\_pi-adv

August 19th, 2024

Linux Gameplan

Based on the Aperture Science Ubuntu, and Bloons TD 6 Image

Preface

This gameplan is made for competition use only and use at your own risk when doing another image. Read any README carefully and make corrections to this document accordingly. This is still very much new so expect more efficient and crafted gameplans in the future.

Gameplan

Make1 – Gathering Information

Gathering information is crucial to the success of your team. You’ll need a couple of things.

* Gather information from the README
  + Users
  + Required Programs
  + Need to update Programs
  + Critical Services
  + Any other crucial information for the image.
* Look at the operating system
  + Look around on the operating system to see if you can find anything to help.

Make2 – Forensic Questions

Starting out, just glance at these. Unless you absolutely know that you can answer a forensic question,

save it for later and make note if you have to save a user, or a certain file for later use.

Make3 – Apps & Scripts

Next is getting rid of random scripts on the system. Especially in the Aperture Science there is a script that runs every 5-10 minutes after starting the image that starts a timer and will shutdown the image. Scan the operating system for any sort of script and either delete it or quarentine it. Look in these common directories to find a script (if there is one):

* /etc/ (common subdirectories like apt/)
* any /home/ directory
* /lib/.(hidden directory)/

Common apps to remove are:

* Wireshark
* Nginx
* ophcrack
* hydra
* john

Make4 – Users, Password & Groups

Consult the README but make sure to remove and add the proper users on the system. Of course modify the groups as needed and change any insecure passwords.

Popular commands:

* Make a new user:
  + sudo adduser \_\_\_\_\_\_\_\_
* Change password of a user
  + sudo passwd \_\_\_\_\_\_\_\_
* Add user to a group
  + sudo usermod -aG \_\_groupname\_\_ \_\_user\_\_\_

Make5 – Forensic Questions \*Again

Now is the time to crack open a web browser and analyze the forensic questions deeper than the previous check. Make sure to take your time, this presumably will take some time to do.

Make6 – Configuring Critical Services

This has a couple parts to it.

1. Configure the settings of your services (example shown of openssh)
   * Use the /etc/ssh/ssh\_config and /etc/ssh/sshd\_config to configure settings.
   * For example: In the ssh\_config file, and sshd change the port number to another port than just 22.
2. Updating the Service
   * Simply just run a sudo apt install \_\_\_\_\_\_ command to update the service.
3. Start the Services
   * You can start the service by running sudo systemctl start \_\_\_servicename\_\_\_
   * You can also set a service to run automatically at startup but it’s not required. The only program that you can do this quickly on if ufw.

Make7 – Updates

This is pretty simple to do just a few things to knock off.

1. Set the automatic updates in the ‘Updates & Software’ app and go to the ‘Updates’ section
2. Run the sudo apt update and sudo apt upgrade commands to update the software on the machine.

Make8 – PAM

The only thing that is tough is figuring out what will and what won’t break the computer so I suggest doing these last unless you absolutely have to do them.

1. Common-auth configuration
   * Add or change the following to the file:
     + auth [default=die] pam\_faillock.so authfail
     + auth sufficient pam\_faillock.so authsucc
2. pmquality configuration
   * Add or change the following to the file:
     + minlen=10
     + ucredit=-1
     + lcreadit=-1
     + ocredit=-1
     + dcredit=-1
     + dictcheck=1
     + usercheck=1
3. Common-password configuration
   * On the pam\_unix.so line add the remember=5 argument

Make9 – Login.defs configuration

A couple of changes need to be done to this file. Open the /etc/login.defs file.

1. LOGIN\_RETRIES 5
2. PASS\_MAX\_DAYS 120
3. PASS\_MIN\_DAYS 30

Make10 – sysctl.conf

The sysctl.conf file seems to deal with all sorts of network settings for the computer. More detailed things like ipv4/ipv6 cookies and spoofing protection. Open the /etc/sysctl.conf file.

1. **Uncomment the following**
   * net.ipv4.tcp\_syncookies=1
   * net.ipv4.conf.all.accept\_source\_route=0
   * (ADD THIS LINE) net.ipv4.conf.default.accept\_source\_route=0
   * net.ipv4.conf.all.send\_redirects=0
   * (ADD THIS LINE) net.ipv4.conf.default.send\_redirects=0
   * net.ipv4.conf.all.log\_martians=1
   * net.ipv4.conf.default.rp\_filter=1
   * net.ipv4.all.rp\_filter=1
   * net.ipv4.conf.all.accept\_redirects=0
   * net.ipv4.conf.default.accept\_redirects=0
   * (ADD THIS LINE) kernel.randomize\_va\_space=12
   * (ADD THIS LINE) kernel.exec-shield=1
2. **Comment the following**
   * net.ipv4.ip\_forward=1