WEBWORM ESPIONAGE APPLICATION TO DETECT UNNOTICED MALPRACTICES IN A SYSTEM

K. Kanimozhi, K. Thenmozhi*

Abstract

Espionage webwork software is an adaptable utility that can perform much differently for personal computers and network systems. The system records the process running on the specified system, the other users' applications and stores them in log files. It will record all the applications open and executed. The application can be run minimized in the system tray or invisibly in the stealth mode. It also helps the user to work on a client system on a networking system. Some specified applications can be blocked by the user, which will be terminated by the system automatically. It automatically stores all the files and can view the server, and we can also set options from the server.

Keywords: Network Spy; Visited websites; System configuration; Application History.

I. INTRODUCTION

Webworm espionages of software require physical installation allow the researchers to indeed view activity logs. It helps the administrator to monitor the remote person concurrently from another machine. It works just like a concurrent key Logger, web URL recorder, plus applications monitor. It is a complete package with all the above components and an extremely user-friendly setting interface; it can be easily configured to fit all investigation and detective purposes[1].

This work involves the following modules:

- Identifying Network systems
- Applications History
- Hardware configuration of the current system
- Desktop Screenshots
- Websites Visited

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

II. OBJECTIVES

It is a versatile utility program that can perform much different protection for our personal computers and computers in networking. On activation of this system, it records the processing running by other users. It performs screen capturing. Captured images are saved in BMP or jpg format. Additionally, it facilitates the user to transfer their files and messages among the systems under the network.

- To monitor the nodes in networking
- To record all the process running on the network
- To watch the user
- It helps to check the systems on the network

III. SYSTEM ANALYSIS

In this section, drawbacks of existing and advantages of proposed are discussed in detail.

A. Existing system

The implementation of Network Management today is made available in the market and some of the prosperity software that the operating system vendors like Microsoft, Linux, UNIX, and supply along with their Operating System as Network Operating System. Some of the popular application that is supported along with operating systems are Netmon.exe. These applications are mainly confining their monitoring activities amongst devices and clients that are connected to the network [2]. This software provides various networking facilities as separate components and not as integrative ones. The existing system has its quality and some disadvantages; to achieve its supremacy, it must be configured to its highest possible limits[3]. There was no

such readymade tool available for the network administrator to administrate everything that's happening on remote machines in the network. The existing system had the facility provide the users regarding network services as separate modules for the features like view-start-stop the services and process running on remote machines [4].

This system involves the following disadvantages:

- Difficulty usage of the tool.
- Need the expertise to handle the software operation.
- More time is consumed in achieving any specific task.
- Less user interactivity.
- Data inconsistency occurs across remote clients.

B. Proposed system

Owing to the number of drawbacks evident in the existing system, a new system is being developed, which leads to the effectiveness of all the users and their activities within a network. There is a need for the company to cope with new facilities required for the Network Administrator with new technological requirements that need to be remote network monitoring as a spy in various communication media, i.e., wireless and wired medial [5]. As for the requirements, the server should have a single tool that would make their work efficient and effective. The proposed system should also be compatible with existing and new technologies with high-security constraints. It efficiently managed and monitors our events, services, processes, running applications, GUI interfaces on remote machines [6]. It also notifies when a user accesses another system. This system involves the following advantages:

- An efficient commercial tool for the network administrator.
- Take little time to process and gather information
- A single centralized tool available to do all tasks
- High-level security features are available and reduce the manual work time.
- System tray support to open and exit the utility, available as an installer.

IV. SYSTEM STUDY AND DESIGN

In this phase, two steps have to be incorporated those are input and output design. The inputs are designed to be user-friendly. Input design is the process of reversing user inputs into the computer-based format. This input design incorporated as much automation as possible [7]. The input for the project is user identification their respective password and various feedback about the product it can be refers for member. The non-members are first sign in as a new user.

The administrator is one of the main users to assign rights to others and the system. The new user gives personal details to join as a member. It is the interface between the user and the system. An interface implies a flow of information. The most exciting trend in interface design is windowing [8]. The user manipulates windows with a mouse. Even though the windowing environment is considered to be graphical, some applications include manipulation of windows through the keyboard [9]. Windows lets the user work on multiple applications at once. The outputs generated should be accurate, reliable, and free from errors. It also provides the output message in the taskbar to inform the user and administrator [10].

- The output should be designed to have the following:
- Every output should have a title.
- Reports should have subtitles to give more information to the user.
- Every column should have a title.
- Redundant data should be hidden or avoided.
- Forms should be user-friendly and informative.

The Form is displayed in the tabbed window manner. The tab Shared Folder will display the shared folders available on the network. The tab Current Session will displays the user

and IP s of the clients available on the network [11].

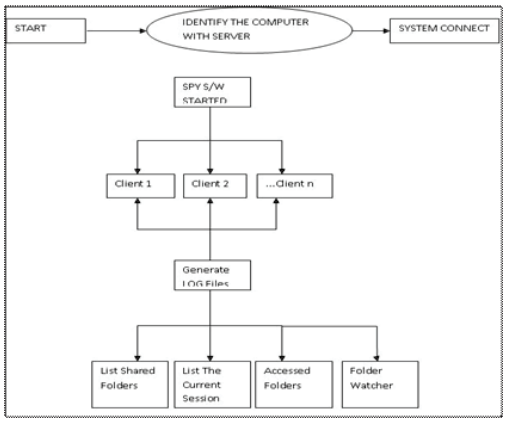

Figure1. Data Flow of Web work Espionage Application

The next step of the work is testing which means checking whether the developed system works according to the actual requirement and objectives of the system. The designed new system is tested with the sample data, and final outputs are verified with the actual manual reports. If these reports are satisfied, then the system input to process with online data entry. Computer program testing is performed to verify that the computer-based business system has met its design objectives. The system includes the computer components as one of its significant elements [12]. The user is responsible for the supply of the input data. System testing reports are prepared to validate system performance. After the design phase is over, the next task is to proceed with developing the proposed system.

The principal activity of system development is preparing the code. In this system, the code is developed for each module separately. That code is prepared for master files, and they are compiled and corrected. Then the source code for the transaction files is prepared, compiled, and corrected [13]. Then the modules are combined and corrected as a whole module.

V. SYSTEM IMPLEMENTATION AND MAINTENANCE

Implementation means converting a new system design into operation. The phase focuses on user training, site preparation, and file conversion for installing a candidate system. The essential factor that should be considered here is that the conversion should not disrupt organization functioning. The following are the steps involved in the implementation plan.

- Test the system with sample data.
- Detection and correction of errors.
- Make necessary changes in the system.
- Check with the existing system.
- Installment of hardware and software.
- Training and involvement of user personal.

The maintenance of the system could be given by describing four activities that are undertaken after the program is released for use [14]. Thus, the process of corrective maintenance for analyzing and correcting errors has been moved through inventing entirely.

VI. CONCLUSION

The application developed is designed in such a way that any further enhancement can be done with ease. The system is more helpful with various applications to predict wrongdoing in that working system. It makes the user not do unwanted malpractices with that system. If so, appropriate warnings and actions will be recorded. Thus, the administrator will have control over every client system even if the user is not present in the system. Hence, the administrator's PC is now can be much secured and robust. This application will be more helpful in all the platforms for monitoring and surveillance. This research work has been checked out in a networking environment to monitor and spy all the systems in the network connection without knowing the user, and the result was highly successful.

VII. FUTURE SCOPE AND ENHANCEMENT

In the future, the following process could be included in the system.

A. Time Scheduling

The system can be set to start and stop at the set time specified by the user [15]. So, the user could start monitor at a time and avoid viewing much of unwanted log of records.

B. User Filter

This software can be set to monitor only a set or group of specific users on our computer or monitor all users except the account administrator.

C. Idle Detector

The use of system resources can be minimized, and capturing many duplicate screenshots can be avoided.

REFERENCES

[1] D. Morgan, W. Banks, W. Colvin, and D. Sutton, "A performance measurement system for computer networks," in Proc. 2019,. Int. Fed. Inform. Processing Congr., pp. 29-33.

[2] G. D. Cole, "Computer network measurements-techniques and experiments,"Univ. California, Los Angeles, NTIS, Rep. AD-739-344, Oct. 2017.

[3] C. T. Apple, "The program monitor-a device for program performance measurement," in Proc. Ass. Comput. Mach. 20th Nat. Conf., Aug. 2004, pp. 66-75.

[4] R. A. Aschenbrenner et al., "Neurotron monitor system," in FaU Joint Comput. Con/., AFIPS Con/. Proc., vol. 39. Montvale, N. J.: AFIPS Press, 2007, pp. 31-37.

[5] A. J. Bonner, "Using system monitor output to improve performance," IBM Syst. J., vol. 8, no. 4, pp. 290-298, 2006.

[6] D. T. Bordsen, "Univac 1108 hardware instrumentation system," in Ass. Comput. Mach. SIGOPS Workshop System Performance Evaluation, Harvard Univ., Cambridge, Mass., Apr. 2017, pp. 1-29.

[7] G. Estrin et al., "SNUPER computer," in 1967 Spring Joint Comput. Conf., AFIPS Con/. Proc., vol. 30. Washington, D. C.: Thompson, 2011, pp. 645--656. [9] L. E. Hardt and G. J. Kipovitch, "Choosing a system stethoscope," Comput. Decisions, pp. 20-23, Nov. 1971.

[8] T. Y. Johnston, "Hardware vs. software monitors," in Proc. SHARE, XXXIV, vol. 1, Mar. 2010, pp. 523-547.

[9] K. W. Kolence, "Software physics and computer performance measurements," in Proc. 2010 Ass. Comput. Mach. Annu. Conf., pp. 1024-1040.

[10] H. Lucas, "Performance evaluation and monitoring," Comput. Surveys, vol. 3, pp. 79-91, Sept. 2000.

[11] R. W. Murphy, "The system logic and usage recorder, in FaU Joint Comput. Conf., AFIPS Conf. Proc., vol. 35. Montvale, N. J.: AFIPS Press, 2012, pp. 219-229.

[12] C. D.Warner, "Hardware techniques," Ass. Comput. Mach. SIGCOSM Newsletter, no. 5, pp. 5-11, Aug. 2001.

[13] M. D. Abrams, "Consumer-oriented measurements of computer network performance," in Proc. Nat. Telecommunications Conf., IEEE Communications Soc., San Diego, Calif., Dec. 2002.

[14] W. Banks and D. Morgan, "A computer controlled hardware monitor: hardware aspects," in Proc. Int. Meeting Minicomputers and Data Communications, Liege, Belgium, Jan. 2009.

[15] J. Hughes and D. Cronshaw, "On using a hardware monitor as an intelligent peripheral," Xerox Corp., EI Segundo, Calif., Oct. 2009.