Kako zaštititi korisnika da ne oda lozinku

Poticaj za ovaj članak došao je nakon u zadnje vrijeme učestalih poruka u kojima se - pod krinkom službene osobe zadužene za e-mail sistem - od korisnika traži da proslijede svoje korisničko ime i lozinku.

Citat dijela poruke:
...
If your inbox becomes too large, you will be unable to receive new email. Just before this message was sent, you had 18 Megabytes (MB) or more of messages stored in your inbox on mail. To help us re-set your SPACE on our database prior to maintain our INBOX, you must reply to this e-mail
and enter your Current User name ( ) and Password ( )
...
Ovo je klasični primjer za "žicanje" osjetljivih osobnih podataka. Pojava je u žargonu poznata kao phishing ***[1]***.
Ne možemo se pouzdati u to da korisnici nisu toliko naivni da nasjednu, pogotovu stoga, jer se u posljednje vrijeme kriminalci da bi bili uvjerljiviji obraćaju korisnicima i na njihovom maternjem jeziku, doduše uz vrlo loš računalni prijevod poruke, ali ipak - nikad se ne zna.

Sa stanovišta sistemca, možda bi bilo zanimljivo, vidjeti u prvom redu koji su korisnici dobili malicioznu poruku. To se može učiniti ili analizom log datoteka (CARnet Debian: /var/log/mail), ili pretraživanjem korisničkih e-mail direktorija po kritičnim ključnim riječima. Za ovo drugo možemo se poslužiti slijedećom perl skriptom:

```
#!/usr/bin/perl
#by lcavara (at) ttf.hr
$path= "/home/$user/Maildir/*";
print "Usage: <script_name> <keyword>\n"
if !$ARGV[0];
exit if !$ARGV[0];
open(PASSWD,"/etc/passwd");
while (<PASSWD>) {
chop;
@F = split /:/;
$user = $F[0] if $F[2] > 500 && $F[2]
#you can exclude some users in the next line
!= 1000 && $F[2] != 65534;
$keyword = $ARGV[0];
#path to users mailbox directory
$path= "/home/$user/Maildir/*";
my $mail =
`grep -R -l $keyword $path 2>/dev/null`;
print "\n$ARGV[0] found in\n$mail" if $mail;
}
```

Ova skripta će pretražiti sve primljene poruke svih korisnika na poslužitelju po nekoj ključnoj riječi i dati naziv poruke i ime korisnika, kod kojeg je nađena. Iz pretraživanja su isključeni samo za sistem rezervirani kor. računi čiji je ID manji od 500. Sistemski korisnik *nobody* čiji je ID 65534 te bilo koji drugi korisnik po želji isključi se u 13 redku skripte. Recimo da želimo naći sve poruke, kojima je pošiljatelj *afisk@foster-miller.com* pokrenemo gornju skriptu:

```
ztk:~/skripte$ sudo perl search_usermail_by_keyword.pl foster-miller
```

Nakon čega dobijemo npr. ispis:

```
foster-miller found in
/home/hpatacic/Maildir/cur/1237431846.24950_0.ztk:2,S
/home/mehoh/Maildir/cur/1237431884.25179_0.ztk:2,S
/home/mantolic/Maildir/cur/1237431887.25195_0.ztkr:2,S
ztk:~/skripte$
```

Pogledajmo zaglavlje neke od nađenih poruka:

```
ztk:~/skripte$ sudo head -50 /home/hpatacic/Maildir/cur/1237431846.24950_0.ztk:2,S| g
rep -B10 Subject:
        Thu, 19 Mar 2009 04:01:34 +0100 (CET)
Received: from mailfrm.foster-miller.com (mailfrm.foster-miller.com [65.209.22.144])
        by ztk.ttf.hr (Postfix) with ESMTP id EC18A7FF8
        for ; Thu, 19 Mar 2009 04:01:23 +0100 (CET)
X-MimeOLE: Produced By Microsoft Exchange V6.5
Content-class: urn:content-classes:message
MIME-Version: 1.0
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Subject: Dear  e-mail user,
@ttf.hr>
```

Nakon što smo se uvjerili, da se uistinu radi o *phishingu*, možemo upozoriti korisnika na opasnost.

Postoji još mogućnost, da se MTA (Mail Transfer Agent), npr. postfix, konfigurira tako da uopće ne prosljeđuje odgovore korisnika na inkriminiranu poddomenu, odnosno na određenu e-mail adresu. Jako dobra, vrlo kratka uputa za ovaj postupak nalazi se na http://madphilosopher.ca/2006/09/how-to-send-an-entire-domain-to-dev-null-in-postfix/ [2].
Prema toj uputi (ovdje je malo prilagođena), dovoljno je da u **/etc/postfix/main.cf** dodamo redak:

```
virtual_alias_maps = hash:/etc/postfix/virtual_alias
```

a u datoteku **/etc/postfix/virtual_alias** upišemo ime poddomene, na koju ne želimo da se prosljeđuje e-mail:

```
@foster-miller.com      blackhole@localhost
```

odnosno ako ne želimo baš isključiti cijelu poddomenu, nego samo jednu konkretnu e-mail adresu, upišemo:

```
afisk@foster-miller.com      blackhole@localhost
```

Još nam samo preostaje da u **/etc/aliases** definiramo "crnu rupu" (*blackhole*) kuda će "propasti" odgovori naivnih korisnika:

```
blackhole:      /dev/null
```

ili, ako želimo vidjeti, koliko je korisnika nasjelo na *phishing*, umjesto **/dev/null** upišemo ili **root** ili **postmaster** ili svoje kor. ime, pa na taj način možemo pročitati namjeravani odgovor i korisnika upozoriti na opasnost pri odgovaranju na takve poruke.
Važno: nakon navedenih promjena u datotekama: **/etc/postfix/main.cf**, **/etc/postfix/virtual_alias** i **/etc/aliases** obvezno treba osvježiti bazu aliasa i učitati ponovo konfiguraciju *posfixa*:

```
# newaliases
# postmap /etc/postfix/virtual_alias
# postfix reload
```

Naravno, sve navedene radnje u vezi *posfixa* obavljamo ili kao **root** korisnik ili uz korištenje **sudo** prefiksa.

pon, 2009-03-30 15:38 - Luka Ćavara**Kuharice:** Linux [3]
Kategorije: Sistemci [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/543

Links
[1] http://en.wikipedia.org/wiki/Phishing
[2] http://madphilosopher.ca/2006/09/how-to-send-an-entire-domain-to-dev-null-in-postfix/
[3] https://sysportal.carnet.hr/taxonomy/term/17
[4] https://sysportal.carnet.hr/taxonomy/term/36