Security threats and features of ldap

1. Introduction to LDAP:

There are many protocols listed in the networking communications such as HTTP, FTP and one among them is LDAP, which is expanded as Light Weight Directory Access Protocol. LDAP is primarily used in thecommunicationof directory services. This protocol runs depending on four models categorized as: informational model (describes about the directory), naming model (structuring and referring the directory data), functional model (describes about the mechanism of protocol on directory services access), security model (describes about the protection of data in a directory from malicious programs or any unauthorized access).

This coursework explains about the various security threats that may raise during the design of a directory service and the security features that LDAP supports. Prior to that, there is a need of understanding the functionality involved and the data transfer or access between client and server needs to be discussed. Later, the directory cannot be used for storing public data if the mechanism or security support is not available for LDAP services for the applications and users. In a reason for developing trust from the users and applications, there is a need of providing some of the important security features along with LDAP systems and services.

2. Protocol Operation:

LDAP is a message oriented protocol, where the LDAP client sends a request for data to LDAP server and server processes the request and returns the client with multiple messages with unique message_id as the result. The

following figure explains about the protocol operation about client server communications.

3. Auditing features in LDAP:

What security auditing features does LDAP support and is it possible to detect brute forcing attacks (such as NAT) against a LDAP server?

The initial security feature while designing a directory can be developed based on security threat or issues that generally make a service insecure. The security problems are difficult to fix if there is no clue form the threats occurred. So, there is a need to maintain a track record of whoever has access the system and the timestamp that the system was accessed. There should be additional information about the operations performed and the impact of the operations with results of some errors or unusual conditions. With the help of such information, it can be easier to analyze the logs which can narrow down the technical security problems insight. Some of the security features in LDAP examples include break-in attempts, trawling attempts, misconfigured applications. The auditing features help in detecting the brute force attacks and supports LDAP operations with the following methods:

Break-in attempt triggers when there is a multiple failures that occurred repeatedly that were noted down in the error logs due to loginfailurewhich raises a choice of break-in attempt.

Trawling refers to unauthorized bulk downloads from the directory services or data from the systems. The trawling attempt is to monitor the repeated

search results such that the limit for download exceeds the allotted administrative limits.

Misconfigured applications: Some of the applications retrieve certain data that is not relevant to the directory systems or the data of directory services. Such application even place unnecessary load on the servers and these are rated as misconfigured applications. Auditing such information helps the administrator of the directory server to counter such threats or can also help in identifying the solutions to make the server with optimal solutions.

The auditing feature is available on LDAP based account or through a local file system access in /etc directory. In most of the cases, the auditing feature is disabled by default on LDAP accounts. The command line option with audusr –a or –d makes the accounts active and disable respectively for auditions.

Once the account of LDAP or local user account was authorized, then the flag for system auditing can be set to enable. Such configuration can be enabled by defining the parameter “ initial_ts_auditing” in the client configuration file “/etc/opt/ldapux/ldapux_client. conf”. Auditing feature is dependent on the host specifications where the setting needs to be enabled for each and exclusive hosts. They share unique audit Ids for different LDAP based accounts which are not synchronized when they are executing in trusted mode.

If the LDAP account changes or gets updated, a unique id is generated for each host that the account is created on. Initially, as discussed auditing flag will be set to disable in “/etc/opt/ldapux/ldapux_client. conf” file. Else,, if the

account is deleted in the directory server, related information will not be completely deleted from the local system. Reason is that the information that is stored in the local system can be re-used when there is a need to use the account again. However, such accounts can be removed from trusted mode manually which can be specified in the directory: /tcb/files/auth/… directory, and … represents the initial of the account name.

4. Security features of LDAP: (RFC 2829)

Authentication security feature for LDAP can be done in two approaches – one way communication, where client enters the simple password texts to the directory server in a LDAP bind operation or the server provides a SSL Secure Socket Layer certification to the client where the connection will be encrypted. Another type of network in LDAP is two way communications, where client and server exchange SSL certificates.

SSL layer divides the data sent across into multiple blocks where each block is associated with check sum value to make sure that the blocks are not tampered in the transit. So, if the data sent will be signed with SSL certificate from the indicated party, there is a little chance of the data to be tampered in the transit and such security feature was termed as Signing.

Encrypted data has very interesting feature that only the receiver for the data can decrypt the data with the code and possibly the sender will know the code to undo from the original. There is minimum chance for the data to get scrambled when sent through the security mechanism of encryption. There needs to be a feature developed in any directory system when the data sent needs to be acknowledged with a end to end security enabled. This

feature needs to be implemented to track the data if the security was compromised and in what manner the security was lost. Such information will be logged inside the error logs of every directory server and such mechanism of tracking records and error logs is defined as auditing security feature.

Firewall is the vital security feature available on LDAP directory systems which prevent unauthorized access on the resources or data inside the network or directory server. Examples are e-commerce websites that are equipped with efficient firewalls which create multiple zones of security where the zones are included with public Internet sites and internal database servers with sensitive information.

These above mentioned mechanisms are the security features which are available inclusive in LDAP In the next section, the area that will be discussed on the security systems that support LDAP in keeping the directory systems more secure.

Intrusion detection systems are mainly supportive while a intruder tries to look-up information and access certain secure data. These systems help in detecting such attack and signals that an attack has occurred on the directory systems. They consists of network intrusion detection systems NIDS, which identifies the network packets and system integrity verifiers SIVs, which monitor system resources such as registry settings.

SSL – Secure sockets layer protocol, as explained earlier is a protocol which was mainly developed for the use of making certain protocols like LDAP, HTTP etc more secure. It is mainly based on the public key cryptography that

comprises of authentication, signing and encryption features of additional security to the directory systems. Kerberos provides authentication and encryption features as well with the directory systems in LDAP. SASL, Simple authentication and Security layer will be applicable for application layer protocols that can negotiate the authentication by supporting encryption, signing and authentication services. Internet Protocol Security, IPsec helps in providing a security mechanism on transport layer connections where LDAP runs on TCP Transfer Control Protocol between machines. IPsec is mainly dependent on public keytechnologythat can be useful in administrative tasks on the directory systems.

5. Implementation of ACL over LDAP

How is it possible to implement an access control list on a LDAP server?

Introduction:

Access control lists (ACLs) over LDAP server has the underlying reason for their implementation as to monitor the individual’s rights and permissions of access on the different resources and directories. The configuration syntaxes are defined for ACL as: {*, self, anonymous, users, Regular expression} where

* represents any connected user (can be self or anonymous user)

Self represents DN, distinguished name of the currently connected user who was successfully authenticated in the previous LDAP bind operation or request.

Anonymous represents non-authenticated user connections

Users represent the opposite of anonymous as the authenticated user

connections

Regular expression represents DN or a SASL identity.

(Source: Carter, 2003).

Example syntax for ACL syntax on LDAP server:

The individual login username will be considered as the form of DN as

(DN="`cn = Gopal Krishna, ou= people, dc= Glamorgan, dc= org") or as the form of SASL identity as (DN=" uid = gk123, cn= Gopal Krishna, cn= auth"). The access privileges vary from one user to another user narrowing from top to bottom where the intensity of access also varies accordingly. Write permission is on the top access level followed by read, search, compare, auth, none. The simplest way to monitor the access level is initially defining a default access level of authorization. The configuration file that includes all such information of LDAP is: " slapd. conf". When there are no rules or roles generated or provided for any user, slapd. conf file has all the parameters that define the access levels for the unspecified users.

Example:

To assign the role or privilege of " searching the directory" is given to all the users. It can be implemented in the slapd. conf file as shown below:

The next implementation of ACL on LDAP is to define the entry and attributes that needs to be applied on directories. They are categorized as: regular expression, LDAP search filter, comma-separated list of attributes. (Source: Carter, 2003).

Regular expression:

It defines the distinguished name (DN) of the proposed or desired ACL that needs to be set on directory systems. Then, the syntax will be written as: “ dn. targetstyle= regex” where,

Target style represents one of the bases (can be sub tree, one or children). It has the default value of sub tree where it is used to broaden or narrow down the scope of ACL for the authenticated or non authenticated users (anonymous users). If we consider example of sub tree comparing the target style value as one, then the scope of ACL limits to the value of children immediately next to the defined DN. However, in most of the real time scenarios, the default value does not gets changes as most of the users need to be provided the privilege of sub tree scope of limit on ACL over LDAP.

Regex term represents the actual regular expression specification of DN. It follows the most commonly used normal regular expression rules such that the regular expression will not affect the DN value to make it in a normalized form.

LDAP search filter:

LDAP search filter is configured by specifying the filter as “ Filter = ldapFilter”. If the LDAP query searches all entries of an “ object class attribute”,

Search scope defines the “ LDAP search queries”, by default has sub tree as the target list searches for all the entries from the directory server that was defined by –b option. When the search filter targets with target style = children, number valued as one; the immediate children of the base suffix

entry or searching the single entry. The entries are specified as sub, base, or one are identified by the search scope –s (RFC 2820).

Comma separated attributes:

The file “ slapd. conf”, with the query of “ slapd” returns the attributes which are non-operational. For every entry in the directory, there will be an extending list of attributes inside the directory. When the results target operational attributes, the examples of such attributes are: modify Timestamp and modifiers name.

A comma separated list of attributes is written with the syntax:

” attrs= attribute List”. The ACL applies to all the attributes held by such entries which match the distinguished name regular expression pattern. If there are no such search filters present and the requirement shifts towards the asterisk (*) which will be used as a placeholder that consist of every attribute list filters. If the access needs to be provided for every user, for example when a read operation needs to be allotted for all the available users, the syntax is written in the form as:

Space indicates that the other line is continuation of the earlier command. The entire syntax can be written in a single line where most of the complex ACLs makes the easier readable format in such spaces.

If the user needs to be restricted on the access with a password attribute, user can access and does not have any explicit permissions of read and write permissions. The implementation can be written as follows:

Else, if the password permission for updating by the user, implementation of ACL on LDAP can be obtained by:

(Source: Carter, 2003).

6. References

LDAP System Administration by Gerald Carter, Copyright 2003 O’ Reilly & Associates, Inc published on March 2003 First Ed.

Understanding and Deploying LDAP Directory Services, Second Edition By Timothy A. Howes Ph. D., Mark C. Smith, Gordon S. Good

Access Control Requirements for LDAP (RFC 2820). E. Stokes, D. Byrne, B. Blakley, and P. Behera, 2000. Available on the World Wide Web at http://www. ietf. org/rfc/rfc2820. txt.

Authentication Methods for LDAP (RFC 2829). M. Wahl, H. Alvestrand, J. Hodges, and R. Morgan, 2000. Available on the World Wide Web at http://www. ietf. org/rfc/rfc2829. txt.

Chris McNab, Network Security Assessment: Know Your Network, Second Edition, O’Reilly, 2007, ISBN: 0-596-51030-6.