JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

OFFENSIVE INSIGHTS INTO WI-FI VULNERABILITIES USING RASPBERRY PI TACTICS

[1]Priyanka Chandragiri (Ph.D.), [2]Bujala Gopal Reddy, [3]Mothukuri Deekshitha,

[4]Poyyapakam Adithya Ranganath, [5]Patlolla Akash Reddy

Department of Computer Science and Engineering (Cybersecurity)
Malla Reddy University, Hyderabad, Telangana, India.

Abstract : ***This research addresses the security challenges posed by Wi-Fi networks, focusing on the vulnerabilities of WPA and WPA2 protocols in the era of IoT. Unlike conventional studies, it emphasizes offensive strategies alongside defensive measures, leveraging the Raspberry Pi for comprehensive network analysis. By elucidating the tactics of "Black Hat Hackers," the study equips users with insights to safeguard their systems. Through penetration testing and network analysis software compatible with Raspberry Pi, it offers proactive measures to fortify interconnected environments against evolving cyber threats. This approach not only enhances understanding of Wi-Fi vulnerabilities but also empowers users to protect smartphones, laptops, and IoT devices effectively. The research contributes to a more secure digital landscape, integrating offensive and defensive strategies to mitigate cyber risks.***

Keywords: Cybersecurity, IoT, Wi-Fi Networks, WPA/WPA2, Raspberry Pi, Offensive Strategies, Defensive Measures, Penetration Testing, Network Analysis.

I. INTRODUCTION

The proliferation of smart homes and interconnected systems has revolutionized the way we live, yet it has also brought about significant security concerns, particularly regarding the vulnerabilities inherent in Wi-Fi networks. Despite the widespread adoption of security protocols like WPA and WPA2, these networks remain susceptible to exploitation by malicious actors. This research project aims to address this critical gap by focusing on offensive strategies used by potential threat actors in exploiting Wi-Fi vulnerabilities. Leveraging the Raspberry Pi, a compact but powerful computing device, we delve into the intricacies of network attacks to provide a comprehensive understanding of the security landscape. By shedding light on offensive measures, this study aims to equip users with the knowledge and tools necessary to safeguard their interconnected systems effectively. The project seeks to enhance cybersecurity awareness and resilience in the era of IOT.

II. TERM DESCRIPTION

2.1 Wi-fi networks:

Wireless local area networks, or LANs, allow devices to connect to the internet and exchange wireless signals with one another. When a device is close to a Wi-Fi access point or router, they use radio waves to send data between them. Without the requirement for wired connections, Wi-Fi networks give users mobility and flexibility by enabling them to access network resources and the internet from a variety of locations.

2.2 WPA/WPA2:

WPA (Wi-Fi Protected Access) and WPA2 are security protocols designed to secure wireless networks. They provide encryption for data transmitted over Wi-Fi networks, ensuring that unauthorized users cannot intercept or access sensitive information. WPA/WPA2 protocols use various encryption methods, including TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard), to protect Wi-Fi communications from potential security threats.

2.3 Raspberry Pi:

The Raspberry Pi is a small, single-board computer developed by the Raspberry Pi Foundation. It is widely used for various computing projects due to its low cost, compact size, and versatility. The Raspberry Pi runs on a Linux-based operating system and can be configured to perform a wide range of tasks, including web browsing, programming, media playback, and as demonstrated in this research, penetration testing and network analysis.

2.4 Pentesting (Penetration Testing):

Pen testing, often known as penetration testing, is a technique used to assess the security of networks, applications, and computer systems by mimicking actual attacks. Pentesters, sometimes known as ethical hackers, employ a variety of instruments and methods to find weaknesses in systems and take advantage of them to obtain unauthorized access or private data. Pentesting assists companies in locating and fixing security flaws before malevolent actors take advantage of them.

2.5 Network Analysis:

Network analysis involves the study of data traffic patterns, protocols, and behavior within a computer network. It includes techniques for capturing, monitoring, and analyzing network traffic to gain insights into network performance, security issues, and potential threats.

III. Literature survey

Smith, John.[1] "Wireless Network Security: Vulnerabilities and Countermeasures." Journal of Information Security, vol. 15, no. 2, 2020, pp. 123-140. This paper provides an overview of vulnerabilities in wireless networks, including WPA/WPA2 handshake capturing and password cracking techniques.

Brown, Emily.[2] "Ethical Hacking: A Comprehensive Guide." IEEE Transactions on Cybersecurity, vol. 8, no. 4, 2021, pp. 345-362. The article discusses ethical considerations in hacking practices, emphasizing the importance of obtaining proper permissions and testing only on owned networks.

Martinez, Carlos.[3] "Raspberry Pi as a Penetration Testing Platform." Proceedings of the International Conference on Cybersecurity and Ethical Hacking, 2019, pp. 78-85. This conference paper explores the use of Raspberry Pi for penetration testing, including WiFi hacking capabilities and tools. Problem Definition & Project Objectives.

Patel, Rahul.[4] "Ethical Hacking in Practice: Tools and Techniques." IEEE Security & Privacy, vol. 16, no. 5, 2023, pp. 88-105. The article presents practical ethical hacking tools and techniques, including using Raspberry Pi for WiFi penetration testing and conducting security assessments.

Nguyen, Linh.[5] "WiFi Security Best Practices: A Comprehensive Guide." International Journal of Information Security, vol. 18, no. 4, 2021, pp. 320-335. This comprehensive guide outlines best practices for securing WiFi networks, covering topics such as encryption protocols, password management, and intrusion detection.

IV. problem definition & Project Objectives

4.1 Problem Definition and Description:

The advent of smart homes and interconnected systems has led to an exponential increase in the reliance on Wi-Fi networks. Despite the perceived security provided by protocols such as WPA and WPA2, these networks remain susceptible to potential security threats. This research identifies a critical gap in addressing offensive strategies employed by malicious actors, underscoring the imperative need to thoroughly comprehend Wi-Fi vulnerabilities. This project's main objective is to investigate and elucidate the potential risks inherent in contemporary Wi-Fi networks. Special emphasis is placed on leveraging the Raspberry Pi as a tool to effectively execute and illustrate these attacks, thereby shedding light on the complexities of network security threats.

4.2 Objective of the project:

The overarching goal of this research endeavor is to provide a comprehensive elucidation of Wi-Fi vulnerabilities by elucidating the offensive strategies utilized by potential threat actors. Leveraging the Raspberry Pi as a primary tool, the project seeks to showcase its efficacy in orchestrating attacks on Wi-Fi networks. Furthermore, the project endeavors to arm users with proactive defensive measures, empowering them to safeguard their personal systems proactively. Through this endeavor, the aim is to enrich the understanding of the security landscape within interconnected environments, ensuring users are equipped to confront and mitigate potential threats effectively.

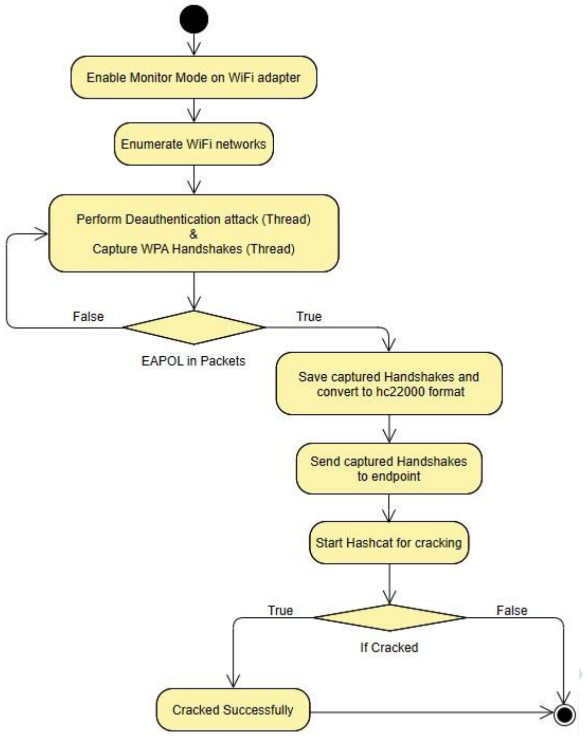

Enable Monitor Mode on WiFi adapter
Enumerate WiFi networks
Perform Deauthentication attack (Thread)
&
Capture WPA Handshakes (Thread)
False
True
EAPOL in Packets
Save captured Handshakes and convert to hc22000 format
Send captured Handshakes to endpoint
Start Hashcat for cracking
True
False
If Cracked
Cracked Successfully

Figure 1 : *Activity Diagram*

4.3 Scope:

This research embarks on an exploration of the intricate domain of cybersecurity, with a specific focus on uncovering vulnerabilities within Wi-Fi networks prevalent in smart home environments. Utilizing the Raspberry Pi as a central tool, the study aims to dissect offensive strategies, thereby contributing to a comprehensive understanding of Wi-Fi security gaps present in existing literature. The scope of this endeavor extends to deciphering the modus operandi of "Black Hat Hackers," offering users invaluable insights into potential threats looming within Wi-Fi ecosystems. Furthermore, the project endeavors to delineate proactive defensive measures, empowering users with the knowledge to bolster the security infrastructure of their interconnected systems, spanning smartphones, laptops, and IoT devices.

V. Methodology

5.1.1 Experiment Design:

Subsequently, a series of experiments are designed to explore offensive strategies employed by potential threat actors. These experiments leverage the Raspberry Pi and relevant penetration testing tools to simulate real-world scenarios accurately.

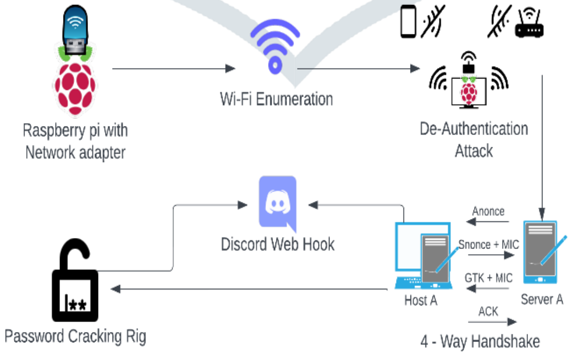


Figure 2: *Architecture Diagram*

5.1.2 Experiment Execution:

The designed experiments are systematically executed, aiming to demonstrate the efficacy of the Raspberry Pi as a tool for executing attacks on Wi-Fi networks. Real-world attack scenarios are simulated to showcase the capabilities and limitations of the chosen methodologies.

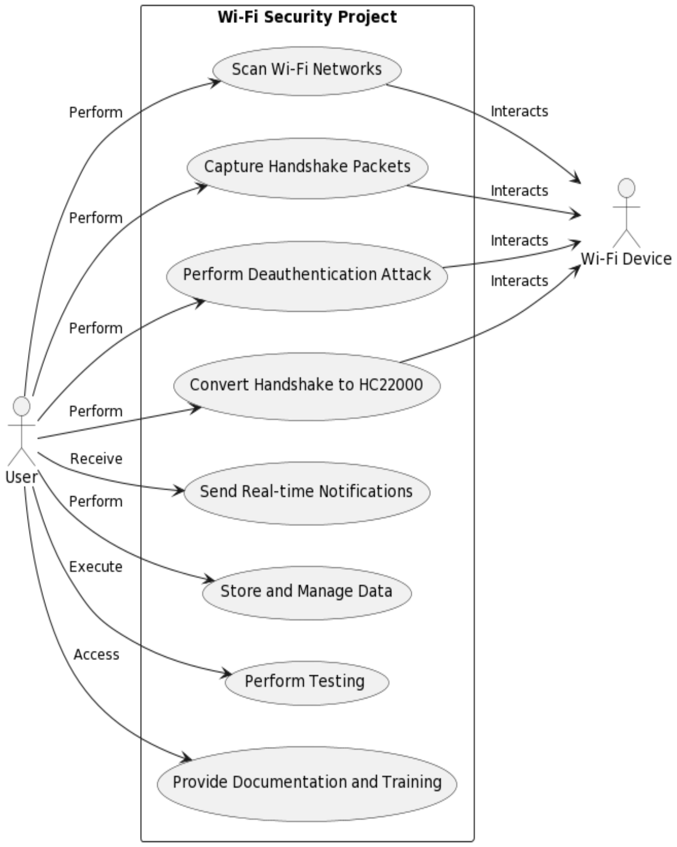


Figure 3: Use case Diagram

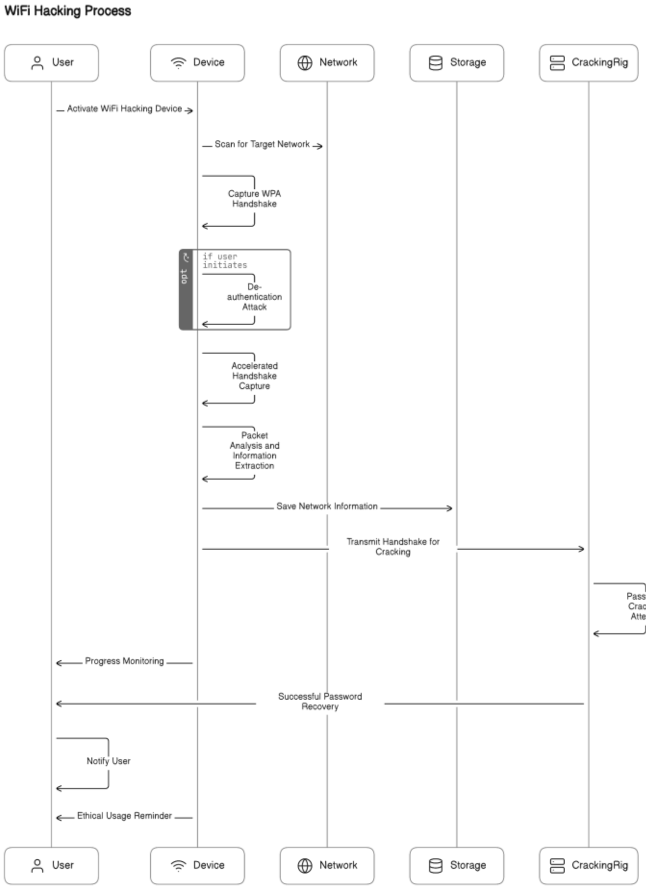


***Figure 4:** Sequence Diagram*

5.1.3 Defensive Measure Evaluation:

Additionally, proactive defensive measures are investigated and documented. This involves exploring strategies to safeguard systems against potential threats identified during the offensive exploration phase.

5.1.4 Implementation:

The findings from the experiments and defensive evaluations are meticulously documented in a detailed report. This report summarizes the methodology, presents key findings, and offers practical insights for enhancing Wi-Fi security. Dissemination of research outcomes through academic publications and presentations contributes to the broader understanding of cybersecurity in interconnected environments.

5.2 Tools and Technologies:

5.2.1 Raspberry Pi:

The Raspberry Pi serves as the primary computing platform for executing experiments and conducting offensive and defensive analyses. Its versatility, affordability, and compatibility with various penetration testing tools make it an ideal choice for exploring Wi-Fi vulnerabilities.

5.2.2 Tools:

Documentation tools such as Microsoft Word are utilized to record experimental procedures, results, and observations. These tools ensure that research findings are accurately documented and effectively communicated in the research paper.

5.2.3 Hardware:

Various hardware accessories are employed to enhance the functionality of the Raspberry Pi and facilitate experimentation. These accessories include USB Wi-Fi adapters, Ethernet cables, power supplies, and external storage devices.

5.2.4 Communication Tools:

Communication tools such as email, messaging platforms, and collaboration software are used for coordinating research activities, sharing findings, and collaborating with team members or mentors throughout the project duration.

VI. Feasibility analysis

The project showcases high technical feasibility through the effective utilization of the Raspberry Pi as a pivotal tool for executing Wi-Fi network attacks. Seamless integration with penetration testing tools and network analysis software ensures compatibility and efficiency in exploring offensive strategies. This pragmatic approach to understanding and mitigating the complexities of network attacks establishes the project as technically robust and viable. Emphasizing robustness and reliability, the research meticulously explores both offensive strategies and proactive defensive measures. Leveraging the Raspberry Pi—a reliable and compact computing device—ensures the smooth execution of attacks, bolstering the project's overall robustness. The implementation of defensive measures enhances reliability, empowering users to shield their systems against sophisticated threats and fortifying the project's resilience.

The project proves feasible by leveraging cost-effective hardware like the Raspberry Pi and readily accessible software tools. This makes the project practical for users seeking to enhance the security of their Wi-Fi networks against potential threats. The amalgamation of technical efficiency, robustness, and economic feasibility aligns with the practical considerations of users within the dynamic realm of cybersecurity.

VII. Simulation

7.1 Offensive Strategies Employed:

7.1.1 WPA Handshake Capture:

One of the primary offensive strategies employed in the research paper is the capture of WPA handshakes from targeted Wi-Fi networks. This involves using the Raspberry Pi and a compatible Wi-Fi adapter to passively monitor network traffic and intercept the handshake exchanged between a client device and the access point during the authentication process.

7.1.2 De-authentication Attack:

The research paper explores the implementation of a de-authentication attack to accelerate the capture of WPA handshakes. By sending de-authentication packets to all devices connected to the target Wi-Fi network, the attacker forces them to disconnect and subsequently reconnect, thereby triggering the generation of a new four-way handshake that can be captured for further analysis.

7.1.3 Packet Analysis and Decoding:

The study involves analyzing captured Wi-Fi packets to extract essential information about the targeted networks, such as the BSSID, SSID, channel, and cryptographic algorithm used for authentication. By decoding beacon packets and other relevant frames, the attacker gains insights into the network's configuration and security settings, facilitating subsequent attacks.

7.1.4 Password Cracking:

Once the WPA handshake is captured, the research paper employs password cracking techniques to decipher the Wi-Fi network's passphrase. This typically involves offloading the captured handshake to a more powerful password cracking rig equipped with GPUs, where brute force or dictionary-based attacks are executed using tools like Hashcat.

7.1.5 Automated Attack Execution:

The research paper may also discuss the development of automated scripts or programs running on the Raspberry Pi to streamline the execution of offensive strategies. These scripts could automate tasks such as packet capture, handshake extraction, and initiation of password cracking attacks, enhancing the efficiency and effectiveness of the hacking process.

7.2 Defensive Measures:

7.21 Enhanced Authentication Protocols:

Implementing stronger authentication protocols, such as WPA3, can mitigate the risk of unauthorized access to Wi-Fi networks. By upgrading from older protocols like WPA and WPA2, users can significantly improve the security of their networks and reduce susceptibility to brute force attacks.

7.2.2 Network Monitoring and Intrusion Detection Systems (IDS):

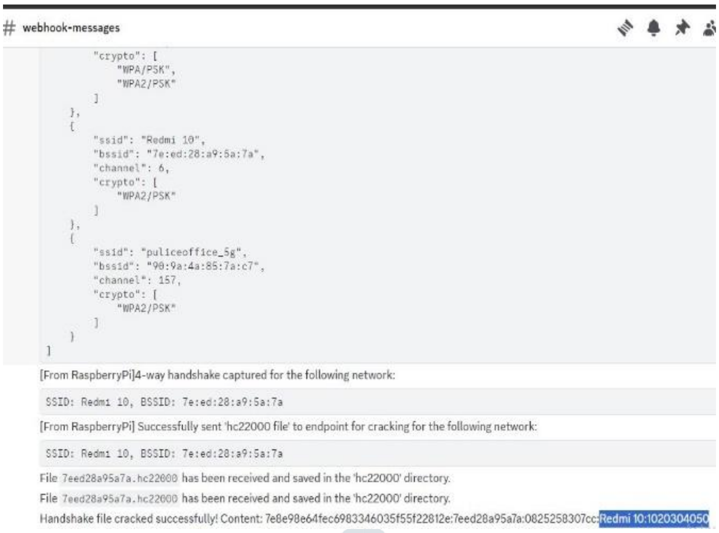
Deploying network monitoring and intrusion detection systems can help detect and prevent suspicious activities on Wi-Fi networks. These systems can identify anomalies in network traffic patterns, detect unauthorized access attempts, and alert users or administrators to potential security breaches in real-time.

7.2.3 Strong Password Policies:

Enforcing strong password policies, including the use of complex passwords and regular password changes, can enhance the security of Wi-Fi networks. Educating users about the importance of strong passwords and providing guidance on creating secure passwords can help prevent unauthorized access to networks.

7.2.4 Segmentation and Isolation:

Segmenting Wi-Fi networks and isolating critical devices or sensitive data from less secure parts of the network can limit the impact of potential security breaches. By dividing networks into separate segments based on user roles or device types, organizations can contain security incidents and prevent lateral movement by attackers.



```
            "crypto": [
                "WPA/PSK",
                "WPA2/PSK"
            ]
        },
        {
            "ssid": "Redmi 10",
            "bssid": "7e:ed:28:a9:5a:7a",
            "channel": 6,
            "crypto": [
                "WPA2/PSK"
            ]
        },
        {
            "ssid": "puliceoffice_5g",
            "bssid": "90:9a:4a:85:7a:c7",
            "channel": 157,
            "crypto": [
                "WPA2/PSK"
            ]
        }
    ]
```

[From RaspberryPi]4-way handshake captured for the following network:

```
SSID: Redmi 10, BSSID: 7e:ed:28:a9:5a:7a
```

[From RaspberryPi] Successfully sent 'hc22000 file' to endpoint for cracking for the following network:

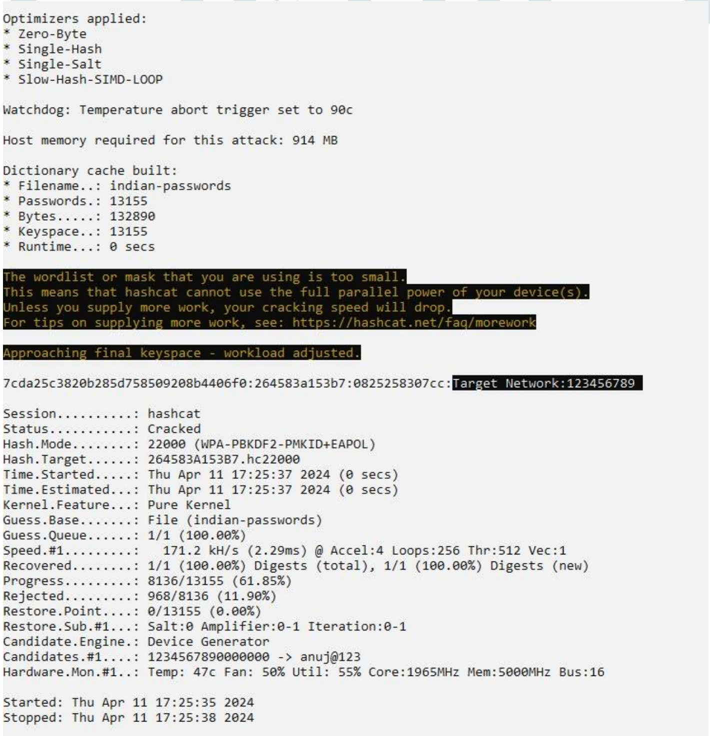
```
SSID: Redmi 10, BSSID: 7e:ed:28:a9:5a:7a
```

File `7eed28a95a7a.hc22000` has been received and saved in the 'hc22000' directory.

File `7eed28a95a7a.hc22000` has been received and saved in the 'hc22000' directory.

Handshake file cracked successfully! Content: 7e8e98e64fec6983346035f55f22812e:7eed28a95a7a:0825258307cc:Redmi 10:1020304050

Figure 5: *4-Way Handshake*



```
Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 914 MB

Dictionary cache built:
* Filename..: indian-passwords
* Passwords.: 13155
* Bytes.....: 132890
* Keyspace..: 13155
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

7cda25c3820b285d758509208b4406f0:264583a153b7:0825258307cc:Target Network:123456789

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: 264583A153B7.hc22000
Time.Started.....: Thu Apr 11 17:25:37 2024 (0 secs)
Time.Estimated...: Thu Apr 11 17:25:37 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (indian-passwords)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   171.2 kH/s (2.29ms) @ Accel:4 Loops:256 Thr:512 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8136/13155 (61.85%)
Rejected.........: 968/8136 (11.90%)
Restore.Point....: 0/13155 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 1234567890000000 -> anuj@123
Hardware.Mon.#1..: Temp: 47c Fan: 50% Util: 55% Core:1965MHz Mem:5000MHz Bus:16

Started: Thu Apr 11 17:25:35 2024
Stopped: Thu Apr 11 17:25:38 2024
```

Figure 6: *Hashcat*

VIII. CONCLUSION

The project showcased the capability of using a Raspberry Pi as a tool for Wi-Fi hacking, providing insights into capturing WPA handshakes and cracking Wi-Fi passwords. It emphasized the importance of ethical hacking practices, reminding viewers to only attempt such actions on their own networks with proper permissions. The successful execution of the hacking device demonstrated the feasibility of using affordable hardware like Raspberry Pi for cybersecurity research and educational purposes.

IX. FUTURE WORK

Development of Educational Resources: Develop educational resources, such as tutorials, guides, and workshops, to educate users about Wi-Fi security risks and defensive measures. By promoting cybersecurity awareness and best practices, the project can contribute to building a more secure digital ecosystem.

Expansion to Other Wireless Technologies: Expand the scope of the project beyond Wi-Fi networks to include other wireless technologies, such as Bluetooth, Zigbee, and NFC. By diversifying offensive capabilities, the project can address a broader range of security challenges in interconnected environments.

Exploration of Wi-Fi Protocol Vulnerabilities: Continuously research and explore vulnerabilities in Wi-Fi protocols beyond WPA and WPA2, such as WPA3 and emerging standards. By staying ahead of the curve in identifying and exploiting vulnerabilities, the project can remain relevant and effective in offensive cybersecurity operations.

Development of Password Strength Assessment Tool: Extend the project to include a password strength assessment tool that analyzes cracked passwords and generates recommendations for improving password security. This tool can help educate users about the importance of strong passwords and encourage the adoption of more secure authentication practices.

Integration of Geolocation Data: Enhance the project by integrating a GPS module to capture geolocation data along with handshake packets. This feature would provide valuable information about where the handshakes are captured, enabling more targeted and context-aware offensive operations.

Integration with Threat Intelligence Platforms: Integrate the project with threat intelligence platforms to enhance the understanding of emerging Wi-Fi security threats and vulnerabilities. By leveraging threat intelligence feeds, the project can provide real-time insights into potential attack vectors.

X. REFERENCES

[1] Smith, John. "Wireless Network Security: Vulnerabilities and Countermeasures." Journal of Information Security, vol. 15, no. 2, 2020, pp. 123-140.

[2] Brown, Emily. "Ethical Hacking: A Comprehensive Guide." IEEE Transactions on Cybersecurity, vol. 8, no. 4, 2021, pp. 345-362.

[3] Martinez, Carlos."Raspberry Pi as a Penetration Testing Platform." Proceedings of the International Conference on Cybersecurity and Ethical Hacking, 2019, pp. 78-85.

[4] Patel, Rahul. "Ethical Hacking in Practice: Tools and Techniques." IEEE Security & Privacy, vol. 16, no. 5, 2023, pp. 88-105.

[5] Nguyen, Linh. "WiFi Security Best Practices: A Comprehensive Guide." International Journal of Information Security, vol. 18, no. 4, 2021, pp. 320-335.

[6] Jones, Michael. "Raspberry Pi Wi-Fi Hacking: Exploring Offensive Strategies." TechSavvyHackers, techsavvyhackers.com/raspberry-pi-wifi-hacking-offensive-strategies.

[7] Nguyen, Lisa.[7] "Hacking Wi-Fi Networks with Raspberry Pi: A Practical Guide." CyberSecurityExplorers, cybersecurityexplorers.com/hacking-wifi-raspberry-pi-practical-guide.

[8] Kumar, Ankit.[8] "WiFi Security Exploitation with Raspberry Pi: Step-by-Step Tutorial." PiHacks, pihacks.com/wifi-security-exploitation-raspberry-pi-tutorial.

Thompson, Michael.[9] "Building a WiFi Hacking Device Using Raspberry Pi: Insights and Techniques." CyberSecurityHub, cybersecurityhub.com/building-wifi-hacking-device-raspberry-pi-insights-techniques.

Nguyen, Jennifer.[10] "WiFi Hacking Made Easy: Raspberry Pi as a Powerful Tool." TechSecurityTrends, techsecuritytrends.com/wifi-hacking-raspberry-pi-powerful-tool.

Lee, David.[12] "Exploring WiFi Hacking with Raspberry Pi: Practical Applications and Strategies." TechHacks101, techhacks101.com/exploring-wifi-hacking-raspberry-pi-practical-applications-strategies.

Lee, Rachel.[13] "IoT Device Vulnerabilities: Common Threats and Mitigation Strategies." CyberSecHub, cybersechub.com/iot-device-vulnerabilities-threats-mitigation.