

# Securing Netscape Directory Server ( last update 23-09-2001 )

By Sacha Faust : <mailto:sacha@severus.org>

## Introduction

This article will focus only on the Microsoft Windows NT 4.0 version of the Netscape Directory Server 4.13. It will focus on the operating system and the application security. This article does'nt talk about the communication security and if the code is secured from exploits ( buffer overflow and format bug ).

The environment used for this article was the following:

- o Operating System : Microsoft Windows NT 4.0 service pack 6
- o LDAP Server : Netscape Directory Server 4.13 for NT 4.0
- o Server Name : Wazzup
- o Server Domain : captkirk.com
- o Directory Server configuration
  - Root dn : cn=Directory Manager
  - Root password : 123456789
- o Directory Administration server configuration
  - Administrator user : admin
  - Administrator user password : 123456789
  - Server port : 13597

A lot of structure of the directory server is reliant on the server name and domain name so when examples or solutions are shown your need to replace those name with the one you are using.

## OS Security ( Microsoft Windows NT 4.0 )

Netscape Directory Server install itself on NT with no real security. Every read and modified by the Everyone group. Every configuration and data files are in clear text, this makes it very easy for a attacker or a user that as access to the system to completely steal the directory data and, run arbitrary code and gain higher privilege on the operating system.

### **Dangerous Files**

Every files that it installed should have the Everyone group removed . Here are a few files that need to be monitored and can cause serious security risk for the operating system and the directory server.

## Files

C:\Netscape\Server4\start-admin.cmd  
C:\Netscape\Server4\startconsole.exe  
C:\Netscape\Server4\stop-admin.cmd

## Permissions

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

## Risk

- These files are used to start/stop the directory server service and to load the main management console.
- Anyone can modify the code and make it run on the system with the privilege of the user that execute the code. These files are often executed by high privilege users

## Fix

- Remove the Everyone Group from the ACL
- A alternative is to set the Authenticated Users group and only allow them the execute permission so they are unable to change the code that will be run

## File

C:\Netscape\Server4\admin-serv\config\adm.conf

## Permissions

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

## Risk

- This file contain the Directory Administration server administrator password in clear text in the siepid field
- This file is world readable by default and anyone can use this information to automatically gain administrator access to the directory server. This can be use to gain system privilege by using the directory server behavior ( load perl , java, ... as SYSTEM ).

Example :

```
C:\Netscape\Server4\admin-serv\config>type adm.conf
```

*ldapStart: slapd-wazzup/start-slapd*

*ldapHost: wazzup.captkirk.com*

*ldapPort: 389*

*SIE: cn=admin-serv-wazzup, cn=Netscape Administration Server, cn=Server Group, cn=wazzup.captkirk.com, ou=captkirk.com, o=NetscapeRoot*

**siepid: 123456789**

*ISIE: cn=Netscape Administration Server, cn=Server Group, cn=wazzup.captkirk.com, ou=captkirk.com, o=NetscapeRoot*

*host: wazzup.captkirk.com*

*port: 13597*

*C:\Netscape\Server4\admin-serv\config>*

### Fix

- Remove the Everyone Group from the ACL
- Monitor the access to this file by any users or group

### File

*C:\Netscape\Server4\admin-serv\config\local.conf*

### Permissions

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

### Risk

- This is a configuration file for the Administration Console. This file contains many valuable information on the Administration service and can be modify by anyone on the system by default
- This configuration file contains information on the encrypted user password in clear text. This password can be pass to a password cracker. ( see Useful Tool section )
- This file contains java class to load and could be used to load malicious code, modify host allowed to connect, ...
- This file contains mapping to the administration tools. A malicious user could change the mapping and make the server point to arbitrary code.

Example :

*C:\Netscape\Server4\admin-serv\config>type local.conf*

*nsserverid: admin-serv*

**userpassword: {SHA}98O8HYCOBHMq32eZZczDTKeuNEE=**

<more data ...>

configuration.nsadminaccesshosts: \*.captkirk.com

configuration.nsadminaccessaddresses: \*

<more data ...>

configuration.nsclassname:

com.netscape.management.admserv.AdminServer@admserv42.jar@cn=admin-serv-wazzup, cn=Netscape Administration Server, cn=Server Group, cn=wazzup.captkirk.com, ou=captkirk.com, o=NetscapeRoot

<more data ...>

Tasks.Operation.Stop.nsexecref: stopsrv

Tasks.Operation.Stop.nsclassname:

com.netscape.management.admserv.task.Stop@admserv42.jar@cn=admin-serv-wazzup, cn=Netscape Administration Server, cn=Server Group, cn=wazzup.captkirk.com, ou=captkir

k.com, o=NetscapeRoot

Tasks.Operation.Restart.nshelpref: admin/restartadm.html

Tasks.Operation.Restart.nsexecref: restartsrv

Tasks.Operation.Restart.nsclassname:

com.netscape.management.admserv.task.Restart@admserv42.jar@cn=admin-serv-wazzup, cn=Netscape Administration Server, cn=Server Group, cn=wazzup.captkirk.com, ou=c

aptkirk.com, o=NetscapeRoot

<more data ...>

C:\Netscape\Server4\admin-serv\config>

## Fix

- o Remove the Everyone group. No one should have to edit this file manually in normal production conditions

## Files

C:\Netscape\Server4\admin-serv\config\admpw

## Permissions

User/Group	Owner	DACL
Administrators	X	All
Every one		RWXD
SYSTEM		All

### Risk

- This file contains the username and encrypted password to access the Administration service.
- Everyone can read or modify the file. This information can be pass to a password cracker to crack or a new encrypted password can be manually added to gain access to Directory Administration server. ( see Useful Tool section )

Example:

```
C:\Netscape\Server4\admin-serv\config>type admpw
admin:98O8HYCOBHMq32eZZczDTKeuNEE=
C:\Netscape\Server4\admin-serv\config>
```

### Fix

- Remove the Everyone group from the ACL
- Monitor access to this file by any users or groups

### Files

C:\Netscape\Server4\admin-serv\logs\access  
C:\Netscape\Server4\admin-serv\logs\error

### Permissions

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

### Risk

- By default, anyone on the system can modify the Administration service log files
- A intruder can erase is intrusion attacks on the Administration service

### Fix

- Remove the Everyone group from the ACL
- Monitor access to this file by any users or groups

### Folder/Files

C:\Netscape\Server4\bin\base\jre

## Permissions

User/Group	Owner	Permissions	
		Directory	Files
Administrators	x	all	all
Everyone		RWXD	RWXD
CREATOR OWNER			all
SYSTEM		All	all

## Risk

- This folder contains the Java Runtime Environment (JRE) that is used by the Directory server.
- Everyone as execute permission so anyone can use the JRE to run java code. This might brake the system policy you have for your user.
- Everyone as execute and write permission on the folder and files so anyone can modify or add code on the system. Since there is a high risk of this code being run by a high privilege rights this is very dangerous

## Fix

- Remove the Everyone group from the ACL
- If various users need to use the JRE, create a specific group for them and only allow them the execute permission and remove write permission.

## Files

C:\Netscape\Server4\bin\slapd\admin\bin\Cgi.pm  
C:\Netscape\Server4\bin\slapd\admin\bin\getConfigInfo  
C:\Netscape\Server4\bin\slapd\admin\bin\migratedsgw  
C:\Netscape\Server4\bin\slapd\admin\bin\migrateInstance  
C:\Netscape\Server4\bin\slapd\admin\bin\migrateLocalDB  
C:\Netscape\Server4\bin\slapd\admin\bin\migratePwdFile  
C:\Netscape\Server4\bin\slapd\admin\bin\migrateTo4  
C:\Netscape\Server4\bin\slapd\admin\bin\uname.lib  
C:\Netscape\Server4\bin\slapd\admin\bin\updatedsgw

## Permissions

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

## Risk

- These are all Perl scripts or modules files and can be modified by everyone.
- These scripts are executed when the Directory server administrator is running maintenance options in the Administration console and are executed as SYSTEM

## Fix

- Remove the Everyone group from the ACL
- If some users need to modify these files, make sure they can be trusted (remember that they are executed as SYSTEM) and monitor the changes. For most systems, no one should have to modify these.

## Files

C:\Netscape\Server4\install\perl.exe

## Permissions

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

## Risk

- This is a perl interpreter. By default, everyone can run perl code by calling this executable. This might brake the system policy you have for your users.
- Anyone can overwrite this file with anything by default. The perl interpreter is often used by the Directory server and Administration server to execute maintenance scripts. These scripts are often executed with SYSTEM privilege.

Example :

```
C:\Netscape\Server4\install>perl -v
```

*This is perl, version 5.005\_02 built for MSWin32-x86*

*Copyright 1987-1998, Larry Wall*

*Perl may be copied only under the terms of either the Artistic License or the GNU General Public License, which may be found in the Perl 5.0 source kit.*

*Complete documentation for Perl, including FAQ lists, should be found on this system using `man perl' or `perldoc perl'. If you have access to the Internet, point your browser at <http://www.perl.com/>, the Perl Home Page.*

### **Fix**

- Remove the Everyone group from the ACL.
- If some users need to use this Perl interpreter, limit the access to it and remove the write permission so they can't overwrite the executable.

### **Files**

C:\Netscape\Server4\java\base.jar  
C:\Netscape\Server4\java\ldapjdk.jar  
C:\Netscape\Server4\java\mcc42.jar  
C:\Netscape\Server4\java\mcc42\_en.jar  
C:\Netscape\Server4\java\nmclf42.jar  
C:\Netscape\Server4\java\nmclf42\_en.jar  
C:\Netscape\Server4\java\ssl.zip  
C:\Netscape\Server4\java\swingall.jar  
C:\Netscape\Server4\java\jars\admserv42.jar  
C:\Netscape\Server4\java\jars\admserv42\_en.jar  
C:\Netscape\Server4\java\jars\ds41.jar  
C:\Netscape\Server4\java\jars\ds41\_en.jar

### **Permissions**

<b>User/Group</b>	<b>Owner</b>	<b>DACL</b>
Administrators	X	All
Everyone		RWXD
SYSTEM		All

**Risk**

- These files are the core code files for the Directory and Administration server. Since everyone can change permissions on them, they are at high risk of modification and injection of malicious code.
- Someone could de-compile the code with a Java de-compiler and inject malicious arbitrary code and repackage it and overwrite the file. Once the code is injected, every time the system would use the file, the malicious code would be executed. ( see Useful Tool section )

**Fix**

- Remove the Everyone group from the ACL.

**Files**

C:\Netscape\Server4\shared\bin\admin\_ip.pl  
C:\Netscape\Server4\shared\bin\ldapcmp.exe  
C:\Netscape\Server4\shared\bin\ldapdelete.exe  
C:\Netscape\Server4\shared\bin\ldapmodify.exe  
C:\Netscape\Server4\shared\bin\ldapsearch.exe  
C:\Netscape\Server4\shared\bin\modutil.exe  
C:\Netscape\Server4\shared\bin\NativeToAscii.exe

**Permissions**

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

**Risk**

- These files are used for internal and external server management. Anyone can change these files to run malicious code by overwriting the file with a new one with arbitrary code.

**Fix**

- Remove the everyone group from the ACL

## Folder

C:\Netscape\Server4\slapd-wazzup\bak

## Permissions

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

## Risk

- This folder contains all the directory server backups. Everyone can read and modify this data.

## Fix

- It is mandatory to remove the Everyone group from this folder and monitor the access to this folder.
- A good thing would be to store the backups in a external device so they don't lay around the file system

## Files

C:\Netscape\Server4\slapd-wazzup \conf\_bk\slapd.conf

## Permissions

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

## Risk

- This file is a backup file for the directory server configuration.
- This file contains valuable information on the server configuration including the root dn username and password in the rootdn and rootpw fields. That information can be pass to a password cracker to get the it. ( see Useful Tool section )

Example :

```
from C:\Netscape\Server4\slapd-wazzup\conf_bk\slapd.conf
< ... >
rootdn "cn=Directory Manager"
rootpw {SHA}9808HYCOBHMq32eZZczDTKeuNEE=
< ... >
```

### Fix

- Remove the Everyone group from the ACL

### Files

C:\Netscape\Server4\slapd-<server name>\config\slapd.conf

### Permissions

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

### Risk

- This file is the directory server configuration. This file contains valuable information on the server configuration including the root dn username and password in the rootdn and rootpw fields These can be pass to a password cracker. ( see Useful Tool section )
- Since everyone as write permission, anyone can change the rootdn password and access the directory server with full control

Example :

```
from C:\Netscape\Server4\slapd-wazzup\conf_bk\slapd.conf
< ... >
rootdn "cn=Directory Manager"
rootpw {SHA}9808HYCOBHMq32eZZczDTKeuNEE=
< ... >
```

### Fix

- Remove the Everyone group from the ACL
- Monitor any access to this file

**Files**

C:\Netscape\Server4\slapd-<server name>\db

**Permissions**

User/Group	Owner	Permissions	
		Directory	Files
Administrators	x	all	all
Everyone		RWXD	RWXD
CREATOR OWNER			all
SYSTEM		All	all

**Risk**

- This folder contains all the directory server data and is world readable by default. Anyone can bypass the server security by directly reading the data
- Anyone as write permission on the server data and can damage or overwrite it.

**Fix**

- Remove the Everyone group from the ACL

**Files**

C:\Netscape\Server4\slapd-<server name>\logs

**Permissions**

User/Group	Owner	Permissions	
		Directory	Files
Administrators	x	all	all
Everyone		RWXD	RWXD
CREATOR OWNER			all
SYSTEM		All	all

**Risk**

- By default, anyone on the system can modify the Directory service log files
- An intruder can erase intrusion attacks on the Directory service

**Fix**

- Remove the Everyone group from the ACL
- Monitor access to this file by any users or groups

**Files**

C:\Netscape\Server4\slapd-<server name>\bak2db.bat  
C:\Netscape\Server4\slapd-<server name>\db2bak.bat  
C:\Netscape\Server4\slapd-<server name>\db2ldif.bat  
C:\Netscape\Server4\slapd-<server name>\getconf.bat  
C:\Netscape\Server4\slapd-<server name>\getpwenc.bat  
C:\Netscape\Server4\slapd-<server name>\ldif2db.bat  
C:\Netscape\Server4\slapd-<server name>\ldif2ldap.bat  
C:\Netscape\Server4\slapd-<server name>\monitor.bat  
C:\Netscape\Server4\slapd-<server name>\restart-slapd.bat  
C:\Netscape\Server4\slapd-<server name>\restoreconfig.bat  
C:\Netscape\Server4\slapd-<server name>\saveconfig.bat  
C:\Netscape\Server4\slapd-<server name>\start-slapd.bat  
C:\Netscape\Server4\slapd-<server name>\stop-slapd.bat  
C:\Netscape\Server4\slapd-<server name>\vlvindex.bat

**Permissions**

User/Group	Owner	DACL
Administrators	X	All
Everyone		RWXD
SYSTEM		All

**Risk**

- These files are used for server management and anyone can add arbitrary code to them. These files are runs under SYSTEM or high privilege access.

**Fix**

- Remove the Everyone group from the ACL

**Dangerous Registry**

Every registry keys that it installed should have the Everyone group removed . Here are a few registry keys that need to be monitored and could cause serious security risk for the operating system and the directory server.

**Registry Key ACL Synthax**

Q: Query Value

S: Set Value

C: Create Subkey

E: Enumerate Subkeys

N: Notify

D: Delete

R: Read Control

**Registry Key**

HKEY\_LOCAL\_MACHINE\SOFTWARE\Netscape\Administration\4.2

**Permissions**

User/Group	Owner	Permissions	
		Key	Inheritance
Administrators	x	all	All
Everyone		QSCEN D R	QSCEN D R
CREATOR OWNER			All
SYSTEM		All	All

**Data**

"RootPath"="C:\\Netscape\\Server4"

**Risk**

- This registry key hold the binding for the Directory Server root directory.
- Anyone on the system can change or remove the value. This could enable a malicious user to load arbitrary code if a user change the mapping.

**Solution**

- Remove the Everyone group.

**Registry Key**

HKEY\_LOCAL\_MACHINE\SOFTWARE\Netscape\Administration\4.2\admin42-serv

**Permissions**

User/Group	Owner	Permissions	
		Key	Inheritance
Administrators	x	All	All
Everyone		QSCEN D R	QSCEN D R
CREATOR OWNER			All
SYSTEM		All	All

**Data**

"ConfigurationPath"="C:/Netscape/Server4/admin-serv/config"

**Risk**

- This registry key hold the binding for the Directory Server Administration configuration path
- Anyone one the system can change or remove the value. This could enable a malicious user to load a dangerous configuration file.

**Solution**

- Remove the Everyone group
- Monitor the access to this registry key

**Registry Key**

HKEY\_LOCAL\_MACHINE\SOFTWARE\Netscape\Directory\4.1\slapd-<server name>  
(ie : HKEY\_LOCAL\_MACHINE\SOFTWARE\Netscape\Directory\4.1\slapd-wazzup )

## Permissions

User/Group	Owner	Permissions	
		Key	Inheritance
Administrators	x	all	all
Everyone		QSCEN D R	QSCEN D R
CREATOR OWNER			all
SYSTEM		All	all

## Data

"ConfigurationPath"="C:\\Netscape\\Server4\\slapd-wazzup\\config"

## Risk

- This registry key hold the binding for the Directory Server configuration path
- Anyone one the system can change or remove the value. This could enable a malicious user to load a dangerous configuration file.

## Solution

- Remove the Everyone group
- Monitor the access to this registry key

## Registry Key

HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Netscape\\Directory\\4.1\\SNMP\\CurrentVersion

## Permissions

User/Group	Owner	Permissions	
		Directory	Files
Administrators	x	All	all
Everyone		QSCEN D R	QSCEN D R
CREATOR OWNER			all
SYSTEM		All	all

## Data

Pathname"="C:\\Netscape\\Server4\\bin\\slapd\\server\\ns-ldapagt.dll

## Risk

- This registry key hold the binding for the Directory server SNMP dll
- Anyone one the system can change or remove the value. This could enable a malicious user to load a dangerous dll file.

## Solution

- Remove the Everyone group
- Monitor the access to this registry key

## Application Security

Netscape Directory Server implements access control instructions in a proprietary format. For more information on Netscape Directory server ACL syntax please consult <http://docs.ipplanet.com/docs/manuals/directory/41/admin/acl.htm#1013769>

### Default Netscape Directory server ACL

Here are the ACL for a default installation of Netscape Directory server. This was collected using NetscapeGetACL tool ( see Useful Tool section )

#### **ACL for context [o=captkirk.com]**

```
dn:o=captkirk.com :
    (targetattr = "**")(version 3.0; acl "Allow self entry modification"; allow
(write)userdn = "ldap:///self";)
    (targetattr != "userPassword") (version 3.0; acl "Anonymous access"; allow (read,
search, compare)userdn = "ldap:///anyone";)
    (targetattr = "**")(version 3.0; acl "Configuration Administrator"; allow (all) userdn =
"ldap:///uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot");)
    (targetattr = "**")(version 3.0;acl "Configuration Administrators Group";allow (all)
(groupdn = "ldap:///cn=Configuration Administrators, ou=Groups, ou=TopologyManagement,
o=NetscapeRoot");)
    (targetattr = "**")(version 3.0;acl "Directory Administrators Group";allow (all)
(groupdn = "ldap:///ou=Directory Administrators, o=captkirk.com");)
    (targetattr = "**")(version 3.0; acl "SIE Group"; allow (all)groupdn =
"ldap:///cn=slapd-wazzup, cn=Netscape Directory Server, cn=Server Group,
cn=wazzup.captkirk.com, ou=captkirk.com, o=NetscapeRoot");)
dn:ou=People, o=captkirk.com :
    (targetattr = "userpassword || telephonenumber ||
facsimiletelephonenumber")(version 3.0;acl "Allow self entry modification";allow (write)(userdn
= "ldap:///self");)
    (targetattr != "cn || sn || uid")(targetfilter = "(ou=Accounting)")(version 3.0;acl
"Accounting Managers Group Permissions";allow (write)(groupdn = "ldap:///cn=Accounting
Managers,ou=groups,o=captkirk.com");)
    (targetattr != "cn || sn || uid")(targetfilter = "(ou=Human Resources)")(version
3.0;acl "HR Group Permissions";allow (write)(groupdn = "ldap:///cn=HR
Managers,ou=groups,o=captkirk.com");)
```

```
(targetattr != "cn || sn || uid")(targetfilter = "(ou=Product Testing)")(version 3.0;acl "QA Group Permissions";allow (write)(groupdn = "ldap:///cn=QA Managers,ou=groups,o=captkirk.com");)
```

```
(targetattr != "cn || sn || uid")(targetfilter = "(ou=Product Development)")(version 3.0;acl "Engineering Group Permissions";allow (write)(groupdn = "ldap:///cn=PD Managers,ou=groups,o=captkirk.com");)
```

### **ACL for context [o=NetscapeRoot]**

dn:o=NetscapeRoot :

```
(targetattr="*)(version 3.0; acl "Enable Configuration Administrator Group modification"; allow (all) groupdn = "ldap:///cn=Configuration Administrators, ou=Groups, ou=TopologyManagement, o=NetscapeRoot");)
```

```
(targetattr="*)(targetfilter=(o=NetscapeRoot))(version 3.0; acl "Default anonymous access"; allow (read, search) userdn="ldap:///anyone");)
```

```
(targetattr="*)(version 3.0; acl "Enable Group Expansion"; allow (read, search, compare) groupdnattr="uniquemember");)
```

dn:ou=TopologyManagement, o=NetscapeRoot :

```
(targetattr!=userpassword)(version 3.0; acl "Default anonymous access"; allow (read,search) userdn="ldap:///anyone");)
```

dn:ou=captkirk.com, o=NetscapeRoot :

```
(targetattr=*)(targetfilter=(ou=captkirk.com))(version 3.0; acl "Enable anonymous access"; allow(read,search) userdn="ldap:///anyone");)
```

dn:ou=Global Preferences, ou=captkirk.com, o=NetscapeRoot :

```
(targetattr=*)(version 3.0; acl "Enable anonymous access"; allow(read,search) userdn="ldap:///anyone");)
```

### **Dangerous ACI**

#### **DN : o=captkirk.com**

##### **ACI**

```
(targetattr = "*)(version 3.0; acl "Allow self entry modification"; allow (write)userdn = "ldap:///self";)
```

##### **Risk**

This allow a user to modify all its attributes. This can be very dangerous if some of the user attributes are used to change behavior of certain environment or system ( ie: single signon )

##### **Solution**

This ACI should be removed. This kind of access will be taken care of in the ou=People, o=captkirk.com.

## ACI

```
(targetattr != "userPassword") (version 3.0; aci "Anonymous access"; allow (read, search, compare)userdn = "ldap:///anyone");
```

## Risk

This ACI allow anyone to read , search and compare any attribute inside the o=captkirk.com except for the userPassword attribute.

Anyone can get a listing of users and any other information in the directory server. A good example of the impact of this rule, is to run Ldapminer without providing a binddn and password againts a default install of Netscape Directory server and see the information it is able collect.

## Solution

This ACI should be remove. This can of access will be taken care of in the ou=People, o=captkirk.com.

## DN : ou=People, o=captkirk.com

This entry is used to store the directory server users

Most of the ACI here are for default groups in the directory server. You should analyze if you will be using the default groups and then rewrite the ACI to restrict access to the data base what each group need to access. A good thing when using multiple servers that need to access the directory is to create groups based on the purpose of each server and only allow access to the information that the server need. This way, if 1 of your server is compromised and starts trying to access information is it not suppose to need, you will know something is wrong in the log and the attacker will not have access to the entire data.

## DN: o=NetscapeRoot

This entry is used for the Directory and Administration server configuration

## ACI

```
(targetattr="*)(targetfilter=(o=NetscapeRoot))(version 3.0; aci "Default anonymous access"; allow (read, search) userdn="ldap:///anyone");
```

## Risk

This ACI permits anyone to read configuration information on the directory server. For a good example on the kind of information available with this ACI, run LdapMiner againts a Netscape Directory server with this ACI.

## Solution

This ACI should be removed

## **DN: ou=TopologyManagement, o=NetscapeRoot**

### **ACI**

```
(targetattr!=userpassword)(version 3.0; acl "Default anonymous access"; allow (read,search)
  userdn="ldap:///anyone");
```

### **Risk**

This aci allows anyone to read and search information from ou=TopologyManagement, o=NetscapeRoot . This allow access to information like who as access to the Administration service . This can be use to build more precise attacks on the server.

### **Solution**

- This ACI should be removed
- If access to this information is needed, you should only enable the Configuration Administrators group.

### **Example**

Limiting access to the administrators of the Configuration Administrators

```
(targetattr!=userpassword)(version 3.0; acl "us access"; allow (read,search)
  groupdn="ldap:///cn=Configuration Administrators, ou=Groups, ou=TopologyManagement,
  o=NetscapeRoot");
```

## **DN: ou=captkirk.com, o=NetscapeRoot**

### **ACI**

```
(targetattr=*)(targetfilter=(ou=captkirk.com))(version 3.0; acl "Enable anonymous access";
  allow(read,search) userdn="ldap:///anyone");
```

### **Risk**

- This ACI allow read and search access to the data when the query includes ou=captkirk.com .
- This allow anyone to have information on the data under ou=captkirk.com, o=NetscapeRoot

### **Solution**

Not allot of information can be viewed by default but it's a good thing to remove this ACI.

## **DN: ou=Global Preferences, ou=captkirk.com, o=NetscapeRoot**

### **ACI**

```
(targetattr=*)(version 3.0; acl "Enable anonymous access"; allow(read,search)
  userdn="ldap:///anyone";)
```

### **Risk**

- This ACI allow read and search access to the data under ou=Global Preferences, ou=captkirk.com, o=NetscapeRoot .
- Anyone as access to the Directory and Administration server configuration data. This can help a attacker gain more knowledge about the configuration of the server and can help him create more precise attacks. A good example of the kind of information available with this ACI is to run LDAPMiner on a server with this ACI enabled and look at the data the tool can collect.

### **Solution**

The information contained in ou=Global Preferences, ou=captkirk.com, o=NetscapeRoot might be used for other software using directory server ( Netscape Messaging Server, .... ). If you don't intent to plug other applications to this server, you can remove the ACI or you can create a specific group where you include the other server that need to communicate to your server and add them in the ACI instead of letting everyone.

### **Example**

After creating a group in ou=Groups, o=captkirk.com to group servers that need configuration information from the server, ( ie : cn=LinkedServers, ou=Groups, o= captkirk.com ) you can create this ACI to limit the access to this group

```
(targetattr=*)(version 3.0; acl "Enable linked servers"; allow(read,search)
  userdn="ldap:///n=LinkedServers,ou=Groups,o= captkirk.com " ;)
```

## **Dangerous ACI attributes for single signon**

LDAP servers are very usefull to store users to create a single signon solution for a hybrid network. When using Netscape Directory server as a repository of users so other system can replicate or access the information for authentication purpose, a few things as to be considered. Here is 2 example samples of things to consider when using the Directory server for NT authentication , PAM LDAP.

### **NT Authentication using Netscape Directory Server**

To enable NT authentication using Netscape Directory Server, the server replicate is user and group information to the a NT system that as authentication authority for the network ( PDC or standalone server ). The information is replicated to the server by using the Netscape NT Sync service that receive and fetch information on the directory server. To do this, a special objectclass as to be added to the user called ntUser.

### **Risk**

This object class includes a few attributes that specify specific NT user information. Letting the user change is Nt information can create serious security problem because the user information will be automatically replicated to the NT SAM ( username, home directory, group, ... ). A list of specific attributes is available at

[http://docs.iplanet.com/docs/manuals/directory/schema/oc\\_dir47.htm - 1301640](http://docs.iplanet.com/docs/manuals/directory/schema/oc_dir47.htm - 1301640)

### **Solution**

A simple modification of the ACI allowing a user to change is information can be done to make sure the user is unable to modify is NT information and control is NT user creation. A quick way to fix this, is to restrict modification to all attributes that starts with nt . Make sure no important attributes you are using are not affected.

### **Example**

This ACI help secure the NtUser objectclass attributes used when synchronizing users with a NT system.

In o=captkirk.com

Add the following ACI :

```
(targetattr != "userPassword || telephoneNumber || nt*")(version 3.0; acl "Allow self entry modification Protecting posixAccount attributes"; allow (write)userdn = "ldap:///self";)
```

### **PAM authentication via LDAP**

PAM LDAP module use the posixAccount objectclass attributes to get is information. A list of specific attributes is available at

[http://docs.iplanet.com/docs/manuals/directory/schema/oc\\_hpu12.htm - 1278312](http://docs.iplanet.com/docs/manuals/directory/schema/oc_hpu12.htm - 1278312)

### **Risk**

Some of the information is uidNumber and gidNumber and all attributes can be changed their values and set their uid and gid to 0. This basically let user become who ever they want on the system that relies on the Directory server for credential information

### **Solution**

By rejecting the uidnumber and gidnumber from the ACI that control the user access to is information, he wont be able to change is user level on the sytem using PAM LDAP for authentication.

### **Example**

This ACI make sure the uidnumber and gidnumber attribute can't be written by the users.

```
(targetattr != "uidnumber || gidnumber || nt*")(version 3.0; acl "Allow self entry modification Protecting posixAccount attributes"; allow (write)userdn = "ldap:///self";)
```

## Useful Tools

### LDAPRootDSE

This tool dump the root DSE content of LDAP v3 compliant servers.

This tool can be found at <http://www.smugline.net/zorky/ldap/ldaprootdse/>

### NetscapeGetACL

This tool tries to grab ACL rules in Netscape Directory servers.

This tool can be found at <http://www.smugline.net/zorky/ldap/netscapegetacl/>

### LDAPMiner

This tool tries to collection information various types of LDAP servers by identifying the type of server then fetching specific information.

This tool tries to grab ACL rules in Netscape Directory servers.

This tool can be found at <http://www.smugline.net/zorky/Ldapminer/>

### John The Ripper

This tool is use to crack the Netscape Directory SHA password. You will need the SHA patch by K Evangelinos .

This tool tries to grab ACL rules in Netscape Directory servers.

This tool can be found at <http://www.smugline.net/zorky/ldap/netscapegetacl/>

John the Ripper is available at <http://www.openwall.com/john/>

The netscape directory password support is available at

<http://www.bastard.net/~kos/john-sha/>