International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 706-709 www.ijaem.net ISSN: 2395-5252

Safeguarding from Cyber-Attacks

Vinayak Sharma, Ajay Kaushik
Student, IT Department MAIT (Rohini), affiliated to GGSIPU
Asst. Prof., IT Department MAIT (Rohini), affiliated to GGSIPU

Submitted: 25-05-2021 Revised: 01-06-2021 Accepted: 05-06-2021

I. INTRODUCTION

The year is 1876, hundreds of people have gathered to see & hear as Graham Bell makes the first ever telephone call to his assistant Mr. Watson, and on the other side, in a distorted and poor-quality audio signal, one hears the words “Mr. Watson, come here. I need to see you.” through the receiver. History is made and a technological revolution has begun. This news is in every newspaper for the coming couple of weeks. Now, the year is 2021, and Mr. Narendra Modi tweets to the nation of India about vaccination and adhering to Covid protocols, and the tweet reaches lakhs of people in and out of India. The tweet didn’t even make it to the local newspaper of any district. Technology surely has seen an exponential growth in the past decades and so have the consumers.

The curious nature of man has led to many revolutionizing inventions in fields likeaviation, biology & medicine, automobile, and electronics to name a few. This curiosity however has always come at a price. Technology has always had its own merits and demerits.

With the Internet began another revolution. New terms were being introduced in the world of computers viz. networking, e-mails, communication protocols, web surfing, websites. Hundreds of protocols were made and implemented in order to monitor the communication between devices over as well as apart from the internet. Data theft and online animosity were soon given the much-needed consideration. Unprotected and unsupervised access to resources is a serious matter indeed.

Through the means of this research paper, I wish to aware the billions of internet and computer users about the potential threats associated with the digital world of today, and more importantly- about how one can safeguard themselves from cyber-criminals.

II. WHAT ARE CYBER-ATTACKS?

Before breaking down the term, we should understand what is a threat. A threat can be understood as an area where a potential breach of security layers, protocols, and measures can occur. A cyber-attack can be understood by conjunction of the two terms- cyber and attack. In computers and networking, an attack is said to occur when a threat is able to breach the security of a system and the security measures of the victim system stand compromised. Adding the word cyber- which is used when associating a system or a device with an active internet connection, or when one is online. Thus, a cyber-attack is an attack performed over a specific target- which can be a network, system, server, or even a private device that is using an active internet connection.

Further, a vulnerability is a weak point in the architecture of the target system which is a threat to its security. An exploit is a malicious piece of software or code that takes advantage of the vulnerability of a system and advances itself to a threat or an attack. Virus and malwares too are infected chunks of codes created with the intention of destroying the target system and/or gain control over it violating the cyber-laws. A cyber-attack is carried out deliberately with the aid of malicious software and programs by an attacker which in today’s world is wrongly called as a hacker; he should be referred to as a black-hat hacker. The reason behind a cyber-attack is neither ethical nor justifiable. Along with data theft, confidential information is at risk which could be disastrous at even national levels in the wrong hands. This could lead to huge monetary losses and/or destruction of the victim’s reputation and personal data.

III. HOW IS AN ATTACK PERFORMED?

In order to learn how to safeguard oneself from the cyber-attacks, one must know about how these attacks are performed. Computers have seen technical advancements since invention of the ENIAC, but so have the cyber-attacks.A cyber-attack at the primary level requires two things:

a. A dedicated operating system
b. Specialized set of tools

The popular choice of OS is Kali Linux. Kali Linux is generally installed as a virtual machine on the host OS. Kali by default comes pre-installed with a variety of hacking tools that a hacker or a penetration tester might need. Some tools used in Kali in order to carry out the attacks are:

- Metasploit Framework: it contains a huge database of all the known and available exploits ofnearly all the operating systems. The attacker simply has to search through the database to choose an exploit. Further, it also assists in connecting to the victim once the exploit has been launched.
- Maltego: Maltego is a hacker's search engine, which can be used to identify links of the victim which plays major role in planning of an attack. It is also used as a recon tool.
- Bettercap: is used when the attacker plans to launch attack(s) on the system that is connected to the same network as him.
- Veil Framework: is used to create an undetectable backdoor- which negates the functioning of security measures and tries to bypass authentication in order to gain control of the system.
- BeEF: short for Browser Exploitation Framework Project, is a special tool used for penetration testing focused on web browsers.
- Zenmap: is a scanning tool that is used to obtain information about a victim who is on the same network as your own, and about all the open ports and applications running on it.
- XeroSploit: this tool is used to launch various types of attacks along with network scanning widgets that aim to test the security of a system or a server.

IV. WHO PERFORMS THESE ATTACKS?

The people and media have over exaggerated the term hacker to such an extent that tech geeks had to create new terms in order to rectify the correct and original meaning of the word. A hacker is considered as a bad person or an attacker which is why the term ethical hacker came into play. The truth is, a hacker or a penetration tester is a person appointed to test or monitor the security mechanisms and attack-prevention techniques of a system with the permission of the system's rightful owner. Now, the definition above stands true only for an 'ethical' hacker, and a hacker is now considered a cyber-criminal. Nonetheless, there are three types of hacker:

1. White-Hat Hackers: or the good guys. They perform penetration testing only with the intention of testing or strengthening the security mechanism of a system, with the permission of the owner.
2. Grey-Hat Hackers: their intention is unknown while they carry out penetration testing and attacks on the target system. A whistle-blower can be vaguely identified as a grey-hat hacker.
3. Black-Hat Hacker: a black-hat hackerperforms the same tasks as a white-hat hacker but with unethical or bad intentions. Their aim is to cause harm to the victim.

So, coming back to the question- it is a black-hat hacker who performs these cyber-attacks. A grey-hat hacker may or may not indulge in the same.

V. PREVENTION FROMCYBER-ATTACKS

It is safe to say that cyber-attacks are a serious threat to the modern world. With billions of devices connecting to each other through the means of the internet, privacy and security are the biggest concerns of the digital population. Thankfully, prevention of falling victim to cyber-attacks is achievable to the majority of the extent using the discussed methods. These do not guarantee complete security but will definitely act as bodyguards to a person's devices.

1. Antivirus programs:

Always use paid antivirus programs. An antivirus program acts as the first and the strongest line of defence for your system. Modern antivirus programs not only identify a threat, virus, trojan, or a malware, but can also repair, modify, and quarantine the suspected or infectious files. They actively scan the system for the mentioned threats and informs the user about the same.

A modern antivirus program, along with system protection, offers various other features like phishing protection, firewalls and proxy, VPNs, safe net banking mode, and many more.The most important thing about using an antivirus is to only use the paid versions, not the free ones. The latter is generally the reason people end up buying paid antivirus programs.

2. Updating your system regularly:

Another important step is to keep your systems and devices up to date with the latest security patches. The cyber-world keeps on evolving with the latest exploits and attacks, and the software providers and developers keep working to make the software immune to the existing and the latest attacks.Updating your system regularly does not only guarantee stronger protection for your system, but also helps the developers to gain information about the usage statistics and the overall behaviour of a system. This in-turn helps the developers to better understand the end user's needs which leads to better, more convenient defensive programs being launched for us.

3. Using strong passwords:

There are a number of wordlists and applications available to create a custom wordlist to perform a brute force attack or password-cracking on a specific system. To prevent this, one must use stronger, longer, and random passwords across all their devices. Further, we must ensure that no two devices or applications use the same passwords. Furthermore, one must keep changing their passwords at regular intervals and never save the passwords on their system.

4. Avoid clicking random links/URLs:

It is relatively very easy to infect any random link or create a fresh infected link that when opened by the victim can perform a number of tasks in the back-end without the target's consent. Such links are generally used to spy on a victim machine, or even for reconnaissance purposes. Moreover, opening an infected linkmay also anonymously install a virus in the victim machine. In a nutshell, one should never click any random link be it on a website or an online ad, and especially if the link is received from an unknown/unverified sender.

5. Beware of frauds:

With increase in digital population and in the number of internet users, cyber-criminals have ample targets to exploit. Apart from infected links, one should never download any application or software for free from the internet, as most of them have an undetectable backdoor or spywares installed in the using which the hacker may gain private information about the victim very easily. Further, using keyloggers the hackers can obtain every data entered using the system's keyboards including credit card numbers, bank details, logins and passwords, etc. Before sharing any personal or confidential information to a stranger on the internet or uploading the same on a new portal, one must verify the sender using reverse IP or WhoIs lookups. In case someone falls victim to an online fraud, they must notify the cyber-cell department as soon as possible or call them at 155260.

6. Avoid public networks:

Most attacks are performed after joining the same network or access point as the victim, which gives rise to Man In The Middle attacks. By joining a public network, it saves the hacker considerable amount of computational work as it become a lot easier to gain access to a victim on the same network. One should never transmit confidential information or personal details using public networks, such as the ones of airports, hotels, restaurants, etc. However, if one still has to join a public network, they must use paid antivirus and a firewall in order to safeguard themselves as much as possible.

7. Use network analysing software:

There are a number of network and traffic analysing software for commercial as well as domestic purposes, which facilitates monitoring of the network overall. Wireshark is a good example of such tool. Wireshark notifies the user of suspicious activities and connections happening inside the admin's server/network. The domestic version of this tool is free to download.

8. Check for alterations:

Lastly, if a user has to open a link from an unknown source or download a file from the same, they must check if the file has been altered with mid-air. This type of attack is gaining popularity among hackers. To prevent this, one must match the MD5 (Message Digest 5) values of the original file with the downloaded file. If there appears to be an alteration in the MD5 values, one should not download the file and if possible, notify the developers.

Another method to check for alterations is to perform a reverse IP lookup on the sender. There are a number of online websites that help the user to verify the basic details of the sender like the IP, website name and registration, location, etc.

VI. CONCLUSION

Technology today knows no bounds but sadly neither does the cyber-crimes. One's safety is in their own hands and using the discussed methods, one can prevent themselves from falling a victim to cyber-crimes. All the preventive measures discussed in this paper are tested and provide promising results. Man is the biggest security flaw, but being cautious and aware will surely help in patching this up. With this paper I would like to draw the attention of concerned authorities to include the basics of ethical hacking and cyber-attacks right from secondary school to make the coming generations digitally safer and smarter.

REFERENCES

[1]. TheWeb Application Hacker's Handbook,Dafydd Stuttard & Marcus Pinto.

[2]. OWASP- Web Application PenTesting.
[3]. The Hacker PlayBook 2, by Peter Kim.
[4]. Network Security Essentials, William Stallings.
[5]. Hacking: Art of Exploitation, Joe Ericson.
[6]. Hacked, Josh Thompsons, Alan T. Norman.
[7]. Computer Networking- a Top-Down Approach, Jim Kurose.
[8]. Ethical Hacking, Zaid Sabih.