Ferhat Elmas
Przemyslaw Pietrzkiewicz
Javier Martín De Valmaseda Castro

Lab-5 NIS and Passwords

Existing NIS Setup

Alfa

First, we entered into alfa:
$> vzctl enter 1000
Then, we got the content of /etc/passwd file by cat and getent, with diff tool we compared them and there were exactly same.
$> cat /etc/passwd >cat.txt
$> getent passwd >getent.txt
$>diff -s cat.txt getent.txt # returns 'Files cat.txt and getent.txt are identical

Functionality of the getent

$> getent database [key …]
The getent program gathers entries from the specified administrative database using the specified search keys. Where database is one of passwd, group, hosts, services, protocols, or networks. In the exit, getent return 0 for success, 1 for Unknown database, 2 for Key not found in database, 3 for database does not support enumeration.

Character x

In /etc/passwd file, x character indicates that encrypted password is stored in /etc/shadow file.

Charlie

When we execute above commands on Charlie, we see difference between /etc/passwd file and the result of getent. When we just print /etc/passwd file, we can't see the info of the users, nobody, alice, dilbert, bob, wally. Moreover, there are some additional fields in the result of the getent. In /etc/passwd file, we see x in the second column but here we actually see encrypted passwords with salt. These difference comes from that getent gets the info of the users of LDAP service, too. However, other lines are identical.

/etc/nsswitch.conf

In alfa,

- passwd: compat
- shadow: compat
- group: compat

In charlie,

- passwd: files nis
- shadow: files nis
- group: files nis

Other lines are identical. These configuration forces charlie to use local files for databases while also requesting them from NIS(Network Information System) server. However, compat says local files must be used so alfa will use only local files and if databases exist, they are the only source of information.

stopped ypbind on Charlie

$> /etc/init.d/ypbind stop
When we stopped ypbind service, extra lines(alice, dilbert, etc.) are disappered. When we run diff on two results, diff now returns that files are identical.

ypbind server finding

The file /etc/yp.conf is read at startup or when receiving signal SIGHUP. The entries are used for the initial binding. Valid entries are:

- domain nisdomain server hostname
- domain nisdomain broadcast
- ypserver hostname

Therefore, we checked /etc/yp.conf file, and found this entry:

- domain example.com broadcast

As a result of this entry, client will use broadcast to find NIS server for the domain example.com. Moreover, we can also see the domain under /var/yp/binding/[domain_name].[version].
We can use ypwhich to learn to whom we bind by this command:

- ypwhich -d example.com # return 10.10.0.2 - alfa

So, server is alfa that has an IP address of 10.10.0.2.
There are three services that provides some functionalities for NIS, namely:

- ypserv - main NIS service
- yppasswdd - enable change of passwords from clients
- ypxfrd - map tranfer server

Therefore, at least ypserv must run by alfa, we check it by this command on alfa:
$> ps -ef | grep yp # return just ypserv, so the name of the service is ypserv

Joining Bravo

Bravo configuration

$> vzctl enter 1001 # enter into Bravo container
Firstly, we checked configuration file /etc/yp.conf and it was identical to the configuration of Charlie. So, domain is correct. Then, we checked nsswitch.conf for ypbind, passwd, shadow and group configuration were wrong

- passwd: compat → files nis
- shadow: compat → files nis
- group: compat → files nis

Finally, we checked ypbind if it is working, it was running so we tried getent and it worked.

New user phb

We added new user on alfa:
$> useradd phb
then we checked it on alfa by:
$> getent passwd phb
new user phb was created by no password credentials.

In Bravo, we can't see the new user. Since there is only one server, alfa is the master and master converts /etc/passwd, /etc/shadow, hosts, … files into NIS GNU dbm database format and generates a make file. Since we add new user, this database should be updated so we update it by this command:
$> make -C /var/yp
Then, we can new user on Bravo.

Why NIS sucks?

Password entries with lower UIDs (the root and system entries) aren't put into NIS password database, for security. MINUID is the lowest uid will be included in the password maps. If shadow maps is created, the UserID for a shadow entry is taken from passwd file. if no map is found, shadow entry is ignored and MINUID is set to 500.

- MINUID=500

Moreover, there is an option in the configuration file to merge passwd and shadow files:

- MERGE_PASSWD=true

Live password database is stored under domain directory, example.com/

- passwd.byname
- passwd.byuid

Since merge is true, the database files contain password hashes instead of just x.

Is it really insecure?

NIS used to have a major security flaw: it left your password file readable by virtually anyone in the entire Internet, which made for quite a number of possible intruders. As long as an intruder knew your NIS domain name and the address of your server, he could simply send it a request for the passwd.byname map and instantly receive all your system's encrypted passwords. With a fast password-cracking program like **crack** and a good dictionary, guessing at least a few of your users' passwords is rarely a problem.
Client get passwd file with this command:
$> ypcat -k passwd.byname # or passwd.byuid

Fix

We should add /var/yp/securenets file to limit the subnet the server(alfa) that service. For example for bravo:
> 255.255.255.255 127.0.0.1 # for server itself
> 255.255.255.255 10.10.0.3 # for bravo
Then we should restart the ypserv service to get advantage of securenets.
> /etc/init.d/ypserv restart

Spoofing and Initialization

This technique does not provide protection from an IP spoofing attack, but it does at least place limits on what networks the NIS server services.
Initializing a client by host name consists of explicitly identifying the IP address of its trusted server. Initializing by the host name method is more secure than the broadcast method because it specifies the IP address of the trusted server, rather than relying on a server to identify itself. However, if a router exists between the client and the trusted server, it can intercept messages to the trusted IP address and route the messages to an untrusted server.
> domain nisdomain server hostname

Thoughts on NIS

NIS is a good solution for maintenance and handling updates / changes of big systems but there are a lot of configuration steps that should be taken to make system really secure, even if necessary steps are taken, there are insecure points, so it is replaced by NIS+ or LDAP.

Yummy Passwords

- $ character is used to seperate id of hash algorithm, salt and encrypted hash.
- All information in /etc/login.defs with parameter ENCRYPT_METHOD
    - We can get id mappings of hash algorithms from
        - man 3 crypt
            - 1 → md5
            - 2a → Blowfish
            - 5 → SHA-256
            - 6 → SHA-512
    - In our case, id is 6 so passwords are encoded by SHA-512.
    - Moreover, with ENCRYPT_METHODSELECT, we can change the hash algorithm
- $> john -i=all password.db
    - We have found
        - bob:1234 # he is the silly user