Computer Security 1, COMPGA01, 2011-12

Answer ALL questions. 2.5 hours.

Correct answers should be short, straightforward and clear, rather than long and obscure.

Marks for each part of each question are indicated in square brackets

Calculators are NOT permitted

Question 1. Questions about theory and mathematical models.

1. What is an order relation? Is a relation over integers where each element is related only to itself an order relation? Is it also a lattice?

   [5 marks]

2. Given a poset $A, \leq$ give an exact **mathematical** definition of LUB (defined as a certain element of a certain set satisfying certain properties). Explain the acronym LUB.

   [5 marks]

3. Let $\mathbb{N}, |$ be a poset where $|$ is the division relation. Show that $|$ is not a total order. Compute $LUB(5,12)$ and $GLB(4,6)$.

   [5 marks]

4. Given a lattice of type $C = P(Cat)$, and a totally ordered set of classifications H write a definition of the Bell-LaPadula product lattice.

   [5 marks]

5. Can one make a program that always says Y when a file contains a virus?

   [5 marks]

[Question 1.6 is on the next page]

6. In Biba's integrity model we have three integrity levels
   $L = \{Untrusted(UN) < UserSpace(US) < SystemHigh(SH)\}$. Imagine that files on a USB stick are at the $Untrusted(UN)$ level, user files and third-party software such as Adobe Acrobat on a PC are at the $UserSpace(US)$ level, and the OS runs at the highest integrity level. Consider the following set of categories

   $$Cat = \{SensitiveWorkFiles(S), PersonalData(P)\}.$$

   Let Bob be a subject with $\lambda(Bob) = (SH, \{S\})$ and let $\lambda(document1) = (UN, \{P\})$. Imagine that Bob runs Adobe Acrobat and tries to open document1 to read it.

   Is this operation allowed with the strict Biba model?

   Is this operation allowed with LWM = Low Water Mark policy for subjects?

   What happens with the Integrity Audit policy?

   [5 marks]

[Total 30 marks]

Question 2. Small questions about OS and computer security.

1. What is the meaning of the exe permission for directories in Unix?

   [5 marks]

2. Explain what sticky bit is. When does it apply?

   [5 marks]

3. In Unix, when an ordinary process is run by a user, does it have the access rights of the user, or the rights of its owner? Give one example of an executable which has additional privileges and behaves differently.

   [5 marks]

[Questions 2.4-2.8 are on the following pages]

4. Consider the following Unix file listing:

```
bash> ls -l /etc/shadow
-rw-r-----  1 root shadow  680 Dec  16 22:02 shadow
```

Is it possible to be able to run a dictionary attack on the passwords of all users, this without obtaining root access? Explain why.

[5 marks]

5. Give just one example how the hard drive file system affects the security in a multi-user setting.

[5 marks]

6. In Windows implementation of Access Control Lists (ACL's), each object (example file) has a security descriptor, which contains a list of Access Control Elements (ACE) objects. What kind of data does one ACE contain? Are these ACE objects stored in the object's directory of the hard drive, in system directories, user data files, in RAM, or in the registry?

[5 marks]

7. Explain how in compiled C code, a program will call a sub-routine, and store some pointers on the stack using PUSH and PULL instructions, and how this can be exploited to run arbitrary code.

[10 marks]

8. State the main objective of Memory Protection in modern PCs. Explain in which cases data in some parts of the memory can be prevented from being executed. Is Internet Explorer 8 run under windows Vista likely to be protected against execution of assembly code injected in a buffer allocated on the stack?

[5 marks]

[Total 45 marks]

Question 3. Consider the network illustrated in the Figure on the next page. We want to configure a simple stateless firewall with 3 zones. It should be a simple packet filter which inspects the IP and TCP headers and has no memory of previous packets. It should be able to prevent connections from being initiated from the 'wrong' side by checking if a certain appropriate flag in the header of packets is set. It should enforce the following policies:

1. any external client is allowed to connect to the Web server via the https protocol (tcp/443);
2. subnet1 is allowed to connect to the FTP server via the ftp protocol (protocol=tcp/port=21 for commands; tcp/20 for data);
3. any internal machine is allowed to connect to the Web server with ssh (tcp/22);
4. packets coming from the Internet showing a source IP included in the Internal IP addresses must be explicitly denied;
5. any other connection (both directions) not explicitly authorized by the rules must be blocked (for example telnet, mail http and many other types of insecure traffic are banned).

Implement this policy by filling a table with a certain number of firewall rules such as the example given. The correct answer expected contains a total of 10 rules.

Direction	IP Source	IP Dest	Protocol	Port Source	Port Dest	Flag ACK	Action Taken
Internet →DMZ	any	34.123.145.6	TCP	$\geq$1024	443	any	permit
Intranet →DMZ							

[The figure appears on the next page]

[Total 25 marks]

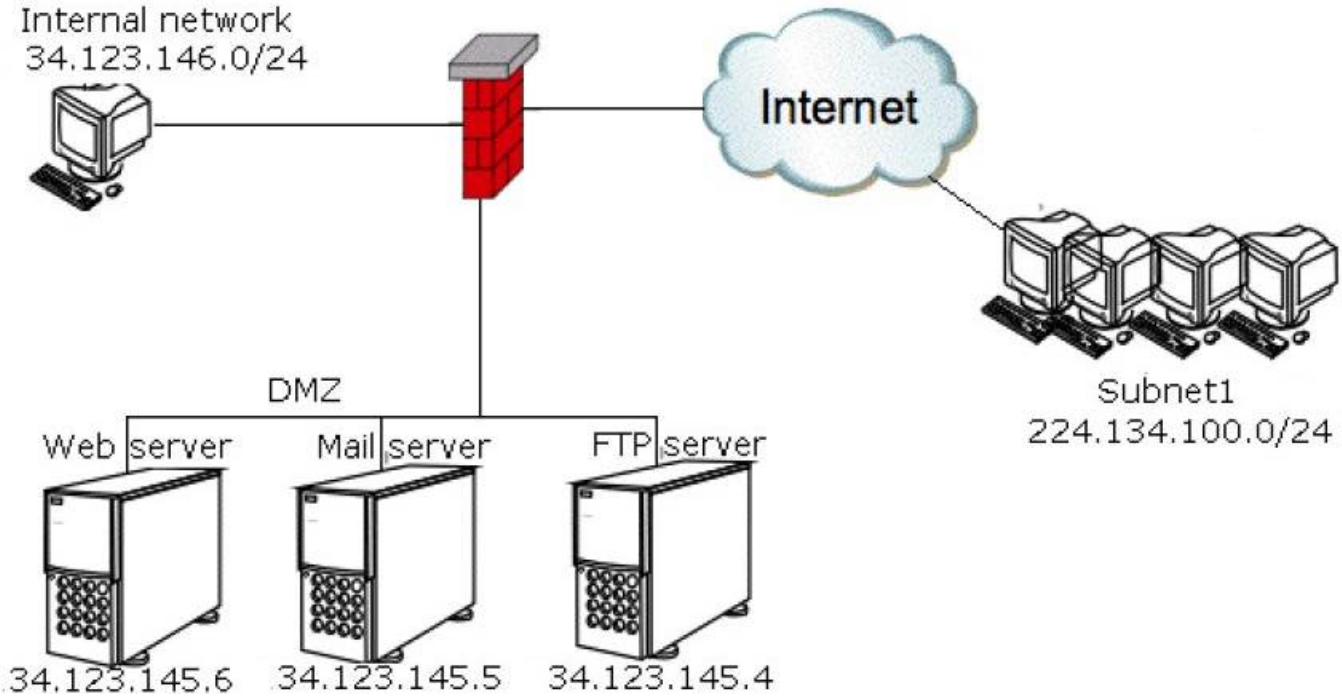

Figure 1: The network for Question 3.

[Total For The Whole Exam 100 marks]

END OF PAPER