Philippines' Free Wi-Fi Roll-out Project: Safe or Not?

Eric B. Blancaflor*, Eli Christ Paula C. Castillo, Jan Miguel N. Coretico, Geremie B. Rubiano, and Angela Marie D. Tobias

School of Information Technology, Mapua University, Philippines; Email: {ecpcastillo, jmncoretico, gbrubiano, amdtobias}@mymail.mapua.edu.ph
*Correspondence: ebblancaflor@mapua.edu.ph

***Abstract*—Free Wi-Fi networks are widely implemented in public areas to provide benefits for the people. This paper focuses on the vulnerabilities around Wi-Fi networks that people are unaware of. Discussing the risks of using free internet is viable as public places in the Philippines have started implementing free Wi-Fi networks. Along with this, the Department of Information and Communication Technology (DICT) of the Philippines is expanding the number of free Wi-Fi to help the Filipinos adjust to the new normal caused by the pandemic. With the increase of internet access, Filipinos should be informed of the risks they may have. In this study, the security of free Wi-Fi has been exploited through various technical methods of Wi-Fi penetration testing. The study simulated penetration testing using the Kali Linux in a virtual environment from consented Wi-Fi owners. The overall result of the study shows that free Wi-Fi networks in public areas may not be safe. Free Wi-Fi users must be aware of the risk; hackers accessing their devices and inevitably stealing their private personal information.**

***Keywords*—wireless network, penetration test, kali Linux introduction**

I. Introduction

In today's current situation, internet becomes an essential part of our lives. Different services in this infrastructure should reach if not all but at least most of the target users. Because of this need to stay connected, places in the Philippines, installed free public Wi-Fi connections in nearby areas. This effort, at least helps conusmers who cannot afford internet subscriptions at home, and a moving user still be able to access internet services he/she needs. PLDT and Smart, two of the biggest internet service providers in the country, helped on this project because they wanted to create a seamless and connected environment [1].

This paper talks about the topic of free public Wi-Fi spots, and it aims to explore the question of the safety of the massive rollout of public Wi-Fi connections to the public.

A. Background of the Study

Free Wi-Fi has long been implemented in some commercial establishments in the Philippines. The purpose of providing free Wi-Fi in public areas is to give entertainment, which encourages customers to remain longer and attract customers. Now, the Philippines' Department of Information and Communication Technology (DICT) is expanding the reach of free Wi-Fi. They announced to install 6,000 free Wi-Fi sites to public Wi-Fi in schools, government buildings, and other public places to help transition to remote work and education to the new normal caused by the global pandemic [1].

However, issues arise, as free Wi-Fi may easily be exploited to disseminate harmful software, collect personal information, and hack into network-connected devices. This review paper tackles the security of Filipino users in using Free Wi-Fi, whether it is safe or not. Users are focused on the benefits of free Wi-Fi. Still, they are unaware of possible private credentials that public Wi-Fi networks can access through their devices. Users are more susceptible to such cyber-attacks when using public Wi-Fi [2]. It is an easy opportunity for cybercriminals to access target-sensitive data. Some Filipinos are unaware of the risks that come with the usage of free public Wi-Fi. The subject matter of the study will revolve around the vulnerabilities that come along with using public Wi-Fi through ethical hacking.

B. Purpose of the Study

The purpose of the study is to determine the security capabilities of free Wi-Fi. The study will coordinate with free Wi-Fi owners and local government units associated with the rollout of free Wi-Fi to conduct Wi-Fi Hacking and other penetration testing techniques. Upon successful penetration, the study will provide an in-depth discussion on the possible activities that attackers could perform. It would help identify the effect of using free public Wi-Fi and tackle data privacy, vulnerabilities, and keeping a secured online community.

II. Literature Review

Free Wi-Fi networks offer a practical and cost-effective way to access the internet in areas where wired

Manuscript received February 17, 2022; revised March 25, 2022; accepted April 16, 2022; published February 8, 2023.

infrastructure is difficult to deploy. However, according to Zhang *et al.*, using mobile devices in public settings is risky since attackers can access personal information like PINs, security codes, etc. When a user enters a password, an attacker can gain personal information by observing the user's typing movement on a website's state information [3]. Some wireless networks often do not have user authentication or identity required, allowing attackers or hackers to attack their victims. In the study of Maimon *et al.*, he states that people who use a public Wi-Fi network should employ protective measures to secure their data from hostile actors on the same network and others who are literally and metaphorically snooping over their shoulders [4].

Lusekelo Kibona and Hassana Ganame visited different reviews and highlighted that there are still concerns in totally securing the network against attacks, threats, and vulnerabilities. Their study addressed the various security risks and ways of securing wireless networks by proposing network security solutions [5]. This study also tackles strategies for reducing current problems and ensuring security users' privacy and security. Their study, Wireless Network Security Challengers, Threats, and Solutions A Critical Review, is the closest published work to what is conducted by the researchers because both papers delve deep into Wi-Fi technology pros and cons. The researchers in both publications also bring up the safety of this technology to its users. The difference between both works is that Kibona and Ganame's work tackles the broader side of Wireless Network technology. In contrast, ours tackles the specific side of it, specifically Wi-Fi.

A relevant study that is important to mention is a study by Choi *et al.*; Their study came to be with the dramatic increase of public Wi-Fi available in the last decade for the United States [6]. Despite widespread knowledge about vulnerabilities of using public Wi-Fi, most people connect without hesitation—this study investigates this phenomenon. Through 1313 respondents, the researchers found that factors such as avoidance motivation, risk averting propensity, and intrinsic & extrinsic motivations affect intention to use public Wi-Fi [6].

A. *Potential Attacks on Free Wi-Fi Network*

Studies conducted by the Kaspersky Security Network and Admed Lofty discovered that Wi-Fi hotspots in public places are becoming increasingly popular across the world. They also learned that nearly a quarter of the world's public Wi-Fi hotspots are not using encryption, and 60% of participants are unaware of the risks of utilizing an untrusted network and feel their personal information is secure, respectively. It is critical to ensure that the Wi-Fi network users connect to is encrypted for data safety. However, risks are still present even if a hotspot uses encryption [7, 8]. Using public free Wi-Fi in public areas can expose users' sensitive information. Most people aren't aware of the risks of using public Wi-Fi. The following are some of the risks that a user could encounter:

- Theft of Personal Information

The hackers may obtain private information on users' devices such as log-in credentials, pictures, financial information, and personal data. Once the hacker gets in, they can damage finances and damage the user's reputation [9].

- Man in the Middle Attacks

This attack occurs when impersonating a legitimate Wi-Fi service to trick the user into connecting to that specific Wi-Fi. Hackers unintentionally implement Secure Sockets Layer (SSL) to reroute all interaction into their channels to listen to transmitted network activity [10].

- Malware Distribution

The hacker could implement malware on public Wi-Fi users' devices. It can be trojan horses, worms, viruses, adware, and ransomware. If users connect to a public Wi-Fi network, they may inject malware on the connected devices if it is not adequately protected.

- Packet Sniffing

Users on the same Wi-Fi network can use a packet sniffer tool to listen to what you send and receive. This tool may be used for both good and bad objectives. An organization could employ a packet sniffer to identify and address security flaws with its system. However, hackers can obtain users' personal information, which is the disadvantage of packet sniffing [9], [10].

III. Methodology

Fig. 1 shows the technical steps the researchers used to conduct the Wi-Fi penetration test. It compromises setting the wireless network card to monitor mode, scanning, gathering data from nearby networks, listening, and monitoring targeted network, Wi-Fi password cracking attacks, and simulated attacks on connected users to the network.

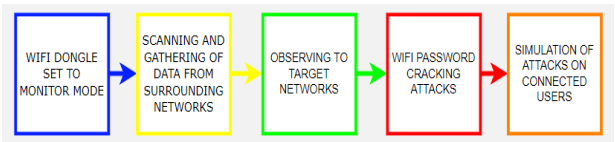

Figure 1. Steps on Wi-Fi penetration test.

A. *Wi-Fi Dongle Set to Monitor Mode*

The Wi-Fi dongle is set to monitor mode to automatically look for Wi-Fi data networks. It is the preparation stage that scans all packets around it. The command airmon-ng start [interface] will be used to put the Wi-Fi dongle to monitor mode. This script is part of the aircrack suite that is typically used to test the network security of Wi-Fis. The following command is iwconfig to determine if the Wi-Fi card has been changed to monitor mode.

B. *Scanning and Gathering of Data from Surrounding Networks*

This step primarily consists of gathering information on wireless networks and devices within reach of penetration testing. This step will show the list of wireless networks, and network devices. By setting up

the card to monitor mode to scan all the data packets, this step aims to gather data from nearby networks. It solely monitors traffic received via wired and wireless networks.

C. Observing of Target Networks

Upon gathering the information needed by the attacker, this step highlights the information that could be obtained from the targeted networks. The connected devices and their respective information could be obtained by targeting the chosen networks. Using the script, *airodump-ng --bssid [bssid] --channel [channel] --write [file-name] [interface]*, this enables the attacker store the data from the targeted client in a Wi-Fi network.

D. Wi-Fi Password Cracking Attacks

The attacker will execute the penetration test in this step. Two brute force methods are used in Wi-Fi password cracking attacks on targeted networks. The first is cracking the password using a wordlist (crunch), a tool for constructing pre-installed wordlists on Kali Linux. It's used to create custom keywords with the use of wordlists. The attackers will execute the airodump-ng and aireplay-ng commands to deauthenticate a connected device. This attack focuses on the connection between the router and the device, and to capture the full WPA. Then, a dictionary attack will be used to obtain access to a password-protected system. In this case, the attacker used the command *crunch [min] [max] [characters=lower|upper|numbers|symbols] -o filename* to create a disk space of length and characters. The attacker then used the aircrack-ng command to crack the password, then generating PMK using handshake and wordlist file will result in password cracking result.

E. Simulation of Attacks of Connected Users

The attacker may now connect to the target access point of the target network after completing the four steps in obtaining the password. The final step involves simulating attacks on users connected to the network. But before proceeding to the attacks, using various scanning or listening tools, the attackers will obtain detailed information on the target users connected to the free Wi-Fi network.

In this step, the attackers in this study utilized Netdiscover to find the target network's live clients, IP and MAC addresses, and subnets. The attackers also utilized Zenmap to obtain lists of hosts, operating systems, connected devices, services, and other information. After scanning the target network's comprehensive information, the attackers will execute Man-in-the-Middle attacks.

ARP Poisoning is the initial attack it is executed in a Local Area Network. It mostly involves sending malicious ARP packets to a default gateway on a LAN to modify the IP to the MAC address table The next attack is DNS Poisoning, and it works by substituting a malicious address for an Internet address to compromise an internet server's domain name system database. This is when an attacker leads a user to a fraudulent website to provoke their victims to access it, and the attackers are impersonating the nameservers.

IV. Experimentation and Results

This study started with informing and getting consent from the necessary personnel of the locations where the attackers simulated the penetration testing. The study chose a mall in Taguig, and in Bataan, as both locations have an abundance of free Wi-Fi. The testing was used with the Kali Linux machine in a virtual environment. Both attackers used the VMware virtualization technology and 300Mbps Wireless N USB Adapter TL-WN821N.

A. Setting up of Wi-Fi Card

The wireless adapter used is by default set to Managed Mode, which only receives data sent to the hacker with the computer's MAC address. The Wi-Fi card should be in Monitor Mode to capture all the data within the Wi-Fi range. The command for this is airmon-ng start [interface]. Using the iwconfig helps determine if the connection of the wireless card to the machine is successful, frequency, interface name, and checks its activation status.

B. Information Gathering

Upon connecting the wireless card to the virtual machine, it is changed into monitor mode to capture all of the data packets it can possibly obtain. The nearest wireless network and the connected clients can be obtained by running the airodump-ng [interface] command. Other network information is masked, and the data from the network used in the experiment is provided, as depicted in Fig. 2. The physical address, encryption mode, channel of the target AP, and username are all collected.

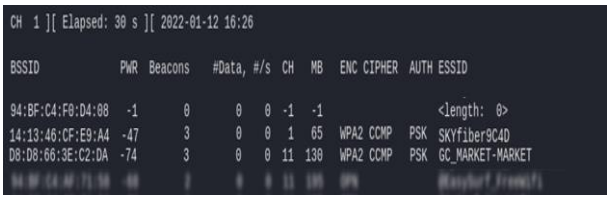

Figure 2. Targeted access point (SKYFIBER9C4D).

C. Listening to Targeted Devices

After running the airodump, the attackers targeted the consented individuals' network to attack. The MAC address and other data of the connected clients can be acquired here. Command used in this part are: airodump-ng --bssid [bssid] --channel [channel] --write [file-name] [interface]

D. Wi-Fi Password Attack

To further show the importance of knowing the vulnerabilities of the Wi-Fi network, in this study two brute force methods on the target wireless networks used are: Cracking the password using wordlist and using hashcat (GPU). Both methods require capturing handshake packets, and by capturing the four-way handshake between the client and wireless network, aircrack commands, and GPUs are used to identify the passwords set.

E. Brute Force Attacks

Researchers deauthenticated a connected device to capture the full WPA handshake. The commands below are used, and Fig. 3 is the results.

airodump-ng --bssid [bssid] --channel [channel] --write [file-name] [interface]

aireplay-ng --deauth [deauth packets number] -a [networkBSSID] -c [targetBSSID] [interface]

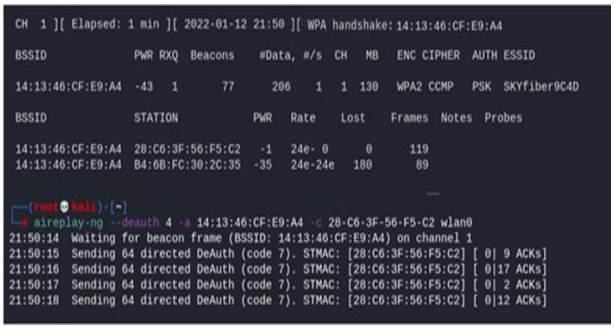

Figure 3. Capturing of WPA handshake.

The attackers used Crunch, a wordlist generator, to make a dictionary name "crack-wifi" for the password cracking on the target wireless network. A dictionary attack takes a lot of disk space as it depends on the set length and characters set by the attacker. [11] This study assigned a minimum of 5, a maximum of 8, and characters involving SKYfiber12345, as seen in Fig. 4.

crunch [min] [max] [characters=symbols|numbers|lower|upper] -o [filename]

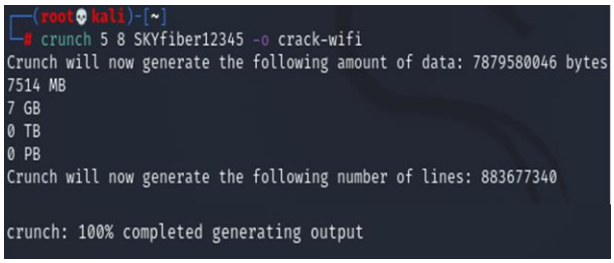

Figure 4. Generation of brute force dictionary.

The password was cracked using aircrack-ng. The Pairwise Master Key (PMK) is compared to the handshake file after integrating every password from the dictionary with the targeted network to calculate a PMK using the pbkdf2 algorithm.

F. Cracking the Password Using GPU (Hashcat)

The attacker's second brute force method is through Hashcat, a GPU. It speeds up the password cracking process [12, 13]. Similar to the first method, the attackers started with retrieving the full handshake of the target network. The sudo wifite command is used. The target network is CPM_FreeWifi. With the wifite command, different attacks will be asked if the user wants to implement it; the said attacks are pixie-dust, null pin, wps pin attack, pmkid capture, and wpa handshake capture [11, 12]. In this case, the attackers only need the handshake capture, seen in Fig. 5.

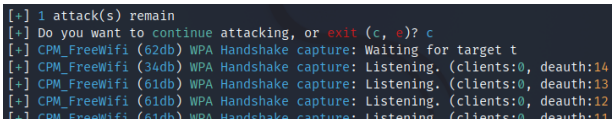

Figure 5. Handshake capture.

Once the handshake is captured, the wifite system will proceed with cracking it, using the default wordlist, wordlist-probable.txt, in the system of Kali Linux, which is illustrated in Fig. 6. It will fail as the password is not common.

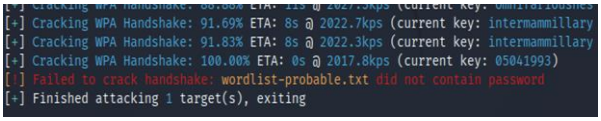

Figure 6. Failed crack of password.

The hccapx are then copied to the directory in the desktop that the attackers will use. The attackers will proceed with the brute force (WPA-EAPOL-PBKDF2) to wpa.hccapx using the hashcat. It will proceed with all the variations to crack the password. After 6 mins 55 secs, it cracked the password. The following command is used to display the password, which is shown in Fig. 7.

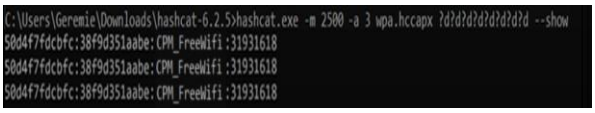

Figure 7. Cracked password.

G. Different Attacks on Connected Clients

Upon successfully retrieving the password, the attackers can now connect to the target access point. The attackers can now launch sophisticated attacks on the target users. Before proceeding to the actual attacks, the attackers will gather detailed information about the target users connected to the free Wi-Fi network using different scanning/listening tools. All of this were successfully simulated in this study. After scanning the necessary information about the target users, the study will proceed with varying man-in-the-middle attacks.

1) Scanning/Listening tools

- **Netdiscover**. It is an ARP scanner that can be used to discover connected/live clients in a network, and it is a very quick scanning tool performed during the reconnaissance phase of penetration testing [14]. IP, Mac address, and sometimes the manufacturer is seen from the result in this tool.
- **Zenmap**. It is a GUI of Nmap, a network discovery tool that can collect comprehensive data about the network, devices connected, services each host is operating, and many more [15].

2) Man-in-the-Middle Attacks (MITM)

This part of the study focuses on man-in-the-middle attacks. They are dangerous and effective attacks that can intercept communications between the target user and the attacker's device. Since we have the Wi-Fi password, the target users' data can be read, modified, and drop secretly [16].

ARP poisoning is a type of MITM that operates by sending malicious ARP packets to a default gateway on a local area network to manipulate the pairings in the IP address to the MAC address table. A hacker can steal information by sending ARP messages to the host while pretending to be the default gateway. The attacker aims to poison the host ARP cache and trick it into using the attacker's IP add as the default gateway [17, 18].

Ettercap is used to initiate the poisoning attack. To start the attack, the attacker must scan the network for hosts. Host 192.168.133.1 will be the victim, and the IP address gets added to TARGET 1 in Ettercap. The attacker will have to trick the router for the attack to work; TARGET 2 will be the router, 192.168.33.254. The attacker in this study then clicks the Man-In-The-Middle option to choose the ARP poisoning attack. Once the attack starts, the victims' computer will receive strange ARP messages that claim to be from the router but come from the attackers' machine.

DNS poisoning is the process of compromising an Internet server's domain name system database by substituting a malicious address for an Internet address. This occurs when an attacker redirects the user to a malicious website where the attackers want to prompt their victims [19]. In Fig. 8, Cain & Abel, a tool for retrieving and capturing Microsoft operating system passwords by sniffing the network, is used to change the IP address of Youtube.com and change it to the attacker's IP address, which is 10.0.2.15, and did the same to facebook.com [20]. Once the victim tries to go to Youtube.com, they will be prompted to input their password and username that the attacker made.

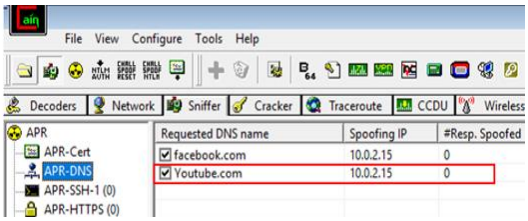

Figure 8. Changed IP of the websites.

The attacker in this study has now acquired the possible account of the victim by poisoning the DNS cache of the personal computer.

V. Conclusion & Recommendation

In this study, the security of free Wi-Fi has been exploited through various technical methods of Wi-Fi penetration testing. The study simulated penetration testing using the Kali Linux in a virtual environment from consented Wi-Fi owners. The penetration steps are executed accordingly: wireless card to monitor mode, scanning, gathering data from networks, monitoring target network, Wi-Fi password cracking attacks, and Man-in-the-Middle attacks on connected users to the network.

The overall result of the study shows that free Wi-Fi networks in public areas may not be safe. Free Wi-Fi users must be aware of the risk; hackers accessing their devices and inevitably stealing their private personal information. It is beneficial for the public if they are aware of the above-mentioned risk for them to be more vigilant when connecting to public Wi-Fi. Dealing with cyber-attacks is getting more attention as it can bring harm to us. More so, mitigating these vulnerabilities will keep the online platform secured and safe for all.

Based on the result of the Wi-Fi penetration test, the study suggests the following practices: (a) to add extra security, public users should enable two-factor authentication, especially on accounts that contain personal information, (b) avoid always using public Wi-Fi, even if it is a well-known establishment. Wi-Fi networks that require inputting information such as name, number, email, etc. are attack vectors that hackers could exploit. (c) Even it saves data subscription, avoid downloading applications, and installing updates when using public Wi-Fi. For Public Wi-Fi Owner, (a) it advisable to change the password to complex credentials with at least 12 characters, (b) to ensure that the Wi-Fi is secure, the owner could perform wireless penetration testing and determine if there is signal leakage (c) a survey and simulation where target users may be a bait of the attack similar to the attack simulation conducted in the study entitled 'Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools' is highly recommended [21].

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization: Eric B. Blancaflor, Eli Christ Paula C. Castillo, Jan Miguel N. Coretico and Geremie B. Rubiano and Angela Marie D. Tobias; methodology: Geremie B. Rubiano, Angela Marie D. Tobias and Eric B. Blancaflor; simulation: Eli Christ Paula C. Castillo, Jan Miguel N. Coretico; resources: Geremie B. Rubiano; writing, review and editing, Angela Marie D. Tobias, Eli Christ Paula C. Castillo and Geremie B. Rubiano; project administration: Eric B. Blancaflor; All authors have read and agreed to the published version of the manuscript.

References

[1] R. Talabong. (2021). Only 882 of 6,000 sites covered so far under the public Wi-Fi project. [Online]. Available: https://www.rappler.com/nation/sites-installed-public-wifi-project-may-2021/

[2] C. Westgarth. (2017). Decrypting cyber insurance: A practical framework for organisations. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=0609d-1c02f2-add3-3d5e8b85

[3] J. Zhang, M. Li, Z. Tang, *et al.*, "Defeat your enemy hiding behind public Wi-Fi: WiGuard can protect your sensitive information from CSI-based attack," *Applied Sciences*, vol. 8, no. 4, 10.3390/app8040515, 2018.

[4] D. Maimon, C. Howell, S. Jacques, *et al.*, "Situational awareness and public Wi-Fi users' self-protective behaviors," *Security Journal*, vol. 35, pp. 154-174, 2022.

[5] L. Kibona and H. Ganame, "Wireless network security: Challenges, threats and solutions. A critical review," *International*

Journal of Academic Multidisciplinary Research, vol. 2, no. 4, pp. 19-26, April 2018.
[6] H. Choi, D. Carpenter, and M. Ko, "Risk taking behaviors using public Wi-Fi™," *Information Systems Frontiers*, 2021, https://doi.org/10.1007/s10796-021-10119-7.
[7] Y. Lotfy, A. Zaki, T. A. El-Hafeez, *et al.*, "Privacy issues of public Wi-Fi networks," in *Proc. the International Conference on Artificial Intelligence and Computer Vision*, 2021, pp. 656-665.
[8] N. Sombatruang, Y. Kadobayashi, M. A. Sasse, *et al.*, "The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan," in *Proc. 16th Annual Conference on Privacy, Security and Trust*, 2018, pp. 1-11.
[9] A. Campbell. (2022). These 7 public Wi-Fi risks could endanger your business. [Online]. Available: https://www.inc.com/comcast/risks-of-using-public-wifi.html
[10] P. Abdalla and C. Varol, "Testing IoT security: The case study of an IP camera," in *Proc. 8th International Symposium on Digital Forensics and Security*, 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116392.
[11] Hacking tutorials. (2015). The 10 top hacking tools in Kali Linux. [Online]. Available: https://www.hackingtutorials.org/wifi-hacking-/top-10-wifi-tools-in-kali-linux/
[12] H. J. Lu and Y. Yu, "Research on WiFi penetration testing with Kali Linux," *Complexity*, vol. 2021, article ID 5570001, 2021, https://doi.org/10.1155/2021/5570001.
[13] D. Bombal. (2020). Brute force WiFi WPA2. [Online]. Available: https://www.youtube.com/watch?v=J8A8rKFZW-M,
[14] R. Sankar. (2017). Netdiscover - Live host identification - Kali Linux tutorials. Kali Linux tutorials. [Online]. Available: https://kalilinuxtutorials.com/netdiscover-scan-live-hosts-network/
[15] M. Ferranti. (2018). What is Nmap? Why you need this network mapper. Network World. [Online]. Available: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html
[16] D. Swinhoe. (2019). Man-in-the-middle (MitM) attack definition and examples. [Online]. Available: https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html
[17] P. Suresh, U. Saravanakumar, and M. S. H. A. Salameh, "Advances in smart system technologies," in *Proc. ICFSST*, 2019, https://doi.org/10.1007/978-981-15-5029-4_8
[18] Radware. (2022). ARP poisoning. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning/#:~:text=ARP%20Poisoning%20(also%20known%20as,IP%20addresses%20into%20MAC%20addresses
[19] S. Agarwal, S. Pramanick, N. Bhandari, *et al.*, "A case study solution to DNS cache poisoning attacks," *International Journal of Advanced Research in Basic Engineering Sciences and Technology*, vol. 3, no. 36, pp. 91-97, March 2017.
[20] Z. Balogh, S. Koprda, and J. Francisti, "LAN security analysis and design," in *Proc. IEEE 12th International Conference on Application of Information and Communication Technologies*, 2018, pp. 1-6.
[21] E. Blancaflor, A. Alfonso, K. Banganay, *et al.*, "Let's go phishing: A phishing awareness campaign using smishing, email phishing, and social media phishing tools," presented at the International Conference on Industrial Engineering and Operations Management, Harbin, China, July 9-11, 2021.

Eric B. Blancaflor is a professor in Mapua University, Philippines. He is an author of Scopus indexed published articles focusing on Cybersecurity, Internet of things and Network and Systems Design, and Web Development. A licensed Electronics Engineer with a degree in Doctor of Technology, Master of Engineering major in Computer Engineering and Bachelor of Science in Electronics and Communication Engineering. He has various IT Certification such as CCNA, CCNP, CompTIA Security+.

Eli Christ Paula C. Castillo is a 3rd-year college student taking up a Bachelor of Science in Information Technology at Mapua University, Makati City, Philippines. She is diligent, motivated, confident, multitasking, highly passionate about workload, and a consistent student interested in the field of cybersecurity. Throughout her education, she improved her leadership, analytical, and problem-solving abilities and assisted the team in overcoming challenges. She received one of the top honors in her high school class, and she is a dean's lister awardee in college.

Jan Miguel Coretico is 3rd year IT student specializing in App Development currently enrolled at Mapua University. A consistent dean's lister, he considers himself a programmer who is well versed in programming languages such as Java and C++ and other languages such as HTML, CSS, PHP, and SQL, to name a few. He is also familiar with Bootstrap, Laravel, Spring Boot, and Spring frameworks. He considers himself an advocate for collaboration, efficiency, and inquisitiveness, which means he is someone who wants to learn more. Jan Miguel is currently interning with a startup company as a full stack web developer, further improving his skills on new frameworks.

Geremie B. Rubiano grew up fond of technology. Throughout his childhood, he has always been fond of computers. After school, he would always play with their computer after accomplishing his assignments. Regardless of this, he was able to excel in his studies in his primary and secondary education. He graduated as Salutatorian and Top 10, respectively. Currently, in his final year at Mapua University Makati, he took a Bachelor of Science in Information Technology. His passion for gadgets during his childhood finally came to fruition. During his university stay, he has been a consistent dean's list awardee. Aside from actually knowing and experiencing hands-on computer-related activities, he has developed an interest in cybersecurity, which is why he took his specialization in cybersecurity. Now, as part of the curriculum, he is taking up his internship at a renowned cyber security company.

Angela Tobias is a third-year student from Mapua University currently taking Bachelor of Science in Information Technology, and her specialization is cybersecurity. She chose cybersecurity because she is a victim of cybercrimes such as phishing, email or internet fraud, and other social engineering attacks and got interested in how attackers perform these attacks and how to prevent them. She also started her internship at Chimes Consulting Company as a QA intern last March 28, 2022. Her interest includes UI/UX design and web design, cybersecurity.