0 - Debian 10 - Bloons TD 6

Difficulty: `0`

OS : `Debian 10`

Main User: `dartmonkey`

Created By: `Mobmaker`

Table of Contents:

Prohibited software has been removed

How to secure:

Firefox blocks dangerous downloads

How to secure:

Forensic Question 1 is correct

Points: `7`

How to secure:

1) Run the command `id snipermonkey`
2) Find the user's `uid`, and read the number
3) Put the UID in `Forensic Question 1` located on the desktop.

Forensic Question 2 is correct

Points: `7`

How to secure:

1) Read `/etc/ssh/sshd_config`
2) Find `Port ##`, and read the numbers
3) Put port number in the answer in `Forensic Question 2` located on the desktop.

Forensic Question 3 is correct

Points: `7`

How to secure:

1) Think about who made this.

2) Put that answer in `Forensic Question 3` located on the desktop.

Removed unauthorized users

Points: `5` each

How to secure:

1) Run the command `getent passwd {1000..6000}`
2) Read the resulting list of users, and compare them to the readme.
3) Run `sudo deluser [user]` for every discovered unauthorized user.

Ensure correct administrators

Points: `5` each

How to secure:

1) Read `/etc/group`
2) Check the `sudo` group and compare against admins in the readme.
3) If someone is an unauthorized administrator, run the command `sudo gpasswd -d [user] sudo`
4) If someone should be a user but isn't, run the command `sudo usermod -aG sudo [user]`

Change insecure passwords

Points: `4`

How to secure:

1) Run `sudo passwd [user]` for every user, and follow the prompts. You do not need to do this for dartmonkey

Create user in readme

Points: `5`

How to secure:

1) Run `sudo adduser [username]` and follow the prompts

Uncomplicated Firewall (UFW) has been enabled

Points: `6`

How to secure:

1) Install UFW (`sudo apt install ufw`)
2) Enable UFW (`sudo ufw enable`)

FTP has been uninstalled

Points: `6`

How to secure:

1) Uninstall FTP with `sudo apt purge vsftpd`

The system automatically checks for updates daily

Points: `5`

How to secure:

1) Open "Software & Updates"
2) In the "Updates" tab, set "Automatically check for updates:" to "Daily"

Important security updates are selected

Points: `5`

How to secure:

1) Open "Software & Updates"
2) In the "Updates" tab, check "Security updates (buster/updates)" under "Install updates from:"

OpenSSH root login disabled

Points: `6`

How to secure:

1) Edit `/etc/ssh/sshd_config`
2) Set `PermitRootLogin` to "no"

Prohibited files have been removed

Points: `4` each

How to secure:

1) Open Nautilus, and search the `/home` directory until you delete all of the unauthorized files.

Prohibited software has been removed

Points: `4` each

How to secure:

1) Find all installed packages with `sudo apt list --installed`
2) Delete unauthorized packages with `sudo apt purge [package]`

Firefox blocks dangerous downloads

Points: 6

How to secure:

1) Open Firefox's settings
2) Go to "Privacy & Security"
3) At the bottom, check "Block dangerous and deceptive content" and all sub-checks