ANNEX A · DOMAINS AND DIRECTORY SERVICES · PRACTICAL 6.6 (PART 1)

Name: _____ **Date:** _____

PART A · WORKSHEET (IN PAIRS)

1. 12 people must be able to use any of 12 PCs in a workgroup. Local accounts needed: _____

2. In that workgroup Marta changes her password. Number of changes: _____

3. "Which server is the controller of this domain?" The PC asks with: _____

4. "Prove that you are Marta, without sending the password to the file server": _____

5. "Which groups is Marta a member of?" The question is asked with: _____

6. The PC's clock is 20 minutes late and logins fail. Which protocol refuses? _____

7. The server that holds the directory is called the: _____

8. NetBIOS name of our domain: _____

PART B · PRACTICAL 6.6, PART 1 · BUILD THE DOMAIN CONTROLLER `DC1`

Domain `tramuntana.internal` · realm `TRAMUNTANA.INTERNAL` · NetBIOS name `TRAMUNTANA`. Your teacher ticks the boxes today; keep this sheet, the report is handed in after part 2.

1 · The VM. virt-manager → New VM → Import existing disk image → `dc1-base.qcow2` · Ubuntu 26.04 · 2048 MB · 1 CPU · name `dc1` · network `default`. Log in (user and password on the board). Run `ip -br a`. My interface: _____ `ubu-srv` is `192.168.122.10`; **`dc1` will be `192.168.122.20`**.

2 · Name and fixed address. `sudo hostnamectl set-hostname dc1`. Then, as on 14/04: `sudo nano /etc/netplan/60-static.yaml` with the text below (your interface; spaces, not tabs), `sudo chmod 600 /etc/netplan/60-static.yaml`, `sudo netplan apply`:

```
network:
  version: 2
  ethernets:
    enp1s0:
      dhcp4: false
      addresses: [192.168.122.20/24]
      routes:
        - to: default
          via: 192.168.122.1
      nameservers:
        addresses: [192.168.122.1]
```

In `/etc/hosts` (`sudo nano`), **replace** the line that starts with `127.0.1.1` by:

```
192.168.122.20 dc1.tramuntana.internal dc1
```

☐ **Done when:** `hostname -f` prints `dc1.tramuntana.internal`, `ip -br a` shows `192.168.122.20`, `ping -c 2 debian.org` works and `sudo grep -n '^%admin' /etc/sudoers` prints **nothing**.

From now on you can work from your host: `ssh sysadmin@192.168.122.20`.

3 · Packages and services.

```
sudo apt update
sudo apt install -y samba-ad-dc krb5-user bind9-dnsutils
sudo systemctl disable --now smbd nmbd winbind
sudo systemctl mask smbd nmbd winbind
sudo systemctl unmask samba-ad-dc
sudo systemctl enable samba-ad-dc
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.orig
```

☐ **Done when:** `ls /etc/samba` shows `smb.conf.orig` and no `smb.conf`.

4 · Provision the domain. Capital letters matter.

```
sudo samba-tool domain provision --use-rfc2307 --interactive
```

`Realm:` **TRAMUNTANA.INTERNAL** · `Domain [TRAMUNTANA]:` Enter · `Server Role [dc]:` Enter · `DNS backend [SAMBA_INTERNAL]:` Enter · `DNS forwarder IP address:` **192.168.122.1** · `Administrator password:` at least 7 characters, with capitals, small letters and digits. Write it here: _____

☐ **Done when:** the command ends with a summary. DNS Domain: _____ NetBIOS Domain: _____

5 · The DC becomes its own DNS client. Start it.

```
sudo systemctl disable --now systemd-resolved
sudo unlink /etc/resolv.conf
printf 'nameserver 127.0.0.1\nsearch tramuntana.internal\n' | sudo tee /etc/resolv.conf
sudo cp -f /var/lib/samba/private/krb5.conf /etc/krb5.conf
sudo systemctl start samba-ad-dc
```

6 · Is it alive? `systemctl status samba-ad-dc`

☐ **Done when:** it says `active (running)`. If not: `journalctl -u samba-ad-dc -n 30` and read.

7 · Verify: find, prove, look up. Copy every output into your notes for the report.

```
host -t SRV _ldap._tcp.tramuntana.internal.
host -t SRV _kerberos._udp.tramuntana.internal.
host -t A dc1.tramuntana.internal.
dig +short debian.org
kinit Administrator
klist
smbclient -L localhost -N
```

☐ **Done when:** LDAP's SRV record gives port _____ and host _____ · Kerberos' SRV record gives port _____ · `klist` shows a ticket for `krbtgt/` _____ · `smbclient` lists the shares _____ and _____

8 · The domain's password policy, and a snapshot. `sudo samba-tool domain passwordsettings show`

Minimum password length: _____ Maximum password age (days): _____ Then `sudo poweroff` and, in virt-manager, a snapshot of `dc1` called `dc-ready`.

☐ **Done when:** the snapshot exists, and today's entry is in `~/server-log.md` on `ubu-srv` (the new machine, its address, the domain names, your checks).

Teacher's ticks (10): ☐ name + address 2 ☐ provisioned 2 ☐ SRV + A records 2 ☐ Kerberos ticket 2 ☐ forwarder + snapshot 2

EXIT TICKET

☐ **1.** In a domain, where does Marta's account exist?
A) On every PC B) On her own PC only C) Once, in the directory on the domain controller D) In a file she carries

☐ **2.** How does a PC find the domain controller of `tramuntana.internal`?
A) It asks DNS for SRV records B) It tries every address C) It reads `/etc/hosts` of the DC D) It asks Kerberos

☐ **3.** What does a Kerberos ticket let Marta do?
A) Read any file B) Prove who she is to a service without sending her password
C) Change the policy D) Find the DC

☐ **4.** Logins fail on one PC only. Its clock is 15 minutes late. Why does that matter?
A) DNS needs the time B) LDAP is slow C) It does not matter D) Tickets are only valid within 5 minutes of clock difference

☐ **5.** Which protocol is used to ask the directory "which groups is marta in"?
A) DNS B) LDAP C) SMB D) DHCP