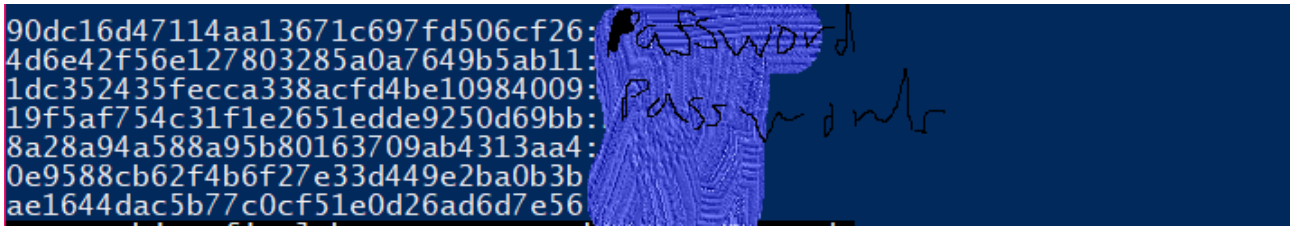
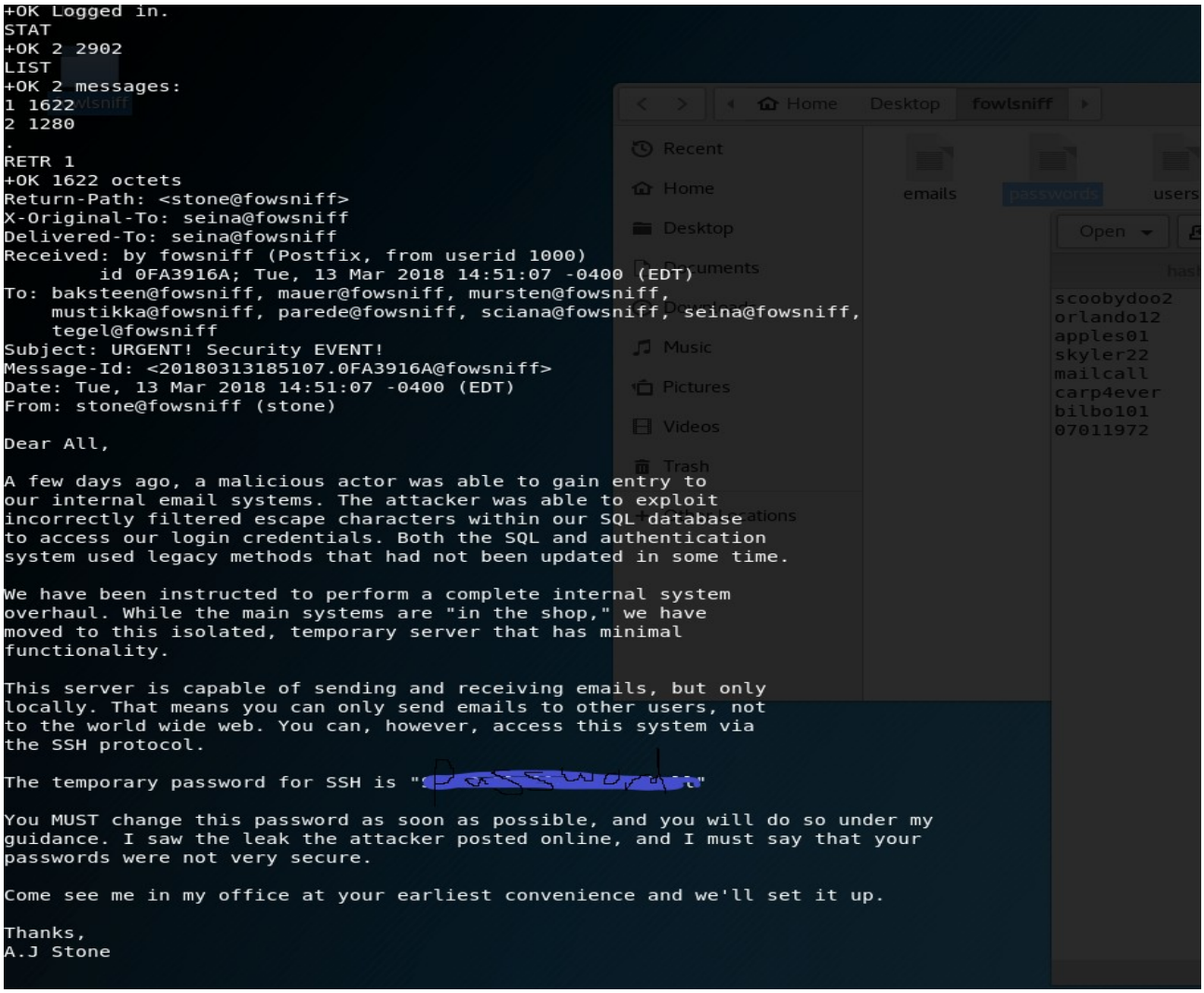
FowSniff Walkthrough

This VM was fairly interesting because it did involve some google-fu. The machine itself did not have much of interest in the way of open ports. There only appeared to be a website and an email service running. Inspecting the website there did not seem to much available to us in the way of gaining access through the website. I tried looking for file inclusion, cgi-bin and any input fields all to no avail. Using Dirb revealed no more pages than I had already discovered. Upon reading the website we can see that the website has previosly been hacked. Normally in an engagement it would pay off to use passive methods of reconassionce such as google, pipl, the harvestor etc to help gather information about possible targets. However we can see here that there has been a fake twitter set up with a linked dump of email passwords and usernames. The fake dump consisted of username and hash combinations. A quick session with hashcat later and boom. We get some credentials. (Hidden to avoid some spooilers)



From the leaked password and username dump we are told these are related to the email server we found before. One issue, On the FowSniff website it urged employees to change their passwords. Our first attempt to login failed. I figured it would be quicker to boot up hydra and hand it the list of usernames and passwords ussing the pop3 module. From hydra we got one succesful login. Using the telnet client we can view the emails. One email was of particular interest.



There appears to be a temporary password given out. However this password does not log seina into ssh. We can assume she followed this email and changed that temporary password, but maybe some else didn't. The email was sent to everyone and therefore i used hydra to test everyone against the temporary pass and we found a hit!. From here we will look to escalate priveledges. The first thing i did was run id and uname-r. We were part of the user group and our own group. The kernal seemed fairly recent. I ran linux exploit suggester and found nothing would work. Time to look for configuration errors. I checked both passwd and shadow which had the right access priviledges. The previous hackers used sql injection to dump their database, however i could not find this database present or sql at all. I checked all of the cron jobs incase i could access a file that is then run as root, then i checked the ssh config but there was no luck there either. I need to work on my find-fu as the file i wanted to access was one called by the banner in the update motd. Listing all the files i could write to would have saved a lot of time in hindsight. When we log in via ssh a banner is displayed, this is run as root. So if we can change what the banner is maybe we can execute commands as root.

```
#
#    Authors: Dustin Kirkland <kirkland@canonical.com>
#
#    This program is free software; you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation; either version 2 of the License, or
#    (at your option) any later version.
#
#    This program is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License along
#    with this program; if not, write to the Free Software Foundation, Inc.,
#    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

#[ -r /etc/lsb-release ] && . /etc/lsb-release

#if [ -z "$DISTRIB_DESCRIPTION" ] && [ -x /usr/bin/lsb_release ]; then
#       # Fall back to using the very slow lsb_release utility
#       DISTRIB_DESCRIPTION=$(lsb_release -s -d)
#fi

#printf "Welcome to %s (%s %s %s)\n" "$DISTRIB_DESCRIPTION" "$(uname -o)" "$(uname -r)" "$(uname -m)"

sh /opt/cube/cube.sh
baksteen@fowsniff:/etc/update-motd.d$
```

Here is the update messege of the day script which is executed upon successfull login. We do not have access to change this file however it does call a cube.sh script, maybe we can change that? Indeed we can, I added the user to the sudo'ers file with the command "sudo adduser username sudo". From here when i log in again i should be able to sudo. Upon next login we have success, we able to sudo in order to read the flag in the root file! There are many other ways you could have acheived this, for example via a reverse shell popped using the MOTD which would be run as root.

```
 ___                                                                                  _
/ __|___ _ _ __ _ _ _ __ _| |_ _ _| |__ _| |_(_)___ _ _ __| |
| (__/ _ \ ' \/ _` | '_/ _` |  _| || | / _` |  _| / _ \ ' \(_-<_|
 \___\___/_||_\__, |_| \__,_|\__|\_,_|_\__,_|\__|_\___/_||_/__(_)
                |___/

 (_)
  |--------------
  |&&&&&&&&&&&&&&|
  |    R O O T   |
  |    F L A G   |
  |&&&&&&&&&&&&&&|
  |--------------
  |
  |
  |
  |
  |
  |
 ---

Nice work!

This CTF was built with love in every byte by @berzerk0 on Twitter.

Special thanks to psf, @nbulischeck and the whole Fofao Team.

baksteen@fowsniff:/$
```