VSDC-NFC Hacking and Skull Penetration Testing Framework

Mahmoud Akram Mahmoud Fahmy Abdulghany
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University of Technology
and innovation (APU)
Kuala Lumpur, Malaysia
TP057122@mail.apu.edu.my

Nor Azlina Abd Rahman
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University of Technology
and innovation (APU)
Kuala Lumpur, Malaysia
nor_azlina@apu.edu.my

Julia Juremi
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University of Technology
and innovation (APU)
Kuala Lumpur, Malaysia
julia.juremi@apu.edu.my

Kuruvikulam Chandrasekaran Arun
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University of Technology
and innovation (APU)
Kuala Lumpur, Malaysia
kchandran.arun@apu.edu.my

***Abstract*— Near-Field Communication (NFC) is a set of technologies and communication protocols that enable electronic devices such as smart phones to initiate or setup a radio communication with each other. It's security and reliability can be embraced by various banks, telecom operators, third-party payment platforms and of course mobile devices terminal manufacturers. A security researcher developed and implemented a malicious application that simulates an NFC card that the user needs to install on their phone. In a contactless transaction, the terminal detects, as soon as you have a card sufficient for the payment terminal card, it does not recognize that the card is set up to continue with the transaction. Due to the current inconsistency between the implementation, and therefore standards, it is tended to point out a related attack that compromises the privacy of the user by collecting the user's payment details. By proposing these attacks, will be raising awareness of privacy and security issues within the specifications, standardization, and implementation of contactless cards and readers. This paper will focus on the overview of NFC, Visa Smart Debit Credit Card (VSDC), Visa payWave and EMV security vulnerabilities. In addition, a Skull Penetration Testing Framework will be developed. It will consist of more than 300 hacking tools including NFC and RFID hacking.**

Keywords*— *near-field communication (nfc), penetration testing, visa smart debit credit card (vsdc), smart phone

I. Introduction

If there is one word that defines modern times its wireless. We cut the cord on the phone, unplug the internet cable, program new TVs with WIFI and paint holes with small windshield transmitters. Radio waves are everywhere. NFC and RFID can be used through smartphones. Today hackers do not need a scanner anymore in order to clone all type of cards including contactless credit card. As long as they do have a smartphone with NFC feature in it. Near-Field Communication (NFC) is a set of technologies and communication protocols that enable electronic devices such as smart phone (Android & IOS) to initiate or setup a radio communication with each other in a way. By bringing the devices together or in a proximate range generally of 3cm or more.

Where users can send or receive apps, documents, or even do contactless transactions. It’s security and reliability can be embraced by various banks, telecom operators, third-party payment platforms and of course mobile devices terminal manufacturers. Concurrently, it has also drawn attention from hackers and security researchers. Were NFC gained a lot of attention, threats, vulnerabilities and challenges (Arwa Alrawais, 2020).These threats and vulnerabilities that can found in the smartphones can lead the attacker to exploit of the EMV security standard which stands for the Europay MasterCard Visa security standard. EMV is a national security standard that is implemented in order to secure transactions, withdrawal transactions, deposit and purchase. Europay MasterCard Visa is a set of technologies, messages, and security rules that are exchanged between the available transaction users or actors in order to assure significant vital security properties such as authentication, authorization and integrity. Nevertheless, as stated before, several studies and investigations stated that the EMV is vulnerable to various attacks. Same goes for the Visa Smart Debit Credit (VSDC) and Visa payWave (Contactless Card) (Visa Public, 2016). In a contactless transaction, the terminal detects, as soon as you have a card sufficient for the payment terminal card, it does not recognize that the card is set up to continue with the transaction.

Due to the current inconsistency between the implementation, and therefore standards, it is tended to point out a related attack that compromises the privacy of the user by collecting the user's payment details. The hackers can start implementing all various attacks in order to steal the credit card from the victim. A security researcher developed and implemented a malicious application that simulates an NFC card that the user needs to install on their phone. As soon as the user try to make contactless payments while inserting your card into the edge of their phone, this app connects to the terminal in front of the card. Although the terminal detects a card collision (the application basically behaves like a card), it gives in to the EMV protocol. To show that the application is pulling the group action data from the terminal, including information about the payment, amount and date. Experimental results show that the used app can effectively spy on contactless payment transactions and win the card collision race by 65% once tested with different cards. By proposing these attacks, will be raising awareness of privacy and security issues within the specifications, standardization, and implementation of contactless cards and readers.

That’s why, as a security researcher, will be focusing on how the hackers can implement this kind of attack and steal credit card info.

With that, the attacker can do various transactions. This paper will focus on the overview of NFC and EMV security vulnerabilities. How to exploit those vulnerabilities and what are the proposed technologies and techniques that can reduce or even prevent this kind of attacks.

In addition, as a security researcher, develop a Penetration Testing Framework that will have and consist of more than a 300 hacking tools for security researchers. This framework is called Skull Penetration Testing Framework. The Framework will have a full section for NFC & RFID Hacking. A lot of various tools will be available in this framework including the 5 steps and Phases of Penetration testing which are Information Gathering & Reconnaissance, Scanning &Vulnerability Assessment, Gaining Access. Maintaining Access, Clearing Tracks. Moreover, for malware analysts, the developer will add ransomware samples or full samples for studies and research. This paper will also give an overview of the Tool and how it can be used in order to install the available tools from this framework.

The main aim of this project to reduce various attacks related to contactless payments and prevent the user's exposure to profuse fraud from hackers or spammers. Furthermore, to create a penetration testing framework that will consist of various main and vital tools that can be used by security researchers and hackers. Up-to-date framework. To provide an awareness program for Malaysian citizens. To reduce various attacks associated to NFC and Contactless Payments using Skull PTF. To prevent numerous attacks linked to Contactless Cards. To help security researchers find all needed main and vital tools, malwares and researches for penetration testing. Provide one framework with more than 300 tools. To help security researchers identify security weaknesses that can be found on the operating system, websites, server, network, hardware, or software using Skull PTF.

The VSDC-NFC Hacking awareness program will help and aware people of the vulnerabilities that can be found in the contactless payments and contactless cards. As, it involves numerous technologies and attacks that are related to the software and hardware of the product, app, POS devices, POS terminal, and contactless credit cards. The citizens need to be aware of this kind of vulnerabilities and attacks. As Malaysia is one of the top countries that be using this kind of technologies that are implemented and used in their everyday life. Most of the grocery stores, malls, manufacturers and companies be using the contactless payments. As a security researcher, Mahmoud will be stating most of the vulnerabilities and attacks that can be used by hackers and spammers. How to reduce most of the attacks and prevent the others. Using Skull Penetration Testing Framework as an implementation tool for this kind of attacks.

Furthermore, the development of Skull Penetration Testing Framework that will consist of more than 300 tools will include tools associated to 5 stages of Penetration Testing. With the inclusion of Malware Analysis, Forensic Analysis, NFC & RFID. The purpose of this framework is to quantify the possibility of frameworks. devices, programming, or end-client compromise and assess any connected outcomes such occurrences might have on the elaborate assets, activities, or procedures.

II. Literature Review

A. NFC Characteristics

Near Field Communication (NFC) is an assortment of short-range remote advances that require an association distance of 4cm or less to set up. NFC permits you to move small information payloads between NFC tag and an Android cell phone, or between two Android devices (Carlos Bermejo, Pan Hui, 2017).

Tags may be straightforward or convoluted. Straightforward labels have just perused and compose semantics, with one-time-programmable areas to transform the card into a read-just gadget. Math tasks are accessible on more modern tags, and cryptographic equipment is utilized to verify admittance to an area. The most developed tags have working conditions that take into consideration confounded connections with the label's code. The information in the tag can be written in an assortment of arrangements, yet a considerable lot of the Android structure APIs depend on the NDEF standard from the NFC Forum (NFC Data Exchange Format) (SSLA, 2013).

NFC-enabled Android devices support three major modes of operation at the same time (Carlos Bermejo, Pan Hui, 2017):

- The NFC devices can read and/or write passive NFC tags and stickers in **reader/writer mode**.
- Android Beam operates in **P2P mode**, which allows the NFC device to exchange data with other NFC peers.
- Emulation mode for the host card, which allows the NFC device to operate as an NFC card. An outside NFC per user, for example, a NFC retail location terminal, can then peruse the recreated or replicated NFC card. It is referred as **Host Card Emulation Mode**.

There are numerous types of NFC chips & devices that are associated with the various ISO standards, which are stated below:

- **ISO 7816** → Associated with the contactless & contact cards
  The ISO 7816 international standard is divided into fourteen parts. smart cards are covered by ISO 7816 Parts 1, 2 and 3, which depict the card's actual aspects, electrical connection point, and interchanges conventions, in addition to other things. Parts 4, 5, 6, 8, 9, 11, 13, and 15 of ISO/IEC 7816 are material to all types of smart cards (contact just as contactless). ISO 7816 is viable with ISO 1444 (Comprion, 2022). They indicate the card's coherent construction (records and information components), just as various orders for fundamental use, application the board, biometric confirmation, cryptographic administrations, and application naming. Memory cards for applications, for example, prepaid phone cards or candy machines follow ISO 7816 Part 10. Section 7 of ISO 7816 characterizes a solid social information base methodology for smart cards utilizing SQL interfaces (SCQL) (Thales,2022).

- **ISO 14443** → Associated with the proximity tags and devices
  ISO 14443 is an international standard governed by the ISO defining the physical characteristics and working interaction between contactless (proximity) tags and devices operating at 13.56 MHz (NFC – RFID) at up to 10 cm in distance. ISO 14443 is the underpinning standard for many types of NFC tags and devices, although not often directly used by developers as the specific details are abstracted by other higher-level technology layers. Within 14443, a tag is mentioned to as a PICC (proximity integrated circuit card) and a device as a PCD (proximity coupling device). In order for the system to comply with ISO 1443, it must meet the requirements which are: Physical characteristics, Radio frequency power & signal interface, Initialization & anticollision, and Transmission protocol (Thales,2022).
- **ISO 15693** → Associated with the contactless vicinity tags and devices
  ISO 15693 depicts norms for "vici-nity" cards. In particular, it sets up norms for the actual qualities, radio recurrence power and transmission connection point, and hostile to crash and transference/communication convention for area cards that work to a limit of 1 meter (roughly 3.3 feet). Because ISO 15693 allows for a read range higher than 10 cm, it theoretically does not comply with the NFC specification. The NFC specification does, however, enable ISO 15693 tags that are structured in the NDEF format. Furthermore, many (but not all) NFC enabled devices can communicate with ISO 15693 tags that aren't NDEF compliant. As a result, while choosing parts for an ISO 15693 system, it's critical to do your homework (Thales,2022).

As it has been stated above, this are the various standards and characteristics that are relevant for smart card implementations, contactless tags & devices, and proximity. With some focused-on industry specific applications. Each smart card, contactless cards, devices and tags do have a specified standards that should be implemented.

B. NFC Contactless Security Vulnerabilities

The NFC Contactless Security Vulnerabilities will be stated in point numbers as seen below:

1. NFC technology allows two devices to communicate over a small distance of "4-10cm." As a result, the EMV consortium has projected that a contactless-NFC purchase transaction will not be able to travel more than this short distance (Information Security 2022). As a result, a relay attack shown in defies this assumption by demonstrating that an NFC purchase transaction can be completed using an NFC bank card that is many kilometers away from the POS as shown in Fig1.

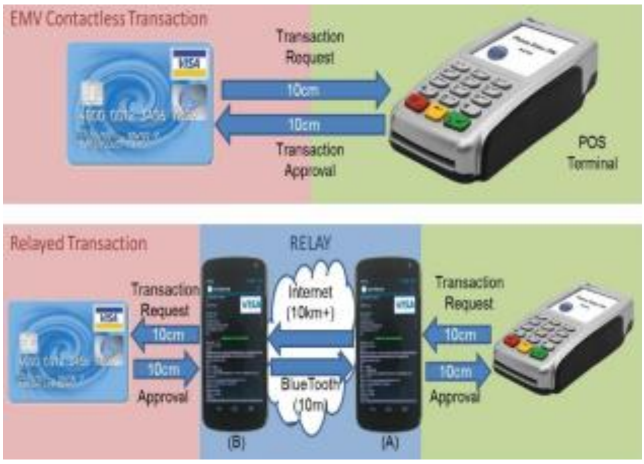
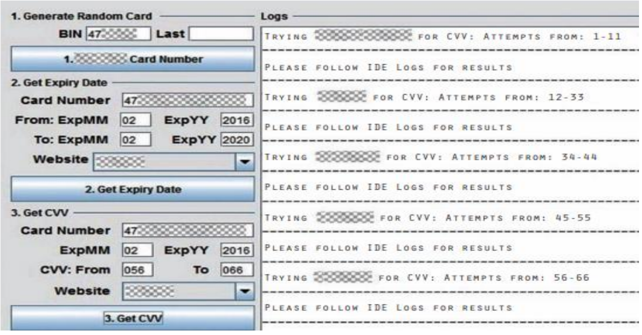


Fig. 1. Contactless relayed transaction attack

2. A contactless-NFC purchase transaction is carried out wirelessly, which opens the door to data hacking attempts such as eavesdropping and extending the reading distance. During an NFC purchase transaction, an attacker can eavesdrop on the NFC communication and get the financial data supplied without encryption (Thomas P.Diakos, Johann A.Briffa and Tim W C Brown, 2013). Also, by using an amplifier that can be linked to the NFC antenna of an unauthenticated NFC reader to expand the NFC reading distance up to 1.50 meters, the attacker can remotely steal banking data from NFC bank cards. In fact, the attacker can utilize the financial information to conduct fraudulent online purchases, track the client's PAN number, and perform a brute force attack to gain the security code. The needed tools in order to implement this attack consist of website bot and automated scripts written in java. Figure 2 displays a screenshot of the website bot that was used to automate the guessing of relevant card details. To locate the proper information, the bot cycles through all of the potential values for each field (Mohammed Aamir Ali, Budi Arief, Martin Emms and Aad Van Moorsel, 2017). Moreover, at least, there are two ways for obtaining legitimate PANs are known. On the web, lawbreakers sell tremendous arrangements of charge card data.


1. Generate Random Card
BIN 47[redacted] Last

2. Get Expiry Date
Card Number 47[redacted]
From: ExpMM 02 ExpYY 2016
To: ExpMM 02 ExpYY 2020
Website [redacted]

3. Get CVV
Card Number 47[redacted]
ExpMM 02 ExpYY 2016
CVV: From 056 To 066
Website [redacted]

Logs

```
TRYING [redacted] FOR CVV: ATTEMPTS FROM: 1-11
--------------------------------------------------
PLEASE FOLLOW IDE LOGS FOR RESULTS
--------------------------------------------------
TRYING [redacted] FOR CVV: ATTEMPTS FROM: 12-33
--------------------------------------------------
PLEASE FOLLOW IDE LOGS FOR RESULTS
--------------------------------------------------
TRYING [redacted] FOR CVV: ATTEMPTS FROM: 34-44
--------------------------------------------------
PLEASE FOLLOW IDE LOGS FOR RESULTS
--------------------------------------------------
TRYING [redacted] FOR CVV: ATTEMPTS FROM: 45-55
--------------------------------------------------
PLEASE FOLLOW IDE LOGS FOR RESULTS
--------------------------------------------------
TRYING [redacted] FOR CVV: ATTEMPTS FROM: 56-66
--------------------------------------------------
PLEASE FOLLOW IDE LOGS FOR RESULTS
--------------------------------------------------
```

Fig. 2. Website Bot, CCV@ value verification

At the point when these rundowns come up short on the CVV2, they are considered less important; be that as it may, such a rundown may be used as a wellspring of PANs from which the expiry date, CVV2, and address data could be made. Another methodology is to exploit the contactless usefulness found on many as of late given installment cards. NFC skimming gives an assailant admittance to the cardholder's

PAN, lapse date, and, in certain circumstances, name. 11 It's likewise conceivable to produce PAN and have it affirmed utilizing the initial six digits of a PAN and the Luhn's strategy (Mostafa Menessy, 2020).

3. An attacker's radio frequency device captures and modifies the data being sent. The attacker's device can temporarily disable NFC data exchange, but only long enough to change the binary coding. This type of attack is extremely difficult to carry out, although data alteration is possible in certain circumstances, particularly for active mode NFC information transmission.
   Data manipulation could be detected by inserting code in the NFC source device that measures the intensity of frequencies, therefore choosing the one that is genuinely the nearest and most likely valid. The transmitter can detect this form of attack by checking the RF field during transmission. Another option is to alter the data so that it appears to be valid to the receiver; in this case, the attacker only has to deal with single bits of the RF signal. The attack's viability is determined by a number of parameters, including the amplitude modulation's strength. It is associated with the Data Modification and of course eavesdropping. As it can be shown in Figure 3 below. The attacker can modify the data while listening (Mohamed Mostafa Abd Allah, 2011).

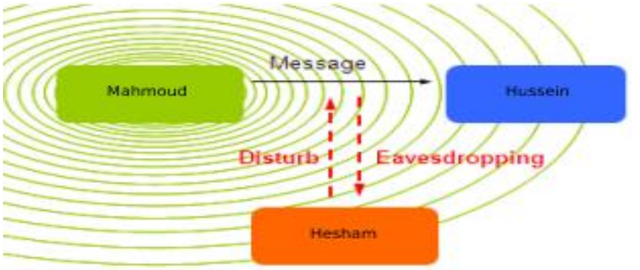


Fig. 3. Data Modification and Eavesdropping

C. EMV Standard Specifications

EMV referred for “Europay, Mastercard and Visa”. EMV is an open-standard arrangement of particulars for shrewd card installments and acknowledgment devices. Worldwide, monetary establishments have moved from attractive stripe bank cards and foundation to EMV chip cards and framework. information shows that greater part of POS terminals has been changed over to EMV-empowered due to the shift of faults that happens when deceitful exchanges occur. NFC versatile contactless installment exchanges between a cell phone and a POS terminal utilize the standard ISO 14443 correspondence convention which is at present utilized by contactless EMV credit and charge cards (NCR, 2015). The EMC chip particulars depend on the necessities of the ISO 7816 series principles and are a subset of them. In any case, ISO 7816 is a bunch of principles rather than an execution situated determination like EMV, which makes terminals that help every one of its necessities exceptionally intricate. EMC chip particulars ought to be perused related to the ISO 7816 norm. Nonetheless, assuming the EMC determination's particulars or definitions vary from the ISO standard, the EMC detail will win. All the more exactly, ISO 78163 indicates the card/terminal point of interaction, yet EMV determines the card and terminal necessities independently, making it troublesome and essentially significant to analyze the two archives straightforwardly. Not dependably. Contrasting the prerequisites of EMV Book 1 with the ISO 78163 standard ought to uncover the distinctions that ought to be considered according to the gadget maker's perspective. EMVCo doesn't have such a correlation. Concerning ISO 78164, which determines the arrangement, security, and orders of the trade, the EMC detail utilizes a portion of the predefined orders, yet not all choices are upheld. Notwithstanding the orders characterized in ISO 7816 and ISO 78164, EMV likewise characterizes extra orders that cards and terminals should uphold (ACS, 2000).

The resolution behind the EMV Specifications is to work with the overall interoperability and acknowledgment of secure installment exchanges. The EMV Chip Specification portrays required and discretionary terminal conduct and the point of interaction between the terminal and card. Card usefulness past this card to terminal connection point isn't portrayed. Supplemental details from the Payment Systems (or from EMVCo for Common Payment Application cards) give prerequisites to inward card handling of the exchange. These card details and extra merchant prerequisites are needed alongside the EMV Chip Specification to construct a total card. Extra terminal details are additionally required for a total terminal plan to cover regions that are random to the card-terminal connection point, for example, the terminal to have interface (EMVCO, 2014).

D. EMV Contactless Kernel

Kernel 1, 2, 3, and 4 are the four levels of the EMV Contactless Specifications for Payment Systems. They're called "kernel" standards since they're aimed largely at terminal software that interacts with compliant payment cards. The payment mechanisms of various credit card brands are covered by each kernel specification. The findings are focused on the Kernel 2 Specification, although no other kernel specifications were examined for commonalities. Part 2 covers the conventions needed to connect with installment cards that acknowledge the MasterCard PayPass, Visa PayWave brands, or any other payment card that specifically demands Kernel 2 usage, according to the specification document.

Kernel 2's EMV protocol supports two alternative operating modes: mag-net-ic stripe copying over contactless exchanges (Mag Stripe mode) and complete EMV convention (EMV mode). A PayPass card bearing the MasterCard brand should consistently permit contactless Mag-Stripe mode exchanges and may alternatively uphold EMV mode exchanges, as indicated by MasterCard's PayPass M/Chip necessity standard. Essentially, MasterCard PayPass terminals should consistently offer contactless Mag-Stripe mode exchanges and may alternatively permit EMV mode exchanges, according to that standard (EMV, 2016).

Furthermore, according to Mastercard's guidelines, cards and terminals issued in 2013-2021 and after must accept both PayPass EMV and PayPass Mag-Stripe modes inside the Single European Payment Area (SEPA). PayPass cards with the Maestro logo, on the other hand, must never support contactless Mag-Stripe technology. The card issuer signs the static data included on the card in EMV mode. the imbursement terminal can affirm that the card information is real. Besides, the card signs the installment exchange utilizing a mysterious key that is just known by the card and is generally difficult to extricate from the card. This can be utilized to guarantee that the card is certified. Therefore, an installment terminal could even confirm and record exchanges that host been verified by a third gathering or a disconnected card (EMV, 2016). The authorization of EMV mode transactions necessitates additional interfaces between payment terminals, the acquiring bank, and the card issuer when compared to executing a traditional magnetic stripe transaction. Kernel 2 supports Mag-Stripe mode, which allows you to use your existing magnetic stripe infrastructure without making any significant changes. The card provisions inf-orm-ation similar to that found on a magnetic stripe in Mag-Stri-pe mode. To authorize payments, the card generates dynamic authentication codes instead of a static authentication code contained in the Mag-Stripe data (or printed on the back of the card). Only the card and not the contents of a payment transaction are authenticated by the authentication code (dynamic card verification code, CVC3) (EMV, 2016).

In addition, Visa Smart Debit Credit (VSDC) does have the similar technology and rules associated with Master Card. As both of them do implement the EMV standards, procedure and technologies. VSDC and Master-C Follows smart card command sequence describes a run of the mill Mag-Stripe mode contactless charge card exchange which can be referred as transactions. Those are the command sequence (NMI, 2021):

a) The POS picks the Pro-ximity Pay-ment Syst-em Environment (PPSE) **(SELECT command)**, and the card responds with a list of EMV payment apps that are supported.
b) The credit/debit card application is selected (SELECT command) by the POS, and the card responds with application details.
c) The credit card application's processing settings are requested by the POS **(GET PROCESSING OPTIONS command)**. The application exchange profile and at least one application document finders are returned by the Mastercard applet. The application exchange profile determines in the event that the card upholds EMV notwithstanding Mag Stripe, what kinds of information validation it supports, and whether or not cardholder check is conceivable. The application document finders highlight records containing static charge card information (for instance, the Mag-Stripe information, which is typically found in record 1 of a rudimentary record with the short record ID 1).
d) The POS go through the Mag-Stripe data from record 1 of the data file with the short file Identification 1 **(READ RECORDS command)**. The Mag-Stripe ve-rs-ion, track 1 and track 2 data are returned by the credit card applet. This data also includes instructions on how to incorporate the active CVC3, ATC, and UN into track 1 and track 2 optional/ or unrestricted data.
e) The card is instructed by the POS to compute the cryptographic checksum for a supplied unexpected number **(COMPUTE CRYPTOGRAPHIC CHECKSUM command)** (UN). The application exchange counter (ATC) and the powerfully created CVC3 for track 1 and 2 are utilized by the Visa applet to answer.

Most of the information traded in a Mag-Stripe exchange (for instance, the Mag-Stripe information) is steady all through all exchanges. The main APDU order reaction pair that contains powerfully produced information that contrasts for every exchange is COMPUTE CRYPTOGRAPHIC CHECKSUM: the erratic number (UN, 4 bytes) created by the POS, the exchange counter (ATC, 2 bytes), and the card's dynamic CVC3s (2 bytes for each track). Another GET PROCESSING OPTIONS order should go before each COMPUTE CRYPTOGRAPHIC CHECKSUM order gave to the card (GlobalPlatform, 2014).

E. EMV Security Vulnerabilities

The EMV Security Vulnerabilities will be stated in point numbers as seen below:

1. In the offline situation of the EMV step 3, an attacker can authorize an EMV purchase transaction by providing a wrong PIN code. Step 3 is modified by the attacker sending a message to the POS indicating that the PIN entered (by the attacker) has been well verified by the client's payment device and is correct, as well as informing the client's payment device that the transaction is verified by a signature and no PIN is required. The fundamental reason for this attack is that the POS does not confirm the client's payment device's response indicating that the PIN code was accurate (Steven J. Murdoch, 2013).
2. Assuming the customer's installment device is a bank card that upholds the SDA technique, it tends to be promptly cloned and used to go through with disconnected buy exchanges. Subsequently, the cloned card can be set up to acknowledge the CVM' disconnected plaintext PIN' and affirm any PIN got for confirmation. Indeed, just the responsible bank, not the POS, detects this vulnerability (Michael Roland, Josef and Josef Langer, 2013).
3. The EMV installment framework guarantees that customer installment devices from different giving banks are acknowledged at any POS/ATM of any securing/ATM bank around the world. Therefore, the EMV essential exchange stage is needed to make any customer's installment gadget interoperable with any POS/ATM. Research paper expressed the interaction and imperative weaknesses in the EMV, this cycle uncovered a basic weakness in the EMV standard, since it permits an assailant to change the capacities of the customer's installment gadget or the POS/ATM, delivering the POS/ATM defenseless. A downsize attack is the name for this kind of assault (Martin Emms, 2013).

By omitting the guarantee of two security features, the EMV standard falls short of providing the whole needed security for a purchase or deposit/withdrawal transaction (Mostafa Menessy, 2020). The secrecy of banking data: during the initialization step, the client's payment device communicates banking data "the PAN and the expiration date" in clear to the POS/ATM. • The POS/authenticity ATM's is not guaranteed to the client's payment device. By sending banking data without encryption to any unauthenticated reader, the latter can converse with them (Mostafa Menessy, 2020).

F. *VSDC-NFC Attack Reduction and Prevention*

VSDC-NFC Attack Reduction and Prevention procedures will be stated in point numbers as seen below:

1. The contactless credit card user can purchase an RFID-Blocking wallet which stands for Radio Frequency Identification. As, all contactless payments can communicate wirelessly with the POS devices and of course card readers (The Money Pages, 2021).
2. Create an awareness program for the citizens and let them know how to secure themselves from this kind of attack and prevent others which is related to NFC contactless payments and contactless credit cards.

One of the researchers' proposals is to stop producing the contactless credit cards or produce new one's with fingerprint technology feature in it. Were the user won't be able to utilize the contactless cards and do payments except when the users put their fingerprints in the card chip in order to activate it (The Money Pages, 2021).

G. *Penetration Testing Strategies and Types*

- *Strategies of Penetration Testing*

Security researchers and hackers should contemplate two main areas when deciding the objective and scope of penetration testing. The two areas are: *testing types* and *strategies* that are used.

There are three infiltration testing tactics which are white box, grey box and black box. In the **white box penetration testing**, the tester or hackers are given with all the required detailed data about the test or victim aim where they do have the full permission from the company in order to test the company's system for vulnerabilities.

So, basically the company and the hackers work together in order to simulate a real-life attack in order to find vulnerabilities and patch them up. While for the **grey box penetration testing**, the hackers already do have a partial disclosure of the information related to the victim's organization. Where the gray hat hackers have a limited information related to the company. So basically, only limited information is shared to the hackers. On the other hand, **black box penetration testing** is where the organization does not provide or share any kind of information to the hackers. Can be called as Black Hat. Black Hat Hackers follows unauthorized and unprivileged approach towards the organization to implement the attack (Red Scan, 2022).

Furthermore, there are two strategies of organization penetration testing which are **Internal Penetration Testing** and **External Penetration Testing**. Outer Penetration Testing alludes to any assaults on the test targets utilizing methodology performed structure outside the association that claims the test target. The target of this sort of outer testing is to see whether there any external assailant who can get in the framework and how far he/she can intensify privilege once obtained entrance. While for Internal Penetration Testing, this kind of testing is performed from inside the organization itself. This kind of procedure and strategy is useful from calculating how much damage can an employee achieve.

If an employee tried to hack into the system or server. It's basically about studying what may happen if the employee was able to penetrate into the system and gain an authorized access (Red Scan, 2022).

- *Types of Penetration Testing*

External/Internal Organization Penetration Testing: An assessment of on-reason and cloud network substructure, for example, firewalls, device hosts and device alongside switches and routers. Can be outlined as both an inward entrance test, that work in property in the organization local area, or an external infiltration test, focused on web going through foundation. To scope a test, you might need to understand the wide assortment of inward and outside IPs to be tried, network subnet length and wide assortment of locales (MitnickSecurity, 2020).

Automation and Vehicle Penetration Testing: Automotive penetration testing rivals a dose on automotive software in an effort to discover or look for any vulnerabilities and measures the potential damage from an attack. The attacks are done on vehicles and any automotive. Pen Tester use software and tool in order to test the automotive software and try to detect vulnerabilities before hackers can. It is basically related to software testing. Test the automotive software before a malicious actors can abuse the car's software in order to obtain a personal data, steal or damage a vehicle, control the vehicle, or even harm the manufacturer's servers (Tsystem, 2022).

Web Application Penetration Testing: An evaluation of sites and *custom* applications conveyed over the web, hoping to uncover coding, plan and improvement defects that could be noxiously taken advantage of. Prior to moving toward a testing supplier, it's essential to determine the quantity of applications that need testing, just as the quantity of static pages, dynamic pages and info fields to be surveyed, tested and assessed (IT Governance, 2022).

NFC & RFID Penetration Testing: The testing of NFC and RFID components/devices can be accomplished through various ways. Each way does have a different attacking vector. Each penetration testing attack does have a technique. So, it's according to the goal hacker or security researcher want to reach and his/her objective. One of the tools that can be used is Proxmark. Proxmark can be used to enumerate-based attacks, perform algorithmic bypasses on password protected cards, evaluate card type or perform card cloning attacks. Like stated before, there are other ways to penetrate the NFC and RFID, in order to find vulnerabilities (Mohamed Mostafa Abd Allah, 2011).

Wireless Penetration Testing: A test that explicitly focuses on an association's WLAN (remote neighborhood), just as remote conventions including Bluetooth, ZigBee and Z-Wave. Assists with recognizing rebel passages, shortcomings in encryption and WPA weaknesses. To scope a commitment, analyzers should know the quantity of remote and visitor organizations, areas and one of a kind SSIDs to be evaluated (IT Governance, 2022).

Mobile Penetration Testing: The testing of portable applications on working frameworks including Android and iOS to recognize confirmation, approval, information spillage and meeting dealing with issues. To scope a test, suppliers should realize the working framework types and forms they'd like an App to be tried on, number of API calls and necessities for jailbreaking and root identification (RSI Security, 2018).

H. *Skull Penetration Testing Framework*

Skull Penetration Testing Framework consist of more than 300 tools that are associated with the six phases of penetration testing and NFC & RFID Hacking. NFC & RFID Hacking is associated with the VSDC-NFC Hacking. As it has been stated in the research document, VSDC-NFC Hacking is related to the contactless payments and contactless credit cards. The framework will be divided into **14 categories** which are information gathering, vulnerability analysis, wireless attacks, web applications, exploitation tools, stress testing, forensics tools, sniffing & spoofing, password attacks, maintaining access, reverse engineering, hardware hacking, NFC & RFID hacking, drone security, voice cloning, reporting tools, and etc.

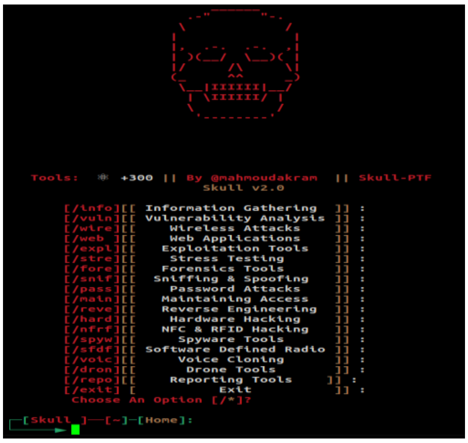
Each category will have some tools inside of it. The user will be able to install various tools from this framework in his device that are related to the stated 14 categories. The tools that will be provided in the framework are from trusted sources as the developer went through each one of them. The developer provides the tools in the framework from various sites including **GitHub Repositories**, **GitLab**, **Source Forge**, and **Deep Web**.

The *developer* will be adding the following commands in the source code in order for the framework to get the tools from the associated repositories or sites. Down below are commands:

* git clone https://github.com/xxxx
* curl -O https://gitlab.com/xxxx
* curl -O https://sourceforge.net/xxx
* wget http://www.xxxx.com/filename.zip
* wget -O filename.zip http://www.domain.com/filename-2.1.0.zip
* wget http://xxxxxxxxx.onion/xxx
* wget https://xxxxxxxxx.onion/xxx/filename.zip

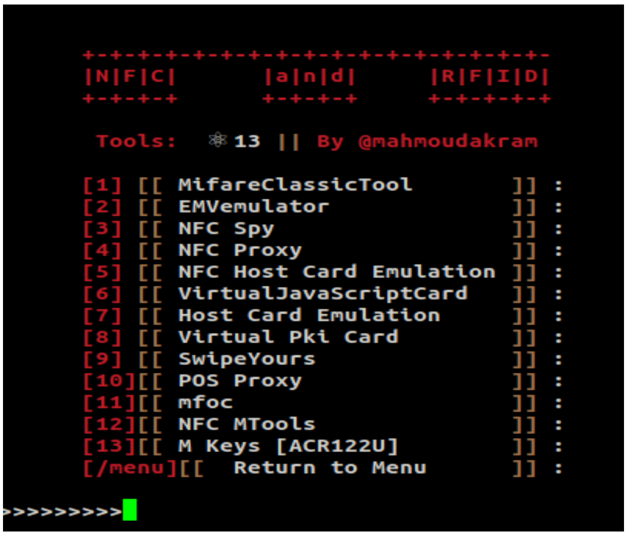
Skull *Penetration* Testing Framework will be an up-to-dated framework. New tools and resources will be added in this framework every two to three months. Each specified category in the Skull PTF will consist a range from 5 to 60 tools inside the stated categories. So, it’s according to the future updates and enhancements for the framework. For example, the reporting tool category will consist of 10 tools inside of it.

Where the user can install the selected tool (s) from this category in their device. The Skull Penetration Testing Framework is a user-friendly. The user will be able to use the framework easily. Fig. 4 and 5. Shows a Prototype of Skull PTF.



```
Tools:   ⚛ +300 || By @mahmoudakram  || Skull-PTF
                  Skull v2.0

   [/info][[ Information Gathering  ]] :
   [/vuln][[ Vulnerability Analysis ]] :
   [/wire][[    Wireless Attacks    ]] :
   [/web ][[    Web Applications    ]] :
   [/expl][[   Exploitation Tools   ]] :
   [/stre][[    Stress Testing      ]] :
   [/fore][[   Forensics Tools      ]] :
   [/snif][[  Sniffing & Spoofing   ]] :
   [/pass][[    Password Attacks    ]] :
   [/main][[   Maintaining Access   ]] :
   [/reve][[   Reverse Engineering  ]] :
   [/hard][[    Hardware Hacking    ]] :
   [/nfrf][[   NFC & RFID Hacking   ]] :
   [/spyw][[     Spyware Tools      ]] :
   [/sfdf][[ Software Defined Radio ]] :
   [/voic][[     Voice Cloning      ]] :
   [/dron][[      Drone Tools       ]] :
   [/repo][[    Reporting Tools   ]] :
   [/exit] [          Exit          ]] :
    Choose An Option [/*]?

┌─[Skull ]──[~]─[Home]:
└──►
```

Fig. 4. Skull PTF



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|N|F|C|       |a|n|d|       |R|F|I|D|
+-+-+-+       +-+-+-+       +-+-+-+-+

 Tools:  ⚛13 || By @mahmoudakram

[1] [[ MifareClassicTool      ]] :
[2] [[ EMVemulator            ]] :
[3] [[ NFC Spy                ]] :
[4] [[ NFC Proxy              ]] :
[5] [[ NFC Host Card Emulation ]] :
[6] [[ VirtualJavaScriptCard  ]] :
[7] [[ Host Card Emulation    ]] :
[8] [[ Virtual Pki Card       ]] :
[9] [[ SwipeYours             ]] :
[10][[ POS Proxy              ]] :
[11][[ mfoc                   ]] :
[12][[ NFC MTools             ]] :
[13][[ M Keys [ACR122U]       ]] :
[/menu][[  Return to Menu     ]] :

>>>>>>>>>
```

Fig. 5. Category 13 | NFC and RFID

III. METERIALS AND METHODS

Having considered methodologies such as Quantitative Research, Qualitative Research and Mixed Research, it is ultimately decided that the research will be carried out through Mixed Research, with the help of an online survey and interview. The online survey will be created with the help of Google Forms.

With the research methods and data collection methodology determined, two surveys have been implemented. Which are associated with Contactless Payments and Contactless Credit Cards as well as Penetration Testing Framework.

IV. RESULT AND DISCUSSION

A. *Contactless Payments and Contactless Credit Cards*

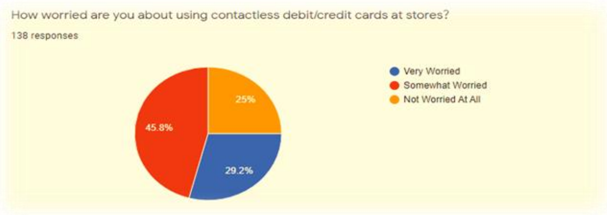


Fig. 6. Contactless debit/credit cards at stores

This question was about asking how worried are the users while utilizing the contactless cards at stores. 45.8% stated that they are somewhat worried. 29.2% stated they are very worried while 25% of the participants stated they are not worried at all while using the contactless debit/credit cards at stores. That shows that the majority of are somewhat worried.

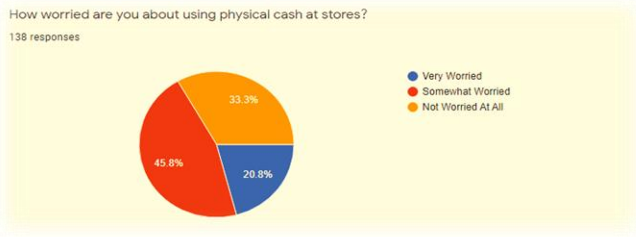


Fig. 7. Physical cash at stores

This question was about asking how worried are the users while utilizing the cash payment at stores. 45.8% of the respondent were somewhat worried. 33.3% were not worried at all. While 20.8% of the respondents were not worried at all

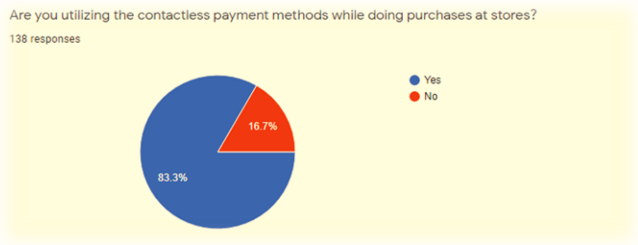


Fig. 8. Contactless payment methods

This question was asking the user if they were utilizing the contactless payment techniques and methods while doing purchases or not. 83.3% of the respondents are utilizing the contactless payment methods while 16.7% are not using the contactless payment methods.

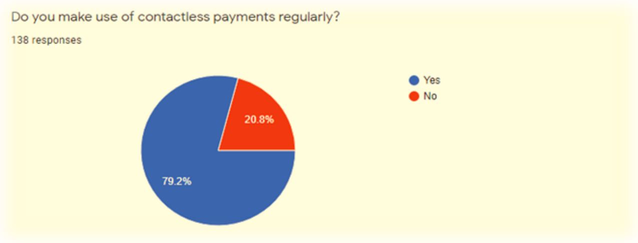


Fig. 9. Usage of contactless payment

This question was about asking the participants if they are using the contactless payments regularly or not. 79.2% of the respondents answered YES. They are using the contactless payments regularly while 20.8% answered NO.

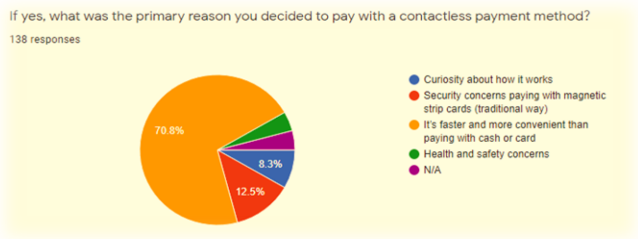


Fig. 10. Reason for utilizing contactless payments

This question is associated with the fourth question that has been stated above. The participants who answered yes, what was the main reason the users or participants be using the contactless payment methods.

70.8% of respondents stated that it's faster and more convenient. 12.5% answered that do have security concerns paying the traditional way. While 8.3% of the respondents had curiosity about how the contactless payment work.

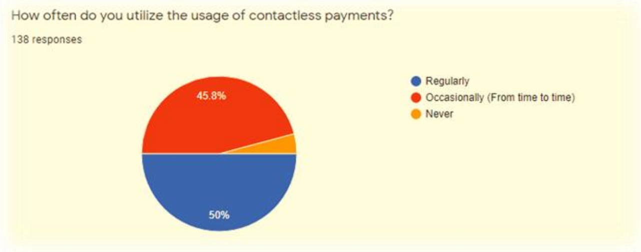


Fig. 11. Usage of Contactless Payments

This question asks the participant how often do they utilize the contactless payments. 50% of the respondent stated regularly be using the contactless payment. While 45.5% stated Occasionally be using the contactless payments.

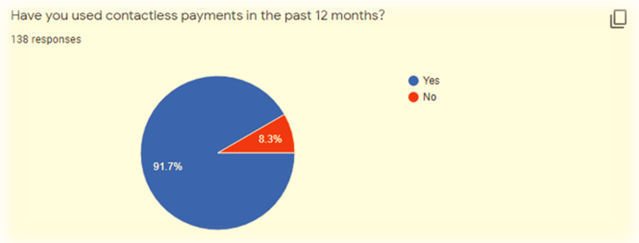


Fig. 12. Usage of contactless payments in the past 12 months

This question asks the participants if they used the contactless payments in the past 12 months. 91.7% of the respondents stated YES. While 8.3% of the respondents answered NO.

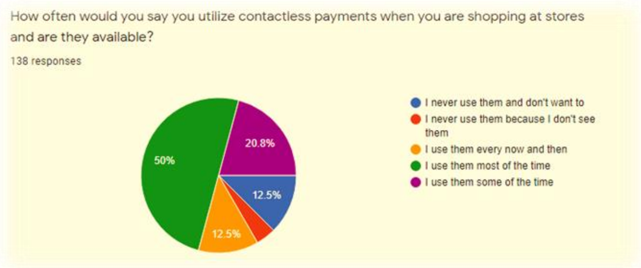


Fig. 13. Availability of Contactless Payments at Stores

This question asks the participants how often do they utilize the contactless payment at stores and is it available in their place or country or not. 50% of the respondents stated that they use the contactless payments most of the time. 20.8% of the respondent use it some of the time. While 12.5% be using it every now and then. And another 12.5% of the respondent never use them and don't want to. So basically, the ones who don't use the contactless payments, be using cash.

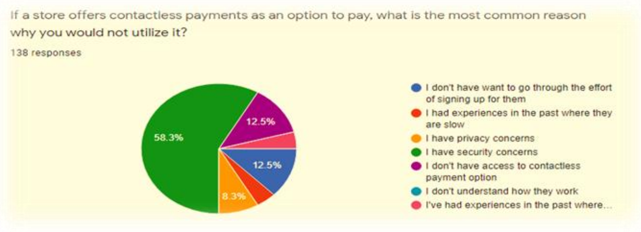


Fig. 14. Common reason to utilizing contactless payments

This question asks the participants if a store or company offers contactless payments as an option to pay, what will be the most common motive that the participants may not utilize it. 58.3% of the respondents stated do have security concerns with the contactless payments. 12.5% answered don't have access the various contactless payment options. Another 12.5% of the respondents stated don't understand how the contactless payment works. While 8.3% had some concerns related to privacy.

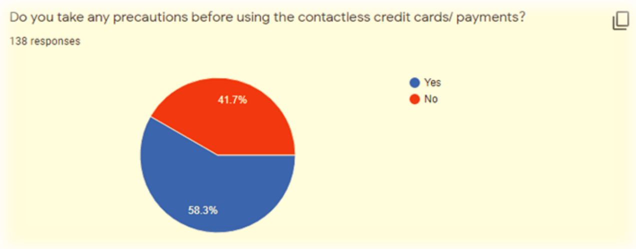


Fig. 15. Precautions before using contactless credit cards

This question asks the participants if be implementing any safety measures before using the contactless payment methods. 58.3% of the respondents stated YES. While 40.7% of the respondents answered NO.

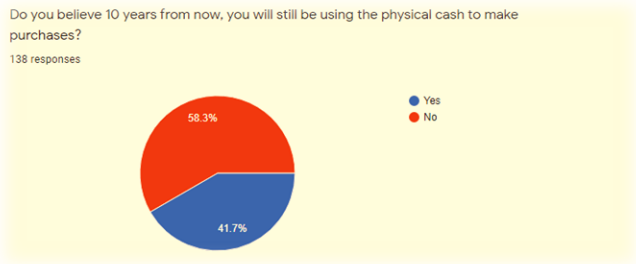


Fig. 16. Usage of physical cash

This question asked the participant If there will be any change in the payment method especially in cash in the coming 10 years. 58.3% stated NO. While 41.7% of the respondent stated YES, utilizing the cash for purchasing products.

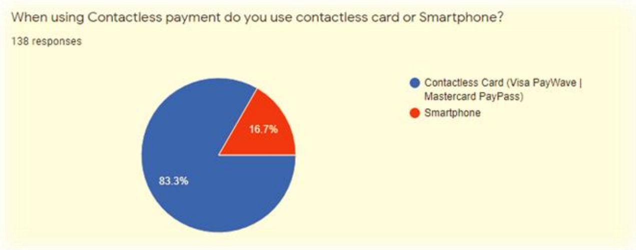


Fig. 17. Contactless card or smartphone

This question asked the participants when utilizing the contactless payment, are they using the contactless card such as Visa PayWave and Mastercard PayPass. Or be using Smartphone. 83.3% of the respondent stated be using the contactless card. While 16.7% be using the Smartphone.

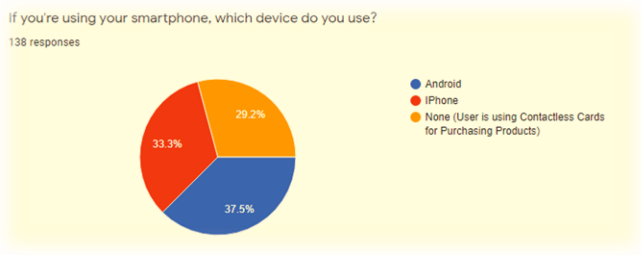


Fig. 18. Device that is utilized for payments

This question is associated with the previous question. If the user be using the smartphone, what operating system or device they be using. If not, then the users are utilizing Contactless Cards. 37.5% of the respondents are utilizing Android device. 29.2% be utilizing contactless credit cards. While 33.3% be utilizing the iPhone device.

B. *Penetration Testing Framework*

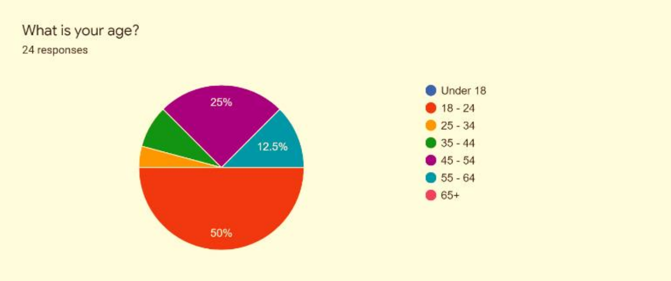


Fig. 19. Overall age

The question lets the researcher know the participants and respondents age range.

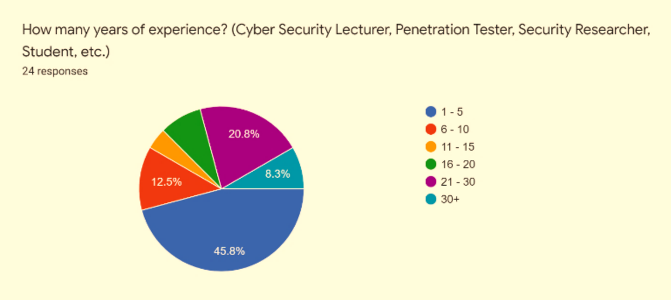


Fig. 20. Years of experience

The question asks the participants how many years of experience in the penetration testing field. 45.8% of the respondents had 1-5 years of experience. 20.8% of the respondents had 21-30 years of experience. 12.5% 6-10 years of experience. While 8.3% had 30 years of experience in the field.

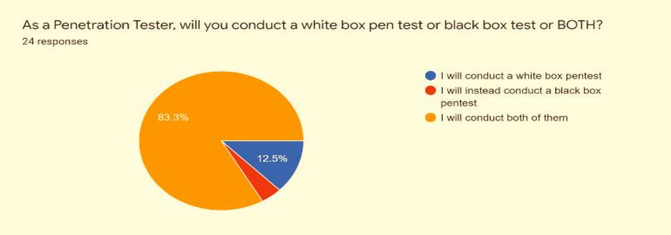


Fig. 21. Conduct white box or black box pen-test

This question asks the penetration testers if they will conduct a white box pen-test, black box pen-test or both. 83.3% of the respondents will conduct both of them. While 12.5% will conduct white box pentest.

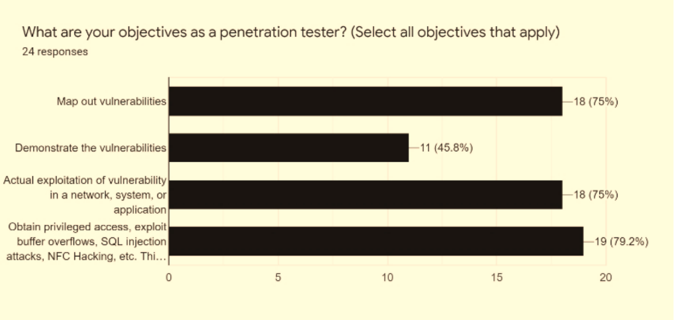


Fig. 22. Objective as a penetration tester

This question asks the penetration tester what are their objectives. 79.2% of the respondent’s objective was obtain privileged access and etc. 75% of the respondents were Map out the vulnerabilities and actual exploitation of vulnerability. While 45.8% was demonstrating the vulnerabilities.

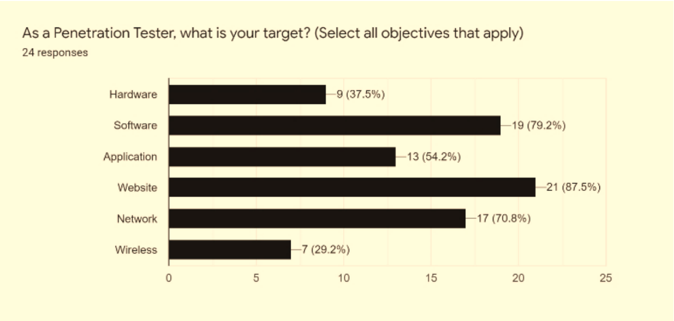


Fig. 23. Penetration Tester Target

Question asks the penetration testers what is their target. 87.5% of the respondent stated website. 79.2% is software. 37.5% is Hardware. 54.2% is application. 70.8% is Network. While 29.2% is Wireless. The penetration testers (participants) select all the targets. So, the percentage is associated with all the targets that have been selected.

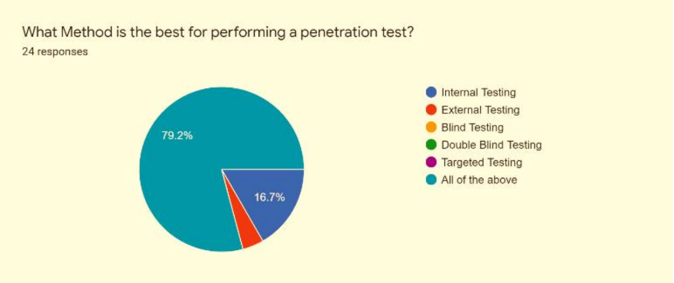


Fig. 24. Method utilized for performing a penetration test

This question asks the penetration tester what method is preferable in performing or conducting a pentest. 79.2% of the respondents selected all of the above. While 16.7% selected internal testing.

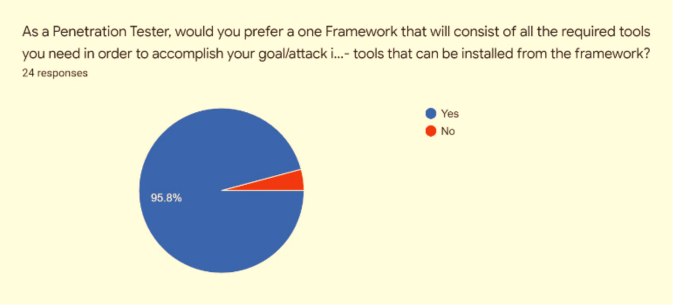


Fig. 25. One framework with all required tools

Most of the participants stated that they would prefer a one Framework that will consist of all the required tools. 95.8% of the respondents stated YES. While 1 person stated NO.

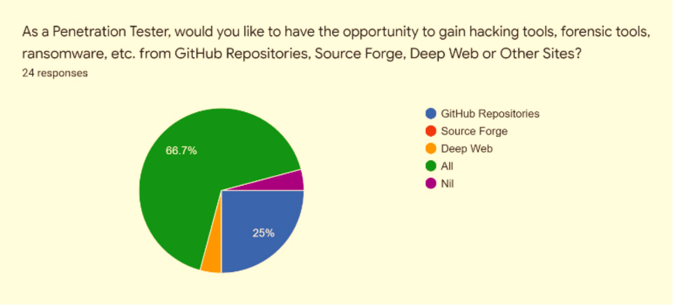


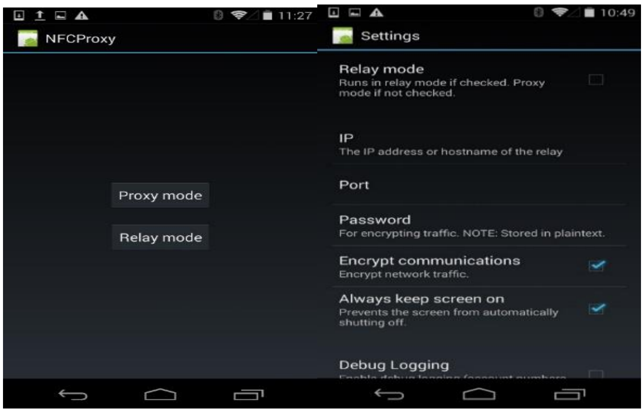
Fig. 26. Platforms to get the tools from

The question asks the penetration testers if they prefer getting the hacking tools form GitHub Repositories, Source Forge, Deep Web or Other Sites. 66.7% of the respondents stated from All. While 25% selected form GitHub Repositories.

V. Presentation and Analysis of Experimental Results

In this section, the researcher will be showing how to implement a successful attack on the Contactless Credit/Debit Cards. Where the researcher can clone, modify and use the card through an android phone. Basically, the android device should have NFC feature in it. In order for the attack to succeed. The android device will simulate the card and act as it is a contactless card. Where the researcher can attach it near a POS terminal device. And transaction will be successful. There are various types of attacks that can be implemented using the NFC and RFID features. In order to implement the attack, the researcher needs to pass by any person who do have a contactless credit card in their wallets, pockets and etc. Just simply holding the android phone and getting it near the wallet or victim’s pocket.

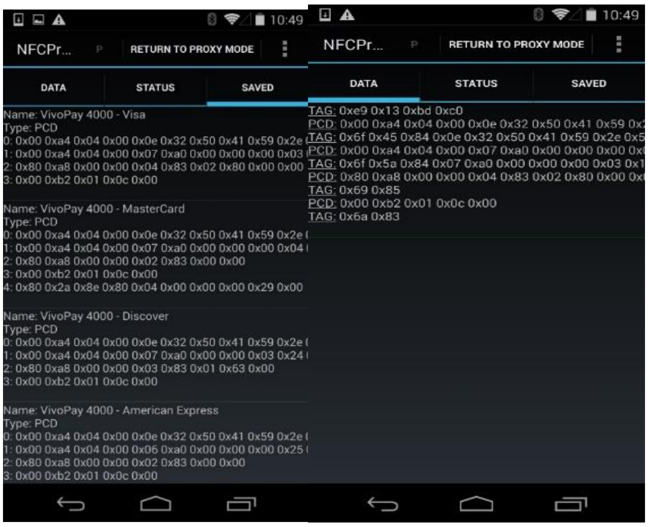
The app that been used will detect the contactless smart debit/credit card and clones it. Once it is successful the attacker can start purchasing products from any available stores. The second way of doing the attack using the same tool. Is to use a proxy and replay devices to implement the attack. Where one device will collect the cloned data and send it to the second device. The second device will be neat the POS device where the attacker can successfully do the transaction or purchasing products from store.



```
Relay mode
Runs in relay mode if checked. Proxy mode if not checked.   □

IP
The IP address or hostname of the relay

Port

Password
For encrypting traffic. NOTE: Stored in plaintext.

Encrypt communications
Encrypt network traffic.   ☑

Always keep screen on
Prevents the screen from automatically shutting off.   ☑

Debug Logging   □
```

Fig. 27. User interface and settings

After activating the app and giving all required permissions to the device. Once the user opens the apk app, will be find two open in the interface. First one is PROXY MODE. Second one is RELAY MODE. Each of the mode does have a functionality to implement and use. While for the settings, if the user selects the proxy mode, then once the user go through the settings, will see that the relay mode is switched off. As, one device cannot be a proxy and relay in the same time. As it can be seen, there is an IP. Both of the devices should be connected to the same network. The user does have the encryption option for communication between the devices.



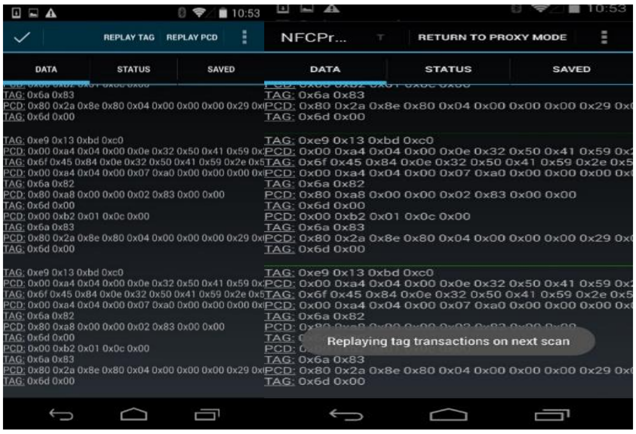
```
Name: VivoPay 4000 - Visa
Type: PCD
0: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x2e
1: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x00 0x03
2: 0x80 0xa8 0x00 0x00 0x04 0x83 0x02 0x80 0x00 0x00
3: 0x00 0xb2 0x01 0x0c 0x00

Name: VivoPay 4000 - MasterCard
Type: PCD
0: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x2e
1: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x00 0x04
2: 0x80 0xa8 0x00 0x00 0x02 0x83 0x00 0x00
3: 0x00 0xb2 0x01 0x0c 0x00
4: 0x80 0x2a 0x8e 0x80 0x04 0x00 0x00 0x00 0x29 0x00

Name: VivoPay 4000 - Discover
Type: PCD
0: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x2e
1: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x03 0x24
2: 0x80 0xa8 0x00 0x00 0x03 0x83 0x01 0x63 0x00
3: 0x00 0xb2 0x01 0x0c 0x00

Name: VivoPay 4000 - American Express
Type: PCD
0: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x2e
1: 0x00 0xa4 0x04 0x00 0x06 0xa0 0x00 0x00 0x00 0x25
2: 0x80 0xa8 0x00 0x00 0x02 0x83 0x00 0x00
3: 0x00 0xb2 0x01 0x0c 0x00
```

```
TAG: 0xe9 0x13 0xbd 0xc0
PCD: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x2
TAG: 0x6f 0x45 0x84 0x0e 0x32 0x50 0x41 0x59 0x2e 0x5
PCD: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x00 0x
TAG: 0x6f 0x5a 0x84 0x07 0xa0 0x00 0x00 0x00 0x03 0x1
PCD: 0x80 0xa8 0x00 0x00 0x04 0x83 0x02 0x80 0x00 0x
TAG: 0x69 0x85
PCD: 0x00 0xb2 0x01 0x0c 0x00
TAG: 0x6a 0x83
```

Fig. 28. DTS and Data Tab

In the proxy mode. The user will see three different tabs in the interface. DATA, STATUS and SAVED tab. The data tab acts as a reader and reads the card. The status tab sees if the card has been read / detected or not. While the saved tab, do have 4 PCD saved data that was used for testing and etc.

In the proxy mode. Once the user goes through the data tab. It will be empty. So, the user needs to attach a contactless debit/credit card behind the smartphone. As the phone does have the NFC feature. The used app/tool will try to read the card and clone the data. It may fail a couple of times in order to detect the PCD.



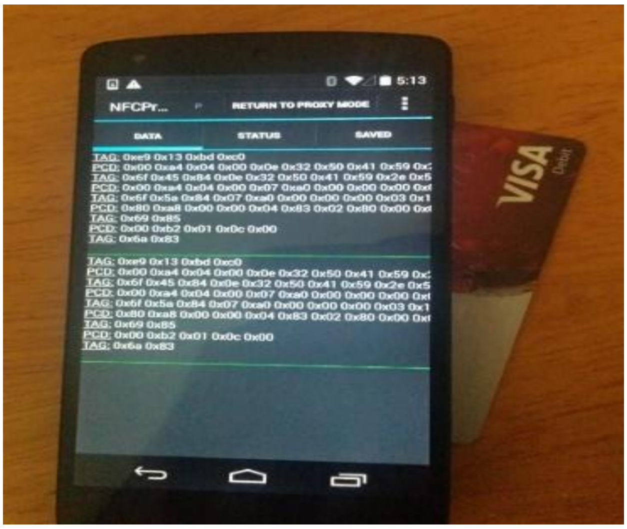
```
TAG: 0x6a 0x83
PCD: 0x80 0x2a 0x8e 0x80 0x04 0x00 0x00 0x00 0x29 0x
TAG: 0x6d 0x00

TAG: 0xe9 0x13 0xbd 0xc0
PCD: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x
TAG: 0x6f 0x45 0x84 0x0e 0x32 0x50 0x41 0x59 0x2e 0x5
PCD: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x00 0x
TAG: 0x6a 0x82
PCD: 0x80 0xa8 0x00 0x00 0x02 0x83 0x00 0x00
TAG: 0x6d 0x00
PCD: 0x00 0xb2 0x01 0x0c 0x00
TAG: 0x6a 0x83
PCD: 0x80 0x2a 0x8e 0x80 0x04 0x00 0x00 0x00 0x29 0x
TAG: 0x6d 0x00

TAG: 0xe9 0x13 0xbd 0xc0
PCD: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x
TAG: 0x6f 0x45 0x84 0x0e 0x32 0x50 0x41 0x59 0x2e 0x5
PCD: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x00 0x
TAG: 0x6a 0x82
PCD: 0x80 0xa8 0x00 0x00 0x02 0x83 0x00 0x00
TAG: 0x6d 0x00
PCD: 0x00 0xb2 0x01 0x0c 0x00
TAG: 0x6a 0x83
PCD: 0x80 0x2a 0x8e 0x80 0x04 0x00 0x00 0x00 0x29 0x
TAG: 0x6d 0x00
```

```
TAG: 0x6a 0x83
PCD: 0x80 0x2a 0x8e 0x80 0x04 0x00 0x00 0x00 0x29 0x
TAG: 0x6d 0x00

TAG: 0xe9 0x13 0xbd 0xc0
PCD: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x
TAG: 0x6f 0x45 0x84 0x0e 0x32 0x50 0x41 0x59 0x2e 0x5
PCD: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x00 0x
TAG: 0x6a 0x82
PCD: 0x80 0xa8 0x00 0x00 0x02 0x83 0x00 0x00
TAG: 0x6d 0x00
PCD: 0x00 0xb2 0x01 0x0c 0x00
TAG: 0x6a 0x83
PCD: 0x80 0x2a 0x8e 0x80 0x04 0x00 0x00 0x00 0x29 0x
TAG: 0x6d 0x00

TAG: 0xe9 0x13 0xbd 0xc0
PCD: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x
TAG: 0x6f 0x45 0x84 0x0e 0x32 0x50 0x41 0x59 0x2e 0x5
PCD: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x00 0x
TAG: 0x6a 0x82
PCD: 0x
TAG: 0
PCD: 0
TAG: 0x6a 0x83
PCD: 0x80 0x2a 0x8e 0x80 0x04 0x00 0x00 0x00 0x29 0x
TAG: 0x6d 0x00
```

Replaying tag transactions on next scan

Fig. 29. Replay Tag and PCD

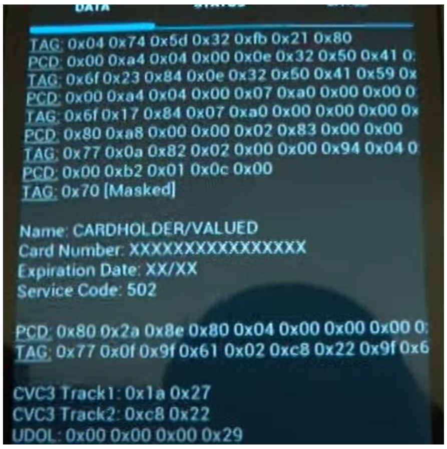
The user needs to attach the contactless debit/credit card behind the smartphone. In order for it to detect and read the card. Once it reads the cards, the TAG and PCD will be shown. The user then clicks in the replay tag as it can be seen form the right figure. In the left figure, it can be shown the card been cloned and it can be used for transaction.



```
TAG: 0xe9 0x13 0xbd 0xc0
PCD: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x
TAG: 0x6f 0x45 0x84 0x0e 0x32 0x50 0x41 0x59 0x2e 0x5
PCD: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x00 0x
TAG: 0x6f 0x5a 0x84 0x07 0xa0 0x00 0x00 0x00 0x03 0x1
PCD: 0x80 0xa8 0x00 0x00 0x04 0x83 0x02 0x80 0x00 0x
TAG: 0x69 0x85
PCD: 0x00 0xb2 0x01 0x0c 0x00
TAG: 0x6a 0x83

TAG: 0xe9 0x13 0xbd 0xc0
PCD: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x59 0x
TAG: 0x6f 0x45 0x84 0x0e 0x32 0x50 0x41 0x59 0x2e 0x5
PCD: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x00 0x
TAG: 0x6f 0x5a 0x84 0x07 0xa0 0x00 0x00 0x00 0x03 0x1
PCD: 0x80 0xa8 0x00 0x00 0x04 0x83 0x02 0x80 0x00 0x
TAG: 0x69 0x85
PCD: 0x00 0xb2 0x01 0x0c 0x00
TAG: 0x6a 0x83
```

Fig. 30. Detection process

As a proof of concept and implementation, here it can be shown that the Visa PayWave card is behind the smartphone. It tries to detect the card and read it. Once it is successful. The card holder name and info will be shown.



```
TAG: 0x04 0x74 0x5d 0x32 0xfb 0x21 0x80
PCD: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0:
TAG: 0x6f 0x23 0x84 0x0e 0x32 0x50 0x41 0x59 0x
PCD: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0
TAG: 0x6f 0x17 0x84 0x07 0xa0 0x00 0x00 0x00 0x
PCD: 0x80 0xa8 0x00 0x00 0x02 0x83 0x00 0x00
TAG: 0x77 0x0a 0x82 0x02 0x00 0x00 0x94 0x04 0
PCD: 0x00 0xb2 0x01 0x0c 0x00
TAG: 0x70 [Masked]

Name: CARDHOLDER/VALUED
Card Number: XXXXXXXXXXXXXXXX
Expiration Date: XX/XX
Service Code: 502

PCD: 0x80 0x2a 0x8e 0x80 0x04 0x00 0x00 0x00 0:
TAG: 0x77 0x0f 0x9f 0x61 0x02 0xc8 0x22 0x9f 0x6

CVC3 Track1: 0x1a 0x27
CVC3 Track2: 0xc8 0x22
UDOL: 0x00 0x00 0x00 0x29
```

Fig. 31. Detection successful

As it can be seen, the card holder name, number, expiration date and service code are detected. The contactless card has been successfully cloned.

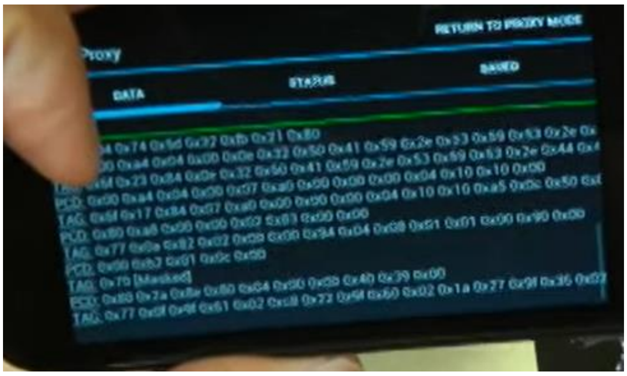
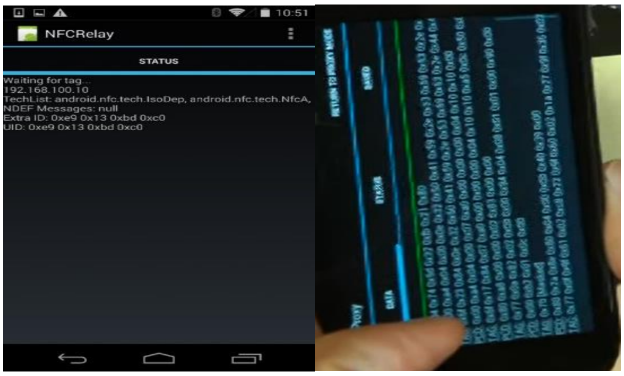


Fig. 32. Transaction process

The user can get the smartphone device near the POS device and the transaction will be successful. The user can purchase the product.



```
Waiting for tag...
192.168.100.10
TechList: android.nfc.tech.IsoDep, android.nfc.tech.NfcA,
NDEF Messages: null
Extra ID: 0xe9 0x13 0xbd 0xc0
UID: 0xe9 0x13 0xbd 0xc0
```

Fig. 33. Figure 1: NFC relay

The other way of doing the attack, is to use the relay method. Where the user needs to use two devices in order to implement the attack. one device will be the proxy and the second device will be the replay. The user needs to attach the contactless card near the replay device. once it detects it. It will automatically send it to the proxy device. and the user can get the proxy device near the POS device. transaction will be successful.

VI. Conclusions

The purpose of the research was to reduce various attacks related to contactless payments and prevent the user's exposure to profuse fraud from hackers or spammers. Furthermore, to create a penetration testing framework that will consist of various main and vital tools that can be used by security researchers and hackers. Up-to-date framework. To provide an awareness program for Malaysian citizens, reduce various attacks associated to NFC and Contactless Payments using Skull PTF, prevent numerous attacks linked to Contactless Cards, help security researchers find all needed main and vital tools, malwares and researches for penetration testing, provide one framework with more than 300 tools, and help security researches identify security weaknesses that can be found on the operating system, websites, server, network, or in a software using Skull PT Framework. Furthermore, the researcher gathered data from the respondents who participated in answering the surveys. Same goes for the one who interviewed with.

In the order to achieve the project, the developer had to implement a real-life scenario attack related to contactless payment in order as a proof of concept.

Skull PTF – VSDC NFC Hacking –. In order for the user to install the tools from the framework associated with the NFC & RFID hacking, the user need to select the tool name from the menu / list. After that, automatically the framework creates a folder in the user's Linux desktop with the tool that have been selected. The framework will go through the associated site in order to install the selected tool. After that, the user will need go through the tool either unzip or just open the terminal and use the required command for running or setting up the tool.

References

Arwa Alrawais (2020), Security Issues in Near Field Communications vol. 11, no. 11, International Journal of Advanced Computer Science and Application. Retrieved from : https://thesai.org/Downloads/Volume11No11/Paper_76-Security_Issues_in_Near_Field_Communications.pdf.

Visa Public (2016), Visa Smart Debit/Credit. Retrieved from: https://www.visa.com.pe/dam/VCOM/regional/na/us/partner-with-us/documents/visa-smart-debit-credit-vsdc-visa-paywave-vpw-us-acquirer-implementation-guide.pdf.

Carlos Bermejo, Pan Hui (2017), Steal Your Life Using 5 Cents: Hacking Android Smartphones with NFC Tags. Retrieved from: https://arxiv.org/pdf/1705.02081.pdf.

Ssla (2013), ssla-co-uk. Retrieved from: https://www.ssla.co.uk/near-field-communication/.

Comprion (2022), ISO 7816. Retrived from: https://www.comprion.com/products-solutions/interfaces-technologies/isoiec-7816/.

Thales (2022), ISO 14443 contactless card standard. Retrieved from: https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/iso14443.

Information Security (2022), Are there any contactless (RFID/NFC) card vulnerabilities that are still unsolved? even minor ones. Retrieved from: https://security.stackexchange.com/questions/239479/are-there-any-contactless-rfid-nfc-card-vulnerabilities-that-are-still-unsolve.

Thomas P.Diakos, Johann A.Briffa and Tim W C Brown (2013), Eavesdropping_near-field_contactless_payments. Retrived from: https://www.researchgate.net/publication/260083712_Eavesdropping_near-field_contactless_payments_a_quantitative_analysis

Mohammed Aamir Ali, Budi Arief, Martin Emms and Aad Van Moorsel (2017), Does the Online Card Payment Landscape Unwittingly Facilitate Fraud?, Vol 15, Issue: 2. Doi: 10.1109/MSP.2017.27

Mostafa Menessy (2020), Digital Fraud: PAN | BIN/ASI Card Attacks. Retrived from: https://medium.com/@mostafamenessy/digital-fraud-bin-asi-card-attacks-dfb8bbda0619.

Mohamed Mostafa Abd Allah (2011), Near Field Communication Strengths and Weaknesses. Retrived from: https://globaljournals.org/GJCST_Volume11/7-Strengths-and-Weaknesses-of-Near-Field-Communication.pdf.

NCR (2015), The Road To Contactless Payments | EMV, Apple Pay and Tokenization. Retrieved from: https://www.ncr.com/content/dam/ncrcom/content-type/white_papers/15FIN3279A_Contactless_EMV_Apple_Pay_wp.pdf.

ACS (2000), Advanced Card System Ltd. Card & Reader Technologies | EMV Specification. Retrieved from: https://downloads.acs.com.hk/technology/491-08-emv.pdf.

EMVCO (2014), A Guide to EMV Chip Technology. Retrieved from: https://www.emvco.com/wp-content/uploads/2017/05/A_Guide_to_EMV_Chip_Technology_v2.0_20141120122132753.pdf.

EMV (2016), EMV®* Architecture and General Requirements. Retrieved from: https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf.

GlobalPlatform (2014), GlobalPlatform Card Technology | Card Specification - ISO Framework. Retrieved from: https://globalplatform.org/wp-content/uploads/2014/03/GPC_ISO_Framework_v1.0.pdf.

NMI (2021), EMV Level 2 Kernels. Retrieved from: https://www.level2kernel.com/emv-mastercard-contactless-transaction.html.

Steven J. Murdoch, Saar Drimer, Ross Anderson and Mike Bond (2013), Department of Computer Science and Technology – Security Group: EMV PIN verification "wedge" vulnerability. Retrieved from: https://www.cl.cam.ac.uk/research/security/banking/nopin/.

Michael Roland, Josef and Josef Langer (2013), Cloning credit cards: a combined pre-play and downgrade attack on EMV contactless. Retrieved from: https://www.researchgate.net/publication/262271594_Cloning_credit_cards_a_combined_pre-play_and_downgrade_attack_on_EMV_contactless.

Martin Emms, Budi Arief, Nicholas Little and Aad Van Moorsel (2013), Risks of Offline Verify PIN on Contactless Cards. Retrieved from: https://link.springer.com/chapter/10.1007/978-3-642-39884-1_26.

Mostafa Menessy (2020), Digital Fraud: PAN | BIN/ASI Card Attacks. Retrieved from: https://medium.com/@mostafamenessy/digital-fraud-bin-asi-card-attacks-dfb8bbda0619.

The Money Pages (2021), How to protect your contactless card and digital wallet from criminals. Retrieved from: https://www.themoneypages.com/saving-banking/protect-contactless-card-digital-wallet-criminals/.

Red Scan (2022), Strategies and Types of pen testing: white box, black box and everything in between. Retrieved from: https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/.

MitnickSecurity (2020), Understanding the 6 Main Types of Penetration Testing. Retrieved from: https://www.mitnicksecurity.com/blog/understanding-the-6-main-types-of-penetration-testing.

TSystem (2022), Automotive and Vehicle Penetration Testing. Retrieved from: https://www.t-systems.com/de/en/industries/automotive/automotive-security/penetration-testing.

IT Governance (2022), Web Application Penetration Testing | IT Governance UK. Retrieved from: https://www.itgovernance.co.uk/web-application-penetration-testing#:~:text=A%20web%20application%20penetration%20test%20aims%20to%20identify%20security%20vulnerabilities,of%20software%20or%20a%20website.&text=Assessing%20the%20web%20applications%20for,XSS.

RSI Security (2018), What You Need To Know About Mobile Penetration Testing | RSI Security. Retrieved from: https://blog.rsisecurity.com/what-you-need-to-know-about-mobile-penetration-testing/.

Mohamed Mostafa Abd Allah (2011), Near Field Communication Strengths and Weaknesses. Retrieved from: https://globaljournals.org/GJCST_Volume11/7-Strengths-and-Weaknesses-of-Near-Field-Communication.pdf.