Topics on *FreeBSD* virtual machine

1. A non-empty password for the user *root*
2. Create group *animals*

   Hint - Handbook/Users and Basic Account Management chapter 3.3
3. Create a users *dog*, *cat*and *fox* in the group *animals*, first name and surname *"Rex Barks"* for user *dog*, *"Felix Meow"* for user *cat* and *"Sly Fox"* for user *fox*, home directory with rights `0700`, shell `/bin/sh`, password like login

   Hint - Handbook/Users and Basic Account Management chapter 3.3
4. Edit the main configuration file `/etc/rc.conf`:

   ```
   hostname="HOSTNAME_FROM_TABLE"              # replace
   ifconfig_em0="DHCP"
   ifconfig_em1="inet 192.168.56.201/24"
   ifconfig_em2="inet IP_AND_MASK_FROM_TABLE"  # replace
   sshd_enable="yes"
   growfs_enable="yes"
   ```

   if above there are some extra lines, then rewrite them as well and *reboot* your machine

   . . . FROM_TABLE means table
5. Check your VM's internet connection to the world and bi-directional connection to the host, it is recomended to disable firewall *pf* on *FreeBSD VM*

   ```
   #  pfctl -d
   ```

   and similarly try to disable the firewall on the host machine (*Windows*, *Linux*, *macOS*, . . .)
6. Configure the *SSH server* (*sshd*, file `/etc/ssh/sshd_config`) changing option for remote user *root* login, via a *private/public* key pair only:

   ```
   PermitRootLogin   prohibit-password
   ```

   Remember to reload the service:

   ```
   # service sshd reload
   ```

   Hint - Handbook/OpenSSH chapter 16.7
7. Generate *SSH* keys for all users (*root*, *dog*, *cat* and *fox*) algorithms: *ecdsa* and *ed25519* (no passwords)

   ```
   $ ssh-keygen -t ecdsa
   $ ssh-keygen -t ed25519
   ```

   Hint - Handbook/OpenSSH chapter 16.7

8. Connect via *ssh* (use *Putty* and *PuttyGen* on *Host* and/or *ssh-keygen ...* on *VM*) **Host-> Guest** as users *dog*, *cat* and *fox* without passwords, using a *private/public key* pairs

9. Connect via *ssh* (use *Putty* and *PuttyGen* on *Host* and/or *ssh-keygen ...* on *VM*) **Host-> Guest** as user *root* without password (mind the `PermitRootLogin prohibit-password` option in *sshd* configuration file), using a *private/public key* pair

10. Setup web server `nginx` and try to enable *PHP* processor

```
# pkg install nginx php84-extensions
...
# # adjust nginx configuration file, especially php section:
# ee /usr/local/etc/nginx/nginx.conf
...
```

add two extra lines to `/etc/rc.conf` file:

```
nginx_enable="yes"
php_fpm_enable="yes"
```

and start new services:

```
# service php_fpm start
# service nginx start
```

Hint - adjust almost ready configuration sampels in `/usr/local/etc/nginx` *VM* directory and/or Nginx documentation

11. Check *WWW* connections **Host-> Guest** (by browser, url: `http://192.168.56.201` or/and `http://192.168.56.201/info.php`)

```
# cat /usr/local/www/nginx/info.php
```

```
<?php
    phpinfo();
    exit( 0 );
?>
```

12. For the web server `nginx` setup the OpenSSL self-signed certificate and check secure/encrypted *HTTPS* connections **Host-> Guest** (by browser, url: `https://192.168.56.201` or/and `https://192.168.56.201/info.php`) adding *unknown issuer* browser-exception.

    Hint - review the chapter: Handbook/OpenSSL, chapter 16.8

Extra, self-studying topics - for higher grade (> 4.0)

1. Add extra two lines to the main configuration file `/etc/rc.conf`:

```
pf_enable="yes"
pflog_enable="yes"
```

and reboot machine

2. Setup firewall *PF* (*PacketFilter*), configuration file `/etc/pf.conf`, *block/pass* for some selected services like *ssh, http, https*

   Hint - review the chapter: Handbook/Firewalls/PF Packet Filter, chapter 33.3

3. Try to defend against malicious attacks (DDoS attacks) on *ssh* service, by blocking such IP addresses (apply `max-src-conn` and `max-src-conn-rate` *pf* rules options)

   Hint - review the chapter: Handbook/Firewalls/PF Packet Filter, chapter 33.3

Preparation of the environment, uploading work

1. Logins and passwords for the new *Linux* machine *pass.math.uni.lodz.pl* (replaces the *xor* machine) one can find in *USOSweb*: *Student's section/Final Grades/Winter Semester/2024-25/Security of Computer Systems/("details" button)*

2. It is recomended to disable firewall *pf* on *FreeBSD VM*

   ```
   #  pfctl -d
   ```

   and similarly try to disable the firewall on the host machine (*Windows*, *Linux*, *macOS*, ...)

3. Start your *FreeBSD* virtual machine, log as *root* user and after completing the above tasks, execute the command:

   ```
   #  fetch https://pass.math.uni.lodz.pl/make.sh
   ```

   now you have script *make.sh* in the current directory, so you can run next command:

   ```
   #  sh  make.sh  STUDENT_NUMBER  LOGIN_FROM_USOSWEB
   ```

   first time you should type *yes* to confirm keys, then provide the password from USOSweb. Do not type hash '#' in above commands (this is PROMPT only!)

4. Now upload tiny presentation about security in *pdf* format (filename: *STUDENT_NUMBER.pdf*) with command (e.g. with command prompt on Windows):

   ```
   scp  STUDENT_NUMBER.pdf  LOGIN@pass.math.uni.lodz.pl:LOGIN/passing.d/
   ```

   (LOGIN is your login from USOSweb) again, first time you should type *yes* to confirm keys, then provide the password from USOSweb.

5. Wait for evaluation (few days).