Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Staying Ahead of Threats: Real Time Autonomous Penetration Testing with Embedded Vulnerability Assessment Process for Iot Devices

Venkata Naga Satya Sai Sri Sibbena[1,3], Dr. G. Victo Sudha George[2,3], Dr. S. Geetha[2,3]

[1]Postgraduate Student, [2]Professor,
[3]Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute

Abstract- IoT devices has many security challenges due to default passwords, weak encryption, outdated software, and insecure physical security. These vulnerabilities can lead to unauthorized access, data leaks, and exploitation by hackers. Improving these concerns is crucial to ensure the safety and privacy of users by making strong security protocols and regular updates essential in IoT device development. The project deals with the penetration testing of the IoT Devices using Wifite2 tool and adding a vulnerability scanner for further improvements in terms of security concerns in IoT devices like smart home gadgets, wearables, industrial sensors, and more. It comes under the IoT Cybersecurity field and deals with the embedded Vulnerability and Penetration Testing on IoT Devices. It is one of the types of software testing tools used to penetrate and know the password of a certain selected network. The project is experimented on IoT Devices as IoT devices are everywhere in our day-to-day life. Specifically, here it deals with the IoT Home security Model. The project's main objective is to improve the security of IoT devices as they are very vulnerable and exploitable. This project gives accurate and detailed information on the vulnerabilities found from the scanning process. The methodology used is penetration test using wifite2 in kali Linux as a virtual machine on a system. The next methodology deals with the vulnerability scanner and its results in text form.

Keywords: *IoT Cybersecurity, Wifite, Penetration Testing, Vulnerability Assessment*

1.Introduction

Penetration testing is an attempt to uncover the vulnerabilities on a computer system by manually testing them which is helpful for mitigating the vulnerabilities and enhance the security of the system. Most of the pen-testing is done manually and its time consuming. Pen-testing became mandatory by industry standards and regulations like GDPR, HIPAA, PCI DSS etc. It is important to select the right pen-testing tool by its characteristics like easy implementation, compatibility with existing security configurations and comprehensiveness of the results. There are many known tools for pen-testing like Nmap, Wireshark, legion, jok3r, Owasp Zap, Nikto2, OpenSCAP, sqlmap, scapy, crackstation and Aircrack-ng. The process of pen-testing is where first the port scanning is done to know about the running services and ports and identify the vulnerabilities that can lead to attacks. Next is the analysis of the information collected from the port scanning. Next is the vulnerability scanning where it checks for vulnerabilities in software patches, software updates, applications, firewalls and security settings. Next is the password cracking to check the strength of the password by using brute force attack. The last step is the report of the vulnerabilities found in the pen-testing process. The report is useful for documentation purpose in an organization.

In this paper, we will describe the general introduction for IoT Cybersecurity, vulnerabilities, attacking layers in IoT, penetration testing and tools and vulnerability assessment process.

1.1 IOT CYBERSECURITY

As everyone knows attacks have evolved alongside the advancement of IoT devices. So IoT Cybersecurity focuses on the measures and practices that can be implemented specifically on the cybersecurity aspects within the IoT domain, addressing threats to devices, networks, and data to protect the entire IoT Ecosystem. It is critical aspect in protecting the security of IoT devices.

1.2 VULNERABILITIES

1.2.1 Wi-Fi

Wi-Fi is a technology that allows users to access internet through their devices such as computers, tablets, and other electronic devices. It can be done wirelessly or local area network (LAN). Its full form is Wireless Fidelity. A Wi-Fi consists of one or more access points called as wireless access points (WAPs). They behave as base stations. These stations are connected to a wired network such as Ethernet network. They help in transmitting and receiving the data wirelessly between users within the range of around 30 to 45 meters. It varies on different factors such as transmission power of WAP. Higher transmission is for longer range. Next is obstacles like walls and floors that block the Wi-Fi signals . Next is the frequency bands that operates in 2.4 GHz and 5 GHz that gives speed and range. 2.4 GHz is for longer range but with slow speed whereas 5 GHz is for shorter range but with faster speed. Lastly even environmental factors affect the quality of Wi-Fi speed and range due to factors such as humidity, temperature, and electromagnetic interference.

1.2.2 Encryption standards

In terms of Wi-Fi encryption standards are protocols used to transmit data wirelessly with protection against unauthorized access. It is important to use the advanced encryption protocol other than a weak encryption protocol for improved security. The protocols are:

WEP - WEP is short for Wired Equivalent Privacy. WEP used to be the original encryption protocol for Wi-Fi introduced in 1997. WEP uses a stream cipher called RC4 with 64-bit or 128-bit key lengths. Later it was stopped in mid-2000s as it is highly insecure, has a lot of security vulnerabilities. It was no longer recommended to use as there are more secure alternatives available.

WPA - WPA is short for Wi-Fi Protected Access. WPA uses TKIP(Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) for data encryption. But TKIP has many known vulnerabilities. It is weak and vulnerable to attacks. So WPA with AES is recommended to use for better security.

WPA2 - WPA2 is the upgraded version of WPA which is the current standard for Wi-Fi security. It is widely used for every Wi-Fi networks for better security as default. WPA2 uses AES. It also supports TKIP for backward compatibility. However, in WPA2 vulnerabilities like the KRACK attack have been discovered leading to use WPA3 for improved security.

WPA3 - WPA3 is more advanced form of WPA2. It uses a special handshake called SAE protocol. It stands for Simultaneous Authentication of Equals. It is individual data encryption giving unique keys so if one device is compromised it prevents from jeopardizing the security of other devices. It uses AES-CCMP for encryption as it is resistant to brute force attacks like offline dictionary attacks. It is an option for backward compatibility for older devices.

1.2.3 4-way handshake in AES

For AES to operate securely in Wi-Fi networks the 4-way handshake is implemented. It determines the authenticity. It can be seen in WPA2 and WPA3. The process is of five steps between the Client-(A) and Access Point-(B). They are:

Key Generation - In the key generation phase the (A) and (B) both generate a random nonce and possess a pre-shared key(PSK).

Four Way Handshake - The 4-way handshake phase involves the following steps:

i) (A) requests for connection with (B).

ii) (B) responds with the network information and a nonce to (A).

iii) (A) acknowledges the response of (B) and generates a nonce and computes the Pairwise Transient Key (PTK) using PSK, both nonces and network information. (A) sends nonce and computed PTK to (B)

iv) (B) acknowledges the confirmation of A and now both have necessary information to generate encryption keys.

Deriving Encryption Keys - (A) and (B) use the PSK and nonce to generate the encryption keys. They derive the Pairwise Master Key (PMK) along with the other keys such as PTK and Group Transient Key (GTK) from the PSK and nonces. PTK is unique for each client and GTK is shared among all clients on the network.

Data Encryption - Now the data encryption begins with established PTK and GTK. The data exchanged between (A) and (B) is encrypted with AES algorithm. The PTK is used for encryption and decryption of data for secured transmission.

Data Transmission - After the data is encrypted, they are transmitted between (A) and (B). It is now more secure to transmit the encrypted data using the derived keys.

1.2.4 Krack

KRACK is short for Key Reinstallation Attacks. It consists a set of vulnerabilities that target WPA and WPA2. It takes advantage in the weakness of 4-way handshake. The process starts from Device-(A) and Router (B). (A) requests for connection with (B) and it goes through 4-way handshake. The encryption keys are exchanged between (A) and (B). The attacker manipulates the keys in WPA/WPA2 using KRACK attack by reinstalling an already-in-use encryption keys. This causes reuse of encryption keys compromising the security of Wi-Fi. This happens at the 3rd step of 4-way handshake process i.e., deriving process of encryption keys. Now with knowledge of encryption key the attacker can decrypt the data transmitted between the users.

1.2.5 Weak passwords

A weak password can expose networks to vulnerabilities and attacks. The password should not be created that is too easy to guess like names, birthdates, addresses, or other details about the user and even the repetitive patterns or sequence of characters like 1234, pass@123 etc. It is important to have a strong password. It is vulnerable to attacks such as brute force attack, dictionary attack and WPS exploitation. WPS (Wi-Fi Protected Setup) exploitation is a feature designed to simplify the process of connecting devices to Wi-Fi networks. However, WPS has been found to have security vulnerabilities that can be exploited by attackers to gain unauthorized access to Wi-Fi networks. The common attacks of WPS exploitation are PIN based Attack, Reaver Attack, Pixie Dust Attack and Offline Attack. It is better to disable WPS on the router if it's not needed.

1.2.6 Attacking layers

To address the attack surfaces on IoT devices one should check the hardware and software and how it works. In IoT (Internet of Things) architectures, the most commonly used layered model is typically a three-layered architecture. These layers are perception, network and application. An approach is given for these :

Perception Layer - This is the first and lowest layer of the three layered IoT architecture. It is where the input is collected by sensing the input through various sensors and devices. This contains the collection of data from physical world. From sensors like cameras, temperature sensors, humidity sensors and other types of sensors are used for collecting the data. The collected data at this layer is uncompressed and raw format.

Network Layer - This is the second layer of the three layered IoT architecture. It is essential for communication & transfer of data between devices in the IoT world. It manages the connection between the perception layer(data collected) and the application layer(collected data utilized). It use protocols for communication like MQTT(Message Queuing Telemetry Transport), CoAP(Constrained Application Protocol) and HTTP(Hypertext Transfer Protocol).

Application Layer - This is the last and top most layer of three layered IoT architecture. The collected information from the perception layer is processed and used in this layer. It is used for making decisions, insights on various applications. It involves data analysis, interpretation and presentation in the IoT devices for user friendly experience in the IoT device or system. Few examples in this layer are smart home systems, industrial automation, health care and etc.

1.3 PENETRATION TESTING

Penetration testing is used for identifying vulnerabilities. Penetration testing is also called as Pen Test. The Pen Test is done using certain tools for checking if the IoT device is penetrable. Few tools can used as a vulnerability scanner to identify vulnerabilities in system, network, and applications. For example, Outdated software, missing patches, Weak encryption, Weak password, SQL Injection, Cross Site scripting (XSS), Open ports etc. Few examples for Pen Testing tool are Nmap, Metasploit, Wireshark and wifite. The wifite is used for checking the Wi-Fi's security. It uses reaver, PMKID, deauthenticate, and dictionary attack to crack the Wi-Fi password. The reaver uses the WPS and exploits the Wi-Fi network.

Penetration testing is used by ethical hackers and should be conducted by skilled professionals. There are nine phases followed in Penetration Testing in Figure 1. Penetration testing can be done on any device but with the permission of the device's owner. It is illegal to conduct Pen Test on a device without permission. In terms of information gathering Shodan is a search engine for IoT devices. It can help identify devices that are open or hacked that are connected to the internet and collect information about them. It scans the whole internet and it is very useful for security professionals so they can know the vulnerabilities.

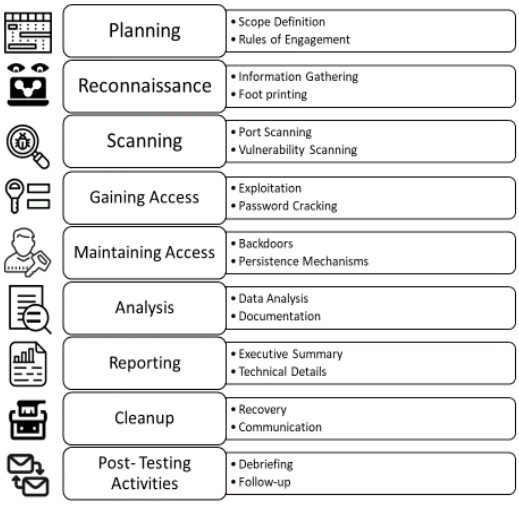

Figure 1. Phases of Penetration Testing

1.4 VAP

VAP is short for Vulnerability assessment process that involves scanning, identifying and analysing the vulnerabilities found in the device. It is a part of the penetration testing where the findings are documented into a report for documentation purpose in an organization. The vulnerability assessment process is done with help of testing tools or penetration testing tools as explained in Section . The rrport gives a detailed information on the vulnerabilities and how they can be mitigated. The vulnerabilities that will be focused in this project are Sensors, Wi-Fi and Password.

2. BACKGROUND RESEARCH

2.1 GREEN IOT

This paper [1] is a systematic review of energy saving technique in IoT. In terms of IoT Framework the summarized into four topics. They are Machine to Machine(M2M), Radio Frequency Identification (RFID),

Microcontroller Units (MCUs), Integrated Circuits (ICs) and Wireless Sensor Network (WSNs). These are considered for Green IoT as they are energy efficient in terms of data transmission, hardware, multicore platform processors, routing and WSN architecture. In M2M the energy efficient in data transmission the approaches are data compression, cooperation between devices, ML algorithms, power control and energy efficient protocols. For WSN the approach is Eco sustainable WSN. For energy efficient routing and WSN Architecture the approaches are cluster architecture, multipath routing and relay mode placement. For RFID the approaches are either battery for long term and steady power or capacitor for short term but high power. For Microcontroller Units and Integrated Circuits, the approaches is the run time. The data processing which it reads , analyses and transmits only in run time and hibernate when not in use.

2.2 SECURITY AND CYBERSECURITY IN IOT DEVICES

In paper [2] they gave the general introduction of cybersecurity in IoT in the field of healthcare and how it impacts the cybersecurity aspects of the sensitive information of patients in a health organization where in the paper [3] they explained the importance of IoT security in every IoT as it covers overall security of the IoT device. A review [4] from online discussions were taken from a social media application called Twitter where a group of non-expert users discussed their knowledge on Cybersecurity. The paper [5] discusses the importance of cyber security, various tools used in cyber security, their applications, and potential areas for future research in the field. By conducting a systematic literature review [6] , the authors aimed to provide a comprehensive overview of the current state of IoT cybersecurity, highlight gaps in existing research, and propose recommendations for future research directions. This type of study can help researchers, practitioners, and policymakers gain insights into the key issues surrounding IoT cybersecurity and develop effective strategies to address them.

2.3 THREATS, ATTACKS AND VULNERABILITIES

In papers [7][8] they explained the impact of DDoS and E-DDoS attack impact on Smart City IoT and the devices, system and network used in smart city along with threats and solutions using technologies. The devices used are sensors, PLC, Smart meter, street lights and CCTV. System used are Server, database, management system and HMI (Human Machine Interface). And in network they used Wi-Fi, LoRa, Zigbee and TCP\IP. The threats for devices were masquerade, unauthorized access , malicious code and software. In System the threats are staff's mistakes, unauthorized access and alteration or destruction of important information. At last in Network the threats were wiretapping, Man in the Middle attack and Traffic analysis. The solutions using technologies were Blockchain technology, data driven approach, HSCCA method, probability-based model and ICADS. In this paper[9] they did a systematic review on the known attacks such as Vladimir Levins attack, Melissa Virus, ILOVEYOU Worm3, MyDoom worm4, Covidlock Ransomware, Kaseya Ransomware Attack etc. and how they were originated i.e. from which vulnerabilities they used these attacks. In the paper [10] they gave an intelligent approach by combining the algorithms ML, DT, RF, ET, NB and SVM with PCA whereas in paper [11] they used DT along with the DNN for threat detection in IoT. In the papers [12][13]they summarized the vulnerabilities and their countermeasures. At last, the paper [14] shows the vulnerability of IoT cloud-based security camera in IoT infrastructure.

2.4 WI-FI AND WLAN NETWORKS

In the paper [15] they explained the applications of WSN in IoT and how they impact the IoT framework and Industry 4.0. In the paper [7] they showed an experiment of impact of DDoS and E-DDoS attack on Wi-Fi of IoT device. In the paper [16] they explained the Wi-Fi calling services and their vulnerabilities, attacks and solutions. The vulnerabilities are 3GPP WLAN, IPSec where 3GPP WLAN doesn't prevent the device from connecting to insecure networks. The IPSec is vulnerable to side channel attacks. They gave a solution by introducing Wi-Fi Calling Guardian. In the book [17] in module 13 they the need of network protection system for reducing the network attacks using firewalls and Intrusion detection and prevention systems. In this paper [18] they did a systematic review on Wi-Fi security through wardriving technique with the data of WLAN security networks. The collected networks were of 21,345. In that 23 networks use WEP encryption, 18 networks use WPA-TKIP, 5359 networks are unencrypted, 9139 networks use WPA2 and 13 networks use WPA3. Some used legitimate SSID and some use masked SSID. 73.11% of the networks used 2.4 GHz in 1, 6 and 11 channels whereas 27.89% of them

used 5.0GHz in 36, 52, 161 and 120 channels. This research [19] aims to improve the security posture of WiFi networks by introducing a new approach to creating hidden networks that are less vulnerable to unauthorized access and potential attacks. The review [20] covers various aspects related to security and privacy in IoT, including data breaches, unauthorized access, malware attacks, and privacy violations. The authors also discuss the challenges faced in securing IoT devices due to their limited processing power and storage capacity.

2.5 PENETRATION TESTING AND VULNERABILITY ASSESSMENT

The literature review on Vulnerability Assessment and Penetration Testing (VAPT) talks about how we keep computer systems safe from hackers. It looks at different papers [21-45] that explore this topic in detail. These papers start by explaining why VAPT is really important for keeping our information safe. They then talk about all the different ways we can find and fix problems in computer systems. This includes using both automated tools and manual testing to make sure we don't miss any vulnerabilities. They also focus on techniques like scanning networks, checking for weaknesses, and trying to break into systems to see if they're secure. They spend a lot of time looking at popular tools like Nessus and Nmap to see how well they work. They even share stories of times when people found problems in systems and what they did about it. But, even though VAPT is super helpful, there are still some challenges, like when the system says there's a problem when there isn't one, or when it takes a lot of time and resources. They discussed the frameworks like OWASP, NIST and OSSTMM analyzing these approaches to vulnerability assessment and penetration testing as an approach to the vulnerabilities. Comparisons are highlighted between strengths and weakness in devices. However, the papers also give some good tips on how to deal with these challenges. They also talk about what might happen in the future, like using fancy technology like AI to find problems even better and making sure we're always checking for issues, not just once in a while. Overall, these papers show that VAPT is a big deal for keeping our digital world safe and strong.

3. Model Environment

As shown in Figure 2 the sensors are connected properly to the ESP32-CAM board. It is Wi-Fi enabled with CAM. This hardware is used for the general home security model. At first the

3. Model Environment

3.1 HARDWARE

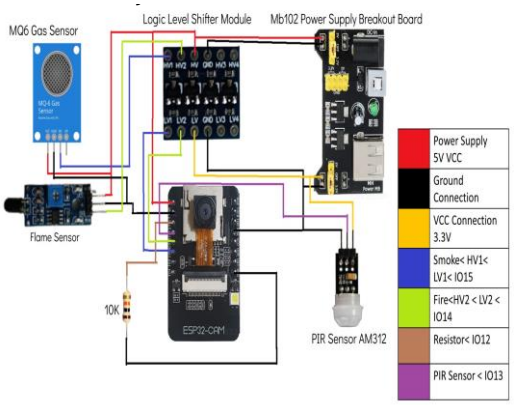

Figure 2. Home Security Model Architecture

Flame Sensor (3.3V VCC) - This sensor operates at 3.3V. It typically has four pins - VCC (power supply), GND (ground), D0 (digital output), and A0 (analog output). VCC should be connected to a 3.3V power source and GND to ground. The digital or analog outputs can be used to interface with a microcontroller or other logic circuitry.

MQ6 - The connections of the MQ6 gas sensor typically include VCC, GND, an analog output, and possibly a digital output. VCC connects to a 5V power source, GND to ground, and the analog output can be connected to an analog input pin on a microcontroller for gas level monitoring.

PIR Sensor - PIR sensors typically have three pins - VCC, GND, and a digital output. VCC connects to a power source, GND to ground, and the digital output connects to a digital input pin of a microcontroller for motion detection.

Smoke Sensor (HV1 & LV1) and Fire Sensor (HV2 & LV2) - These sensors likely have similar power and output connections as the MQ6. HV1, LV1, HV2, and LV2 probably refer to high voltage and low voltage connections.

Level Shifter TTL 5V to 3.3V - This device is used to convert signal levels from 5V to 3.3V or vice versa, enabling compatibility between devices with different voltage requirements.

ESP32-CAM - The ESP32-CAM will typically need connections for power (3.3V or 5V and GND), and it may also require connections for camera control, flash, and communication (e.g., UART, I2C, or SPI).

MB102 Power Supply Breakout Board - This board has connections for input power (DC in) and outputs for both 3.3V and 5V power. It also has ground (GND) connections. This board can be used to power the various components of the security system. These are general guidelines for connecting the mentioned components. However, specific connections could vary based on the exact specifications of the components, and it's always important to consult the datasheets or manuals for each component for precise wiring instructions.

3.2 SOFTWARE

3.2.1 Arduino

The ESP32-CAM is programmed used the Arduino IDE so the Arduino IDE is installed. In order to start the process with ESP32-CAM the necessary libraries should be installed for involving the telegram bot. The library needed are Universal Telegram Bot library and ArduinoJson Library. The library are installed from the Sketch > Include library > Manage Libraries and find the library name. Universal Telegram Bot Library is communicating with the bot using the users chatID. After installing the libraries the code is compiled and executed as shown in the Figure 3.

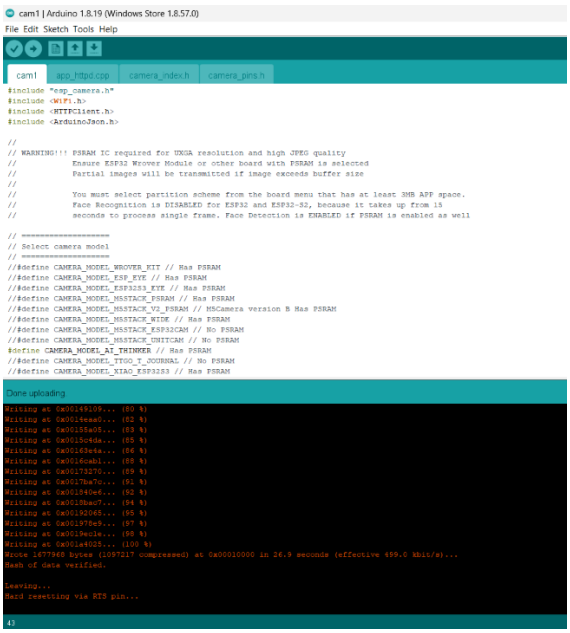

Figure 3. HSM Code Executed

As shown in Figure 4 the output of Vulnerability assessment is shown with the details about the model and vulnerabilities along with the solutions is shown in the console of Arduino IDE.

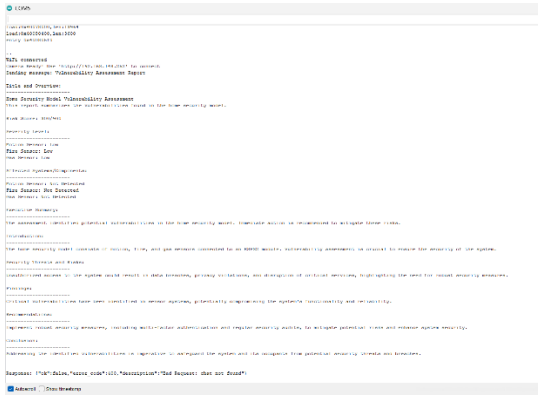

Figure 4. HSM Output in Console of Arduino IDE

3.2.2 Wifite2 and Monitor Mode

There is no need to install Wifite on Kali Linux using the command line as when downloading Kali Linux for Oracle VM Virtual box it gives preinstalled Wifite in it.

Step 1: Open a terminal in Kali Linux.

Step 2: Update the package repository by running the following command:

$ sudo apt update

Step 3: Now run Wifite by typing the following command:

$ sudo wifite

Step 4: Sometimes the Wifite doesn't work properly or doesn't start properly then use this command:

$ sudo wifite --kill

Step 5: An error appears asks for the missing files pyrit, hcxdumptool, hcxtools then use the commands:

$ sudo apt-get install pyrit

$ sudo apt-get install hcxdumptool

$ sudo apt-get install hcxtools

Step 6: Another error saying the networkmanager is not working:

$ sudo service NetworkManager start

Step 7: Once the installation is complete, you can run Wifite by typing the following command:

$ sudo wifite

This command will start Wifite, and you can use its various options and features for Wi-Fi penetration testing.

Now you have successfully installed Wifite on Kali Linux using the command line. You can utilize Wifite's capabilities to automate Wi-Fi penetration testing tasks and assess the security of wireless networks.

3.2.3 Enabling Monitor Mode for Adapter

Some adapters use commands to enable monitor mode to use the Wi-Fi connection. Some adapters have monitor enabled in them. For example, in TP-LINK Wi-Fi adapter Version 1 it has inbuilt monitor mode whereas in Version 2 & 3 we need to manually enter commands to enable the monitor mode using the commands:

For Version 1 -

Step 1: Open a terminal in Kali Linux.

Step 2: Identify the name of your wireless adapter by running the following command:

$ iwconfig

Step 3: Look for the wireless interface name (e.g., wlan0 or wlan1).

Step 4: Disable the interface by running the following command (replace "wlan0" with your interface name):

$ sudo ifconfig wlan0 down

Step 5: Enable monitor mode on the wireless adapter using the following command:

$ sudo iwconfig wlan0 mode monitor

Replace "wlan0" with your wireless interface name.

Step 6: Bring the interface back up by running the following command:

$ sudo ifconfig wlan0 up

Again, replace "wlan0" with your interface name.

Step 7: Verify that monitor mode is enabled by running the following command:

$ iwconfig

Look for the "Mode: Monitor" entry next to your wireless interface.

For Version 2 & 3:

Step 1: Open browser and type download compat-wireless kali linux

Step 2: Now select the link

https://mirror2.openurt.org>sources

Step 3: Download the compat-wireless-2010-06-28.tar.bz2

Step 4: Extract in the downloads folder itself.

Step 5: Open terminal in download folder.

Step 6: Enter the following command to enter into root terminal:

$ sudo su

Step 7: It asks for password and enter the password for root terminal.

Step 8: Enter the following command:

ls

Step 9: Enter the following command:

cd compat-wireless-2010-06-28

Step 10: Enter the following command:

ls

Step 11: Enter the following command:

make unload

Step 12: Enter the following command:

make load

Step 13: Open terminal in downloads folder and enter the following command to check wlan:

iwconfig

Step 14: Enter the following command to check the wlan:

ifconfig

By following these steps, you should be able to enable monitor mode for your wireless adapter in Kali Linux. Please note that not all wireless adapters support monitor mode, so it's essential to check the compatibility of your adapter before attempting to enable it. It can be seen in Figure 5.

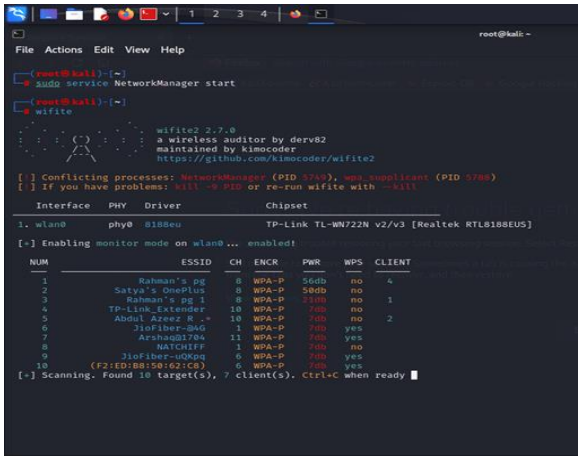

Figure 5. Wifite Running on Kali Linux

3.2.4 Telegram

For setting up the telegram bot first the application is installed on smartphone. Next get the ChatID from Botfather or IDBot as shown in Figure 6. In order to get the report from ESP32-CAM to telegram chat, the chatID is important. It is similar to API codes. Next create a bot for the home security model using Masterbot called BotFather. The created new bot generates a bot token for interaction purpose. This bot token is inserted into the code of ESP32-CAM.

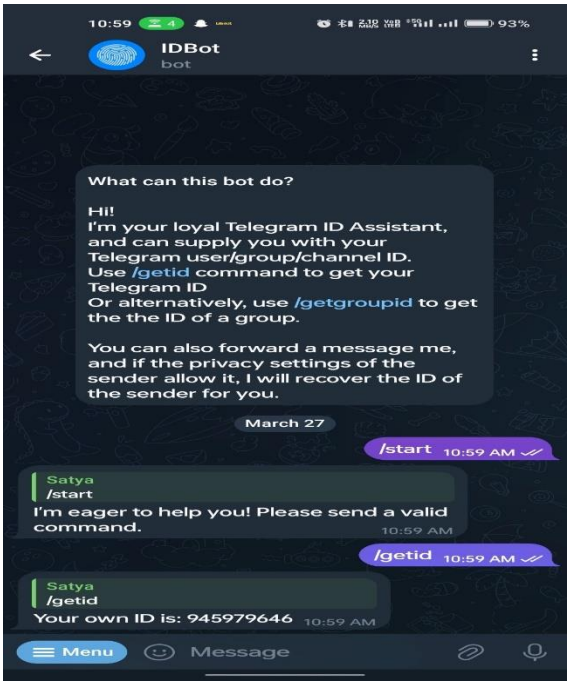

Figure 6. IDBot

4. Methodology

Building a Home Security Model using various gadgets: an ESP32-CAM for capturing images, a PIR Motion Sensor to detect movement and Smoke and Flame Sensors to identify potential fire hazards. a tool called Wifite on a virtual computer created with Oracle VM VirtualBox. This tool helps us test the wireless security of the devices in our Home Security Model. A Vulnerability Assessment Process is made, which is like a safety check to see if there are any weak points in our security setup. Think of it as checking all the doors and windows in your house to make sure they are locked and secure. This process helps us find and fix any potential problems, making our Home Security Model stronger and more reliable.

4.1 ARCHITECTURE DIAGRAM

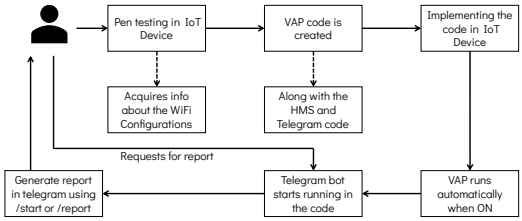

Figure 7. Project Architecture

As shown in the Figure 7 first the user conducts the penetration testing on the IoT device to check if its penetrable or not. After the pen-test the VAP code along with the HMS and telegram code is implemented. The code is now compiled and executed. The VAP runs simultaneously to the HMS and Telegram code. So when the HMS model is connected to the laptop or any power supply it will automatically sends the vulnerability report to the bot and the user receives it.

4.2 OUTPUT

4.2.1 Penetration test

Before running the Wifite command first the root terminal should be opened like in the Figure 8. For opening the root terminal, the user needs to enter password. To check the wlan0 is present or not the following command should be used

$ iwconfig

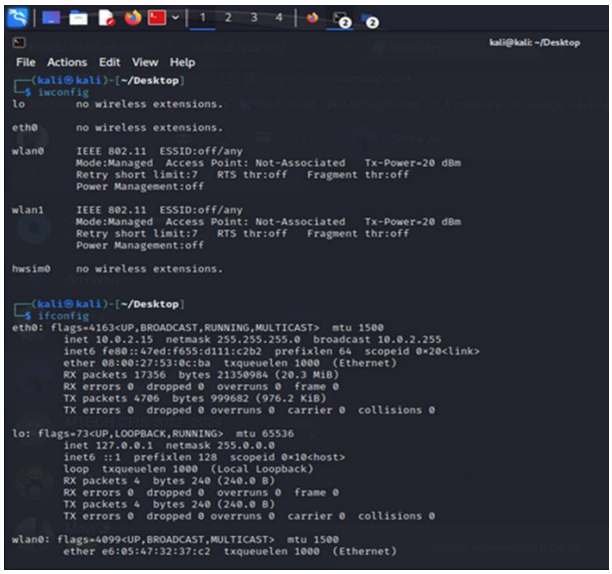

Figure 8. WLAN0 Verification

Figure 9. Pen Testing

At every scanning process the network manager should be started. To start the networkmanager this command is used:

$ sudo service NetworkManager start

$ sudo Wifite

Then the Wifite is started and it starts running and scans for network connections. It is shown in Fig . To check for more network connections, I even included my own device's "Satya's OnePlus" hotspot connection. It can be seen in Figure 9.

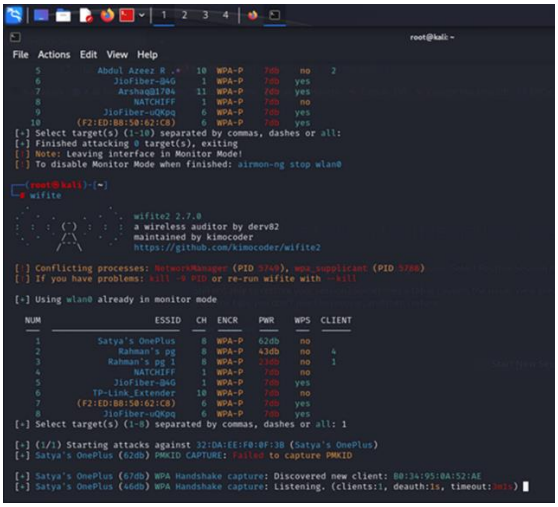

Figure 10. Capturing PMKID

For legal reasons I selected my own device "Satya's OnePlus". It's illegal to crack or do penetration testing on other network connections. Permission is needed to select other network connections. It starts the attack against my device for a time limit of 5 minutes. It failed to capture PMKID as my personal hotspot password is strong. It can be seen in the Figure 10 . It starts the WPA handshake capture to deauthenticate or crack the clients connected to the network connection. After trying the capture for 5 minutes it couldn't crack the client device as the client's device has strong security measures but the WPA handshake capture deauthenticates the client device from the network connection. The Wifite cracks only the recently connected clients of the network connection.

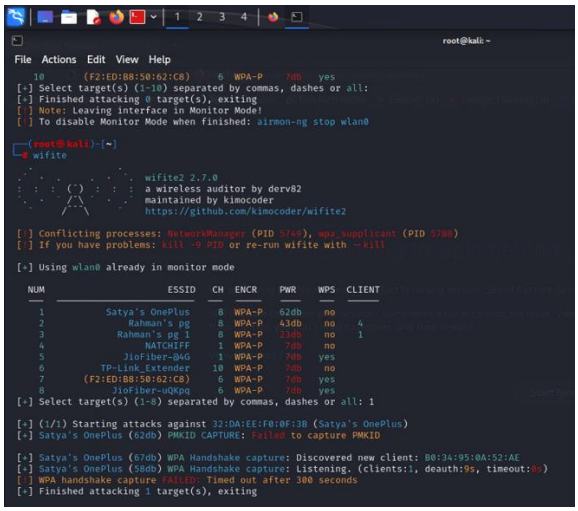

Figure 11. Pen-Testing Result

After failing the PMKID capture and WPA Handshake Capture it disconnects the client connected to the home network and finishes the attacking as shown in the Figure 11.

4.2.2 VAP and reporting

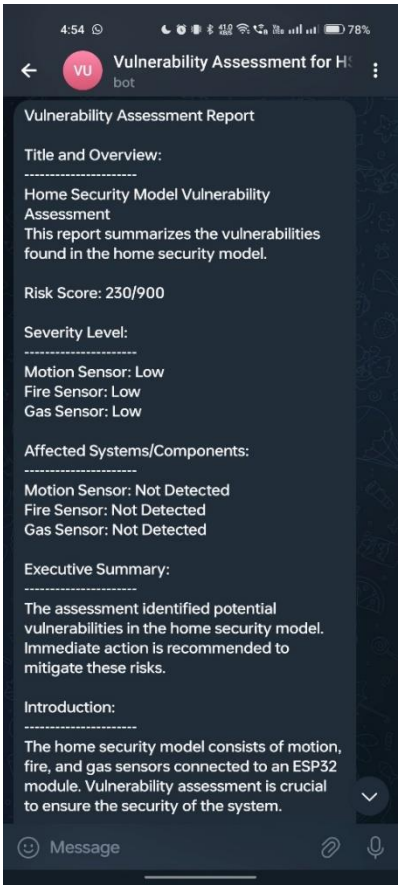

Figure 12 (A) Vulnerability Report in Telegram without Sensor in HSM

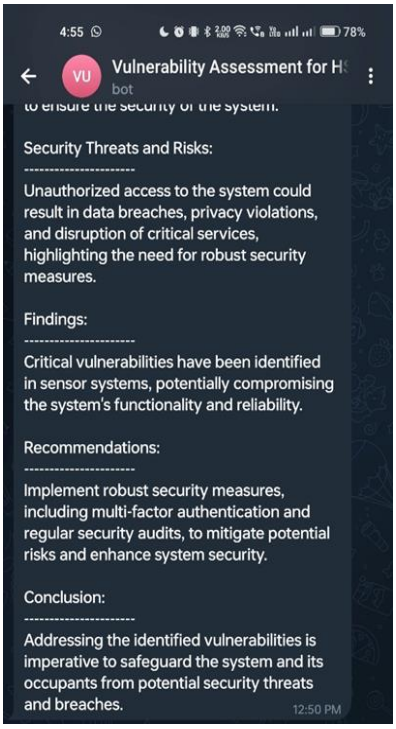

Figure 12 (B) Vulnerability Report in Telegram without Sensor in HSM

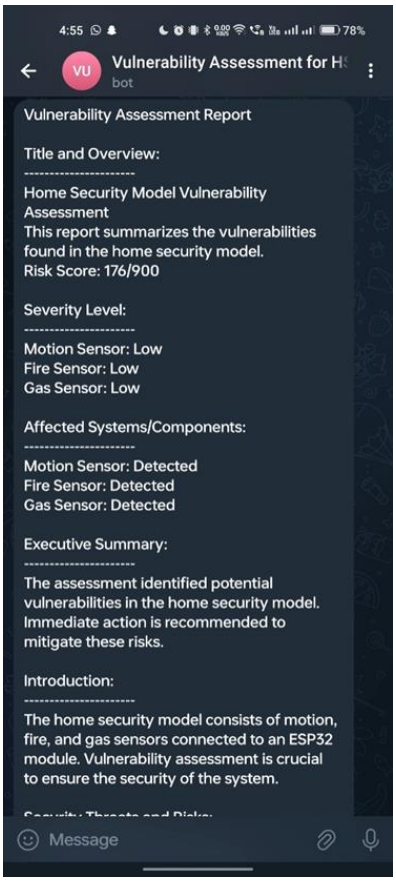

Figure 13 (A) Vulnerability Report in Telegram with Sensor in HSM

Figure 13 (B) Vulnerability Report in Telegram wi (B) or in HSM

The Figure 12 (A) and (B) shows the vulnerability assessment report ge... when the home security model runs but without sensors whereas Figure 13 (A) and (B) shows the vulnerability assessment report generated when the home security model runs with sensors. The risk score is generated based on the vulnerabilities found. The report gives the general introduction, severity level, affected system or components, summary of the report, finds, suggestions and conclusion. It also shows the security risks and threats. The report is generated and sent to telegram bot which has been created using telegram inbuilt feature 'botfather'.

5. Results And Discussion

The project is done within the controlled environment. There are some important factors to be noted when the project is implemented.

5.1 NETWORK INTERFACE AND RANGE

The adapter used has typically a range of 100 meters (approximately 328 feet) in open spaces but may vary when any obstacles are there such as walls, floors and other structures that interfere or block the Wi-Fi signals reducing the quality of network.

5.2 TIME TAKEN TO CRACK NETWORK PASSWORD

In the latest version of wifite it uses pixie dust attack, brute force attack and attempts for cracking the handshake. The time taken to crack the password using the wifite is five minutes and it keeps trying every attack for five

minutes leading to taking even more time. Each step is done for five minutes. Wifite attempts each step till it is successful before moving on to the next step. Depending on the complexity of the password in the five minutes it will keep trying to crack the password. The five minutes is fixed in the wifite's protocol and it cannot be altered.

5.3 COMPARISON TO RELATED WORK

The inclusion of inbuilt Vulnerability Assessment Process within this project is what differentiates from the existing systems that use external VAP. Unlike traditional systems which uses separate tools or services for scanning the vulnerabilities, the inbuilt Vulnerability Assessment Process is an advancement that runs simultaneously with original code of the model and give solution in the form of report through telegram bot. This inbuilt Vulnerability Assessment Process enables the users of home security model for continuous monitoring and detection of vulnerabilities.

6. CONCLUSION

In this project, the development of a home security model and subsequent penetration testing using Wifite provided invaluable insights into the vulnerabilities and strengths of our system. Building the home security model involved meticulous planning and implementation of various defence mechanisms. Our goal was to create a robust system capable of safeguarding residential spaces against potential threats. Leveraging advanced technologies and comprehensive strategies, we aimed to establish a proactive approach to home security. The penetration testing phase using Wifite allowed us to simulate real-world attack scenarios, revealing vulnerabilities that could compromise our system's security. Thus created a vulnerability assessment process for IoT device to detect vulnerabilities such as sensors, Wi-Fi and passwords. If the process shows no vulnerabilities, it means it is secured else it can identify, analyse, and do risk assessment. The remedies for mitigating vulnerabilities can be given as a detailed report for future enhancement for the users. Looking ahead, continual monitoring and staying updated on emerging security threats will remain crucial. These steps will bolster our efforts to create a more secure environment for homes. While this project marks a significant milestone in enhancing home security, it's essential to acknowledge that ensuring comprehensive protection is an ongoing endeavour. Our dedication to continuous improvement will drive us to adapt and evolve our security model to effectively combat future challenges.

References

[1] Alsharif, M. H., Abu Jahid, Anabi Hilary Kelechi, & Raju Kannadasan. (2023). Green IoT: A Review and Future Research Directions. Symmetry, 15(3), 757.

[2] Javaid, M., Haleem, A., Singh, R., & Suman, R. (2023). Towards insighting Cybersecurity for Healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications.

[3] Akhilesh, R., Bills, O., Chilamkurti, N., & Chowdhury, M. J. M. (2022). Automated Penetration Testing Framework for Smart-Home-Based IoT Devices. Future Internet, 14(10), 276.

[4] Pattnaik, N., Li, S., & Nurse, J. (2022). Perspectives of Non-Expert Users on Cyber Security and Privacy: An Analysis of Online Discussions on Twitter.

[5] Pandey, P., Wazid, M., Mishra, A. K., Mohd, N., & Singh, D. P. (2023). Need of Cyber Security, Tools, Uses and Future Research. In 7th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 570-574). Tirunelveli, India: IEEE. doi: 10.1109/ICOEI56765.2023.10125792.

[6] Lawu, B. L., Filbert, F., Asih, K., Suharjito, S., & Ohliati, J. (2023, April). A systematic literature review of internet of things cybersecurity. In AIP Conference Proceedings (Vol. 2594, No. 1). AIP Publishing.

[7] Tushir, B., Dalal, Y., Dezfouli, B., & Liu, Y. (2021, April 15). A Quantitative Study of DDoS and E-DDoS Attacks on WiFi Smart Home Devices. IEEE Internet of Things Journal, 8(8), 6282-6292. doi: 10.1109/JIOT.2020.3026023.

[8] Alamer, M., & Almaiah, M. A. (2021). Cybersecurity in Smart City: A Systematic Mapping Study. In 2021 International Conference on Information Technology (ICIT).

[9] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 12(6), 1333.

[10] Cam, N. T., & Trung, N. G. (2023). An Intelligent Approach to Improving the Performance of Threat Detection in IoT. IEEE Access, 11, 44319-44334. doi: 10.1109/ACCESS.2023.3273160.

[11] Jahromi, A. N., Karimipour, H., Dehghantanha, A., & Choo, K. K. R. (2021, September 1). Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems. IEEE Internet of Things Journal, 8(17), 13712-13722. doi: 10.1109/JIOT.2021.3067667.

[12] Haseeb Touqeer, Shakir Zaman, Rashid Amin, Mudassar Hussain, Fadi Al-Turjman, & Muhammad Bilal. (2021). Smart home security: challenges, issues and solutions at different IoT layers. The Journal of Supercomputing, 77.

[13] Anand, P., Singh, Y., & Selwal, A. (2021). Internet of Things (IoT): Vulnerabilities and Remediation Strategies. In P. K. Singh et al. (Eds.), Recent Innovations in Computing (pp. 269-277). Springer. doi: 10.1007/978-981-15-8297-4_22

[14] Tayag, M., Napalit, F., & Napalit, A. (2021). Iot Security: Penetration Testing of White-Label Cloud-Based IoT Camera Compromising Personal Data Privacy. International Journal of Computer Science and Information Technology, 12, 12.

[15] Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., & Lin, J. C.-W. (2022). Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. Sensors, 22(6), 2087.

[16] Xie, T., Tu, G.-H., Yin, B., Li, C.-Y., Peng, C., Zhang, M., Liu, H., & Liu, X. (2021, November 1). The Untold Secrets of WiFi-Calling Services: Vulnerabilities, Attacks, and Countermeasures. IEEE Transactions on Mobile Computing, 20(11), 3131-3147. doi: 10.1109/TMC.2020.2995509.

[17] Wilson, R. (2022). Module 13 in Hands-on ethical hacking and network defense. Cengage Learning.

[18] Etta, V. O., Sari, A., Imoize, A. L., Shukla, P. K., & Alhassan, M. (2022). Assessment and Test-case Study of Wi-Fi Security through the Wardriving Technique. Hindawi Mobile Information Systems.

[19] Murugesan, K., Sriram, S., Kumar, K., & V N, M. (2023). Closed WiFi Hotspot - Truly Hidden Network. In IEEE International Conference on Consumer Electronics (ICCE) (pp. 01-06). Las Vegas, NV, USA: IEEE. doi: 10.1109/ICCE56470.2023.10043474.

[20] Aqeel, M., Ali, F., Iqbal, M. W., Rana, T. A., Arif, M., & Auwul, M. R. (2022). A Review of Security and Privacy Concerns in the Internet of Things (IoT). Hindawi Journal of Sensors.

[21] Asaad, R. R. (2021). Penetration Testing: Wireless Network Attacks Method on Kali Linux OS. Academic Journal of Nawroz University, 10(1), 7–12. doi: 10.25007/ajnu.v10n1a998

[22] Lu, H.-J., & Yu, Y. (2021). Research on WiFi Penetration Testing with Kali Linux. Complexity, 2021, Article ID 5570001. doi: 10.1155/2021/5570001

[23] Wang, L., Abbas, R., Almansour, F., Gaba, G., Alroobaea, R., & Masud, M. (2021). An empirical study on vulnerability assessment and penetration detection for highly sensitive networks. Journal of Intelligent Systems, 30(1), 592-603. doi: 10.1515/jisys-2020-0145

[24] Haq, I. U., & Khan, T. A. (2021). Penetration Frameworks and Development Issues in Secure Mobile Application Development: A Systematic Literature Review. IEEE Access, 9, 87806-87825. doi: 10.1109/ACCESS.2021.3088229.

[25] Tabassum, M., Mohanan, S., & Sharma, T. (2021). Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework. International Journal of Innovation in Computational Science and Engineering, 2(4), 9-22.

[26] Landoll, D. (2021). The security risk assessment handbook: A complete guide for performing security risk assessments. CRC Press.

[27] Leszczyna, R. (2021). Review of Cybersecurity Assessment Methods: Applicability Perspective. Computers & Security, 108, 102376. doi: 10.1016/j.cose.2021.102376.

[28] Duan, X., et al. (2021). Automated Security Assessment for the Internet of Things. In IEEE 26th Pacific Rim International Symposium on Dependable Computing (PRDC) (pp. 47-56). Perth, Australia: IEEE. doi: 10.1109/PRDC53464.2021.00016.

[29] Hu, W., Chang, C.-H., Sengupta, A., Bhunia, S., Kastner, R., & Li, H. (2021). An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 40(6), 1010-1038. doi: 10.1109/TCAD.2020.3047976.

[30] Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity Risk Assessment in Smart City Infrastructures. Machines, 9(4), 78.

[31] Bishop Fox. (2023). 8 Network Pen Testing Tools. Retrieved from https://bishopfox.com/blog/8-network-pen-testing-tools (Accessed on 29th August 2023).
[32] Infosec Institute. (2021). 13 Popular Wireless Hacking Tools. Retrieved from https://resources.infosecinstitute.com/topics/hacking/13-popular-wireless-hacking-tools/ (Accessed on 29th August 2023).
[33] Hacking Articles. (2021). Wireless Penetration Testing: Wifite. Retrieved from https://www.hackingarticles.in/wireless-penetration-testing-wifite/ (Accessed on 29th August 2023).
[34] Wilson, R. (2022). Module 11 in Hands-on ethical hacking and network defense. Cengage Learning.
[35] Le, T. H., Chen, H., & Babar, M. A. (2022). A survey on data-driven software vulnerability assessment and prioritization. ACM Computing Surveys, 55(5), 1-39.
[36] Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2022). Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. Applied Sciences, 13(1), 395.
[37] Færøy, F. L., Yamin, M. M., Shukla, A., & Katt, B. (2023). Automatic Verification and Execution of Cyber Attack on IoT Devices. Sensors.
[38] Thant, K. S., & Tin, H. H. K. (2023). The Impact of Manual And Automatic Testing On Software Testing Efficiency And Effectiveness, 88-93.
[39] Alhamed, M., & Rahman, M. M. H. (2023). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. Applied Sciences, 13(12), 6986.
[40] Fatima, A., Khan, T., Mohamed Abdellatif, T., Zulfiqar, S., Asif, M., Safi, W., Al Hamadi, H., & Al-Kassem, A. (2023). Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat, 1-8.
[41] Cathcart, J., & Khan Mohd, T. (2023, February). Password Hacking Analysis of Kali Linux Applications. In International Conference on Intelligent Sustainable Systems (pp. 815-828). Singapore: Springer Nature Singapore.
[42] Norman, A. T. (2023). Computer Hacking Beginners Guide How To Hack Wireless Network, Basic Security And Penetration Testing, Kali Linux, Your First Hack. Jamil Ahmed.
[43] Singh, S., Srivastava, G., Kumar, S., & Singh, S. (2023). Penetration Testing and Security Measures To Identify Vulnerability Inside The System. IOSR Journal of Computer Engineering, 25, 50-64.
[44] Greco, C., Fortino, G., Crispo, B., & Choo, K.-K. R. (2023). AI-enabled IoT penetration testing: state-of-the-art and research challenges. Enterprise Information Systems, 17(9). doi: 10.1080/17517575.2022.2130014
[45] Tyagi, Y., Bhardwaj, S., Shekhar, S., & P, A. (2023). Efficient Vulnerability Assessment and Penetration Testing: A Framework for Automation. In International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES) (pp. 553-557). Greater Noida, India: IEEE. doi: 10.1109/CISES58720.2023.10183397.