CHEAT-SHEET Leonardo competition

Capiaghi Ludovico - Unige 22/23

A Strategy???

- ssh all virtual machines (hosts)
    - change all password
- connect to OPNsense
    - change root password
- look for all services listening on ports (netstat -anp | grep -v 127.0.0.1)
    - eliminate dangerous one
- OPNsense:
    - create floating substitute (**floating on every interface but WAN)**
    - create rules for every service (that need to be accessible from WAN)
    - disable floating
    - look for other users/group that have access to firewall
- SERVICES:
    - client (with chrome and libeoffice)
        - be able to restart them with systemd in case they are stopped
    - server www:
        - look at site code and phpmyadmin if present
        - check if the db is hosted on srv-intranet in case change passwords
    - dns:
        - open configuration file and look for problems

    - srv-intranet
        - look site code and configuration
        - check DB, in case change password
-
- **REPORT**
    - when services are down/some one is losing points (dashboard) : register time to then access logs in opnsense

General commands

- Connecting to a host with shh

```
ssh [user]@[ipaddr]
```

- Best way of listing files

```
ls -la
```

- Change a user password

```
passw [user]
```

- Kill a process with a certain pid

```
kill [pid]
```

- Kill a process with a certain name

```
pkill [name]
```

- Changing permission on a file

```
Possible permission: r +  w + x
Possible subjects: owner- group - others
```

```
Add with "+"
Remove with "-"
```

    - adding execution (x) to everyone

```
chmod +x [filename]
```

    - adding execution (x) to owner (user)

```
chmod u+x [filename]
```

    - adding execution (x) to group

```
chmod g+x [filename]
```

    - adding execution (x) to others

```
chmod o+x [filename]
```

- Find details about current users

```
id
```

- Change user

```
su [new_user]
```

- Adding, deleting, modify users

```
useradd
userdel
usermod
```

- Look for users and groups info in:

```
cat /etc/passwd
cat /etc/groups
groups [user]
```

- Systemd

```
sudo systemctl start [service]
sudo systemctl stop [service]
sudo systemctl restart [service]
```

LOGS

Logs are in

```
/var/log
```

> auth.log -> ssh

OPNsense

- Default credentials:
  - Username: root
  - Password: opnsense
- Useful part of the interface:
  - **Lobby/Password:** changing the password
  - **System/Access:** control users (access)
  - **System/Audit** (set debug mode): control log after attack
  - **Interfaces/Virtual IPs:** understand which public ip firewall exposes
  - **Firewall/NAT:** port forward and one to one configuration
  - **Firewall/Rules** (floating): RULES
  - **Firewall/Log Files/Live View:** logs in real time
- Console

```
pfctl -e
pfctl -d
```

Services and ports

Listing services bind to ports

```
netstat -anp
```

Removing the useless ones (internal)

```
netstat -anp | grep -v 127.0.0.1
```

List of standard service for a port

```
cat /etc/services | grep [port]
```

DNS

Test dns (try to resolve a name into an ip)

```
nslookup
host [name]
```

Local configuration for dns in `/etc/resolve.conf`

- DNS server:

  > Look which service is running on 53 (probably is bind ...see in /etc/services)

  Configurations in `/etc/bind` , then look at the configuration files (`named.conf` and similar)

  > Find the real configuration files...something like this

  ```
  root@srv-ns:/etc/bind# cat db.leodardo.ii
  $TTL    3600
  @       IN      SOA     ns.leodardo.ii. root.leodardo.ii. (
                                3         ; Serial
                           604800         ; Refresh
                            86400         ; Retry
                          2419200         ; Expire
                           604800 )       ; Negative Cache TTL
  ;
  @       IN      NS      ns.leodardo.ii.

  @   IN  A   198.51.100.101
  ```

```
www     IN      A       198.51.100.101
ns      IN      A       198.51.100.100
fw  IN  A   203.0.113.2
```

@ means empty string

Services...

APACHE (Web Server)

Available sites in `/etc/apache2/available-sites`, default is `/var/www/html`

Apache configuration in `/etc/apache2/apache2.conf` (look for directory permission...)

Webmin

Hosted on `10000`, it is really **dangerous**

MySql

Find the host where the DB is hosted, it could not be the web server (attention not to break the services modifying the DB)

Launch mysql

```
mysql
```

Useful queries

```
show databases;
show tables from "db_name";
```

Wordpress

Wordpress configuration should be in `[folder_hosting_the_site]/wp-config` so normally it is `/var/ww/html/wp-config`

PhpMyAdmin

> Control site-availabe and check for an include...

```
/etc/phpmyadmin
/etc/phpmyadmin/config.php #useful configuration
```