[WIP] Training - Basics Linux configuration

Loïc Delestra

Training subject

You need two VMs. A kali and a lubuntu.
With two connections for both (NAT and internal)

In your Lubuntu

update packages

sudo apt-get update; sudo apt-get upgrade
sudo apt-get install openssh-server

Fail2ban

- install fail2ban in your lubuntu.
- sudo apt-get-install fail2ban
- **Look** the configuration file /etc/fail2ban/jail.conf. And create a configuration to limit ssh try to 2 and ban for 20 secondes.
  - sudo vi /etc/fail2ban/jail.d/defaults-debian.conf
    ```
    [sshd]
    enabled = true
    maxretry = 3
    bantime = 20
    ```
  - restart fail2ban service
    -sudo service fail2ban restart
  - test fail login from kali and check your log in the lubuntu /var/logs/auth file

firewall

sudo vi /etc/init.d/firewall.sh
sudo chmod a+x /etc/init.d/firewall.sh
sudo update-rc.d firewall.sh defaults 20
sudo /etc/init.d/firewall.sh

//check if fail2ban is working

Up-to-date

install and use unattended-upgrades

https://wiki.debian.org/UnattendedUpgrades

logs

Use rsyslog to send your log from lubuntu to kali.
http://www.thegeekstuff.com/2012/01/rsyslog-remote-logging

Some folks prefer to use logwatch and send report by mail
Logwatch for mailing
https://doc.ubuntu-fr.org/logwatch

install http

Install apache2
Add an ipforwarding in the virtualbox interface, forward the port 80 from guest to 8080 to host.

Update your firewall rules

DOS

try some basic DOS with your kali. Use hping3

Simple DOS protection

Try a simple dos protection
http://blog.nicolargo.com/2012/02/proteger-son-serveur-en-utilisant-fail2ban.html

Useful tools

Netstat

Print network connections

-t –tcp
-u –udp
-a –all Show both listening and non-listening (for TCP this means established connections) sockets
-e –extended Display additional information
-p, –program Show the PID and name of the program to which each socket belongs.

Lsof

List Open File (root).
-i [i] This option selects the listing of files any of whose Internet address matches the address specified in i

To list all open IPv4 network files, use:
lsof -i 4 -a

Fuser

File user. Identify processes using files or sockets
-n space. Select a different name space. The name spaces file (file names, the default), udp (local UDP ports), and tcp (local TCP ports) are supported.
-v Verbose mode. Processes are shown in a ps-like style. The fields PID, USER and COMMAND are similar to ps.
sudo fuser -v -n tcp 22

Logger

write log in syslog

Traceroute

Tail -f