I&M Red Team Assessment Strategy

Introduction

Commencement: 4th Nov 2020
Finish: 31st Jan 2021

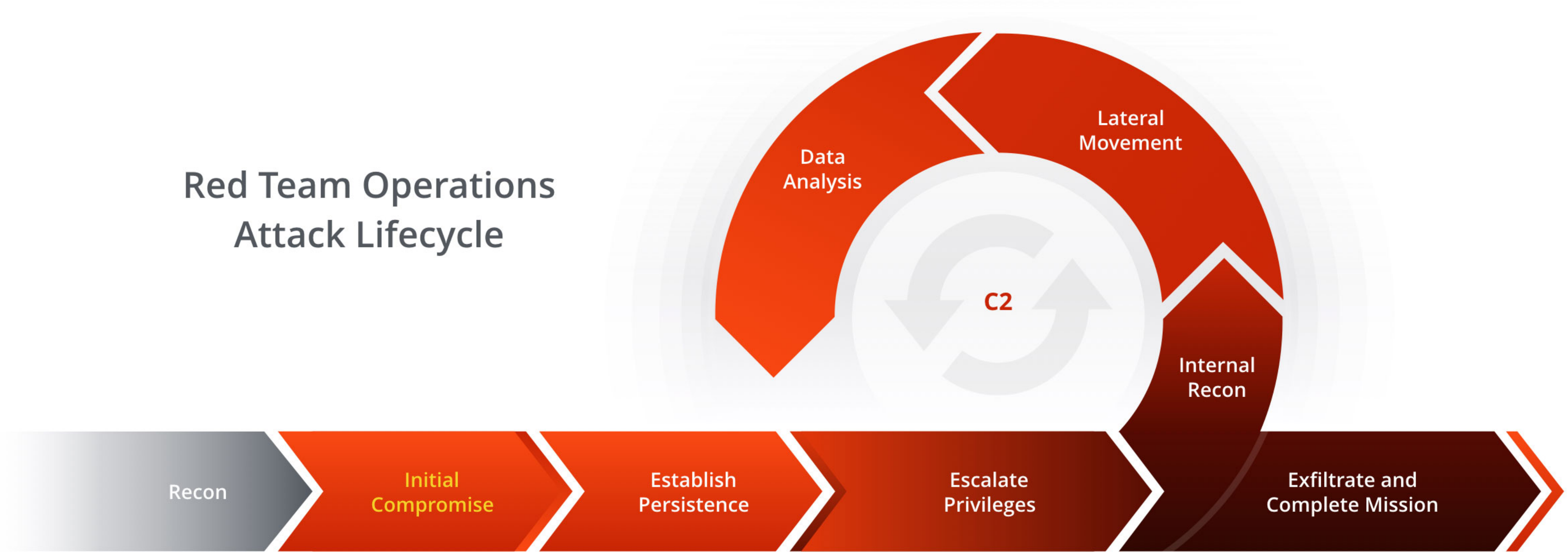
Scope

1) Remote Working abuses and unauthorized access to Bank’s VPN
2) Cyber penetration testing including Cloud Infrastructure for I&M systems
3) Possibility of Wifi Based Attacks to compromise critical data or applications
4) Posture of ATMs in regard to jack potting and/or any other physical attacks
5) Extent of exposure that can result from compromise of a third party
6) Introducing a malicious device in the Bank network from any location
7) Physical breach
8) Targeted & Whale Phishing

Framework:
https://attack.mitre.org/
https://osintframework.com/
https://owasp.org/

Tools
https://github.com/infosecn1nja/Red-Teaming-Toolkit

Red Team Operations



Project Management

Initial Reconnaissance

Attack Scenario	Aim	Who	Comments/ Milestones
Initial Reconnaissance Incorporate both positive and active scans Framework: OSINT Network Surveying Port Scanning System Identification Services Identification Vulnerability Research Internet Application Testing Router Testing Firewall Testing Enumerating Sub-domains Enumerating Employees Internet File Searches (shared file links) Extracting metadata from documents (PDF) Enumerate all Internet Connected Devices Wardriving, warbiking, warcycling, warwalking Previous Red Team reports	Extensive information gathering regarding the target.	SM, CM	1. I&M ASN (Autonomous System Number): This enable us track all IP addresses belonging to I&M associated with the ASN. ◦ Action: Seth to send to team members all IPs and domain names associated with I&M for further review. Continuous ◦ Action: Charles to continue poking the IPs and exploit vulnerabilities. Continuous 2. Default passwords used on content management system cmstz.imbank.com. ◦ Done: File upload vulnerability successful. Shell Into a docket container acquired. Failed to escalate privileges. ◦ Action: Find out HR person to download malicious file. 3. List of I&M employees. ◦ Done: Brian to prepare a list of the employees discovered on social media, emails, their position and department. 4. I&M cloud: ◦ Action: Charles to find out I&M assets on Google cloud, Azure, AWS etc. 5. Mimecast is I&M's email security provider. ◦ Action: Morgan, What can we do with this info? 6. List of emails discovered on https://haveibeenpwned.com/ . ○ Action: Charles. Find out passwords of hashes available for iclick@imbank.co.ke on dark web. ○ Action: Charles. Find password hashes or actual passwords for emails discovered on haveibeenpwned. ◦ Action: Brian update the phishing list with passwords/password hashes 7. imbank.co.ke, the real domain expires on 2020-12-31 ○ Done: Morgan: Can we take over imbank.co.ke domain? From discussions, this can be catastrophic for the bank. 8. Historical records of Bank hacks,

Attack Scenario	Aim	Who	Comments/ Milestones
			○ Action: Research on how banks are hacked and how we can incorporate this into out tactics. Charles

Using data obtained from recon, establish the target’s vulnerabilities, create weapons and delivery mechanisms to attain the following objectives:

VPN Testing

Attack Scenario	Aim	Who	Comments/ Milestones
I&M employee whose home network security infrastructure has vulnerabilities e.g. improper configuration or unpatched software or other zero day vulnerabilities.	Compromise vulnerable	MK, SM, CM	1. Checkpoint https://vpn.imbank.com. Portal is blocked. 2. Enumerate IP and domain names and pock each of them looking for a VPN portal. ○ Action: Charles Find another way to access VPN traffic or another VPN portal. Done, result “not found.” 3. VPN access through social engineering 1. Action: Morgan, social engineer contact at I&M ▪ Philip Kirimi – Skinner, Manager, Datacentre & Bcp Services at I&M Bank ▪ Pretext is needing to view his car with the possibility of buying a new one. Aim get access to wifi for further hacks. 2. Action: Charles, social engineer contact at I&M (Kinyua). Pretext is assistance to develop software. Contact compromised. 3. Action: Brian, social engineer contact at I&M ▪ Ruth Syowai. ▪ Pretext: Take brother to employee home, get wireless network and hack. Aim get access to wifi for further hacks and inquire about how staff connect to work information assets. 4. ...
Use of unsecured personal devices	Enable pivoting to other devices		
Force employee to stop using VPN	Denial of service		
Gain access to victims computer	Gain access to VPN keys and other organisational confidential/sensitive information		
Exploit vulnerabilities in enterprise VPN products	Pivoting		

Cloud Infrastructure Hack

Attack Scenario	Aim	Who	Comments/ Milestones
Enumerate cloud infrastructure	Discover vulnerabilities for future attacks	SM	1. I&M uses Google cloud 1. Action: Seth & Charles to compiles a list of Ips to be sent to group. Clearly indicate which ones belong to the cloud. 2. cmstz.imbank.com. In AWS ○ Action: After getting shell, Seth can we get the destination to the redis http calls to enable lateral movement 3. …..
Use various tool sets https://github.com/toniblyx/my-arsenal-of-aws-security-tools	Compromise organizational infrastructure on the cloud	SM, CM	

WiFi Based Attacks

Attack Scenario	Aim	Who	Comments/ Milestones
Strength of wifi key Peer-to-peer Attacks De-authentication attacks MAC Spoofing Evil-twin attack Management Interface Exploits	Find out whether one can access corporate data through WiFi.	SM, CM	Buy Long range wireless adapter. Action Morgan, delivery in 2 weeks Action: Charles collect wireless networks around ATMs, so that we compare with previous years.

ATMs

Attack Scenario	Aim	Who	Comments/ Milestones
Spoof responses from the processing centre or obtain control of the ATM. Intercept data transmitted between the ATM and processing centre.	Access ATM network, targeting available network services e.g. GSM, WiFi routers	MK, CM	1. Acquire ATM model numbers: ○ Action Charles. Done 2. Acquire ATM keys from model numbers: Action Charles, Morgan

Attack Scenario	Aim	Who	Comments/ Milestones
Access ATM Operating System through unsecured peripherals.	Access ATM services though insecure connections between ATM peripherals and ATM OS. For example lack of authentication.		3. Schedule for Maintenance: ○ Action: All Find out schedule for ATM maintenance. Items to find out; what day of week, what type of maintenance. 4. Scan for blue-tooth peripheral devices used on ATMs. The following branches have been sccanned. ○ 2nd Ngong Avenue: No blue-tooth ○ Kenyatta Avenue: No blue-tooth ○ Biahara street: No blue-tooth
Test the following: • Configuration lapses (e.g. lack of hard drive encryption, • Authentication errors, • Poor protection against exiting kiosk mode, • Ability to connect arbitrary devices) • Inherent vulnerabilities in application e.g. OS vulnerabilities or application control vulnerabilities.	Exploit vulnerabilities or Improper configuration of systems or devices		
Obtain ATM keys from the internet Obtain ATM maintenance details (e.g. company, schedule) with aim of attacking unattended ATMs.	Insufficient physical security		

3rd Party Comprise

Attack Scenario	Aim	Who	Comments/ Milestones
Obtain list of service providers	Create a list of 3rd parties	GM, SM	**3rd Parties** • Innovar (innovar.co.ke): Custody & Investement Services. • Naya (naya.com): Supply wireless I&M have a CustodyOnline application that is supplied to them by innova.co.ke, which can be found at https://i-invest.imbank.com/CustodyOnline/Account/Login?. This software plugs directly into the I&M CBS (core banking system). One of the employees at Innova pushed a Git commit with his corporate email: cmwange@innova.co.ke Action: Brian, find out I&M information that we can get from Innovar (https://innova.co.ke). How important is innovar's hack for this red team? Action: Gladys, Talk with CEO to find out possibility of Free VA for Innovar. Aim • Get the source code • Understand support operations between I&M and Innovar looking for a possible entry channel
EVIProfile 3rd parties according to sensitivity of services offered, cyber security vulnerabilities and possible exploitation.	Create an assessment of attack scenarios		
Prepare exploit			
Exploit			

Attack Scenario	Aim	Who	Comments/ Milestones
			Action: Brian. Find out which other companies provide software development and software support services for I&M

Introduction of Malicious Devices on Bank Network

Attack Scenario	Aim	Who	Comments/ Milestones
Scan for unattended or unsecured physical network points	Create a list of unsecured physical networ points Rate their accessibility according to ease of compromise	MK, GN	1. Buy LAN Turtle and Rubber Duckies. Action Morgan, Gladys. In progress 2. I&M Karen Branch has a computer, reserved for corporate clients and connected to Internet via network cable. Action: Gladys, Morgan, Seth Gain access to bank network through computer.
Connect LAN Turtle-3G			

Physical Security Review

Attack Scenario	Aim	Who	Comments/ Milestones
Social engineering	Get access to NFC or RFID card		Action: Charles, find out where is the I&M data centre?
Cloning card	Gain access to restricted areas		Action: Morgan, buy Proxmark. In progress
Camera placement review	Take advantage of blind spots for malicious activity		Action all, wherever any red team member visits any I&M branch.
Fire cracker explosion; Point smoke on fire detector	Alarm Response Testing Gain access to sensitive areas taking advantage of confusion		Not applicable
Guard placement review and shifts			Action all, wherever any red team member visits any I&M branch.
Environment Review (See physical security check-list below)			Action all, wherever any red team member visits any I&M branch.

General, Targeted & Whale Phishing

Attack Scenario	Aim	Who	Comments/ Milestones
Email: Attachment on recently found covid-19 victims in the area. Email: Fake meeting invites Social Media: Get information through social media accounts SMIShing: patients in vicinity, lock-down movements		SM, SK	Domain to use: Imbank.co.ke Exploit: Hashell. Action: Seth develop macros for execution of Hashell. Servers: Gophish server and CNC server configured on mvps.net Targets: HR Christopher, customer care staff, sales & procurement, HR recruitment. Action: Gladys to call and find out whether the machine in Karen can be used for select Banking. • Meet-up on Wed for internal scanning at Karen Branch. Action: Seth, Prepare payload (Hashell + Micros) to be attached to the phishing files. Action: Morgan/Gladys, Send phishing emails to customer care. Pretext, reconciliation issue with account. Action: Gladys. Prepare an Email list of customer care personnel. Action: Kevin, Send phishing email to sales & procurement. Pretext, new company profile. Action: Brian, Apply for a job via HR portal. Action: Charles • Send mail to Margaret Gitau with questions regarding acquiring card for his account. https://www.imbank.com/prepaid/select-card • Open CBO account at SouthC, while doing network recon with Seth. Action: Morgan/Send fake receipts, order confirmation emails to employees. Action: Bribe employee/contractor by 15th Jan id phishing does not work.

Notes

Physical Security Checklist

1. Are employees access to controlled areas restricted? If it’s by use of a badge do they have pictures on them?
2. Does access to a controlled area prevent "Tail-gating" by unauthorized people who attempt to follow authorized personnel into the area?
3. Are there non-standard entry points to secure areas?
4. Are these non-standard entry points secured and/or monitored?
5. Are visitors required to have supervision at the organization’s offices?
6. Are secured areas controlled?
7. Are visitors allowed within secure areas?
8. If the organization shares access to their facilities, does it have proper controls to segregate access?
9. Do guards at entrances and exits randomly check briefcases, boxes or portable PCs to prevent unauthorized items from coming in or leaving?
10. Do guards allow visitors to bring laptop computers into the institution without proper signoff or authorization?
11. Are fire detectors and an automatic extinguishing system installed on the ceiling, below the raised flooring and above dropped ceilings in computer rooms and tape/disk libraries?
12. Are documents containing sensitive information not discarded in whole, readable form? Are they shredded, burned or otherwise mutilated?
13. Are DVD and CDs containing sensitive information left idling on the desktop or they are not discarded in whole, readable form? Are they "shredded" or mutilated with no restoration possible? (This also should be asked of hard drives and other data storage technology prior to disposal).
14. Are data center and server center activity monitored and recorded on closed-circuit TV and displayed on a bank of real-time monitors?

Phishing Emails

From Kevin to Procurement.
Action: Kevin

Hello Mr/Mrs/Miss <name>

On behalf of everyone at Datasec limited, we would like to thank you for your support..

We value the trust you have put in our services and would like to thank you for that. It’s always a pleasure serving you and we certainly look forward to doing that in the future.

We have lately updated our company's profile as we re-brand to accommodate more services. Kindly find attached the updated company profile.

Your Kindly do have a look at it because your feedback is very important as we are constantly looking for ways to improve our services.

From Gladys to Customer care
Action: Gladys

Hello <name>,

I perceive there is an error in my Bank statement that needs your urgent attention because I suspect that there are fraudulent transactions.

Kindly find attached my Bank statement for the period …….. to ………. I would like to call your attention to transactions ID …..and ….. because I cannot recall making or authorising these transactions.

Kindly do respond asap before these kind of transactions are escalated.

Emails to Personal Accounts
Action: Brian

Hello <name>,

Thank you for shopping on Abacud! Click here to confirm your order details.

Once the order has been confirmed, it will be packaged and shipped as soon as possible. Once the item(s) is out for delivery or available for pick-up you will receive a notification from us.

Thank you for shopping on Abacud.

Please note:

If you ordered for multiple items, they may be available at the pick up station on different days. This is because they are sold by different sellers on our platform and we want to make each item available to you as soon as possible after receiving it.

Format Email as shown in image below and send from info@abacud.com

JUMIA

Fashion | Phones | Computers | Electronics | Home appliances | Daily deals

Dear [redacted],

Thank you for shopping on Jumia! Your order 3[redacted]2 has been successfully confirmed.

It will be packaged and shipped as soon as possible. Once the item(s) is out for delivery or available for pick-up you will receive a notification from us.

Thank you for shopping on Jumia.

Please note:

- If you ordered for multiple items, they may be available at the pick up station on different days. This is because they are sold by different sellers on our platform and we want to make each item available to you as soon as possible after receiving it.

Estimated delivery date(s) Check our delivery information page	**Delivery method** Collection from our Pickup Station
Recipient details [redacted]	**Delivery address** [redacted] Business Centre, Shop No. [redacted] Road Embakasi - [redacted]

You ordered for:

	ITEM	QUANTITY	PRICE
	Canvas Elastic Woven Stretch Braided Belt	1	Ksh 639
	Mi Smart Band 5 - AMOLED Screen - Black	1	Ksh 3,984

SHIPPING COST	Ksh 185
SHIPPING DISCOUNT	Ksh 0
DISCOUNT	Ksh 0
TOTAL	Ksh 4,808
PAYMENT METHOD	Payment on delivery/pick-up

If you would like to know more, please visit our Help Center.

Please don't forget to thank your Jumia delivery agent, who is keeping you safe at home! You can also encourage them through our Facebook page using the #jumiaheroes flag. Stay safe & stay healthy.

Happy Shopping!

Warm Regards,

Jumia Team

Jumia Kenya Team

Got any questions?

- Have a look at our Help Center page
- JumiaPay and Jumia will never ask you for your password, PIN, CVV or full card details over the phone or via email.

E-card to all Staff from Head HR
Action: Seth

Note: The Email is from a fictitious company known as Talibee Stationaries.
This organisation has a web page:https://talibee.com/ that displays a page to enter a code then one can download card from “Nyamaiko Ondati”. nyamaiko.ondati@lmbank.co.ke

Dear <staff-name>,

Kihara Maina has sent you an ecard.

You can view your card here.

You can also send a reply to Kihara Maina using a special Talibee email Stationary! – just click where it says "Send a Reply" at the bottom of the card.

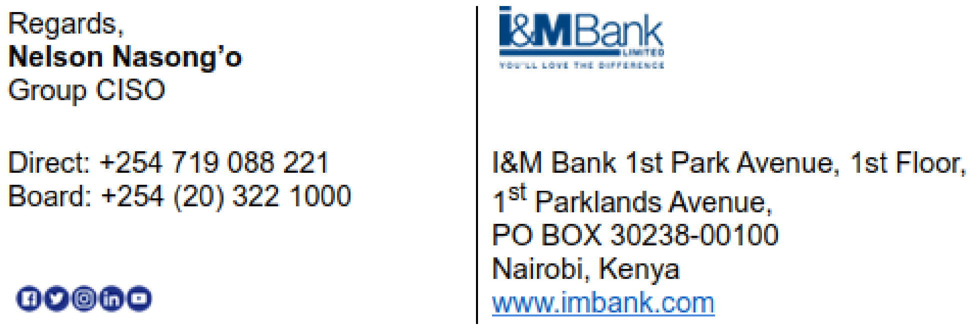
If you are not familiar with our ecards, and are uncomfortable clicking a link in an email, we quite understand. Instead, you can pick up your card and read your message from Kihara Maina by going to www.talibee.com, clicking the Pick Up Card option in the menu, and entering your personal pickup code, which is: 2c281d8d

With best wishes,
Talibee Team

If your email program has not displayed a link above, then please copy the following into the Address bar of your Internet browser to view your card.

https://www.talibee.com/ecard/pickup/r2c281d8df48944b7b191773e461a7ed5?source=jl999

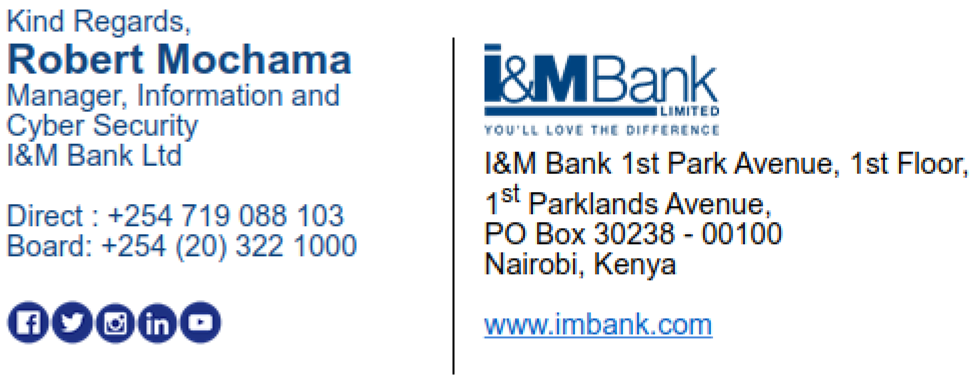
I&M Sample Email Signatures



Regards,
Nelson Nasong’o
Group CISO

Direct: +254 719 088 221
Board: +254 (20) 322 1000

I&M Bank 1st Park Avenue, 1st Floor,
1st Parklands Avenue,
PO BOX 30238-00100
Nairobi, Kenya
www.imbank.com



Kind Regards,
Robert Mochama
Manager, Information and Cyber Security
I&M Bank Ltd

Direct : +254 719 088 103
Board: +254 (20) 322 1000

I&M Bank 1st Park Avenue, 1st Floor,
1st Parklands Avenue,
PO Box 30238 - 00100
Nairobi, Kenya

www.imbank.com

Regards,
Janet Wachira
Officer, Information & Cyber Security
I&M Bank Ltd

Direct : +254 719 082 130
Board: +254 (20) 322 1000

I&M Bank
LIMITED
YOU'LL LOVE THE DIFFERENCE

I&M Bank 1 Park Avenue, 1st Floor,
1st Parklands Avenue,

PO Box 30238 - 00100
Nairobi, Kenya

www.imbank.com

Mail from Charles to Maureen of customer care
Action: Charles

Dear Maureen,

I hope this finds you well.

I refer to the conversation we had earlier this Month (Dec 2020) at I&M Industrial Area regarding the requirements for opening a savings account for an unregistered group.

I truly appreciate your guidance, hence I am writing to provide the additional documents required for opening this account.

Kindly find the documents attached. Let me know if they are sufficient and the next steps towards opening this account.

Sincerely,

Charles Mungai

Bloomsfield
Kindergarten & School
Daycare, Playgroup , PP1 , PP2 & Primary

FEE STRUCTURE 2021

CLASS	TUITION	LUNCH & TEA BREAK	SWIMMING
BEGINNER (3-4 YRS)	KSH 32,000	KSH 7,000	KSH 2500
PP1 (4-5 YRS)	KSH 34,000	KSH 7,500	KSH 2500
PP2 (5-6 YRS)	KSH 35,000	KSH 7500	KSH 2500

Grade 1	KSH 36,000	KSH 8,000	KSH 2,500
Grade 2	KSH 36,000	KSH 8,000	KSH 2,500
Grade 3	KSH 36,000	KSH 8,000	KSH 2,500

PERSONAL ACCIDENT INSURANCE: KSH1,500.00 (ANNUALLY)

REGISTRATION FEE: KSH 5,000.00

NOTE THE ABOVE TUITION INCLUDES DIGITAL LITERACY AND MUSIC

EXTRA CURRICULAR ACTIVITIES: PARENT ENCOURAGED TO TAKE AT-LEAST ONE ACTIVITY

CLASS	PIANO	GUITAR	SKATING
BEGINNER (3-4 YRS)	KSH 5,000	KSH 4,500	KSH 4,500
PP1 (4-5 YRS)	KSH 5,000	KSH 4,500	KSH 4,500
PP2 (5-6 YRS)	KSH 5,000	KSH 4,500	KSH 4,500

Grade 1	KSH 5,000	KSH 4,500	KSH 4,500
Grade 2	KSH 5,000	KSH 4,500	KSH 4,500
Grade 3	KSH 5,000	KSH 4,500	KSH 4,500

Transport Charges

Siblings discount of 7.5% will apply on both School and transport charges.

ZONES	ROUND TRIP	ONE WAY
ZONE 1	KSH 8,000	KSH 5,500
ZONE 2	KSH 9,500	KSH 6,500
ZONE 3	KSH 12,500	KSH 7,500
ZONE 4	KSH 14,000	KSH 11,500
ZONE 5	KSH 17,000	KSH 13,000
ZONE 6	KSH 20,000	KSH 16,500

School Bank Account No.

CO OP BANK, RUAKA BRANCH: 01129412329200
EQUITY BANK, WESTLANDS BRANCH: 0550298603005

For Mpesa payment, follow the procedure below:

PAYBILL NUMBER: 727455
ACCOUNT NUMBER: NAME OF CHILD

- Select Paybill on the MPESA menu
- Enter Business no 247247
- Enter School account no - 0550298603005
- Enter amount
- Send confirmation message and Child's name to 0713794843

Kindly note that cash and personal cheques are not allowed.