International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-05, Issue-01, April 2019

NETWORK ATTACKING USING DRONE

[*]S.Likhitesh, [#]T.S.R. Maanvi, [$]A.Mohan

[*,#]UG Student, [$]Asst.Professor, CBIT Hyderabad and India.

[*]slikhit@cbit.ac.in, [#]ruchieatha97@gmail.com, [$]mohanmtech9@gmail.com

Abstract - The insecure nature of networks poses a grave threat to the underlying IT infrastructure of any organization. The present work aims to create a drone that tests and attacks networks within its range, reporting the same in the form of saved data files. It can be controlled through a networked connection. The drone shall have the flexibility to be run by any Linux powered microcontroller, with the necessary interfaces (communication and control) built. Such drones can be made commercially available and shall help automate the internal security auditing of an organization's critical IT infrastructure. The drone shall test the nearby networks against a wide variety of standard network attacks, allowing the flexibility to perform custom designed attacks on the fly. The work presented here is, an attempt to unify two unrelated domains - automation and robotics; with network security. The expected outcome is a drone that can be remotely controlled, with the capability to do everything in a networked environment that any standard linux machine can do.

Keywords* : *Network attack, media access control(Mac),ARP.

I. INTRODUCTION

Aerial vehicles, especially unmanned aerial vehicles (UAV) are emerging as a new technology domain, finding many uses in almost every sector of life. In addition to the traditional UAV's which were once RC piloted, todays technological advances focus mainly on autonomous behavior and mini atomization of such vehicles.

Securing critical network infrastructure has never been such an important issue as it is today. However, a mechanism is not available till date to remotely audit network infrastructure for weakness or vulnerability. Responding to the emerging trend of personal UAVs, the current project aims to explore the uses of such unmanned aerial vehicles in the field of network security, and how they can be leveraged to ease up the life of pen tester or a network administrator.

This work aims to deal with the lack of an efficient automatable platform for testing network infrastructure. Also, to test the network infrastructure spread over larger landscapes, this project aims to provide a remote solution in the form of a drone that carries with it a full Linux operating system, and can be controlled remotely. The drone thus becomes a remotely controlled aviary computer which has the capabilities of testing networks against insecure connections.

To create a remotely operable aerial reconnaissance vehicle that can remotely be piloted, and carries with it a full Linux operating system that has the capabilities of testing network infrastructure. The Linux box shall be responsible to handle all the motion control of the drone, and provides a remote interface to control the network testing toolkit that it houses.

Currently there exist network auditing tools that are too rigid in their implementation, many of which are not cross platform and are also not generic. Several existing tools are also not open sourced. Added to everything, they require the testing personnel to move around with the entire machine in hand to be able to test for vulnerabilities in a network that is spread over a larger geographical area, for example, colleges and corporate buildings.

There are aerial vehicles which serve the purpose of consumer product delivery or agricultural monitoring systems. These happen to be autonomous, but lack in the capability of being aware of the networking environment around them, making them susceptible to remote takeover.

An aerial vehicle, which was chosen to be a quadcopter, which would carry with it a complete Linux operating system. The operating system shall be equipped with network analysis frameworks that can check for vulnerabilities specified by the auditor. They can also be scripted and run to automate the process. Additionally, there shall be the capability to delegate heavy processing intensive applications to the operating base; So that a record of the audit can be maintained even in the unfortunate event of unrecoverable damage to the drone.

Advantages of proposed system:

- It provides the capability to remotely survey a networked environment.

 DOI : 10.18231/2454-9150.2019.0310

- Corporates and organizations can use such devices to speed up their network auditing mechanisms.

II. LITERATURE SURVEY

2.1 Quadcopter

A quadcopter is a type of an unmanned aerial reconnaissance vehicle, which runs on the basic principles of aerodynamics. Not delving deep into the physics involved, every quadcopter is expected to have the following basic components:

1. Four propellers, two clockwise and two counter clockwise. Attached to four motors, these form the propulsion system of the quadcopter.
2. A flight controller that controls the power delivered to each of the motors to position the drone for a stable flight
3. A frame, which is light enough, so the thrust produced by propellers can lift it.
4. A battery pack with sufficient discharge rate to power the propulsion system [21].

Applications

- Quadcopters are a useful tool for university researchers to test and evaluate new ideas in a number of different fields, including flight control theory, navigation, real time systems, and robotics. There are numerous advantages to using quadcopters as versatile test platforms. They are relatively cheap, available in a variety of sizes and their simple mechanical design means that they can be built and maintained by amateurs.
- The largest use of quadcopters in the USA has been in the field of aerial imagery. Quadcopter UAVs are suitable for this job because of their autonomous nature and huge cost savings. Drones have also been used in light-painting photography.
- In 2014 The Guardian reported that major media outlets have started to put serious effort into exploring the use of drones for reporting and verifying news on events that include floods, protests and wars. Some media outlets and newspapers are using drones to capture photography of celebrities.
- Quadcopters have also been used in various art projects including but not limited to drone photography. They may be used in performance art with new degrees of positional control that allows for new uses of puppets, characters, lights and cameras. They have also been used in light shows
- Quadcopters are used all over the world for racing (also known as "drone racing") and freestyle events. Racing and freestyle quadcopters are built for speed and agility. Racing and freestyle drones tend to be relatively small in size, with 250 mm between the propeller shafts and/or 5-6 inch props being the usually upper end of the size scale

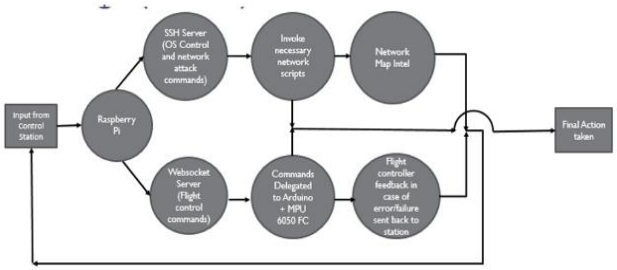
2.2 SSH

SSH, or Secure Shell, is a remote command line interface to an operating system, usually Linux and Unix based. It is very similar to the Telnet utility the only difference is that SSH uses cryptographically secure encryption standards in its communications as opposed to Telnet that uses plain text communications.

2.3 WebSocket

WebSocket is a bidirectional fully duplex communications protocol over a single TCP channel. It is used to communicate over the web, much like the HTTP protocol, but allows communications with lower overheads.

III. DESIGN



. **Figure 3.1.***Network Attacking Drone*

As shown in figure, Elaborating the data flow further, the input from the control station (which can be command or control) is received by either of the two independent servers (SSH and WebSocket) running on the Raspberry Pi. Like can be seen, The SSH server is responsible for handling the commands required for interacting with the network environment, while the web sockets server handles the commands responsible for the fight control. The SSH server can be used to invoke necessary scripts that analyze and reckon the networks or attack them. The information is sent back to the control station over SSH. The commands delegated to the flight controller by the web sockets server are executed by the flight controller, and any feedback of the sates of motors (such as failures) is sent back over WebSocket's. This information can then be used to take further steps, such as invoking the necessary scripts to perform suitable attacks.

The advantage of using two independent servers is that each can be equipped with its own internet interface, thereby allowing any final work to be accomplished in the unfortunate event of any damage to any single communication interface. Also, each module can be run independently with its own dedicated system resources, like

 DOI : 10.18231/2454-9150.2019.0310

a dedicated processor core and memory page, thereby ensuring independent subsystems working at their peak performance [3].

IV. IMPLEMENTATIONS

4.1 Building the Quadcopter

Parts Required:

- Frame 1x (F450)
- 4x Brushless DC Motors
- 4x ESC (Electronic Speed Controllers)
- 1x LiPo Battery (12V)
- 2x Clockwise Propellers
- 2x Counter Clockwise Propellers

Assembling the Parts:

The four arms of the Frame are connected to the power distribution board that comes inbuilt with the frame. The assembly can be done referencing a manual that comes with the frame itself. The wire leads are soldered to the outputs of the power distribution board. The motors are attached to the four arms and ESCs are attached to the motors. The ESCs take a pulse width modulated signal from the flight controller and accordingly vary the output voltage to the motors. The input voltage to the ESCs comes from the power distribution board. The ESCs are connected to this board. The clockwise and counter clock wise propellers are attached at the respective places and this completes the building of the frame.

The Arduino Nano and the MPU 6050 are connected via wire leads and the combination serves as the flight controller. This is placed in the central hollow of the drone to provide maximum stability and closeness to the center of gravity. The Raspberry Pi is placed on the top shelf of the drone, and is connected via USB to the underlying Arduino Nano. The power supply to the Flight controller is obtained via the Pi's USB terminal, and a 5V - 12A DC Power source, powers the Pi.

The power to the motors and the ESCs is delivered via the LiPO battery which is taped to the bottom of the drone, and this assembly completes the building of the drone.

4.2 Working of the Quadcopter

The Raspberry Pi is the brain of the device. It runs a web sockets server which receives connection from the web sockets client, which, in this case happens to be an Android application. This communication channel is used to transmit three-dimensional motion commands to the drone. These commands are parsed and delegated to the underlying flight controller[21].

It also runs an SSH server that provides a remote access to the operating system interface. This channel is used to test, attack and survey the networks around by making use of the operating system capabilities. SSH service is used to remotely access the capabilities of the Linux operating system and invoke the necessary scripts for network reconnaissance/surveillance or attacks.

The combination of an Arduino Nano and IMU MPU 6050 serves as the flight controller.

The MPU 6050 uses its inbuilt accelerometer and gyroscope to calculate the three-dimensional state of the drone, and passes the information to Arduino Nano. The Arduino Nano board then takes this information, receives the motion commands from the Pi, calculates the amount of thrust needed at each motor to shift the vehicle from its current state (given by MPU 6050) to the required state (given by the Pi). Appropriate signals are then sent to each of the four electronic speed controllers that accordingly vary the speed of the motor they are connected to, thereby changing the thrust supplied by each motor[3].

Protocols Used

SSH

SSH service is used to remotely access the capabilities of the Linux operating system and invoke the necessary scripts for network reconnaissance/surveillance or attacks.

WebSocket's

WebSocket protocol is used to send navigation commands to the drone via an Android application that functions as the control station

Networking Scripts

Description of concepts

The network attacking scripts have been divided into two broad categories. Structures, where the definitions of standard communication protocol packets have been defined and implemented. Attacks, which use the structures available in the Structures part and customize the behavior and flow of these packets. Brief description of each follows [20].

Structures

The structures have been classified and categorized according to where they belong to in the OSI architecture. Each protocol implementation is available in its corresponding layer.

Layer 2

Layer 2 is the immediate layer above the physical layer, and in the OSI model, it deals with managing raw bit addresses and managing communication interfaces. It has a variety of protocols like Ethernet, Ethernet II, ARP, RARP etc. For this project, Ethernet and ARP have been implemented at the Layer 2 level.

 DOI : 10.18231/2454-9150.2019.0310

Ethernet

The original Ethernet (IEEE 802.3) is a protocol designed to negotiate addressing at the physical level between two communicating end points. It's main objective is to uniquely identify a network interface card and provide for a communication facility between them.

The Ethernet protocol has three fields in it (excluding the preamble).

A packet that implements the Ethernet protocol is appended to any payload that needs to be transmitted. Any end point that receives this packet can then check for the field destination MAC address. If it matches with that of its own, it accepts the packet and forwards it to the kernel. Or else it simply discards it.

ARP

The Address Resolution Protocol is designed to link logical IP addresses at the higher level with the physical MAC addresses at the lower hardware level. At the beginning of communication, every device only has its physical MAC address. A service like DHCP that runs on the network may then assign them logical addresses. A logical address belongs to a communication end point. It is not a property of the device located at that point. For instance, if two devices at two end points are swapped, their IP address are swapped too. This is because the IP address did not belong to the systems, rather to the end points to which the systems were connected.

If two devices in a network wish to communicate with each other, the only information available to them is the logical address of the corresponding end point. There has to be a way to identify which hardware address is now sitting at the end point. Because the behavior of network interface cards is such that if the Ethernet header destination MAC address corresponds to it's own MAC address, it accepts the packet. Thus, ARP is used to bind hardware MAC addresses to logical addresses. A logical address can either be IPv4 or IPv6 (in the future) ARP proceeds as follows.

Every device maintains a cache table of hardware address – logical address association entries. This is called the ARP cache. Initially this cache is empty at each device. When a device wishes to communicate with another device whose logical address it knows, it broadcasts an ARP request asking for the MAC address of the corresponding logical address, and inserts its own hardware address – logical address association entry in the packet. If a device is present at the requested end point, it updates its ARP cache with the association entry of the sender and then sends an ARP reply to the sender, informing it of its own hardware address. The original sender then updates its ARP cache with the association entry, and a communication may now proceed.

ARP also has the facility to send broadcast messages about updates in a device's association entry. If a device with a static logical address joins a network and wishes to declare its association entry, it sends a gratuitous ARP message to the broadcast informing all devices of its hardware MAC address with IP address and so on. Port scanning is usually done by attempting to make a full TCP connection to all the TCP ports. Open ports respond with a successful establishment of connection. The aim of a port scan is to determine the services running over a target device. For example, open port 80 indicates a webserver is running. This information can then be used to fingerprint the operating system. A suitable exploit can then be found that remotely exploits the given combination of operating system and services. Or else, attempts may be made to have access remotely via default credentials. For eg, default SSH credentials, or default FTP server credentials etc.

Packet Injections

Packet Injections are a type of attack where stray packets are injected into the network with the intention of disrupting normal communication. When rogue packets are injected, they can cause unexpected behavior, which can range from crashing services to flooding a network, or leaking credentials to arbitrary code execution.

Two types of packet injections have been implemented in the current project [1].

ARP Poisoning

ARP poisoning is the use of gratuitous ARP packets to intentionally modify the ARP cache of devices in a network. The defacto implementation is to poison the cache such that attacking node appears as the router to the client and as client to the router.

Procedure

1. Send gratuitous ARP to client to update gateway IP with attacker MAC
2. Send gratuitous ARP to gateway to update client IP with attacker MAC
3. Enable IP forwarding in the attacker machine

In some cases, it might be needed to poison all the devices in a network. In such a case, the gratuitous ARP packets are sent as addressed to broadcast, and no packets are sent to the gateway. This however makes the attacker unable to capture communication packets from the gateway to the client.

Deauth Frames

This is an attack where WLAN De-authentication Frames are injected into the network. Either targeted to a specific device or addressed to broadcast, thereby de-authenticating all stations. For targeted de-authentication, packets are also sent to the AP. Thus the station is de-authenticated from the

 DOI : 10.18231/2454-9150.2019.0310

AP and the AP is de-authenticated from the station[4],[5].

V. RESULT ANALYSIS

4.1 Establishing a connection

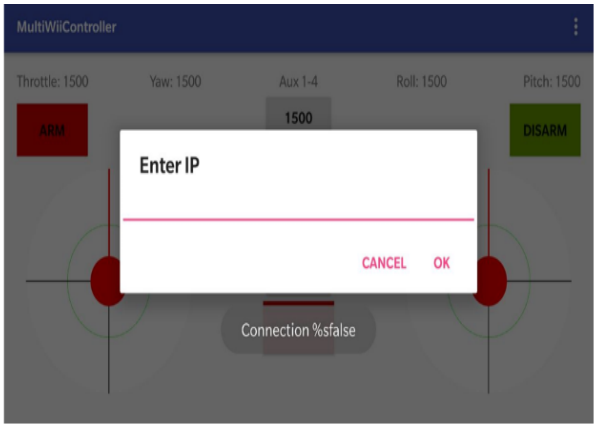


Figure 4.1Connection Establishment

Description: Figure 4.1 shows the connection request from the android app to the WebSocket server running on the raspberry pi. The android application acts as the WebSocket client and this application is used to control the motion of the drone

4.2 Acquiring network configurations

The first logical step to do is to identify what network the drone is in, so we employ sniffing for this purpose.

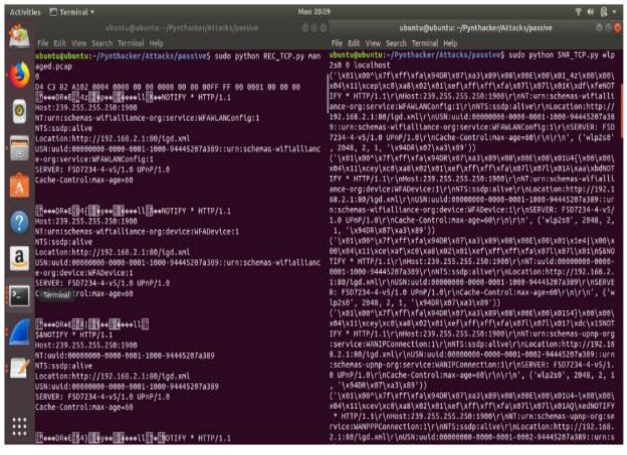


Figure 4.2 Execution for Sniffing the network

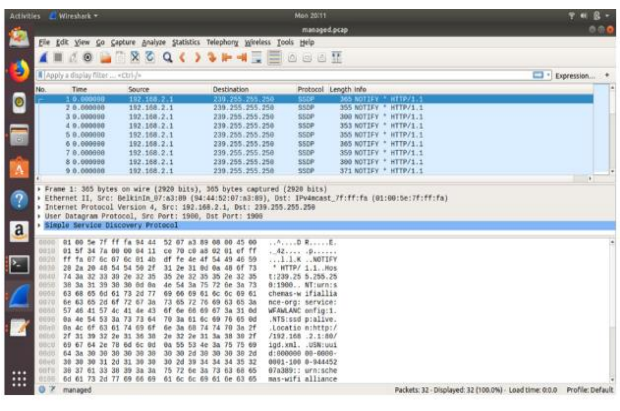


Figure 4.3. Available Network Configurations

Description: The above figures show one way of obtaining the network configuration state by using sniffing (promiscuous mode). These network configurations are acquired by executing commands on the drone remotely via SSH connection.

4.3 Passive Attacks

Passive attacks do not involve in any interaction with the network around them. They stealthily recon for information. Sniffing is the best example, used in almost all passive attacks[4].

Promiscuous Mode Sniffing

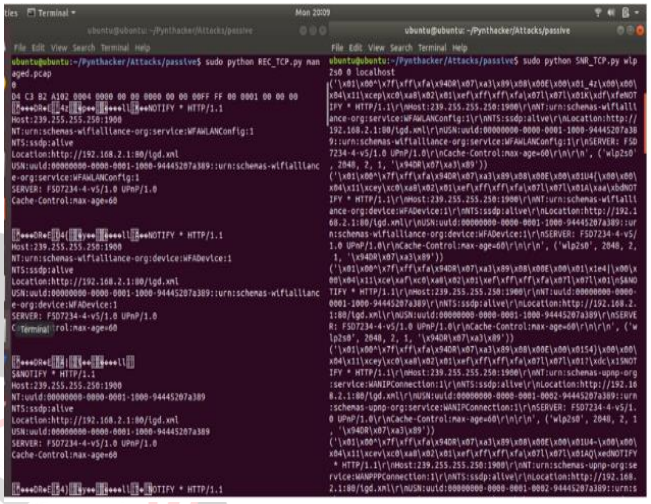


Figure 4.3(a) Server and Client Execution

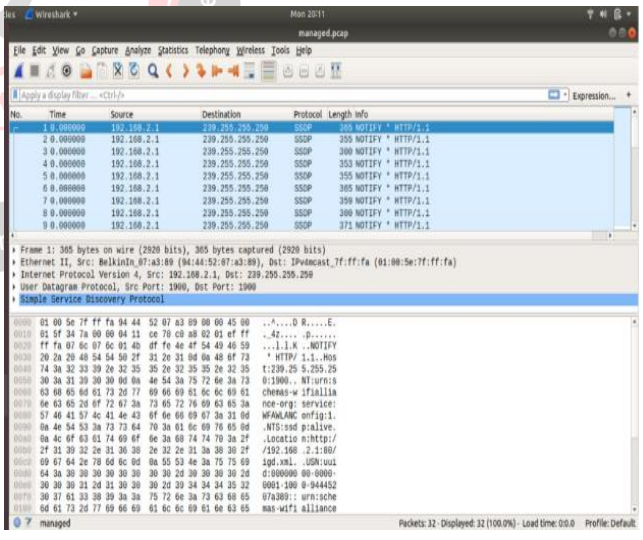


Figure 4.3(b). Sniffed Results (Promiscuous Mode)

Description: The above figures show sniffing in managed/promiscuous mode. The sniffer is executed remotely via SSH and the results are sent back to the command center. The command center stores the result in a file which can be analyzed further.

 DOI : 10.18231/2454-9150.2019.0310

Monitor Mode Sniffing

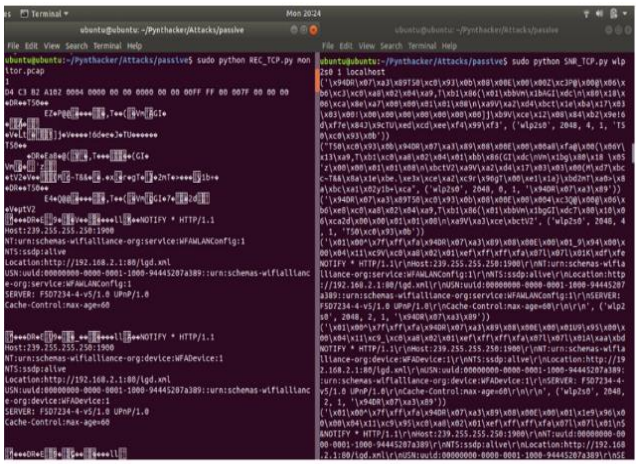


Figure 4.3(c). Server and Client Execution

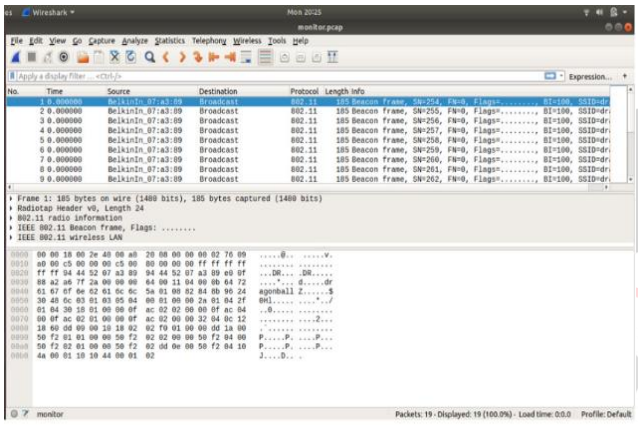


Figure 4.3(d). Sniffed Results(Monitor Mode)

Description: The above figures show sniffing in monitor mode. The sniffer is executed remotely via SSH and the results are sent back to the command center. The command center stores the result in a file which can be analyzed further.

4.4 Active attacks

Unlike passive attacks, active attacks involve some sort of interaction with the target system. There are many types of active attacks, ranging from port scanning to Remote Code Execution [4].

Port Scanning

Figure 4.4.(a) ***Available open ports***

Description: Figure 4.4.(a) shows the results of a port scan of remote machine enumerating the open ports. These ports can be mapped to specific services and attacks can be carried further.

Directed and Definite De-authentication

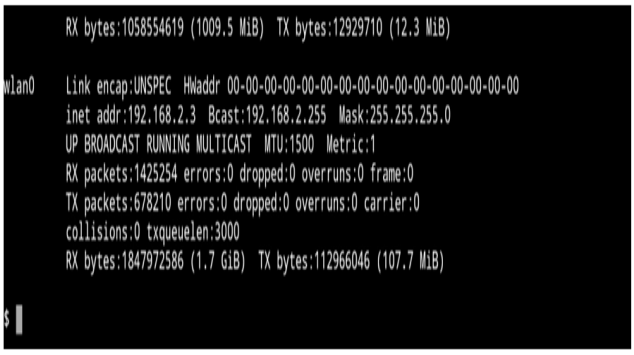


Figure 4.4(b). Targeted Device before Deauthentication

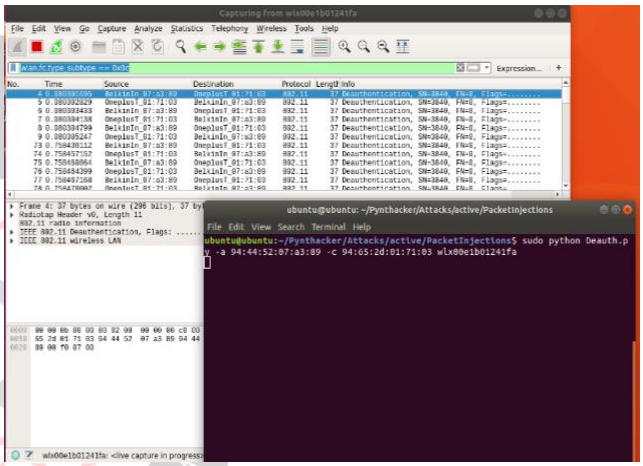


Figure 4.4(c). De-authentication Packets

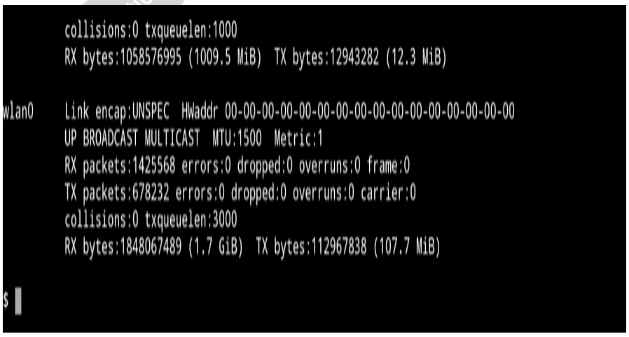


Figure 4.4.(d). Targeted Device after De-authentication

Description: The above figure shows the result of performing a targeted deauthentication attack on a station with definite number of deauthentication packets.

VI. CONCLUSION AND FUTURE SCOPE

A drone has been built which is controlled by and carries with a Linux machine. The drone is augmented with the capability to interact with the network environment around it, so it can survey, recon or attack the network infrastructure around it. A library of required structures and

 DOI : 10.18231/2454-9150.2019.0310

procedures to attack the networks has been developed and deployed, which can be customized according to need. A few attacks have been implemented which demonstrate the proof of concept of customizing attacks. This paper has investigated the possibility of unifying disjoint domains of automation and robotics, with network security.

FUTURE SCOPE

This work explores the idea of providing locomotion to computers by augmenting them with motion peripherals. Besides, this also has the capability of network surveillance and attacks. This is just one variation of what can be done and how functionality of computers can be extended by providing locomotion to them. The amount of scope for future works is only limited by creativity of individuals. Many improvements can be made such as creating dedicated chip sets (application specific integrated circuits) which can be used to speed up the execution of required objective. Instead of an aerial reconnaissance vehicle, attempts may be made to develop their equivalents over land and also under water. From the software perspective, multithreaded programming can be implemented to leverage the full power of today's multicore processors.

REFERENCES

[1] A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends, Yulong Zou, Jia Zhu, Xianbin Wang, Lajos Hanzo, Published in: Proceedings of the IEEE (Volume: 104, Issue: 9, Sept. 2016)

[2] A SURVEY OF WIRELESS NETWORK SECURITY, S. Gopalakrishnan, Published in The International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 1, January 2014

[3] Modelling and control of quadcopter, Teppo Luukkonen, Aalto University, School of Science, Independent research project in applied mathematics.

[4] M. Whitman and H. Mattord, Principles of Information Security, 4th ed. Independence, KY, USA: Delmar Cengage Learning, 2012.

[5] Y. Xiao, H.-H. Chen, B. Sun, R. Wang, and S. Sethi, "MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks," EURASIP J. Wireless Commun. Netw., 2006, doi: 10.1155/WCN/2006/93830.

[6] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha, "Securing electronic commerce: Reducing the SSL overhead," IEEE Network, vol. 14, no. 4, pp. 8–16, Jul. 2000.

[7] K. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in Proc. IEEE Int. Conf. Sensor Netw. Ubiquitous Trustworthy Comput., Taichung, Taiwan, Jun. 2006, doi: 10.1109/ SUTC.2006.1636182, pp. 244–251.

[8] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," IEEE Pers. Commun., vol. 1, no. 1, pp. 25–31, Aug. 2002.

[9] G. Raju and R. Akbani, "Authentication in wireless networks," in Proc. 40th Annu. Hawaii Int. Conf. Syst. Sci., Waikoloa, HI, USA, Jan. 2007, doi: 10.1109/HICSS.2007.93.

[10] L. Venkatraman and D. P. Agrawal, "A novel authentication scheme for ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., Chicago, IL, USA, Sep. 2000, pp. 1268–1273.

[11] A. H. Lashkari, K. Lumpur, M. Mansoor, and A. S. Danesh, "Wired equivalent privacy (WEP) versus Wi-Fi protected access (WPA)," in Proc. Int. Conf. Signal Process. Syst., Singapore, May 2009.

[12] K. J. Hole, E. Dyrnes, and P. Thorsheim, "Securing Wi-Fi networks," Computer, vol. 38, no. 7, pp. 28–34, Jul. 2005.

[13] RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2", Aug. 2008.[Online].Available: https://tools.ietf.org/ html/rfc5246

[14] RFC 4346, "The Transport Layer Security (TLS) Protocol Version 1.1", Apr. 2006.[Online]. Available: https://tools.ietf.org/ html/rfc4346

[15]RFC 2246, "The Transport Layer Security (TLS) Protocol Version 1.0", Jan. 1999. [Online]. Available: https://tools.ietf.org/ html/rfc2246

[16] Mitchell Ashley , "A Guide to Wireless Network Security" Information systems Control Journal ,Volume 3,2004.

[17] Karen Scarfone, Derric Dicoi, "Wireless Network SecurityforIEEE 802.11a/b/g,Bluetooth(DRAFT)",NISTPublication-800-48.Augest 2007.

[18] Tom karygiannis, Les Owens, "Wireless Network Security for IEEE 802.11a/b/g,Bluetooth(DRAFT)",NISTPublication-800-48.November 2002.

[19] Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen, "IEEE 802.11 Wireless LAN Security Overview", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006.

[20] "Cryptography and Network Security" By William Stallings

[21] http://www.instructables.com/id/The-Pi-Quadcopter

 DOI : 10.18231/2454-9150.2019.0310