Quiz 1)

Quiz 1-1) What is the primary purpose of the DYLD_PRINT_TO_FILE environment variable introduced in OS X 10.10?

I think (B) is the correct answer.
The purpose of this environment variable is to redirect the dynamic linker’s log output to a specified file.

Quiz 1-2) What actions can an attacker perform by exploiting the DYLD_PRINT_TO_FILE vulnerability?

Due to the lack of essential security checks in this feature, environment variables can be used even in Set-UID root binaries.
If this Set-UID mechanism is exploited, an attacker may be able to create or modify files in arbitrary locations on the system with root privileges, leading to a serious security vulnerability.

Quiz 1-3) How did the DYLD_PRINT_TO_FILE vulnerability in OS X Yosemite enable adware like VSearch to gain unauthorized root access and install itself without user consent?

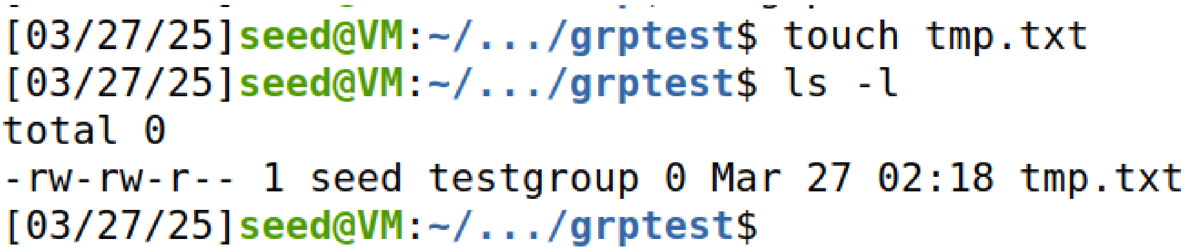
As mentioned above, due to the lack of environment variable validation, Set-UID programs running with root privileges could write logs to attacker-specified files with root access.
Adware like VSearch took advantage of this to overwrite critical system files with root privileges and install itself without the user's consent.

Quiz 2)

Quiz 2-1) Please explain the meaning of chmod 6777 grptest command.

This command sets the permissions for the grptest directory.
The first digit, 6, is the sum of Set-UID (4) and Set-GID (2), which grants both special permissions.
When the file is executed, it runs with the owner’s privileges and also retains the group’s privileges.
The 777 means that anyone can read, write, and execute the file.
In conclusion, this command makes the file executable and editable by anyone, but it runs with the owner’s and group’s privileges.

Quiz 2-2) Examine the permissions, ownership, and group of the created tmp.txt file, and explain the reasons behind these attributes.



```
[03/27/25]seed@VM:~/.../grptest$ touch tmp.txt
[03/27/25]seed@VM:~/.../grptest$ ls -l
total 0
-rw-rw-r-- 1 seed testgroup 0 Mar 27 02:18 tmp.txt
[03/27/25]seed@VM:~/.../grptest$
```

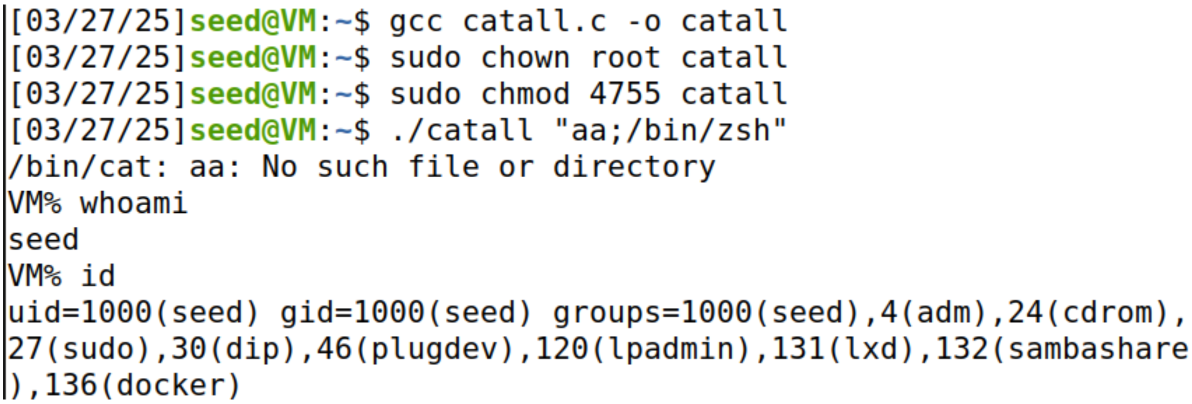
When checking the permissions of the tmp.txt file, the Set-UID and Set-GID bits were not set.
The owner (seed) has read and write permissions, and the group (testgroup) also has read and write permissions.
Other users have read-only access.

Since the currently logged-in user is seed, the file's owner is set to seed.
Because the user's default group is testgroup, the file's group is also set to testgroup.

These permissions are determined by the system's default umask setting.
If the default umask value is 002, the default permissions for newly created files will be rw-rw-r--.

Quiz 3)

The following code is the catall.c file used in Lab2) Task2.



```
[03/27/25]seed@VM:~$ gcc catall.c -o catall
[03/27/25]seed@VM:~$ sudo chown root catall
[03/27/25]seed@VM:~$ sudo chmod 4755 catall
[03/27/25]seed@VM:~$ ./catall "aa;/bin/zsh"
/bin/cat: aa: No such file or directory
VM% whoami
seed
VM% id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),
27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare
),136(docker)
```

In the case of Dash, when executing a Set-UID binary, Dash applies its own environment variable security policy.

As a result, unsafe operations may be denied or executed with downgraded privileges.

Because of this, even though /bin/zsh was launched, it did not run with root privileges, but instead with the privileges of the regular user.