A Review of Dangers on Internet

[1]Ankit Sonker, [2]Shubham Kumar, [3]Prabjhot Kaur, [4]Sonal Sharma

[1] Student, Department of Computer Application, Uttaranchal University
Dehradun, Uttarakhand, India
ankitsonker001@yahoo.com

[2] Student, Department of Computer Application, Uttaranchal University
Dehradun, Uttarakhand, India
shuvhubeniwal6@gmail.com

[3] Assistant Professor, Department of Computer Application, Uttaranchal University
Dehradun, Uttarakhand, India
work.prabh@gmail.com

[3] Associate Professor, Department of Computer Application, Uttaranchal University
Dehradun, Uttarakhand, India
sonal_horizon@rediffmail.com

Abstract - The Internet is a big ocean that does not have any end, but the ocean has many harmful creatures too in it. Like that the Internet has some anonymous user profiles which are known to as HACKERS which are used to stolen user's information for there own benefits and interests. Hacking is an illegal activity when it is done without the permission of the government. For Hackers, it is an easy task to get into someone's system and use that information as they want. In this research, an effort has been made on how to detect the unwanted activity on our system if there is an issue on how to fix that and the best ways to protect ourselves from Hackers to enter our systems, how to browse safely on the Internet. Brute Force attacks, Phishing attacks, Keylogger, etc are the common methods used by hackers to hack. This study helps the Users form all this type of attack and how to get rid of these types of situations likes:-

- How to detect a attack on our system.
- If finds, then how to fix.

Keywords - ***Anonymous Users, Ethical Hacking, Phishing.***

1. Introduction

The connection which binds the whole world together is the Internet, the network of networks. Nowadays Internet works like oxygen for Human Beings because in every field the Internet plays the most important role whether it is business, education, medical field, etc. An ever-incrementing sort of computers get associated with the online, wireless contrivances and networks are blasting thanks to the propelled innovation of the online, the administration, personal trade, and conjointly the customary laptop shopper have fears of their information or personal data to be get taken or hack by the hacker (Pandey). There is the word 'Anonymous' what does it mean?. Innominate is a decentralized international hacktivist group that is prominent for its sundry DDoS cyber attacks against several regimes, regime institutions and regime agencies, corporations, and the Church of Scientology. This hacktivist group started in 2003 by 4Chan.org website, there is a profile named as 'Anonymous' means the profile was undetectable to the website users and Internet world no one can trace that profile. This group says that "we are anonymous, we are legions, we don't forgive, we don't forget, Expect us", everyone on this planet has the right to express their feelings. The group is also known by 'Digital Robin hoods'. Anonymous profiles are harmful for Internet users because every human is not a part of this 'Anonymous group', these types of profiles square measure a part of hacking as in today's world there square measure such a large amount of users profiles that square measure operating anonymously for his or her welfare and their advantages. Hackers and Attackers that job Anonymously while not exploit any footprints behind, misuse the information, get management over to a different system while not knowing the users. These types of hackers square measure known as ebony hat hackers WHO will covertly take the association's data and transmit it to the open internet? throughout this implies, to surmount these authentic issues, another class of hackers appeared and these hackers ar hand-picked as ethical hackers or white hat hackers.

This paper can characterize hacking, moral hacking, determine the anonymous activity, attacks, show a little of the typically utilize terms for aggressors, provides a summation of the quality administrations offered to utilize moral hacking to battle assailants, verbalize concerning problems and their obviations.

2. What is Hacking?

A hacker could be a one that finds and exploits a weakness in a very ADP system to gain access or a person who thinks outside the box to achieve something. Hacker is a programmer who bridges a bridge to another system to exchange, modify information without authorization. Hacker uses tools and program to hack a victim. Haplessly, some of these hackers additionally became experts at accessing password-bulwarked computers, files, and networks and came to kenned as "crackers". A cracker is additionally referred to as a black hat hacker whereas Hacking could be a method used by associate assailer to require management of a target while not his can or it's associate endeavour to use associate computer system or a private network among a laptop. Simply put, it is the unauthorized access to or management over network security systems for a couple of illicit purports.

3. What is Ethical Hacking?

Ethical Hacking generally referred to as Penetration Testing or it's additionally referred to as white hat hacking is Associate in Nursing act of intruding/perforating system or networks to determine threats, vulnerabilities in those systems that a maleficent offender might realize and exploit inflicting loss of information, loss or alternative major damages. In this there some certified hacker who works under the guidelines of government means they have authority to do changes a targeted victim (Kumar, 2018). The purport of moral hacking is to ameliorate the safety of the network or systems by fine-tuning the susceptibilities found throughout testing. moral hackers might utilize an equivalent strategies and implements used by the malevolent hackers however with the sanction of the sanctioned person to ameliorate the safety and bulwark the systems from attacks by malevolent users. moral hackers square measure expected to report all the susceptibilities and impotence found throughout the method to the management.

4. Types of Hacking Techniques

4.1 Bait and Switch

Bait & Switch is associate assailment or fraud that utilizes comparatively sure avenues - ads - to illude users into visiting malignant sites. These assailments usually occur within the kind of advertising area being sold by websites and purchased by shady corporations. Once the villain assailants purchase the ad area, they succeed the ad with associate innocuous link that can be later accustomed transfer malware or browser protection or to compromise targeted systems.In some cases, the ad might in addition link to a legitimate web site, programmed to direct you to a way more hostile web site.

4.2 Cookie Theft

Cookies area unit minuscule files that area unit hold on on a utilizer's pc, they're designed to hold a modest quantity of data concrete to a specific shopper and data processor and may well be accessed either by the net server or the patron computer. This sanctions the server to distribute a page tailored to a specific user, or the page itself contains some script that wakeful of the information among the cookie. Predicated on cookies this attack is performed. Cookie stealing happens once a 3rd party copies unencrypted session knowledge and utilizes it to impersonate the authentic user. Cookie stealing most frequently happens once a user accesses trusty sites over associate unprotected or public Wi-Fi network. Albeit the username and parole for a given web site are encrypted, the session knowledge peregrinating back and forth (the cookie) isn't.

By utilizing these cookies, a hacker will access sites and perform baneful actions. counting on the sites accessed whereas the hacker is watching the network, this might be something from creating mendacious posts in this individual's name to transferring mazuma out of a checking account. Hacking computer code has created it a lot of facile for hackers to hold out these assailments by watching the packets going back and forth. Cookie stealing will be evaded by solely work in over SSL affiliations or using HTTPS protocol to write the connection. Otherwise, it's best to not access sites over unsecured networks.

4.3 Virus, Trojan, Worms

Virus stands for "very important resource under suppression " or "vital important resource under siege". A virus is an infectious computer program or small lines of code that may disturb the normal working of a computer system. It attaches itself to files stored on hard drives, USBs, email attachments. If this infected is copied to some other computer, a virus is also copied to another system.

A malicious program or trojan may be a cumulation of malevolent and computer code or may be a variety of malware that's typically dissimulated as legitimate computer code. Trojans are often utilized by cyber\-purloiners and hackers endeavouring to realize access to a utilizer's system. Users square measure generally tricked by some type of gregarious engineering into loading and corporal punishment Trojans on their system. Once activated, Trojans can modify a hacker to spy on you, glom your sensitive info, and gain backdoor access to your system. These actions will embrace:-

- Deleting knowledge
- interference knowledge
- Modifying knowledge
- repeating knowledge
- Reducing the performance of laptops or computer networks.
- not like laptop viruses and worms, trojans don't seem to be ready to self replicate.

The worm is homogeneous virus and likewise a self duplicating program. The distinction between a virus and a worm is that a worm does not append itself to other codes.

4.4 Phishing

Phishing may be a trial to steal sensitive information like usernames, passwords, and credits cards details, typically for malicious reasons, by disguising as a trustworthy entity in transmission. Phishing is typically distributed by email spoofing or instant transmission (Fruhlinger, 2020), and it typically directs users to enter personal information at a faux scientific discipline system, the design and feel of that square measure similar to the legitimate one and also the solely distinction within the uniform resource locator of the web site.

Types of Phishing (Rashid, 2017)

4.4.1 Spear phishing

When assailants endeavour to craft a message to charm to a concrete individual, that's referred to as spear phishing. (The image is of a skilled worker aiming for one categorical fish, rather than merely casting associate enticed hook among the dihydrogen compound to visually perceive UN agency bites). Phishers confirm their targets (sometimes utilizing the data on sites like LinkedIn) and use spoofed addresses to send electronic mails which may most likely look treasure they're emanating from co-workers. as associate example, the spear phisher could target someone among the finance department and faux to be the victim's manager requesting a sizably voluminous bank transfer on short notice.

4.4.2 Whaling

This type of assailment has been directed significantly senior executives and different high-profile targets within a business, and thus the term whaling has been coined for these sorts of attacks. Whale phishing, or whaling, may be a sort of spear phishing aimed toward the deeply and vastly large fish — CEOs or alternative high-value targets.

4.4.3 Vishing

It is a type of attack that is conducted by phone and often target users by Voice over IP (VoIP) services like skype, etc.

4.4.4 Clone Phishing

It is a sort of assailment within which AN wrongdoer engenders a just about identical email, Annexation or link with some malevolent modification so sent from an email correspondence address spoofed to look to emanate from the pristine sender. it's going to claim to resend of the pristine or AN updated version of the pristine.

4.5 Eavesdropping (Passive Attacks)

The term eavesdropping means to listen to someone's private conversation without them knowing. It is also termed as a sniffing attack. In this attacker hiding itself identity over the network and listening to other people talks or steals some valuable information that is transmitted over the network (Admin, 2018). VoIP calls created utilizing IP-predicated communication will be intercepted and recorded utilizing protocol analyzers and captured knowledge area unit later reborn to audio files. The assailers create this attainable with the avail of a network somebody or alternative network observation code either on the laptop or on a server for observation and capturing knowledge throughout transmission. There area unit 2 sorts of eavesdropping attacks in each wired and wireless networks particularly Passive Eavesdropping and Active Eavesdropping.

4.6 Denial of Service

This is the most prevalent attack utilized by Innominate Hackers. A denial-of-accommodation (DoS) assailment may be a variety of cyber attack within which a malignant actor aims to a web site or an online Server to incapacitate its functionalities (Chahuhan). This achieves by flooding the objective with traffic or adventure it data that triggers an accident through this a machine or system is finishing. Survivors of DoS assaults in some cases target web servers of prominent associations like banking, business, and media firms, or system and exchange associations.

DDoS may be a Distributed Denial of Service attack. In straightforward DoS attack here target may be a single machine whereas, in DDoS multiple machine or network server is targeted.

There square measure 2 ways of DoS attacks: flooding accommodations or unmitigated accommodations (Threads). Once associate extravagant quantity of traffic receives for the server to buffer is kenned to be flood attack, inflicting them to decelerate and ceases. Flood attack are:-

4.6.1 Buffer overflow attack

In this the offender is to send a lot of traffic to a network address that the engineer has created the system to handle. It includes the list below:-

- ICMP Flood

In this assailment, Associate in Nursing assailer utilizes a protocol selected net management Message Protocol ~ICMP ping traffic target at an online Broadcast Address.It gains by a misconfigured arrange by causing parodied parcels that ping each PC the focused on organising, in role of 1 machine. The result of this can be decelerating the network by triggered ample traffic. it's in addition referred to as the smurf attack.

- SYN Flood

An assaulter sends need the interest to associate with a server yet never fulfils the affirmation. Propagates until every single open port ar soaked with solicitations and none are available for authentic clients to interface with.

4.7 Keylogger

Keylogger is a function that records the keystrokes produced by keyboard or we can say that keeps an eye on each activity that is done with keyboard ie. typing. It is a tool which is created to steal the login credentials of the logged users in any of the website or any other information which can harm the user. It can be used in the form of both hardware and software.

4.8 DNS spoofing

DNS stands for Domain Name Server. On the internet world, all website or server works on IP address. The IP address is complicated and not easy to remember (Definition of 'Dns Spoofing'), so DNS is a service that transforms a certain Domain into its respective IP address. For example, google.com will be transformed into 172.68.75.200. Here spoofing means to confuse the target. DNS satirizing is finished by overriding the IP addresses put away in the DNS server with the ones heavily influenced by the attacker. when it is done, at whatever point the utilizer tries to go on that specific site, they get coordinated to the unauthentically false site set by the assailer in the ridiculed server.

It is of two types:-

- DNS Cache Spoofing
- DNS ID Spoofing

5. How to detect any Anonymous activity

While studying the study of cyberattacks. We found some signs that are used by Anonymous users (HACKER) to keep an eye on our systems (Grimes, 2019). Our best research found some of those signs that are:-

5.1 After using the internet or insert any third-party plugin devices. After restarting the system you suddenly observe unexpected and unwanted software installs in our systems that itself is a big sign that your device is hacked. It can't be easily removed.

5.2 You get a fake antivirus message on your machine. While aquatics the online, you bought a popup message on your computer or mobile that it's infected. The popup message pretends to be a true antivirus scanning product and is detects dozen of malware infections on your pc. once users click thereon will cause browser failure or creates a lacking drawback in our machine.

5.3 Ransomware messages, in this a message suddenly seems on the screen telling all of their knowledge is encrypted and inquiring for a payment to unlock it. concerning 50\% of the victims square measure paid a ransom, during this variety of condition.

5.4 Your internet searches are redirected, which means that is if a user searches for something and when they clicked on the link the user redirected to somewhere else where the user doesn't want to go or the landed page is not as per the user. The hacker gets paid by obtaining your clicks to seem on someone's else web site.

5.5 When a user landed to a website they see frequent, random popups, ads in this some of are genuine and some of are very dangerous, when got clicked on that popups or ads automatically 3 or 4 pages get open in another tab of the browser which is set by the hacker to steal the user personal information or some other sensitive information.

5.6 Your password no longer works. If your on-line account isn't acceptive your parole otherwise you obtaining logged out of your on-line account would possibly betoken that you simply have fallen into a phishing page. I this a hacker use is to send Associate in Nursing authentic-looking email from a bank or the other accommodations you are signed up for, asking to update your parole by clicking the enclosed link within the electronic message. Once you clicked the link you offer your account access to the hacker.

5.7 If you watched that your cursor is moving on its own or watching words appear on the screen without you typing is a sign of being hacked.

5.8 Your saved files, folder, or any other information are deleted automatically without your permission or the files may missing. It is another clue of being hacked.

5.9 Many people want to use premium services of software or application but they wanted free. In the internet market, there are many cracked versions of the software are available which provide premium service for free with the minimum modification or no viruses in it but some are infected with very harmful viruses in it. After installation that infected software, we can give our PCs in hackers' hands now they can control our system as they want.

6. Prevention:- How to fight back and be safe from Anonymous users and Internet world.

As the above study of different types of a cyber attack on that note below is some security measures on how to detect any type of attack on our system (Grimes, 2019).

6.1 Highly recommended use the best antivirus program of your system, smartphones, tablets, etc. Do not install any cracked or modded antivirus on your system. If it did not have any antivirus you may do enable windows security protection.

6.2 Download software only from trusted websites. While installing the software read all the terms and conditions given there. Some of the software included search bars and other items in it, install it if you want otherwise not. Before download, any software from the internet checks whether it is nor infected or may not contain any viruses in it. I recommended a website that checks online whether the downloaded file contains any virus or not that is: http://www.virustotal.com

6.3 Never click on a suspicious link because it may steal your login details. Only browse https links. While surfing on public network clear all cookies and cache files and history from the browser.

6.4 We would suggest you use private tabs or Incognito mode of the browser, it will help you to browse safe and secure on the network as it will not record our browsing history. Sometimes your searches area unit redirected to some unknown webpages follow these steps for abstracting the unauthentically spurious toolbars and programs, move to C:\Windows\System32\drivers\etc\hosts file to visually understand if there area unit any maleficent-looking redirections designed inside. The host file tells your laptop wherever to travel once a specific universal resource locator indited in. If the file stamp on the host files is something recent, then it'd be malevolently changed. during this case, you simply rename or excise it.

6.5 Nowadays advertisement can be used for most cyber attacks. As when we click on this, we redirected to some other link. On the gap between when we clicked on ads and redirected to another website hackers done his work. Here you guys always enable the ads blocker it helps you to protect from the annoying ads to appear on the screen or websites you visited.

6.6 The websites which need login credentials or signup always choose a strong password. Here strong password means the combination of uppercase and lowercase of alphabets, special characters, and numeric digits.

6.7 When the password is strong then it is difficult for hackers to crack it.

6.8 Do not share any one of your passwords with anyone whether it belongs to social media, ATM pin, net banking, or any other websites.

6.9 Never installs cracked or hacked versions of software on your systems it may contain malware and harmful viruses. For mobiles do not install modded APKs(Andriod Application Packages) it may slow down the performance of mobiles.

6.10 To surf additional in private use VPN(Virtual personal Network). VPNs, sanction you to engender a secure affiliation to a distinct network over the online. VPNs is also acclimated to access region-restricted websites, defend your browsing activity from prying ocular perceivers on public Wi-Fi, and more.

Note: The Internet may be used for better learnings not to harm people. Hacking is a crime.

References

Admin, O. (2018, August 11). EAVESDROPPING ATTACK. Retrieved April 25, 2020, from https://blog.olalekanadmin.pro/blog/2018/08/11/eavesdropping-attack/

Chahuhan, A. a. (n.d.). RETROACTIVE ANALYSIS OF DENIAL OF SERVICE ATTACKS AS PART OF NETWORK FORENSIC.

Definition of 'Dns Spoofing'. (n.d.). Retrieved May 08, 2020, from https://economictimes.indiatimes.com/definition/dns-spoofing/

Fruhlinger, J. (2020, April 7). What is phishing? How this cyber attack works and how to prevent it. Retrieved April 24, 2020, from https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Grimes, R. A. (2019, July 2019). signs you've been hacked. Retrieved Mat 12, 2020, from https://www.csoonline.com/article/2457873/signs-youve-been-hacked-and-how-to-fight-back.html

Kumar, S. a. (2018). Hacking attacks, methods, techniques and their protection measures. *Int. J. Adv. Res. Comput. Sci. Manage, 4*, 2353--2358.

Pandey, B. K. (n.d.). ETHICAL HACKING.

Rashid, F. Y. (2017, October 27). Types of phishing attacks and how to identify them. Retrieved April 22, 2020, from https://www.csoonline.com/article/3234716/types-of-phishing-attacks-and-how-to-identify-them.html

Threads. (n.d.). What is a denial of service attack (DoS) ? Retrieved April 30, 2020, from https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos/