ANNEX A · PRACTICAL 6.7 · GUARDS FOR THE OFFICE SERVER

Name: _____ **Date:** _____

The rule. You scan and test **only your own VMs**. Never the school network, a classmate's machine or a website.

`ubu-srv` (`192.168.122.10`, `ssh srv`) is the server; `deb-lab` plays the outsider. Take a snapshot of `ubu-srv` first.

Task 1 — The before picture. On `ubu-srv`, start the installs. On `deb-lab`, scan your server.

```
sudo apt update && sudo apt install -y fail2ban clamav lynis        # on ubu-srv
sudo apt install -y nmap && nmap 192.168.122.10                          # on deb-lab
```

Open ports before: _____

DONE WHEN you have the list, and you can name the service behind each port.

Task 2 — The firewall. On `ubu-srv`. Allow SSH **before** you enable.

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow OpenSSH
sudo ufw allow from 192.168.122.0/24 to any app Samba
sudo ufw allow from 192.168.122.0/24 to any port 2049 proto tcp comment 'NFS'
sudo ufw allow from 192.168.122.0/24 to any port 631 proto tcp comment 'printing'
sudo ufw allow 8080/tcp comment 'Tramuntana Git web'
sudo ufw allow 2222/tcp comment 'Tramuntana Git ssh'
sudo ufw enable
sudo ufw status verbose
```

DONE WHEN `status verbose` says `deny (incoming)`, and from `deb-lab` these still work: `ssh srv`, `ls /mnt/projects`, `curl -I http://192.168.122.10:8080`.

Task 3 — fail2ban. Create `/etc/fail2ban/jail.local` with `sudo nano`:

```
[sshd]
enabled  = true
maxretry = 3
findtime = 10m
bantime  = 15m
```

```
sudo systemctl restart fail2ban
sudo fail2ban-client status sshd
sudo fail2ban-client set sshd banip ADDRESS-OF-DEB-LAB      # then try ssh from deb-lab
sudo fail2ban-client set sshd unbanip ADDRESS-OF-DEB-LAB    # and try again
```

What happened to `ssh` from `deb-lab` while banned? _____

DONE WHEN the jail `sshd` lists one banned IP, and after `unbanip` you can connect again.

Task 4 — Updates by themselves.

```
cat /etc/apt/apt.conf.d/20auto-upgrades
sudo unattended-upgrade --dry-run --debug | head -n 8
```

DONE WHEN both lines of the file end in `"1"` and the allowed origins include one that ends in `-security`.

Task 5 — Antivirus. Create the harmless EICAR test file in a share (paste the line from Google Classroom), scan, then quarantine.

```
echo 'X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*' > ~/eicar.com
sudo cp ~/eicar.com /srv/samba/dev/
sudo clamscan -r /srv/samba
sudo mkdir -p /root/quarantine && sudo clamscan -r --move=/root/quarantine /srv/samba
```

DONE WHEN the first scan says `Eicar-Test-Signature FOUND` and after the second the file is no longer in the share.

Task 6 — The after picture and the verdict. Scan again from `deb-lab`, then audit on `ubu-srv`.

```
nmap 192.168.122.10                              # on deb-lab
sudo lynis audit system --quick                # on ubu-srv, read the end
```

Open ports after: _____

Hardening index: _____ Two suggestions worth doing: _____

Utility	What it stops	What it does NOT stop	Keep it?
ufw			
fail2ban			
Automatic updates			
ClamAV			

DONE WHEN the two scans differ, you can explain every port that is still open, today's entry is in `~/server-log.md` and **line 11** of the project checklist is ticked.

Hand in `practical-6.7-surname.md` on Google Classroom by Monday 17/05, 23:59: the commands, the outputs (both scans, `ufw status verbose`, the jail status, the ClamAV summary), and the table above in your own words. **Marking (10):** scans 1.5 · ufw 2.5 · fail2ban 1.5 · updates 1 · ClamAV 1 · evaluation 1.5 · report 1.

EXIT TICKET Circle one answer.

1. You enable ufw with "deny incoming" and forget to allow SSH while connected by SSH. What happens?
a) nothing changes b) ufw refuses to start c) you are locked out of the server
d) only the password stops working

2. What does fail2ban read to decide a ban?
a) the logs of failed logins b) the files in the shares c) the list of open ports
d) the list of pending updates

3. ClamAV finds malware by…
a) closing ports b) counting failed logins c) asking the user
d) comparing files with signatures of known malware

4. After your work, `nmap` shows port 22 as open. Is that a mistake?
a) yes: a firewall must close every port b) no: the server offers SSH, and keys protect that door
c) yes: fail2ban should have closed it d) no: nmap cannot see through ufw