Twitter Hack

Vikash Madhav Sridhar[1], Sagarika Naik[2]

1. 18BCAR3012
2. 18BCAR3022

1,2 VI Semester, BCA – DA, School of Computer Science, Jain University

Abstract:

The internet is a vast network of nodes that constantly communicate with each other and share information. Most of this communication is encrypted in such a way that only the sender or receiver can read the content. But within this network exist individuals who hold the power of breaking this encryption. These individuals can decide whether to use this knowledge for ethical or unethical purposes. They are called hackers. The result of the work of hackers is called hacking. Hacking means gaining unauthorized access to classified/ private information. Hacking is characterized as an unlawful act and the activities considered to be a cybercrime. Hacking has evolved from teenage mischief into a billion-dollar business. Growth hacking is the process of rapidly experimenting and implementing marketing and promotional strategies that solely focused on efficient and rapid business growth. Hackers also get paid to get something illegal done. In this paper, we discuss the types of hackers and introduce the various Linux distros used for hacking, what are some of the tools used for hacking and some of the most notorious hacking incidents, most importantly, the twitter hack of 2020.

Introduction:

In early 2020, a group of individuals hacked twitter accounts of notable personalities, and in this paper, we diagnose how it was done, for that one needs prior knowledge of certain technical terms which are explained clearly in this introduction. There are three kinds of hackers, White hat hacker, Black hat hacker and Grey hat hacker. White hat hackers are also known as ethical hackers, they are hired by companies to protect them from hackers who plan on exploiting any vulnerabilities that the company has. There are three types of white hat hackers, Red team, Blue team and security analyst. Red team hackers are the offensive team, they hack other companies or individuals to make sure their company is not at any major/ immediate threat from them. The blue team is responsible for stopping hackers from getting into the company’s databases and other sensitive information. A security analyst notifies the blue team whenever there is a breach in the company. A black hat hacker is one who hacks in an unlawful or unethical way. Their main purpose is to gain unauthorized access to classified data and sell it on the dark web for financial purposes or in exchange for other sensitive information. A Grey hat hacker is also a person who gains unauthorized access to classified information but has no malicious ideas in mind. Their reasons for hacking are purely for the sense of power and pleasure.

Although any Linux distro can be used for hacking by installing necessary packages, hackers prefer “Kali Linux” or “Parrot OS” as it comes preinstalled with all the necessary and extra tools as they are configured to work almost flawlessly with the kernel. Despite its popularity among “techies”, there are many reasons why people prefer Parrot OS over Kali Linux, some of them are, it is lightweight, i.e, its built on Ubuntu, it does not require a graphics card, the OS can only requires 16 GB of space for it to function without any issues, It also comes preinstalled with IDEs and Compilers, a debatable comparison is its user interface, Kali has a simple UI whereas, Parrot OS has a better UI. Parrot OS also comes preinstalled with more tools compared to its rival counterpart. Regardless, people mostly prefer Kali Linux due to a simple reason, it's more popular as Parrot OS is relatively new in the market and thus, easier to find tutorials and learn. On the other hand, some companies demand hackers to build their own OS for hacking due to its added advantage of masking easability and numerous other reasons. On given occasions, companies already have a custom-built OS specific to the organization.

There are hundreds of thousands of tools for hacking, we will discuss these popularly used tools: n-map, metasploit, aircrack-ng, wireshark, airodump-ng, aireplay-ng, wifite. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing (monitoring) computer networks, including host discovery, the process of sending a ping to a computer network and analyzing the response and discovering the operating system of a device.

Metasploit is a penetration testing framework that makes hacking simple. It's an essential tool for many attackers and defenders. Point Metasploit at your target, pick an exploit, what payload to drop, and hit Enter. It's not quite as simple as that, of course, so let's begin at the beginning. Back in ye olden days of yore, pentesting involved a lot of repetitive labor that Metasploit now automates. Metasploit is a hacker's Swiss army chainsaw. The core Metasploit Framework is both free and libre software and comes pre-installed in Kali Linux. The framework offers only a command-line interface, but the pro version provides a neatly designed GUI (Graphical User Interface). Aircrack-ng is a complete suite of tools to assess WiFi network security.

It focuses on different areas of WiFi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools.

- Attacking: Replay attacks, deauthentication, fake access points and others via packet injection.
- Testing: Checking WiFi cards and driver capabilities (capture and injection).
- Cracking: WEP and WPA PSK (WPA 1 and 2).

All tools are a command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily Linux but also Windows, OS X, FreeBSD, OpenBSD, NetBSD, as well as Solaris and even eComStation 2.

Aircrack-ng is a set of utilities for analyzing WiFi networks for weaknesses. You can use it to monitor WiFi security, capture data packets and export them to text files for additional analysis. Capture and injection of WiFi cards can be done to verify their performance.

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng. If you have a GPS receiver connected to the computer, airodump-ng is capable of logging the coordinates of the found access points.

Wireshark is another tool that is extensively used in hacking. Once we monitor and capture packets of information using airodump-ng, we use wireshark to crack the encryption and to view the contents of the packets. We can view the sender's and receiver's IP and MAC addresses. This way, we can catch any malicious information being shared on the internet as long as the hacker is connected to the same wifi network as the perpetrator.

Wifite is a program that has unified all the above mentioned commands used for hacking wifi and capturing packets as a single command. Using Wifite, enables monitor mode on the network, monitors all the available networks, then we can use a password dictionary to crack passwords of the network by sending deauth packets to devices connected to that particular network. Deauthenticated devices will want to reconnect with the network when our hacking machine will act as the network modem and receive the encrypted password, wifite will then use the password dictionary to decrypt the password. Thus wifite is one of the most commonly used wifi hacking tool among new hackers.

Background:

Now that we have explained what hacking is and various tools that are used for hacking are, we will discuss highly notable hacking events that have occurred over the years.

Adobe

As reported in early October of 2013 by security blogger Brian Krebs, Adobe originally reported that hackers had stolen nearly 3 million encrypted customer credit card records, plus login data for an undetermined number of user accounts.

Later that month, Adobe raised that estimate to include IDs and encrypted passwords for 38 million “active users.” Krebs reported that a file posted just days earlier “appears to include more than 150 million username and hashed password pairs taken from Adobe.” Weeks of research showed that the hack had also exposed customer names, IDs, passwords and debit and credit card information.

Canva

In May 2019 Australian graphic design tool website Canva suffered an attack that exposed email addresses, usernames, names, cities of residence, and salted and hashed with bcrypt passwords (for users not using social logins — around 61 million) of 137 million users. Canva says the hackers managed to view, but not steal, files with partial credit card and payment data.

The suspected culprit(s) — known as Gnosticplayers — contacted ZDNet to boast about the incident, saying that Canva had detected their attack and closed their data breach server. The attacker also claimed to have gained OAuth login tokens for users who signed in via Google.

eBay

eBay reported that an attack exposed its entire account list of 145 million users in May 2014, including names, addresses, dates of birth and encrypted passwords. The online auction giant said hackers used the credentials of three corporate employees to access its network and had complete access for 229 days—more than enough time to compromise the user database.

Dubsmash

In December 2018, New York-based video messaging service Dubsmash had 162 million email addresses, usernames, PBKDF2 password hashes, and other personal data such as dates of birth stolen, all of which was then put up for sale on the Dream Market dark web market the following December. The information was being sold as part of a collected dump.

LinkedIn

In 2012 the company announced that 6.5 million unassociated passwords (unsalted SHA-1 hashes) were stolen by attackers and posted onto a Russian hacker forum. However, it wasn’t until 2016 that the full extent of the incident was revealed. The same hacker selling MySpace’s data was found to be offering the email addresses and passwords of around 165 million LinkedIn users for just 5 bitcoins (around $2,000 at the time).

The Twitter Hack

Among these hacks was “The Twitter Hack” of 2020, where twitter accounts of notable personals such as Barack Obama (Former US President), Joe Biden (Current US President), Elon Musk, Apple Co. , Bill Gates, Kanye West and Michael Bloomberg. When the breach came to twitter’s notice, the company decided to block every tweet from a verified profile until the problem was solved.

Methodology:

To explain how the hackers managed to hack one of the most influential and secure social media, Twitter, we must learn to hack the most complicated yet highly delicate machine of all time, “The Human Mind”. They hacked Twitter by hacking the human mind, but how? The answer is Social Engineering and phishing and eavesdropping. There are currently two sources claiming to know how the hack happened through actual hackers: The New York Times and The Vice. Both of the methodologies mentioned in these articles match with the official report from Twitter, explained below.

The social engineering that occurred on July 15, 2020, targeted a small number of employees through a phone spear phishing attack. AvPhone Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons. ... This is the most successful form of acquiring confidential information on the internet, accounting for 91% of attacks. A successful attack required the attackers to obtain access to both Twitter’s internal network as well as specific employee credentials that granted them access to Twitter’s internal support tools. Not all of the employees that were initially targeted had permissions to use account management tools, but the attackers used their credentials to access Twitter’s internal systems and gain information about our processes. This knowledge then enabled the Hackers to target additional employees who did have access to Twitter’s account support tools.

Results:

Using the credentials of employees with access to these tools, the attackers targeted 130 Twitter accounts, ultimately Tweeting from 45, accessing the DM inbox of 36, and downloading the Twitter Data of 7.

This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to Twitter’s internal systems.

Conclusion:

By the end of July 17, 2020, Twitter affirmed what had been learned from these media sources, stating that "The attackers successfully manipulated a small number of employees and used their credentials to access Twitter's internal systems, including getting through our two-factor protections. Even today, the culprit roams free. The anonymity of the hacker is truly to be appreciated in this hack. The identity of the individuals who claimed to be the actual hackers to the New York Times and The Vice were never discovered.

Appendices:

https://www.researchgate.net/publication/316431977_Ethical_Hacking_and_Hacking_Attacks

https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised

https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html

https://networkchuck.com/

Twitter.com