SettingUpNISHowTo

This needs to be written. It needs to be *easy*

link: http://tldp.org/HOWTO/NIS-HOWTO/index.html

See also the HOWTO in the package.

My attempt at satisfying the above:

NIS Server Config

Matthew Caron

Note: This assumes your server and clients have static IP addresses. NIS with dynamic IP addresses present a serious security hazard. See the "Security" section, below, for a discussion of security problems inherent with NIS and how to avoid them.

1. (Warty only) Add any client name and IP addresses to /etc/hosts. The server's IP should already be here. I do not mean 127.0.0.1, I mean the real IP available to the world. This ensures that NIS will still work even if DNS goes down. You could rely on DNS if you wanted, it's up to you.

2. Add the following line to hosts.allow:

```
SRUWP DS NSVHUY NSELQG OLVW RI,3 DGGUHVVHV
```

Where the "list of IP addresses" string is, you need to make a list of IP addresses that consists of the server and all clients. These have to be IP addresses because of a limitation in portmap (it doesn't like hostnames).

3. Install NIS:

```
VXGR DSWJHW LQVWDOO SRUWP DS QLV
```

You will be asked for the name of your NIS domain. This can be anything; you're naming it. It just has to be the same domain for the server and all clients.

4. Edit /etc/default/portmap and comment out the ARGS="-i 127.0.0.1" line

5. Edit /etc/default/nis and set the NISSERVER line to NISSERVER = master

6. Edit /etc/yp.conf and add a server line of the form:

```
GRP DLQ[illegible]GRP DLQQDP H ! [illegible]VHUYHU[illegible]VHUYHUQDP H !
```

where <domainname> is the name of your domain (entered when you installed nis) and <servername> is the name of the server you're setting all this up on. (This lives in /etc/defaultdomain for the curious)

7. Edit /var/yp/Makefile and read the instructions. It probably won't need a lot of modification. The only thing I changed was the MINGID line so that the group memberships would be propagated across the domain. I set it to 1.

8. Edit /etc/ypserv.securenets and add lines to restrict access to domain members. I use lines for specific hosts, like:

```
KRVW[illegible]
KRVW[illegible]
HWF[illegible]
```

IMPORTANT!!!: comment out the 0.0.0.0 line. Otherwise, everyone gets access. (See "Security" below for discussion of why this is bad).

9. Build the DB for the first time, run:

```
VXGR[illegible]KVUDE[illegible]KS[illegible]KSQLW[illegible]P
```

and follow the instructions. This will probably throw some errors about not being able to talk to certain things. This is okay. (Other errors probably aren't).

10. Restart everything:

```
VXGR[illegible]HWF[illegible]QLW[illegible]G[illegible]SRUWP DS[illegible]UHVWDUW
VXGR[illegible]HWF[illegible]QLW[illegible]G[illegible]QLV[illegible]UHVWDUW
```

Note that I had some problems with portmap releasing the port which it was listening on and ended up having to reboot the machine for it to take effect. You can test it with `ypcat passwd`.

11. If you change anything (add a user, etc.), make sure to do:

```
VXGR[illegible]P DNH[illegible]&[illegible]YDU[illegible]S
```

Security: NIS is a dangerous thing. Anyone who can get access to the daemon can dump your password lists. If they can do that, then they have your passwords. It doesn't matter that the passwords are encrypted; they are plaintext equivalent (since authentication is done with encrypted passwords, you don't need to know the text password, you just need to write an app to provide the encrypted one to the authentication system correctly). So, let's make sure that doesn't happen. How? Well, first, we restrict access:

1. Only allow domain members to talk to the appropriate services in hosts.allow. This implied that hosts.deny is set to domething like ALL:ALL in order for this to work.

2. Limit who the server will respond to by putting domain members in /etc/securenets

3. (Alternatively?) To enable NIS password verification from non-priveledged processes the following line may need to be added (before others for shadow.byname) to /etc/ypserv.conf

<server ip> : * : shadow.byname : none

That will make shadow password info available to any process on the server so you may want limit logins accordingly.

3. Restrict the ports that the yp services run on by specifying what port each service should run on in /etc/default/nis.

```
# Additional options to be given to ypserv when it is started.
YPSERVARGS="-p [illegible]"

# Additional options to be given to ypbind when it is started.
YPBINDARGS="-p [illegible]"

# Additional options to be given to yppasswdd when it is started. Note
# that if -p is set then the YPPWDDIR above should be empty.
YPPASSWDDARGS="--port [illegible]"

# Additional options to be given to ypxfrd when it is started.
YPXFRDARGS="-p [illegible]"
```

For your firewall settings only allow your network (e.g. 192.168.0.0/24) access to the server

```
iptables -A INPUT -p ALL -s! [illegible] --dport [illegible] -j DROP
iptables -A INPUT -p ALL -s! [illegible] --dport [illegible] -j DROP
iptables -A INPUT -p ALL -s! [illegible] --dport [illegible] -j DROP
iptables -A INPUT -p ALL -s! [illegible] --dport [illegible] -j DROP
```

These ports are unassigned according to IANA. Credit should be given to the Redhat manual entry on NIS for this method of securing NIS.

So, now we have the access restricted to specific IP addresses, we're good, right? Well, not quite. What if someone were to punt one of your machines off the network, assume it's IP address and dump the password file? You're still dead.

Solution #1: IPSec. You can set up all your domain members to only talk to each other over IPSec which will effectively authenticate that your client is who it says it is. How? Well, it encrypts traffic to the server with the server's key, and the server sends back all replies encrypted with the client's key. The traffic is decrypted with the respective keys. So, if the client doesn't have the keys that the client is supposed to have, it can't send or receive data. Provided the file containing the keys is reasonably secret (only readable by root), you can't get the keys unless you compromise the client. And, if you compromise the client, you can dump the password list anyway, so the attacker has got you (which is a flaw in most domain authentication systems).

Solution #2: Private network. With 2 ethernet cards and a separate switch, all your domain members can connect via a private network. This avoids the overhead of IPSec, but requires more hardware and physical security - if someone can plug in to the network, then you have the same problem as described above.

NIS Client Config

Matthew Caron

A note about administration: Since the root user's account is disabled, make sure that whomever is to admin the machine is in the /etc/sudoers file on the client machine. It is also a good idea to have those users as local users on the client machine, with the **same UID** as is in the domain password list. It keeps things nice and consistent, and if there ever was a problem, you might need to have a local account to gain access to the machine.

1. Add server to /etc/hosts. This means that you can still find the server if there is a DNS failure.

2. Install the software you need

```
VXGR DSWJHW LQVWDOO SRUWPDS QLV
```

You will be asked for the name of your NIS domain. Enter the name of your NIS domain. If you entered wrongly or want to change the defaultdomain of NIS change it in the file /etc/defaultdomain

```
LRERWLFV
```

For example, robotics is the name of my NIS server. Remember this parameter is case sensitive. It is probably a good idea to then add a portmap line to /etc/hosts.allow for security reasons:

```
SRUWP DS▮▮▮ 1 ,6 VHUYHU,3 DGGUHVV!
```

Where "NIS server IP address" is the IP address of the NIS server.

3. Set up name services to use NIS:

Edit /etc/passwd to add a line at the end saying:

```
▮ ▮▮▮▮▮
```

Edit /etc/group to add a line at the end saying:

```
▮ ▮▮▮
```

Edit /etc/shadow to add a line at the end saying:

```
▮ ▮▮▮▮▮▮
```

This sets up those services to include NIS entries if a match isn't found in the file. You could change other services to use NIS by using the NIS service in /etc/nsswitch.conf, but these are the important ones.

4. Edit /etc/yp.conf and add the line:

```
\SVHUYHU▮▮ ▮ ▮ ▮▮ ▮ ▮▮ ▮ ▮▮ ▮
\SVHUYHU▮▮ ▮ ▮ ▮▮ ▮ ▮▮ ▮ ▮▮ ▮
```

Where 123.45.67.89 and 987.65.43.21 are the NIS servers.

5. Restart NIS:

```
▮HWF▮QLWG▮QLV▮UHVWDUW
```

Note: sshd will need to be restarted to use the new authentication system. Just an FYI.

Note: The above restart didn't work for me - I had to reboot the machine in order for it to work.

Note: A frequently asked question is how to give NIS users audio, DRI, video privileges. Simply add the user's group to video in file /etc/group

Alternatively, on the NIS Server, perform the following procedure:

- Add the relevant user account(s) to the audio group (group 29). In the example the user account is called 'user1' (uid=1000 and gid=1000) and is also added to additional groups that may be useful:

```
XVHUP RG [illegible] KVHU
```

- Edit the file /var/yp/Makefile and change the MINGID value (the original value is normally 1000):

```
0 ,1* ,' [illegible]
```

- Recreate the NIS maps:

```
P DNH [illegible] YDUNS
```

The full set of groups are now exported via NIS from the server, and can be verified by issuing the id command on the client:

```
[illegible] IG KVHU
XIG [illegible] KVHU [illegible] IUG [illegible] KVHU [illegible]
JURXSV [illegible] KVHU [illegible] GIDRXW [illegible] FGURP [illegible] IRSS\ [illegible] DXGIR [illegible] YLGHR [illegible] SOXJGHY [illegible] KVHUV
```

Sound will now work properly. Adjust the other groups to add or remove rights as necessary.

Note: I'm not an expert in NIS, so I'm reluctant to change the above instructions. However, to get things to work on a mixed Dapper (clients) and Breezy (server), I had to ignore Step 2 of the server instructions - this messed up Apache for me - and I had to manually edit /etc/defaultdomain on the client. This last step might be because I made an error earlier on, but I'm not sure where.

CategoryDocumentation CategoryCleanup

SettingUpNISHowTo (dernière édition le 2008-10-07 18:59:51 par https://login.launchpad.net/+id/kfTBFMn @ adsl-70-237-158-57.dsl.pltn13.sbcglobal.net[70.237.158.57]:kevin-cameron)