FreeNAS - Bug #28406

Do not grant extra privileges to users when a Directory Service is enabled

02/09/2018 04:56 AM - Andrew Walker

Status:	Done		
Priority:	No priority		
Assignee:	John Hixson		
Category:	OS		
Target version:	11.2-BETA2		
Seen in:	11.0-U6	**Needs Merging:**	No
Severity:	Med High	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	n/a
Reason for Blocked:		**Hardware Configuration:**	
Needs QA:	No	**ChangeLog Required:**	No
Needs Doc:	No		

Description

Customer system was hanging on boot because we were trying to grant "SeTakeOwnershipPrivilege", "SeBackupPrivilege", "SeRestorePrivilege" to all of the ldap users in the environment.

We should have an extra check for the server role so that we don't do this in environments where directory services are enabled. If they are required, perhaps we should grant them to a foreign group rather than every ldap user.

Related issues:

Copied to FreeNAS - Bug #40704: Do not grant extra privileges to users when a...	**Done**

History

#1 - 02/13/2018 04:56 AM - Andrew Walker

Here's a bit more of a background. This was observed on one of McGill's servers. Large LDAP environment and boot was hanging. Hitting <ctrl-c> once allowed boot to continue and resulted in the following:

```
Importing account for root...ok
Enabled user root.
Traceback (most recent call last):
File "/usr/local/libexec/nas/generate_smb4_conf.py", line 1655, in <module>
main()
File "/usr/local/libexec/nas/generate_smb4_conf.py", line 1644, in main
smb4_grant_rights()
File "/usr/local/libexec/nas/generate_smb4_conf.py", line 1437, in smb4_grant_rights
pdbedit_out = p.communicate()
File "/usr/local/lib/python2.7/subprocess.py", line 800, in communicate
return self._communicate(input)
File "/usr/local/lib/python2.7/subprocess.py", line 1417, in _communicate
stdout, stderr = self._communicate_with_poll(input)
File "/usr/local/lib/python2.7/subprocess.py", line 1471, in _communicate_with_poll
ready = poller.poll()
KeyboardInterrupt
Script /etc/ix.rc.d/ix-pre-samba interrupted
```

Disabling this function allows boot to proceed normally. This sounds hackish, but I think that we should be careful about assigning these rights since they may cause unexpected behavior / privilege escalation in a Windows environment.

For instance default rights are as follows:

```
root@SAMBADC:~ # net rpc rights list accounts --user=administrator
Enter administrator's password:
BUILTIN\Print Operators
```

```
SeLoadDriverPrivilege
SeShutdownPrivilege
SeInteractiveLogonRight

BUILTIN\Account Operators
SeInteractiveLogonRight

BUILTIN\Backup Operators
SeBackupPrivilege
SeRestorePrivilege
SeShutdownPrivilege
SeInteractiveLogonRight

BUILTIN\Administrators
SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeSystemtimePrivilege
SeShutdownPrivilege
SeRemoteShutdownPrivilege
SeTakeOwnershipPrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeProfileSingleProcessPrivilege
SeIncreaseBasePriorityPrivilege
SeLoadDriverPrivilege
SeCreatePagefilePrivilege
SeIncreaseQuotaPrivilege
SeChangeNotifyPrivilege
SeUndockPrivilege
SeManageVolumePrivilege
SeImpersonatePrivilege
SeCreateGlobalPrivilege
SeEnableDelegationPrivilege
SeInteractiveLogonRight
SeNetworkLogonRight
SeRemoteInteractiveLogonRight

BUILTIN\Server Operators
SeBackupPrivilege
SeSystemtimePrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeShutdownPrivilege
SeInteractiveLogonRight

BUILTIN\Pre-Windows 2000 Compatible Access
SeRemoteInteractiveLogonRight
SeChangeNotifyPrivilege
```

#2 - 02/13/2018 08:23 AM - Ben Gadd

- FreeNAS

- Target version changed from N/A to 11.1-U2

#3 - 02/13/2018 08:25 AM - Ben Gadd

- Assignee changed from Ash Gokhale to John Hixson

#4 - 02/13/2018 08:34 AM - Ben Gadd

- Target version changed from 11.1-U2 to TrueNAS 11.2

#5 - 02/14/2018 05:51 PM - Ben Gadd

- Subject changed from Samba - don't grant privileges to users when role = member to Samba - do not grant privileges to users when role = member

- Category set to OS

#6 - 02/15/2018 07:13 AM - John Hixson

Other than this affecting mcgill, what is the problem with this? I think removing this is a bad idea. Making it configurable is okay, but I disagree with removing it. It should be default behavior.

#7 - 02/20/2018 02:20 PM - Andrew Walker

John Hixson wrote:

> Other than this affecting mcgill, what is the problem with this? I think removing this is a bad idea. Making it configurable is okay, but I disagree with removing it. It should be default behavior.

The main problem is that once users have setakeownership privilege they can take ownership of a file regardless of the file's ACL. Once they have taken ownership of the file, they become superuser as to that file and can rewrite its ACL as they desire.

Honestly, those rights shouldn't be granted by default. It effectively breaks ACLs. I didn't think through the full implications of these rights until this weekend and confirmed that I can change permissions as an unprivileged user today.

#9 - 03/01/2018 05:38 PM - Andrew Walker

Dropped original PR and made a more specific one to stop granting these rights. https://github.com/freenas/freenas/pull/931

#10 - 03/01/2018 05:39 PM - Andrew Walker

- Subject changed from Samba - do not grant privileges to users when role = member to Samba - do not grant extra privileges to users

#11 - 03/20/2018 08:20 AM - Dru Lavigne

- FreeNAS

- Project changed from TrueNAS to FreeNAS

- Category changed from OS to OS

- Target version changed from TrueNAS 11.2 to 11.2-RC2

- Migration Needed deleted (No)

- Hide from ChangeLog deleted (No)

- Support Department Priority deleted (0)

#12 - 03/28/2018 11:16 PM - John Hixson

- Assignee changed from John Hixson to Timur Bakeyev

#13 - 04/16/2018 02:15 PM - Nick Wolff

- Severity set to Med High

#14 - 06/13/2018 08:53 AM - John Hixson

- Assignee changed from Timur Bakeyev to John Hixson

- Target version changed from 11.2-RC2 to Backlog

#15 - 07/11/2018 12:49 PM - John Hixson

- Status changed from Not Started to Ready for Testing

Merged https://github.com/freenas/freenas/pull/1262

#16 - 07/11/2018 09:56 PM - Dru Lavigne

- Subject changed from Samba - do not grant extra privileges to users to Do not grant extra privileges to users when a Directory Service is enabled

- Target version changed from Backlog to 11.2-BETA2

- Needs Doc changed from Yes to No

- Needs Merging changed from Yes to No

#17 - 07/30/2018 10:10 AM - Rishabh Chauhan

FreeNAS-11.2-MASTER-201807300838
As directed by A Walker...
Step1: binding my machine to

1. **LDAP01 (NO SSL, anonymous bind enabled)**
   Hostname: ldap01.tn.ixsystems.com (NO SSL, anonymous bind enabled)
   Base DN: dc=ldap01,dc=tn,dc=ixsystems,dc=com
   Bind DN: cn=admin,dc=ldap01,dc=tn,dc=ixsystems,dc=com
   Bind password: OpenSource123!
   source: https://docs.ixsystems.com/qa-directory-servers

Step2: Turn on Samba

Step3:
@tdbdump /var/db/samba4/account_policy.tdb {
key(51) = "PRIV_S-1-5-21-3930969452-860074701-1042548808-3002\00"
data(8) = "\00\0E\00\00\00\00\00\00"
} {
key(21) = "minimum password age\00"
data(4) = "\00\00\00\00"
} {
key(31) = "refuse machine password change\00"
data(4) = "\00\00\00\00"
} {
key(20) = "reset count minutes\00"
data(4) = "\1E\00\00\00"
} {
key(18) = "PRIV_S-1-5-32-550\00"
data(8) = "\00\00\00\00\00\00\00\00"
} {
key(18) = "PRIV_S-1-5-32-548\00"
data(8) = "\00\00\00\00\00\00\00\00"
} {
key(18) = "PRIV_S-1-5-32-551\00"
data(8) = "\00\00\00\00\00\00\00\00"
} {
key(18) = "PRIV_S-1-5-32-549\00"

```
data(8) = "\00\00\00\00\00\00\00\00"
} {
key(16) = "disconnect time\00"
data(4) = "\FF\FF\FF\FF"
} {
key(35) = "user must logon to change password\00"
data(4) = "\00\00\00\00"
} {
key(17) = "password history\00"
data(4) = "\00\00\00\00"
} {
key(51) = "PRIV_S-1-5-21-3930969452-860074701-1042548808-3000\00"
data(8) = "\00\0E\00\00\00\00\00\00"
} {
key(17) = "lockout duration\00"
data(4) = "\1E\00\00\00"
} {
key(20) = "min password length\00"
data(4) = "\05\00\00\00"
} {
key(51) = "PRIV_S-1-5-21-3930969452-860074701-1042548808-3004\00"
data(8) = "\00\0E\00\00\00\00\00\00"
} {
key(18) = "PRIV_S-1-5-32-544\00"
data(8) = "\F0\FF\FF\1F\00\00\00\00"
} {
key(13) = "PRIV_S-1-1-0\00"
data(8) = "\00\00\00\00\00\00\00\00"
} {
key(21) = "maximum password age\00"
data(4) = "\FF\FF\FF\FF"
} {
key(20) = "bad lockout attempt\00"
data(4) = "\00\00\00\00"
} {
key(13) = "INFO/version\00"
data(4) = "\03\00\00\00"
}
@
```

Step 5: pdbedit -Lv
No output

#18 - 07/30/2018 11:43 AM - Rishabh Chauhan

- Status changed from Ready for Testing to Passed Testing

- Needs QA changed from Yes to No

After a thorough investigation with Andrew, we think that the patch works!

#19 - 07/30/2018 11:47 AM - Dru Lavigne

- Status changed from Passed Testing to Done

#20 - 08/03/2018 11:51 AM - John Hixson

- Copied to Bug #40704: Do not grant extra privileges to users when a Directory Service is enabled added