Versatile Exploitation Techniques: Drone Hacking and Jamming with Raspberry-Pi and Wi-Fi Pineapple

J Caroline El Fiorenza, Revanth Kumar Lokku, Kirthika Sivakumar, M Reene Stephanie

Abstract—The utilization of Internet-of-Things (IoT) innovation is developing exponentially as more shoppers and organizations recognize the benefits offered by the savvy and shrewd gadgets. The major purpose of this paper arose due to the reason that since drone innovation is a quickly rising segment inside the IoT and the danger of hacking couldn't just purpose an information break, it could likewise represent a noteworthy hazard to the open well-being. On account of their flexible applications and access to ongoing data, commercial drones are used across a wide variety of smart city applications. However, with many IoT devices, security is frequently an untimely idea, leaving numerous drones helpless against programmers. What is being done in this paper is that this paper examines the present condition of automation security and exhibits a lot of Wi-Fi empowered drone vulnerabilities. Five distinct sorts of assaults, together with the capability of robotization of assaults, were identified and connected to two unique kinds of scientifically accessible drones. For the execution, the methodologies and techniques used are the correspondence connections that are researched for the assaults, for example Disavowal of Service, De-authentication Methods, Man-in-the-Middle, Unauthorized Root Access and Packet Spoofing. Ultimately, the unapproved root access was computerized using a Raspberry-Pi 3 and Wi-Fi Pineapple. Besides, the strategy for each assault is laid out, also the test part diagrams the findings and procedures of the assaults. The Basic Intrusion Detection Systems and Intrusion Protection System so as to avoid the UAV (unmanned aerial vehicles) from entering the confined airspace are discussed. At long last, the paper tends to the present condition of automaton security, the executives, control, flexibility, protection concerns by using GPS spoofing as a method to secure the target which is the drone from being vulnerable to the attacker.

Keywords—Cybersecurity, Hacking, GPS spoofing, Raspberry-Pi, Wi-Fi Pineapple

I. INTRODUCTION

Unmanned aerial vehicles (UAVs), when an apparatus utilized distinctly by the military, is currently ending up progressively well-known with the business and non-business showcase.

Revised Manuscript Received on November 05, 2019.

J Caroline El Fiorenza, Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

Revanth Kumar Lokku, UG Scholar, B Tech, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

Kirthika Sivakumar, UG Scholar, B Tech, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

M Reene Stephanie, UG Scholar, B Tech, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

Unmanned aerial (UAVs) vehicles, or drones, are an unmanned aerial vehicle that has no pilot ready, and are explored by either a remote control, or by ready PCs. Drones are normally partitioned into three unique sorts of classes: (a) recreational, (b) business and (c) military drones.

The expansion of recreational drone usage has prompted discourses in regards to the security of the unregulated drone usage, and how to maintain a strategic distance from specialist abusing airspace rules. At a similar time as buyers utilized drones as specialists, organizations have progressively investigated utilizing rambles for business use.

In 2016 they uncovered that they were trying a conveyance administration where clients could get little bundles up to five pounds in weight with-in 30 minutes or less, using rambles. The expanded use of drones implies that they will end up being a progressively regular objective for malevolent aggressors. In 2017, McAfee Labs referenced "Drone Hacking" as one of the greatest forthcoming dangers in their 2017 Threats Predictions Report. In situations where drones are delivering products, the automations need to not just have dependable well-being techniques for its activities; it additionally needs solid framework security estimations. Besides, a drone equipped for putting away pictures, recordings, GPS areas and different sorts of private information is an ideal objective for various kinds of programmers. In a world, where the use of reconnaissance drones is winding up increasingly likely, it is extraordinarily essential to stay away from delicate information falling in an inappropriate hand.

Drone security is a field that is genuinely new, and is something that is becoming increasingly more popular as drones become more publicly available. As with any other Internet-of-Things (IoT) framework or savvy city application, rambles are helpless somehow, and as a rule are anything but difficult to access.

So as to control UAV's interruption into any private airspace or Restricted airspace as indicated by Global Drone Policies, all security estimated have been executed till date viably are not any more effective tomorrow on account of the developing tech for stealthy methods of different offending demonstrating in Drones. So as to annihilate any sort of interruptions and the trading off of characterized data or reconnaissance through the limited territories like Area 51 for instance that may prompt numerous tricks, can be confined by flexible hacking techniques and sticking of transmission mechanisms of the drones may confine them removing arranged data which triggers

risk to the entire security and honesty of the safeguard arrangement of any nation. To deal with Defense frameworks without getting any characterized data to be undermined from the automatons, we can do GPS mocking utilizing Kali Linux conveyance devices, sticking sign with the assistance of Wi-Fi pineapple and Raspberry-Pi. With the goal that we can be able to make a LOC for any sort of UAV's into limited airspace.

II. LITERATURE SURVEY

[1]A penetration test was taken in the process of ethical hacking using raspberry pi. The degrees of penetrating are mostly 4 parts. When they are joined, they develop a powerful activity to test the security level of a system. The primary thought is to adopt a hacker's strategy and think like one, with respect to hackers generally utilize similar strides to break systems. The merit of this penetration system is that, to keep the penetration testing focused and advancing, also utilizing the output results from every level to use in ensuing steps as it is important in an organized approach. Another merit is that, by using raspberry pi, there is combination of various techniques and technologies. The demerits include gaining unauthorized access to various devices also, it could lead to many web attacks and Wi-Fi attacks.

[2] Collaborative cognition technology was used for detecting cyber security threats at an early stage. The merit is definitely reducing the cognitive load on the analyst. The demerit is that, regardless of the presence of a few tools in the domain of security, attack detection is as yet a difficult assignment. Frequently, assailants adjust to more up to date security frameworks and find new ways past them. This area depicts a few difficulties in identifying cyber security attacks. Introductory plan of the Modbus convention [3] did not put a high need on security; thus, Modbus based control frameworks are vulnerable to traditional data security dangers. Modbus neither scrambles traffic, nor checks the honesty of messages or confirms ace and slave gadgets. The merits would be that the Modbus control system is presently associated through the Internet to corporate systems which enables remote access to the control system and in this manner to the control gadgets. The demerits of Modbus can be misused by programmers to make destruction on control frameworks as assaults, for example, Man-in-the-middle attack, Denial-of-service attack, replay attack and unapproved order execution assaults.

In Ethical Hacking and network defense [4], the technique used is vulnerability scanning and hands on ethical hacking practice. Here, the merits are the defense provided for various networks and the hands-on experience in this field. The demerits include the limited accessibility to various techniques and the difficulty involved in troubleshooting which hinders the overall process.

The innovation behind independent vehicles is one of the quickest developing ventures in America. They are disturbing the car business as a few organizations, for example, Google, Tesla, BMW, Toyota, and Mercedes are building up their own independent vehicles. The security of these frameworks could influence the lives of millions sooner rather than later and could turn into a moral problem [5]. The merits would be the prevention of man in the middle attacks and prevention of GPS spoofing attacks. The demerits are requirement of more layers and GPS chips drain power. [7] In the current scenario, drone security is something that is quite newly introduced and is becoming increasingly popular as drones are nowadays being more publicly available. On the other hand, smart technologies like IoT being on the rise, makes the drones more vulnerable and gaining access easier. To avoid this, drone hacking is done by using various tools and other hardware's.

III. MODULE DESCRIPTION

The architecture diagram for the proposed system to hack a drone by using GPS spoofing is given below:

Fig. 1 Architecture diagram

A. Identification of UAV

At first, when an unnamed aerial vehicle (UAV) or a drone enters a specific line of control, the drone's action depends upon the line of control which can be broadly categorized into two categories. The first scenario would be the drone entering into the restricted airspace and getting licensed after being identified by a known or a legal authorization, while the second scenario would be the drone entering the airspace without any authorization and confirmed to be rogue. The scenario that this paper is dealing with is the second one as it is an illegal or unlicensed authority.

B. Network Scanning

This authorization is provided by any Wi-Fi or blue-tooth any kind of transmission that comes under radar which is created by a virtual environment such as Kali Linux or Parrot OS. These virtual environments contain various network scanning tools for recognizing the UAV's that are enabled by Wi-Fi such as Acunetix, OpenVAS, Wireshark, Nikto, AngryIP scanner and hcidump for Bluetooth signals that comes under radar. In this paper, Parrot OS is used. Parrot Linux is a Linux distribution which is based on Debian by focusing majorly on computer security.

It is designed for penetration testing, vulnerability assessment and mitigation, computer forensics and anonymous web browsing.

Some of the popular tools in Parrot OS are:

- TOR (The Onion Routers)
- Anon Surf
- I2P
- Electrum Bitcoin Wallet
- Kayak – The Car Hacking Tool
- EtherApe
- GPA – GNU Privacy Assistant
- Nmap
- Nikto
- SQLMap
- Metasploit Framework
- Aircrack-ng
- OpenVAS
- Netcat

For the Bluetooth signal reconnaissance, tools such as Blue log, Bluemaho, Blueranger, Btscanner, Redfang, spooftooph and many more tools like these can be used.

C. Setting up Hardware

To hack the drones that are led by using Wi-Fi and blue-tooth, hard-wares like raspberry pi and Wi-Fi pineapple are required. The raspberry pi is a hardware device which is pretty much like a mini computer that has Bluetooth, Wi-Fi and USB port connections whereas the Wi-Fi pineapple is a hardware which is basically a router that acts as a transmission medium that provides Wi-Fi to the raspberry pi when connected together. Here, raspberry pi helps in disclosing the potential threats of any sort of intrusion. Wi-Fi pineapple works in order to hack the transmission medium of a drone and aids in taking control of the respective drone.

D. Hacking of Drone

The offensive techniques takeover, in the meanwhile the vulnerabilities are once done, they are Wi-Fi and Bluetooth signal jamming with a perimeter set according to the airspace with raspberry pi and Wi-Fi pineapple. For jamming Bluetooth signals, the following tools are used:

1. Blueprinting
2. Bluesnarfing
3. Bluebugging
4. Bluejacking
5. Bluesmack

Whereas, Wi-Fi can be taken under control using:

1. Aircrack-ng,
2. Airgeddon-ng
3. Other GPS spoofing tools.

IV. TECHNIQUES USED

A. Intrusion Detection

In the process of identification of UAV, firstly, the type of intrusion is detected and intrusion protection needs to be done. Following the process of intrusion detection, the license and detection of the model occurs. If the drone is not licensed, then it means that it is an unauthorized drone and immediately needs to be brought into the radar therefore it would be kept out of LOC and restricted airspace.

Fig. 2. UAV (Drone)

B. Vulnerability and Backtracking

For bringing the drone into the line of control, network scanning needs to be done. This is possible by Parrot OS and some of the tools involved in network scanning are:

1. G-SAT
2. COM-SAT
3. Hping or Hping3
4. Aircrack-ng
5. packet spoofing
6. aireplay-ng

By using these tools, the vulnerabilities of the drones are assessed. The vulnerabilities can be classified into exploitation and compromising the strategies.

C. Raspberry Pi 3 and Wi-Fi Pineapple

a) Raspberry Pi:

Raspberry-Pi 3 is a hardware which is very similar to a mini-computer as it has almost all the features of one. As Raspberry-Pi has various facilities like blue-tooth, Wi-Fi and USB ports, it proves to be versatile, compact and economic. Since it is very smaller in size, it is also portable and light-weight.

Fig. 3 Raspberry Pi 3

b) Wi-Fi Pineapple:

Wi-Fi Pineapple is also a hardware that acts as a router for providing Wi-Fi facility. Wi-Fi Pineapple acts as a transmission medium between devices and it is a source for Wi-Fi.

Fig. 4 Wi-Fi Pineapple

D. Ethical Hacking

Finally, to bring the drone completely to the users line of control, ethical hacking is done. An ethical hacker, mostly called as a white hat hacker, is a data security expert who deliberately endeavors to infiltrate a PC framework, system, application or other registering asset in the interest of its administrators - and with their authorization - to discover security vulnerabilities that a malevolent hacker could conceivably exploit. To do ethical hacking, the following tools are used:

1. GPS spoofing
2. Man in the Middle attack
3. DDOS
4. DOS
5. ping
6. nslookup
7. nping
8. Bluetooth jamming
9. Jamming radio frequencies
10. Proxy chains

V. IMPLEMENTATION

A. Implementation of Virtual Machine

Virtual Machine: In processing, a virtual machine (VM) is an imitation of a PC framework. Virtual machines depend on PC models or computer architectures and gives functionality of a physical computer. Their executions may include specialized hardware, software, or both put together.

1) System virtual machines: (also termed full virtualization VMs gives an alternative to an actual machine. They give functionality required to execute the whole working frameworks. A hypervisor utilizes native execution to manage and share various hardware, that allows variable environments which are segregated from each other, yet existing on the same physical machine. Hardware-assisted virtualization and virtualization-specific hardware are primarily used form host CPUs by the Modern hypervisors.

2) Process virtual machines: In a platform-independent environment, Process virtual machines are designed to execute computer programs.

Some virtual machines, for example, QEMU, are intended to emulate various structures or architectures and permit execution of software applications and working frameworks composed for another CPU or design. Operating-system-level virtualization enables the resources of a PC to be apportioned by the kernel. The terms are not all around exchangeable.

Installation and Configuration of VMware Workstation: The steps covered in the process are:

a) Enable virtualization in your PC's BIOS settings
b) Download VMware Workstation Player
c) Install VMware Workstation Player
d) Configure a manual IP address on your PC's VMware NIC
e) Configure a static route to the lab

The step by step instructions are:

- Ensure Virtualization Technology VT is enabled in your laptop's BIOS. The method for doing this varies slightly between different laptop manufacturers. Power on your laptop and then press the manufacturer dependent function key to enter the BIOS settings. In the BIOS settings, ensure that Virtualization Technology VT is turned on. It may also be called Vanderpool Technology or Virtual Machine Extensions. Save the settings, power off, then power back on again.
- Open the VMware downloads page at https://my.vmware.com/web/vmware/downloads in your browser.
- Download VMware Workstation Player and run the installer
- Accept the license agreement and click Next
- Tick the checkbox to install the Enhanced Keyboard Driver
- Accept the defaults and click Next on the remaining pages in the installation wizard, then click Install
- When the installation has completed click Finish. There is no need to enter a license.
- Click yes to reboot.
- Open VMware Workstation Player from the Start menu or the shortcut on your desktop.
- Choose the option to use VMware Workstation Player for free and click on continue and then Finish.
- Click Skip This Version if prompted to download VMware Workstation Pro. The Pro version requires a paid license.
- VMware Workstation Player installation is now completed.
- Next, we need to configure an IP address on your laptop for connectivity to the lab.
- In Windows, open Control Panel > Network and Sharing Center.
- Click on Change adapter settings
- Right-click VMware Network Adapter VMnet1 and then select Properties
- Click Internet Protocol Version 4 (TCP/IPv4) and select Properties
- Configure the IP address 172.23.1.10 and Subnet mask 255.255.255.0. Leave the rest of the settings blank and click OK then Close

- Set the location. If you do not see it, move to other, you will then view all the continents in the world. Choose the suitable continent and followed by your country, press Enter.

Fig. 5 Installation

- Next, we need to configure a static route to the lab's IP subnets.
- Open a command prompt on your laptop by clicking the Windows button and then type cmd in the search box. Right-click Command Prompt and choose the option to Run as administrator.
- Enter the command route add 172.23.0.0 mask 255.255.0.0 172.23.1.254 –p

VMware Workstation Player setup is now complete.

A. Implementation of Parrot OS

a) Parrot Security OS:

ParrotOS is a Debian based pen-testing and security-oriented GNU/Linux distribution featuring a collection of utilities which is designed for penetration testing, anonymity, cryptography, hacking, computer forensics, privacy and reverse engineering. The default desktop environment is MATE which is developed by Frozenbox. For security and digital forensics experts, a full portable laboratory is included although, it additionally incorporates all that a user might need to build up their own programming projects or ensure privacy with anonymity and crypto devices. By default, the ParrotOS has veracrypt, truecrypt, gpg, tccf, zulucrypt, TOR, I2P, anonsurf, Luks and various other technologies developed for defending privacy and identity of user.

b) Installation and Configuration of Parrot OS:

Parrot has been designed for everyone, from Professional pen-testers to the beginners, since it provides the most professional devices consolidated in a simple to use, speedy and lightweight pen-testing environment. The greater part of the penetration testing tools is found under the Parrot section of the main menu, where they're sorted out in subsections. Similarly, an anonymous surfing mode is accessible for people who would prefer not to be traced. Among the included applications, TrueCrypt, Ettercap, Vidalia, Wireshark, Iceweasel, RecordMyDesktop, VLC Media Player, XRCed, PyCrust, BleachBit, aircrack-ng, Hydra, Nmap, and many others will be mentioned.

- First of all, Download Parrot OS latest version from its official website, Boot it from the DVD or USB. The Parrot installation page shows as follows, hit install to continue more.
- Then select the type of installation to be performed. For example, we're selecting the Standard installer.
- Then, choose the language you'll use for the installation from the next screen and press Enter.

Fig. 6 Parrot OS

- Configure your keyboard settings by choosing the type of keyboard you want to use.
- You will see the screen here, which indicates further components are being loaded.
- Create a root password and click on continue.
- Next, set up a user account. Firstly, Set new user and password for the Parrot OS. Then press Enter to advance.
- After setting username and password, choose "manual" partition to create a partition of your own.
- Next, you'll view a list of the current disk partitions on your hard disk from the interface under. Choose your hard disk and press enter.
- Click on yes to proceed further.
- Create a partition table by selecting the hard disks free space.
- Now click on "Create new partition" and press enter
- Specify the size and hit Enter to create it.
- Select the type of partition, then, make the root partition primary as in the interface below and proceed to the next stage. After that also set the root partition to be created initially of the available free space and press Enter to continue.
- Confirm the partition settings and select "done setting up the partition."
- To create a swap partition, click on "create new partition".
- Specify a size for the swap partition and make sure that it's twice your RAM size.
- Select your partition type and proceed to the next step by pressing Enter.
- Set the location for the new partition.
- Confirm your system partition details.
- Then choose the "swap area" for the partition table.
- Now select "done setting up the partition."
- When you have created all the partitions, you will be in the screen below. Transfer down to "Finish partitioning and write changes to disk", then hit Enter to proceed.
- Click on yes to confirm and proceed further.
- At this point, the system files will be copied to disk and installed, depending on your system specs; it'll take a few minutes.

- Choose “yes” to install grub boot loader.
- Select your hard disk for grub installation.
- Once the setup is completed, click on continue and then reboot the system.

After rebooting, enter into the Parrot OS using the login credentials. Thus, the Parrot OS is successfully installed.

c) Implementation of ParrotOS tools:

Hackers may target various other platforms, operating systems, and hardware but still, the methodology stays remarkably same. The steps involved in hacking generally involve:

1. Footprinting
2. Scanning and Enumeration
3. System Hacking
4. Plant Rootkits and Backdoors
5. Covering Tracks
6. Expanding Influence

i. Anonsurf:

Anonymizing a framework in a perfect manner isn't something that simple. Nobody can perfectly anonymize a framework. There are numerous tools accessible on the web that state they anonymize frameworks. Anonsurf is a decent tool to anonymize a framework however can't state it a generally excellent tool since we said before that no tool is perfect when talking about anonymizing. Anonsurf uses TOR iptables for anonymizing the entire framework. Anonsurf provides users with the ability to start or stop the I2P project. The user is free to experiment in Parrot OS running Anonsurf in the background. Its repository comprises both Anonsurf and Pandora bundle. Pandora overwrites the RAM when the user shuts the PC down and furthermore clears the cache. That implies it wipes all hints of the user's work from the system. It very well runs both manually and automatically.

ii. Footprinting, Scanning and Enumeration

a) Bluetooth:

i. Hcitool

Most Bluetooth adapters can be configured with HCI utilities and are USB based. Some Bluetooth devices such as Atheros Bluetooth adapters require a device firmware to be installed in the system. Before beginning the scanning, it needs to be confirmed that the blue-tooth device is unblocked and turned on which can be checked with the rfkill command.

Fig.7 Hcitool

ii. Bluesnarfer

Bluesnarfing is the unapproved access of information from wireless devices by a Bluetooth connection, regularly between phones, desktops, laptops, and PDAs (individual advanced right hand). This enables access to calendars, contact records, messages and emails and on certain phones, users can copy pictures and private recordings. Both Bluesnarfing and Bluejacking exploit others' Bluetooth connections without their insight. While Bluejacking is basically innocuous as it just transmits data to the objective device, Bluesnarfing is the theft of data from the objective gadget.

i. Btscanner

Btscanner is a tool which extracts how much ever data as it could be expected from a Bluetooth device without the necessity to match or pair. A detailed information screen extricates HCI and SDP data, and keeps up an open connection with the monitor the RSSI and link quality.

b) Wi-Fi based networks:

ii. Nmap

Nmap (Network Mapper) is an open-source and network scanner which is made by Gordon Lyon (additionally known by his pseudonym Fyodor Vaskovich). On a computer network, Nmap is used to discover hosts and services by sending packets and response analyzing. It gives various features for testing computer networks, which also includes detection of operating system and discovery of host and other services. These features are extensible by the scripts which gives a little more of advanced service detection, detection of vulnerability and various other features. Nmap can adjust to network conditions including dormancy and blockage during a sweep. Nmap began as a Linux utility and was ported to different frameworks including Windows, macOS, and BSD. Linux is the most prominent stage, followed by Windows.

iii. Wireshark

Wireshark is fundamentally the same as tcpdump, however has a graphical front-end, in addition to some incorporated arranging and separating choices. Wireshark gives the client a chance to put arrange interface controllers into unbridled mode (whenever bolstered by the system interface controller), so they can see all the traffic obvious on that interface including unicast traffic not sent to that system interface controller's MAC address. Be that as it may, catching with a parcel analyzer in indiscriminate mode on a port on a system switch, not all traffic through the switch is essentially sent to the port where the capture is done, so catching in unbridled mode isn't really adequate to see all system traffic. Port reflecting or different system taps stretch out catch to any point on the system. Basic latent taps are incredibly impervious to altering. On GNU/Linux, BSD, and macOS, with libpcap 1.0.0 or later, Wireshark and later can likewise put remote system interface controllers into screen mode. On the off chance that a remote machine catches packets and sends the caught bundles to a machine running Wireshark utilizing the TZSP convention or the convention utilized by OmniPeek, Wireshark dismembers those packets, so it can investigate packets caught on a remote machine at the time that they are caught.

Fig.8 Wireshark

iv. Kismet

For 802.11 remote LANs, Kismet is an intrusion detection system, network detector and also a packet sniffer. Kismet works with any knd of a wireless card supporting raw monitoring mode and capable of sniffing 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program keeps running under OpenBSD, Mac OS X, Linux, FreeBSD and NetBSD. The user can likewise keep running on Microsoft Windows, albeit, beside external drones, there's just one upheld wireless equipment accessible as packet source.

v. OpenVAS

A software framework containing various tools and services that offers scanning and management of vulnerability is OpenVAS. Most of the products of OpenVAS are free software and other components are licensed under GNU General Public License. Nessus Attack Scripting is used for writing Plugins for OpenVAS.

vi. Air tools:

a) Aircrack-ng

Aircrack-ng is a system programming suite comprising of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis instrument for 802.11 remote LANs. It works with any remote system interface controller whose driver supports raw observing mode and can sniff 802.11a, 802.11b and 802.11g traffic. The program keeps running under Linux, FreeBSD, macOS, OpenBSD, and Windows; the Linux rendition is bundled for OpenWrt and has likewise been moved to the Android, Zaurus PDA and Maemo stages; and a proof of concept port has been made to the iPhone.

b) Airmon-ng

Airmon-ng responds with a key data on our wireless adapter that includes drivers and chipsets. In particular, it is to be noted that it changes designation for the wireless adapter from wlan1 to mon0.

c) Airodump-ng

The following tool in the aircrack-ng suite which is airodump-ng, that empowers capturing packets to the user's requirement. It is especially valuable in password cracking. This particular tool must be activated by giving the airodump-ng command and the renamed monitor interface (mon0).

d) Aireplay-ng

Aireplay-ng is another incredible tool in aircrack-ng, and it tends to be utilized to produce or quicken traffic on the AP. This can be particularly helpful in attacks like a death attack that knocks everybody off the access point, WEP and WPA2 password attacks, just as ARP injection and replay assaults.

e) Airdecap-ng

Airdecap-ng empowers us to decode wireless traffic once the key has been cracked. As it were, when the key is at access point, not exclusively would we be able to utilize the data transfer capacity on the access point, however with airdecap-ng we can decode everybody's traffic on the AP and watch all that they're doing (the key is utilized for both access and for encryption).

f) Airtun-ng

Airtun-ng is a virtual passage interface maker. We can utilize Airtun-ng to set up an IDS on the remote traffic to recognize vindictive or other traffic on the wireless access point. Along these lines, in case we're hoping to get an alert of a specific sort of traffic, we can utilize Airtun-ng to set up a virtual passage that associates with an IDS like Snort to send us alarms.

g) Airolib-ng

Airolib-ng stores or manages ESSID's (the name of the access point) and password lists that will help speed up WPA/WPA2 password cracking.

h) Airbase-ng

Airbase-ng empowers us to transform our workstation and wireless card into an AP. This can particularly be helpful when performing a rogue access or evil twin attacks. Essentially, airbase-ng enables us to attack the users, as opposed to the AP and urges the users to connect with us as opposed to the original AP. aircrack-ng is definitely not a single tool, but instead a suite of devices for controlling and cracking Wi-Fi systems. Inside this suite, there is a tool called aircrack for cracking passwords, however to get to crack, we have to complete a few stages utilizing different tools. Likewise, aircrack-ng can do DOS attacks also rogue access points, caffe latte, evil twin, and numerous others.

Fig.9 Airbase-ng

VI. EXPERIMENTAL OUTPUT

The drone is hacked and brought completely to the line of control of the hacker and the drone will not be able to reach the target as it has lost its line of control from the attacker. When the attacker tries to control the drone, it becomes a failed attempt. With the help of various tools and techniques in the virtual environment Parrot OS, ethical hacking was possible and the drone could be hacked.

VII. FUTURE SCOPE

For the future scope of this project would be using more enhanced techniques in ethical hacking other than the ones used in this paper. As technology keeps advancing, so are the risks and vulnerabilities of hackable devices. Hence the existing techniques would definitely not suffice the security systems in the future and that is the reason to try ethical hacking with newer tools.

VIII.CONCLUSION

The Daily usage and inclination of demand for Drones in the market has been outrageous which might cause major intrusions possible in various sectors inclusive of compromising the integrity of civil rights and as well as being the major threat to a lot of Governance Agencies. Taking the reference of the Military and Defense Research and Development into account, the integral part of intruding any kind of restricted airspace is possible through a lot of drones through their stealthy nature which enables them to enter with ease. This leads the restricted airspace of any integral part of Army, Naval, or any kind of place to be most vulnerable to be exploited for classified information or to be terminated. In order to protect and deploy vigilance system that will be able to keep watch over the modified UAV's which are more likely to be stealthy on the radar of the restricted airspace. So that using almost the best Linux's Distro i.e. ParrotOS in Virtual Machine(VMware) platform along with ParrotOS's best hacking and Penetration-Testing tools to Deploy the anonymity of the Intrusion Detection System, IPS and it's counter measures such as hacking the medium of transmission on which the UAV is relying on. However the hacking of the drone can be done by taking down the transmission medium of the UAV with effective tools of the ParrotOS along with the hardware such as Raspberry-pi 3 and the Wi-Fi pineapple to push the limits in successfully hacking down the UAV in the Restricted Airspace. As a Offensive Counter measure we can also infect the OS of the drone with replacing Metameres(IMAJ's) with it's actually captured data as a payload(referred to a method called Steganography) in order to take down the control-station and its operations as whole. Hence it can be concluded that we created a Line of control LOC in order to restrict the UAV's.

REFERENCES

1. Ethical Hacking and Penetration Testing using Raspberry-Pi, Maryna Yevdokymenko, Elsayed Mohamed, Paul Onwuakpa Arinze Infocommunication Engineering department Kharkiv National University of Radio Electronics Kharkiv, Ukraine
2. Early Detection of Cybersecurity Threats Using Collaborative Cognition, Sandeep Narayanan, Ashwinkumar Ganesan, Karuna Joshi, Tim Oates, Anupam Joshi and Tim Finin Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County, Baltimore, MD 21250, USA
3. A Cyber-Defensive Industrial Control System with Redundancy and Intrusion Detection, Dayne Robinson and Charles Kim Electrical Engineering and Computer Science Howard University Washington, DC: USA
4. PENTOS: Penetration Testing Tool for Internet of Thing Devices, Vasaka Visoottiviseth, Phuripat Akarasiriwong, Siravitch Chaiyasart, Siravit Chotivatunyu Faculty of Information and Communication Technology Mahidol University, Nakhonpathom, Thailand
5. Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool, Yien Wang, Jianhua Wang, TSYS School of Computer Science Columbus State University Columbus, GA 31907, USA
6. Securing the Positioning Signals of Autonomous Vehicles, Shahab Tayeb*, Matin Pirouz*, Gabriel Esguerra1, Kimiya Ghobadi1, Jimson Huang1, Robin Hill2, Derwin Lawson2, Stone Li3, Tiffany Zhan3, Justin Zhan*, Shahram Latifi* *University of Nevada-Las Vegas, 1AEOP UNITE, 2RET, 3UNLV STEM Las Vegas, Nevada
7. Drone Hacking with Raspberry-Pi3 and Wi-Fi Pineapple: Security and Privacy Threats for the Internet-of-Things. Ottilia Westerlund1 and Rameez Asif2.

AUTHORS PROFILE

J Caroline El Fiorenza, Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India. Holds a PG degree M Tech (CSE) from SRM IST, Kattankulathur. Has more than six years experience of teaching. She can be reached at email: caro.fiorenza@gmail.com

Revanth Kumar Lokku, UG Scholar, B Tech, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India. He can be reached at email: revanthkumarloki98@gmai.com.

Kirthika Sivakumar, UG Scholar, B Tech, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India. She can be reached at email: kirthika_siv@yahoo.com.

M Reene Stephanie, UG Scholar, B Tech, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India. She can be reached at email: reenestephanie@gmail.com.