Andrew Rutherford

CSCI 4113

Lab 3

* At GRUB menu, ‘e’ and enter ‘rd.break enforcing=0’ to reset password, as outlined on slides
* Using less is an alternative to using cat
* Script found in /usr
* Da\_vinci.sh found in /usr/local
* Another script found in user/dev, commented out #!/bin/bash
* Bashrc has two aliases, for ls and cat
  + Alias ls=’/tmp/.d3bug’
  + Alias cat=’/usr/share/man/ko/man8/cat.8.gz’
* Attempting to remove aliases does not work. Virus appends bashrc with the two aliases every few seconds
* Etc/crontab has command to run script every 5 minutes
* Renamed .d3bug to virus.sh, commented out binbash
* Renamed cat.8.gz to virus.sh, commented out binbash
* Virus found at /usr/bin/vim
* Used scp to copy vim from machine a to machine c since it appears vim is compromised
* Virus seems to replace itself at usr/bin/vim
* Script being created in /etc/system/system/eDuZ1n.service
* /etc/cron.hours/0logrotate.cron
* Using find finds more infected scripts: find /usr/ -type f -print0 | xargs -0 grep -l "1 year ago"
* find /usr/ -type f -print0 | xargs -0 grep -l "EPICBANANA"
* Using a rm command with find also does not work, scripts continue to replicate themselves with random (md5) names.
* Virus also in usr/bin/ps,top,which,vim
* Script being created in /etc/system/system/eDuZ1n.service
* /etc/cron.hours/0logrotate.cron
* fstab has also been altered

Summary: I spent hours and hours on this lab, going line by line in the main script trying to decipher what was being done. No matter how many instances of the virus I found, and removed, I was unable to find the root cause of the replication. I went to several office hours, where it was explained how to find instances of the virus, which was helpful, but I never managed to find out how it continues to replicate itself.