CS458 Assignment 2

Name: Ron Ng Jian Ying

UWaterloo UserID: r32ng

Student Number: 20801876

Written Response Questions

Q1a)

```
//Drops all packets connecting to IRC server
DROP 0.0.0.0/0 ==> 72.36.115.175 ALL PORTS BY UDP/TCP

//Only allows St. Pierre & Miquelon spies to SSH into our
server
ALLOW 70.36.0.0/20 ==> 72.36.115.150 PORT 23 BY TCP

//ALLOW AGENTS TO ACCESS IRC
ALLOW 72.36.115.128/28 ==> 72.36.115.175 PORT 6667 BY TCP

//Allow DIFFIDENT MOLE to connect to IRC
ALLOW 56.172.1.164 ==> 72.36.115.175 PORT 6667 BY TCP


//Game Server Access
ALLOW 0.0.0.0/0 ==> 72.36.115.175 PORT 4700 to 4799 BY UDP
ALLOW 72.36.115.175 ==> 0.0.0.0/0 PORT 4761 BY UDP


//Web Access for Agents
ALLOW 72.36.115.128/28 ==> 0.0.0.0/0 PORT 0-1023 BY TCP
ALLOW 72.36.115.128/28 ==> 0.0.0.0/0 PORT 0-1023 BY TCP
ALLOW 72.36.115.128/28 ==> 0.0.0.0/0 PORT 0-1023 BY TCP
ALLOW 72.36.115.128/28 ==> 0.0.0.0/0 PORT 0-1023 BY TCP
ALLOW 72.36.115.128/28 ==> 0.0.0.0/0 PORT 0-1023 BY TCP
ALLOW 72.36.115.128/28 ==> 1.1.1.1 PORT 0-1023 BY TCP and UDP
ALLOW 1.1.1.1 ==> 72.36.115.128/28 PORT 53 BY TCP and UDP

//Webpage Access from Internet
ALLOW 0.0.0.0/0 ==> 72.36.115.150 PORT 80 BY TCP
ALLOW 0.0.0.0/0 ==> 72.36.115.150 PORT 443 BY TCP
ALLOW 0.0.0.0/0 ==> 72.36.115.150 PORT 21 BY TCP
```

```
DROP RESET //Denies all packets that are not covered by above
rules
```

Q1b)
Yes, it's possible as all agents' machines are able to access the web allowing GROUCHY PUMA to transfer files via FTP to dump data. The rule required to prevent GROUCHY PUMA from releasing data to the outside world is

```
DROP 72.36.115.191 ==> 0.0.0.0/0 ALL PORTS BY UDP/TCP
DROP 0.0.0.0/0 ==> 72.36.115.191 ALL PORTS BY UDP/TCP
```

The rule should be placed at the very top as rules at the top override all other rules below it

Q1c)
No. Two reasons:

1. The IRC channel is hosted on the same server as the COMPETITIVE ONLINE GAME server. Anyone who uses a packet sniffer would be able to see the IRC packets.

2. Since the IRC isn't secured by TLS/SSL, the packets aren't encrypted and are in plain text.

Measures to take would be to move the IRC channel to a separate IP and machine as well as to use TLS/SSL to encrypt the packets.

Q1d)
The firewall does not protect against black hole attacks. Black hole attacks are caused by malicious routers dropping all packets flowing through it instead of routing it to its destination which in this case would be our website.

Q1e)
Yes. The adversary could perform an MITM attack where all packets between our servers and the source can be analysed. Using this, the adversary could, for example, read a packet and pass it on or modify it before passing it to the server/source and the end-to-end machines would be none the wiser.

Q1f)
Advantage:
More machines can be connected to the central node easily thereby increasing the network size with minimal effort.

Disadvantage:

The gateway node is a single point of failure. If it fails, all machines in the network would be isolated from one another as well and the outside world.

Q2a)

i) Read only
ii) Both
iii) Write only
iv) Both
v) Neither
vi) Neither
vii) Read only
viii) Neither

Q2b)

Executive > Management > Developer > Customer Support > Public

Subject: (Management, {ϕ, υ, ρ, η})

Object: D413 (Executive, {ϕ, υ, ρ, χ})

	OBEISANT QUOKKA	Object
Initial	(Management, {ϕ, υ, ρ, η})	D413 (Executive, {ϕ, υ, ρ, χ})
Write D413 (Empty string)	(Management, {ϕ, υ, ρ, η})	D413 (Management, {ϕ, υ, ρ})
Read D513	(Developer, {ϕ, υ, ρ, η})	D413 (Management, {ϕ, υ, ρ})
Write D413	(Developer, {ϕ, υ, ρ, η})	D413 (Developer, {ϕ, υ, ρ})
Read D553	(Customer Support, {ϕ, η})	D413 (Developer, {ϕ, υ, ρ})
Write D413	(Customer Support, {ϕ, η})	D413 (Customer Support, {ϕ})
Read D200	(Public, {Ø})	D413 (Customer Support, {ϕ})
Write D413	(Public, {Ø})	D413 (Public, {Ø})

Q3a)

The format `$id$salt$encrypted` means that the hash `$1$$353881A96DE856756C3FA8C1DD24A40C` was generated with md5crypt.

Q3b) No it is not secure. MD5crypt is no longer collision resistant due to advancements in technology. This means that brute force attacks can crack the hash of MD5 in very little time with COTS GPUs. [1]

http://phk.freebsd.dk/sagas/md5crypt_eol.html

Q3c) Yes there is a weakness. Refer to Q3a, the notation shows that no salt was used in hashing the password. Not salting the password means anyone with access to a pre-computed hash table would be able to decrypt the password.

Q3d) The password is `diffident`

Q3e) The company can introduce Two-factor authentication such as by sending a One-Time Password to the customer's mobile phone to ensure that the users logging in are legitimate.

Q3f)

1 in 5,000 users are illicit

4,999 users are licit. Amongst those, 1% are false positives.

So the program detects 1 + (4,999 * 1%) = 1 + 49.99 = 50.99 illicit users detected per 5000 users.

The actual probability that one of the users are illicit is 1/50.99 ≈ 0.019611

It is therefore not a good decision to adopt this system as out of 50.99 illicit users detected per 5000 users in the system, only 1.96% of the users are actual illicit users.

Around 98% of alerts will be false positives.

Programming Response Questions

Q1ciii)

We can use prepared statements instead of relying on sanitizing user input. Prepared statements make use of variables that are passed in after a developer defines the SQL code.

For example, the SQL statement "`SELECT Username FROM Users WHERE Password = ?`" would first be written. The question mark indicates a variable to be passed in later.

By separating the query syntax with query data, should the user attempt to pass in a query like "`'password' or ''=''`", the query would be executed by finding a password in the User table that is literally "`'password' or ''=''`".

Q2c)

Same-origin policy (SOP) prevents scripts from one domain to access data from another domain if they do not have the same origin i.e. Scripts on twitter.com cannot access data on facebook.com since they do not have the same origin (URI, host name and port number).

It **does not protect** against XSS as the malicious script is executed on the same webpage which means it has the same origin. Because of this, SOP does not protect against XSS.

Q2d)

The specific XSS attack done in Q2 is called a Persistent/Stored XSS Attack as the malicious code is stored in the website's database.

Our XSS attack was done by inserting script tags into the HTML body of the website. To prevent this specific HTML attack, we need to escape "& < > " ' /" characters with entity encoding so the browser never interprets it as code to execute.

Q3c)

One defence that can be made against this CSRF is through the use of escape. Escaping characters like < ' " > will be encoded in a format that makes it harmless.

An example would be the script tag. Instead of allowing <script> to be placed in the HTML, <script> is used instead so that the browser does not interpret the input as JavaScript.

Q3d)

Sanitization can be used as it removes harmful tags such as <script>, <object> and <iframe> thus making the user input safe and not making the server store more information.

Q3e)

No. HTTPS just means that all communications between the host and server is encrypted which prevents MITM attacks. CSRF attacks can still be stored and retrieved from the server hence the threat is still there.

Q3f)

No. Our website does not have CORS enabled from looking at the HTTP headers. This means that SOP is in effect. XMLHttpRequests originating from outside our website would be rejected.