Written Questions

Jack Eadie

jeadie

20865679

Question 1

Part A

I) Cannot read StudentPresentation.pdf because {slides, exams, marks} is not a subset of {assignments, exams, marks} (slides is not in {assignments, exams, marks}). Cannot write for similar reasons

ii) Can read Quiz1.csv as professor ≥ TA and {marks} is a subset of {assignments, exams, marks}. Cannot write down, for inverse reasons (Alice dominates Quiz1.csv).

Iii) Cannot read StudentReportMarked.mp3 as, although Professor ≥ student, {slides, marks, evaluations} contains evaluations which is not in {slides, exams, marks}. Alice does not dominate StudentReportMarked.mp3. Cannot write because StudentReportMarked.mp3 does not dominate Alice.

iv) CourseOverview.sql dominates Alice (Course Coordinator ≥ Professor and {assignments, exams, marks} a subset of {assignments, exams, marks, evaluations}). Alice can write to CourseOverview.sql but not read.

v) Alice dominates Assignment4.exe (professor ≥ professor and assignments in {assignments, exams, marks}). Alice can read assignment but cannot write.

Part B

I) Bob's integrity changes to (Professor, {exam, marks})

ii) record2 integrity stays at (TA, {marks}) as Professor ≥ TA and {exam, marks} ≥ {marks}

iii) Bob's integrity changes because Professor ≥ Student, {feedback, marks, evalua-

tions} & {exam, marks} == {marks}. Bob's integrity is (Student, {marks})

iv) record4 loses integrity to Bob's level: (Student, {marks})

v) record5 loses integrity to Student and since {marks} & {exams} is empty, record5 becomes (Student, {}).

Question 2

Part A

Least privilege is not enforced because *“Administrator accounts are given privileges to operate in read, write and execute modes on all objects”*.

Part B

If Charlie runs an unsigned program as administator then it has the ability to access and execute any file. If the program turns out to be a virus or malware, then Charlie and Bob cannot have the same degree of trust in the system because any arbitrary change could have been made by the unsigned program to the system. Therefore any assumption, such as when access controls are set discretionarily by the user they are infact set, cannot be safely trusted; the malware could have changed this operation to only appear as if access controls are working.

Part C

This service violates the fail safe principle. It should not default to read, write and execute permissions unless a more restrictive policy is applied. A fail safe principle would do the opposite: no permissions are assigned by default unless a more open permissions is provided.

Part D

This design violates the OS principle of Least Common Mechanism. The design does not constrain possible security issues (such as invalid inputs that could reduce system availability) in a way that provides a minimal mechanism to communicate between subsystems. An error or failure in the validation should not propgate outside to other children processes. Instead, any failures should be contained within the single processes. Children processes should be able to survive whilst the larger service restarts. By providing a smaller mechanism for this communication the currently, children thread could become standalone and thus not affected by parsing errors and only communicated with via validated data.

Question 3

Assume preexisting infrastructure/network topology is as specified in diagram for Part C (i.e. use this topology for all parts, not just part C).

Part A

The packet filtering gateway can detect packets from within the private networks which has source addresses not in 172.16.100.0/24 or 172.16.101.0/24 and vice versa (packets from the internet that have sources in these subnet mask). This however, cannot stop spoofing within the private network (i.e. a packet coming directed to an address in the private network, with a spoofed source address).

Part B

For criterion 1, the firewall will need to drop all packets with destination IPs in the domain 172.16.100.0/24. Thus, no external traffic can connect to the experiment computers and server yet the work stations can. For the second criterion an application proxy would be required, that way the traffic from the private network can be inspected and any malicious destination addresses can be dropped (using a whitelist, of course). The last criterion can be achieved by an application proxy via requiring user authentication. Thus any remote login operations (SSH, RDP, etc) can be logged.

Part C

No. Traffic from the work computers to the experiment computers, for example, will go via switch 2 -> Router -> Switch 1 -> Experiment Computers. The firewall would not receive these packets and therefore not be able to control any access.

Part D

Direction	**Protocol**	**Source**	**Port**	**Destination**	**Port**
Out	TCP	172.16.100.0/24	22	172.16.101.0/24	22
In	TCP	172.16.101.0/24	22	172.16.100.0/24	22

Part E

Adding intrusion detection systems to the network both host and network based would improve the security. Host based IDS would be beneficial, especially on the server and experiment computers as this is where a significant amount of data and processing are done. Malware on these computers thus pose additional risk. Network based IDS would benefit the configuration more broadly.

Depending on how valuable the data and research is to a potentially malicious actor (as compared to an interested third party whom can just wait for results in published papers), a honeypot may be useful to detect these intrusions. A high interaction server could be setup, either outside the two private networks, but still behind the router and firewall or could be within the existing private networks. Mock data and processing, in this scenario, would not be difficult to construct by the research team.

Part F

The research team should consider deploying their public webserver in a demilitarised zone (DMZ) topology. This would entail adding an additional firewall and router. This external firewall is then responsible for protecting the DMZ specific services (i.e. the public web server) and the first router then directs traffic to either the internal firewall (that should be configured as previously discussed) or onto the new public webserver. This would still allow private network specific protections for the experiment and work computers whilst having more relaxed restrictions for public traffic accessing the webserver. Further, if the webserver is maliciously targeted, it too still has to breach the internal firewall.