7 Cybersecurity (fms27)

A Linux-based server hosts containers from various users. Each container has its own IP address. Users in group `webdev` may define host-level port redirects by adding a line with container IP, external port and internal port to the plain text file `/var/cfg/port/map.txt`. For example, the line "`12.34.56.78 80 8080`" requests that traffic for 12.34.56.78:80 be sent to 12.34.56.78:8080.

A root cron job regularly runs the bash script `/usr/local/bin/ptfwd` shown below, which creates the requested port mapping for each line of `/var/cfg/port/map.txt`. [*Note:* The bash builtin `read [variable ...]` reads a line from stdin, splits it into whitespace-delimited fields, and assigns the first field to the first variable, the second field to the second variable, and so on. If there are more fields than variables, the remaining fields and delimiters are assigned to the last variable. A backslash (\) removes any special meaning for the next character.]

```
while read IP EXTPORT INTPORT; do
    bash -c "/usr/sbin/iptables -t nat -A PREROUTING -d $IP -p tcp \
        --dport $EXTPORT -j DNAT --to-destination $IP:$INTPORT"
done  </var/cfg/port/map.txt
```

The following files and directories are on the system.

```
drwxr-xr-x 2 root  admin   4096 Aug 18  2020 /usr/local/bin
-rwxr-xr-x 1 root  root     209 Jan 15  2020 /usr/local/bin/ptfwd
drwxr-xr-x 2 root  admin  36864 Sep 23  2024 /usr/sbin
-rwxr-xr-x 1 root  root  224424 Apr  8  2024 /usr/sbin/iptables
drwxrwxr-x 2 bob   staff   4096 Apr 12  2016 /var/cfg
drwxr-xr-x 2 root  admin   4096 Apr 12  2016 /var/cfg/port
-rw-rw---- 1 root  webdev  3484 Dec  8  2025 /var/cfg/port/map.txt
```

(*a*) Give a complete description of a privilege escalation attack through which user `alice`, who is in group `staff` but not in `webdev`, `admin` or `root`, gains the ability to run arbitrary commands as root. First, clearly describe the overall strategy. Second, for each step of the attack, specify: (i) the exact Linux command the attacker executes, (ii) what the command accomplishes. [8 marks]

(*b*) Identify the critical vulnerabilities in the above configuration. Justify your answer by showing what step(s) of your attack in Part (*a*) would stop working if each vulnerability were eliminated, without impairing the desired functionality. For each identified vulnerability, describe how to remedy it. [8 marks]

(*c*) Consider now user `charlie`, who is in group `admin` but not in any of the others, and user `daria`, who is in `webdev` but not in any of the others. For each, if the attack is possible, repeat Part (*a*); else, convincingly argue that no such attack

is possible. [4 marks]