].

Shrivastava [90] implements this type of attack in two stages: a passive phase, where the attacker waits for the client, and an active phase, where the client is forcibly disconnected. During the passive phase, Evil Twin boosts its signal strength to capture the Basic Service Set Identifier (BSSID) and channel as it waits for the client to connect. In the active phase, after establishing a connection, Evil Twin sends a deauthentication attack to break the connection to the legitimate access point, attempting to redirect the client's connection to itself only. Patel [67] executed an identical attack, by knowing the client's BSSID and using the aircrack-ng tool to deauthenticate the client from the device, thus capturing the network password and successfully connecting the client to the fake access point.

Analyzing MitM attacks is challenging due to the variety of techniques and objectives associated with them. For instance, some authors classify Spoofing as a MitM attack, while others do not, complicating direct comparisons across studies. A significant aspect of MitM attacks is that the devices involved in communication remain unaware that their transmissions are being intercepted and that the information exchanged can be modified.

it's crucial to note that monitoring communications can reveal critical data, such as passwords embedded within payloads, thereby facilitating additional cyber-attacks.

Outlining all the attacks described, it's crucial to note that monitoring communications can reveal critical data, such as passwords within payloads, thereby facilitating additional cyber-attacks. Also, by performing an ARP cache poisoning attack, communications can be rerouted through the attacker first rather than the user of the device, thus avoiding the need to crack the WPA2 protocol, as demonstrated by [51].

2.3.4 Jamming

Jamming the Radio Frequency (RF) communications between the drone and the controller can be used for several purposes.RF jamming serves to block the reception of control commands, potentially causing the drone to crash or activate safety protocols (e.g., returning to the starting point). GPS jamming can also be used to interfere with the drone's GPS communications, which is even more effective than RF jamming as the drone is unable to know where it is and return to its controller [16]. One point to note is that jammers can interfere with other devices in the same frequency range. Table 2.8 shows the different jamming attacks performed on UAVs and their objectives.

Using a Software Defined Radio (SDR), Slimeni and Dalleji [91] developed a system for detecting, identifying, and jamming communications to the parrot AR drone. Mekdad *et al.* [92] carried out the same attack but with a different target, the Crazy Real Time Protocol from the Crazyflie 2.0 UAV.

Saputro's *et al.* [93] work consists of GPS jamming on the DJI Phantom 3 drone. GPS-SDR-SIM software was used to generate a GPS signal, which was then converted into a RF signal by an SDR. The drone's GPS signal was interrupted, demonstrating that the attack had been carried out successfully.

Table 2.8: Jamming attacks on UAVs.

Target	Author	Objective
Parrot AR	Slimeni [91]	Detect and disrupt communications
Crazyflie 2.1	Mekdad [92]	Detect and disrupt communications
DJI Phantom 3	Saputro [93]	Jamming the GPS signals
DJI Phantom 4 Pro	Rahman [94]	Jamming the GPS signals

However, the ground controller still operated the drone, as the frequency of the UAV control and the GPS were different. Rahman *et al.* [94] performed the same attack, but with the aim of observing the maximum range at which the jamming was effective in a DJI Phantom 4 Pro drone. The equipment used was a SDR, an amplifier and an antenna. The following characteristics were considered when performing the attack: the height and distance of the drone, the height of the antenna, and the angle of the drone to the reference level. The various tests conducted demonstrated that increasing both the angle and distance reduces the effectiveness of a GPS jamming attack.

Performing this type of attack on WLAN devices is very similar, as both use a SDR to disrupt Wi-Fi communications [95–98]. One aspect in this attack topology is the frequency used by the drones, whether it has several frequency bands for different data transmissions. This aspect is crucial to the success of this attack, as there may be mechanisms to detect interference and thus change the communication channel or even change the bandwidth. These frequency or bandwidth hopping mechanisms are essential for protecting against these attacks. However, it is necessary to take into account some characteristics of the operation of these mechanisms, such as the time it takes to detect any interference and in turn change the channel, and also the number of channels available within the same band.

2.3.5 Command and Code Injection

Command and Code Injection are attacks that exploit vulnerabilities in order to execute commands (or code) in an interpreter in the victim component. There are several ways to perform this attack, such as Script injection, Shell injection, and Remote command injection, depending on the vulnerabilities found in the target systems, drones, or WLAN devices [48]. Table 2.9 shows the papers that performed this attack, along with the target, objective and tools.

Table 2.9: Command and Code Injection Attacks on UAVs.

Target	Author	Objective	Tool
DJI Tello Drone	Rubbestad [7]	Drone disable	Pyhton script
3DR X8+	Kwon [8]	Control	-
WLAN device	Gustafsson [88]	Access	Pyhton script

Rubbestad and Söderqvist [7] use the Ryze Tello drone, which has a Software Development Kit, making it possible to send commands to the drone, change the drone's SSID and password. However,

the approach taken by Kwon *et al.* [8] was completely different. The drone under study, 3DR X8+, uses the MAVLink communication protocol, so was necessary to use the specific fields of each packet to communicate between the drone and the controller. This attack was conducted successfully with this type of drone because it was possible to inject packets when the drone was in a state of waiting for commands. If a command was received by the controller, the injected packets were not executed until the current task was completed and no other tasks were pending.

Remote code execution was conducted by Gustafsson and Kvist [88], who exploited a vulnerability in the WLAN device. By using a script to execute a reverse shell, they were able to gain root privileges and remotely control the device.

This type of attack requires an in-depth study of all communication protocol parameters, primarily focusing on flight commands, allowing packet injection and, consequently, control of the UAV. Drones and remote controllers need to reject packets or commands coming from other devices in order to avoid this type of cyber-attack. For this to happen, these devices need to have distinction mechanisms that are not based exclusively on IP or MAC addresses.

2.3.6 Unauthorised Access

This type of attack involves gaining unauthorised access to a system in order to retrieve information or data without permission [68]. All the papers that report this attack first collected information using the Nmap tool. Table 2.10 presents the papers that perform this attack, as well as their target and objectives.

Table 2.10: unauthorised Access Attacks on UAVs.

Target	Author	Objective
Parrot AR Cheerson CX-10W	Westerlund [9]	Access
Parrot AR	Astaburuaga [64]	Access

Westerlund and Asif [9] employed Nmap to scan two drones. The CX-10W model had no open ports, rendering it invulnerable to this type of attack, whereas the Parrot AR had open File Transfer Protocol (FTP) and telnet ports. By accessing the system through these ports, they could view files on the drone, including the device's password and data received during flight.

Westerlund and Asif [9] used Nmap on two drones. The CX-10W had no open ports, so it was not vulnerable to this attack, whereas the Parrot AR had open File Transfer Protocol (FTP) and telnet ports. By accessing the system through these ports, was possible to observe the files on the drone, such as the password and data received. The same procedure and result were also achieved in [64], demonstrating in more detail the files obtained: software controls, update files, camera stream, Wi-Fi configurations, access point, and other services.

This attack is only possible when there are open ports on the system. As observed in the papers, a similar approach has been applied to both drones and WLAN devices. All the access and data captured

through this cyber-attack are very sensitive. The attacks described are known vulnerabilities, such as the open ports that contain the telnet or FTP services. In order to better protect drones from this attack, the following options could be considered: disabling the specified ports; using the same services with encryption protocols, such as Secure Shell and Transport Layer Security.

2.4 Common Vulnerability Scoring System

The CVSS aims to assess and assign a score to software, hardware, and firmware vulnerabilities. The main objective of CVSS is to provide a way to measure the severity and impact of vulnerabilities, to support organizations in their responses to security incidents [99].

This vulnerability classification model was used as the basis for developing the D3S method. CVSS was very important because it has a very similar objective to the proposed D3S method. Therefore, its entire construction was developed based on an in-depth analysis of the CVSS, such as the group of metrics and the score that each metric has. However, CVSS and D3S differ in some characteristics since CVSS evaluates vulnerabilities found in systems based on impact, risk, and severity, while D3S evaluates the security of a drone based on security characteristics.

The CVSS version 4.0 uses the following groups of metrics, as shown in detail in Table 2.11 [100].

- **Base**: define the intrinsic characteristics of a vulnerability that remain constant over time and is the only mandatory group. This group is divided into exploitability, which corresponds to the properties of the vulnerability that make the attack succeed, such as the attack vector, complexity, requirements, required privileges, and user interaction. The other is the impact related with confidentiality, integrity, and availability in the vulnerable and subsequent system.

- **Threat**: This group also reflects the characteristics of a threat but with changes over time. These characteristics are based on current exploit techniques and the degree of accessibility or functionality of the exploit code.

- **Environmental**: represents the characteristics that are relevant and unique to an user's environment, such as the presence of security protocols. Also, this group has the modified base subgroup, which consists of a new analysis of the base group's metrics, taking into account the user's environment.

- **Supplemental**: This group is optional and describes the extrinsic attributes of a vulnerability in order to better understand the impact of a vulnerability in a unique environment.

The classification of this model consists of a score from zero to ten, where the highest value means critical vulnerability. This applies only to the base group or to the base, threat, and environmental groups. This CVSS model is used in the Common Vulnerabilities and Exposures (CVE) program. A program to identify, classify, and catalog cybersecurity vulnerabilities. Each CVE record has a description and an identification number, which is shared to ensure that the vulnerability is the same and that

no repeat vulnerabilities occur [101]. This model was used in the work of Rubbestad [7] to classify each vulnerability found in the UAV under study.

2.5 Summary

This chapter presented the background and related work with the aim of providing theoretical concepts and existing research into cyber-attacks to support all the work done.

Regarding the UAV, an element of the UAS, has several components, such as propellers, motors, sensors, speed controllers, flight controller, receiver, and battery. An essential aspect is communications, where it's important to consider the modulation, the communication protocols, and the associated security protocols.

Penetration methodologies are one way of performing cyber-attacks. An example of a methodology is PTES, which has several phases such as pre-engagement interactions, information gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting. In contrast, the NIST SP 800 15 methodology has fewer phases and divides the attack into gaining access, escalating privileges, system browsing, and additional tools.

A variety of cyber-attacks can be performed, depending on the objective of the attack, as presented in Section 2.2.3, and there are many tools available for these attacks, as shown in Section 2.2.4. Several papers were presented in which cyber-attacks and tools were implemented, with multiple objectives, such as intercepting and breaking communications between the UAV and the remote controller, gaining control of the drone, or accessing its systems. In addition, papers targeting WLAN devices were also used since some attacks conducted on Wi-Fi communications are very similar.

The CVSS classification method consists of evaluating vulnerabilities using various evaluation metrics. This model was the basis for the development of the D3S method, presented in Chapter 3.

Table 2.11: Metrics of the CVSS method, adapted from [100].

Metrics Group		Metrics	Value
Base	Exploitability	Attack Vector	Network (**N**), Adjacent (**A**), Local (**L**), Physical (**P**)
		Attack Complexity	Low (**L**), High (**H**)
		Attack Requirements	None (**N**), Present (**P**)
		Required Privileges	None (**N**), Low (**L**), High (**H**)
		User Interaction	None (**N**), Passive (**P**), Active (**A**)
	Impact	Confidentiality to the Vulnerable System	None (**N**), Low (**L**), High (**H**)
		Integrity to the Vulnerable System	
		Availability to the Vulnerable System	
		Confidentiality to the Subsequent System	
		Integrity to the Subsequent System	
		Availability to the Subsequent System	
Threat		Exploit Maturity	Not Defined (**X**), Attacked (**A**), Proof-of-Concept (**P**), Unreported (**U**)
Environmental		Security Requirements	Not Defined (**X**), Low (**L**), Medium (**M**), High (**A**)
		Modified Base	Same values of the Base metrics group
Supplemental		Safety	Not Defined (**X**), Present (**P**), Negligible (**N**)
		Automatable	Not Defined (**X**), No (**N**), Yes (**Y**)
		Provider Urgency	Not Defined (**X**), Red (**R**), Amber(**A**), Green (**G**), Clear (**C**)
		Recovery	Not Defined (**X**), Automatic (**A**), User (**U**), Irrecoverable (**I**)
		Density	Not Defined (**X**), Diffuse (**D**), Concentrated (**C**)
		Vulnerability Response Effort	Not Defined (**X**), Low (**L**), Moderate (**M**), High (**H**)

Chapter 3

Drone Security Scoring System

This chapter provides a detailed presentation and discussion of D3S, a method for evaluating the security of an UAV. The following sections will provide an in-depth description and analysis of how this method was created and implemented. It begins with a general overview that outlines the system's structure and objectives. This is followed by a detailed explanation of the development process for the entire method. The scoring method used is then described, followed by an in-depth interpretation of all the metrics that compose the method. Lastly, a summary of the D3S method.

3.1 D3S Overview

The primary purpose of D3S is to evaluate the security of an UAV, providing a method with groups of metrics for evaluating the components of a drone, through a security score. Figure 3.1 displays the groups of metrics that are part of the D3S method and will be presented in detail within Section 3.4, namely: **communications**, **characteristics**, **cyber-attacks**, and **software**. Each metric group has subgroups (white squares presented in Figure 3.1), each subgroup contains a number of metrics with an associated score. This scoring system is used to assess the overall strength of the UAV's security, thus providing a degree of defence and allowing for a precise determination of the drone's potential vulnerability to cyber-attacks.

Although D3S is built on the framework of CVSS, it serves a different purpose. CVSS aims to evaluate and describe a software, hardware, or firmware vulnerability found in a system to observe its characteristics in terms of its impact on the target, such as the recent Windows TCP/IP remote code execution vulnerability (CVE-2024-38063) has a CVSS score of 9.8 (critical). On the other hand, D3S does not assess a vulnerability but rates the security of a drone, where the rating indicates the possibility of vulnerabilities being found. This method can be performed before or after a vulnerability has been found and, therefore, be adapted to any vulnerability.

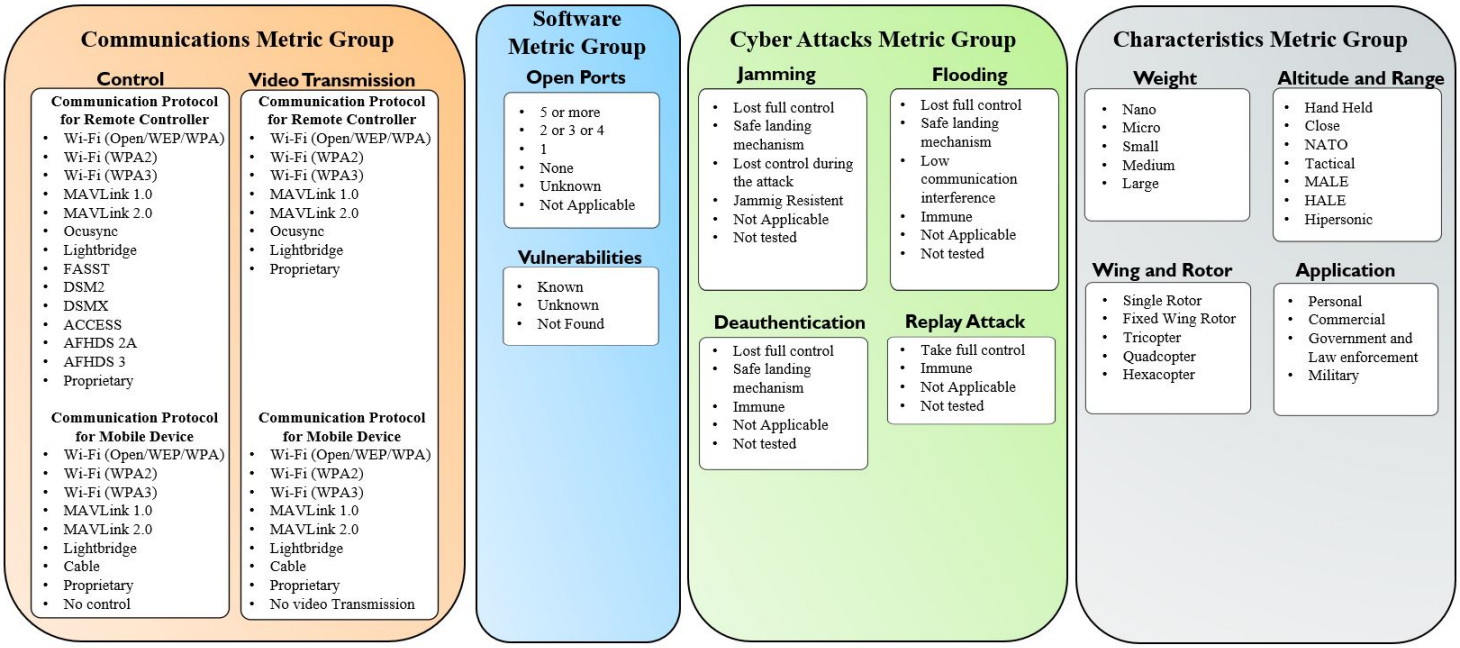


Figure 3.1: D3S Metric Groups.

3.2 D3S Development

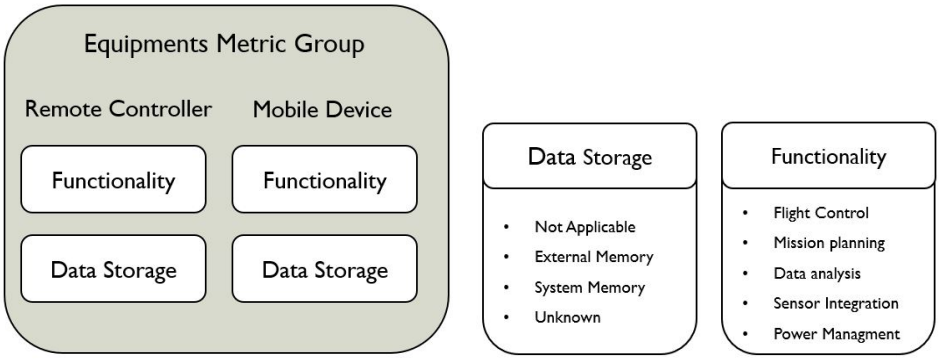
The preliminary version of this method consisted of identifying the most effective way to categorize UAV components into evaluation groups, resulting in the following groups of metrics: **communications**, **software**, **equipment**, **characteristics**, and **cyber-attacks**.

The **communications** group was divided into the **command and control**, **video transmission**, and **telemetry data**. This division of three subgroups aimed to obtain the possible division of communication channels between the remote controller/mobile device and the drone. However, the communication protocols used for **command and control** and **telemetry** data are identical to the UAVs analysed, so these two subgroups were merged in the **control** subgroup.

The **equipment** metrics group, as described in Figure 3.2, is present in the preliminary version but was removed. The figure includes the division of the remote controller and the mobile device (Figure 3.2a) and the metrics of each subgroup (Figure 3.2b). The purpose of this group is to determine the several functionalities that a remote controller or mobile device can have, which are directly related to the **communications** group. Concerning the **functionality** subgroup, the score of each metric is represented as a weight. For instance, if the remote controller included all possible functionalities, it would receive a score of five. This weight would then be combined with the value obtained from the **communication** subgroup to calculate the functionality subgroup value.

The **data storage** subgroup relates to where the data is being stored. An important note to consider on the remote controller and mobile device. However, **equipment** is not part of the D3S because it does not assess the security of the drone but rather the impact it may have on the UAV's devices.

In the preliminary version, there is a **hardware** group related to the **software** group. This **software** group concerns ports and vulnerabilities that the drone may have, specifically addressing attacks that do



(a) Equipment Metric Group. (b) Metrics of each subgroup.

Figure 3.2: Equipment Metric Group in the preliminary version of D3S development.

not require physical access, unlike the deprecated **hardware** group, which considered attacks involving physical access. The **hardware** group was excluded from D3S since a higher priority was given to remote attacks. In a war scenario, where attacks are typically carried out remotely, addressing remote vulnerabilities was considered more critical.

For the reasons explained above, D3S comprises four metrics groups in Figure 3.1. However, the major challenge throughout the development of the D3S was the selection of the metrics in each subgroup and, consequently, the scoring of each. This factor was mainly in the communication protocols, included in the **communication** metric group, as most of the time, a lot of information is not made available by the manufacturers, which makes it difficult to achieve an effective categorization and optimal classification. Therefore, it was necessary to collect each metric's security characteristics in the best possible way and relate them to each other.

D3S is based on a model that represents an UAV, similar to what happens with CVSS, which is a classification system for software vulnerabilities. Like any model, D3S does not consider all possible attacks against UAVs or all possible components that may be attacked. The attacks and components recognised are those that were considered more relevant. Like many uses of models in engineering, adding more details is negative as it makes the model harder to use and understand.

3.3 Scoring System

The scoring method for D3S is based on the CVSS approach. However, instead of extending to ten as the CVSS method, the D3S classification only goes up to five. This allows for a more intuitive representation of security levels, using terms such as very low, low, medium, high, and very high, as shown in Table 3.1.

This classification translates into an inversion of the CVSS values, as the highest CVSS value corresponds to a vulnerability with the greatest risk. As D3S is related to security, the highest value is assigned to the drone that has the most security. Also, the final score is obtained from the average of all the metrics selected from the different groups.

In addition to this scoring system, which provides an average of security, it is possible to assign

Table 3.1: Scoring Method of the D3S

Level of Security	D3S Score
Very High	4.0 - 5.0
High	3.0 - 3.9
Medium	2.0 - 2.9
Low	1.0 - 1.9
Very Low	0.0 - 0.9

different weights to the subgroups of metrics to obtain a security score aimed at the video transmission or control aspects. In other words, instead of an average score, the D3S will have a score more focused on a specific aspect of the drone.

Metrics can have seven different values, from zero to 5, and the ”-” parameter. This parameter means that the metric in question was not performed and, therefore, will not be included in the average score.

3.4 Metrics Groups

As presented previously, D3S has four major groups of metrics, which will be presented in detail in the following subsections. The most important and hardest part is not the selection of metrics but the classification that each one has and how it relates to the others. This was due to the limited information available in terms of communication protocols, which was necessary to try to obtain a coherent classification system that would make sense in all metrics. Most of the information that will be presented in each group of metrics has been documented in chapter 2. The repetition of information was made to provide the best possible explanation, focusing mainly on security features.

3.4.1 Communications

Table 3.2 shows all the protocols used as metrics in this **communications** group, with a brief description of their security, as well as their scores, a higher score means that they are more secure. The **communications** metrics group is divided into two parts: **control** and **video transmission**. In turn, each part has groups of metrics for the **remote controller** and **mobile device**. Before describing each subgroup, it is necessary to have a general understanding of the classification of all the protocols (metrics) used.

Wi-Fi is a communication protocol that usually uses OFDM modulation and may or may not have different security mechanisms. Wi-Fi (Open) indicates the absence of any security mechanisms, thereby taking a value of zero. With the same score, the Wi-Fi (WEP), which has been discontinued since 2004, and has weak protection against cyber-attacks, such as DoS, Mac Spoofing, dictionary attacks, brute force attacks, and Replay attacks [102]. Wi-Fi (WPA) received the same score of zero for several reasons: (i) it is vulnerable to the cyber-attacks mentioned before, except for the replay attack, which has

a more robust initialization vector than WEP and can make it more difficult to perform the attack; (ii) the classification of each metric was not given exclusively by the characteristics of the metric itself but also by a comparison between all the protocols used in this group; (iii) the defined scale of values (integers from zero to five) delimits the assignment of scores, but provides a simpler system to comprehend. Wi-Fi (WPA2) has a score of one because it is still vulnerable to some of the cyber-attacks mentioned, but it takes longer to carry out a brute force attack successfully. It also has an initialization vector against replay attacks and has a better encryption mechanism. Finally, Wi-Fi (WPA3) has a superior encryption mechanism and is no longer as vulnerable to most cyber-attacks. It is immune to DoS and replay attacks, and it takes many years to carry out a brute force attack successfully. It has, therefore, been given a score of three.

The MAVLink protocol has two versions. The first has no security features reported by the producers, so it was given a score of zero. On the other hand, the second version has some security in terms of encryption and authentication of messages, which has been given a score of one. This assignment was due to not knowing the encryption algorithm implemented and the modulation used.

The protocol with the highest value is OcuSync, as it protects against communication hijacking, MitM attacks, replay attacks, and eavesdropping. This protection factor against numerous attacks was higher than the fact that its modulation was unknown. However, it must have robust security mechanisms to be effective against many cyber-attacks. On the other hand, the ACCESS protocol was awarded a score of four because it guarantees the security of communications between the transmitter and receiver through a double-checking mechanism, which is a very important target for many attacks and also has an advanced encryption algorithm. Despite the limited information available on this protocol, it ensures the security of communications between the controller and the device (UAV) is a key factor.

The other protocols were classified by their modulation, mainly because it was one of the few security characteristics found on them. Thus, protocols with a combination of FHSS and DSSS modulation obtained a score of three, which guaranteed more excellent protection against interference attacks. This score was attributed to the following protocols: Lightbridge; FASST; DSMX. The protocols DSM2 and AFHDS 2A, which only have one modulation, were given a score of two. Despite this criterion, the AFHDS 3A protocol has only one modulation, but it has a unique frequency hopping algorithm and an authentication mechanism, so it was given a score of three.

Regarding the metrics for each subgroup, the protocols presented were used and placed according to their use for control (Table 3.3) or video transmission (Table 3.4), and in each table between the mobile device and the remote control.

Extra protocol metrics were added to cover all possible cases. One metric that is used in all subgroups is designated `proprietary`, with a value of two. When the protocol used in UAV communications is unknown, a rating of two was deemed most appropriate on the scale because an unknown protocol is less likely to have many security features, resulting in a lower intermediate value being assigned. Another metric is the `cable`, which corresponds to when the mobile device's communication is not directly with the drone but with the remote controller via a cable. This gives the drone one less communication channel, which in turn is attributed to a score of five. When evaluating drones with fewer communication

Table 3.2: Classification of the Communication Protocols used in the Communications Metric Group.

Protocols	Value	Description
Wi-Fi (Open/WEP/WPA)	0	Open: No security features. WEP: Uses the RC 4 encryption. It also uses the Cycle Redundancy Check value, and has been obsolete since 2004 [26]. WPA: Uses the Temporal Key Integrity Protocol (TKIP) encryption for authentication. However, the keys are created by RC 4, the main vulnerability [26].
Wi-Fi (WPA2)	1	It uses Advanced Encryption Standard (AES), among others, ensuring greater security than the WEP and WPA protocols [26].
Wi-Fi (WPA3)	3	It features SAE, among others, which has a secure key exchange protocol [26].
MAVLink 1.0	0	No security features.
MAVLink 2.0	1	Has a message encryption and authentication mechanism (Message Signing), which has a 32-byte secret key used for signing messages [27].
OcuSync	5	It uses the AES algorithm for UAV control communication. It is a protocol that protects against communication hijacking, MitM attacks, replay attacks, and eavesdropping [28].
Lightbridge	3	Uses FHSS and DSSS modulation, which provides resistance to interference [29].
FASST	3	It has a combination of FHSS and DSSS modulation that provides greater resistance to jamming [25].
DSM2	2	Uses DSSS modulation and DuaLink technology, operates and hops on two channels [25].
DSMX	3	Uses FHSS and DSSS modulation, and has a unique frequency hopping sequence on 23 channels in the 2.4 GHz band [25].
ACCESS	4	Uses 24 channels. The Automatic binding mechanism guarantees security between the transmitter and receiver through double-checking and an advanced encryption algorithm [30].
AFHDS 2A	2	Uses FHSS modulation and allows duplex communications [25].
AFHDS 3	3	It has the same characteristics as AFHDS 2A. However, it has a unique frequency hopping algorithm and an authentication mechanism [31].

Table 3.3: Metrics of the Control subgroup.

(a) Communication Protocol for Remote Controller.

Remote Controller	Score
Wi-Fi (Open/WEP/WPA)	0
Wi-Fi (WPA2)	1
Wi-Fi (WPA3)	3
MAVLink 1.0	0
MAVLink 2.0	1
Ocusync	5
Lightbridge	3
FASST	3
DSM2	2
DSMX	3
ACCESS	4
AFHDS 2A	2
AFHDS 3	2
Proprietary	2

(b) Communication Protocol for Mobile Device.

Mobile Device	Score
Wi-Fi (Open/WEP/WPA)	0
Wi-Fi (WPA2)	1
Wi-Fi (WPA3)	3
MAVLink 1.0	0
MAVLink 2.0	1
Lightbridge	3
Cable	5
Proprietary	2
No control	5

Table 3.4: Metrics of the Video Transmission subgroup.

(a) Communication Protocol for Remote Controller.

Remote Controller	Score
Wi-Fi (Open/WEP/WPA)	0
Wi-Fi (WPA2)	1
Wi-Fi (WPA3)	3
Ocusync	5
Lightbridge	3
Proprietary	2
No video transmission	5

(b) Communication Protocol for Mobile Device.

Mobile Device	Score
Wi-Fi (Open/WEP/WPA)	0
Wi-Fi (WPA2)	1
Wi-Fi (WPA3)	3
Lightbridge	3
Cable	5
Proprietary	2
No video transmission	5

channels, it's important to consider the impact of limited connectivity. In this case, the absence of video transmission and control becomes a crucial metric.

3.4.2 Software

The **software** metrics group is divided into two subgroups: **open ports** (Table 3.5) and **vulnerabilities** (Table 3.6).

The **open ports** subgroup has some metrics related to the number of open ports that a UAV can have, and the choice of value ranges was based on the tests made in Section 4.2.2. In addition, there is an `Unknown` metric, which means that the number of open ports is unknown because the appropriate tests have not been performed. Finally, the `Not Applicable` metric does not have a score because it is impossible to use this subgroup due to the UAV not using network ports, due to the fact certain communication protocols are not built on the internet protocol.

The **vulnerability** subgroup is directly related to the vulnerability classification of the CVE system, which guarantees D3S interoperability. This means that if vulnerabilities are found in the various com-

Table 3.5: Metrics of the Open Ports subgroup.

Open Ports	Score
5 or more	0
2 or 3 or 4	1
1	3
None	5
Unknown	2
Not Applicable	-

ponents of the drone, the classification assigned to that vulnerability is used. However, the CVE classification is assigned by the CVSS, which in turn ranges from a maximum value of ten, in the sense that the higher the value, the more critical the vulnerability is. Thus, in the `Known` metric, the CVE value is used with a reduced transformation of the scale to half and with an inverted transformation of the value because, in D3S, the higher score means a greater degree of security. The other metrics correspond to when no vulnerability search is performed, the `Unknown` metric, and when none is found, the `Not Found` metric.

Table 3.6: Metrics of the Vulnerabilities subgroup.

Vulnerabilities	Score
Known	CVE
Unknown	2
Not Found	4

3.4.3 Characteristics

The **characteristics** metrics group has a documentary value only, in other words, it has no classification. The subgroups used and their respective metrics are shown in Table 2.1, which are `Weight`, `Wing and Rotor`, `Altitude and Range`, and `Application`.

The reason for this group is to provide different classifications that an UAV can have with the D3S classification. This way, it will be possible to observe the basic characteristics of an UAV with the D3S score and relate it to other D3S classifications of others UAVs.

3.4.4 Cyber-Attacks

The **cyber-attacks** group corresponds to the different attacks performed and the result obtained that provides a level of security on the drone in the target component. All subgroups in this category include two unclassified metrics, `Not Applicable`, which indicates that the attack could not be executed, and `Not Tested`, meaning the attack was not attempted.

Table 3.7: Metrics of the Jamming subgroup.

Jamming	Score
Lost full control	0
Safe landing mechanism	3
Lost control during the attack	3
Jamming Resistant	5
Not Applicable	-
Not Tested	-

Table 3.8: Metrics of the Flooding subgroup.

Flooding	Score
Lost full control	0
Safe landing mechanism	3
Communication interference	3
Immune	5
Not Applicable	-
Not Tested	-

The **jamming** subgroup in Table 3.7 and the **flooding** subgroup in Table 3.8 have almost the same metrics. The metrics start with the worst case, which is when the operator loses total control of the UAV, then there is the case that the UAV has a security mechanism in which it makes a safe landing or remains stable in the air. These two metrics have the same classification, as they guarantee an intermediate level of security that the UAV has. However, it was thought that the safe landing mechanism might pose a danger to the UAV due to the fact that is possible to be captured after landing. On the other hand, the drone remaining stable in the air may also have an inability to recover the drone if the attack is not interrupted, so the same classification was given. Finally, the UAV is Immune or Resistant to the attack, with the highest score.

Table 3.9: Metrics of the Deauthentication subgroup.

Deauthentication	Score
Lost connection	0
Safe landing mechanism	3
Immune	5
Not Applicable	-
Not Tested	-

The **deauthentication** subgroup, Table 3.9, has almost all the metrics mentioned previously, except the one when the drone staying in the air, because when the drone loses communication with the

Table 3.10: Metrics of the Replay Attack subgroup.

Replay Attack	Score
Take full control	0
Immune	5
Not Applicable	-
Not Tested	-

controller or device, this was not observed in the drones tested and was therefore not included in this subgroup.

Finally, the replay attack subgroup, shown in Table 3.10, has two metrics with evaluation to demonstrate whether the attack was successful or not, with no middle term.

3.5 Summary

The D3S method has groups of metrics for performing a UAV safety assessment. The construction of this method was based on CVSS through its evaluation metrics, but it also uses vulnerability scores, which guarantees interoperability between CVSS and D3S.

This evaluation method has four main groups: **communications**, **characteristics**, **cyber-attacks** and **software**. The metrics groups include a study of the security of communications protocols, with a division to achieve the best classification of the drone, an analysis of vulnerabilities and open ports related to the **software** group, and the performance of **cyber-attacks** to evaluate the security mechanisms that the drone may have.

Chapter 4

Experimental Evaluation

This chapter presents the data and experimental tests used to evaluate the newly introduced D3S method applied to a selection of drones. It begins by presenting the materials used for testing and the UAVs involved. Then, the information gathering and exploitation phase, and the use of D3S with the results of cyber-attacks to observe the security of several UAVs. Lastly, a summary of the results obtained.

4.1 Material

The selection of materials was a critical decision to achieve the best possible results and ensure that the necessary criteria for data validation were met. The decision on the materials ranged from the operating system used, the multiple tools for penetration tests, the choice of antenna, and, above all, the choice of UAVs.

The operating system used was Kali Linux, with multiple pre-installed tools to implement all phases of a penetration testing methodology. The Subsection 2.2.4 explains some of the tools mentioned in Section 4.2 and 4.3. In addition to the tools, it has several pre-installed commands that make it easier to perform the tests. ALFA AC1900 Long Range USB Wireless Adapter antenna was selected which is a high-performance wireless adapter designed for long-range Wi-Fi connections. This will ensure sufficient range when the drones are in flight. The adapter is capable of monitoring and injecting packets in Dual-Band (2.4 GHz/5 GHz) and supports WEP, WPA, WPA2, and WPA3 security protocols. Additionally, it is compatible with Windows, macOS, and Linux operating systems.

Table 4.1 describes some characteristics of the UAVs employed. The price was used as a metric to allow the selection UAVs with different levels of sophistication. The E88 is the cheapest drone and related to the S2S UAV, is unbranded. The JJR/C Elfie+, although discontinued, is the only drone acquired in 2016, while the others were acquired in 2023 and 2024. This might explain why, it is pricier than the E88. These drones operate on the 2.4 GHz frequency band and lack GNSS. They use a remote controller and an application on the mobile device for video transmission, control, and flight modes. The SG108 UAV is very similar to those presented above. However, it's more expensive, has GNSS, uses

Table 4.1: Characteristics of the UAVs used

Name	Brand	Price(€)	Year of purchase	Remote Controller Protocol	Mobile Device Protocol	GNSS
E88	No Brand	€	2023	Unknown/Proprietary	Wi-Fi	No
Elfie+	JJR/C	€	2016	Unknown/Proprietary	Wi-Fi	No
S2S	No Brand	€€	2023	Unknown/Proprietary	Wi-Fi	No
SG 108	ZLL	€€	2024	Unknown/Proprietary	Wi-Fi	Yes
Zino Mini Pro	Hubson	€€€	2024	Unknown/Proprietary	Do not use	Yes
Evo Nano+	Autel	€€€	2024	Unknown/Proprietary	Do not use	Yes
Mini 3	DJI	€€€	2024	OcuSync	Do not use	Yes
Mini 3 Pro	DJI	€€€	2024	OcuSync	Do not use	Yes

the 5 GHz frequency band, and has more application options.

The remaining four UAVs are much higher in price. These drones have distance sensors to provide a high degree of security for the user and take-off mechanisms when there's a GNSS signal and automatic preflight modes. The Hubson Zino Mini Pro and Autel Evo Nano+ are similar drones as they use a cable connection between the remote controller and the mobile device, so it's only possible to watch the drone's video transmission through the mobile application, and it only works with a cable connection. The Mini 3 and Mini 3 Pro UAVs diverge from the others UAVs by not using a mobile device for control or video transmission. Instead, these drones come equipped with remote controllers that incorporate built-in displays, enhancing user engagement.

In representing the results of the information gathering and exploitation phases, the names of the UAVs will not be mentioned to not attribute potential vulnerabilities to a specific brand, which is not the objective. Thus, the following designations will be used: UAV A, UAV B, UAV C, UAV D, UAV E, UAV F, UAV G, and UAV H.

All tests were conducted on drones using the Wi-Fi protocol, achievable only by connecting the UAV to a mobile device via Wi-Fi. Using the remote controller was not feasible because it operated on a protocol that either wasn't Wi-Fi or was a modified version created by the manufacturer.

The cyber-attacks that will be presented in the exploitation phase were executed in the Army Technological Experimentation (ARTEX 24) exercise organized by the Portuguese Army. The ARTEX 24 is an exercise with several phases that consist of testing systems to promote technological advancement. This exercise has allowed various conditions to execute cyber-attacks on UAVs as outlined in the exploitation phase, including obtaining authorization for the use of airspace.

4.2 Information Gathering

To perform any cyber-attack, it is essential to understand how the drone's system works and to obtain as much information as possible from it. Various information gathering tests were carried out, such as

monitoring communications (Subsection 4.2.1) and port scanning (Subsection 4.2.2). All the tests were selected to provide better information for the cyber-attacks carried out in the next phase, Exploitation. It's crucial to understand the organization of communications between the UAV and the mobile device, as well as which ports are used for control and video transmission.

4.2.1 Network Traffic Analysis

To capture the packets received and sent exclusively by the UAV, it was necessary to put the antenna in monitor mode and the following commands and tools.

- `iwconfig`: to see which interface the antenna was connected to.
- `sudo iwlist <interface> scan`: consists of scanning the Wi-Fi networks and observing various characteristics illustrated in Figure 4.1, mainly the MAC address, channel and frequency.

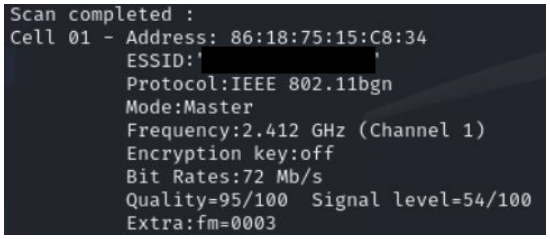


Figure 4.1: Example of a UAV Wi-Fi network found by the command `sudo iwlist <interface> scan`.

- `sudo airmon-ng check kill`: shows and immediately stops any processes that might interfere with the aircrack-ng tools.
- `sudo airmon-ng start <interface>`: used to put the antenna in monitor mode.
- `sudo airodump-ng --channel <channel> --bssid <bssid> --write <file> <interface>` : For capturing/monitoring packets on a network. Some filters were used, such as the channel to be listened to, the MAC address, and the file name to save the packets.

Through Wireshark, packets were analyzed in detail to understand how control and video transmission were being performed. Several diagrams were drawn to demonstrate the analysis of the UAV packets visually. The diagrams were made with a few criteria in place: only the ports used by the UAV were identified because the mobile device ports are constantly changing; the identification of the number of bytes in the payload is placed (e.g., TCP: 10 bytes) when there is a pattern; the value of the payload is identified when it always the same; and finally, the relevant interactions are identified.

- **UAV A:** The port 52612 is thought to be used for video transmission, as the payload transmitted is always variable. In port 8800, the same payload is always sent to the mobile device from another IP address of the UAV, which could be a confirmation of whether the UAV is receiving data. The port 7099 may be related to the control, by sending commands via a 9-byte payload and receiving a confirmation packet with the payload "4802000000". Additionally, the payload "0101" is repeated periodically to possibly keep the channel active. On the other hand, from the packets received and sent in port 7070, it was impossible to conclude what this port was used for.

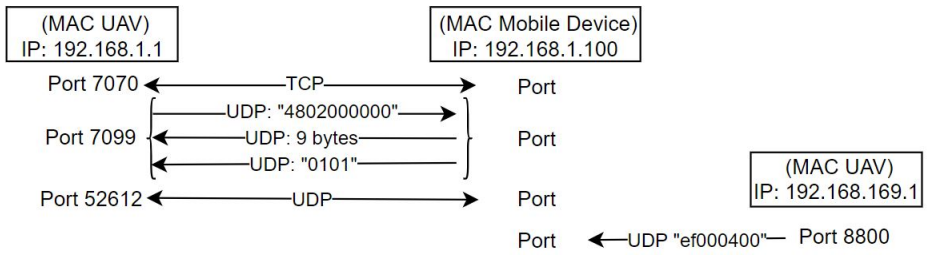


Figure 4.2: UAV A Communications Diagram.

- **UAV B:** Port 1234 is dedicated to sending packets with consistently variable payloads, likely for video transmission. Port 8080 only receives packets with 4, 6, 88, 124, and 156 bytes, which may correspond to different flight commands or UAV functions. Port 18881 is not fixed and is transmitted TCP SYN packets related to a 3-way handshake.

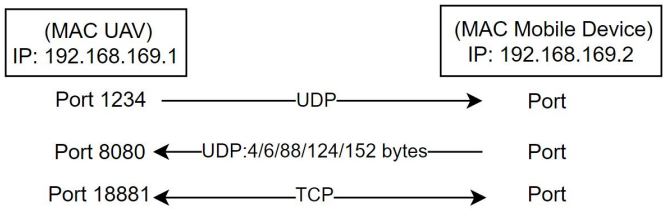


Figure 4.3: UAV B Communications Diagram.

- **UAV C:** On port 19798, 17 and 18 bytes packets are exchanged for the mobile device and 16 and 21 bytes for the UAV. In addition, a packet of 255 bytes is periodically sent to the mobile device, and its effect is unknown. Video transmission takes place on port 554, on the initial packets it is possible to see a link to a Web page, that could be used for the video transmission.

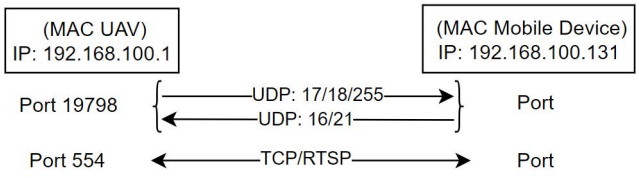


Figure 4.4: UAV C Communications Diagram.

- **UAV D:** Port 8888 is thought to be used for video transmission, as it sends the mobile device several packets ranging from a few bytes to 1460 bytes and receives acknowledgment packets. Meanwhile, port 8080 initially sends two or three packets with 1 byte and 29 bytes, and the remaining packets have 11 bytes, which must be related to sending commands.

There are very different ways of sending commands to the UAV, mainly regarding the number of bytes carried in the packets and the mechanisms used to respond to them. However, there are some doubts about the execution of certain ports, so it was necessary to conduct port scanning to discover the services of the ports mentioned and others that were not captured.

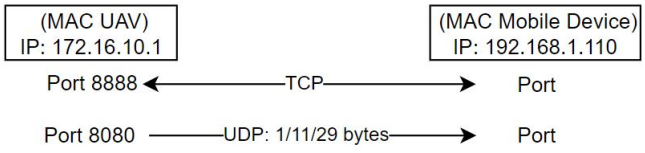


Figure 4.5: UAV D Communications Diagram.

4.2.2 Port Scanning

Several port scanning tests were done with the Nmap tool. For this purpose, a search was made for the different commands that this tool contains, and the following were used: `-Pn` to consider all hosts as online; `-p` to scan a specific port or `-p-` to consider all ports; `-A` to allow detection of the operating system, version and traceroute; `-sU` to scan ports with the UDP protocol; `-sS` to scan ports with the TCP protocol [56].

Table 4.2: The services and ports found in UAVs with the Nmap tool.

UAV	Port/Protocol	State	Service	Figure
A	53/UDP	open	domain	B.1b
	67/UDP	open-filtered	Dynamic Host Configuration Protocol (DHCP)	B.1b
	7070/TCP	open	RTSP	B.1c
	7099/TCP	closed	lazy-ptop	B.1d
	5007/TCP	open	wsm-server-ssl	B.1a
	5555/TCP	filtered	freeciv	B.1e
	80/TCP	open	HTTP	B.1e
	2210/TCP	filtered	noaaport	B.1a
	2459/TCP	filtered	community	B.1a
	4772/TCP	filtered	unknown	B.1a
B	53/UDP	open	domain	B.1b
	67/UDP	open-filtered	DHCP	B.1b
	1234/UDP	open-filtered	search-agent	B.2a
	1234/TCP	closed	hotline	B.2c
	5228/TCP	closed	hpvroom	B.2b
	8800/TCP	closed	sunwebadmin	B.2d
C	1720/TCP	open	h323q931	B.3
D	23/TCP	open	telnet	B.4c
	53/TCP	filtered	domain	B.4a
	8080/TCP	filtered	http-proxy	B.4b
	8888/TCP	open	sun-answerbook	B.4c

Table 4.2 shows all the results obtained from the Nmap tests on the UAVs under study, identifying the port, service, and state. Each test can be viewed in the corresponding figure in appendix B. A

significant difference can be seen in the number of ports found on the UAVs. Despite this, what matters is the open ports found and the service being executed, as some vulnerabilities may be found.

In UAV A, where most ports were found, some of which did not appear in the monitored traffic, such as ports 5007 and 5555. However, there was some doubt about the purpose of port 7070, which could be concluded from the service it performs. Port 7070 has the Real Time Streaming Protocol (RTSP) service, which means it controls video transmission but does not send video packets, done by port 52612. A search was made of the services found on the UAVs, but almost none provided any helpful information for better execution of any cyber-attack. The only exception is UAV D, which has an open telnet service, which consists of a documented vulnerability, CVE-2024-6422, which has a critical score by CVSS and also reported in subsection 2.3.6.

4.3 Exploitation

This section will present all the cyber-attacks performed, the tools used, and their commands. According to the objectives of this thesis, the cyber-attacks performed were two types of DoS, the deauthentication and Flooding attacks, to intercept or interfere with communications. Lastly, a replay attack was executed to gain control of the UAV.

As noted in subsection 4.2.2, a port with an open telnet service was found on UAV D. Therefore, an attempt was made to enter in the UAV's system, which was successful, as can be seen in Figure 4.6. After establishing the connection, it was possible to introduce some operating system commands and conclude that the UAV's system was very similar to Linux. However, the producer made some changes because not all the commands worked. With some research and command attempts, it would be possible to find out more about the UAV D.

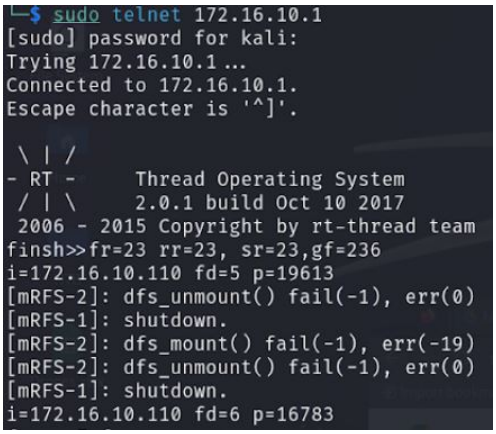


Figure 4.6: Access to the UAV D system via the telnet service.

4.3.1 DoS Deauthentication Attack

The aireplay-ng subtool of aircrack-ng was used to perform this attack. The following command was used: `aireplay-ng -0 <number packets> -a <MAC> wlan`. The value `-0` corresponds to the option

for the attack in the tool, then the number of deauthentication packets is inserted, and finally, the MAC address of the target. This last topic was only realized with the UAV's MAC address, so all connected devices were unauthenticated. However, it was also possible to make specifications with the MAC addresses of the UAV and the mobile device to only realize this attack between two MAC addresses.

Figure 4.7 shows an example of the attack explained above, with a total of ten deauthentication packets sent and the MAC address of one of the drones.

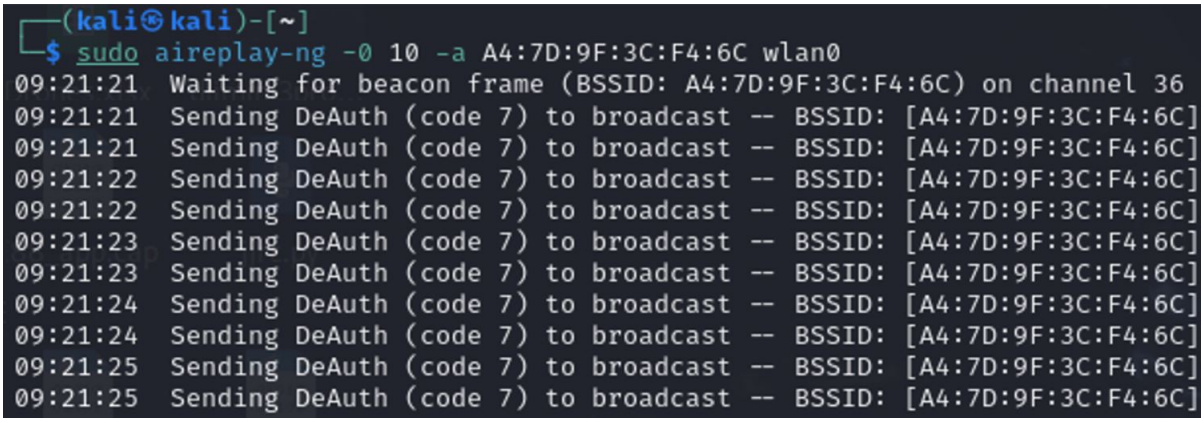


Figure 4.7: Example of a deauthentication attack.

The attack succeeded on all the UAVs used, but not all of them behaved in the same way, the only UAVs having the same behavior were UAVs A, B, and D. When the attack was launched, the video transmission stopped after a few seconds, and it was impossible to control it. This resulted in the UAV losing control instantly and crashing if it was flying. If the user wanted to reconnect with the UAV, it wasn't possible until the drone crashed and the UAV's Wi-Fi network reappeared on the mobile device. On the other hand, UAV C connection was lost in a very similar way, but after losing the signal, the drone remained stable in the air. Then made an emergency landing, automatically stopping the propellers and waiting for a new connection. This emergency landing mechanism provides excellent security for the drone and, above all, for people and buildings nearby.

Table 4.3: Results of the DoS deauthentication attack on the UAVs under study

UAV	Result	Observation
A	Successful	User lost connection with UAV immediately
B	Successful	User lost connection with UAV immediately
C	Successful	User lost connection with UAV immediately but made a safe landing
D	Successful	User lost connection with UAV immediately

During this attack, all communications were monitored, using the procedure explained in Subsection 4.2.1, to observe the packets sent initially after a loss of connection and the re-establishment of a new connection. The authentication packet is shown in Figure 4.10, which says it is an Open System. This packet was observed in all UAVs. This means that no UAV has an authentication mechanism, not even with the application used on the mobile device.

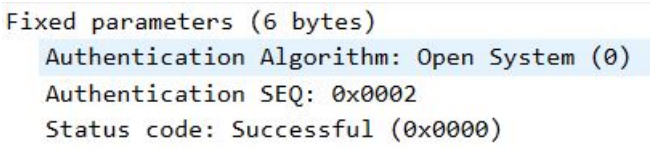


Figure 4.8: The payload of the authentication package

In this type of DoS attack, the only tool factor influencing the attack is the number of deauthentication packets sent. Therefore, various tests were carried out on the different UAVs with several numbers of authentication packets, but the number was irrelevant because the attack succeeded with just one packet.

4.3.2 DoS Flooding Attack

A method to assess the robustness of a drone involves overloading its system to observe and analyze its behavior. So the DoS Flooding attack was performed with the following tool: `sudo hping3 -V <options> <mode> -p <port> <IP address> -I <interface>`. The `-V` stands for verbose mode, which provides the attacker with the largest number of results at the attack level, for example, the number of packets sent and received by the target system. The `<options>` field is related to the operating mode of the number of packets sent. In this attack, –flood mode is used, meaning the largest number of packets is sent. However, other modes have been tested in order to compare the results more accurately. The `<mode>` option refers to the type of protocol of the packet sent, using the default mode, TCP mode, and the value `-2`, UDP mode. The remaining fields are `-p`, to specify the port, `<IP address>`, to enter the UAV's IP address, and finally `-I <interface>`, to use the interface used by the antenna.

Table 4.4 shows DoS Flooding attacks on UAVs using different modes of operation related to the number of packets sent per second, observing the effect on control and video transmission. The attack was also made on each UAV at the different ports found, however, the result was the same, which is why it is not detailed in the table.

Table 4.4: Results of the DoS Flooding Attack on the UAVs under study

UAV		**Number of packets sent in the DoS Attack**			
		–fast (10 packets/s)	**75 packets/s**	**–faster (100 packets/s)**	**–flood**
A	Control	✗	✗	✗	✓
	Video	✗	✗	✗	delay
B	Control	✗	✗	✗	delay
	Video	✗	✗	✗	delay
C	Control	✗	✗	✗	✗
	Video	✗	✗	✗	✗
D	Control	✗	delay	✓	✓
	Video	✗	delay	delay	✓

The symbol ✓ represents the attack's success. If it only caused interference in communications, the word delay was added, and the symbol ✗ was used if the attack was unsuccessful.

Some communications interference was detected on UAV B, such as a delay in processing control packets and video transmission. A similar result was seen in UAV A, where there was some interference in the video transmission, but control was completely lost a few seconds after the attack was launched. On UAV D, the DoS flooding attack was a success but also a success for lower packet number sending modes. In the mode of 75 packets per second, some communication interference was observed, and in `--faster` mode, the control of the UAV was lost.

It's possible to conclude that UAV D has a weaker system than other UAVs in the face of these overload attacks. The delay identified in UAVs A and B may introduce some difficulty in controlling the drone, but it doesn't make it an issue. Finally, UAV C is immune to this type of DoS attack.

4.3.3 Replay Attack

One way to gain complete control of the UAV is to use the flight commands captured in the information gathering phase, which consists of the payload of various analyzed packets. Therefore, it was very important to carry out a complete communications analysis and port scanning to know with as much certainty as possible which channel was being used for control. To perform this attack, a python code, shown in Figure 4.9, was used to send packets with a specific payload.

The code presented can be divided into three stages: declaring variables, building the packet, and send the packets.

- The variables are the IP and MAC addresses captured from the mobile device and the UAV, the port, the protocol used, the interface, and the list of commands.
- The function builds the packet with all the variables shown. However, a similar function was made without the source and destination MAC address, to determine whether the UAV system has any mechanisms for checking the MAC address or just the IP address.
- The packets are sent in two cycles, one that sends each packet three times and another to send all the commands in the list.

The commands presented were chosen from the packets captured after the deauthentication attack to observe the initial commands sent to the drone, as there may be commands that are only sent once. The quantity of commands required for UAVs A, B, C, and D differed, reflecting their use in various operational phases. For instance, a UAV might use a solitary command for takeoff or employ multiple commands sequentially to prepare for takeoff, activate the propellers, and ultimately take off.

This attack doesn't demonstrate total control of a UAV, but it does show that it's possible to do it. In other words, it was demonstrated that it is possible to send commands to the drone and control it, but total control was not realized because a very in-depth study of each drone's payload had to be made.

Table 4.5 show the results of this attack in different situations. The letters PC were used to refer to the attacker's computer, where the code is running.

```python
from scapy.all import IP, UDP, TCP, Ether, sendp # type: ignore
from time import sleep


DEST_IP =  '192.168.100.1'      #destination IP adress
DEST_PORT = 19798               #destination port
DEST_MAC = 'a4:7d:9f:3c:f4:6c'  #destination MAC adress

SRC_IP = '192.168.100.192'      #source IP adress
SRC_MAC = 'aa:68:ac:50:36:d6'   #source MAC adress

protocol = 'UDP'                #protocol used
iface = 'wlan0'                 #interface


commands = [                    #list with the payloads
    bytes.fromhex('4800041168010d8080808020180000000000000034'),
    bytes.fromhex('4800040c680b0800000000000000000003'),
    bytes.fromhex('4800041168010d8080808020180400000000000030'),
]
#function to make the packet
def send_spoofed_packet(src_ip, src_mac, dst_ip, dst_mac, dst_port, payload, iface, protocol):
    ether = Ether(src=src_mac, dst=dst_mac)
    ip = IP(src=src_ip, dst=dst_ip)
    if protocol.upper() == 'UDP':
        transport = UDP(dport=dst_port)
    elif protocol.upper() == 'TCP':
        transport = TCP(dport=dst_port)
    packet = ether / ip / transport / payload
    sendp(packet, iface=iface)

#for cicle to send 3 packets for each command in the order presented
for n in range(len(commands)):
    for _ in range(3):
        send_spoofed_packet(SRC_IP, SRC_MAC, DEST_IP, DEST_MAC, DEST_PORT, commands[n], iface, protocol)
        sleep(0.05)
```

Figure 4.9: Python code used for the Replay Attack

The first situation consists of connecting the PC to the UAV only, to observe if the packets can be sent and the UAV accepts them. This testing option succeeded for all UAVs, and is not necessary to use the IP and MAC addresses of the mobile device.

The second situation tested involved the UAV being initially connected to the mobile device and then the PC establish the connection. This hypothesis was impossible to implement on UAV A because the drone only allowed one device to connect to it. In other words, if the drone were already connected to the mobile device, it would be impossible for another device to send commands and join the drone's Wi-Fi network. However, this was not the case in UAVs B, C, and D, where it was already possible to send commands that overlapped those sent by the mobile device. The exception is that on UAV C and D, it was necessary to use the MAC address in the function to send the commands, or the commands were rejected. However, if the MAC address differs from the mobile device MAC address, the first commands are accepted, with subsequent commands being discarded. This occurs because UAVs have a MAC address verification mechanism, but it is only applied after executing the first set of commands sent. This test option was used to check whether it was possible to send commands after an established connection. However, these overlapped commands do not provide exclusive drone control.

The last test option was supported by a deauthentication attack. On UAV A, as only one device can

Table 4.5: Replay Attack results with the different options used.

UAV	Replay Attack testing options		
	Only the PC connected	**PC and mobile device connected**	**Connected PC and a deauthentication attack**
A	✓	Impossible	✓(First the attack)
B	✓	✓	✓(Continuous attack)
C	✓	✓(Only with MAC address)	✓(Continuous attack)
D	✓	✓(Only with MAC address)	✓(Continuous attack)

be connected, the deauthentication attack was performed first, and then the code was started, making it impossible for the mobile device to connect again. On UAVs B, C, and D, it was necessary to perform the deauthentication attack continuously, meaning always sending deauthentication packets aimed at breaking the connection between the mobile device and the UAV, so as not to interfere with the packets sent by the PC, since was possible to connect more than one device to the UAV.

4.3.4 Jamming

The results of the jamming attack were conducted by a working group at ARTEX 2024, which performed an investigation into this cyber-attack. The equipment used was a computer, an amplifier, an antenna and an SDR. The results are shown in Table 4.6, where it was observed that UAV F is resistant to this attack due to a bandwidth hopping mechanism. Other UAVs completely lost control, remaining in the air until the attack was interrupted and the user established control again.

Table 4.6: Results of the Jamming attack on the UAVs under study.

UAV	Result	Observation
E	Successful	Lost control during the attack
F	Unsuccessful	Jamming Resistant
G	Successful	Lost control during the attack
H	Successful	Lost control during the attack

4.4 Experimental D3S Results

Following the information gathering and exploitation phases, all the results obtained from each drone were applied to the D3S method. Also, this phase of obtaining the D3S score for each UAV was divided into theoretical and experimental scores.

The theoretical scores were calculated with the information gathered from the internet and the use of the drone, which means that no cyber-attacks were performed. In contrast, the experimental scores are based on the results obtained in the information gathering and exploitation phases.

Table 4.7 shows the calculated scores of the UAVs under study. The metrics chosen to evaluate the experimental scores are detailed extensively in Tables 4.8 and 4.9.

Table 4.7: UAV D3S scores with and without experimental data

UAV	Theoretical Scores	Experimental Scores
A	1.8	1.3
B	1.8	1.9
C	1.8	2.4
D	1.8	0.9
E	4.4	4.5
F	3.8	4.3
G	3.8	4.0
H	4.4	4.5

The theoretical values show that there are different groups of D3S scores. UAVs A, B, C, and D share the same theoretical score due to similar communication characteristics and protocols. However, when the experimental scores are compared, this is no longer the case, revealing variations in security performance. The other group are the UAVs E, F, G, and H, which have higher D3S scores,indicating a greater level of security.

An important feature to keep in mind is the price of the drones, which may or may not be directly linked to the security of the UAV. A comparison of the D3S scores with UAV prices was made, as shown in Figure 4.10. The groups were once again represented, and it can be seen that as the price increases, the value of the D3S also increases.

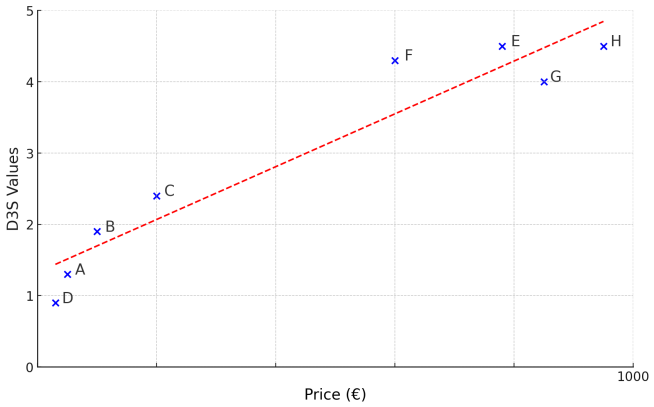


Figure 4.10: Graph of the price versus experimental D3S scores

Table 4.8: First part of the metrics used to calculate the UAV security scores with D3S.

Drone Security Scoring System			UAV A	UAV B	UAV C	UAV D
Characteristics		**Weight**	Nano	Nano	Nano	Nano
		Wing and Rotor	Quadcopter	Quadcopter	Quadcopter	Quadcopter
		Altitude and Range	Hand Held	Hand Held	Hand Held	Hand Held
		Application	Personal	Personal	Personal	Personal
Communications	**Control**	**Communication Protocol for Remote Controller**	Proprietary	Proprietary	Proprietary	Proprietary
		Communication Protocol for Mobile Device	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)
	Video Transmission	**Communication Protocol for Remote Controller**	No Video Transmission	No Video Transmission	No Video Transmission	No Video Transmission
		Communication Protocol for Mobile Device	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)
Software		**Open Ports**	4 Open Ports	1 Open Port	1 Open Port	2 Open Ports
		Vulnerabilities (CVE)	Not found	Not found	Not found	Know
cyber-attacks		**Jamming**	Not tested	Not tested	Not tested	Not tested
		Flooding	Lost full control	Low communication interference	Immune	Lost full control
		Deauthentication	Lost connection	Lost connection	Safe landing mechanism	Lost connection
		Replay Attack	Take full control	Take full control	Take full control	Take full control
Final Score			1.3	1.9	2.4	0.9

Table 4.9: Second part of the metrics used to calculate the UAV security scores with D3S.

Drone Security Scoring System			UAV E	UAV F	UAV G	UAV H
Characteristics		**Weight**	Nano	Nano	Nano	Nano
		Wing and Rotor	Quadcopter	Quadcopter	Quadcopter	Quadcopter
		Altitude and Range	Hand Held	Hand Held	Hand Held	Hand Held
		Application	Personal	Personal	Personal	Personal
Communications	**Control**	**Communication Protocol for Remote Controller**	Ocusync	Proprietary	Proprietary	Ocusync
		Communication Protocol for Mobile Device	No control	Cable	Cable	No control
	Video Transmission	**Communication Protocol for Remote Controller**	Ocusync	No Video Transmission	No Video Transmission	Ocusync
		Communication Protocol for Mobile Device	No Video Transmission	Cable	Cable	No Video Transmission
Software		**Open Ports**	Not Applicable	Not Applicable	Not Applicable	Not Applicable
		Vulnerabilities (CVE)	Not found	Not found	Not found	Not found
cyber-attacks		**Jamming**	Lost control during the attack	Jamming Resistant	Lost control during the attack	Lost control during the attack
		Flooding	Not Applicable	Not Applicable	Not Applicable	Not Applicable
		Deauthentication	Not Applicable	Not Applicable	Not Applicable	Not Applicable
		Replay Attack	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Final Score			4.5	4.3	4.0	4.5

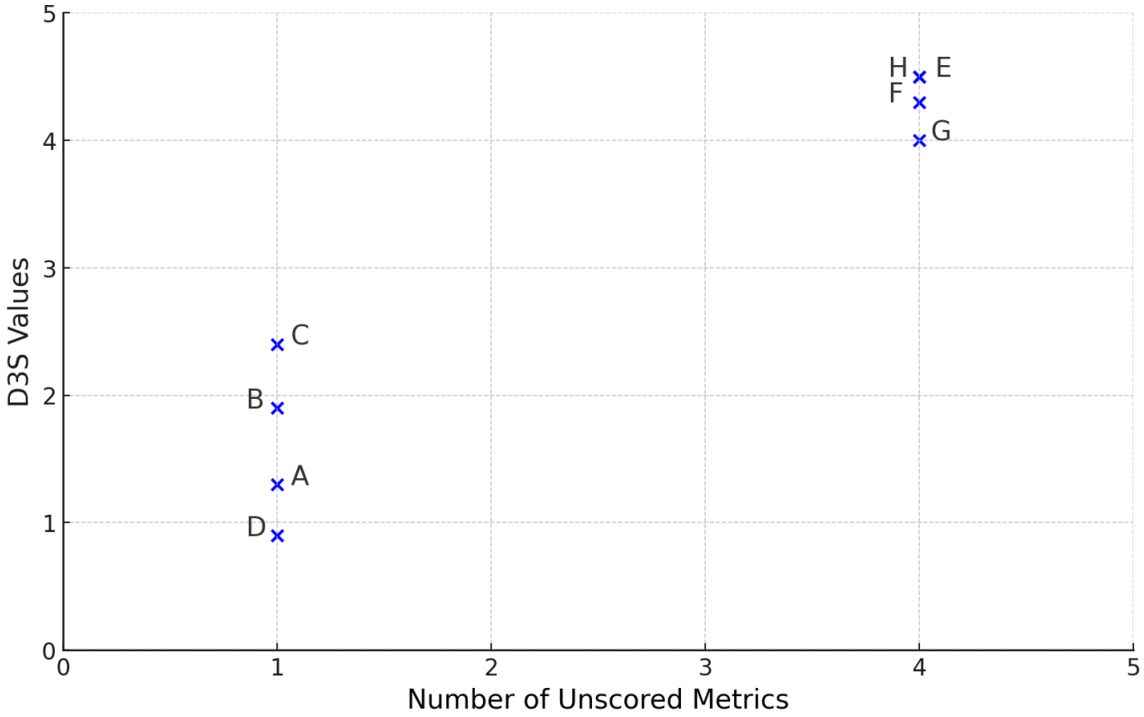


Figure 4.11: Graph of the number of unscored metrics and the experimental D3S scores

An important point to consider is that half of the drones used in D3S have not been subjected to cyber-attacks, which means that there are unscored metrics. This leads to comparing scores that have not all been subjected to the same number of metrics. To observe the unscored metrics in each D3S classification obtained, the following graph was made (Figure 4.11).

All these types of analyses are essential to verify the veracity of the scores calculated. One of the reasons for this is that drones don't use the same communications protocols with the remote controller or the mobile device, which means that some cyber-attacks can't be performed. This occurred in the group of UAVs with the highest D3S scores and the highest number of unscored metrics since the only cyber-attack executed was jamming. This does not mean that the scores obtained do not accurately represent the reality of these UAVs security. The use of communication protocols with higher security ratings, coupled with the inability to conduct cyber-attacks on the Wi-Fi communications of these UAVs, which supports the validity of the results.

4.5 Summary

The results of this chapter, which are summarised in Table 4.10, have made it possible to extract the following information. Regarding open ports, it should be mentioned that UAV D had an open port with the telnet service, which allowed unauthorised access to the UAV's system. The DoS deauthentication attack was successfully performed, and it was observed that UAV C had an emergency landing mechanism when the drone lost connection. This attack was possible since the drones used an open system, without the use of pairing mechanisms. On the other hand, the DoS Flooding attack was only

unsuccessful for UAV C. It is directly related to the system's ability to process and reject a large number of packets without overloading the system. Regarding the replay attack, it was possible to gain control of the four drones. To prevent the user from interfering with the control obtained, a deauthentication attack was carried out together. Except for UAV A, which only needed to be deauthenticated once because the UAV only allowed a single connection, the others UAVs required a continuous deauthentication attack.

The classifications obtained by D3S reflect the security performance of the drones under study, as can be seen. It can be noted that as the classification increases, the drone becomes progressively less vulnerable to cyber-attacks and has better security mechanisms.

Table 4.10: Summary of all the results obtained.

UAV	Open Ports	Control Communications Analyses	Deauthentication Attack	Flooding Attack	Replay Attack	Jamming	D3S score
A	4	9 bytes packets	Successful	Successful	Successful (First the Deauthentication)	Not realised	1.3
B	1	4/6/88/124/152 bytes packets	Successful	Successful (only delay observed)	Successful (Continuous Deauthentication)	Not realised	1.9
C	1	16/21 bytes packets	Successful (safe mechanism)	Unsuccessful	Successful (Continuous Deauthentication)	Not realised	2.2
D	2	1/11/29 bytes	Successful	Successful	Successful (Continuous Deauthentication)	Not realised	0.9
E	Not Applicable	Not Applicable	Do not use Wi-Fi	Do not use Wi-Fi	Do not use Wi-Fi	Successful	4.5
F	Not Applicable	Not Applicable	Do not use Wi-Fi	Do not use Wi-Fi	Do not use Wi-Fi	Unsuccesfull	4.3
G	Not Applicable	Not Applicable	Do not use Wi-Fi	Do not use Wi-Fi	Do not use Wi-Fi	Successful	4.0
H	Not Applicable	Not Applicable	Do not use Wi-Fi	Do not use Wi-Fi	Do not use Wi-Fi	Successful	4.5

Chapter 5

Conclusions

This thesis was developed to obtain a Master's Degree in Military Electrical Engineering. This paper concerns cybersecurity in drones, an area that is currently very popular due to the widespread use of UAVs. The malicious use of drones can pose significant risks to individuals and structures, potentially threatening overall security. This area of drone security is extremely important, and mechanisms or resources capable of ensuring security in the event of a drone being used incorrectly, and providing security for the drones so that they don't suffer any enemy attacks are necessary. Therefore, a method has been created to provide security scores to guarantee defence levels that can be used for drone defense knowledge.

This work shows that a UAV is not a simple system and that, to assess its degree of security, several in-depth analyses of its component's security are required. The development of Drone Security Scoring System required continuous study and the development of several phases to obtain group divisions, capable of providing the best classification and the correct choice of score for each metric. The division established for this method involved a communication group, a key aspect to be taken into account by existing protocols, and to obtain an in-depth division of a drone, a division was made between control and video transmission. Then a software group, to analyse open ports and existing vulnerabilities in the UAV, because attacks without physical access were prioritised. The cyber-attack group is important for identifying the drone's defence mechanisms and whether or not it is vulnerable to the cyber-attacks mentioned. Finally, the characteristics group consists of an approach to identifying the type of UAV to be analysed by the method through several classifications.

Defining the score was a challenge in the development of this method, especially in the communication protocols, as security aspects are often not made public, and so modulation, bandwidth, and frequency hopping mechanisms and security mechanisms that had been found were used as a selection process. An important aspect of this system is its interoperability with Common Vulnerabilities and Exposures, intending to use existing vulnerability classifications. Another aspect was the choice of metrics to provide all the hypotheses that a user can choose from and the method being easy to interpret and use.

This method was not only based on the analysis of its software and communications protocols but

also on the level of defense against cyber-attacks. To reach the greatest success in the cyber-attacks performed, it was necessary to study the tools used in order to employ all the appropriate options and commands, such as wireshark, nmap, aircrack-ng tools and commands to operate with the antenna. Furthermore, an information gathering phase was performed, which was necessary for the exploitation phase. Although no specific penetration methodology was used, structuring the process into sequential phases facilitated a more efficient workflow and the observation of results.

From the analysis conducted and the results obtained on the UAVs under study, we can conclude that there are major security differences. The deauthentication attack was successfully carried out on the UAVs tested, with Wi-Fi communication being interrupted shortly after the attack was performed. One aspect to highlight in this attack was the defence mechanism of UAV C, which made an emergency landing, unlike the others which continued to operate and ended up crashing due to not receiving flight commands. To assess the drone system's ability to receive countless packets, a flooding attack was carried out with different modes (number of packets sent). Success was observed in UAVs A and D, and a delay in UAV B. On the other hand, UAV C is immune to this attack. Concerning the replay attack, it was noted that regardless of the success obtained, several characteristics had to be taken into account, such as the specific use of the MAC address in the packets sent and the initial or continued performance of the deauthentication attack to prevent the user from interfering with the sending of commands. In the selected drones, it was possible to determine two distinct groups, those using Wi-Fi communications on the mobile device, and those exclusively using the remote controller for control. This provided different degrees of security, as can be seen from the D3S ratings obtained. Another important conclusion is that the price of drones is directly related to the degree of security.

5.1 Achievements

The development of this work has resulted in the implementation of a successful security classification method for UAVs. Capable of evaluating communications protocols, software aspects, and defense mechanisms against cyber-attacks. This method is well designed and implemented as the classification results are consistent with all the vulnerability analyses performed on the drones under study.

A good performance was achieved in the information gathering and exploitation phases. An in-depth analysis of communications and port analysis was performed, which in turn provided successful results in the cyber-attacks. The entire process applied proved to be effective in the cyber-attacks executed. It started with an analysis of the tools and equipment chosen, followed by the information gathering phase, which was vital for carrying out the attacks and understanding how each drone's control and video transmission communications worked. Then there was the exploitation phase, where each attack was implemented, having achieved the objectives of interfering with the drone's communications and system. And also, to reach control of the UAV, while making it impossible for the operator to have control at the same time.

5.2 Future Work

For future work, D3S can be improved in various aspects to create a more complex and extensive method. An improvement that could be made is to increase the number of metrics in the communications and software groups, to achieve a more complete system. On the other hand, more cyber-attacks could be done to obtain more metrics for analyzing security, and in turn new groups of metrics could be created, e.g. at the level of UAV hardware security.

Another improvement that can be made is in the execution of cyber-attacks, so that the attacks are not exclusively directed at the mobile device, but rather at the remote controller. Also, the automatic execution of cyber-attacks can be important, because the time required to perform these attacks is an essential factor.

To achieve a more reliable security classification system, it is essential to validate it with a larger number of UAVs covering a wide range of characteristics, prices, and components.

Bibliography

[1] T. Höglund Gran and E. Mickols. Hacking a Commercial Drone. Master's thesis, Stockholm University, 2020.

[2] D. Kunertova. The war in Ukraine shows the game-changing effect of drones depends on the game. *Bulletin of the Atomic Scientists*, 79(2):95–102, 2023.

[3] E. Hecht. Drones in the Nagorno-Karabakh War: Analyzing the Data. *Military Strategy Magazine*, 7(4):31–37, 2022.

[4] V. Modebadze. The Importance of Drones in Modern Warfare and Armed Conflicts. *KutBilim Sosyal Bilimler ve Sanat Dergisi*, 1(2):89–98, 2021.

[5] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, 11:39, 2020.

[6] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak. Detection, Tracking, and Interdiction for Amateur Drones. *IEEE Communications Magazine*, 56(4):75–81, 2018.

[7] G. Rubbestad and W. Söderqvist. Hacking a Wi-Fi based drone. Master's thesis, Stockholm University, 2021.

[8] Y.-M. Kwon, J. Yu, B.-M. Cho, Y. Eun, and K.-J. Park. Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles. *IEEE Access*, 6:43203–43212, 2018.

[9] O. Westerlund and R. Asif. Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things. In *2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*, pages 1–10. IEEE, 2019.

[10] E. Dahlman and K. Lagrelius. A game of drones: Cyber security in UAVs. Master's thesis, Stockholm University, 2019.

[11] G. Abro, S. Zulkifli, R. Masood, S. Asirvadam, and A. Laouti. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats. *Drones*, 6(10), 2022.

[12] K. AL-Dosari, Z. Hunaiti, and W. Balachandran. Systematic Review on Civilian Drones in Safety and Security Applications. *Drones*, 7(3), 2023.

[13] R. Altawy and A. Youssef. Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. *ACM Transactions on Cyber-Physical Systems*, 1:1–25, 2016.

[14] A. Fatima, T. A. Khan, T. M. Abdellatif, S. Zulfiqar, M. Asif, W. Safi, H. Al Hamadi, and A. H. Al-Kassem. Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat. In *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, pages 1–8. IEEE, 2023.

[15] M. Parveen and M. A. Shaik. Review on Penetration Testing Techniques in Cyber security. In *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, pages 1265–1270. IEEE, 2023.

[16] V. Chamola, P. Kotesh, A. Agarwal, N. Gupta, M. Guizani, et al. A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques. *Ad hoc networks*, 111:102324, 2021.

[17] M. Krichen, W. Y. H. Adoni, A. Mihoub, M. Y. Alzahrani, and T. Nahhal. Security Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures. In *2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, pages 184–189, 2022.

[18] V. U. Castrillo, A. Manco, D. Pascarella, and G. Gigante. A review of counter-UAS technologies for cooperative defensive teams of drones. *Drones*, 6(3):65, 2022.

[19] R. K. Barnhart, D. M. Marshall, and E. Shappee. *Introduction to Unmanned Aircraft Systems*. CRC Press, 2021.

[20] K. Warnakulasooriya and A. Segev. Attacks, Detection, and Prevention on Commercial Drones: A Review. In *2024 International Conference on Image Processing and Robotics (ICIPRoB)*, pages 1–6. IEEE, 2024.

[21] M. P. Stewart and S. T. Martin. Unmanned Aerial Vehicles: Fundamentals, Components, Mechanics, and Regulations. In N. Barrera, editor, *Unmanned Aerial Vehicles*. Nova Science Publishers, Inc., New York, 2021.

[22] E. Ebeid, M. Skriver, and J. Jin. A Survey on Open-Source Flight Control Platforms of Unmanned Aerial Vehicle. In *2017 Euromicro Conference on Digital System Design (DSD)*, pages 396–402, 2017.

[23] Y. Mekdad, A. Aris, L. Babun, A. E. Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac. A survey on security and privacy issues of UAVs. *Computer Networks*, 224:109626, 2023.

[24] M. Y. Arafat, M. A. Habib, and S. Moh. Routing protocols for UAV-aided wireless sensor networks. *Applied Sciences*, 10(12):4077, 2020.

[25] O. Simon and T. Gotthans. A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception. *Electronics*, 11(19), 2022.

[26] A. Halbouni, L.-Y. Ong, and M.-C. Leow. Wireless Security Protocols WPA3: A Systematic Literature Review. *IEEE Access*, pages 112438–112450, 2023.

[27] MAVLink. MAVLink Developer Guide. Technical report, MAVLink, 2024. Available online: `https://mavlink.io/en/`.

[28] DJI. Drone security white paper, version 3.0. Technical report, DJI, 2024. Available online: `https://www.dji.com/pt/trust-center/resource/white-paper`.

[29] Da-Jiang Innovations. DJI Lightbridge Release Notes, May 2014. Available online: `https://www.dji.com/pt/dji-lightbridge`.

[30] FrSky. Advanced Communication Control Elevated Spread Spectrum, 2024. Available online: `https://www.frsky-rc.com/`.

[31] Flysky. Third Gen Automatic Frequency Hopping Digital System, 2024. Available online: `https://https://www.flysky-cn.com/`.

[32] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh. Technical Guide to Information Security Testing and Assessment. Technical Report 115, NIST Special Publication, 2008.

[33] F. Abu-Dabaseh and E. Alshammari. Automated penetration testing: An overview. In *The 4th international conference on natural language computing, Copenhagen, Denmark*, pages 121–129, 2018.

[34] A. Aibekova and V. Selvarajah. Offensive security: Study on penetration testing attacks, methods, and their types. In *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, pages 1–9, 2022.

[35] Open Information System Security Group. *Information Systems Security Assessment Framework (ISSAF)*, 2005. URL `https://untrustednetwork.net/files/issaf0.2.1.pdf`.

[36] Institute for Security and Open Methodologies. *Open Source Security Testing Methodology Manual (OSSTMM)*, 2010. URL `https://www.isecom.org/OSSTMM.3.pdf`.

[37] The PTES Team. The Penetration Testing Execution Standard v2.0, 2023. URL `https://pentest-standard.com/`.

[38] J. Malimban, B. R. Payne, and T. T. Abegaz. Drone Hacking: Applying the Cyber Kill Chain to Hijack Unmanned Aerial Systems. *Quarterly Review of Business Disciplines*, 8:213, 2021.

[39] A. Villalon-Huerta, H. M. Gisbert, and I. Ripoll-Ripoll. SOC Critical Path: A Defensive Kill Chain Model. *IEEE Access*, 10:13570–13581, 2022.

[40] Q. K. A. Mirza, M. Brown, O. Halling, L. Shand, and A. Alam. Ransomware Analysis using Cyber Kill Chain. In *2021 8th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 58–65, 2021.

[41] S. Faily, R. Scandariato, A. Shostack, L. Sion, and D. Ki-Aries. Contextualisation of data flow diagrams for security analysis. In *Graphical Models for Security: 7th International Workshop, GraMSec*, pages 186–197. Springer, 2020.

[42] P. Hamza and A. Qassim. How Secure are Drones?: A security analysis of a drone system. Master's thesis, Stockholm University, 2021.

[43] Microsoft. Threat Modelling, 2023. URL `https://playbook.microsoft.com/code-with-engineering/security/threat-modelling/`.

[44] A. H. A. Kamal, C. C. Y. Yen, G. J. Hui, P. S. Ling, et al. Risk assessment, threat modeling and security testing in SDLC. *arXiv*, 2020. URL `https://arxiv.org/abs/2012.07226`.

[45] A. Shostack. *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[46] B. Oktorianto, M. A. A. Soetomo, and C. Lim. Risk Assessment For Enterprise Application In The Insurance Sector. In *2021 6th International Conference on New Media Studies (CONMEDIA)*, pages 124–128. IEEE, 2021.

[47] Joint Air Power Competence Centre. *A Comprehensive Approach to Countering Unmanned Aircraft Systems*. January 2021. URL `https://www.japcc.org/books/a-comprehensive-approach-to-countering-unmanned-aircraft-systems/`.

[48] H. A. Noman and O. M. Abu-Sharkh. Code injection attacks in wireless-based Internet of Things (IoT): A comprehensive review and practical implementations. *Sensors*, 23(13):6067, 2023.

[49] F. H. S. S. AL-Ghafri and L. Vidhya. Unmanned Aerial Vehicles (UAV) Jammer. In *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2021*, pages 439–453. Springer Singapore, 2022.

[50] H. Fereidouni, O. Fadeitcheva, and M. Zalai. IoT and Man-in-the-Middle Attacks, 2023. URL `https://arxiv.org/abs/2308.02479`.

[51] R. Buckle. Performing Man in the Middle Attacks Within a Wireless Local Area Network. *Authorea*, page 4, 2022.

[52] A. ElShafee and W. El-Shafai. Design and analysis of data link impersonation attack for wired LAN application layer services. *Journal of Ambient Intelligence and Humanized Computing*, 14 (10):13465–13488, 2023.

[53] S. Maji, H. Jain, V. Pandey, and V. A. Siddiqui. White hat security-an overview of penetration testing tools. *Proceedings of the Advancement in Electronics & Communication Engineering*, July 14 2022.

[54] S. Raj and N. K. Walia. A study on metasploit framework: A pen-testing tool. In *2020 International Conference on Computational Performance Evaluation (ComPE)*, pages 296–302, 2020.

[55] Aircrack-ng. Aircrack-ng 1.7, 2023. Available online: `https://www.aircrack-ng.org/`.

[56] OffSec Services Limited. Kali Linux, 2024. Available online: `https://www.kali.org/tools/`.

[57] J. Feng and J. Tornert. Denial-of-Service attacks against the Parrot ANAFI drone. Master's thesis, Stockholm University, 2021.

[58] Netwox, 2007. Available online: `https://ntwox.sourceforge.net/`.

[59] M. Alhamed and M. M. H. Rahman. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences*, 13(12), 2023.

[60] G. de Carvalho Bertoli, L. A. Pereira, and O. Saotome. Classification of denial of service attacks on Wi-Fi-based unmanned aerial vehicle. In *2021 10th Latin-American Symposium on Dependable Computing (LADC)*, pages 1–6. IEEE, 2021.

[61] K. Kadripathi, L. Y. Ragav, K. Shubha, and P. H. Chowdary. De-authentication attacks on rogue UAVs. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, pages 1178–1182. IEEE, 2020.

[62] G. Vasconcelos, R. S. Miani, V. C. Guizilini, and J. R. Souza. Evaluation of dos attacks on commercial wi-fi-based UAVs. *International Journal of Communication Networks and Information Security*, 11(1):212–223, 2019.

[63] K. Intwala, S. Jatav, and K. Kolhe. System to capture WiFi based Drones using IoT. In *2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, pages 1–6. IEEE, 2022.

[64] I. Astaburuaga, A. Lombardi, B. La Torre, C. Hughes, and S. Sengupta. Vulnerability analysis of AR. drone 2.0, an embedded linux system. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0666–0672. IEEE, 2019.

[65] E. F. M. Josephlal and S. Adepu. Vulnerability Analysis of an Automotive Infotainment System's WIFI Capability. In *2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE)*, pages 241–246, 2019.

[66] M. Alhamry and A. Alomary. Exploring Wi-Fi WPA2-PSK protocol weaknesses. In *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*, pages 190–195. IEEE, 2022.

[67] K. C. Patel and A. Patel. Rogue Access Point: The WLAN Threat. In *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pages 943–950. IEEE, 2022.

[68] F. Z. Lidanta, A. Almaarif, and A. Budiyono. Vulnerability analysis of wireless lan networks using penetration testing execution standard: A case study of cafes in palembang. In *2021 International Conference on ICT for Smart Society (ICISS)*, pages 1–5. IEEE, 2021.

[69] N. Pimple, T. Salunke, U. Pawar, and J. Sangoi. Wireless Security — An Approach Towards Secured Wi-Fi Connectivity. In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pages 872–876. IEEE, 2020.

[70] A. Raghuprasad, S. Padmanabhan, M. A. Babu, and P. Binu. Security analysis and prevention of attacks on IoT devices. In *2020 International Conference on Communication and Signal Processing (ICCSP)*, pages 0876–0880. IEEE, 2020.

[71] F. Fikriyadi, R. Ritzkal, and B. A. Prakosa. Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method. *Jurnal Mantik*, 4(3):1658–1662, 2020.

[72] D. N. Astrida, A. R. Saputra, and A. I. Assaufi. Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES). *Sinkron: jurnal dan penelitian teknik informatika*, 6(1):147–154, 2021.

[73] D. Overstreet, H. Wimmer, and R. J. Haddad. Penetration Testing of the Amazon Echo Digital Voice Assistant Using a Denial-of-Service Attack. In *2019 SoutheastCon*, pages 1–6. IEEE, 2019.

[74] P. Biondi, S. Bognanni, and G. Bella. Vulnerability assessment and penetration testing on IP camera. In *2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pages 1–8. IEEE, 2021.

[75] K. C. Patel and A. Patel. Rogue Access Point: The WLAN Threat. In *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pages 943–950. IEEE, 2022.

[76] Y.-H. Lu, S. H.-Y. Hsiao, C.-Y. Li, Y.-C. Hsieh, P.-Y. Chou, Y.-Y. Li, T. Xie, and G.-H. Tu. Insecurity of Operational IMS Call Systems: Vulnerabilities, Attacks, and Countermeasures. *IEEE/ACM Transactions on Networking*, 31(2):800–815, 2022.

[77] M. Dasari. Real time detection of MAC layer DoS attacks in IEEE 802.11 wireless networks. In *2017 14th IEEE annual consumer communications & networking conference (CCNC)*, pages 939–944. IEEE, 2017.

[78] Z. Liu and J. Zhang. Launching low-rate dos attacks with cache-enabled wifi offloading. In *2018 14th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, pages 171–176. IEEE, 2018.

[79] S. Ditton, A. Tekeoglu, K. Bekiroglu, and S. Srinivasan. A proof of concept denial of service attack against bluetooth IoT devices. In *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 1–6. IEEE, 2020.

[80] R. Singh, R. Thakkar, M. Thakkar, U. Rote, S. Patil, and B. Ingle. WiFi Deauth and Cloning using ESP8266. In *2022 5th International Conference on Advances in Science and Technology (ICAST)*, pages 1–5. IEEE, 2022.

[81] N. Hoque, H. Rahbari, and C. Rezendes. Systematically analyzing vulnerabilities in the connection establishment phase of Wi-Fi systems. In *2022 IEEE Conference on Communications and Network Security (CNS)*, pages 64–72. IEEE, 2022.

[82] Y. Kristiyanto and E. Ernastuti. Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test. *CommIT (Communication and Information Technology) Journal*, pages 45–51, 2020.

[83] M. K. Kissi and M. Asante. Penetration testing of IEEE 802.11 encryption protocols using Kali Linux hacking tools. *International Journal of Computer Applications*, 975:8887, 2020.

[84] D. Koutras, P. Dimitrellos, P. Kotzanikolaou, and C. Douligeris. Automated WiFi incident detection attack tool on 802.11 networks. In *2023 IEEE Symposium on Computers and Communications (ISCC)*, pages 464–469. IEEE, 2023.

[85] B. B. M. Bakry, A. R. B. Adenan, and Y. B. M. Yussoff. Security Attack on IoT Related Devices Using Raspberry Pi and Kali Linux. In *2022 International Conference on Computer and Drone Applications (IConDA)*, pages 40–45. IEEE, 2022.

[86] A. Carranza, D. Mayorga, C. DeCusatis, and H. Rahemi. Comparison of Wireless Network Penetration Testing Tools on Desktops and Raspberry Pi Platforms. In *16th LACCEI International Multi-Conference for Engineering, Education and Technology*, pages 1–5, 2018.

[87] S. Syed, F. Khuhawar, K. Arain, T. Kaimkhani, Z. Syed, H. Sheikh, and S. Khan. Case Study: Intranet Penetration Testing of MUET. *Mehran University of Engineering and Technology*, pages 17–19, 2020.

[88] H. Gustafsson and H. Kvist. Cyber Security Demonstrations using Penetration Testing on Wi-Fi Cameras. Master's thesis, Linkoping University, 2022.

[89] G. Karmakar, M. Petty, H. Ahmed, R. Das, and J. Kamruzzaman. Security of Internet of Things Devices: Ethical Hacking a Drone and its Mitigation Strategies. In *2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, pages 1–5. IEEE, Dec. 2022.

[90] P. Shrivastava, M. S. Jamal, and K. Kataoka. EvilScout: Detection and mitigation of evil twin attack in SDN enabled WiFi. *IEEE Transactions on Network and Service Management*, 17(1): 89–102, 2020.

[91] F. Slimeni, T. Delleji, and Z. Chtourou. RF-Based Mini-Drone Detection, Identification & Jamming in No Fly Zones Using Software Defined Radio. In *International Conference on Computational Collective Intelligence*, pages 791–798. Springer, 2022.

[92] Y. Mekdad, A. Acar, A. Aris, A. E. Fergougui, M. Conti, R. Lazzeretti, and S. Uluagac. Exploring Jamming and Hijacking Attacks for Micro Aerial Drones, 2024. URL https://arxiv.org/abs/2403.03858.

[93] J. A. Saputro, E. E. Hartadi, and M. Syahral. Implementation of GPS attacks on DJI phantom 3 standard drone as a security vulnerability test. In *2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE)*, pages 95–100. IEEE, 2020.

[94] A. D. B. A. Rahman, K. A. Ghani, N. H. H. Khamis, et al. Unmanned aerial vehicle (UAV) GPS jamming test by using Software Defined Radio (SDR) platform. In *Journal of Physics: Conference Series*, volume 1793, page 012060. IOP Publishing, 2021.

[95] J. Villain, V. Deniau, C. Gransart, A. Fleury, and E. P. Simon. Characterization of IEEE 802.11 communications and detection of low-power jamming attacks in noncontrolled environment based on a clustering study. *IEEE Systems Journal*, 16(1):683–692, 2021.

[96] J. Liu, Y. He, C. Xiao, J. Han, L. Cheng, and K. Ren. Physical-world attack towards wifi-based behavior recognition. In *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*, pages 400–409, 2022.

[97] V. Sokolov, P. Skladannyi, and A. Platonenko. Jump-Stay Jamming Attack on Wi-Fi Systems. In *2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT)*, pages 1–5. IEEE, 2023.

[98] F. tu Zahra, Y. S. Bostanci, and M. Soyturk. The Consequences of Jamming Attacks on Wireless IoT Networks: Evaluating the Performance Metrics in Noiseless and Noisy Environments. In *2023 31st Signal Processing and Communications Applications Conference (SIU)*, pages 1–4. IEEE, 2023.

[99] Forum of Incident Response and Security Teams. Common Vulnerability Scoring System SIG, 2024. Available online: https://www.first.org/cvss/.

[100] Forum of Incident Response and Security Teams (FIRST). *CVSS v4.0 Specification*, November 2023.

[101] Common Vulnerabilities and Exposures. CVE Program, 2024. Available online:https://www.cve.org/About/Overview.

[102] E. Baray and N. Kumar Ojha. WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique. In *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, pages 23–30, 2021.

Appendix A

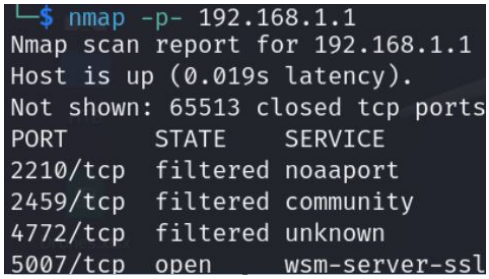
Classification of the DREAD method

Table A.1: Description of each DREAD method classification, adapted from [1]

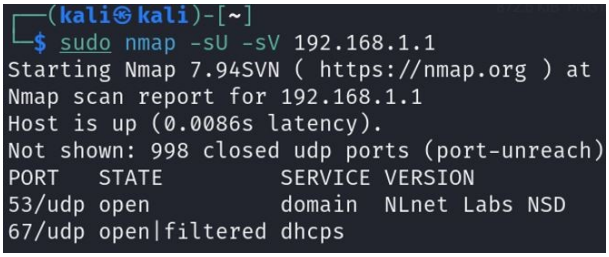
		Classification		
		High (3)	**Medium (2)**	**Low (1)**
D	Damage Potential	The attacker has the highest level of access to the system	Leakage of sensitive information	Leakage of information with a degree of importance
R	Reproducibility	The attack can be replayed at any time	The attack can be reproduced in time intervals	The attack is very difficult to be reproduced again
E	Exploitability	A beginner programmer is able to carry out the attack in a short space of time	An experienced programmer is capable of executing the attack	A very experienced programmer with a deep knowledge is able to carry out the attack
A	Affected Users	All users are affected	Some users are affected	Very few users are affected
D	Discoverability	The vulnerability is easily discovered, and is found in an area of the system that is used by the majority of users	The vulnerability lies in a part that is not frequently used by users	The vulnerability is located in an area of the system that is almost unused

Appendix B

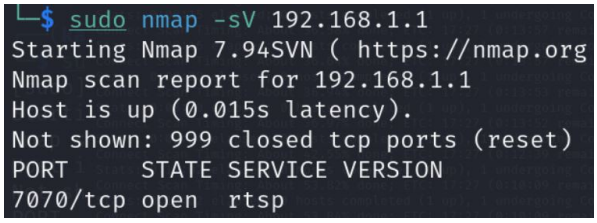
Port Scanning Images



(a) Nmap scan with the -p- command

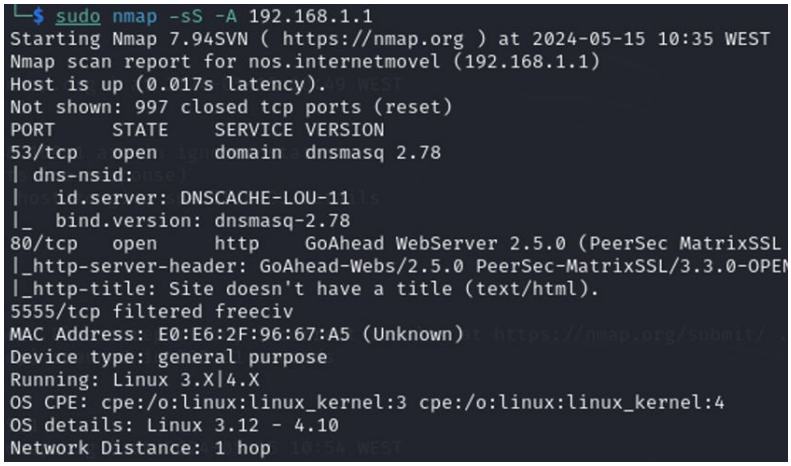


(b) Nmap scan with the -sU and -sV command



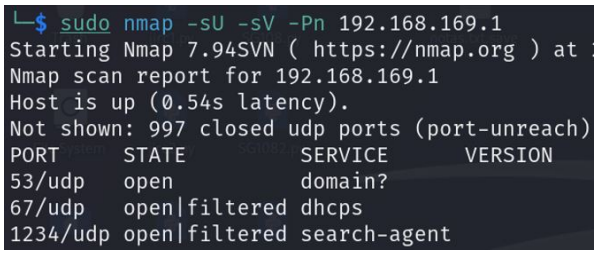
(c) Nmap scan with the -sV command

(d) Nmap scan with the -p command on port 7099

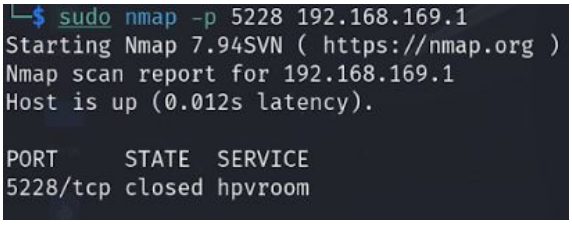


(e) Nmap scan with the -sS -A command

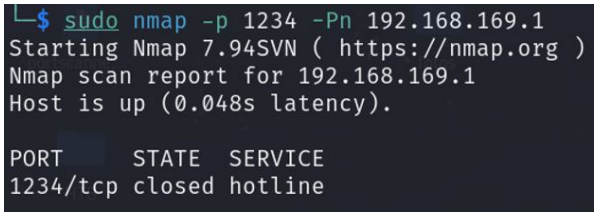
Figure B.1: UAV A port scanning results



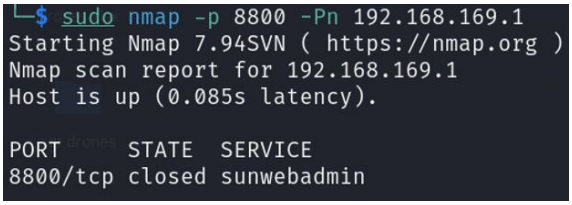
(a) Nmap scan with the -sU and -sV command



(b) Nmap scan with the -p command on port 5228



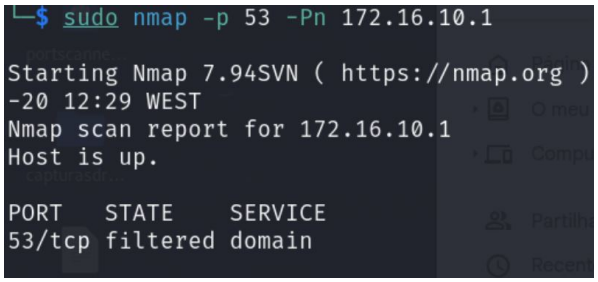
(c) Nmap scan with the -p command on port 1234



(d) Nmap scan with the -p command on port 8800

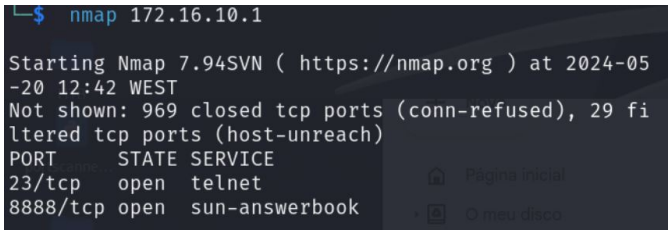
Figure B.2: UAV B port scanning results

Figure B.3: UAV C port scanning results



(a) Nmap scan with the -p command on port 53

(b) Nmap scan with the -p command on port 8080



(c) Nmap scan without any command

Figure B.4: UAV D port scanning results