Simulation of an Enhanced Network Security Framework for Federal Polytechnic Mubi

Abstract

The research, Simulation of an enhanced network security framework for Educational Enterprise system such as Federal Polytechnic Mubi was carried out of the desire to protect the enterprise network against accidental or deliberate attempt to modify or temper with valuable data. The aim is to develop a workable security framework for the enterprise network of Federal Polytechnic, Mubi while focusing on parameters such as authenticity, confidentiality, integrity and non-repudiation of data. These problems were solved in the research by securing unused ports with encrypted passwords and securing access lines of all network devices such as routers and switches. The methodology adopted for the system development was the survey method and this is because it provides reliable results used to identify network security problems and experimental methods for the construction of the framework. While data was elicited from extensive review of related journals articles, lecture notes, textbooks, face to face interview and interaction with relevant stakeholders. Design tools such as Diaw were used to produce structure diagrams effectively. Cisco Packet Tracer was then used to carry out the simulation process and the results was found to be in tune with the overall objective of the design.

Keywords: Enhanced, Enterprise, Parameters, Security, Simulation.

1.0 Introduction

The enterprise network is known as that portion of the computing set-up that provides access to network communication services and resources to end users and devices spread over a single geographic location. It might be a single floor, building or even a large group of buildings covering a protracted geographic area. As computers and networked systems thrive in today's world, there is a need for increased robust PC and network security becomes more and more necessary [1]. The escalation of the network system will expose it to several varieties of internet threats. The security precaution embraced include identification, authentication, authorization and to safeguard the integrity, convenience, authenticity of the Packet transmitted over the network. Network security must be designed to suit the requirements of an organization [2]. Campus network as a form of an enterprise network is vital, and it plays an important role in any organization. Network architecture and its security are as vital should be considered by the organization. A campus network is an independent network under the control of an institution within a local geographical place and sometimes it may be a metropolitan area network [1]. The campus network, as defined for the aim of the enterprise design guides, consists of the unified elements that include the set of services used by a group of users and end devices that share the same high-speed communications' fabric. These include the data transport services which can be both wired and wireless, traffic identification and regulation which includes security, and application optimization, traffic monitoring, and organization, and overall systems management and provisioning. These basic functions are implemented in such a way as to provide and directly support the higher-level services provided by the IT organization for use by the end user community [3]. Network security begins with authorization to use the network, commonly with the use of username and password, and consists of the provision of policies adopted by the network administrator to prevent and monitor illegal access, alteration in the system, misappropriation, or denial of a computer network and network-accessible resources. Also, network security involves the sanction for access to data in the network, which is controlled by the network admin. When access is granted, the firewall then enforces policies such as what services are allowed to be accessed by the different levels of the network users. Authorization alone cannot prevent potentially harmful content, such as computer worms or Trojans being transmitted over the network, that is why Anti-virus software or an intrusion detection system (IDS) can be used to detect the malware. Communication between two hosts using a network may use the tunneling technology. This publication will show the proper methods of creating and enforcing an enterprise network security plan. Once there is a clear image of what needs the most protection, then all the necessary measure for the protection is put into consideration.

2.0 Literature review

Different research papers are consulted for security in the campus network. [2] presented various network security problems and their solutions. They denoted the security status of a campus network, analyzed security threats to the campus network and described the strategies to the maintenance of network security.[4] provide theoretical contribution as a format model architecture of a university campus network that can be used to build a vigorous and supple network that responds to the next generation necessities, secure network design is planned based on the requirements and the proposed network infrastructure is realizable with adjustable infrastructure. [5] shows the configuration of standard ACL and extended ACL on the router. The standard ACL creates a filter based on source addresses only and is used for server-based filtering, whereas, extended ACL provide more security by creating filters based on source addresses as Well, destination addresses, protocol, and port number.

Choi et al. (WAP-Wormhole Attack Prevention) [6] have presented a protocol that not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during the route discovery phase. This has been achieved through the use of the neighbor node monitoring method of each node and wormhole route detection method of the source node on the selected route.

Jain and Jain [7] have presented a trust-based model based on identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means. In this method, trust levels are derived in neighboring nodes based upon their sincerity in the execution of the routing protocol. This derived trust is then used to influence the routing decisions, which in turn guides a node to avoid communication through the wormholes.

Saha. et.al [8]: In a mobile ad hoc network, all the nodes cooperate to forward the packets in the network, and hence each node is effectively a router. The process of forwarding network traffic from source to destination is termed as routing. Consider, the scenario in Fig. 1, if node S sends data to node D, which is three hops away, the data traffic will get to its destination only if A and B forward it

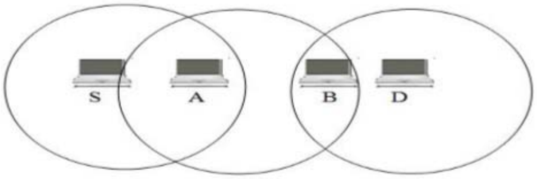


Fig 1: Routing Process in MANET

Traditional link-state and distance-vector approaches do not scale well in large and dense MANET. Several routing protocols have been proposed to address the problems associated with the link-state and distance-vector approaches in MANET. These protocols can be classified into three different groups reactive (or on-demand), proactive (or table-driven) and hybrid. Reactive protocols obtain the necessary route when it is required, by using the route discovery process. In proactive protocols, nodes periodically exchange information to maintain up-to-date routing information. Hybrid routing protocols combine the basic properties of both approaches. The process of forwarding network traffic from source to destination, such that data traffic is not hampered by active and passive attacks [6], is called secure routing.

Chhabra et al. [9] proposed a protocol to prevent and handle Distributed Denial of Service (DDoS) attacks in the networks as early as possible and before reaching the victim. Dealing with DDoS attacks is difficult due to their properties such as dynamic attack rates, various kinds of targets, the big scale of a botnet, etc. Therefore, it is better to prevent the distributed denial of service attack rather than allowing it to occur and then taking the necessary steps to handle it. The advantage is that, after the victim node is removed from all the network tables, the paths through which this node sends packets are traced and those broadcast ids are nullified. The disadvantage is that it cannot mitigate other attacks.

[10] Discuss the use of VLANs on enterprise networks and how VTP reduces the administrative work on VLANs and different challenges and issues of VLAN and VTP such as insertion of a rouge switch.

2.1 Conceptual Framework

[11] There are various categories of networks 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).

The campus network of this research is designed in a hierarchical manner that may be a common practice of campus and enterprise networks. It offers a typical topology design of standard building blocks that enable the network to evolve simply. A hierarchical design avoids the necessity for a fully-meshed network in which all network nodes are interconnected [12,13]. Designing a campus network might not seem as mesmerizing or thrilling as designing a VoIP network, an associate IP video network, or designing a wireless network. However merging applications like these are engineered upon the campus basis. Very similar to the building a bridge, if the engineering work is skipped at the foundation level, the Bridge can crack and eventually collapse[14,15].

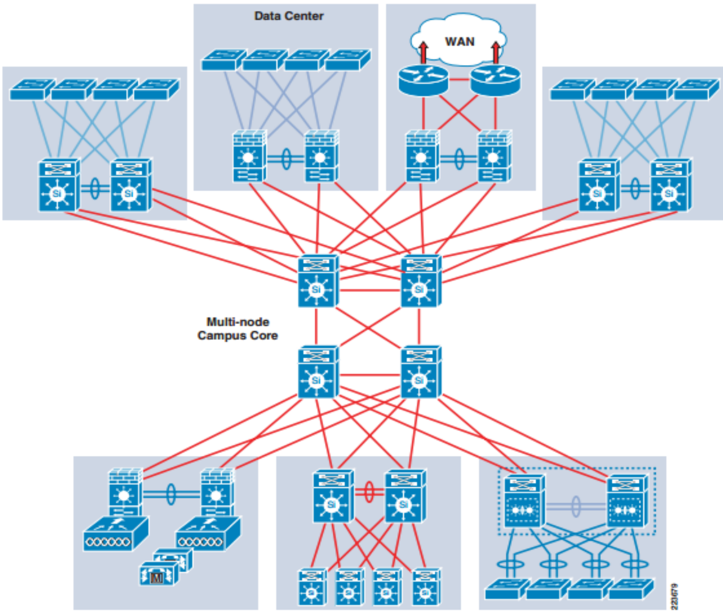


Fig 2: Hierarchical Framework of an enterprise network [14, 15]

2.2 Types of Network Attacks

The different types of network attacks include passive network attack, active network attacks, close-in attacks, exploitation from within the network, and attacks through the service provider. Information systems and networks are targets and should be impervious to attack from all threat agents. (Nadir et al. 2015). A system should be able to limit the damage done during an attack and recover rapidly after the attacks. Here are some attack types:

i. Passive Attack: Passive Attack on a cryptosystem is one in which the cryptosystem cannot interact with any of the parties involved, attempting to break the system solely based upon observed data

ii. Active Attack: An active attack is a network exploit in which a hacker attempts to change the data on the target or data on course to the target.

iii. Distributed Attack: This is an attack where multiple comprised systems, which are often infected with a trojan, are used to target a single system causing a denial of service attack

iv. Insider Attack: An insider attack is launched by an internal user who may be authorized to use the system that is attacked. It may be intentional or accidental

v. Close-in Attack: A close-in attack is a type of attack where the attacker is physically close to the target system.

vi. Phishing Attack: Phishing attack is a type of social engineering attack often used to steal user data, including login credentials and credit card details. It occurs when an attacker masked as a trusted entity and then dupes a victim.

vii. Hijack attack: A hijack attack is a form of active wiretapping in which the attacker seizes control of previously established communication associations.

viii. Spoof attack: In the context of information security, and especially network security, a spoofing attack is a situation in which a person or a program successfully pretends as by falsifying data, to gain illicit access.

ix. Buffer overflow: A buffer overflow or buffer overrun, is a common software programming mistake that an attacker could exploit to have access to your network. 10. Exploit attack: An exploit is an attack that takes advantage of vulnerabilities in applications, networks or hardware.

x. Password attack: Hackers can use cracking programs, dictionary attacks, and password sniffers in password attack. Defense against password attack is rather limited but usually consists of a password policy including a minimum length, unrecognizable words, and frequent changes.

2.2.1 Solutions to Network Attacks

i. Antivirus and Antimalware Software: This software is used for protecting against malware, which includes spyware, ransomware, Trojans, worms, and viruses. Malware is very dangerous and can infect a network and then remain quiet for a given period. The antivirus and anti-malware contain the threat through scanning for malware, detecting anomalies, remove the malware, and fix the damage done by the virus or malware.

ii. Network Applications Security: It is essential to have application security for applications running on the network. It is possible for any application to comprise of vulnerabilities, or holes, that are used by attackers to enter your network.

i. Performance Analytics: To detect irregular network behavior, you will have to know the normal behavior of the network. Performance analytics tools are capable of routinely knowing activities that deviate from normality. Your security team will thus be able to efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats.

ii. Loss of data prevention: Organizations should guarantee that their staff does not send sensitive information outside the network. They should then use Data Loss Prevention technologies, such as network security measures, that avert people from uploading, forwarding, and printing important information in an insecure manner.

iii. Email Security: Emails are known to be the number one threat vector for a security fissure in a network. Attackers use the idea of social engineering to build refined phishing operations to deceive users within the network and then send them to sites full of malware. Email security applications are proficient in blocking incoming attacks in an email and controlling sent messages to avoid the loss of sensitive data.

iv. Firewalls: Firewalls place a barrier between your internal network and outside networks, like the Internet. A set of defined rules are used to either block or allow traffic from coming into the network or leaving the network. A firewall can be software, hardware, or both. The free firewall efficiently manages traffic on your PC, monitors in/out connections, and secures all connections when you are online.

v. Intrusion Prevention System (IPS): An IPS is network security capable of scanning network traffic to actively block attacks. The IPS Setting interface permits the administrator to configure the ruleset updates for Snort. It is possible to schedule the ruleset updates allowing them to automatically run at particular intervals and these updates can be run manually on demand.

vi. Mobile Device Security: Mobile devices and apps are increasingly being targeted by cybercriminals. There is the need to control which devices can have access to your network

vii. Network Segmentation: Software-defined division put network traffic into varied taxonomies which make enforcing security policies on a network a lot easier. The classifications are based on end-user identity, not just IP addresses. Privileges can be accessed based on location, role, and more so that the right people get the correct level of access.

viii. Virtual Private Network (VPN): A VPN is another type of network security that is capable of encrypting the connection from an endpoint to a network, mostly connections over the Internet. A remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between the network and the device.

ix. Web Security: A preferable web security solution is controlling your staff's web usage by denying access to malicious websites and blocking access.

x. Wireless Security: Wireless networks are not as secure as wired networks and this will be easy for an attacker to penetrate. It is thus important for the wireless security to be strong in the network. It should be well-known that without rigorous security measures on wireless LAN, Ethernet ports should be placed everywhere for wired connections.

xi. Network Access Control (NAC): This network security process helps in controlling who access a network. It is important to know every device and user in the network to kick out potential attackers. This indeed will help you to enforce your security policies.

3.0 Materials and Methods

In this research, the survey method which provides reliable results used to identify the network security problems and experimental methods for the construction of the framework is used. Primarily, interviews were carried out to the staff of the MIS and ICT unit, Students and relevant records were also observed. For the secondary method of data collection, Journal articles, Magazines, lecture notes were reviewed in trying to gather relevant data for the research.

To actualize effectively the objectives of this research, Cisco Packet Tracer (for simulating the network), and Diaw (A software for drawing structured diagrams) were used.

3.1 Network Design

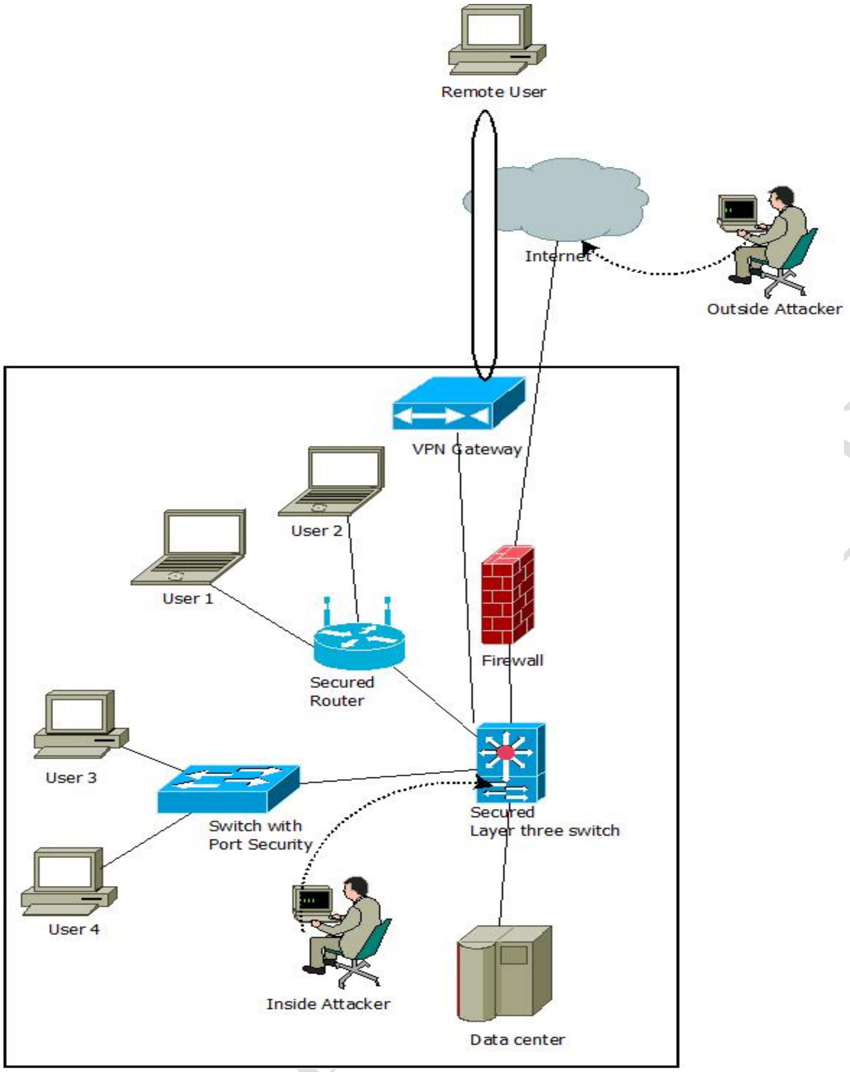


Fig 3: Defining Security parameters for an Enterprise Network

3.1.1 Port security:

The use of port security technology on the switches added more security to the enterprise network. Port security is the way of preventing network devices from using a particular or set of the port on a switch. At the port level, only certain MAC addresses are allowed or deny to use the port. This can be done either statically or dynamically. MAC addresses are either manually configured or dynamically learned by the switch. MAC Addresses that are dynamically learned can be saved on the switch and manually configured MAC addresses are called static MAC addresses. To enable port security on the switch port, this command is used on an interface that has been set as a switch port:

```
Central(config-if)#switchport port-security

Command rejected: GigabitEthernet1/0/20 is a dynamic port.
```

If an error message pops out, then there is a need to configure the port for switch port mode access before continuing:

```
Central(config-if) #switchport mode access

Central(config-if) # switchport port-security
```

Once Port security is enabled, there are options to use:

```
Central(config-if) #switchport port-security?

aging               Port-security aging commands

mac-address         Secure mac address

maximum Max         secure addresses

violation           Security violation mode

<cr>
```

In this research, an interface is configured to accept packets only from the MAC address 0001.43B5.1676:

```
Central(config-if) #switchport port-security mac-address 0001.43B5.1676
```

By default, only one MAC address can be added to the permit list. To increase the limit, use the switch port port-security maximum command, hence, you can add another MAC address:

```
Central(config-if) #switchport port-security maximum 5

Central(config-if) # switchport port-security mac-address 0001.16C6.1423
```

When a port is configured with port security, and a packet arrives that is not in the permit list, it’s considered a violation. There are three actions the switch can perform when there is a port-security violation:

Protect:

When a violation occurs, the switch drops all packets from the MAC addresses that have not to meet the configured requirements of the switch.

Restrict

When a violation occurs, the switch drops all packets from MAC addresses that do not meet the configured requirements of the switch. And an SNMP trap is generated, the log on the switch is attached, and the violation counter is deployed.

Shutdown

When a violation occurs, the switch puts the port into the error-disabled state. This will stop all packet traffic from entering and leaving the port. This is the default behavior for port-security-enabled ports.

To change the port-security violation action, use the switch port port-security violation command:

```
Central(config-if)#switchport port-security violation ?

protect          Security violation protect mode

restrict         Security violation restrict mode

shutdown         Security violation shutdown mode
```

3.1.2 Securing Access Lines.

Access lines are logical or physical interfaces on network devices such as switches and routers that are used for administration of the network. The console and aux port on routers and switches are the physical lines, whereas the logical (VTY) lines are Telnet and SSH. Securing access lines has to do with providing a password on the line using the password command:

```
Mainrouter(config-line)#password Secret
```

Passwords are case-sensitive and may include space but cannot use special characters. If a password is not set on the VTY lines, you will get an error when telnetting to the network device:

```
Password required, but none set
```

Passwords that are entered in clear text are shown by default. To have the IOS encrypt all passwords in the configuration, enable the password encryption service with the service password-encryption command as shown below:

```
Mainrouter#sho run | include password
```

```
password Secret1
```

To configure the password-encryption service to encrypt all the passwords, the configuration below is used:

```
Mainrouter#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Mainrouter(config)# service password-encryption

Mainrouter(config)# exit.
```

3.2 Analysis of the existing system:

The existing network system has less security features. Passwords of network devices such as routers and switches are stored in clear text which is visible when tracking packets using software like Wireshark. The unused ports on the routers and switches are vulnerable to inside attack since they are not secured. The absence of a firewall within the network makes outside attack easier on the servers in the network. On the existing network, there is no secure connection for a remote user of the network

3.3 Analysis of the Proposed system:

The proposed system in this research have capabilities and features that provide a counter against the loopholes in the existing system. In the proposed system, all unused ports of the network devices are secured using encrypted passwords whereby only authorized users are allowed to use the devices and hence, inside attacks to the network are contained. A firewall is placed between the internet connection to the network and the core layer switch of the network: hence, preventing an outer attacker from having access to the network. Remote users of the network can have a secured connection to the network using the VPN technology.

Access lines to the network devices are all secure with encrypted password authentication which enables only the network administrator access for the management of the devices.

4.0 Results

The results and analysis of tests carried out are discussed in the following sections

4.1 Result for Show IP Route Command on Core Router

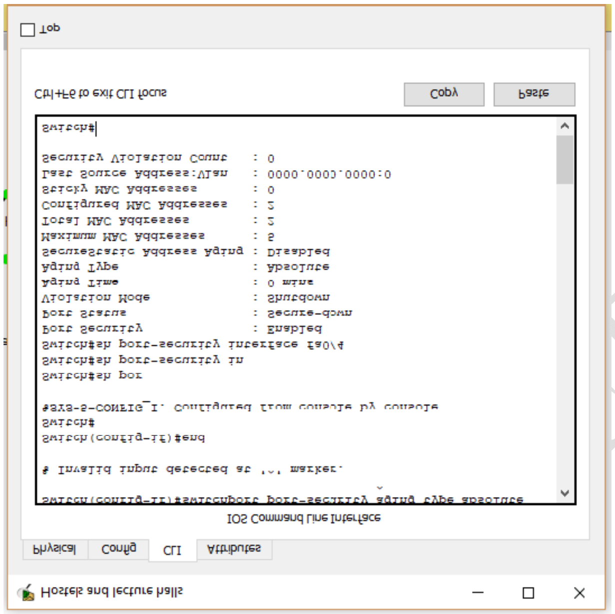
Figure 4: Depicts the result of the command on the core router’s command line interface as input “**show port-security interface fa0/4**” and the result is as follows:

Port security: Enabled

Port status: Secure down

Violation Mode: Shutdown

This shows that the Unused ports are all secured to prevent unauthorized parties.

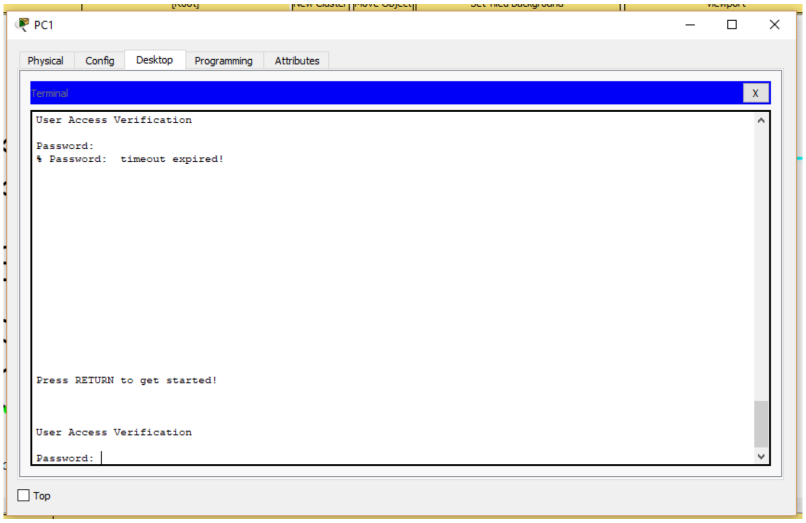

□ Top
Ctrl+F6 to exit CLI focus
Copy
Paste
IOS Command Line Interface
Physical
Config
CLI
Attributes
Hostels and lecture halls

```
Switch(config-if)#switchport port-security aging type absolute
                                              ^
% Invalid input detected at '^' marker.

Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh por
Switch#sh port-security in
Switch#sh port-security interface fa0/4
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 2
Configured MAC Addresses   : 2
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

Switch#
```

Fig 4: Port security on Interface fa0/4

4.2 Result for Secured Console Port of Router

Figure 5: Below shows password authentication of the console line to access the network device this happens whenever the computer is connected with the console cable to the network device. The password timeout warning shows when the password does not input on time

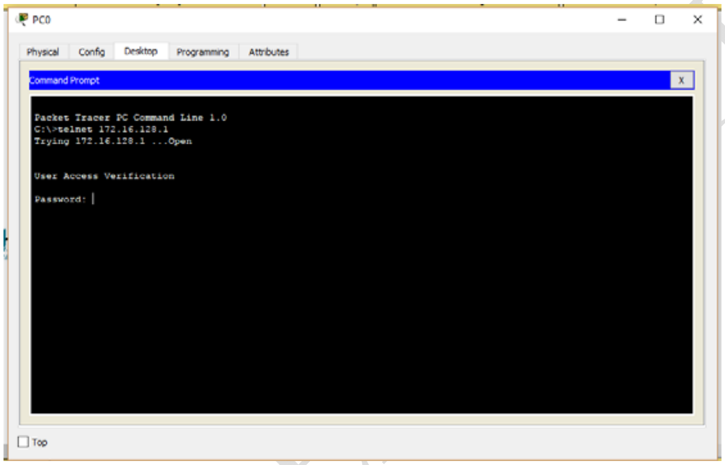


```
User Access Verification

Password:
% Password:  timeout expired!









Press RETURN to get started!


User Access Verification

Password:
```

Fig 5 Secured console port

4.3 Result for Secured VTY Port

Figure 6: The input "telnet 172.16.120.1" was keyed in to access the network devices, hence authentication is required by the input of a password.



```
Packet Tracer PC Command Line 1.0
C:\>telnet 172.16.128.1
Trying 172.16.128.1 ...Open


User Access Verification

Password:
```

Fig 6: Secured Telnet with Password Authentication.

5.0 Conclusion

Network architecture and its security are necessary for any organization. If we tend to use the hierarchic network design, the network will be scalable, performance and security are increased, and therefore the network simple to take care of. During this work, we tend to project a compact price effective secure campus network design based on the work atmosphere and required quantifiability, security and different aspects. The proposed network infrastructure is achievable with flexible 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] Mohammed, N. B. A (2013) Network Architecture and Security Issues in Campus Networks, Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT).

[2] Lalita, K., Swapan D., Radhey, S. Security Problems in Campus Network and Its Solutions, 1, Department of Computer Science1-2, NIT Agartala, India, National Informatics Centre, India.

[3] Cisco Inc. (2016*). Administrative Guide - WAP4410N Wireless-N Access Point.* San Jose: Cisco Press, 2-4.

[4] Nadir, M., Emran, M., (2015) Design and Implementation of a Secure Campus Network, *International Journal of Emerging Technology and Advanced Engineering*, 5(6), 5-6

[5] Suman, K., and Agrawal, N.F., (2016), Implementation and configuration of ACL in an enterprise network, *Indian Journal of researches*, 9(7), 8-10.

[6] Choi, S., Kim, D.Y. Lee and J.I.Jung. “Attack Prevention Algorithm in Mobile Ad Hoc Networks, "in porc. of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, June 2008, pp 343-348

[7] Jain, A., Jain, A., and P. K. Sagar, (2010)" Various Security Attacks and Trust-Based Security Architecture for MANET," *Global Journal of Computer Science and Technology*, (10)14, pp 32-36,

[8] Saha, H. N., Bhattacharyya, D., Banerjee, P. K., Bhattacharyya, A., Banerjee, A. and D.Bose, (2012) “Study of Different Attacks in MANET with its Detection & Mitigation Schemes,” *International Journal of Advanced Engineering Technology (IJAET),* 3(1), 383-389,

[9] Chhabra, M., Gupta B., and A. Almomani, (2013) “A Novel Solution to Handle DDOS Attack in MANET,” *Journal of Information Security*, 165-179,

[10] Sivakumar, G., (2016). *Design and Implementation of Campus Network and Computing Infrastructure*, (1st ed), Bombay, Indian Institute of Technology Press, 5-7.

[11] Michael, G. (2017) Design and Implementation of a Secure Campus Network *International Journal of Pure and Applied Mathematics* 116(8), 303-307

[12] University of California, Davis http://manuals.ucdavis.edu/ppm/310/310-17.htm

[13] Udayakumar R., Kaliyamurthie K.P., Khanna, Thooyamani K.P., Data mining a boon: Predictive university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.

[14] Thooyamani K.P., Khanna V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.

[15]R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)Volume 8, Issue 4, Pp. 376–385, April 2017.