Round 2 Ubuntu Documentation Zeus – 11/12/2021

**Things we noticed at the start:**

* Doing the forensics
* Don’t change the password of the main user
* Machine configured to host OpenVPN server
* Didn’t prompt for sudo password

**Forensics Questions 1:**

* Find an identifier in file service.crt
* Locate server.crt
  + /etc/openvpn/server.crt

**Forensics Question 2:**

* Find IP address range of a virtual network tun0
* Installed net-tools and used ifconfig
* Second IP address seen in ifconfig
* Answer: 10.14(didn’t get full IP address)/24 <- bits

**Forensics Question 3:**

* Find a rogue pearl script
* Use locate \*.pl did not work.
* Used tree, did not work.
* Checked user’s home directory, did not work
* Directory popularity-contest seems sus.
* owl\_shell.pl as answer.
* Back door was in /opt/ericbus/

**Starting the fixing of the image:**

* Changed updates to daily
* Checked users
* PASSWORD: 0ld$cona2021!
* Changed Firefox settings to the most secure
  + Send do not track requests
  + Block pop-ups
  + Make Firefox the default browser
* Keep Sigil and Calibre apps
* sudo snap install shattered-pixel-dungeon
* sudo apt purge imagemagick
* removed hacking tools.
* Remove ftp and twoftpd
* Changed password policy
* Checked sudoers file
  + Added Defaults rootpw
* Use locate \*.png – nothing
* Use locate \*.jpg - nothing
* Use locate \*.mp3 - nothing
* Use locate \*.mov - nothing
* Use locate \*.mp4 - nothing
* Use locate \*.gif - nothing
* Use locate \*.mpeg - nothing
* Check etc for hacking tools
  + Found nothing
* Used locate \*.txt
* Found Easy-RSA
  + Easy RSA is part of OpenVPN
* Checking groups
  + Groups command did not help
* Tried installing ClamAV – nothing
* Used dpkg -l. Created a long list where we manually went through it:
  + Removed goldeneye
  + Found a game zangbang, removed it gave error: not installed.
  + Removed netcat-openbsd – gave points
  + DO NOT REMOVE OPENSSH
* Restarted snap
  + Fixed snap service by re-installing dungeon game.
* Remove packit
* Remove popem
* Removed telnet
* Remove themole
* Sudo visudo
* Used grep “^\s\*linux” /boot/grub/grub.cfg - nothing
* Secure ports using commands
* Change sudoers file
* Removed root privileges on OpenVPN – got us points
* Used sudo systemctl disable opensmtpd.service
* Editing PAM fields
* Deleted no-password-login group
* Changed OpenVPN logging system.

**Made By Rohan Bhargava**