ANUSANDHAN- AISECT University Journal
Vol. 06, Issue No. 12, September-2017, P-ISSN 2278-4187

Hacker's Hacking Technique

Abhishek Gupta[1]* Dr. Jatinder Singh Mahnas[2]

[1]Research Scholar, AISECT University, Bhopal (M.P) India

[2]Sr. Assistant Professor, University of Jammu, (J & K) India

Abstract – Today Hacking has been one of the common practices made by the computer expert in order to try and find vulnerabilities in a network infrastructure. In this paper I have mentioned types of Hackers and types of technique used by them. The word "hacking" has two definitions. The first definition refers to the hobby/profession of working with computers. The second definition refers to modifies computer hardware or software in a way that changes the creator's original intent. Traditionally, a Hacker is someone who likes to play with Software or Electronic Systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically. Recently, Hacker has taken on a new meaning that someone who finds weaknesses in a computer or computer network, though the term can also refer to someone with advanced understanding of computers and computer networks. Finanly I recommend that hacking is the skill miracle so everyone want to become hacker but please used this skill to destroy the crime from society but not to become a criminal.

Keywords: Hackers, Vulnerabilities, Attacks, Black Hat hacker

----------♦----------

I. INTRODUCTION

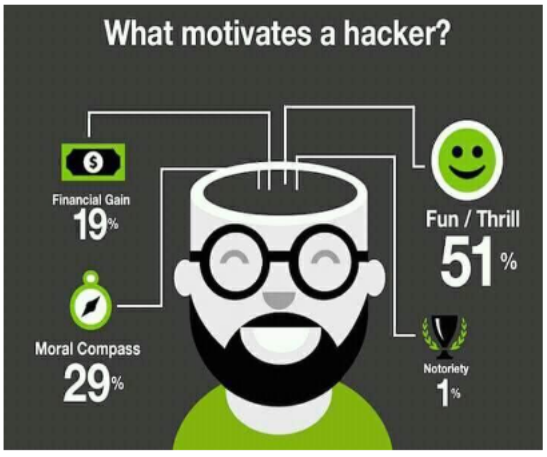
In computing, a **hacker** is any skilled computer expert that uses their technical knowledge to overcome a problem. While "hacker" can refer to any computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems. (Hacker) Today, mainstream usage of "hacker" mostly refers to computer criminals, due to the mass media usage of the word since the 1980s. This includes what hacker slang calls "script kiddies," people breaking into computers using programs written by others, with very little knowledge about the way they work. This usage has become so predominant that the general public is unaware that different meanings exist. (Ben, 2015). While the self-designation of hobbyists as hackers is acknowledged by all three kinds of hackers, and the computer security hackers accept all uses of the word, people from the programmer subculture consider the computer intrusion related usage incorrect, and emphasize the difference between the two by calling security breakers "crackers" (analogous to a safecracker).Currently, "hacker" is used in two main conflicting ways:

(a) as someone who is able to subvert computer security; if doing so for malicious purposes, the person can also be called a cracker (Danish and Muhammad, 2011).

(b) an adherent of the technology and programming subculture.

The controversy is usually based on the assumption that the term originally meant someone messing about with something in a positive sense that is, using playful cleverness to achieve a goal. But then, it is supposed, the meaning of the term shifted over the decades since it first came into use in a computer context and came to refer to computer criminals (Ajinkya, et. al., 2010).

Below mention figure describe how to hacker are attract towards hacking.



II. TYPES OF HACKER

Let me explain about different kind of hackers exist in the cyber security world.

(a) **Script Kiddies-** Script Kiddies are the persons who use tools , scripts, methods and programs created by real hackers. In a simple word, the one who doesn't know how a system works but still able to exploit it with previously available tools.

(b) **White Hat Hacker-**White Hat hackers are good guys who does the hacking for defensing. The main aim of a Whitehat hacker is to improve the security of a system by finding security flaws and fixing it. They work for an organization or individually to make the cyber space more secure.Break The Security only concentrates on white-hat hacking and help you to learn the Ethical Hacking world.

(c) **Black Hat Hacker-** BlackHat hackers are really bad guys , cyber criminals , who have malicious intent. The hackers who steal money, infect systems with malware, etc are referred as BlackHat hackers. They use their hacking skills for illegal purposes.

(d) **GreyHat Hacker-**The hackers who may work offensively or defensively, depending on the situation. Hackers who don't have malicious intentions but still like to break into third-party system for fun or just for showing the existence of vulnerability.

(e) **Hacktivists-**The hackers who use their hacking skills for protesting against injustice and attack a target system and websites to bring the justice. One of the popular hacktivists is Anonymous and RedHack.

III. TECHNEQUE USED BY HACKERS

(a) Bait and Switch

It's been a favorite gag of carnival and street hustlers for centuries: Offer your mark something that they're sure to want, then swap it out for something different when they're not looking. In the digital realm, this trick has several variations.

One of the most common is a scam perpetrated by cyber-criminals on websites (preferably big, high-profile ones) that sell advertising space to third parties. Attackers can acquire sidebars or pop-up panels by registering with a verifiable email address and links to a legitimate-looking site – which is the one that the site administrator gets redirected to. But when the ad goes live, site visitors clicking on the link may be sent to a page that's been booby-trapped with malware. Another variant is the direct appeal to users, with an irresistible download of some fantastic widget or app – which runs malicious code on your website or device once it's installed. If you want great products, software, or desktop/web page gadgets, your best bet is to obtain them from reputable sources (approved app stores, recognized brands and vendors, etc.). And if you're selling advertising space, due diligence should be your watchword.

(b) Cookie Theft

The cookies (little text files) stored in your system or browser cache when you visit various websites can hold a wealth of information about you – including personal and financial data, user credentials, and passwords.Cookies may be stored as plain text, or with varying degrees of encryption (depending on the website). And the use of browser add-ons has made the decades-old practice of cookie theft a richer and easier prospect for hackers.Once stolen, cookies may be read or decrypted to reveal your information, or used to impersonate you online (e.g. if they contain your passwords). Cookie theft may also operate in conjunction with a fake WAP attack (see below), or a hijacked session. Avoiding public or unprotected private networks is your safest bet. Using a VPN (Virtual Private Network) to encrypt and tunnel the connection on your phone or mobile device is also advised. And periodically clearing your browser and system caches will reduce the number of cookies you have available to steal.

(c) Denial of Service/Distributed Denial of Service (DoS/DDoS):

A classic technique used to bring down systems or networks, by overloading them with login attempts, data requests, repetitive tasks, etc.

Attacks range from the fairly basic (configuring a system to continually bombard a site or server with requests), to the orchestrated (infecting a multitude of systems with malware to form a "botnet" that proceeds to flood a target network with unmanageable traffic), to the specific and sophisticated (buffer overflow attack which allow hackers to gain access to personal information by filling online form fields with excess data, so they freeze up).

Systems infected by malware are a common vector for DoS and DDoS attacks, so exercising caution when downloading files or opening email attachments is a basic first step. Having an up to date anti-malware package installed is the next.

If your website hosts an online form, a cloud-hosted security service which uses unified threat management (UTM) technology can be a hedge against overflow attacks.

(d) Eavesdropping:

A passive technique used by hackers to listen in on a network connection and observe and record as much high-value information as possible. Packet sniffing, interception of data transmissions, and other monitoring techniques may be used – but the success of this kind of attack depends on the hackers themselves not being detected or observed.

Unsecured networks are again the greatest gift to eavesdroppers. Users of public WiFi should connect via a VPN. Corporate networks may deploy Intrusion Detection Systems (IDS) and/or Intrusion Prevent Systems (IPS) to guard against eavesdropping.

(e) Keylogging:

One of the simplest and oldest hacking techniques, keylogging allows attackers with basic software to record to a log file the strokes you make on a keyboard (or in more sophisticated cases, the clicks and movements of a mouse). These log files may hold sensitive data like passwords and user names.

Virtual (on-screen) keyboards – which scramble or encrypt your text input as you click on each key – are a guard against this kind of attack. That's why so many banking and online commerce websites use them. They're also available as apps for personal use, and well worth having.

(f) Malware:

One of the greatest weapons in the hacker's arsenal is malicious software of all kinds. Viruses, Trojans (innocent-looking files and programs that deliver a malicious payload later on), worms (for continuous network infiltration), and ransomware can all deliver a handsome pay-day – if you allow them onto your system.

Numerous methods exist to induce unsuspecting users to do just that (some of which are described below).

To avoid becoming infected, exercise caution and due diligence when dealing with email messages and attachments. Disable pop-up windows in your browser, to eliminate the temptation to click on them. Restrict your downloads of software to approved app stores and reputable manufacturers. And keep your anti-malware and security software regularly updated.

(g) Phishing and Related Phenomena:

Using specially crafted email messages to induce a recipient into divulging personal or financial information is the basis of a phishing attack – and hackers have improved on the technique by using social engineering to add an element of increased urgency into their lures.

A not-to-be-missed financial deal or software download. A court summons from the power company, over that unpaid bill. An alert from the police, regarding your recent browsing activity. Any or all of these can be the bait that lures you to a spoofed website where an online form harvests your credentials, or malware is pushed onto your system in a "drive-by download."

Beyond the caution and due diligence already discussed, a dose of common sense is also advised. If you're unsure about a message, call or visit the office or person who supposedly sent it, to verify.

Security awareness training is a good idea for corporate users – as well as the posting of security intelligence, to keep workers advised of the latest threats and scams observed in the wild.

(h) Watering Hole and WAP Attacks:

Setting up a fake wireless access point or WAP (like a spoofed WiFi hotspot) is a great way for hackers to gain a captive audience whose data streams can be monitored, intercepted, or hijacked for various purposes.

Likewise, setting up a bogus but attractive website (like a spoofed social media platform) in a "watering hole" attack is a great way to assemble a herd of unwitting victims in one place – where you can harvest data, or spread a malware infection to the maximum number of recipients.

A Virtual Private Network (VPN) remains your safest option when using wireless access. Caution and a fully updated security and anti-malware suite are your safeguards against watering hole attacks.

(i) "Man in the Middle" (or "MITM") Attack:

Unsecured network connections expose users to this particular tactic, which involves intercepting the data stream between sender and recipient (of an ongoing communication or file transfer). An attacker effectively establishes two connections: One between themselves and a server/sender, and another between themselves and the client/recipient. They can then read or modify the data being passed through their proxy connection.

The objective may be to observe and record a confidential transmission such as an exchange of login credentials or the transfer of intellectual property. Or the attacker may insert malicious code into the data stream, compromising or infecting either or both systems involved in the exchange. If undetected, such attacks may persist for an extended

time period. Secure connections are key to avoiding MitM attacks, and using a reliable VPN is a way of ensuring the required encryption strength and point to point security.

IV. CONCLUSION

The entire world is moving towards the enhancement of technology, and more and more digitization of the real world processes, with this the risk of security increases day by day. In the security empire, we see more and more activity: spyware, viruses, spam. But as the number of malicious black hats increases, we can expect a corresponding increase of security jobs and white hats. We think more and more high-profile attacks on public targets, and snugger controls via legislature. This paper described about the working of hackers and what types of technique they used to hack someone. In conclusion, it must be said that Ethical Hacking is a tool to control the hacker's attack. I think that there is a need of more white hat hackers and need to develop an advanced security system in technology.

REFERENCES

[Hacker07] "Hacker", Wikipedia, 11/8/2007 http://en.wikipedia.org/wiki/Hacker

Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala (2010). "Ethical Hacking, International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, edia.techtarget.com/searchNetworking-Introduction to ethical hacking-Tech Target.

Ajinkya A., Farsole Amruta G., Kashikar Apurva Zunzunwala (2010). "Ethical Hacking", in 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 10

D. Manthan (2010). "Hacking for beginners", 254 pages.

David Melnichuk," The Hacker'sUnderground Handbook ", at http://www.learn-how-to-hack.net

H.M David (2004). "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1.

http://en.wikipedia.org/wiki/Convention_on_Cybercrime

http://www.wired.com/news/politics/0,1283,44007,00.html A 'White Hat' Goes to Jail. MichelleDelio. Wired News.

https://blog.finjan.com/9-common-hacking-techniques-and-how-to-deal-with-them

J. Danish and A. N. Muhammad (2011). "Is Ethical Hacking Ethical? " , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763..

Marilyn Leathers " A Closer Look at Ethical Hacking and Hackers" in East Carolina University ICTN 6865.

Yagoda, Ben (2015). "A Short History of "Hack"". The New Yorker. Retrieved.

Corresponding Author

Abhishek Gupta*

Research Scholar, AISECT University, Bhopal (M.P) India

E-Mail – abhishekgupta141983@gmail.com