CS458 Assignment 2

Name: Darren Poon
uWaterlooID: dyhpoon
Student Number: 20311433

1a) Alice can read: D102, D104
Alice can write to: D101, D105.

1b)
i – Alice reads from D101.
Read: D101.
Write: None.
Alice's integrity level: (Secret, {Visa, MasterCard, EuroCard}).

ii – Alice writes to D102.
Read: D101.
Write: D102.
Alice's integrity level: (Secret, {Visa, MasterCard, EuroCard}).

iii – Alice reads from D103.
Read: D101, D103.
Write: D102.
Alice's integrity level: (Secret, {Visa, MasterCard, EuroCard, Discover}).

iv – Alice writes to D104.
Read: D101, D103.
Write: D102, D104.
Alice's integrity level: (Secret, {Visa, MasterCard, EuroCard, Discover}).

v – Alice writes to D105.
Read: D101, D103.
Write: D102, D104, D105.
Alice's integrity level: (Secret, {Visa, MasterCard, EuroCard, Discover}).

2a) The store clerk can identify Alice by asking her name, and she can authenticate Alice by asking Alice to show her driver license or student card, in order to prove herself.

b) Yes, the music store could still able to effectively identify Alice. Since purchasing CD through the website usually requires users to have their own user accounts, and the website could identify Alice by asking Alice to provide her account name or user ID. On the other hand, the website could authenticate Alice by asking Alice to insert her password when she logs in to her account.

c) The credit card provider can identify Alice by asking her name, and authenticate Alice by asking her to provide the correct credit card number, card security code (CSC), and other information to the provider.

d)
i – Alice can identify the owner of the website by looking at the name, and logo of the website.
ii – Alice can authenticate the owner of the website by looking at the url address carefully, or Alice can check if the web have the correct IP (by looking at the DNS).
iii – If Alice fails to properly authenticate the owner, and she logs in to the fake website. Then her account name, and password might sent to the attacker. This is also known as phishing attack.

e)
i – The website can identify Alice by asking of her credit card number or user ID.
ii – The website can authenticate Alice by asking Alice to provide the correct password, and asking security questions that Alice knows which she provided to the real website when she created her account (ex. When were you born?).
iii – If the credit card issuer does not properly authenticate Alice, an attacker may try to authenticate as Alice, and transfer all the money away from Alice's account.

3a)
Complete mediation: This rule is clearly violated. The web application does not check the user input, so an attacker can provides a crafted website name and execute malicious html or javascript code.

Fail-safe defaults: Fail-safe defaults are violated. The web application allows every user to submit a URL without any password. To be more specific, the web page's namebox and urlbox are disabled if user is not logged in. However, any user can still submit a URL by providing a crafted URL to the web server.

Least privilege: Least privilege is violated in the web application. Since an attacker can create more votes (more than one) to each URL. Therefore, this improper use of privilege ruins the voting system of the web application.

Separation of privilege: the web application violated this rule because the application does not require two or more conditions to be met in order to get access. We can also bypass the authentication to submit a URL.

4a) If there is only room in the budget for a single firewall, I would place the firewall on the database server. Since the database server interact with most of the users, this including user from the web site, internal users, as well as applications on the desktop computers of company employees. Therefore, placing the firewall on the database can be more effectively than other places.
If there is more budget for a second firewall, I would place it on the web site which is hosted on its own server. Since placing the firewall on the web server can examine and filter out most of the packets from the internet, and reduce the burden of the database server's firewall.

b) A user can bypass the firewall to access YouTube by using a proxy server. Even though YouTube's IP addresses were banned from all uWaterloo machines, but proxy servers outside uWaterloo have different IP addresses which are not banned, and we can use it to connect to YouTube. Therefore, students in uWaterloo can still connect to YouTube through proxy servers.

c) By blocking all packets originating from within uWaterloo whose source address is not of the form 129.97.x.y, it prevents an outside attacker spoofing the address of an internal machine within uWaterloo.
By creating a rule to block traffic originating from outside of uWaterloo whose source address is of the form 129.97.x.y, it prevents an attacker within uWaterloo network performing from spoofing attacks against external machines.
However, an internal machine in uWaterloo can still spoof traffic to another machine in uWaterloo, e.g. performing a denial of service attack whose source address and destination address is 129.97.x.y within uWaterloo.

5a) The name for such systems are honeypots. A real-world example of one of these systems is Honeyd. Honeyd is a low-interaction honeypot developed by Niels Provos.

b) Prevention: To deceive or deter attackers.
Detection: To detect attacks or unauthorized activity.
Information gathering: log the activities, capture new viruses or worms for study.

6a) The signature-based IDS keeps a list of all known problems, and it compares with the malicious crafted URLs. It exhibits low false positive rate because it is relatively easy to specify signatures to a known attack by signature-to-signature comparisons.

b) In order to make a native system administrator disable the Snort signature, a clever attacker might try to spoof the naïve system administrator that there are many false positive errors in Snort by supplying non-malicious crafted URLs.
To avoid the attacker's own IP address to be noticed while he carries out this attack, an attacker may choose to use a proxy server.

c) The false positive rates advertised for security software like antivirus and IDS are only based on normal usage only, and the "abnormal" usage of false positive are ignored.

d) The attacker can undetectably exploit the IIS bug by using polymorphism to URLs, so that a different signature is generated, and it is undetectable by the Snort rule in place.