INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Campus Network Security Policies: Problems And Its Solutions

Gursimrat Singh
Student, M.Tech, Computer Engineering, UCoE, Punjabi University, Patiala

Dr. Amardeep Singh
Professor, Computer Engineering, UCoE, Punjabi University, Patiala

Abstract:

With the growth of internet the need for a secure network has also grown. Internet is used in various educational institutes and universities by the students and research scholars. It is convenient on the other hand unsafe to use internet. Therefore network security management has become one of the important issues for the network administrator in the campus. This paper puts light on some of the problems faced by the campus networks and gives solutions to tackle them.

1.Introduction

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator [1].

1.1.Need Of Network Security

The network needs security against attackers and hackers. Network security needs two basic securities. One is to protect the information from unauthorized access and loss. The other one is computer security. Now a days lacs of important information's are exchanged daily and there are many people whose eyes are always to get the information and to misuse them. Same in case of campus sometime students or unauthorized person try to attack the network of the campus to get the useful information. So there is need of network security to protect the loss of information from unwanted editing, accidentally or intentionally by the unauthorized user.

2.Problems In Campus Network Security

There is a considerable risk within the campus networks as the internal users understand the network structures and application models more than the external users. Statistics indicate that 70% of the attacks to the network are done by the internal users. There are illegal visits by the unauthorized users to use the resources in an unauthorized way. Therefore the main threat to the network is internal security threats. Presently the internet is flooded with the hacking tools; hackers use network protocols, server and operating system security vulnerabilities and management oversight to illegally access to network resources, deletion of data, damage the system, these attacks caused to the adverse effects of the campus network of and the damage to the reputation of the school.

A genuine operating system have a lot of security vulnerabilities, these security vulnerabilities pose many serious threats such as the information security, using of the system, network operations and so on.

Another serious problem is the shortage of funds for the network construction in campus Limited funds are invested on network security equipments construction and management of network security has not been taken into account seriously. Because of lack of the awareness in universities, management institutions are not perfect, administration system is imperfect, management technology is not advanced; the campus network management center can't take any preventive measures for network security. There is no strict implementation of standards for the campus network security management; this is an important reason for the vulnerabilities in campus network.

Campus network connected with the internet with routers; of course, internet users can enjoy the convenience of fast and unlimited resources of this platform, but also have to face to the risk of an attack. The internet users in the campus download data or software from the internet which may have virus, Trojan horse, backdoors or other malicious code due to which many systems are invasive and are used by the attacker.

The university campus has a computer room. The computers in this room have direct access to the computer network of the universities. Some students and teachers often use these computers to have internet access. However these computer rooms are not essential in management state due to lack of unified management software and systems for monitoring and logging. The internet is not able to recognize user's identity due to flaws in registration and management system.

Another problem associated with the network is leakage of data due to password disclosure. A campus network have a variety of database systems running online such as teaching management system, card management system, test bank and so on. The database password can be lost due to negligence of the user or misconduct by the user. Also sometime the user discloses the password to others. Due to this the data may be illegally removed or replicated.

A serious influence brought to the network is by the attackers, hackers or distributors who send spam and other harmful information by using unmanaged campus server as a transit station. The hackers also try to use network protocol, the server and crack security of the operating system as well as deletes data, destroy system. The hackers try to decrypt the passwords documents using some software which is known as password invasion. They try to steal passwords of other people using abnormal methods to visit the web.

Another important threat to the network security is physical threat. This is also known as malicious destruction. It includes the network equipment and network system's destruction. The students of the campus network accidently or intentionally destroy the network equipment such as server, motherboard, the switchboard, the router, the concentrator and so on. This results in complete or partial paralysis of the campus network.

Certain people use computer software and hardware system to program a malicious function for special use called computer virus. This malicious function or the virus has huge destructiveness. The network is main way for virus dissemination. The dissemination of virus is done through e-mail, ftp, browsing contamination homepage and so on. When the campus WAN is turned on the hacker attack, security threat such as viral invasion enlarges, the downloading procedure and the email has the virus possibility , but many machine user's password is too simple, establishes shared and so on that make the viral wide spread completely.

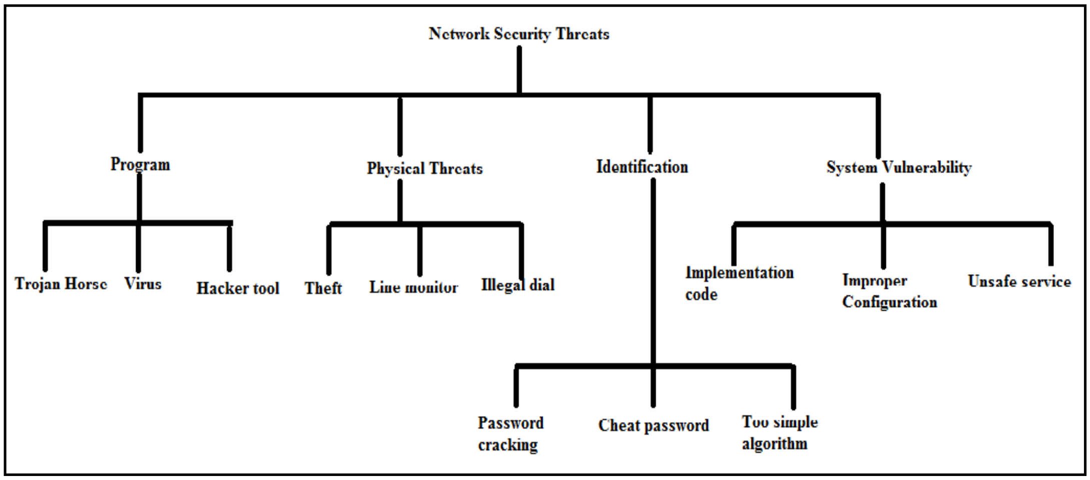

Figure 1: Threats to Network Security

3.Campus Network Security

If we want best campus network firstly we should have plan and take full consideration based on problems and security risks to the campus network. Secondly we should adopt various advanced technologies such as virtual exchange network, firewall technology, encryption technology, virtual private network (VPN) technology, PKI technology, and achieve centralized configuration, monitoring, management. Finally, we should strengthen formulating of systems and specifications about the network security secrecy, and strictly implement it [3].

Physical security is all about who has access to the equipment. In the past, it was clear that only authorized people would have access to the systems. Computers lived in big "glass houses" where only IT people were allowed to go. The systems were always kept under lock and key. Physical Security systems are only as effective as the networks they reside on. The explosive growth of HD surveillance, video traffic, analytics engines, and more are placing higher demands on legacy networks – just as Physical Security becomes more mission critical than ever. Extreme Networks improves physical security by increasing reliability and management, lowering deployment time and cost, and scaling to meet changing requirements over time. Security guards can help to maximize physical security.

Securing hardware is important because if a person has physical access to a device, there is almost always a way to take control of it or to get data out of it. It's at the hardware level, the very bottom of the networking hierarchy, that your network is most vulnerable. A lost laptop, an open USB port, a simple network tap—all these can be a conduit for quick and devastating data loss that no firewall can prevent. Private facilities have always had an advantage over public facilities in that they are easier to physically secure. Public areas, such as hospitals, universities and libraries, can be a challenge to secure because of the lack of physical security. Public or private, there will always be some level of security risk wherever a network jack is active. Classrooms, communications closets and conference rooms are a few of the problem areas commonly found unlocked and accessible to anyone curious enough to peek inside [4].

To provide the most productive learning environment for students and educators (and a productive work environment for campus administrators), it is often the policy for organizations to allow users to bring their own devices for use on the campus network. However, for such colleges, universities and educational institutions, this policy to allow those devices onto the network can also lead to significant risk and ramifications. More common rogue devices on the campus network may include [5]:

- Compromised iPhones or other devices scanning networks
- User introducing rogue DHCP servers
- Systems infected with malware sending large amounts of SPAM

The NetFort support team has worked with a number of colleges to help them more promptly and accurately identify issues caused by rogue devices on the network. The potential damage of a rogue device introduced onto the campus network is a serious challenge for campus network managers and administrators today [5].

Networking and IT professionals responsible for the management of an organizational-wide network within a higher-education institution such as a college, university or other learning institute are faced with one of the most challenging networking environments today. The parameters that exist for campus networking environments are numerous and daunting[5]:

- Large network extended across broad geographies
- Massive user base that’s constantly in a state of change
- Complex networking infrastructures across diverse platforms
- Strong need to track individual user activity due to copyright infringement concerns, cheating, etc.
- Wide array of network devices of all types, makes, operating systems, etc.
- High number of remote and transient users
- Broad and disparate number of applications and databases being accessed across the network
- Unpredictable user base (especially students) apt to misuse or attempt to breach network security
- High volume of large file sharing and file downloading
- Open networks (required especially for remote access) creating higher security risk

The need for security on any network is apparent: the prevention of eavesdropping and the desire for authentication has been the main focus of many network administrators. However, the problems that already exist are added to when you add wireless networking to the equation. As wireless networking becomes more popular, the flawed security of most of those networks becomes more necessary. Several organizations have devised ways to secure their wireless networks from intruders. However, there is currently no wireless security implementation that everyone agrees is always suitable, regardless of what network it is to be used on. Some implementations are satisfactory for some environments, and there is work underway to create future solutions [2].

The modern network environment is getting more and more complex due to the rapid increase of using IT system, and different types of industries, enterprises all have IT to support their business. While different business trenches their demands and funds for Information Technology, more and more various technology and applications are involved into the modern network, and unexpected errors may happen during these overlapped technology instances: routing mechanisms, fault tolerant configurations, firewall policies, integrated 3G gateway, Wi-Fi frequency, endpoint health, management software etc. Each technology units could be a fault point and any unit encounters an error will absolutely cause unforeseen effect to other units, and then consequently result in a series of troubles in your network. When troubleshooting your network, finding the cause of problems costs the most of the time. It is essential to find a useful solution with which you can pinpoint the source of the intermittence [6].

Colasoft Capsa is a product which is widely used for troubleshooting. This tool provides statistics support and gives an insight view at frame level. It enables administrators to trace the digital bits running in your network and translate them into human readable information, thus find the source of problems, and then choose the right solution right against the problem rather than merely symptoms. Fix a problem once for all [6].

There are a lot of opinions about security awareness programs, what they should look like, what they should cover, whether they work at all, etc.

The point of security awareness programs is not to see how cool, hip, or clever the message and the delivery method can be but to change the way people think and act about information, both their own and others when applicable. The point is to get people to want to protect that information from prying eyes or accidental disclosure. It is recommended that instead of looking deeper into the psychology of the user, or trying to find the next viral communications technique, security awareness program developers should look at methods and messages from other areas where communication to a vast number of different people has been necessary and where those messages have been effective over time [7].

For example, how many of the following messages or sayings do you remember and act on, whether you know it or not [7]:

- Click it or ticket
- Don't mess with Texas
- Only you can prevent wildfires
- Don't talk to strangers
- Look both ways before crossing the street
- Do not leave your bags unattended

In university campus there is lot of files having sensitive data that includes name, dob, addresses, credit card information, copies of personal ID's, taxes, licenses, social security numbers, banking information, account login and passwords, and more. So what if the website of the institution or university is hacked. There arises a need for ethical hacker or ethical hacking. Ethical Hacking Services, also known as "White Hats" have three key objectives: Challenge/ Seek, Patch, and Secure. "Challenge/Seek network security systems for vulnerabilities, patch code, secure data, and constantly inform you of new possible types of attacks" [7].

The next solution is backing up critical data. System backups can be easily managed using the YaST System Backup module. Use the YaST System Restoration module to restore the system configuration from a backup. Restore the entire backup or select specific components that were corrupted and need to be reset to their old state.

There are several reasons why a system could fail to come up and run properly. A corrupted file system following a system crash, corrupted configuration files, or a corrupted boot loader configuration are the most common ones.

The rescue system can also be used. openSUSE contains a rescue system. The rescue system is a small Linux system that can be loaded into a RAM disk and mounted as root file system, allowing you to access your Linux partitions from the outside. Using the rescue system, you can recover or modify any important aspect of your system [8]:

- Repairing and Checking File Systems

  Generally, file systems cannot be repaired on a running system. If you encounter serious problems, you may not even be able to mount your root file system and the system boot may end with a "kernel panic".

- Accessing the Installed System

  If you need to access the installed system from the rescue system to, you need to do this in a change root environment. For example, to modify the boot loader configuration, or to execute a hardware configuration utility.

- Modifying and Reinstalling the Boot Loader

Sometimes a system cannot boot because the boot loader configuration is corrupted. The start-up routines cannot, for example, translate physical drives to the actual locations in the Linux file system without a working boot loader.

Funding is a central issue in planning and building networks. The financial part of network planning should include a strategy based on capital funds, support funds, and maintenance funds. Capital funds are generally used for building the basic network infrastructure. Every campus network is different, so it is very difficult to provide a general formula or model to accurately predict the design and development costs. For example, a campus with a network of steam tunnels will find it much cheaper to install conduit and fiber than one that has to dig up or punch under city, county, or state roads.

Support funds, often included in the institution’s operating budget, are required for the ongoing support of network components and services. Examples of such expenses include personnel costs, license fees, Internet line charges, and fees for regional providers of Internet connections. Maintenance funds will be required to replace damaged, worn out or functionally obsolete networking equipment. Keeping an equipment inventory, with the expected replacement cost and the expected lifetime for each item, are necessary so yearly costs can be predicted. For simplicity, if a component is expected to last N years, then each year (100/N) percent of the replacement cost should be deposited in a depreciation reserve fund. And the network management staff should have access to this reserve account on an "as needed" basis [9].

The operating system is the foundation for all computer terminals, workstations and servers to run properly, operating system security is very important. The server version of the genuine operating system should be used in the critical servers and workstations (e.g., database server, www server, proxy server, Email server, backup server and network management stations, etc) [3].

The VPN technology make many internal network long-distance connect with through the public network using the tunnel technology and encrypt ,is a safe transmission path's technology which be through the network data wrapped and the encryption transmission. This technology may allow user spanning public network, visit each other’s by the internal network unified planning address. The VPN has the characteristics such as secure, the grade of service guarantee, the extendibility, the flexibility, the manipuility and the lower cost and so on, it’s used widely just as these characteristics. Applies the

VPN technology in the campus net, may break through the regional limit of the campus private network or optimizes the campus net's management and the application [10].

The main objective of hackers is to steal data and modify the system illegally. Risk assessment tools for system should be used to help system administrators identifY whether the user privileges command should not be installed or should be reduced. In addition, real-time intrusion detection system IDS can track user's activity, invasive testing, also can prevent internal staff from to damage Intranet. When the irregularities detected, the system will immediately notifY the administrator, the administrator can record the corresponding test results and information to track the intruder, to determine whether it endanger the safety of the system and take effective preventive measures to ensure the system's important data and important documents from damage [3,11, 12].

In addition, there is information encryption strategy. Using encryption algorithm to encrypt sensitive information, you can prevent unauthorized persons illegally to steal information. There is a number of encryption software which can encrypt messages; files et al. Use encryption software can effectively protect data, files, password, and control the information to transmit safely through the network [3,13,14].

4.Ideal Campus Network Security Management

The campus network provides the essential first link in connecting scholars to the information universe. As campus planners engage in the process of planning and building campus networks, they need a clear vision of what an "ideal" campus network should be like. Since every college is different, every campus network will use a different approach to envisioning, planning, and building its unique campuses network.

Regardless of the specific planning process or the particular network design used at a campus, there are certain dimensions (or aspects or characteristics) that exist in every campus network. The following model for envisioning the "ideal" campus network, incorporating five dimensions ranging from the physical to the cultural, may be useful to think about during the planning process [9].

- Physical dimension. The ideal campus network is an information channel that reaches every place on campus where "knowledge workers" live and work, including offices, classrooms, laboratories, studios, student residences, student activity areas, and so forth. It includes a physical infrastructure that consists of high-grade copper and fiber cable; junction and termination boxes; communications devices such as fiber hubs, bridges, routers, terminal servers;

and wiring closets to house equipment and termination panels. The ideal campus network provides a seamless interface to on-campus sub-nets and to off-campus locations and resources, such as faculty homes, metropolitan and regional networks, and the Internet. The ideal campus network has physical components that meet defined institutional standards, provide for modularity and expandability, and are well documented and mapped [9].

- Protocol dimension. The ideal campus network handles multiple network protocols, such as TCP/IP, AppleTalk, Netware, etc. Therefore it should not have highly proprietary characteristics that preclude use of other protocols. The ideal network provides a seamless interface between protocols used on sub-nets and meets well-defined institutional standards for network connections and protocols [9].
- Management dimension. On the ideal campus network, management activities are invisible to users. Network growth, while constant, is managed without disruption to users. The ideal network management structure includes appropriate staffing, as well as budgeting, control, and security systems. The institution with an ideal campus network has a funding program that covers continuous growth of the network and replacement of equipment [9].
- Application dimension. The ideal campus network provides easy access from any connection point to all information pools, including the global Internet, library materials, specialized departmental resources, non-print media collections, and institutional databases. The network provides a variety of integrated information resources via a campuswide information system (CWIS). The ideal campus network incorporates a seamless electronic mail system with a common user interface to all members of the institutional family, which may include off-campus constituencies, and provides easy sharing of electronic resources (data, text, images, sound, video) across the network. All members of the campus community find it easy to use shareable computing hardware and software resources such printers, scanners, statistical packages, programming languages, and databases; everyone has full access to Internet applications and information resources; and all applications are well documented and publicized [9].
- Cultural dimension. Ideally, all faculty, staff, and students use the network fluently as a natural and integral part of their communications and information

> exchange activities. On a campus with an ideal network, students use the network as an intrinsic part of their campus life, faculty actively seek to use the network in new and creative ways to enhance teaching and learning, and administrators and staff routinely use the network to improve operations and reengineer archaic administrative systems. The network provides a unifying concept for campus wide integration of information technologies, resources, and services. The institution considers the network a strategic asset, and is committed to supporting the network as a vital strategic resource [9].

5.Conclusion

It is a clear fact that there is not any networking environment that is as challenging and complex as that of colleges, universities and other educational institutions. The campus network is the base of system, so make a network security system which protects the campus information system. There should be a network security guarantee from hardware and software companies for a safe environment. This paper introduces problems faced by the campus network as well as gives solutions to face these problems. This text gives advice how to build an ideal network for campus.

6. Reference

1. http://www.cc.boun.edu.tr/network_security.html
2. SANS Institute 2002 "WIRELESS NETWORKS: Security Problems and Solutions", Jonathan Weiss, SANS Institute 2002, GSEC Practical.
3. Cuihong Wu, "The problems in Campus Network Information Security and its solution", International Conference on Industrial and Information Systems, 2012, pp 261-264
4. www.wikipedia.org
5. LANGuardian-campus-networks-wp.pdf
6. http://www.colasoft.com/network-solutions/network-troubleshoot-solution.php
7. http://www.calibersecurity.com/blog/bid/222618/5-Network-Security-Issues-and Solutions
8. http://doc.opensuse.org/documentation/html/openSUSE_113/opensusestartup/cha .trouble.html
9. http://net.educause.edu/ir/library/html/cem/cem99/cem9916.html
10. Jianzhong Wang, Lv Li, "Based on Campus net's security policy discussion", International Symposium on Knowledge Acquisition and Modeling, IEEE, 2008, pp 366-370
11. Joel S, Stuart M, George K. Hacking Exposed: Network Security Secrets & Solutions [M]. McGraw-Hill, April 2005:23-126.
12. B. Harris, R. Hunt. TCP 1 IP security threats and attack methods .Computer Communications, 1999, (22): Page.885-897.
13. Venter H S, Eloff J H P. Data packet intercepting on the internet: how and why? A closer look at existing data packet -intercepting tools, Computers & Security, 1998, 17(3):683-692
14. SHEN Chang Xiang, ZHANG Huang Guo et al. Survey of information security. SHEN Chang Xiang et al. Sci China Ser F -Inf Sci I June 2007 I vol. 50 I no. 3 I 273-298