

Automatic Campus Network Management using GPS

Dr. Indrakumar J. Shah

K. K. Parekh Commerce College, Amreli – 365601

Abstract:

The Organization Network is the place where large number of attacks is happening. The attackers are using different methodologies to capture the information from the end user without the knowledge of the end-user.

This paper introduces the concepts of Campus Management and Emergency log by using Medium Access Control (MAC) and Global Positioning System (GPS). By using the IP address of an attacker, the MAC address can be found and the attacker's machine can be blocked access with the help of firewall. Using the GPS we can be able to navigate the attacker's position with the help of the position log. The log keeps updating for each and every 10 seconds. The attacker can be identified as if he used his own system or victim (3rd party) system.

1. Introduction

When you think of fear to your Organization /Campus IT Security, what comes to brains? Hackers? Viruses? Laptop/PC thieves? The truth is that every Organization/campus is helpless to a numerous of security threats. Keeping one step ahead of IT security issue can give even the most prepared IT division a headache, but you don't have to go it alone. Here this paper provides the solution such that users, student and staffs can safely access the network 24/7.

2. About Network Log event

The Network log file contains events that are logged by the server system mechanism. These events are often predetermined by the server system itself. Network log files may contain information about Network access, device changes, device drivers, system changes, events, operations and more

In an Organization/Campus system's we need some sudden response for the unexpected warning in the network. So according to warning level, network administrators are need to response for the different levels of warnings to avoid the major crack-up in the network.

The other functional allotment also need some sudden response for the unpredicted warning in the Organization /Campus network. To protect different functional divisions can't completely manage with each other when sudden warnings occurs, clear setting ahead liability of the different functional divisions in network to prevent to avoid it completely within the time of sudden event occurs.

Technical system means when a sudden warning occurs in the Organization/ Campus Network that should be solved in the shortest path time to prevent the network returning to the usual mode.

We have to find solution one by one addressing common network problems and technology systems to the network to continue to avoid new problems. A Sudden reaction scheme is included in the above three parts because the Campus/Organization system and support system are dissimilar to the various organization, research center, universities and colleges.

We will describe about the network monitoring and Security log with Media Access Control (MAC) and Global Positioning System (GPS) it put ahead to help us to record and summarize the proposed occurrences. How to design and use the log will be described in the second part and the conclusion at the last.

3. Technology System Based on Emergency Log

According to the principle of sudden response approach network and Information security emergency response can be divided into five stages

(1) Get Read (2) Detection (3) Restriction (4) Extermination (5) Recovery

Get -Read is avoidance oriented, which include software and hardware preparation, measurement and programs to proposed occurrence. Well knowledge managers are essential. Every day back-up of valuable records are enable security audit log, update the system patch in time, keep ready for firewall, Interruption detection system, anomaly and GPS(Global Positioning System monitoring system and other often used tools are genera methods that well known.

Detection is to discover and determine the nature of the event. Detection method is dependent on the relative software, trough a number of indications to conclude whether there are harmful code, files and directories is being altered with or other set of codes are discovered. When aberrant effect are found, the following actions may obtain a high return: Take to examine aberration, start the audit function or add the amount of audit information, backup system as soon as possible, to avoid attackers track the system or clear the trace of the attack and record what is happening on the emergency/sudden response log Administrators have to calculate the appraisal the range and degree of incident influence and report the process to the leader.

Restriction refers to instantaneous activity which absolute the scope of the attacks and limits the abeyant deficit injury. The Restriction Protocol includes close system, disconnected from the network, modify the firewall filtering rules, block or delete the account of devastating acts and so on. Although the methods are simple, the basic target of inhibition is to find out attackers or malicious program and backdoor set up in the system.

Extermination means enduring healing portion by extermination the causes of occurrence. We must recognize the base/ core causes of the occurrence. Take off all the viruses from the memory, system and backup files, identify and take off the Trojan horse, recovery key documents and information and so on.

Recovery is to recover the system from backup. It should entirely return the destroy system and network equipment to the actual work situation. We usually re-install the system and then restore the data, restore the entire system from a backup, install the operating system and firewall patches, repair the inadequacy in routers and other network equipment, remove temporary securing portion in the abolition and Extermination phase.

4. Working with Emergency Response Log

Organization Network Emergency response systems are often in lower input and require a high level. So we have to use high-tech systems to make up for lack of input. If the network administrator can authorize emergency response log to archive knowledge in credentials with the amplify amount of emergency response information, the log is special higher role in emergency response because some occurrence will gradually from a question – set with a practical solution-set. By

analyzing the features of the question-set, a routine defending issue set will gradually established which can decide the general emergency events, and the solution-set will become excellent and the best.

Logging information should include the causes of the events; the affected extent, processes and countermeasures analysis. When we find the sudden difficulty or problem in the system or server at that time we are tracking the IP address of the attacker. After finding the IP address of the attacker we are blocking that IP address in firewall to stop the further usage in the network. After blocking the IP address we are using the technology called ARP - Address Resolution Protocol included with TCP/IP makes it possible to find the MAC address. Using ARP, each computer maintains a list of both IP and MAC addresses for each device it has recently communicated with. Most computers allow you to see the list of IP and MAC addresses that ARP has collected there. In Windows, Linux and other operating systems, the command line utility ARP shows this information. Using ARP, you can in fact determine the MAC address of some computers from their IP address. ARP works only within the small group of computers on a local area network (LAN), though, not across the Internet. ARP is intended for use by system administrators and is not generally useful as a way to track down computers and people on the Internet. After finding the MAC address, blocking the MAC address in the firewall by doing this that system can't able to access any more in network. Because of the MAC address is permanent physical address of the system provided in the machine. By using IP and MAC address GPS start tracking the attacker position and keeps updating into the log table. If the attacked system want to use the network anymore then administrator want to remove the MAC address from the firewall to access the system in network for anymore.

When we find the sudden difficulty or problem in the system or server at that time we are tracking the IP address of the attacker. After finding the IP address of the attacker we are blocking that IP address in firewall to stop the further usage in the network. After blocking the IP address we are using the GPS (Global Positioning System) to track the IP address and Provider of the attacker and keep tracking the IP address by using GPS whether the attacker is attacking from one place or in roaming by keep tracking of this IP address and updating the log of each and every 10 seconds of the attacker.

5. Use of Emergency log

Emergency events may be divided into two types: Evidable events and inevitable events. Evidable events refer to those events that have clearly defined type and process it may be inside the organization network. Next is an instance event that servers in center of organization network are found being attacked by hackers.

The Establishment of emergency response system is to protect network resources. Any protection system should be based on prevention. So we have estimate the security of campus/organization network. Emergency response log is practical and high detection level of taking preventive measures in the technical system. The key is established emergency response plan lies in the co-ordination of interaction between the different components. The log is also the base of the plan.

REFERENCES

- Improve GPS Positioning Accuracy with Context Awareness
by Jiung-yao Huang, Chung-Hsien Tsai

- QIN Runmei, Guangxi Internet Security Emergency Response and Countermeasures , Guangxi Communication Technology,
- Schultz. E Translated by DUAN Haixin, Response to the Network Security Incidents [M]. Beijing, Posts & Telecom Press, Ensuring GPS Navigation Integrity using Receiver Autonomous Integrity Monitoring by William R. Michalson
- Julia H, Allen CERT, Safety Guide [M], Beijing, Tsinghua University Press

WEBSITES

- <http://www.gps.gov/>
- http://en.wikipedia.org/wiki/Global_Positioning_System
- <http://people.richland.edu/dkirby/141macaddress.htm>
- <http://www.wisegeek.com/what-is-a-mac-address.htm>
- http://www.cert.org/stats/cert_stats.html
- <http://www8.garmin.com/aboutGPS/>

Dr. Indrakumar J. Shah
Residence
A-7 Giriraj Nagar Street No- 3
Chittal Road – Amreli – 365601 (Gujarat)
Ph. 91 94262 34151