PREVENTIVE MECHANISM FOR POTENTIAL SECURITY THREATS AND ATTACKS ON VIRTUAL CLOUD LDAP SERVER

Su Su Win[1], Mie Mie Su Thwin[2]

Abstract

Today, universal cloud computing and digital world cannot exist without virtualization architecture. They are basic tools to support varying demands without sluggish, expensive physical reconfiguration and software stack investment. On the other hand, Information and data are live source of today business in an organization. These data are created more and more every day. Data can be saved, but the weakest link in the cloud security is end point. Users can move on and data can be lost. This can bring more exposure to security threats, no reliable and safety. So, cloud security is becoming an important research topic. To demonstrate the weakness and vulnerabilities of LDAP (Lightweight Directory Access Protocol) server on virtual cloud environment, paper is developed by allowing Kerberos Single-Sign-On with LDAP directory service environment with client/server model in order to prevent third party password sniffing, eavesdropping and stealing password from LDAP database.

Keywords: LDAP Server, Single Sign On, Kerberos Authentication, Ticket, Password Sniffing

Introduction

LDAP server is frequently used by medium-to-large organizations and the scope is ranging from small servers for workgroups to large organizational and public servers. When the enterprise has own LDAP server, this organization can use this service to look up contact of users' information, user management and controlling authentication safely. E-mail register controlling mechanism can also be done by centralized up to date administration. LDAP servers are adaptable and able to replicate data both pushing or pulling methods. LDAP directory server that stores users' information data by means of hierarchically.

One of the techniques to partition the directory is to use LDAP reference model, which enable users to refer LDAP requests to a different server. The main concept of LDAP is the information model, which deals with the kind of information saved in directories and the structuring of information. The information shape model revolves around an entry, which is a collection of attributes with type and value. Entries are organized in a tree-like structure called the directory information tree (DIT). The entries are created around real world concepts, organization, people and objects. Attribute types are link with syntax defining allowed information. A single attribute can enclose multiple values within it. The distinguished names of the configuration in LDAP are read from bottom to top. The other left part is called the relative distinguished name and the right part is the base distinguished name.

The proposed system performed empirical analysis with LDAP server password sniffing attack with Kali Linux platform by using python and Wireshark tool. LDAP server password sniffing procedure can gather client's password information by querying the LDAP host server. LDAP is a kind of single sign on Client/Server model and when the information travel across the network and internet, Unsigned and malicious network traffic is susceptible to man-in-the-middle attacks. In such attacks, an intruder captures packets between the server and the client device, modifies them, and then forwards them to the client device. Where LDAP servers are concerned, an attacker could cause a client device to make decisions that are based on false records from the

[1] Lecturer, M.A.Sc (Computer Engineering), University of Computer Studies, MyitKyina, Ministry of Education
[2] Dr, Professor and Head of Cyber Security Research Lab, University of Computer Studies, Yangon

LDAP directory. To lower the risk of such an intrusion attack in an organization's network, some kind of potential attacks that happen on LDAP server such as LDAP injection and LDAP enumeration attacks can be found on recent research topic.

Background Theory

Kerberos is a kind of network protocol in client/server environment and uses secret key cryptography when clients want to communicate to the server. It is man in middle server. Whenever client want to use the server services, Kerberos requests an encrypted ticket by use of authenticated server. Kerberos, the name of the protocol come from three-headed dog for security guarded at the gates of Hades in Greek mythology. Kerberos was begun and developed by the name of project Athena- it is a joint project linking between the Massachusetts Institute of Technology (MIT), Digital Equipment Corporation and IBM that ran between 1983 and 1991.

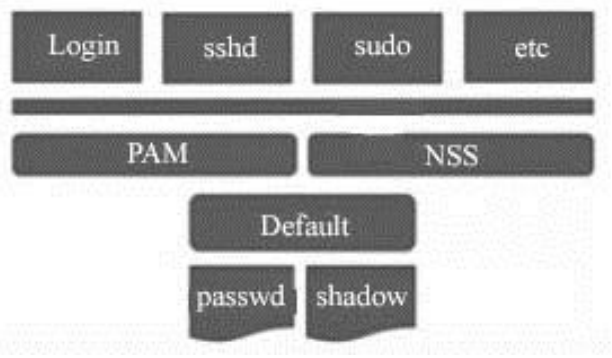


Figure 1 Linux Password Storage system in PC

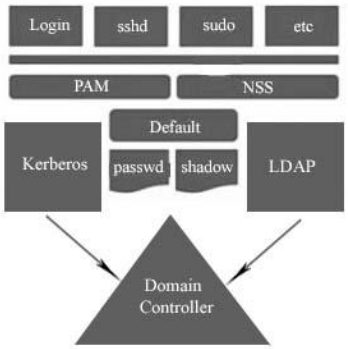


Figure 2 Integrated Design with Kerberos

An LDAP authentication server utilizes a Kerberos ticket to give permission server access and build a session key depend on the requested person's password. Then, the ticket-granting ticket (TGT) is connected to the ticket-granting server (TGS), in order to use the similar authentication server process. The requester (client) receives an encoded TGS key with a time stamp and service ticket, after that returned to the requester and decoded. The client sends the TGS this information and forwards the encoded key to the server to get the required service. When all events are handled accurately, the server takes the ticket and completes the requested user service, which have to verify the timestamp, decode the key and communicate the distribution center to get session keys. This session key is sent to the client requester, which decodes the ticket. As soon as timestamp and keys are valid and acceptable, client-server communication continues to establish. The TGS ticket means time stamped to permit concurrent and parallel client requests during the allow time frame.

Related Works

Kerberos was introduced at the Massachusetts Institute of Technology (MIT) to defend network services support by Project Athena. Versions 1–3 used only internally at MIT. Although Steve Miller and Clifford Neuman are the ordinary designers of Kerberos 4, many members and followers of Project Athena supplied to the design and implementation of Kerberos.

Kerberos 4 was available and published in the late 1980s. Even if it was pointed mainly for Project Athena, growing of it to be used in recent computer networks. Version 5 was invited by John Kohl and Clifford Neuman. It performed as RFC 1510 in 1993 (made obsolete by RFC 4120 in 2005).

To overcoming the limits and security problems troubleshooting of version 4, discuss in that was published in 1988 to support and know the fundamental motives for why Kerberos 4. This contribution is quite related to Kerberos 5. But, the basic principal ideas of the protocol have remained the same.

Problem Statement

Users login and password are recorded as centralized manner in Kerberos architecture, that protects clients from storing passwords on their related machines. Network security authentication protocol weaknesses due to unencrypted data transfer on network facilities of services can be reduced with the help of Kerberos. These are some issue that happen in proposed virtual environment system.

- Sniffing password from LDAP server
- Stealing password from LDAP database

Implementation and Contribution

In this experiment, the system tested with VMware type-1 hypervisor implementation.

As first step of proposed system design, a virtual environment was created for type-1and the networks were configured on the host server machine, with one network allowing access to the Internet and an internal one with the IP address range shown in table (1) and figure (4) as IP address domains. For IP address allocation, 10.0.0.0/24 is used to communicate between the virtual machines. Then, the Management VM was created with Linux Open source software through a desktop environment installed, before the network interfaces were configured and SSH (Secure Socket Shell) access was enabled for remote access.

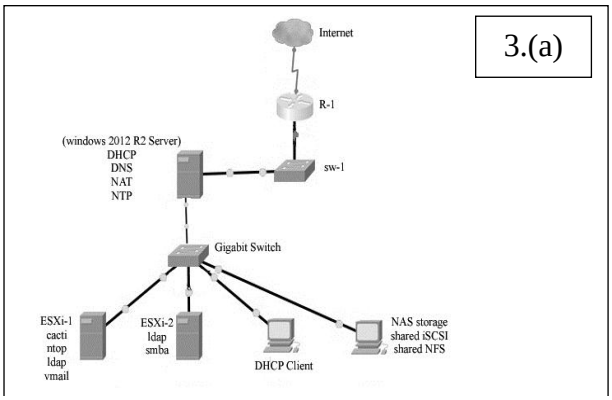


Figure 3(a) Virtualization with LDAP Server Architecture

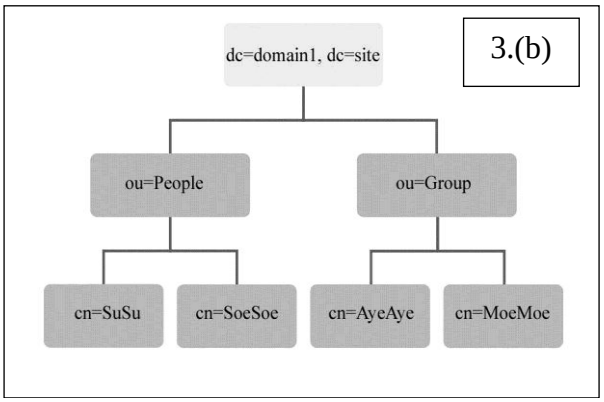
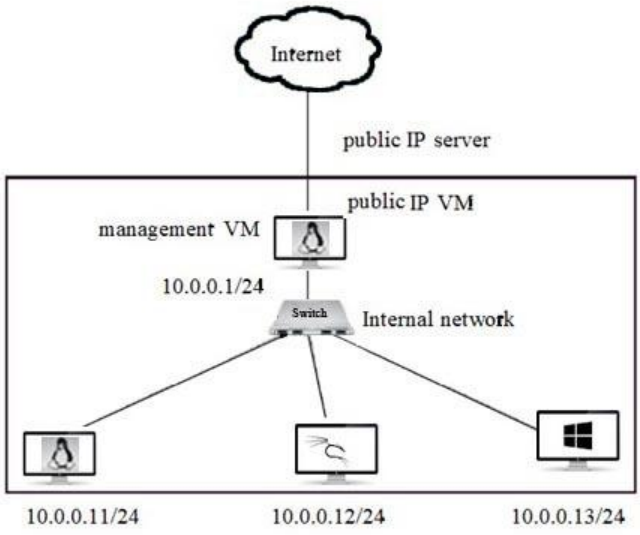


Figure 3(b) LDAP Tree Structure

Table1 IP Addressing scheme of Tested Virtualization Environment

No	FQDN	IP Address	System	Installations
1	vcenter.domain1.site	172.16.10.1	Windows 2012 R2	DNS, DHCP, NAT, NTP and VMware vCenter Server
2	esx1.domain1.site	172.16.10.11	VMware ESX	ESXi 5.0
3	esx2.domain1.site	172.16.10.12	VMware ESX	ESXi 5.0
4	nas1.domain1.site	172.16.10.21	NAS	Openfiler
5	research.domain1.site	DHCP	Windows XP (Management PC)	VMware vShpere Client

The next step is the creation of the basic VM template which was used to create a total of three VMs for the internal network by installing their respective servers one by one.



LDAP (Linux) | Hacker (Kali Linux) | Wireshark (Monitoring)

Figure 4 Tested Procedure for Sniffing Traffic

To implement a Kerberos security system with a proposed system, users have to pass network through three layers before they can access network services from the server. Firstly, Authentication to the Boundary Router and describes the operations to follow in the authentication process. A remote distance user who successfully initiates a PPP (Peer to Peer) session to the communicate the intended site is prompted by the router in order to register with login and password. Although in this phase the user is inside the firewall, to gain access to the network services, it still must authenticate to the Key Distribution Centre (KDC).

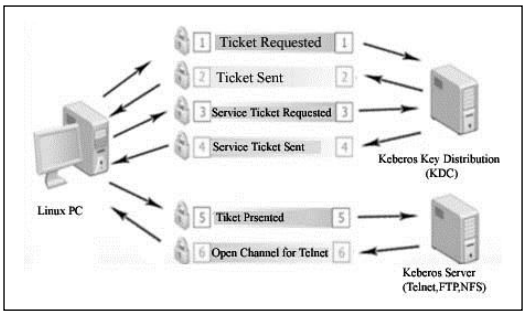


Figure (5-a)

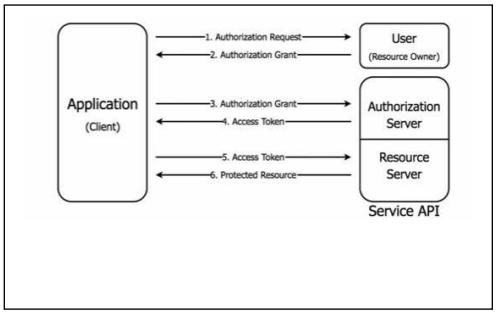


Figure (5-b)

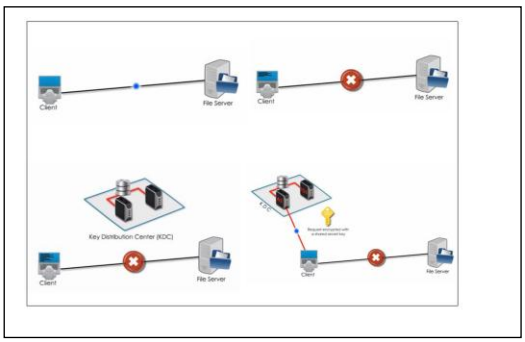


Figure (5-c)

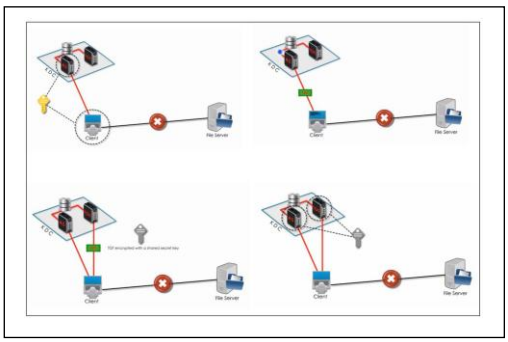


Figure (5-d)

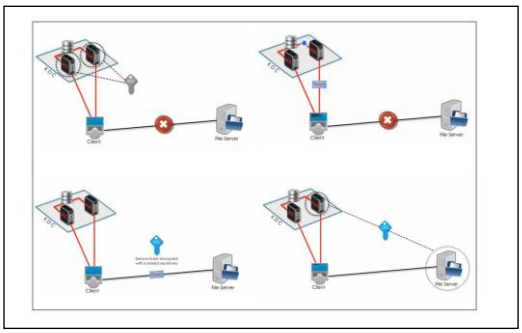


Figure (5-e)

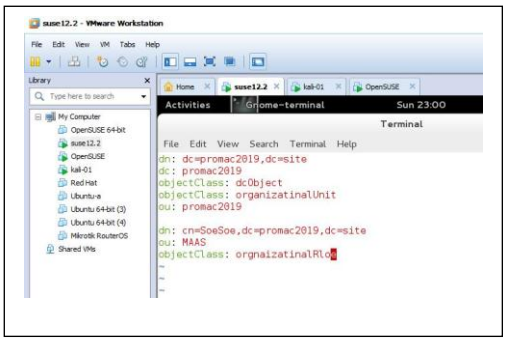


Figure (5-f)

Figure 5 (a-f): Step by Step Working with Kerberos function in Tested Area

After that, ticket TGT issued by the KDC is stored on the router and is not useful for additional authentication unless the user physically logs on the router. Therefore, the next step is Obtaining a TGT from a KDC. it prompts the user for the password to decrypt the ticket if it is successfully, the user has a TGT and can communicate securely with the KDC.

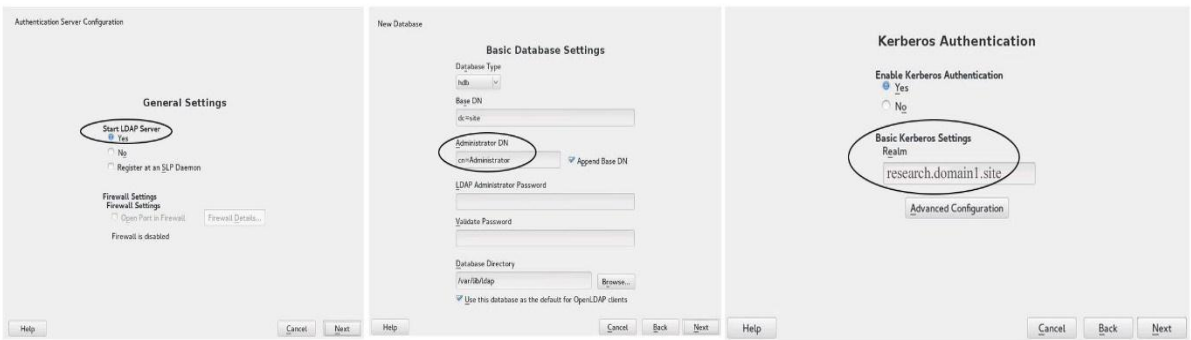


Figure 6 LDAP Server with Kerberos Authentication

In the following figure-7, that illustrate password sniffing for a LDAP server via Wireshark tool.

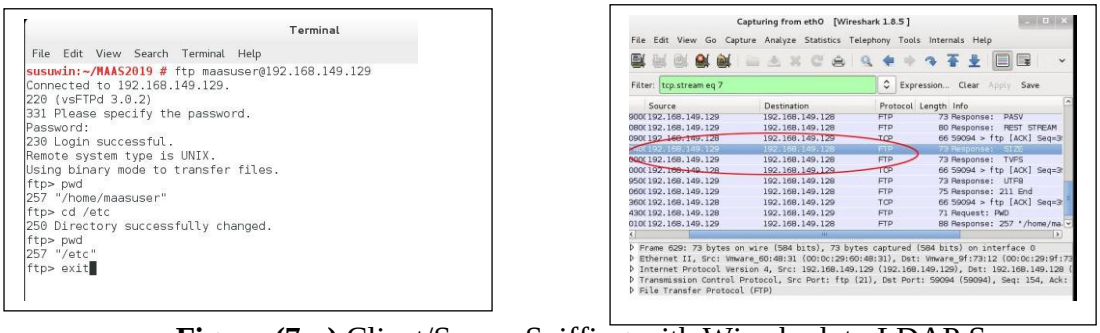


Figure (7-a) Client/Server Sniffing with Wireshark to LDAP Server

Figure (7-b) Plain Text Showing Password that Sniff in Wireshark Tool

In Figure-8, that demonstrate the configuration file of LDAP server for user input.

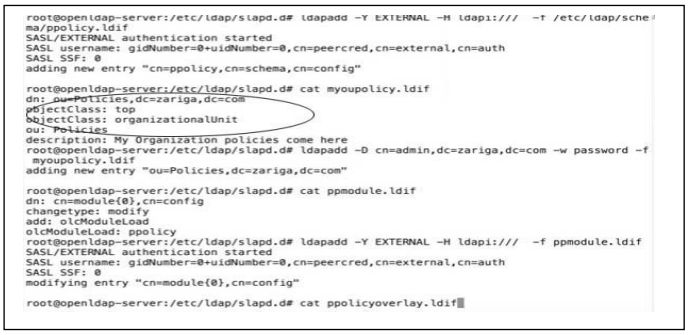


Figure 8 Creating Password Policy in LDAP Server

After the configuration of (ldif.conf) file, this is the output home page of LDAP server in GUI view.

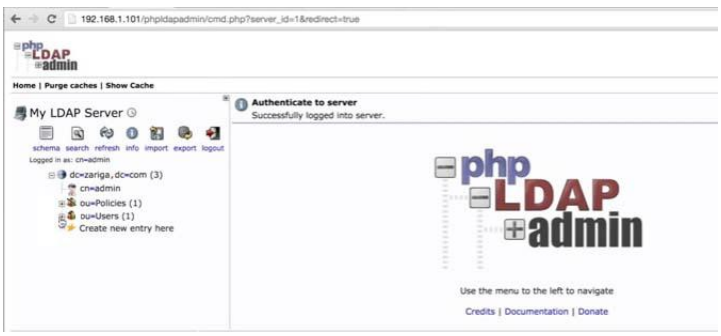


Figure 9 Home Page of LDAP after Configuration

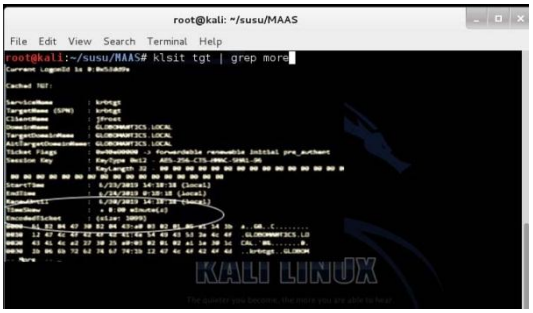


Figure 10 Output Command of Checking Kerberos Ticket

Finding Method and Discussion

The submitted proposal architecture supports LDAP server including both server-side and client-side components. The LDAP queries are known as LDAP exploration filters, which are constructed using prefix symbolization. Below is an sample case of an LDAP search filter: find ("(&(canonical name=" + client username +")(client password=" + pass +"))")

This prefix attachment filter and sorting notation established the query to find an LDAP client with the specified username and password. If the user-controlled values are prefixed to the LDAP search filter without any proof or decleration, a username and password value of '*' alters the intended sense of meaning. The method to prevent code injection techniques include defensive software design with programming, complex input validation, dynamic and live checks with static source code analysis. The job of mitigating LDAP injections must involve similar techniques.

Understanding LDAP database password stealing is little difficult from traffic sniffing other things like SNMP traffic, DNS traffic and NetBIOS information. because the attacker must have good knowledge of Active directory configuration about LDAP server configuration. The system used Wireshark and Kali Linux when it is tested.

Benefits and Limitations

- In Kerberos design architecture, user login information and their credentials are kept in the main centralized server. So, it is a difficult job to transfer all login credentials from local machines #/etc/passwd and #/etc/shadow files to the central server.
- If some hacker gets privilege to control the central server, the entire organization infrastructure will be under control of threat.
- The functions can be protected using Kerberos must have Kerberos efficiently built into the system.
- It is no standards for the authentication management of the Kerberos protocol. This kind of event is different from server implementations.
- The proposed system Kerberos necessitates constant availability of the KDC. When the Kerberos server is not working, the system will have weak point and vulnerable to the single point of failure problem. This can be mitigated by replacing of multiple Kerberos servers.

Conclusion

The system is tested in secure log in that focus on cryptographic protocol intended to achieve authentication over the secure network. The design objective is not only susceptible to password guessing attacks but deploy Kerberos protocol with Linux open SUSE. The proposed system presents a general overview of Kerberos network authentication protocol. Another part of the proposed system is focusing on the Kerberos' successful authentication in the of client/server architecture integrated with LDAP server to prevent password sniffing is demonstrated with Wireshark network traffic sniffing tool. Finally, the system gave the idea of its benefits and limitations.

Acknowledgement

Firstly, I would also like to acknowledge Dr Than Naing Soe, Head of University of Computer Studies, Myint Kyi Nar, Ministry of Education for allow me to submit this paper.

Secondly, I am extremely grateful to my supervisor Dr Mie Mie Su Thwin, Professor and Head of Cyber Security Research Lab, University of Computer Studies, Yangon for her invaluable guidance, supervision, patience, encouragement during the period of this paper.

References

B. Bryant, "Designing an authentication system: a dialogue in four scenes," Project Athena document (February 1988). Available at http://web.mit.edu/Kerberos/dialogue.html

C. Neuman and Ts'o. Theodore, "Kerberos: an authentication service for computer networks," IEEE Communications Magazine. September 1994

FIN 2009 Writing Access Control Policies for LDAP, Findlay, A., UKUUG conference proceedings, spring 2009 http://www.skills1st.co.uk/papers/ldapaclsjan2009/

https://www.techopedia.com/definition/3996/kerberos

J. Kohl, and C. Neuman, "The Kerberos network authentication service (V5)," RFC 1510. September 1993. Available at http://www.ietf.org/rfc/rfc1510.txt, 2005

J. M. Alonso, R. Bordon, M. Beltran and A. Guzman, "LDAP Injection & Blind LDAP Injection," Figure 1 in URJC, 2008, ICCS 2008, p. 4.

J. M. Alonso, R. Bordon, M. Beltran and A. Guzman, "LDAP Injection & Blind LDAP Injection," URJC, 2008, ICCS 2008.

"LDAP Injection: Are your Web applications Vulnerable?". Sacha Faust. SPI Dynamics URL: http://www.spidynamics.com/support/whitepapers/LDAP.pdf URL2 http://www.networkdls.com /Articles/LDAPinjection.pdf

"Open LDAP—Secure Computing Wiki," 2010. http://www.secure-computing.net/wiki/index.php/OpenLDAP

"RFC: 2830: Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security," 2000, http:// www.rfceditor.org/rfc/rfc2830.txt

"RFC 1487: X.500 Lightweight Directory Access Proto-col," 1993.http://www.faqs.org /rfcs/rfc1487.html

"RFC 4512: Light Directory Access Protocol (LDAP): Directory Information Models," 2006. http://tools.ietf. org/ html/ rfc4512

"RFC 2251: Lightweight Directory Access Protocol (v3)," 1997. http://www.faqs.org/rfcs/rfc2251.html

"RFC 4422: Simple Authentication and Security Layer (SASL)," 2006. http://tools.ietf.org/html/rfc4422