(s)AINT

An Awareness on Windows Hacking

[1]Christo Siby, [2]Liya Santhosh, [3]Meera Manoj, [4]Ms. Lisha Varghese

[1,2,3,4] *Amal Jyothi College of Engineering, Kanjirappally, 686518*

[1]christosiby@mca.ajce.in, [2]liyasanthosh@mca.ajce.in, [3]meeramanoj@mca.ajce.in, [4]lishavarghese@amaljyothi.ac.in

Abstract **-- In this digital era, people are more depending on technologies to do their daily works. People are more comfortable in using gadgets such as smartphones, laptops, computers and much more. The most important and essential component of a computer is a system software called operating system. Nowadays majority of the people are using Windows Operating system because of its attractive features. As technology develops system becomes more vulnerable to attacks. This paper discuss about (s)AINT, one such tool that makes the system vulnerable to attacks. Msfvenom, Metasploit, Puppyrat etc. are some other tools that makes the system vulnerable to attacks.**

I. INTRODUCTION

Personal computing users are vulnerable to computer security [1] threats as they have little knowledge of the technology and its complications. Advanced technologies and the internet have provided immense benefits by eliminating geographic boundaries and linking everything together. However when everything become linked together, this benefit has opened up many chances of crimes and fraudulent activities by exposing the home computer's sensitive data to cyber-attacks and threats. The users must be aware of the complications of connecting computers via network [2] and protecting data as it passes through the network along with protecting the personal data in the system from attacks through the network. Honeynets [3] is a simulation network that can be used by researchers in areas of computer security [10] [17] to check for network vulnerabilities. Honeynet provides information on current security threats [18] [19] and techniques and tools used by hackers.

Exploit [6], is a software, a piece of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended behaviour to occur on computer software, hardware. It is an attack on a computer system, especially one that takes advantage of a particular vulnerability the system offers to intruders. Digital certificates ensure that the data in transit or at rest is secure from illegal access. Hackers can exploit the technology by creating fake certificates that resemble the genuine certificates. The forged certificates can be used for malicious intent.

Key logging [4] [15] is a system that is designed to secretly monitor and log all keystrokes [9]. It is a process of secretly recording all the keystrokes of the user. Spyware [5] is software, usually installed without the user's consent or knowledge, that gathers information secretly from a computer and relays that information, also covertly, to someone else. Spy-ware [5] [14] can become installed and active on a computer or network [16] without the user's permission or knowledge makes it a particular threat to businesses, since it can cause harm in a variety of ways if left undetected. Among the various cyber-attacks existing in computers, malware attack is considered dangerous, due to its passive and sleathy nature of attack execution .The malware attack is a type of cyber-attack, which performs the activities on the victim's system initiated by the malware author .The malware attack could be executed by various means such as hardware, spyware [11] [12] [13], keylogger [6] etc.

II. LITERATURE REVIEW

Nik Thompson, Tanya Jane McGill b, Xuequn Wang [1] says the pervasiveness and accessibility of the Internet [1] have provided immense social benefit by linking communities and dissolving geographic boundaries. However, while communities have been brought together by developments in technology, this free, borderless communication has opened up new avenues for crime and fraud, exposing millions of home computer users to cyber criminals across the globe.

According to Camille Cobb, Samuel Sudar, Nicholas Reiter, Richard Anderson, Franziska Roesner, Tadayoshi Kohno, data collected [7] may include information that may be considered sensitive, such as medical or socioeconomic data,

and which could be affected by computer security [20] attacks or unintentional mishandling. The attitudes and practices of organizations collecting data have implications for confidentiality, availability, and integrity of data. Technology has become an important tool for many non-governmental organizations (NGOs) and groups collecting data in the developing world. For example, technology can provide people in remote regions with access to financial services and allow organizations to collect vital information within communities they serve. Information and Communication Technology for Development (ICTD) is the study of what technology can accomplish and how technology is used in such low-resource settings around the world.

Lloyd F. Reese [8] says that the basic threats, fire, water, and people (especially insiders) are still there, as well as a few new ones such as terrorism and viruses. Vulnerabilities [8] become more complicated with the advances of technology and more connectivity.

Stephen E Barnett says that users must understand the implications of connecting computers [2] to networks and protecting information as it traverses the network, as well as protecting information systems from attack via the network.

Shiva Azadegan and Vanessa McKenna describes about honeynet [3] is that it is a vulnerable and simulated computer network using a decoy server designed to test network security. Honeynets are developed in order to help computer security experts to improve security for networks and systems. Honeynets have been proven to be valuable research and teaching tool in the area of computer security and information assurance. A Honeynet is a series of computers with known and unknown vulnerabilities with the express purpose of being compromised by an intruder.

III. METHODOLOGY

System hacking is the process of computer systems and software to gain access to target computer and steal or misuse their sensitive data. Hackers exploits the weakness in the system or network to gain unauthorized access to its data. The hackers are able to hack the systems as they have the knowledge of the actual working of the system and software. These online villains generally use viruses, malware, Trojans, worms, phishing techniques, email spamming, social engineering, exploit operating system vulnerabilities, or port vulnerabilities to get access to any victim's system. When your system gets connected to the internet, the hackers run or install their malware or malicious software on your system to gain access to your system without your concern. After gaining unauthorized access to the target system, they may do the following,

- Use the data
- Delete the files
- Steal files and folders
- Hijack usernames and passwords
- Steal money and credit card details while the victim is doing online transactions and e-marketing.
- Sell victim's information to third parties
- Create network traffic to deny access to the internet
- Manipulate the files and data

Linux is considered to be the most secure OS to be hacked or cracked, but in the world of Hacking, nothing is 100% secured. In many cases, hacker detect bugs that are present in the Linux system to take advantage of them to gain access to the data and files.

The password that appears after the login protects the system and the files from unauthorized access. Choosing a strong password is an excellent practice to prevent unauthorized access. There are several tricks and techniques to crack a windows password. But from the hacker's point of view if a system is found open, he can easily get the password and change it to a new one without the concern of the owner.

(s)AINT is a Spyware Generator used for generating payloads that can be used for hacking Windows systems. (s)AINT is written in Java. It creates an exe file that can be installed on the victim's windows based system and sends system actions to the specified email. It records the user activities of the affected system such as the keystrokes of the user, screenshots of system, webcam capture etc.

IV. IMPLEMENTATION

Steps are as follows

1. Open (s)AINT interface and update to the newer version
2. Entre e-mail address and other options such as the email address (to which the victim's data to be send), password. We can enable (y) or disable (n) other features such as screenshot, persistence, webcam etc. Also set the maximum characters to send to email.
3. Spyware file is generated- Next, confirm all the above entered details. Then enable (y) the option to generate .exe file. Make sure that the access to less secure apps is enable for the entered Gmail account. This can be done in the Google account settings.
4. Run the .exe file in windows system - Copy/Send the .exe spyware file application from the target/ folder to the victim's system. Just a double click (by the victim) will install the spyware on the corresponding system. Then a local folder named (s)AINT will be created inside users/appdata folder. Thereafter all the keystrokes, screenshots, webcam images of victim's computer will be stored in the local folder.
5. Data send to E-mail - All the keystrokes, screenshots, webcam images of victim's computer will be send directly to the given email address at specific time intervals.

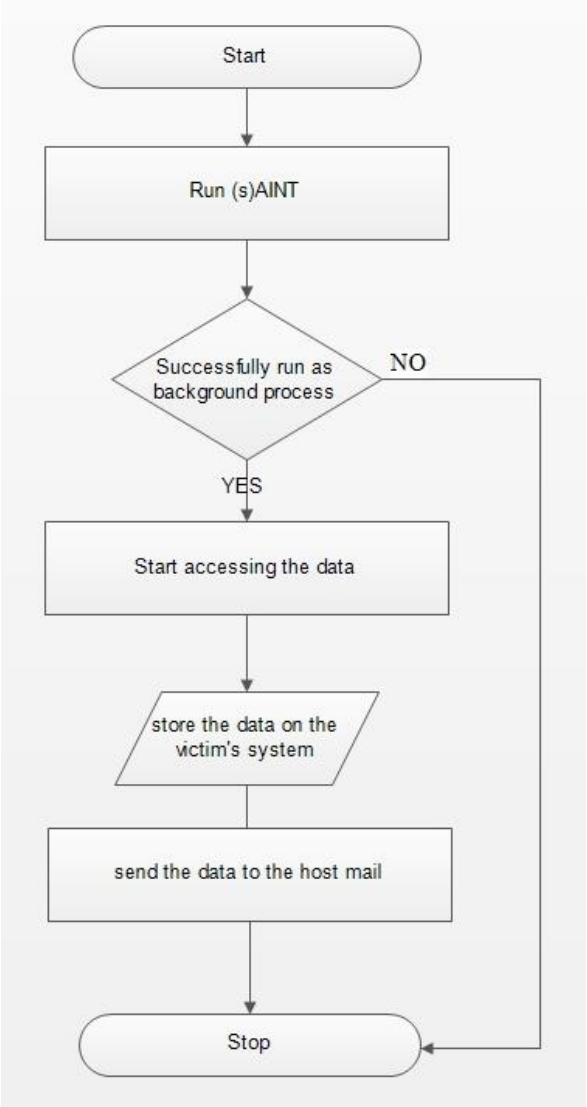

Figure 1 : Working of (s)AINT

V. PRECAUTIONS

Extreme care must be taken while using system and interner. The following precautions must be kept in mind while dealing with internet connected systems.

- Use firewall and keep your system up to date.
- Avoid untrusted websites.
- Use Internet Security Antivirus and Anti-malware software protection and keep them updated.
- Improve browser security settings.
- Download files only from trusted websites.
- Immediately delete those messages which you suspect as spam.
- Always use genuine software and avoid cracked versions.

VI. CONCLUSION

This paper discusses the vulnerabilities and threats that the normal Windows users may experience while using the system. Technology has two sides like a coin, the negative and positive sides. Both sides can be used efficiently and effectively for the betterment and welfare of humans. As technology develops, the exposure to attacks increases. One way to prevent the harms of technology is to create awareness among the users regarding the bad side of technology. The more aware the users are, the less vulnerabilities harms them. Hence it is important to use the technology wisely.

VII. REFERENCES

[1] "Security begins at home": Determinants of home computer and mobile device security behaviour Nik Thompson a, *, Tanya Jane McGill b , Xuequn Wang b. (a) School of Information Systems, Curtin University, Kent Street, Bentley, Western Australia, 6102, Australia (b) School of Engineering and Information Technology, Murdoch University, South Street, Murdoch, Western

[2] COMPUTER SECURITY TRAINING AND EDUCATION: A NEEDS ANALYSIS Stephen E Barnett Deputy Director National Computer Security Center sbarnett@romulus.ncsc.mil

[3] Use of Honeynets in Computer Security Education Shiva Azadegan Towson University azadegan@towson.edu Vanessa McKenna Towson University vmckenna@jhu.edu

[4] Skeleton keys: the purpose and applications of Keyloggers Oleg Zaitsev, Kaspersky Lab

[5] Spyware: the spy in the computer Stephen Hinde

[6] Vulnerability and Exploitation of Digital Certificates Mustafa Jawad Radif Computer Science & Information Technology College, University of Al-Qadisiyah mustafa.radif@qu.edu.iq

[7] Computer security for data collection technologies Camille Cobb, Samuel Sudar,, Nicholas Reiter, Richard Anderson, Franziska Roesner, Tadayoshi Kohno ICTD Lab and Computer Security & Privacy Research Lab Computer Science & Engineering, University of Washington, USA

[8] Challenges Faced Today By Computer Security Practitioners Lloyd F. Reese ADP Security Division Department of Veterans Affairs Washington, D. C. 20420

[9] A Framework for Detection and Prevention of Novel Keylogger Spyware Attacks Mohammad Wazid Avita Katal, R.H. Goudar, D.P. Singh and Asit Tyagi Robin Sharma] and Priyanka Bhakuni

[10] Integrating Computer Security into the Undergraduate Software Engineering Classes: Lessons Learned Susan Pancho-Festin (spfestin@dcs.upd.edu.ph) Marie Jo-anne Mendoza (joannemmendoza@gmail.com)

[11] DETECTION OF SPYWARE IN SOFTWARE USING VIRTUAL ENVIRONMENT Narasima Mallikarajunan K.M.E, Preethi.S.R, Nithish.N Selvalakshmi.S

[12] Defeating Hardware Spyware in Third Party IPs Amr Al-Anwar, Yousra Alkabani, M. Watheq El-Kharashi, Hassan Bedour

[13] Spyware : the spy in the computer Stephen Hinde

[14] Spyware : more than a costly annoyance Dario Forte, Milano University

[15] Keyloggers – your security nightmare? Sacha Chahrvin, SmartLine

[16] Cybergrenade : Automated Exploitation of Local Network Machines via Single Board Computers Anurag Akkiraju, David Gabay, Halim Burak Yesilyurt, Hidayet Aksu, Selcuk Uluagac

[17] Study on Security and Prevention Strategies of Computer Network Fuguo Li

[18] The Study on Computer Network Security and Precaution SUN Xiaoling

[19] COMPUTER SECURITY TRAINING AND EDUCATION: A NEEDS ANALYSIS Stephen E Barnett

[20] Security and Precaution on Computer Network CHEN Yan-ping, LIU Dong-liang, GUO Rui