Implementation of Privilege level and Access - control mechanism for Network Security

Rupali bansal [1], **Pooja sharma**[2]

Student, Dept. Of ECE, GGGI,Dinarpur,Ambala Haryana,India[1],rupaalibansal@gmail.com

Assistant professor,Dept.of ECE, GGGI,Dinarpur,Ambala Haryana,India[2],Pooja.211086 @gmail.com

ABSTRACT

In today's world, computer network is important every organization either at any step. Security is the one of the most important issue in the area of computer network. Security is a protection against internal and external problems. In this paper, implementation of privilege level and access-control mechanism has been done which helps in making the network secure. Privilege level phenomenon is implemented on the network devices that are on layer 2 and layer 3, so that only the chief user of network has the right or power to make changes in the configuration and the chief user is responsible for select the access for the local user. The access-control mechanism is also implemented, which controls and maintains the access of all user in the respective network so that all services are under the control of network administrator. Every authorised user is able to use only those services for which the privilege has been given to user from the administrator end.

Keywords: - *Computer network, Security, Privilege Level, Access-control, administrator.*

1. INTRODUCTION

Security is the process of implementing actions by the network administrator end to protect the network from internal and external threats. There are different types of security methods that are to be implemented at the required levels. Firewalls (Hardware/software), Antivirus server, proxy server and etc. are some of the examples of security methods, which are commonly used at present time. External security means security against the outer world. On the another hand, internal security refers to the security actions performed for securing the network from the users those are belongs to the same network. The heart of the each network are network devices which connect the network to the outer world. So it becomes important to protect the network devices from both the threats external and internal. This paper is all about how to protect the network from internal threats as well as external threats. In this paper, privilege level mechanism and access-control mechanism have been implemented.

Figure 1.

Privilege level and access-control mechanism provides protection to network devices i.e. routers, switches, etc.

2. PRIVILEGE LEVEL MECHANISM

Privilege level mechanism is a technique in which the chief network administrator decides and creates different privilege levels for the local administrator. In large organizational structure, there are many local administrators present at different levels and all of them work under the chief network administrator. In case, if the local administrators wants to access the network devices i.e. router, switches, etc., then there is a different login account present for each local administrator and the access level of each local administrator depends upon the privilege set by the chief administrator end.

In the privilege level mechanism, only the chief administrator has the full access authority to the network. There are three types of privilege levels that are commonly created.

- Privilege with full access permissions of network devices. This privilege is only for the chief network administrator.
- Privilege with Read only permissions of networks devices. This privilege is only for the local administrator level 1, that is only able to see configuration of devices but not to change it.
- Privilege with restricted permissions. This privilege carries only a few low level read only access of network devices. It means, in this privilege, local administrator is able to see only a few set of configuration.

The below given figure describes these three types of privilege levels

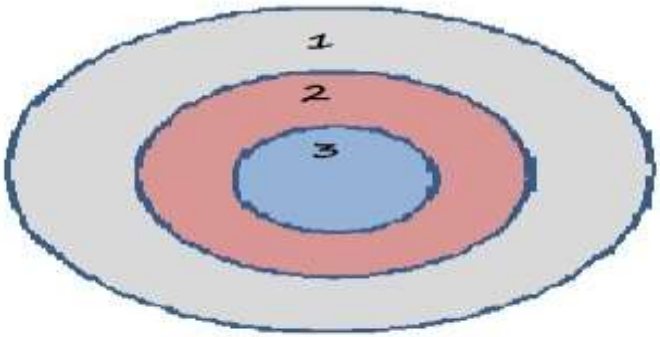

Figure 2.
Access-level of adminstrators.

1 (CHIEF NETWORK ADMINISTRATOR)

2 (LOCAL ADMINISTRATOR LEVEL 1)

3 (LOCAL ADMINISTRATOR LEVEL 2)

As in the above figure, there are three different levels and each of them shows that what type of access is available for which level of administrator. The privilege level mechanism has been implemented on network devices that are on layer 2 & 3. Cisco network devices provide 16 privilege levels (0-15). The level 1 is for the first level entry and level 15 is for chief network

administrator. The chief network administrator is able to create privilege level from 2-15.After implementing this method on the network, the internal security policy has been increased.

3. ACCESS-CONTROL MECHANISM

Access-control mechanism is a technique in which the network administrator is able to control all the access of the host in that respective network. This procedure has been done by blocking the service for the IP address that is allocated to the host party.

Example:
ICMP+TCP service is used for PING utility.

So, if the network administrator blocks the service of TCP, then the user is not able to use PING utility, because as discussed above that TCP service is one of the services that is used by the PING utility. The administrator is also able to control a single service also, as TCP is a connection oriented service and used by many protocols i.e. FTP, PING, DNS, SMTP and etc. so if the administrator wants to control only the FTP (Data transfer) service, then that is also possible, by specifying the port number of FTP (Data transfer), which is 20. So, this type of mechanism is also helpful for the administrator to provide internal security to network. In most of the cases, it is seen that the access-control mechanism has been implemented at the access end of network devices.

The access-control mechanism has been implemented on layer 3 network devices i.e. router. The whole procedure of access-list works in the given manner.

- First, the network administrator implements the access-control for a group of IP addresses or for a single IP addresses.
- When any service is generated against the control of user that is given by the administrator end, then the packet is blocked and user is not able to perform the required task.
- The major function is performed at the router's end, because the internetwork communication is performed by router.

The access-control mechanism is mostly implemented in case of WAN, but in case of INTRANET, this method is not widely used.

4.IMPLEMENTATION

(A). PRIVILEGE LEVEL MECHANISM.

The implementation of privilege level mechanism on layer 3 network device (router).For the implementation, the two privilege level has been created on the routers end. One is for the chief administrator and second is for the local administrator.

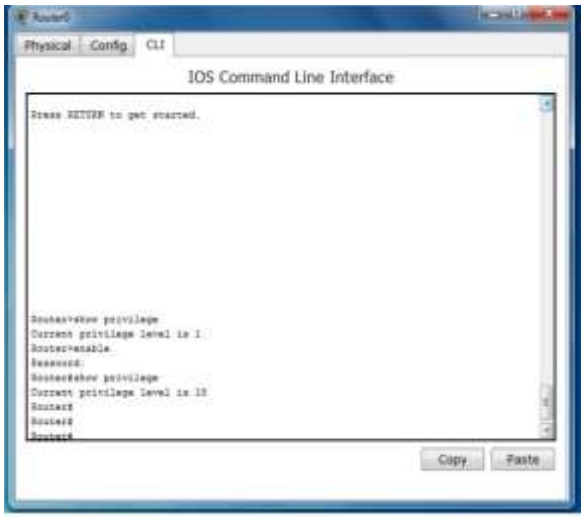

Figure 3

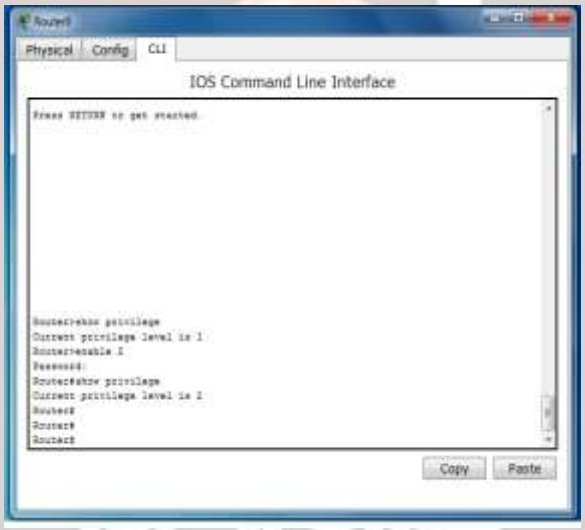

Figure 4

In the both of the above discussed figures (3 and 4) the different administrator will access the network device with their respective privilege levels.

(B). ACCESS-CONTROL MECHANISM The access-control mechanism is totally workable. Administrator is able to control each type of service by using the port numbers also. There is different type of port no is allocated to each type of service. Example: The two given below figures show that what type of response is present when the service of TCP has been blocked by the administrator end and when that is open

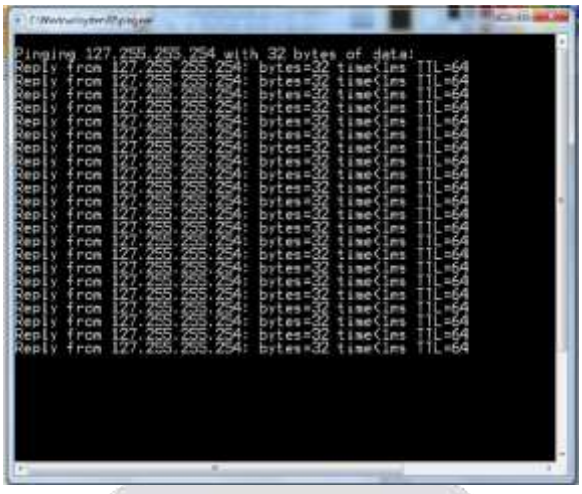

Figure 5 (TCP service is open).

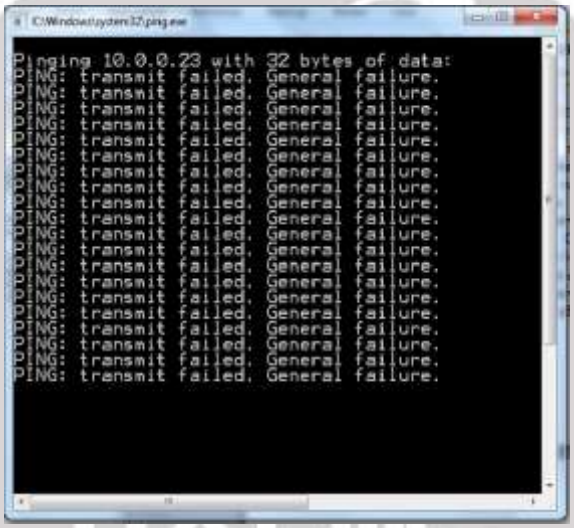

Figure 6 (TCP service is blocked).

5. CONCLUSION & FUTURE SCOPE

This paper defines that how the privilege level and access-control mechanism works, implement and how they provide internal security to network. The future scope of this paper is to implement such type of mechanism in all network devices, in which user interface is possible.

6.REFERENCES

[1] Daniel B. Cid, "8 steps to protect your Cisco router."

[2] Document ID: 26448, Cisco Systems, Jan 28, 2008.

[3] Document ID: 99361, Cisco Systems, Oct 12, 2007.

[4] "Introduction to Firewalls using Cisco ACL's", Cisco Systems

[5] Part VI, Advance Cisco router features.

[6] "Important Notices and Privacy Statement", Page no 1-21, Cisco Systems, Inc.

[7] Cisco Router Command Quick Reference.

8] Sean Odam, Hanson Nottingham, "Cisco Switching", Black book, Comprehensive problem solver.

[9] Joshua Wright, "A new attack paradigm, Cisco routers as targets".

[10] Document ID: 23602, Cisco Systems, Dec 27, 2007.

[11] Aaron Balchunas, "The Cisco IOS v1.22", Cisco Systems

[12] Cisco IOS (internetwork operating system) Access-lists, Help for network administrator, Cisco systems.

[13] Cisco Systems Inc., White Paper, "Understanding ACL Merge Algorithm and ACL Hardware", Resources on Cisco Catalyst 6500 Switches

[14] A.Bobyshev, P.DeMar, D.Lamore, Fermilab, Batavia, "Effect of dynamic ACLl (access control list) loading on performance of Cisco routers", il 60510, U.S.A.

[15] A. Borza, D. Duesterhaus, C.Grabczynski ,J. Johnson, R. Kelly, T. Miller, "Switch Security Guidance Activity of the Systems and Network Attack Center (SNAC), Security Configuration Guide".

[16] Steven Kieffer, "Securing Cisco routers", Network System Architects, Inc. November 2002