SALAMI THEFT-MAJOR THREAT TO INFORMATION SECURITY

Lalitha Venkatesan.A[1]

[1]*Assistant Professor, Department of Computer Science, SreeNidhi Institute of Science and Technology, Hyderabad, Telangana.*

Abstract

Information is a valuable asset to any organization or person in specific. This information should be well maintained (free from danger).When ordinary information is so important, imagine how important the sensitive information is. The information security is called as well-informed sense of assurance that the information risks and controls are in balance. Till now there have been many research were carried out to overcome salami theft, but all of them seems to be very impractical. Salami theft also called as Penny Shaving which happens when an employee or any person steals a few pieces of information at a time, knowing that taking more would be noticed, but eventually the employee gets something complete or usable one which can also be called as NNT(Not Noticed Theft)or (Very Critical When Found Theft (VCWFT)).These type of thefts can be overcome by imposing the concept of ethical hacking on to salami theft to detect and also correct the theft of SInfo (Sensitive Information) at a very earlier stage itself.

Keywords: *salami theft, Sensitive information (SInfo), information risk, ethical hacking.*

----------***----------

1. INTRODUCTION

The components of information system of CNSS model are software, hardware, data, people, procedures and network. These six critical components enable information to be input, processed, output and stored. Rather than seeing the information security as an art or science it is very important to consider it as social science [1].Social behavior is being a major threat in data stealing or data diddling[2]. Data diddling is the changing of data before or after entry into the computer system.

A successful organization should have the necessary layers of security they are physical security, personnel security, operation security, communication security and almost the information security [1].

Information security is to protect the confidentiality, integrity and availability of information assets. It is achieved via the application of policy, education, training, awareness and technology. The CNSS defines the information security as the protection of information and its critical elements.Any defalcation or embezzlement accomplished by tampering with computer programs, data filing operation and equipment or media.

2. EXISTING SYSTEM

2.1 Salami Attack and Piecemeal Strategy

Salami attack [8] is a series of minor attacks that together results in a large or major attack. Salami attack can be of two types they are insider attack and outsider attack. The most often done attack is the insider attack (one knows about the security system) which spoils trust worthiness of an organization. Outsider attack can be made by others for any purpose or sometimes wontedly done attacks. Salami attack is also called as piecemeal strategy used by the Nazi party [8].

2.2 Salami Attack Types

Salami tactics has been used [8] since 1940s to refer to divide and conquer. Salami technique used in e-banking, ,information gathering, fun making, revealing one's sensitive information and so on. Salami attacks can be made either accidental or intentional acts are profound [9].Some of the characteristics of accidental and intentional attacks can be frequency, unsolved problems, act complexity, singularity of source, complexity of perpetrator behavior, sources of security assistance, security checklist, strategy and safe guard independence, safeguard comprise, level of protection, potential perpetrators, loss limits and detection and so on.

2.3 Computer as Target or Tool

The computer is used here as both the target and also a tool to perform the hacking of information i.e., stealing of sensitive information. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult [12], which means the computer acts as both the subject and object of an attack.

Fig 2.3. Computer as the subject and object of an attack

2.4 Techniques Involved

The salami technique can also refer to aggregating small amounts of information from many sources to derive an overall picture of an organization, [3]. For instance,

information from a company's web site, advertisements, trash deposits, media reports, and incidents viewed first-hand, or stolen documents could be used to build a large database. The other names for the salami theft are dividing and conquer, collect- the – round off technique, piggy back or impersonation.

3. PROPOSED SYSTEM

Here I propose the available concept of ethical hacking onto salami theft to overcome such information security issues. As this theft is the NNT or VCWFT it is highly difficult to monitor and trace them and all the most the data loser should be very conscious about the information type (public, for official use only, sensitive, classified). Every hacker (white guys) should have skill sets like Languages, Networks, Operating System, Firewalls, Network Protocols, Mainframes and Project Management as such. The optimal solution to overcome salami theft is to attack my own information (SInfo) from threat, but till now the concept of ethical hacking is widely available but not used in the sense of salami theft. The theft detection has been not introduced much in Salami Attack but gives some preventive measures to overcome the same.

4. EXPERIMENTATION

In this section, I have worked with some tools (Nmap, Traceroute,NSlookup and Key loggers) to know how hacking can be so destructive but in terms of ethical hacking over salami theft, it is very constructive in nature because the SInfo is being protected. The figure 4.1 and 4.2 shows the work done with certain tools to support the preliminary part of the research on Salami Theft.

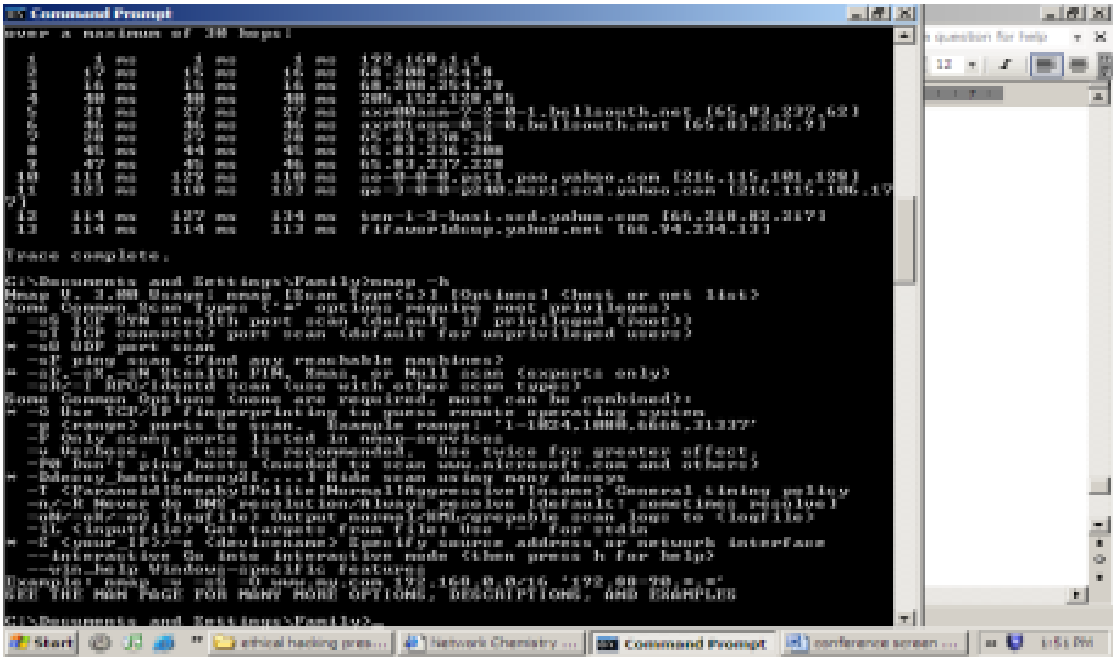

Fig 4.1 Nmap

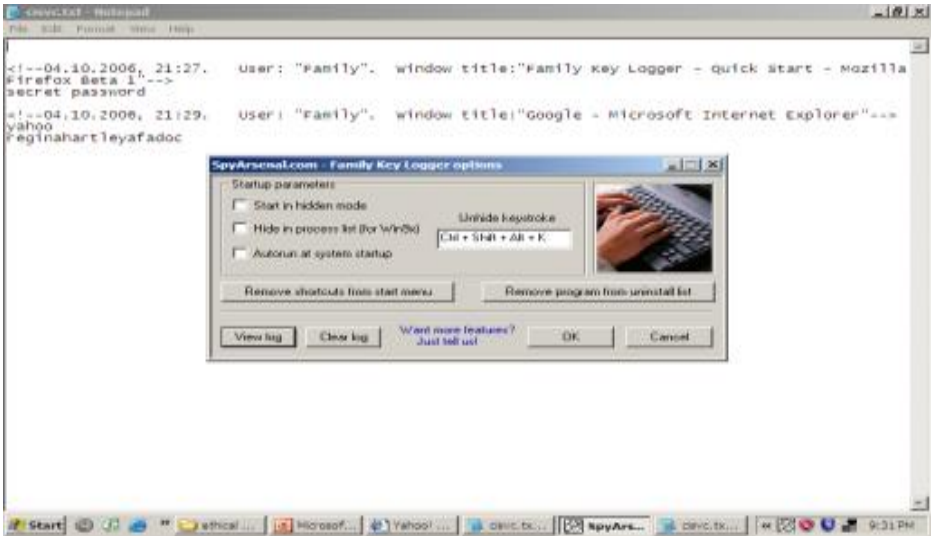

Fig 4.2 Key loggers

5. CONCLUSION AND FUTURE ENHANCEMENTS

According to my knowledge, ethical hacking can be the candidate solution for NNT (Salami Theft) by keeping your password and other SInfo very confidential. Very often found, Salami thefts occur because of user's lethargy especially in maintaining a single password (Unique Password) for many accounts. This particular practice should be avoided so that the theft can be noticed as well and also detected. Proper base lining or bench marking techniques to be followed with best privacy policies. Even a small SInfo (Sensitive Information) can cause serious issues. For any theft concerned, only permanent solution can be "Social engineering" where people are the weakest link in leaking the sensitive information besides best technology. The future enhancements can be made in creating alerts called as "Salami Alerts" or "NNT alerts" as and when the theft happens to monitor and track your information (asset).

REFERNCES

[1]. Principles of Information Security by Michael E.Whitman, Herbert J. Mattord, Cengage Learning, 4th edition.

[2]. Data Diddling http://www.urbandictionary.com/define.php?term=data+diddling

[3]. Salami Fraud by M. E. Kabay, PhD, CISSPAssociate Professor, Computer Information Systems, Norwich University, Northfield VT

[4]. Computer security differences for accidental and intentionally caused losses, DONN B. PARKER, SRI International Menlo Park, California

[5]. Aderucci, Scott. Salami Attacks. www.all.net/CID/Attack/papers/Salami.html [This is a previous student paper written on salami attacks].

[6]. Kabay, M.E. Salami Fraud www.nwfusion.com/newsletters/sec/2002/01467137.html [This is an online excerpt from a publishing in the Network World Security newsletter from 07-24-2002].

[7]. The Security Database: Attack #93 Salami Attacks at www.all.net [This is a reference of threats, attacks, and defenses maintained by Fred Cohen].

[8]. Handbook of Information Security Management: Law, Investigation, and Ethics. www.cccure.org/Documents/HISM/522-525.html [This is an article of several short topics referenced by visiting the CISSP Open Study Guide site].

[9]. Parker, Donn B. Fighting Computer Crime: A New Framework for Protecting Information. New York: John Wiley & Sons, Inc., 1998. [This text explains why current computer security methods often fail].

[10]. http://packetstormsecurity.org/files/108823/common-vulnerabilities.pdf

[11]. Schwinger and S. Defuel, "Information Security Culture -From Analysis to Change," South African Compute. J., vol. 21, pp. 46-52, 2003.

[12]. M. Alnatheer and K. Nelson, "A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context," in 7th Australian Information Security Management Conference, 2009, no. December, pp. 1-3.

[13]. K. D. Mitnick and W. L. Simon, The Art of Deception: Controlling the human element of security. Wiley Publishing Inc, 2002.

[14]. J. Van Niekerk and R. Von Solms, "Information security culture: A management perspective, Comput.Secur" vol.29, no.4, pp.476-486, Jun.2010. [CrossRef]

[15]. K. Thomson, R. Von Solms, and L. Louw, "Cultivating an organizational information securityculture,"Comput. Fraud Secur., no. 10, pp. 7-11, 2006.

[16]. "Schlienger and Teufel (2003) Information Security Culture -From Analysis to Change."

[17]. K. Thomson, "Integrating Information Security into Corporate Culture Corporate Culture."

[18]. S. Furnell and K. -L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security, " Comput. Fraud Secur., vol. 2009, no. 2, pp. 5-10, Feb. 2009. [CrossRef]

[19]. I. Okere, J. Van Niekerk, and M. Carroll, "Assessing information security culture: A critical analysis of current approaches, " in Information Security for South Africa (ISSA), Johannesburg, South Africa, 2012, pp. 1-8.

[20]. http://legal.practitioner.com/computer-crime/computercrime_3_2_11.htm