May-June 2020
ISSN: 0193-4120 Page No. 4661-4666

Rogue Wi-Fi Penetration Framework [RWPF]

[1]Charan Sai Kumar Chittanuru, [2]Gopichand D, [3]B Hrushith

[1,2,3]Department of Computer Science & Technology, REVA University, Bangalore, India,
[1]charanskmr777@gmail.com, [2]pjtchand@gmail.com
[3]hrushith.chowday@gmail.com

Article Info
Volume 83
Page Number: 4661-4666
Publication Issue:
May-June 2020

Abstract
These days, a significant number of us utilize wireless innovation, as internet hotspots are being set up everywhere beginning from the home, cafeteria to various shopping malls. Due to the human tendency of utilizing the wireless internet for nothing in the majority of the situations, we straightaway do connect to Wi-Fi networks that are available with no prerequisite of password and neither do we check how secured is that network. This raises the issue of another sort of danger to wireless networks which is called wardriving. As we know, wireless penetration testing is only minimized to a specific radius on-ground operations, and also war driving has come out of fashion to perform Blackbox testing on a wireless network. Most of the time wireless penetration testing tools are still running on the CLI platform, where all the data will be displayed on the terminal screen and get stored on a document in the backend. So, this kind of output format gives a major gap for real-time analytics. To overcome these issues, we are building a wireless penetration testing device which is operated through a web application that can showcase the data on the web application. War driving has also become limited in rural places where a vehicle cannot reach a particular place for the operations of a penetration tester. To overcome this distance factor issue in any kind of locality we are building a drone that can be controlled with the help of a web application other than the use of a joystick.

Article History
Article Received:*19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *12 May 2020*

Keywords: *raspberry pi, war driving, wireless penetration testing, drone, RF packet sniffing.*

1. Introduction

Penetration testing likewise called pen testing or moral hacking is the act of testing a PC framework, system or web application to discover security flaws or vulnerabilities that an aggressor could abuse. Penetration testing can be computerized with programming applications or performed physically. In any case, the procedure includes gathering data about the objective before the test, distinguishing the conceivable entry points, endeavoring to break in either practically or without a doubt and summarizing back the discoveries. The principle goal of penetration testing is to recognize security weaknesses [4][9] [10][11]. Penetration testing can furthermore be utilized to test an association's security guidelines, its adherence to consistency prerequisites, its representative's security mindfulness, and the association's capacity to distinguish and react to security occurrences. Wi-Fi penetration testing is one approach to recognize holes inside your current systems and actualize rectifications to relieve those risks[4][5][6][8][11]. This is commonly a straight forward procedure that can be especially worthwhile financially when connected with existing inner penetration tests endeavors.

Wardriving is the demonstration of scanning for Wi-Fi systems from a moving vehicle. It includes gently driving around a region to find Wi-Fi signals [4][6][7][15]. This might be cultivated by an individual or by at least two individuals, with one

Published by: The Mattingley Publishing Co., Inc.

May-June 2020
ISSN: 0193-4120 Page No. 4661-4666

individual driving and others scanning for wireless networks. Wardriving might be as basic as looking with the expectation of complimentary Wi-Fi utilizing a cell phone inside a vehicle. Be that as it may, the definition, as a rule, applies to an equipment and programming arrangement explicitly intended for finding and recording Wi-Fi systems [6][7][15].
So, the solution is "Rogue Wi-Fi Penetration Framework". It's a quadcopter which is used to carry a portable computer (Raspberry Pi) and some useful components. The R.W.P.Fis controlled using the internet from the ground with a computer through a web application interface for its operation.

2. Objectives

A. To make an Automated framework for Wi-Fi Penetration Testing[4][5][6][8][11].
B. To help Penetration testers to perform Wi-Fi penetration testing efficiently without any obstacle interruption [4].
C. To build a drone that will be operated with the help of a Web application interface[1].
D. To help the Government bodies to interrupt and intercept the activities and plans being discussed by Terrorists Groups.
E. Replacing the Stingray device is the main objective concerning Wi-Fi surveillance [11].
F. To create awareness of the traps and attacks performed on wireless devices [4].

3. Literature Survey

The literature survey is summarized in table 1.

Table 1: Literature survey

Ref. NO	Methodology	Advantages	Drawbacks
[1][2]	RF Packet Sniffing & Replay	Controlling the e-devices with the assist of Radio signals	Radio frequencies transmission is not encrypted.
[5][6] [12] [13]	Wi-Fi Phisher	Perform the Evil Twin & Man in the Middle Attack.	It cannot switch to different phishing pages during its attack.
[6]	Stingray	The connected end-user calls and messages can be intercepted.	Interferenceof transmission b/w the victim and the intruder.

4. Methodology

Problem statement: Evil twins are not another wonder in wireless transmission. Truly they have been called base station clones or honeypots. What's diverse currently is that more organizations and customers are utilizing wireless gadgets in broad daylight spots and it's simpler for anybody, who doesn't have any specialized skill on technical terminologies to make an evil twin.If these sorts of attacks are established in the populated areas like bus, railway stations, cafeterias, any populated public spots then there will be a huge threat to the individual along with his personal and workspace. Where the many individuals are tricked to provide his/her personal and professional details that may create a threat to an organization or an individual group. The threat can be projected out as a data leak, Denial of Service, and more…

The idea of RWPF is to spy on a specific target that is connected to a Wi-Fi network. The RWPF has a RogueSpy script that is loaded into Raspberry Pi. The script acts as an engine for the RWPF.

RWPF is divided into two parts:
A. Raspberry Pi
B. Quadcopter

Raspberry Pi Requirements

a. Rouge Spy Script
b. RPI Camera
c. Wireless Adapters
d. RF Transmitter
e. 4G Dongle

Rogue spy Components

- AIRODUMP→Airodump-ng is utilized for packet catching of raw 802.11 frames and is especially useful for the compilation of WEP IVs (Initialisation Vector) for use with aircrack-ng.
- HOSTAPD→Hostapd (host access point daemon) is an access point for user-space applications that can transform standard network interface cards into access points and servers for authentication.
- DNSMASQ→Dnsmasq is alightweight, simple to configure DNS forwarder, intended to provide a small-scale network with DNS (and optionally DHCP and TFTP) services.
- APACHE→Apache is an open-source, free web server program that accounts for about 46 percent of the world's websites. The legal name is Apache HTTP Server, and Apache Software Foundation supports and builds it
- PHISHING→Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication.
- DNSSPOOF→DNS spoofing, also known as DNS cache poisoning, is a method of computer security intrusion in which malicious Domain Name System data is injected into the cache of the DNS resolver, allowing the name server to return an incorrect response log, e.g. IP address.
- WEB APPLICATION→In a PC framework, a web application is a customer side and server-side

Published by: The Mattingley Publishing Co., Inc.

May-June 2020
ISSN: 0193-4120 Page No. 4661-4666

programming application in which the customer runs or solicitation in an internet browser. Basic web applications incorporate email, online retail deals, online sell-offs, wikis, texting administrations, and then some.

- MYSQL DATABASE→MySQL is a social database the administration framework dependent on SQL – Structured Query Language. The application is utilized for a wide scope of ideas, including data warehousing, web-based business, and logging applications. The most widely recognized use for MySQL is for a web database.
- FACE RECOGNITION MODULE→Face Recognition is utilized to recognize and manipulate faces from Python or using CLI (command line interface), the world's most straightforward face acknowledgment library. Constructed utilizing 'dlib's best in class face acknowledgment' worked with profound learning.
- SSH→Secure Shell is a cryptographic protocol used within the network convention that guarantees the working system benefits safely over an unbound system. Normal applications incorporate remote command line, login, and remote order execution, yet any system administration can be made sure about with SSH.
- VNC→Virtual Network Computing is a graphical work area sharing framework that utilizes the Remote Frame Buffer convention to remotely manage another PC. It transmits the console and mouse moments starting with one PC then onto the next, handing-off the graphical-screen updates back the other way, over a network.

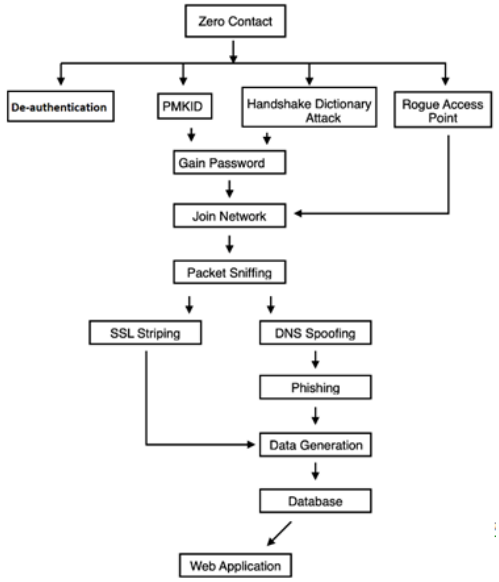

Figure 1: ER Diagram of Rogue Spy

From the above ER diagram (Fig.1) we can see that the scenario starts with the Zero contact.

♦ Firstly, the attack starts with de-authentication which users will start disconnecting from the legitimate Access Point, this can also be called Denial of Service (DOS). This will cause inconvenience to the users from connecting to the Access Point. Whenever users try to connect an Access point a 4-way handshake will be generated, this 4-way handshake contains the information regarding the network and the password associated with it in an encrypted form. The handshake can be captured and also be stored. The Handshake can only be captured when the legitimate user is trying to connect the legitimate network.

♦ In the Second scenario, PMKID is an attack that will provide the encrypted password even when there are no users connected to the network. With the help of the password dictionaries, the encrypted password can be decrypted with the help of brute-forcing. When there is a successful authentication to the network, users connected in that network can be monitored. All the traffic in the network will be sniffed and get stored in a database.

♦ In the Third attack scenario, the handshake needs to be captured from the Access Point, the dictionary brute force attack should take place to recover the encrypted password. When the password is discovered the intruder can join the Access Point and can perform various actions like sniffing DNS Spoofing, Phishing, and more. So that all the data will be stored in a database and can be replicated on a webpage.

♦ In the final scenario, the intruder needs to start performing a de-authentication attack, so that the users connected to the Legitimate access point will get disconnected from the Legitimate access point. At the same time, the intruder starts aRogue Access point with the same ESSID and Channel number. So that the users trying to connect to the Legitimate Access Point will get connected to the Rogue one. At the same time, the intruder performs all the malicious activities like Phishing, Packet sniffing, SSL Striping, DNS Spoofing and more to steal the data. All this data travel and will be deposited at a database. A Web Application will be used to project all the data stored in the database.

a) RPI Camera:The Raspberry Pi camera module is capable of taking full HD 1080p photo and video and can be controlled programmatically. "The Raspberry Pi Camera Board v2 is an excellent 8 megapixel Sony IMX219 picture sensor handcrafted addition for Raspberry Pi, highlighting a fixed center focal point. It's equipped for 3280 x 2464 pixel static pictures, and furthermore underpins 1080p30, 720p60, and 640x480p90 video". It is utilized for supporting the Face Recognition module.

b) Wireless Adapters: Remote connectors are electronic gadgets that permit PCs to interface with the Internet and different PCs without utilizing wires. They send information through

Published by: The Mattingley Publishing Co., Inc.

May-June 2020
ISSN: 0193-4120 Page No. 4661-4666

radio waves to routers that give it to broadband modems or inner systems.

c) RF Transmitter: The Radio Frequency (RF) module is a compact electronic device used for communicating radio signals between two devices. It is also advantageous to connect wirelessly with another computer in an embedded network. Such wireless communication can be accomplished by optical communication or radio frequency communication.

d) 4G Dongle:Dongle is a very lightweight modem capable of linking to 4 G networks or mobile broadband. It's a little gadget that looks like a USB stick or cord. Such dongles grant you access to a 4 G LTE network that helps you to connect to the Internet from your computer everywhere we are.

Quadcopter Requirements:

It consists of the following components:

e) Frame: The structure that holds all the parts together. One of the most significant pieces of the quadcopter is its frame since it underpins engines and different hardware and keeps them from vibrations. You must be exact while making it. They should be designed to be solid yet also lightweight.

f) Brushless DC Motors: These motors or engines are ordinarily utilized for drones that request higher pivot velocities to oversee flights. The Brushless engines are exceptionally vitality effective when contrasted with brushed ones.

g) Electronic Speed Controller: An electronic speed control or ESC is an electronic circuit that controls and maintains the speed of an electric engine. It might likewise give turning around the engine and dynamic slowing down. Smaller than usual electronic speed controls are utilized in electrically serviced radio-controlled models.

h) Lithium Batteries: The lithium battery packs used to control quadcopter have two regular sciences: Lithium polymer (LiPO) and lithium polymer high voltage (LiHV). These two are distinguished different as LiPO cell has an energized voltage of 4.2V whereas the other LiHV cell has a voltage of 4.35V at its maximum charge.

i) Battery Monitor: It will show the maximum voltage of your battery, later cycle through and shows the voltage of every cell. Besides, the unit will screen your battery and sound an alert when one if its cells fall beneath a preset voltage.

j) Power Distribution Board: As the name suggests, Power Distribution Board (PDB) is a printed circuit board that is utilized to disperse the force from your flight battery to every single distinctive segment of the multirotor. Before PDB's turning out to be normal it was important to interface all the various segments utilizing wire and the outcome frequently looked like an octopus and gauged an extensive sum because of the measure of copper and patch joints in the wires.

k) Connectors: Connectors in drones give an interface to dispel power, information, and signals as well and from various subsystems inside the platform.

l) Propellers: One of the most significant pieces of your quadcopter is the propellers. These rotating sharp blades are the wings to your specialty, the very part that makes the winding course that lifts your machine into the air.

m) Multiwii Flight Controller: Multiwii is a quadrotor autopilot framework (FC firmware) created by numerous RC specialists around the globe. This design utilizes an Arduino board as the processor, be that as it may, it's been believed to run on different platforms. This design plans to make the manufacture of gadgets simple.

n) Mounting Pads: Mounting Pads are utilized for retaining engine vibrations, shielding your Flight Controller from the undesirable commotion.

o) RF Receiver (RX): A radio collector, or RX, is the gadget that gets signals from the radio transmitter. It will at that point pass the signal to the flight controller and that is the way by which you control a drone. It's critical to realize that a TX regularly just works with radio recipient (otherwise known as RX) from a similar brand and the equivalent "TX protocol".

p) Flight Control Board: The flight controller (FC) is the intellect of the airplane. It's a circuit board with a scope of sensors that identify displacement of the quadcopter, just as user requests. Utilizing this information, it at that point controls the speed of the engines to make the drone move as instructed.

q) GPS Module: The Global Positioning System(GPS) is a satellite route framework that utilizes a radio collector to gather signals from projecting satellites to decide position, speed, and time.

r) Software Defined Radio: Software-defined radio (SDR) is a radio correspondence framework where the parts that have been customarily actualized in equipment (examplemixers,amplifiers,filters,modulators/de modulators, identifiers, etc.) are rather executed using programming on a PC or implanted framework.

s) Camera: A camcorder is mounted on the unmanned flying vehicle and this camera transmits the live video to the pilot on the ground. Relying upon the quadcopter, the recipient of the live video signals can be either the remote control unit, a PC, tablet or cell phone gadget.

Published by: The Mattingley Publishing Co., Inc.

TEST Engineering & Management

May-June 2020
ISSN: 0193-4120 Page No. 4661-4666

5. Implementation

Controlling of RWPF

1. The Radio Frequency signals of the transmitter will be recorded with the help of a Software Defined Radio (SDR).
2. The SDR records every movement of the drone while it is being operated from a joystick.
3. The recorded signals need to be saturated by clearing the signal noise and other alterations.
4. The recorded signals will be stored in the Raspberry PI(RPI).
5. The SDR will be connected to the RPI for transmitting the signals.
6. The Web application contains controls embedded with RF signals which are used to transmit the RF signals through a transmitter connected to the RPI.
7. The SDR connected to RPI transmits the signals, while the receiver connected to the drone receives the signals.

Working of RogueSpy Script

8. From Fig. 2, the working of RogueSpy Script can be detailed into as following steps:

9. Connect the 4G dongle to Raspberry pi for internet access.
10. Firstly, we need to connect the wireless adapters to the Raspberry pi and start the monitor mode.
11. Run the RogueSpy script now, as it gets started it will show all Access Points (AP's) present in the surroundings.
12. Select the Legitimate AP, then one of the scripts uses Hostapd to create a fake Access Point on the same name and wireless channel.
13. The other script with the help of Dnsmasq configures the DHCP and allocates the DNS server for the Fake Access Point.
14. Now the script performs de-authentication with the help of aireplay/pyrit to disconnect all the users from the Legitimate Access Point and that AP will become invisible for the connected users.
15. At present, the disconnected users will be trailed to connect to the Fake Access Point.
16. When the users get connected to the Fake Access Point, then they will be redirected to a Captive Portal which has an embedded phishing page.
17. The Phishing pages are the ones that look like a genuine web page.
18. The Phishing pages are created in a way that they need to prove their identity as requested by ISP to access the internet.
19. When the details are entered in the captive portal, they will be stored in a MySQL Database in the backend.
20. The information stored in the database will be replicated in the Web Application.
21. So that the information shown in the Web Application will be displayed at ground control ina sorted manner.

Note: RogueSpy script will be operated from a Web Application.

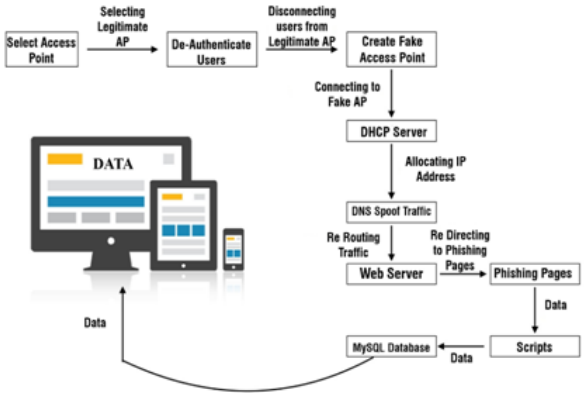

Figure 2: Working of Rogue Spy Script

Working of RWPF:

From Fig 3. RWPF Model we can explain the RWPF working procedure as follows:

1. RWPF is a quadcopter that has a Raspberry Pi (RPI) and a flight controller with a Radiofrequency transmitter and receiver.
2. The radio frequencies are transmitted from a Raspberry Pi (replay the Encoded RF signals) other than a joystick.
3. The RPI has RougeSpy script, SSH, VNC, 4G Dongle, and other features.
4. Using the SSH, VNC, and 4G connectivity, the drone will be controlled.
5. With the help of the SSH, the ground control connects to the RPI which is attached to the RWPF.
6. Once the connection is established, we control the drone from a web application which is running in the RPI localhost.
7. The Web application contains controls embedded with RF signals which are used to transmit the RF signals through a transmitter connected to the RPI.
8. Once the ground control starts using the web application, the transmitter connected to the RPI transmits the RF signals to the Receiver connected to the RWPF.
9. The Transmitter is connected to the RPI, while the Receiver is connected to the Drone.
10. There are two different web applications which will be deployed in RPI:
    - RWPF Web Application Control system.
    - RougeSpy Web Application Control system.
11. Using the web application built for RougeSpy, ground control can perform the

Published by: The Mattingley Publishing Co., Inc.

May-June 2020
ISSN: 0193-4120 Page No. 4661-4666

attacks which are specified at (What does RWPF do).

12. Using the GPS module and camera attached to the RWPF, Ground control can track and monitor the challenges.
13. If the Ground control loses the signal form the RWPF, it will drive back to the coordinates which are allocated to it.

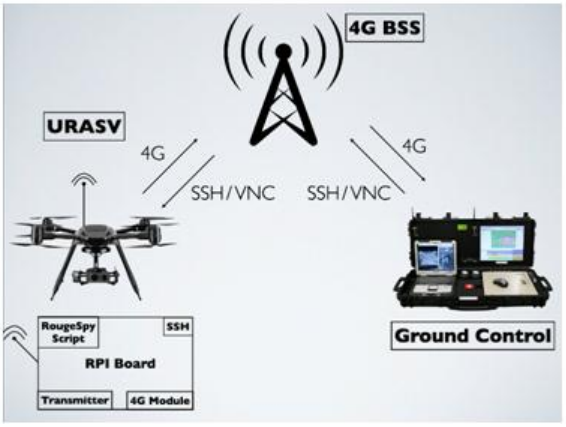

Figure 3: RWPF Model

6. Applications

With the RWPF we can perform a targeted attack, able to geolocate the location of the target once identified and track the data being generated during the work and store all data dumps in the databases. Moreover, the data can be monitored through a web application and we have a drone that can be controlled by radiofrequency via a web interface. Further, there is a scope to move forward this Wi-Fi technology with Base Station's ideology.

7. Conclusion

RogueSpy script helps the pen-testers to save their time and efficiency of processing during Wi-Fi penetration testing. The total design brings out the beauty while performing a Blackbox testing on an organization remotely with various tools and methods. This work will also be helpful for many Defense Agencies to bring down the margin of the threats in society. In the future, the work can also be further developed and be updated with the help of firmware and hardware updates and upgrades.

References

[1] Johannes Pohl and Andreas Noack, "Universal Radio Hacker: A Suite for Analyzing and Attacking Stateful Wireless Protocols", University of Applied Sciences Stralsund – 2018.

[2] Matt Knight, Marc Newlin- "Radio Exploitation 101 Characterizing, Contextualizing, and Applying Wireless Attack Methods"- 2017

[3] Jonathan Andersson, Marco Balduzzi, Stephen Hilt, Philippe Lin, Federico Maggi, Akira Urano, and Rainer Vosseler"A Security Analysis of Radio Remote Controllers for Industrial Applications" - TrendMicro.

[4] Matthias Ghering-"Evil Twin vulnerabilities in Wi-Fi networks" July 7, 2016.

[5] Joseph Ooi, "IMSI Catchers and Mobile Security"- April 29, 2015.

[6] WiFiHop - Mitigating the Evil Twin Attack through Multi-hop Detection, September 2011.

[7] IEEE Draft Recommended Practice for the Evaluation of 802.11 Wireless Performance. IEEE draft 802.11.2-D1.01, February 2008.

[8] IEEE Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std. 802.11-2007, June 2007.

[9] RadomirProdanovi and Dejan Simi, "A survey of wireless security", Journal of Computing and Information Technology - CIT 15, 3, pp – 237–255, 2007.

[10] Bellardo, J., Savage, S.: 802.11 Denial-of-Service Attacks. Real Vulnerabilities and Practical Solutions. In: Proceedings of the 12th USENIX Security Symposium, Washington, D.C, August 4-8, 2003.

[11] Matthew Gast, "802.11 Wireless Networks – The Definitive Guide", O' Reilly, 2002.

[12] V.Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks". In Proceedings of 2002 MILCOM Conference, Anaheim, CA, October 2002.

[13] M. Schiffman, "The Need for an 802.11 Wireless Toolkit". Black Hat Briefings, July 2002.

[14] FCCID.io. (2018). FCCID.io. "Searchable FCC ID Database." https://fccid.io

[15] Linux Wireless Development, (May 2011). Available at: http://linuxwireless.org

Published by: The Mattingley Publishing Co., Inc.