VIVA

Institute of Technology
9th National Conference on Role of Engineers in Nation Building – 2021 (NCRENB-2021)

VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

INTERNET HACKING AND PREVENTION

Suraj K. Yadav [1], Prof.Pragati Mestry[2]
[1](*Department of MCA, Viva School Of MCA/ University of Mumbai, India)*
[2](*Department of MCA, Viva School Of MCA/ University of Mumbai, India)*

Abstract :*Understanding the term hacking as any unconventional way of interacting with some system it is easy to conclude that there are enormous number of people who hacked or tried to hack someone or something. The article, as result of author research, analyses hacking from different points of view, including hacker's point of view as well as the defender's point of view. Here are discussed questions like: Who are the hackers? Why do people hack? Law aspects of hacking, as well as some economic issues connected with hacking. At the end, some questions about victim protection are discussed together with the weakness that hackers can use for their own protection. The aim of the article is to make readers familiar with the possible risks of hacker's attacks on the mobile phones and on possible attacks in the announced food of the internet of things (next IoT) devices.*

.

Keywords -*Scalability, Fault tolerance, Performance, Measurements.*

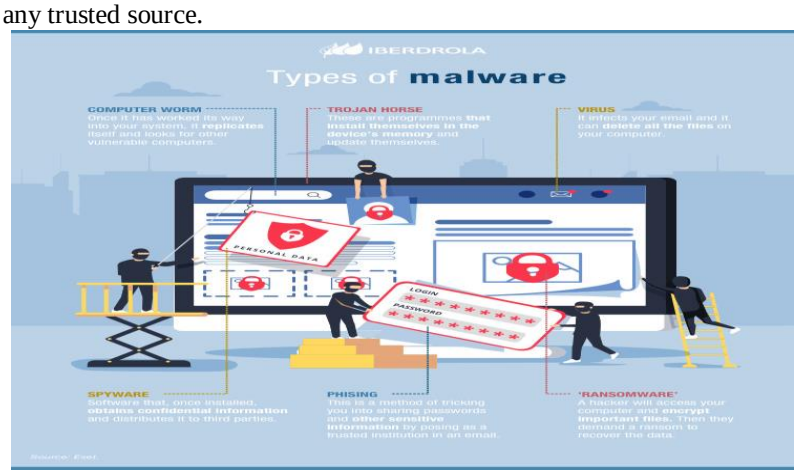
I. INTRODUCTION

Hacking is an unauthorized entry into a network or a computer to steal or manipulate information, data or files. The person involved in this process is named as a hacker. Computer hacking is done using several types of programs such as Rootkit, Trojan, Keylogger etc. Hackers also employ techniques like browser hijacks, spoofing, phishing etc. to capture user's personal or financial details.

Your computer may show certain signs of being hacked such as fake antivirus warning messages, unwanted browser toolbar, redirection to strange websites, random pop ups, ransomware message etc. If you receive any of these warning signs, you can be sure that your computer has been targeted by a hacker.

Prevention:If you are planning to download a music file, video or a utility software do so from a trusted website. Many websites offer a free download of certain high-value software, but those may carry the virus or a spyware released by a hacker to obtain your PC information.

Email is one of the biggest tools through which hackers spread malware. The spyware or virus are hidden in attachments and links clicking on which the infection begins. Hence, never click on random attachments if those are not from any trusted source.



II. SYSTEM INTERACTIONS

Patch and Update Constantly

Ultimately the most hacker-resistant environment is the one that is best administered. Organizations are short cutting system and network administration activities through budget / staff reductions and lack of training. This practice often forces prioritization and choice about what tasks get done sooner, later or at all. Over time this creates a large, persistent baseline of low to medium risk issues in the environment that can contribute to a wildfire event under the right conditions. Lack of a complete asset inventory – both hardware and software – contributes to this risk as applications and devices become unmanaged. Staying on top of patching, system/application updates, end of support/life platform migrations, user administration and configuration management is tedious, time consuming, and generally underappreciated; but this activity - more than any other single task, will reduce the risk of cyber events in an organization and dramatically reduce the risk of opportunistic attacks.

Email Security

Email is the number one entry point for malware into the enterprise. No surprise really. Given all the data that has pointed to this as the root cause of many breach events, it should be the next place where organizations double-down on security. It is very important that organizations take the time to be informed consumers in this regard and understand what threats the email controls are preventing and what the remaining exposures are so that a layered control model can be put in place.

Endpoint Detection and Response

Most of that email is destined for a user that will click on attachments and potentially infect themselves with malware of some kind. The second most common malware infection vector is through malicious web content; also, an end-user action. As a result, it makes sense to have a thorough suite of controls on the endpoints and servers in the environment to identify and shutdown viruses, malware, and other potentially unwanted programs. Making sure that all endpoints are under management and kept current will help prevent whack-a-mole malware infections that can persist in environments with inconsistently applied controls.

Segmentation and Egress Filtering

Just because a hacker or piece of malware makes its way into your environment, doesn't mean they should be able to spread adjacent network nodes or waltz back out with your mission critical, regulated data. Limiting the ability to communicate both across and outside the network through a combination of controls such as firewall policies and requiring the use of proxy servers is an often-overlooked opportunity for organizations to increase their security, limit the impact of an incident and help prevent a network incident from becoming a public data breach.

Robust Detection Control Infrastructure

History teaches us that prevention-centric strategies will fail and should be paired with detective controls to minimize time to detection and remediation. Make certain you have a well-tuned SIEM/SOAPA/SOAR infrastructure as part of your security architecture and that that is receiving logs that cover the internal network and applications as well as through the perimeter. This includes tuning of endpoint, application, and network device logs to enable an early detection and response capability in the environment.

Multi-factor / Multi-step Authentication

The majority of breaches involve the use of cracked, intercepted or otherwise disclosed authentication credentials at some point. Use strong, multi-factor authentication methods by default wherever possible. Combined with the ability to detect and alert on failed login attempts, this practice can provide clues to users that may be the focus of targeted attacks.

III. MASTER OPERATION

In order to prevent this unauthorized intrusion into your systems/networks , you must follow some basic security guidelines:

DOWNLOAD SOFTWARE FROM AUTHORIZED WEBSITES

If you are planning to download a music file, video or a utility software do so from a trusted website. Many websites offer a free download of certain high-value software, but those may carry the virus or a spyware released by a hacker to obtain your PC information.

DO NOT CLICK ON RANDOM EMAIL ATTACHMENTS

Email is one of the biggest tools through which hackers spread malware. The spyware or virus are hidden in attachments and links clicking on which the infection begins. Hence, never click on random attachments if those are not from any trusted source.

SCAN ALL TYPES OF HARD DRIVES BEFORE RUNNING

Hard drives such as pen drives, external hard disk or mobile devices should be scanned by a USB scanner to remove any kind of malware.

ABSTAIN FROM KEEPING EASY PASSWORDS

Do not keep easy passwords such as- your name followed by1234, your pet name or name & date of birth etc. These information can be easily guessed or can be fetched from social media sites, so follow best password management practices. You should keep an alpha-numeric password for your accounts including a combination of special characters.

NEVER STORE OR SHARE YOUR LOGIN INFORMATION

Keeping your user id, password on your PC increases the risk of becoming a victim of hackers. Always try to memorize your login information. It is also important to abstain from sharing your password via email.

Importance of an Anti-hacking Software

Anti-hacking software is also known as a computer antivirus software, which is a must have for every PC. Anti-hacking software protects a PC from these cyber attacks by detecting and removing the virus, spyware, and other malware intrusions. The antivirus software must be kept updated with the latest virus signature so that any types of new threats can be detected. REVE Antivirus software is ideal for internet users as it protects your computer's data from hackers.

IV. FAULT TOLERANCE AND DIAGNOSIS

FAULT TOLERANCE

Fault tolerance is a technique that has proven to be efficient to implement computing systems able to provide a correct service despite accidental phenomena such as environmental perturbations (external faults), failures of hardware components (internal physical faults), or even design faults such as software bugs. Faults are causes of errors, errors are abnormal parts of the computing system state, and failures happen when errors propagate through the system-to-user interface, i.e., when the service provided by the system is incorrect.

When faults are accidental and sufficiently rare, they can be tolerated. To do so, errors must be detected before they lead to failure, and then corrected or recovered: this is the role of error handling. It is also necessary to diagnose the underlying faults (i.e., to identify and locate the faulty components), so as to be able to isolate them, and then replace or repair them, and finally to re-establish the system in its nominal configuration: fault diagnosis, isolation, repair and reconfiguration together constitute fault handling.

There are various techniques for detecting errors. For simplicity, we categorize these as being either property-checks or comparison-checks. Property-checks consist in observing the system state, in particular certain values or events, and verifying they satisfy certain properties or rules. This usually imposes only a small hardware or software overhead (redundancy). Among hardware property-checks, let us note that most microprocessors detect non-existing or unauthorized instructions and commands, non-existing addresses and unauthorized access modes, and that watchdogs can detect excessive execution durations. Software-based property-checks include likelihood tests inserted into programs to check the values of certain variables, or the instants or sequences of certain events (defensive programming).

Error detecting codes and run-time model checking can also be viewed as property-checks. Comparison-checks consist in comparing several executions, carried out either sequentially on the same hardware, or on different hardware units. This requires more redundancy than the first class of error detection techniques, but it also assumes that a single fault would not produce the same effect (i.e., identical errors) on the different executions. If only internal physical faults are considered, the same computation can be run on identical hardware units, since it is very unlikely that each hardware unit would suffer an identical internal fault at the same execution instant to produce the same error. On the contrary, design faults would produce the same errors if the same process is run on identical hardware units, and thus the comparison of the executions would not detect discrepancies. In that case, it is necessary to diversify the underlying execution support, so that a single design fault would affect only one execution, or at least would affect differently the different executions.

To be able to do that, it is necessary to have created and saved copies of the system state, known as recovery points or checkpoints. Another error correction technique is called forward recovery, which consists of replacing the erroneous system state by a new, healthy state, and then continuing execution. This is possible, for example, in certain real-time control systems in which the system can be re-initialized and input data reread from sensors before continuing execution.

Finally, a third technique consists in “masking” errors; This is possible when there is enough redundant state information for a correct state to be built from the erroneous state, e.g., by a majority vote on three (or more)

executions. In most cases, the efficacy of fault tolerance techniques relies on the fact that faults are rare phenomena that occur at random points in time. It is thus possible, for example in a triple modular redundant architecture, to suppose that is unlikely for a second unit to fail while a failed unit is being repaired. An attacker that succeeds in penetrating one system can pursue his attack on that system, and also simultaneously attack other similar systems.

Diagnostic Tools

It should be noted that most currently available intrusion detection systems do not include any intrusion diagnosis mechanisms. The explicit recognition of the fact that misuses and anomalies are indeed errors that can be caused by any sort of fault. Indeed, a good intrusion detection system requires such a fault diagnosis mechanism to minimize the rate of false alarms caused by errors due to other classes of faults.

V. MEASUREMENTS

1. Use a firewall.

Windows and macOS have built-in firewalls – software designed to create a barrier between your information and the outside world. Firewalls prevent unauthorized access to your business network and alert you to any intrusion attempts.Makesure the firewall is enabled before you go online. You can also purchase a hardware firewall from companies such as Cisco, Sophos or Fortinet, depending on your broadband router, which also has a built-in firewall that protects your network. If you have a larger business, you can purchase an additional business networking firewall.

2. Install antivirus software.

Computer viruses and malware are everywhere. Antivirus programs such as Bitdefender, Panda Free Antivirus, Malwarebytes and Avast protect your computer against unauthorized code or software that may threaten your operating system. Viruses may have easy-to-spot effects – for example, they might slow your computer or delete key files – or they may be less conspicuous.Antivirus software plays a major role in protecting your system by detecting real-time threats to ensure your data is safe. Some advanced antivirus programs provide automatic updates, further protecting your machine from the new viruses that emerge every day. After you install an antivirus program, don't forget to use it. Run or schedule regular virus scans to keep your computer virus-free.

3. Install an anti-spyware package.

Spyware is a special kind of software that secretly monitors and collects personal or organizational information. It is designed to be hard to detect and difficult to remove and tends to deliver unwanted ads or search results that are intended to direct you to certain (often malicious) websites.Some spyware records every keystroke to gain access to passwords and other financial information. Anti-spyware concentrates exclusively on this threat, but it is often included in major antivirus packages, like those from Webroot, McAfee and Norton. Anti-spyware packages provide real-time protection by scanning all incoming information and blocking threats.

4. Use complex passwords.

Using secure passwords is the most important way to prevent network intrusions. The more secure your passwords are, the harder it is for a hacker to invade your system.

More secure often means longer and more complex. Use a password that has at least eight characters and a combination of numbers, uppercase and lowercase letters, and computer symbols. Hackers have an arsenal of tools to break short, easy passwords in minutes.

Don't use recognizable words or combinations that represent birthdays or other information that can be connected to you. Don't reuse passwords, either. If you have too many passwords to remember, consider using a password manager, such as Dashlane, Sticky Password, LastPass or Password Boss.

5. Keep your OS, apps and browser up-to-date.

Always install new updates to your operating systems. Most updates include security fixes that prevent hackers from accessing and exploiting your data. The same goes for apps. Today's web browsers are increasingly sophisticated, especially in privacy and security. Be sure to review your browser security settings in addition to installing all new updates. For example, you can use your browser to prevent websites from tracking your movements, which increases your online privacy. Or, use one of these private web browsers.

6. Ignore spam.
Beware of email messages from unknown parties, and never click on links or open attachments that accompany them. Inbox spam filters have gotten pretty good at catching the most conspicuous spam. But more sophisticated phishing emails that mimic your friends, associates and trusted businesses (like your bank) have become common, so keep your eyes open for anything that looks or sounds suspicious.

7. Back up your computer.
If your business is not already backing up your hard drive, you should begin doing so immediately. Backing up your information is critical in case hackers do succeed in getting through and trashing your system.Always be sure you can rebuild as quickly as possible after suffering any data breach or loss. Backup utilities built into macOS (Time Machine) and Windows (File History) are good places to start. An external backup hard drive can also provide enough space for these utilities to operate properly.

8. Shut it down.
Many businesses, especially those operating a web server, are "all systems go" all the time. If you're not operating a complex internet-based company, however, switch off your machine overnight or during long stretches when you're not working. Always being on makes your computer a more visible and available target for hackers; shutting down breaks the connection a hacker may have established with your network and disrupts any possible mischief.

9. Use virtualization.
Not everyone needs to take this route, but if you visit sketchy websites, expect to be bombarded with spyware and viruses. While the best way to avoid browser-derived intrusions is to steer clear of unsafe sites, virtualization allows you to run your browser in a virtual environment, like Parallels or VMware Fusion, that sidesteps your operating system to keep it safer.

10. Secure your network.
Routers don't usually come with the highest security settings enabled. When setting up your network, log in to the router, and set a password using a secure, encrypted setup. This prevents intruders from infiltrating your network and messing with your settings.

11. Use two-factor authentication.
Passwords are the first line of defense against computer hackers, but a second layer boosts protection. Many sites let you enable two-factor authentication, which boosts security because it requires you to type in a numerical code – sent to your phone or email address – in addition to your password when logging in.

12. Use encryption.
Even if cybercriminals gain access to your network and files, encryption can prevent them from accessing any of that information. You can encrypt your Windows or macOS hard drive with BitLocker (Windows) or FileVault (Mac), encrypt any USB flash drive that contains sensitive information and use a VPN to encrypt web traffic. Only shop at encrypted websites; you can spot them immediately by the "https" in the address bar, accompanied by a closed-padlock icon.

VI. CONCLUSIONS

Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking. The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.
Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.
Cybercrime is committing a crime with the aid of computers and information technology infrastructure.
Ethical Hacking is about improving the security of computer systems and/or computer networks.
Ethical Hacking is legal.Today hackers are spread across the world in large quantities. Many government and private agencies are working to detect these hackers, but we also have some duty to protect ourselves and our private data from online frauds. Apart from this, people who are illiterate should be given information about debit cards, credit cards, the internet, and computer. We know it is a bit difficult to catch these hackers because they sit in one country and hack the computer from another country, so the best way to avoid these things is that we have to be careful and alert and all IDs and Passwords on the Internet should always be unique and strong.

Finally, I would like to say that if you use the internet properly and use the secure websites, then it will be difficult for hackers to hack your data.

VII. ACKNOWLEDGEMENTS

I thank my college for giving us the opportunity to make this project a success. I offer my special thanks and sincerity.
I thank Professor Krutikavartak for encouraging me to complete this research paper, for guidance and assistance for all the problems I encountered while doing research.
Without his guidance, I would not have completed my research paper.

VIII. REFERENCES

[1] Sanctum Inc, "Ethical Hacking techniques to audit and secure web enabled applications", 2002.
[2] B. Reto, "Ethical Hacking", in GSEC Practical Assignment, Version 1.4b, Option 1, Nov 24, 2002.
[3] Smith B., Yurcik W., Doss D., "Ethical Hacking: the security justification redux", IEEE Transactions, pp. 375- 379, 2002.
[4] J. Danish and A. N. Muhammad, "Is Ethical Hacking Ethical? " , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011.
[5] Ajinkya A. Farsole, Amurta G. Kashikar and ApurvaZunzunwala , "Ethical Hacking, International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010.
[6] H.M David, "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1, Feb 23, 2004.
[7] Ajinkya A., FarsoleAmruta G., KashikarApurvaZunzunwala"Ethical Hacking", in 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 10
[8] Marilyn Leathers "A Closer Look at Ethical Hacking and Hackers" in East Carolina University ICTN 6865.
[9] Gilberto Tadayoshi Hashimoto, Pedro Frosi Rosa, Edmo Lopes Filho, Jayme Tadeu Machado, A Security Framework to Protect Against Social Networks Services Threats, 2010 Fifth International Conference on Systems and Networks Communications.