ZONAsi Information System Journal
ZONAsi VOL. 4 NO. 1 MARCH 2022
Page: 1 - 17
ISSN: 2656-7407 (Online)
2656-7393 (Print)

INTEGRATION OF APPLICATION LAYER SERVICES WITH CENTRAL AUTHENTICATION SERVER IN EXAMPLE OF HTTP AND FTP RESTRICTION

Abdul Qadeer Rasooli [1], and Khan Mohammad Habibi[2], and Faqeed Ahmad Sahnosh[3]
[1] Ghor Institute of Higher Education, Computer Science Department, Education Faculty, Ghor, Afghanistan
Phone number: +93788 20 3003
qadirrasooli5@gmail.com
[2]Ghor Institute of Higher Edcution, Information Technology Department, Computer Science Faculty Ghor, Afghanistan
phone number: +937860308300
Habibi.cs.ghr@gmail.com

[3]Kabul Education university, Information Systems Department, Computer Science Faculty, Kabul, Afghanistan
Phone number: ++93707929254
Sahnosh1388@gmail.com

[*]Corresponding Author Email Address: qadirrasooli5@gmail.com

Abstract

Nowadays it is very important to have an authenticated and secure network. hackers are always one step further and try to steal credentials or doing malicious actions. Many organizations implement strong authentication systems for taking drastic security measures to prevent threats and vulnerabilities. This paper describes integration of application layer services with central authentication server called Lightweight Directory Access Protocol(LDAP), it covers detailed mechanism to control and restrict any software application or network services which may implement and require central authentication protocols including web (eg: HTTP protocol) and file transfer protocol (eg: FTP protocol). This will enable authenticated web and ftp webpage for reliability and security. The authentication services also provide Ubuntu client domain join and network authentication to enable integrity and authentication across the network. This paper is conducted through deep library research and practical implementation of the services.

The goal of this paper is to introduce a unified secure centralized authentication system to authenticate and grant the authorized users to have access to the restricted Kerberized services in a period of time which is granted. It provides more trust, secure environment, but less traffic and others` interference.

Keywords: *Security, Authentication, Integrity, HTTP, FTP, LDAP, Samba4, Kerberos, KDC, DNS, NTP*

1. INTRODUCTION

Nowadays people and trade depend on networked computer systems to support scattered applications. These scattered applications might act reciprocally with computers on a local area network, "within a corporate intranet, within extranets linking up partners and suppliers, or anywhere on the worldwide Internet." To make better functionality and "ease-of-use", and to allow a cost effectiveness management of distributed applications, data related to the services, users, resources, "and other objects accessible from the applications needs to be organized in a clear and consistent manner." [1].

May be most of this information shared between applications, but this shared information must be protected in order to prevent from unauthorized modification or the exposure of private information. This information often gathered or stored into a database that is called directory that describe the various users, applications, files, printers, and other resources accessible from a network. As the number of different networks, applications and specialized directories has grown, so it is difficult to manage all isolated shared information. If this information could be kept and accessed in a compatible and managed manner, it would provide a central point "for integrating a distributed environment into a consistent and seamless system." [1].

The Lightweight Directory Access Protocol (LDAP) is an open manufacturing standard that could meet these needs, if it integrated with some application layer services like Samba and Kerberos. Information could be updated and accessed with a standard manner which is defined by LDAP directory. A lot of software vendors support the LDAP and has a corporation with a growing number of applications [1].

To have a strong integrated, manageable authentication system that support the mentioned functionalities with further specifications; application layer services like Samba and Kerberos should be integrated with this central authentication server (LDAP) in order to manage, control, authenticate the users and machines. In here Samba act as domain controller that control, manage and apply policies to users. LDAP act as an active directory that authenticate, store and maintain users and machines information. Kerberos act as an authentication system that authenticate users and only authorize and authenticate the users that are defined into LDAP directory and added to the Kerberos principal have the right of access to the services.

Network Time Protocol server does time synchronization between servers and clients, and Doman Name Service provide name resolution. Linux client configurations is required to enable authentication with server.

In fact, LDAP directory is defined as a Kerberos principal. The valid users could access to the Kerberized services after authentication. So, authentication is the process of validating that computer or network users are who they claim to be and that they are authorized to use the facility [1].

The process of user authentication is consisting of: When a user principal writes in a log of a machine which is configured for Kerberos authentication purpose, the Key Distribution Center (KDC has a Principal database in which all LDAP users should be added to be able to authenticate) issues a Ticket

Granting Ticket (TGT). If the user assigned credentials match, so the user is authenticated and then can ask for ticket for using Kerberized services from the Ticket Granting Server (TGS). Finally, the users after receiving service tickets allowed to authenticate to the services and access them without entering their username and password repeatedly.

To the best of our knowledge,this research is never done before in Computer Science Faculty of Ghor University in Afghanistan.

Many information obtained by studying books and reliable internet sites and have been used in this research paper to complete all parts to achieve the goal. It will solve many security problems, as far as these powerful services are integrated together, they will bring safety with a lot of trusty environment in a network.

It restricts accessing to some services like FTP and HTTP from unauthorized users and it introduce a unified secure centralized authentication system to authenticate and grant the authorized users to have access to the restricted Kerberized services in a period of time which is granted. It provides more trust, secure environment, but less traffic and others` interference.

2. PROBLEM STATEMENT

Today people use internet and browse websites every time and in everywhere and is still on progress. In our beloved country Afghanistan, this process is also on progress, but in this country, most of organizations' employees or Universities' students gain access to their relevant organization services without authorization and authentication and use from services for short or long time that they want. And organizations provide services to them without having a security measures; authentication, authorization and determining login session time which is very dangerous from security view. The only things that are more important for organizations are their assets that must be protected, no one could gain access to them. In here two hypotheses are in my mind which solve these problems:

- Restricting access to services like HTTP and FTP will bring reliability and of course authorization of private webpages for an Organization.
- Having a strong security measures which is possible by implementing and integrating application layer services, like Samba and Kerberos with a central authentication server (LDAP) will bring authentication and authorization of network services therefore security in the Network. Additionally, this is the base for integration of application layer services with a central authentication server in order to restrict access to HTTP and FTP services.

To restrict accessing to the services such as HTTP, FTP and decrease the traffic on these Network and Servers, and create an authentication Server to grant the authorized users then determine their presence (or their session time) in that network for using services which are provided in a period of time. We will follow all processes in this research paper.

3. GOALS

The main goal of this paper is to integrate application layer services with central authentication server in order to restrict accessing to HTTP and FTP services. This will help us to mitigate security problems and provide trust. Implementing such systems provides ease and more facilities for all users are going to connect to the network without fear of sniffing and spoofing their credentials, because this system control user access, authenticate users, manage and allow authorized users to access and use from services, determine the time of usage for users, prevent from exchanging credentials in the network and decrease the traffic and load on servers.

4. METHOD

The data collected analyzed from valid resources of the internet and different books and have been used in different section of the research paper. We have done and tested our work on Virtual Box, the practical parts brought in the two final chapters of research.

5. Introduction to Network Services

We will explain about DNS, LDAP, NTP, Samba, Kerberos server, FTP and web server which are related to the research and work on them.

5.1 **Domain Name Service**

Domain Name Service (DNS) is an Internet service which changes "IP addresses and fully qualified domain names (FQDN)" to each other. So, DNS help us to don't remember IP addresses it is enough to know names. Computers in which DNS are configured called name servers. Ubuntu use BIND9 (Berkley Internet Naming Daemon 9), the superlative famous "program used for maintaining a name server on Linux.

5.2 **LDAP**

In this paper, we implement OpenLDAP version3 which is the current version of LDAP defined in RFC4510." The Lightweight Directory Access Protocol [(LDAP)], is a protocol for querying and modifying a X.500- based directory service running over TCP/IP." [2].

By the LDAP we can manage and control all information and configurations such as users, groups, and etc… in centralized method. And we use LDAP for centralized user management purpose. When we configure LDAP server it held all information and credentials that users need to log on the network. Then the users send their credential to the LDAP server from client computers for authentication. We must configure LDAP Directory, because this Directory contains all information which are needed for users to log on to the network. One of the advantages of LDAP Directory is its compatibility with X.500 standard, and other Directory services also use this standard as well. Like "Microsoft Active Directory and Novell eDirectory." [3].

LDAP has a hierarchical structure database which store different configuration information, and information about users, such as their name, last name, e-mail, password and other information [3].

5.3 Samba

Samba cannot play role of an Active Directory Primary Domain Controller (PDC), we can configure the Samba server to act as a "Windows NT4-style domain controller." One of the goodness of the Samba is, it centralizes the machines and users' credentials. For storing the users' information Samba can use multiple backend. So, in here we use LDAP as the Samba backend [2].

"Samba is a software suite that allows a Unix-based system to appear and function as a Microsoft Windows server when viewed by other systems on a network." [4].
Samba has many parts, all parts work together to execute both the client and server "portion of the Common Internet File System (CIFS) protocol." Microsoft operating systems use from CIFS network protocol to access the resources like files and printers which are shared and also use for remote administrations. CIFS is not a file system and is not fitting for the Internet. It is a protocol which is selected for Windows networks.

5.3 **Network Time Protocol (NTP) Server**

Fundamentally a client demands the current time from a server, and uses it to fix its own clock. Network Time Protocol (NTP) pave the ground for client to fix it`s clock, so "NTP is a TCP/IP protocol for synchronizing time over a network." [2].

It was an easy explanation about NTP, but in background it is more complicated, here are layers of NTP servers, one of the "NTP servers connected to atomic clocks," and the layer two and three NTP servers distributing "the load of actually handling requests across the Internet.

Also, the client software has to factor out communication delays, and adjust the time in a way that does not upset all the other processes that run on the server." 5.5 Kerberos Server

We explain the functions and functionalities of Kerberos system and then go through configurations. It is better to understand what we do during configurations to work successfully. Kerberos was developed by Massachusetts Institute of Technology (MIT) for three aims that MIT had: [3].

✓ To find a replacement for passwords that move around the network, Integration of Application Layer Services with Central Authentication Server in Example of HTTP and FTP Restriction to:
✓control "access rights to services".
✓ "deal with user database"

To achieve these three goals, we need Kerberos version 5. Passwords are not stored locally on a machine, and it doesn't matter to Kerberos server, if that machine is server or a client. So, no worry

about losing credentials and it decreases the risk when someone attack to your machine. That is why many people use Kerberos instead of normal authentication methods, and in Kerberized version of Kerberos many Linux services are available [3].

There are three parties in Kerberos which have the important role:

- ✓ Client
- ✓ Server
- ✓ Key Distribution Center (KDC)

In here administrator set up a trusted environment with Client, Server and KDC which they have more confidence to each other, because they are in same realm. When a user login to the KDC at the same time the Kerberos session begin. "The KDC has a database with password hashes (so it doesn't know the actual user passwords). When authenticating, the user creates a hash that is based on his password." Then KDC calculate the hashes and can understand that the user entered the correct password or not. If it was correct, the KDC gives the user a Ticket Granting Ticket (TGT). Next user using that TGT can access to services. "The KDC again plays an important role, because it grants a session ticket for each of the services the user wants to connect to." When the user gains this session ticket, he can access to many related services as long as remained logged in. [3].

We introduce some terms which are related to Kerberos and is good to know these terms before starting to installation and configuration of Kerberos server: (Team, 2016).

- ✓ Principal: "any users, computers, and services provided by servers need to be defined as Kerberos Principals." [2].
- ✓ Realms: "the unique realm of control provided by the Kerberos installation." It is a domain or group which control, and manage all your machines and users, and all of them are related to the realm. The realm should be in uppercase. And it is necessary to have a configured DNS, because it use from DNS domain as the realm which is converted to uppercase, like: 'HOTNET.COM'. [2].
- ✓ Key Distribution Center: In KDC we have three parts, "a database of all principals, the authentication server, and the ticket granting server." We need at least one KDC for each realm and it is necessary.
- ✓ Ticket Granting Ticket: Authentication Server (AS) give Ticket Granting Ticket (TGT) to users, the TGT "is encrypted in the user's password which is known only to the user and the KDC." [2].
- ✓ Ticket Granting Server: (TGS) provide services` tickets to clients when they want to request for service.

- ✓ Tickets: "confirm the identity of the two principals. One principal being a user and the other a service requested by the user." Tickets create "an encryption key which is used for secure communication during the authenticated session." [2].
- ✓ Keytab Files: "are files extracted from the KDC principal database and contain the encryption key for a service or a host." [2].

To combine all these parts together, there should be at least one KDC for a realm, or may be more KDC for replication, and this KDC has a Principal database. When a user principal writes in a log of a machine which is configured for Kerberos authentication purpose, "the KDC issues a Ticket Granting Ticket (TGT)." If the user assigned credentials "match", so the user is authenticated and then can ask for ticket for using Kerberized services from the TGS. Finally, the users after receiving service tickets allowed to authenticate to the services and access them without entering their username and password repeatedly [2].

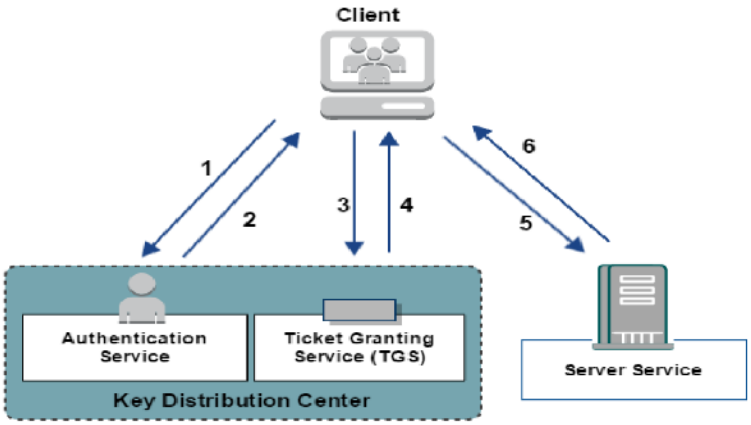

Figure 1. Kerberos and Key Distribution **[3].**

5.5 **Apache2 Web Server**

On Linux systems we commonly use from apache web server. And this server used for browsing web pages which are queried by client machines and view web pages using web browser applications such as Mozilla Firefox, Chrome, Internet Explorer. Then users using this web browsers point to some Web servers by typing their IP address or Fully Qualified Domain Name (FQDN) and its path to the required resource into the Uniform Resource Locator (URL) **Center** Hyper Text Transfer Protocol (HTTP) are the most famous protocols which are used for transferring Web pages to users` computers [2].

5.6 File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a TCP protocol which is used for uploading and downloading files between server and client or between computers. It commonly used in the past, but its usages decreased

nowadays, because it does not use any encryption method and user credential as well as data are transferred in plane text that everyone can see and sniff the data. [2].

And we can manage accessing to an FTP server in two manners:

- ✓ Anonymous
- ✓ Authenticated

In the Anonymous mode, everyone can access to FTP server by default user name which is ftp user and do not ask credential, and use from an email as its credential. And in authenticated mode it requires user name and password for authentication, but it has not secure transaction.

6. PREREQUISITES

Install an Ubuntu 16.04 LTS, then update your system, next install and configure dynamic host configuration protocol (DHCP) server, next install Openssh-server (because we need it) finally determine your system Host Name, Domain Name, Fully Qualified Domain Name and static IP address like below:

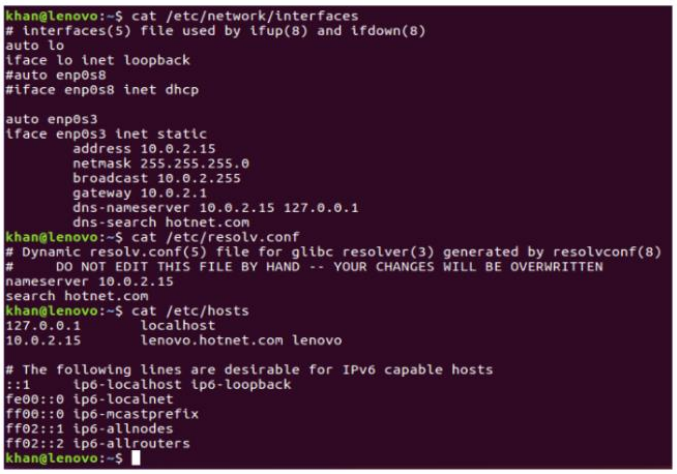

Figure 2. Configuring interface, resolv.conf, hosts

6.1 **Installation and configuration of DNS**

In DNS we have two zone forward lookup zone (which change name to IP) and reverse lookup zone (which change the IP to name). Entire the DNS we should manipulate and configure only four files which shown by figures.

```
#forward lookupZone
zone "hotnet.com" {
        type master;
        file "/etc/bind/db.local";
};

#Reverse lookupZone
zone "2.0.10.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};
```

Figure 3. DNS Zone Configuration **[2].**

6.2 **Installation and configuration of OpenLDAP**

To install OpenLDAP server in Ubuntu, it exists "in Ubuntu's default repositories under the package 'slapd'", so we will install it with ldap-utils which is an extra utility [10].

During the installation you will be asked some questions to configure your OpenLDAP server, so you should configure it carefully.

6.3 **Installation and Configuration of PHPldapadmin**

By PHPldapadmin we will be able to administrate LDAP Directory and it is a web based interface. "This is also available in Ubuntu's default repositories." This will install all PHP dependencies and required web server. [10].

Step1: Install PHPldapadmin

Step2: Log into the Web Interface: Then access phpldapadming interface by server "domainname or IP address followed by /phpldapadmin in your web browser." [10].

1: **hotnet.com**/phpldapadmin.

2: Click on "login" enter ldap admin password.

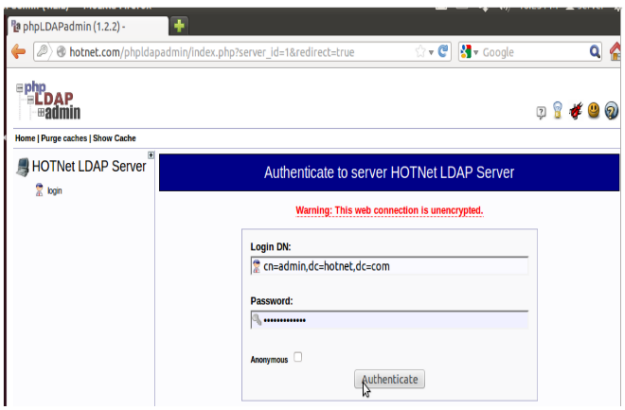

Figure 4. Phpldapadmin web interface **[10].**

6.4 **Installation and configuration of Samba4**

Step1: Install samba4 and it`s necessary packages to change your server into an active directory domain controller server [6].

6.5 **Integration of Samba and LDAP**

In this part we will integrate Samba with LDAP. Samba server play the role of a "standalone" server and the LDAP directory act like a database for storing users, groups, and machines` accounts information. It will provide an authentication layer between server and users. We configured before all the pre-requisite services that we need in order DNS, OpenLDAP server and Samba server [2].

7. Software Installation

We need two packages when we want integrate Samba with LDAP, Samba and smbldaptools. By smbldap-tools package we can manipulate and manage the various Samba entities like: users, groups and computers in an LDAP context.

7.1 **Installation of NTP Server**

First of all, we want to install the Network Time Protocol (NTP) and NTP client utility in Ubuntu

7.2 **Installation of Kerberos Server**

We will install and configure a MIT Kerberos domain like below characteristic:

- ✓ Realm:HOTNET.COM
- ✓ Primary KDC: lenovo.hotnet.com (10.0.1.15)
- ✓ User principal:Rasooli

o Admin principal: rasooli/admin It is preferred

that your network authenticated users have their uid in a different range like start of 1000 than that of your local users. We already configured DNS server properly, it is necessary for our domain, because Kerberos matches its Realm with Domain Name using an agreement [2].

And we already installed and configured NTP server, because "Kerberos is a time sensitive protocol." And it only can tolerate between five minutes' differences other vise the Clients couldn't authenticate with server. So NTP server solve this problem. Now install the krb5-kdc and krb5-admin-server krb5-user krb5-config packages to complete the Kerberos server

7.3 **Integration of Kerberos and LDAP**

Bothe Kerberos and LDAP are the protocols which are used for authentication to authorize the users, but most of the people do not use Kerberos by itself, they prefer LDAP for that purpose. It is more complicate to recreate a Kerberos principal database among two servers, and join an "additional user

database to your network." Luckily, we can configure MIT Kerberos "to use an LDAP directory as principal database." In this section, we will configure a primary Kerberos server to use OpenLDAP Directory as a principal database [2].

7.4 **Result of integrated Samba and Kerberos with LDAP**

That is, it Kerberos is integrated with LDAP server. The result of Samba and Kerberos which are integrated with LDAP shown in the following figures:

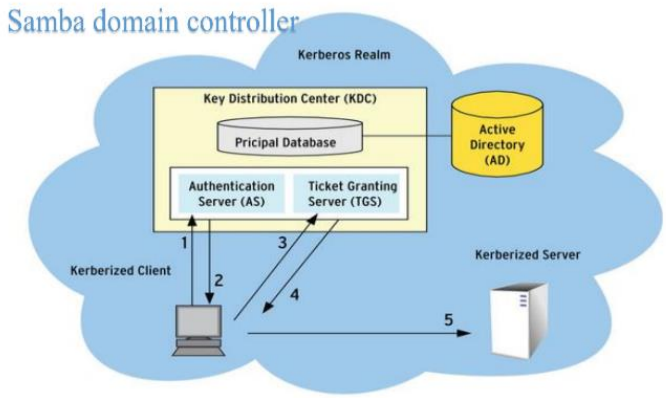

Figure 5. The result of integrated Samba and Kerberos with LDAP in dyagram **[3].**

7.5 **Restricting Access to HTTP Server**

We restrict access to a specific HTTP server site and allow only LDAP users to have access to this server site. In here we restrict accesses to apache2 on specific web page [9].

More details about installations and configurations are available inside the document

7.6 **Installation of APACHE2**

Install the apache2 server on your Ubuntu 16.04 LTS First of all, enable authnz_ldap modul, then create a new file in this path /etc/apache2/sites-available/auth-ldap.conf and write the following content as shown by the following figure [9].

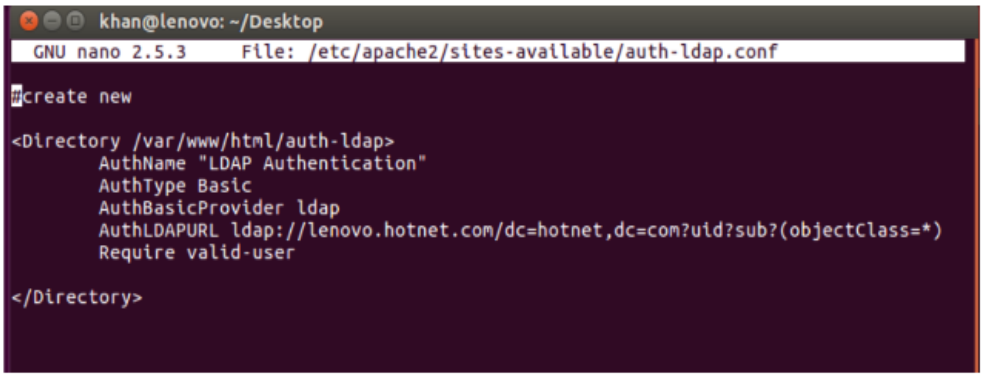

Figure 6. The new created file in which the ldap authentication and path defined.

Users access restricted to the HTTP, know can access using their users and passwords.

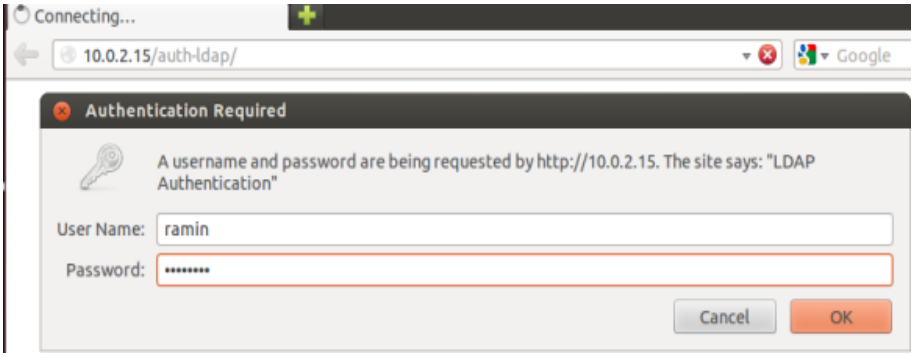

Figure7: Accessing the web page for authentication [8].

7.7 **Restricting Access to FTP Server**

In here we first install vsftpd package

And then configure a VsFTPd server to authenticate with an LDAP server. So we configure that only authorized LDAP users can access to FTP server by the following steps.11 [5].

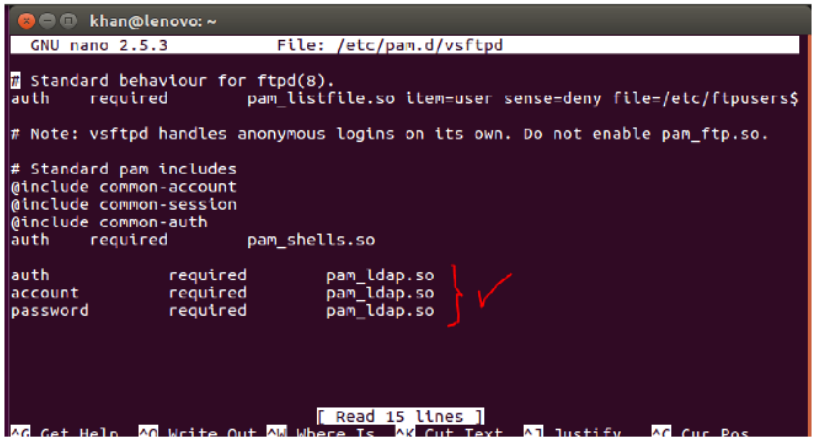

Figure 8. Adding lines into PAM file which is used for authentication to LDAP server.

Users access restricted to the FTP, know can access using their users and passwords.

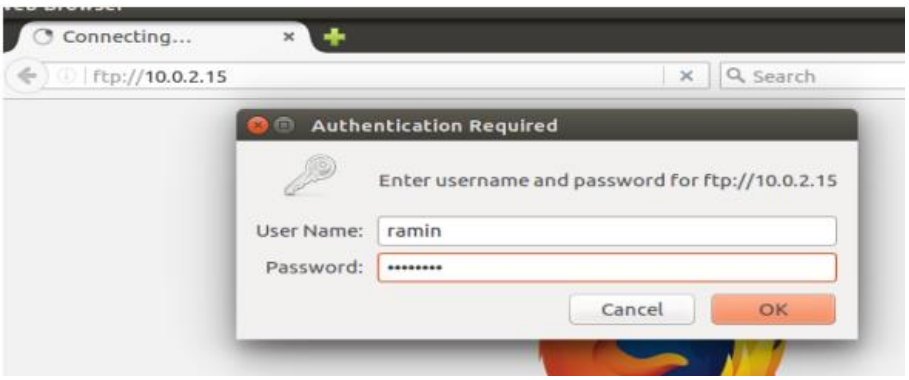

Figure9: Logging test for FTP in web browser

More details about installations and configurations are available inside the document

8. How to Authenticate Client Computers Using LDAP

First we should update the client system then install SSH by **sudo apt-get install ssh** command, because after configuration we do SSH from client to server, follow the following steps [10].

8.1 **Installation**

Step1: Install client packages on the client machine, because if we want to our client machine authenticate with an LDAP server correctly, so we need to install the following packages [10].

$ sudo apt-get install libpam-ldap nscd

Step2: A series of questions asked the same as questions asked during installation of the server components follow the bellow steps.

1- In this step change the original string from "ldapi:///" to "ldap://" then enter the LDAP server IP address: ldap://LDAP-server-IPAddress.

2- This must be the same as the entry that "you put in your LDAP server'/etc/phpldapadmin/config.php file." Like this: "dc=hotnet,dc=com"

3- Select the version of the LDAP server: 3

4- Make local root Database admin: Yes

5- Does the LDAP database require login? No

6- LDAP account for root: This also must be the same as the entry you entered in your /etc/phpldapadmin/config.php file. Find this line "'login','bind_id"' in the file my example is "cn=admin,dc=hotnet,dc=com"

7- LDAP root account password: Your-Server-LDAP-root-password

8- If you did some mistakes you can reconfigure your client again.

9. Configuring Kerberos Linux Client

In this part of configuration, we will configure a Linux client system as a Kerberos machine. And when we successfully logged into the system using a LDAP user. We will able to access to all "kerberized" services which are provided

9.1 **Installation**

If we want to authenticate from a client to a Kerberos Realm, then we need to install "krb5-user and libpam-krb5 packages" with some other necessary packages on the client machine.

When we install auth-client-config package in fact it enables easy "configuration of PAM for authentication from multiple sources, and the libpam-ccreds will cache authentication credentials allowing you to login in case the Key Distribution Center (KDC) is unavailable."

More details about installations and configurations are available inside the document

Figure 10. The client joined to domain and user login to machine

10. Comparisons between existing internet applications from various sides

I want to compare my research, which has a practical and research aspect, with the rest of the programs available on the Internet in terms of security, Functionality and accuracy.

From a security point of view, it has a very high level of security, in which effective protocols, Centralized authentication services and from the point of view of cryptography and hashing are used, including the Kerberos service, MD5, and TGT (Ticket granting ticket Mechanism), with central authentication server (LDAP), it covers detailed mechanism to restrict HTTP and FTP restriction, to introduce a unified secure centralized authentication system to authenticate and grant the authorized users to have access to the restricted Kerberized services in a period of time where users do not worry about losing their username and password because the hackers Cannot get the user's password and username in the network, there for it is excellent from security view. May be there are a lot of internet applications like our worked project which do not support these security measures.

From a functionality point of view, this project has a very effective, accurate and fast performance, because in it we used standard services such as Samba4 as domain controller, LDAP as the active directory, and Key Distribution Center as key distributor for granting users in the system, it is very good system and does not generate a lot of traffic in the network, and in addition to the main services, we also have Secondary services, which prevent from down time or the case of action is not seen in the internal network.

Because the HTTP and FTP service are restricted in here and also every user have its own credential for accessing the network and services, there is a centralized system that control the users and services

and also the time that issued to users for accessing the network and services there for the network that use such system and services there is very low traffic more security and trust and also more availability and accuracy.

This project is better than every other application that we now in the internet like SSO and CAS (Central Authentication Server), "With single sign-on (SSO), users are authenticated only once, regardless of how many other applications they attempt to access after the initial login" (Alex Salazar, 2014).

11. CONCLUSION

In the recent years the business have been grown using networked computer systems, the important things for organization is it's asset, they try to keep it safe from others view. And in the network or internet many applications used to provide services and facilities for customers. These applications might act reciprocally with computers on a local area network, within a corporate intranet, within extranets linking up partners and suppliers, or anywhere on the worldwide Internet. To make better functionality and ease-of-use, and to allow a cost effectiveness management of distributed applications, data related to the services, users, resources, and other objects accessible from the applications needs to be organized in a clear and consistent manner. May be most of this private information shared between applications, which are important for a business man and he don't want spread his private information. But this shared information must be protected in order to prevent from unauthorized modification or the exposure of private information. This information often gathered or stored into a database that is called directory that describe the various users, applications, files, printers, and other resources accessible from a network. As the number of different networks, applications and specialized directories has grown, so it is difficult to manage all isolated shared information.

If this information could be kept and accessed in a compatible and managed manner, it would provide a central point for integrating a distributed environment into a consistent and seamless system.

The Lightweight Directory Access Protocol (LDAP) is an open standard that could meet these needs. And we integrated this service with some application layer services like Samba and Kerberos. After integration a strong integrated, manageable authentication system created that provide more functionalities that prevent from unauthorized modification of data. In here Samba act as domain controller that control, manage and apply policies to users. LDAP act as active directory that authenticate, store and maintain users and machines information. Kerberos act as system authentication that authenticate users and only authorize and authenticate the users that are defined into LDAP directory and added to the Kerberos principal have the right of access to the services. We need further services that complete our network like: Network Time Protocol server which do time synchronization between servers and clients, and Doman Name Service which provide name resolution and also used as samba domain and Kerberos realm that help us to implement a secure network with more confident. The valid users could access to the services after authentication. It restricts accessing to some services like FTP and

HTTP from unauthorized users and it introduce a unified secure centralized authentication system to authenticate and grant the authorized users to have access to the restricted services in a period of time which is granted. So, if a user private information shared between these services there is no worry about losing the shared information. In our beloved country, Afghanistan most of organizations' employees or Universities' students gain access to their relevant organization services without authorization and authentication and use from services for short or long time that they want. And organizations provide services to them without having any security measures, which is very dangerous from security view. The only things that are more import for organizations are their assets that must be protected, no one could gain access to them. To have a powerful system that support more facilities and could meet that needs, you can use from this guide in which, application layer services like Samba4, Kerberos have been integrated with a central authentication server like LDAP (Lightweight Directory Access Protocol) in order to authenticate users and machines, then grant them to use from services. It provides more security, trust, reliability and a confident environment.

REFERENCES

[1] S. Tuttle, A. Ehlenberger, R. Gorthi, J. Leiserson, R. Macbeth, N. Owen, S. Ranahandola, M. Storrs and C. Yang, Understanding LDAP Design and Implementation, Second ed., North Castle Drive Armonk, NY 10504-1785 U.S.A., United state of Amireca: IBM Corporation, 2004.

[2] U. D. Team, Ubutu Server Guide, Author, 2016.

[3] S. v. Vugt, Pro Ubuntu Server Administration, F. Pohlmann, Ed., New York: Springer-Verlag New York, 2009.

[4] G. Carter , J. Ts and R. Eckstein, Using Samba, Third edition ed., A. Oram, Ed., Sebastopol, United States of America: O'Reilly Media, 2007.

[5] J. Ellingwood, "How To Install and Configure a Basic LDAP Server on an Ubuntu 12.04 VPS," 1 October 2013 a. [Online]. Available: https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-a-basic-ldap-server-on-an-ubuntu-12-04-vps. [Accessed 1 October 2017].

[6] M. Cezar, "Create an Active Directory Infrastructure with Samba4 on Ubuntu- part 1," 23 March 2017 a. [Online]. Available: https://www.tecmint.com. [Accessed 12 October 2017].

[7] SK, "Setup Samba Domain Controller with LDAP Backend in Ubuntu 13.04," 18 September 2017. [Online]. Available: https://www.unixmen.com/setup-samba-domain-controller-with-openldap-backend-in-ubuntu-13-04/. [Accessed 11 October 2017].

[8] M. Cezar, "Manage Samba4 Active Directory Infrastructure from Windows 10 via RSAT - Part 3," 7 December 2016 b. [Online]. Available: https://www.tecmint.com. [Accessed 14 October 2017].

[9] S. World, "Basic Auth + LDAP," 13 June 2016. [Online]. Available: https://www.serverworld.info/en/note?os=Ubuntu_16.04&p=httpd&f=11. [Accessed 17 November 2017].

[10] J. Ellingwood, "How To Authenticate Client Computers Using LDAP on an Ubuntu 12.04 VPS," 2 October 2013 b. [Online]. Available: https://www.digitalocean.com/community/tutorials/how-to-authenticate-client-computers-using-ldap-on-an-ubuntu-12-04-vps. [Accessed 1 October 2017].