International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

DESIGN AND IMPLEMENTATION OF A SECURE CAMPUS NETWORK

1Thota Shiva Sai Krishna[1], N.Shiva Priya[2], Dr.C.rajabhushanam[3]

[1]UG StudentIII B.Tech[CSE],Department of CSE,Bharath University

shivasai7392@gmail.com

[2]Assistant Professor,Department of CSE,Bharath University

shivapriyamari@gmail.com

[3]Profeessor,Department of CSE,Bharath University

Rajabhushanam.cse@bhrathuniv.ac.in

Abstract

Security has been a essential issue within the style in readying of an enterprise network. A campus network is a very important part of campus life and network security is crucial for a campus network. Secured network protects an establishment from security attacks related to network. A university network includes a range of uses like teaching, learning, research, management, e-library, result publication. Network security can stop the university network from differing kinds of threats and attacks. The theoretical contribution of this study may be a reference model design of the university campus network that may be pre-designed or custom-made to make strong, however versatile network that the successive generation needs.

Key words: Campus Network, Security, WAN, Security Threats, Network Attacks, VPN, VLAN, Firewall.

Introduction

As the computers and networked systems thrive in today's world, the necessity for increased robust pc and network security becomes more and more necessary . The rise within the network system has exposed several varied styles of web threats.The safety could embrace identification, authentication, authorization and camera to safeguard integrity, convenience, authenticity of element or network instrumentation. There's no laid-down procedure for coming up with a secure network. Network security must be designed to suit the requirements of a organisation .

Campuss network is crucial and it plays a very important role for any organization. Architecture and its security are as necessary as air, water, food, and shelter. Network security threat and architecture are invariably serious problems. A campus network is an autonomous network beneath the management of a university that is at within a neighbourhood geographical place and typically it should be a metropolitan area network .

Generally, IT manager in a very network faces many challenges within the course of maintaining,availability ,performance,good infrastructure, and security. Securing an enormous network has been always a difficulty to an IT manager. There are plenty of similarities between securing an outsized network and university network,however each has its own problems and challenges.Current institution organisations pay a lot of attention to IT to boost their students' learning experience. Architects of campus can do this if IT managers hold on to the basic principles self-addressed during this reference architecture namely LAN or WAN connectivity design considerations, security, and centralized management .

The network infrastructure style has become a vital part for a few IT organizations in recent years. a very important network design consideration for today's networks is making the potential to support future growth in

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

a very reliable, scalable and secure manner. This needs the designer to outline the client's unique situation needed for what significantly the current technology, application, and information design.

Here, completely different analysis papers are consulted for security in campus network.Numerous network info for security issues and their solutions. They represented the current security info standing of the campus network, analysed security threat to campus network and represented the ways to maintenance of network security .

Related Work

1.IS Strategy(by Glasgow university)

- Impact on Network Development and Architecture
- Universal Access
- Security

2. IT Strategy(by ijetae)

- Implement Network Architecture recommendations

Background

There are various categories of network like Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN), campus Area Network (CAN),Storage Area Network (SAN) and Wide Area Network (WAN).

A Personal Area Network (PAN) may be a network organized around a private person. Personal Area Networks usually involve a mobile, a cellphone and/or a hand-held computing device such as PDA. A Local Area Network (LAN) may be a cluster of computers and associated devices that share a standard communications line or wireless link. Typically, connected devices share the resources of one processor or server within a little geographical area. A Metropolitan Area Network (MAN) may be a network that interconnects users with system resources in an exceedingly geographical area or region larger than that filled by even a large Local Area Network (LAN) however smaller than the space filled by a Wide Area Network (WAN). A campus Area Network (CAN) may be a proprietary Local Area Network (LAN) or set of interconnected LANs serving a organisation, federal agency, university, or similar organization. A Storage Area Network (SAN) may be a high-speed network of storage devices that additionally connects those storage devices with servers. It provides block-level storage that may be accessed by the applications running on any networked servers. a Wide Area Network (WAN) may be a geographically distributed telecommunications network. The term distinguishes a broader telecommunication structure from an Local Area Network (LAN). Intensive analysis or project has been done in the position of network architecture and security problems in CAN.

Network Architecture in Campus Area Network

The campus network of our study is meant in an hierarchical manner that may be a common practice of campus and enterprise networks. It provides a standard topology of building blocks that enable the network to evolve simply.A hierarchical design avoids the necessity for a fully-meshed network which all network nodes are interconnected.

Designing a campus network might not seem as fascinating or exciting as designing an associate IP telephone network , an associate IP video network, or maybe planning a wireless network. However , emerging

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

applications like these are engineered upon the campus foundation. Very similar to the development of a house, if the engineering work is skipped at the foundation level, the house can crack and eventually collapse.

If the foundation services associated reference design in an enterprise network don't seem to be rock-solid, applications that depend upon the services offered by the network like IP telephone, IP video and wireless communications can eventually suffer performance and responsibility challenges. To continue the analogy, if a reliable foundation is built and engineered, the house can indicate years, growing with the owner through alterations and expansions to provide safe and reliable service throughout its life cycle.

The same is true for associate enterprise campus network. The design principles and implementation best practices represented during this document are tried-and-true lessons learned over time according to my referred research papers.

Security Issues in Campus Network

There are a large vary of network attacks and security threats, network attack methodologies, and categorizations of network attacks. The question is: how will we minimize these network attacks? The sort of attack, as specified by the categorization of reconnaissance, access, or DoS attack, determines the suggests that of mitigating a network threat .

Table 1:Identify the threat

Threat	Internal \ External	Threat consequences
e-mail with virus	External origination internal use	Could infect system reading email and subsequently spread throughout entire organization.
Network Virus	External	Could enter through unprotected ports, compromise whole network.
Web based virus	Internal browsing to external site	Could cause compromise on system doing browsing and subsequently affect other internal systems.
Web server attack	External to web servers	If web server is compromised hacker could gain access to other systems internal to network
Denial of service attack	Internal	External services such as web Email and ftp could become unusable. If router is attack , whole network could go down.
Network User Attack (Internal employee)	Internal to anywhere	Traditional border firewalls do nothing for this attack. Internal segmentation firewall can help contain damage.

Types of Network Attacks

Classes of attack would possibly add passive observance of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service supplier. Data systems and networks offer attractive targets and will be resistant to attack from the complete vary of threat agents, from hackers to nation-states. A system should be ready to limit injury and recover rapidly after once attacks occur. Here are some attacks types:

1. Passive Attack

2. Active Attack

3. Distributed Attack

4. Insider Attack

5. Close-in Attack

6. Phishing Attack

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

7. Hijack attack

8. Spoof attack

9. Buffer overflow

10. Exploit attack

11. Password attack

Real Time Data: Some Network Attacks

A. Denial of Service (DOS):

Denial of service (DoS) is a interruption of service either as a result of the system is destroyed, or as a result of it's quickly out of stock. Examples add destroying a computer's hard disc, cutting the physical infrastructure, and consumption of all offered memory on a resource. Fig1 shows a true note value of DoS attack knowledge in a very campus network using Cyberoam security device . After configure Firewall and VLAN for DoS attack

Attacker tried DoS Attack however the protection device dropped the traffic that we've shown within the diagram.

Attack Type	Source		Destination	
	Applied	Traffic Dropped	Applied	Traffic Dropped
SYN Flood	Yes	44844	No	0
UDP Flood	Yes	48240	No	0
TCP Flood	No	0	No	0
ICMP Flood	Yes	27	Yes	429

UDP Flooders

IP Address	Last Seen
103.21.42.205	Sat 20 June 14:04:48
103.21.42.206	Sat 20 June 14:56:31
172.16.20.141	Sat 20 June 15:19:15
172.16.20.222	Sat 20 June 16:22:57
172.16.21.140	Sat 20 June 16:04:01
172.16.22.22	Thu 18 June 16:59:49
172.16.22.82	Sat 20 June 13:11:56
173.194.49.104	Sat 20 June 14:03:06
173.194.49.112	Sat 20 June 13:48:55
182.48.85.204	Sat 20 June 15:13:37
182.48.85.206	Sat 20 June 15:56:10
185.23.127.61	Fri 19 June 17:06:11
216.58.220.37	Sat 20 June 23:27:40
52.74.248.98	Fri 19 June 17:02:37
74.125.214.208	Sat 20 June 13:58:12

Fig 1 :Attacker IP List

B. ARP Spoofing Attack

ARP spoofing could be a style of attack during which a malicious actor sends falsified ARP(Address Resolution Protocol) messages over Local Area Network(LAN).This ends up in the linking of associate attacker's mackintosh(MAC) address with IPaddress of a server on the network. We are showing some real time information that attacker using Netcut Software package exploit the weakness within the stateless ARP protocol due to lack of authentication in a campus network. Examples add destroying a computer's hard disc, cutting the physical infrastructure and using all the memory.

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

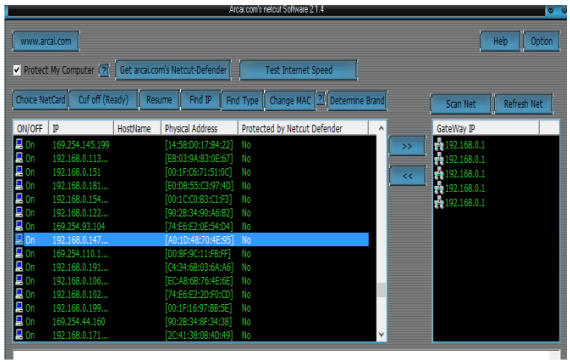

Fig 2. ARP Spoofing Attack in Campus network

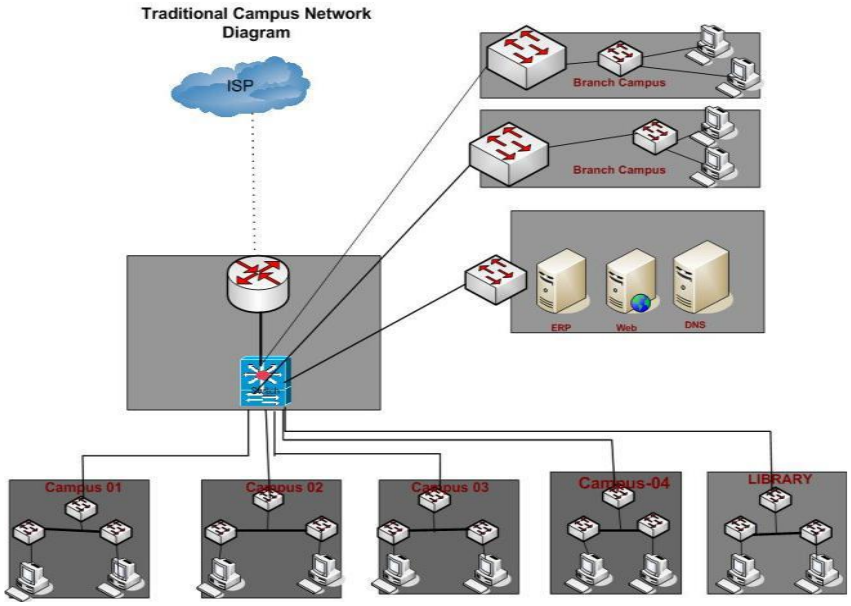

Fig3:Traditional campus network design

Conclusion

Network architecture and its security are necessary for any organization. If we tend to follow the hierarchic network design, network will be scalable, performance and security are increased , and therefore the network are simple to take care of. During this work ,we tend to projected a compact price effective secure campus network design based on the work atmosphere and required quantifiability, security and different aspects.

This proposed network infrastructure is realizable with adaptable infrastructure. It conjointly provides a summary of the most effective practices in mitigating the known attacks and recommendation on a way to stop reoccurrence attacks.

References

1. Network security, Bachelor's Thesis (UAS) Degree Program In Information Technology Specialization: Internet Technology.

2. Network Architecture and Security Issues in Campus Networks, Mohammed Nadir Bin Ali, Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) 2013.

International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

3. Security Problems in Campus Network and Its Solutions, 1Lalita Kumari, 2Swapan Debbarma, 3Radhey Shyam, Department of Computer Science1-2, NIT Agartala, India, National Informatics Centre, India.

4. Network Security: History, Importance, and Future "University of Florida Department of Electrical and Computer Engineering Bhavya Daya ".

5. Security Analysis of a Computer Network, Jan Vykopal , Masary University faculty of informatrics.

6. Security and Vulnerability Issues in University Networks, Sanad Al Maskari, Dinesh Kumar Saini, Swati Y Raut and Lingraj A Hadimani-- Proceedings of the World Congress on Engineering 2011 Vol I WCE 2011, July 6 - 8, 2011, London, U.K.

7. Campus Network Design and Implementation Using Top down Approach by Bagus Mulyawan, Proceedings of the 1st International Conference on Information Systems for Business Competitiveness (ICISBC) 2011.

8. Kansas State University: Wireless Local Area Network Policy. http://www.ksu.edu/cns/policy/wireless.html

9. University of Washington

http://www.washington.edu/computing/wireless/

10. University of California, Davis

http://manuals.ucdavis.edu/ppm/310/310-17.htm