Enumeration of AS/400 users via POP3

Overview

The POP3 service is installed on all modern AS/400 and iSeries servers, and is turned on by default, even in cases when email serving was not set up. To access a POP3 server, you must authenticate and provide a user and a password. Unfortunately, the POP3 users represent real AS/400 user profiles, POP3 will authenticate any valid user profile, and the service provides too much information during authentication.

Details

Let's select a random list of names and passwords, connect to POP3 with a telnet client of your choice, and try to authenticate. Here is what a POP3 session with an AS/400 server looks like:

```
+OK POP3 server ready
USER bogus
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF2204
USER qsysopr
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF22E2
USER jdavid
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF22E3
USER rbenny
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF22E4
USER qspl
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF22E5
USER SCARMEL
+OK POP3 server ready
PASS myrealpwd
+OK start sending message
quit
```

The following table summarizes the server's responses:

User	**Response**	**Meaning**
bogus	Error CPF2204	User profile not found
qsysopr	Error CPF22E2	Good user, password not correct for user profile
jdavid	Error CPF22E3	Good user, bur user profile is disabled
rbenny	Error CPF22E4	Good user, but password for user profile has expired
qspl	Error CPF22E5	Good user, but no password associated with user profile
scarmel	OK	Good password, good user

The POP3 gateway provides us with yet another way to verify the existence and validity of AS/400 user profiles and passwords. In contrast with Telnet, this method will not disable the terminal device because there is no device. This behavior is similar to that of FTP, which also does not disable the client after unsuccessful login attempts. However, the amount of information disclosed by the server is significantly higher than that of FTP. An automated tool can easily create a list of valid user profiles and of their current status on the server, providing a vector for a social engineering attack.

Another factor that is relevant to the POP3 technique is the lack of exit programs associated with the service. Most other services that demand user authentication can be associated with a user-defined exit program that runs whenever the protocol is used. Unsuccessful log in attempts are logged only in the security audit journal, and only if it is turned on. This lack of control makes POP3 the easier anonymous way to enumerate and list the user profiles.

Vulnerable Systems:

OS/400 versions greater than or equal to 4.5.

Previous versions display an uninteresting generic message "-ERR Logon attempt invalid".

Countermeasures:

The POP3 service is very rarely used on iSeries servers, and therefore should be stopped and disabled from starting.

More information about AS/400 vulnerabilities and about AS/400 security issues can be found in the "Hacking iSeries" book, at www.venera.com